IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Minutes Mixed Mode March plenary Sessions 2024  11-15 March 2024 | | | | |
| Date: 2024-03-16 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Stéphane Baron | Canon | Cesson-Sévigné, France |  | [Stephane.baron](mailto:Stephane.baron)@crf.canon.fr |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meetings that took place during the IEEE 802.11 Mixed Mode March session 11-15 March 2024. The on-site location for the meeting was Denver, Texas (USA).

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**Revision:**

R0: initial revision

R1: Addition of sentence, at the end of the post Motion#40 discussion, regarding ‘no’ votes.

**1rst slot : Monday March 11th 2024, 08:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 08:01 Local time.

Agenda slide deck: [11-24-0270r1](https://mentor.ieee.org/802.11/dcn/24/11-24-0270-01-00bi-march-plenary-agenda-tgbi.pptx):

1. Reminder to do attendance

Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.

1. Review of policies and procedures.
   1. IEEE individual process slides were presented.
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 policy and participation rules.
   1. No questions
4. **Discussion of agenda 11-24-0270r1 (slide #15)**
   1. Discussion on agenda

C: Author of Doc 11-24/0579 ask to present on Tuesday AM2

C: Author of Doc 11-24/0553 indicates his document is uploaded and have no preference for the presentation time.

Chair proposes to present this doc today.

C: Author of Doc 11-24/0046 would like to present his document preferably on Thursday AM1

C: Author of Doc 11-24/0561 would like to present his contribution after 11-24/0579.

Q: Chair ask which timeslot fit for Doc 11-23/1984r3

A: After 11-24/0561 presentation on Tuesday

C: Tuesday PM2 may be used to review 11-24/0553 since the document will be presented today but cannot be voted because this is an ad-hoc session.

C: Author of Doc 11-24/068 request to present on Wednesday PM2.

* 1. Adoption of agenda by unanimous consent (33 participants online, 7 in the room).

1. **Administrative**
   1. Reminder that this session is an ad-hoc session (prior to the opening plenary)
   2. Remaining Meetings:

* Tuesday AM2
* Tuesday PM2
* Wednesday PM2
* Thursday AM1

1. **Technical Submissions**
   1. [24/0553r0](https://mentor.ieee.org/802.11/dcn/24/11-24-0553-00-00bi-proposed-spec-text-for-frame-anonymization-functions.docx): Proposed spec text for Frame Anonymization functions: Phil Hawkes

First presentation of the document specifying the usage of some FA parameters for the emitting or receiving of anonymized frames.

* + 1. Discussion

Q: in FA 10.71.4.1you should add a reference on, the retransmission clause that is described latter.

A: thank you for the comment, I add reference to the 10.71.4.7.

Q: “retransmitting functions” is a little fuzzy, I would recommend to use more precise language

A: what if we just indicate the change is described in following sections

A: ok to remove but I think this is good to keep the sentence.

C: I think the sentence around anonymization of the SN is a little complex to understand. I propose alternative text: “The transmitter shall transmit frames OTA by using the OSN value in the Sequence Number subfield of the Sequence Control field (see 9.2.4.4 (Sequence Control field)).”

A: OK.

Modification is done online accordingly.

Q: Did you ever consider simply resetting the SN / PN to 0 instead of obfuscating it?

A: Yes, but the problem is that the sequence number needs to be incremental and avoid replay, and we shall not mess up the encryption part.

A: same PN cannot be reused with the same key. this has been looked at and there is need for both parties to know the real SN and PN; those real values do not change; only the values over the air change.

Q: How does the OSN is computed?

A: There has been a couple of proposal using a dedicated functions or single function call for several parameters, but all rely on a pseudo random computation. The exact mechanism is not defined right now.

Q: Reading 10.71.7 it looks an AP cannot retransmit a frame during the TXOP?

A: We don’t want to mix FA parameters to avoid correlation

Q: For the AP this is probably not the case?

A: For the AP, if the AP do a SIFS bursting we should not mix FA parameters. But let continue this discussion offline.

Q: About reference to the 105 table and there is a sentence saying “If dot11MACPrivacyActivated is true, the counter in each sequence number space shall be set to a random number modulo 4096 when the STA’s MAC address is changed.”. What is the difference here?

A: Let me check this sentence. But here, we do not change the MAC address, only the Over The Air MAC address. So, the case is a little different. But let check it a little more. Maybe we can add a 11bi related text here (in the clause: 10.3.2.14.2 Transmitter requirements)

Q: Is the PN encrypted?

A: No, it is sent in clear in the CCMP header for instance.

Q: regarding IPN (integrated Packet Number), IPN is carried in IE called MMIE. Should we do something for this IPN case?

A: Let see that offline to see if we need to protect IPN for broadcast frames or not.

Q: I think we need more detail on when the anonymization is done

A: OK, I will check that.

No more question

Phil will prepare a new revision and come back on Tuesday.

Chair ask if anyone is ready to present

No answer.

1. Chair adjourn (this is an ad-hoc session) the meeting at 09:19 local time

**2nd slot : Tuesday March 12th 2024, 10:30 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 10:31 Local time.

Agenda slide deck: [11-24-0270r2](https://mentor.ieee.org/802.11/dcn/24/11-24-0270-02-00bi-march-plenary-agenda-tgbi.pptx):

1. Reminder to do attendance

Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.

1. Review of policies and procedures.
   1. IEEE individual process slides were presented.
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 policy and participation rules.
   1. No questions
4. **Discussion of agenda 11-24-0270r2 (slide #15)**
   1. Discussion on agenda

Author indicates that contribution 666r0 is ready for presentation.

Chair indicates that the approval of the minutes is postponed to PM2 waiting for last IMAT report.

* 1. Adoption of agenda by unanimous consent (20 participants online).

1. **Administrative**
   1. Remaining Meetings:

* Tuesday PM2
* Wednesday PM2
* Thursday AM1

1. **Technical Submissions**
   1. [11-24/0579r0](https://mentor.ieee.org/802.11/dcn/24/11-24-0579-00-00bi-periodic-obfuscation.pptx): Periodic obfuscation: Jarkko Kneckt

Document presented by Jarkko.

This document describes a method for automated periodic obfuscation

* + 1. Discussion

Q: concerning the AID obfuscation. I think after association it would be obvious to determine the range and offset will be easily determined so I prefer to have a kind of randomization.

A: the proposed algorithm is a simple one. The range should be sent in the association.

Q: We should have a possibility to have a non-regular range to allow more flexibility for the AP and more easy obfuscation.

Q: Why are you opposing single/group vs periodic, I think those are orthogonal concepts.

A: We can have all those schemes; everything will be optional.

Q: about the Offset. Do you propose a way to compute the offset?

A: I have a method in the annex (slide 11) but I am open to other method to compute this offset.

Q: This offset is stations specific right?

A: yes

Q: Your proposal is to have a fixed Offset, I think this is quite easy to correlate, because we can determine that the AID pattern is just shifted. Isn’t it the case?

A: Yes, the target here is to make things more difficult. We can also discuss to put the elements in clear in a beacon.

Q: But if we AID reassignment, it will take signaling. Do we want it every 100ms?

A: if we change that often, I don’t think tracking is so easy so we can have a simpler mechanism.

Q: On slide 6 you are only obfuscating Address1, so the other are in clear?

A: Yes, the idea here is to make things simpler.

C: My main concern will be on the 100ms order to change the parameters. This is pretty big Jump, so I need more time to discuss on this.

Q: Concerning Aid. If you have a 1000 station, if you just shift the AID, I don’t think this will not hide anything and I don’t see how to non-collide.

A: I don’t believe this tracking is so easy to do. But we can tailor the TIM element to make it not visible and make things more difficult to follow.

Q: Regarding the Offset for MAC address is it the same for all STAs?

A: No, for the MAC headers this is STA specific in contrary to the AID.

Q: For a device that slept to long, how does it determine the offset?

A: We will put the offset indicator in a kind of trigger frame to transmit this value.

C: I have a contribution (11-24/0561) initially planned to trigger the discussion we currently have, so, I withdraw this contribution.

C: Having a third party analyzing the traffic is complex and we are making it extra difficult.

Q: We do not have any indication how to determine the values?

A: The beacon will be self-explicit.

Q: Your mechanism is only valid if all STAs do the same right? or we will have collisions

A: We have a range for AID, and for MAC address we can randomly recompute a MAC address with very low probability of collision.

Q: About the collision avoidance. In case of massive AP, I wonder what kind of controller can handle that change every 100ms, and we may end up with a collision. Do you have mitigation idea in mind?

A: The AP knows all the MAC address used at the same time and can determine the future collision. You are right the AP can detect future collision and avoid it. Then the AP can take actions to correct it.

Q: Do you imagine that each station can have its own obfuscation mask?

A: yes, I think this should be station specific.

Q: For each station do you think we can have station specific fields obfuscated that are not obfuscated for other stations (different protection mask).

A: This is a point we can discuss to have different masks.

No More questions

According to the request of the author of the 11-24/0561r0 contribution, this contribution is removed from the agenda and will not be presented.

* 1. [11-23/1984r3](https://mentor.ieee.org/802.11/dcn/23/11-23-1984-03-00bi-epoch-wagon-proposal.pptx): epoch-wagon-proposal: Domenico Ficara

Document presented by Domenico.

This is the second presentation of the document. This new revision integrates some modification after the feedbacks received during last presentation and offline discussion.

The document especially includes support for group and individual epochs, one-time and periodic.

* + 1. Discussion

Q: Don’t we considered having multiple group Epochs?

A: I did not follow it but I think we can have a single group.

C: It think this solution is good in case we have several groups, useless otherwise

Q: What is the point in changing the MAC address if the group do not have enough STA? I think changing is better than doing nothing right?

A: Well, when you change, you give extra information to an eavesdropper about the fact that you are an 11bi STA and what is the start of the Epoch.

Q: Whether the number is not reach, is it a good or a bad thing? I think this depends on scenario, and station needs.

A: This is why I think the threshold should be given to the STA, so that it can decide to join or not this group depending on its own situation.

C: I do not see the benefit of the added complexity. As said before it is not always bad to change if the threshold is not reached.

A: I agree that there is an additional signaling. But the STA may have different requirement and prefer to change only in a big group for instance.

C: currently, even changing the group key provide issue of complexity, so I would prefer to have something deterministic and less complex.

A: Agree, but by definition we need to obfuscate, so make things more complex.

C: I think we can mitigate the group requirement, if we run a period change in background for all the devices or a set of devices. So, I look forward to work with you.

Q: When a STA withdraws from the Epoch, does it keep running the Epoch values or go back to the pre-Epoch values?

A: You can switch back to an individual approach, and request new EDP epoch settings.

C: I don’t see a lot of benefit for the one-time Group.

A: Yes, I agree that the periodic is more useful, and you can have a 1 iteration periodic group anyway.

C: I think we need to name things explicitly, since periodic is used in a different way for different contribution.

A: agree.

Author request to run the SP.

Then Chair ask if previous presenter wants to run a SP also since the proposals are quite different.

The authors of the two previous contributions will discuss offline to converge, and will come back later.

* 1. [11-24/0068r2](https://mentor.ieee.org/802.11/dcn/23/11-23-0068-02-00bi-proposed-spec-text-for-pre-assoc-keys-establishment.docx) : Proposed spec text for pre-assoc keys establishment: Duncan Ho

New presentation taking into account received comments. Mainly renaming the EPASN to EDPKE (EDP key Exchange) to avoid confusion.

* + 1. Discussion

Q: This is only for MLD or can be used for non MLD?

A: it is supposed to be for MLD, but I don’t think there is MLD specific parts.

Q: PASN and EDPKE seems similar but PAESN do not go to 4-way handshake, but with EDPKE the STA goes to four-way handshake but then the 4-way handshake is useless?

A: The 4-way handshake do not have to perfume the key generation since the Diffie-Hellman already done it.

Q: So, in case we do not need the 4-way handshake, do we need to add a text to mention that?

A: We can discuss offline.

A: The purpose of the 4way HS is not only to generate a PTK, it's also to prove possession of the PMK.

C: editorial change: the reference on page 2 for Authentication is Clause 6.5.5 NOT 6.3.5

A: Thank you.

No more questions

Chair reminds next meeting today PM2.

1. Chair recessed the meeting at 12:29 local time.

**3rd slot : Tuesday March 12th 2024, 16:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 16:02 Local time.

Agenda slide deck: [11-24-0270r3](https://mentor.ieee.org/802.11/dcn/24/11-24-0270-03-00bi-march-plenary-agenda-tgbi.pptx):

1. Reminder to do attendance

Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.

1. The chair mentioned the call for essential patents
   1. No one responded to the call for essential patents
2. Review of policies and procedures.
   1. IEEE individual process slides were presented.
3. The chair covered the IEEE copyright policy and participation rules.
   1. No questions
4. **Discussion of agenda 11-24-0270r3 (slide #15)**
   1. Discussion on agenda

No discussion

* 1. Adoption of agenda by unanimous consent (19 participants online, 7 in the room).

1. **Administrative**
   1. Remaining Meetings:

* Wednesday PM2
* Thursday AM1
  1. Approval of Telecon minutes and Interim session minutes – Motion #39

**Motion#39: Moved** by Jarkko Kneckt **Seconded** by Stephane Baron

**Motion #39 text**: “Approve the prior session minutes and teleconference minutes:

24/125r0 (interim minutes), 24/228r0 (Jan. 31 telecon), 24/274r0 (Feb. 7 telecon), 24/394r0 (Feb. 15 telecon”

**Motion#39 result**: Approved by unanimous consent (23 participants online)

1. **Technical Submissions**
   1. [24/0550r0](https://mentor.ieee.org/802.11/dcn/24/11-24-0550-00-00bi-tx-power-randomization.pptx): Tx Power Randomization: Ugo Campiglio

Document presented by Ugo.

This document proposes that CPE STA rotates otaMAC and adjusts its Tx Power at the same time to increase its anonymity.

* + 1. Discussion

Q: you propose to change the link adaptation, right? What is the order of magnitude of the Tx power change?

A: Few DBs should be enough.

Q: Do you think the range of value for the TX power change is established at association or can be dynamic.

A: In my mind I think this can be dynamic.

C: I will abstain on the PS because most likely we can go down on the TX power and then going down by several DB will change the max MCS and if you change the number of Spatial streams, you will even more perturbate the throughput.

C: I think this is something we should evaluate to determine the maximum perturbation we can afford.

C: I agree with previous comments but I think that we can afford changing the Tx power a little without having a big impact on the MCS.

A: I remember the discussion in 11ax regarding the BSS coloring, and I think we can go in the same direction and use similar algorithm not affecting to much the throughput.

No more question.

Author request a straw poll.

**SP#1 initial text**: “Do you agree that PHY parameters of a CEP STA should also be protected at an epoch edge?

* Yes
* No
* Abstain”

Discussion:

C: Friendly amendment to fix typo and wording (obfuscated instead of protected).

Q: Can we make this as optional operation. Something like: do you agree that non-AP CPE STA may request that its PHY parameters are obfuscated at epoch edge?

**SP#1 final text**: “: Do you agree that non-AP CPE STA may request that its PHY parameters be obfuscated at epoch edge?”

* Yes
* No
* Abstain”

**SP#1 result**: 10Y/ 7N/ 8A and 7 No answer

C: What can also be interesting is to have a graph showing the RSSI and Tx power for different STAs in a network.

A: OK.

* 1. [24/0553r1](https://mentor.ieee.org/802.11/dcn/24/11-24-0553-01-00bi-proposed-spec-text-for-frame-anonymization-functions.docx): Proposed spec text for Frame Anonymization functions: Phil Hawkes

2nd presentation of the document after comments received during last presentation

Phil presents the modification compared to the original revision, and answer to comments or questions received on the documents (discussion in the revision history part)

* + 1. Discussion

Q: regarding the FA MAC, I would like to have something like:

- Local/Global bit set to value 0, local address - Individual/Group bits set to value 0, individual address to randomize the remaining 46 bits.

A: OK, I see and I agree.

A note to the technical editor is added accordingly to include a definition of the FA MAC taking this into account.

Q: I wonder if the restriction to not have 2 frames transmitted in the same Txop to use different parameter set should also be applied to the AP?

A: In some case, it is ok for the AP to mix old and new MAC addresses of the receiving non-AP STA, but in case of SIFS burst (like consecutive fragments separated by SIFS to the same STA), this can allow correlation between the two sets.

Q: within a TXOP belonging to the non-AP STA, what is the issue to have all the frames transmitted/received with same parameters set?

A: This refrains the retransmissions from previous TXOP from the AP, because an AP may send frames to different STAs.

C: So, we can differentiate the case depending on who is the TXOP owner. In case this a non Ap STA, we can have a general sentence like: “All frames transmitted/received by a non-AP STA within a TXOP with non-AP STA as a TXOP holder shall use FA parameters from a single FA parameter set.”

A: OK, thank you.

The newly proposed sentence replaces the original one.

Q: If we consider this sentence, we will have a performance penalty to wait next Txop to retransmit when changing from Epoch to another.

A: I agree.

Q: About the PN offset, I assume this is per STA, right?

A: Yes.

Q: When starting the first Epoch, PN should be set to 1, so the offset is visible.

A: Yes, but we intend to hide the PN between Epochs, not in a given Epoch.

C: I think an offset can be inferred by sniffing the traffic.

Q: Chair: this document still contains some TBDs

A: Yes, but we will not address all the remaining TBD for this revision.

C: I wonder if people are comfortable with this text requesting the tech editor to add a definition or want to fix now.

A: I can remove it.

No more question.

Chair reminds next meeting today PM2.

1. Chair recessed the meeting at 17:18 local time

**4th slot : Wednesday March 13th 2024, 16:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 16:02 Local time.

Agenda slide deck: [11-24-0270r4](https://mentor.ieee.org/802.11/dcn/24/11-24-0270-04-00bi-march-plenary-agenda-tgbi.pptx):

1. Reminder to do attendance

Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.

1. The chair mentioned the call for essential patents
   1. No one responded to the call for essential patents
2. Review of policies and procedures.
   1. IEEE individual process slides were presented.
3. The chair covered the IEEE copyright policy and participation rules.
   1. No questions
4. **Discussion of agenda 11-24-0270r4 (slide #16)**
   1. Discussion on agenda

Request to add 11-24/0604r0 to the agenda

Request to add 11-24/0068r3 to the agenda

* 1. Adoption of agenda by unanimous consent (26 participants online, 7 in the room).

1. **Administrative**
   1. Remaining Meetings:

* Thursday PM1

1. **Technical Submissions**
   1. [24/0568r0](https://mentor.ieee.org/802.11/dcn/24/11-24-0568-00-00bi-transition-period-introductory-text.docx): Transition period introductory text: Stephane Baron

Document presented by Stephane.

The document contains a short introductory text for the transition period definition.

* + 1. Discussion

Q: I disagree with “the previous EDP params remains valid”. It creates confusion. I would prefer to differentiate behavior for reception and transition

A: OK. I will amend the paragraph to discriminate transmission and reception.

Q: Can you specify the difference between periodic Epoch and group Epoch in your definition?

A: Here, we are generic. The text is not depending on the way the starting time on the Epoch is computed, this is a high-level text only talking about the transition period.

Author to prepare a new release for next meeting

* 1. [11-24/0604r0](https://mentor.ieee.org/802.11/dcn/24/11-24-0604-00-00bi-periodic-frame-anonymization.docx): Periodic Frame Anonymization: Domenico Ficara

Document presented by Domenico.

* + 1. Discussion

Q: In your proposal you only consider MAC address collision, why don’t you also consider AID collisions?

A: In our proposal there is no issue on AID

Q: You indicate everybody will change in the BSS, so there is no group anymore?

A: we are missing a frame to join the group.

Q: I understand here that a STA can setup a Group, I am correct?

A: not exactly, a STA can join a group.

Q: there may be stations that are not 11bi that may be part of the AID range?

A: The AP will not assign

Q: So, you have range different for 11bi and legacies?

A: yes.

C: So: in a DTIM you will have issue to signal all those ranges because it doesn’t fit. So, we need to consider this.

Q: EDP IE in beacon frames gives many info for eavesdroppers, I need more time to study this text.

C: To me there is two topics: framework to choose to join some group, other topic is how to compute anonymization mechanism. It is not clear to me how to separate this.

C: I am confused to determine the structure of this document, and link with what we have today.

A: If we want to go with this text, we will need to fit this text in the structure of the D0.2 draft.

Q: I don’t see how we can have a station in several scheme?

A: We can have same mechanism to assign AID value shared between scheme.

Q: The AID space is very crowded so having different group jumping differently may drive issues and collisions.

A: In this case it will not work, this is should be considered

Q: Can a STA belongs to two schemes?

A: The two mechanisms will exist in parallel; this is more a question of scheduling.

C: I still don’t see how this can work.

Q: What difference between Periodic and Group Sequence?

A: Group Sequence as a low frequency and may freely select the obfuscation scheme. The AID is assigned by the AP. In Periodic, the frequency is much higher, and the AID is automatically shifted by a determined offset for the group.

No more question.

* 1. [11-24/0068r3](https://mentor.ieee.org/802.11/dcn/23/11-23-0068-03-00bi-proposed-spec-text-for-pre-assoc-keys-establishment.docx): Proposed spec text for pre-assoc keys establishment: Duncan Ho

New revision of the document presented by Duncan.

* + 1. Discussion

Q: 1X is important, so can we have a TBD to indicate that other AKM schemes may come later?

A: If we want to do that, I think we need a SP on this.

Q: Can we a add a note indicating something like this 3-messages scheme is only valid for SAE?

C: In the text, perhaps use of other AKMs as base can be kept open - say TBD instead of only SAE.

A: Here we provide a solution without closing any door. If we need more, we can add more but more discussion is needed.

Author then request a straw poll to see if the group agree on the addition of this text to the TGbi draft.

**SP#2: text**: “Approve directing the Editor to add the text from 24/68r3 into the current TGbi draft, with the understanding that other authentication schemes may still be added later.”

Q: Can we change the text to indicate that other AKMs can be kept open?

A: You mean to add that in the text of the SP?

A: No, to add this is the spec text.

The text is then amended accordingly to create an R4

Q: now that the text has been modified to include it, we do not need to add the part “with the understanding that other authentication schemes may still be added later.”. Can we remove it?

A: ok.

**SP#2 final text**: “Approve directing the Editor to add the text from 24/68r4 into the current TGbi draft”

**SP#2 result**: no objection.

Note for the technical editor to integrate 24/0068r4 in the TGbi draft.

* 1. [11-24/0553r2](https://mentor.ieee.org/802.11/dcn/24/11-24-0553-02-00bi-proposed-spec-text-for-frame-anonymization-functions.docx): Proposed spec text for Frame Anonymization functions: Phil Hawkes.

Phil presented the difference introduced in this r2 version after last presentation.

Mainly addition of a note for the technical editor to add a reminder that further text is needed to cover the transition period at the end of the document.

* + 1. Discussion

Q: regarding the last sentence of your contribution. You indicate using same anonymization for the retransmission. I think there is an issue here can we take it offline?

A: ok, let’s discuss that.

1. Chair recessed the meeting at 17:59 EDT

**5th slot : Thursday March 14th 2024, 08:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 08:02 Local time.

Agenda slide deck: [11-24-0270r6](https://mentor.ieee.org/802.11/dcn/24/11-24-0270-06-00bi-march-plenary-agenda-tgbi.pptx):

1. Reminder to do attendance

Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.

1. The chair mentioned the call for essential patents
   1. No one responded to the call for essential patents
2. Review of policies and procedures.
   1. IEEE individual process slides were presented.
3. The chair covered the IEEE copyright policy and participation rules.
   1. No questions
4. **Discussion of agenda 11-24-0270r5 (slide #16)**
   1. Discussion on agenda

Request to add the review of documents 568r1 and 553r5 to the agenda.

* 1. Adoption of agenda by unanimous consent (34 participants online, 7 in the room).

1. **Administrative**
   1. Teleconferences Schedule:

Tentative teleconference schedule: 10amEDT Thursdays (or Wednesdays to avoid TGbn)

* Mar 28th
* Apr 4th, 11th, 18th, 25th
* May 02nd, 09th
  1. Discussion

If conflicting with 11bn, date will be moved to Wednesday.

April 4th meeting will require a vice chair to be handled due to unavailability of the TGbi chair at that date. Chair indicates that this meeting may be cancelled.

1. **Technical Submissions**
   1. [11-24/0046r2](https://mentor.ieee.org/802.11/dcn/24/11-24-0046-02-00bi-privacy-protection-for-sae-credentials.docx) : Privacy Protection for SAE Credentials: Jouni Malinen

Jouni presents unchanged document since last presentation, and indicates that he received no comments despite opposition received during last vote.

Author indicates it is not possible to solve issues that are not expressed, so, he cannot amend the document.

* + 1. Discussion

No discussion.

Author then request a motion and a participant request that the motion is a recorded motion.

Chair acknowledged the request for recorded motion.

**Motion #40 text**: “Approve directing the Editor to add the text in 24/46r2 to the current draft”

**Motion #40 Moved** by Jouni Malinen **Seconded** by Stephen Mc Cann.

Chair ask if any body object to have unanimous consent

A participant object and request a count.

**Motion#40** is then run

**Motion#40** **Recorded vote result**:

A B C

--------------------------------------------------------------

[V] Po-Kai Huang Intel | | | |

[V] Noel Stott, Keysight Technologies | | | X |

[NV] Malcolm Smith, Cisco Systems Inc. | | | |

[V] Eldad Perahia HPE | X | | |

[V] Dan Harkins | X | | |

[V] Luther Smith, CableLabs | | | X |

[V] Stephen Orr, Cisco | | X | |

[V]Chenhe Ji Huawei | | | |

[V] Alex Krebs, Apple | | X | |

[V] Subir Das Peraton Labs | | | X |

[V] SK Yong, Apple | | X | |

[V] Gaurav Patwardhan HPE | X | | |

[V] Antonio de la Oliva, IDCC | X | | |

[V] Reza Hedayat, Apple | | X | |

[V] Yong Liu | | X | |

[V] Sid Thakur, Apple | | X | |

[NV] Jonghoe Koo, Samsung | | | |

[PV] Sherief Helwa, Qualcomm Technologies, Inc. | X | | |

[V] Stephen McCann, Huawei | X | | |

[V] Youhan Kim, Qualcomm Technologies, Inc. | X | | |

[V] Ali Raissinia Qualcomm | X | | |

[PV] Giovanni Chisci, Qualcomm | X | | |

[V] Gaurang Naik, Qualcomm | X | | |

[V] Alfred Asterjadhi, Qualcomm Inc. | X | | |

[V] Stephane Baron, Canon | X | | |

[V] Patrice NEZOU, Canon | X | | |

[V] Shinya MIWA, Canon | X | | |

[V] Jouni Malinen, Qualcomm | X | | |

[V] Jouni Malinen, Qualcomm | | | |

[V] Javier Contreras, Cisco | | X | |

[NV] Helene Ralle, Orange | | | |

[V] Domenico Ficara, Cisco | | X | |

[V] Ugo Campiglio, Cisco | | X | |

[V] Julien SEVIN Canon | X | | |

[V] Federico Lovison, Cisco | | X | |

[V] Yuki FUJIMORI Canon | | | X |

[V] Jarkko Kneckt, Apple | | X | |

[V] Duncan Ho, Qualcomm | X | | |

[V] Fumihide Goto, DENSO | X | | |

[V] Qi Wang | | X | |

[PV]Jinjing Jiang | | X | |

[V] George Cherian Qualcomm | X | | |

[NV] Yoshikawa Yuki, Canon | | | |

[V] Hirohiko Inohiza Canon | X | | |

[PV] Yaoshen Cui, TP-LINK | | | |

[V] Okan Mutgan, Nokia | | | X |

[V] Phil Hawkes Qualcomm | X | | |

[V] Jerome Henry, Cisco | | X | |

[V] Manish Kumar -NXP | | | |

[V] Ishaque Kadampot, Qualcomm | X | | |

Ankur [Samsung Electronics] | | | |

**Motion#40 result**: 22 Yes /14 No /5 Abstain: motion failed.

Discussion post motion:

C: It is perfectly fine to be against, but please indicate the reason for your “No” vote.

C: Similar with previous comment. People voting “No” should have a technical reason, otherwise, this is not how this group is supposed to work.

Despite requests, to the 'no' voters, to provide a reason for their votes, people remained silent. No answer nor comment was provided.

* 1. [11-24/0658r2](https://mentor.ieee.org/802.11/dcn/24/11-24-0568-02-00bi-transition-period-introductory-text.docx): Transition-period-introductory-text: Stéphane Baron

Document presented by Stéphane.

Update of the document after offline discussion

* + 1. Discussion

No question

Author asks for a SP to add this document in the TGbi draft.

**SP#3 text**: “Approve directing the Editor to add the text of 24/568r2 to the current draft.”

**SP#3 result**: 31 yes /2 No /7 Abstain

Chair indicated that the SP received strong support and document will be included in the spec text.

* 1. [11-24/0604r0](https://mentor.ieee.org/802.11/dcn/24/11-24-0604-02-00bi-periodic-frame-anonymization.docx): Periodic Frame Anonymization: Domenico Ficara

New revision of the document presented by Jerome Henry after last session presentation to accommodate some received comments.

* + 1. Discussion

C: A lot of modification from yesterday evening text. Need time to digest this text uploaded few minutes ago.

C: general statement is that I also need time to check the text because I have some technical disagreement on the way to determine the start time of the Epoch. Everything is based on beacon reception and multiple of TBTT. A different proposal ([11-23/1983r1)](https://mentor.ieee.org/802.11/dcn/23/11-23-1983-01-00bi-epoch-start-time-setting.pptx) was presented, during last F2F, based on TSF. Need to converge on a common solution.

Q: What is the purpose of the EGCP IE?

A: It is to advertise Group info. Maybe we could add some text to explain the role.

C: Editorial. Chapter numbering needs to be review.

C: This is a different technical approach from previous proposals.

Q: For the individual one, you will use the Epoch sequence discussed in the past right?

A: Similar, yes.

C: Then for group anonymization, you have 2 types: slow and fast.

Q: Maybe we should define 3 anonymization mechanisms: One for individual, on for group, and automatic group that is the fast one?

A: yes, but I want to be cautious to say slow and fast.

A: If you don’t like the automatic group, you can ask for an individual, then for the group, the AP will indicate information before next Epoch.

C: I would propose to have a break to let people read the text, because this is very difficult to follow this new text.

Q: You indicate that all the EPD epoch scheme are using the same anonymization mechanism, right?

A: yes.

Q: Why using the GCMP tool to generate the AID?

A: Because we already use it for other purpose.

Q: Could you explain the AID Offset computation? I think GCMP is not appropriate for this.

A: I understand. I can remove the AID offset computation. But not the previous formula.

C: You should have a better tool since some of the generated bits are used for other purpose.

C: It feels like a very strange thing to use GCMP-256 for that if it was supposed to be a PRF/KDF.

Q: Can I suggest to remove the OTA AID out if you want to have a vote on this now?

A: This BSS specific AID computation is the central proposal here so I would like to keep it.

C: My main concern is that a lot of points are unclear and I need time to read it. My blocking point is that I need time.

C: My proposal would be to wait before taking a decision to integrate this document.

C: I have a concern by just using an offset to obfuscate AIDs. The AIDs distribution pattern will not be changed by a simple offset, then allowing an easy correlation.

Q: You only limit the number of groups to 8 including the default one. This seems limited.

A: Currently yes, but for TWT we limit it to 8 groups also.

C: When having a lot of devices, this may drive to have more groups.

Q: How can we synchronize the change of MAC addresses among links of a given non-AP MLD STA since the beacons are not synchronized?

A: Why should we synchronized change of MAC addresses on the different links?

A: Because there is only one AID per MLD and you need to change it at t he same time as other parameters.

C: We need to discuss more on this, we may have an AID per link.

No more questions.

* 1. [11-24/0658r2](https://mentor.ieee.org/802.11/dcn/24/11-24-0568-02-00bi-transition-period-introductory-text.docx): Proposed spec text for Frame Anonymization functions: Phil Hawkes

Presentation of a slightly modified version by Phil.

* + 1. Discussion

Q: Retransmission is a difficult topic. Here, I understand you can only retransmit using the old MAC address?

A: Right, if you change the MAC address for the retransmission it is easy to correlate old and new MAC address since the payload is the same.

C: I think this is not so easy to retransmit using the same AID for instance.

A: I appreciate to separate the MAC header anonymization and the AID. My understanding is that AID is never used in a frame that can be retransmitted. So, we should not include AID here.

C: OK, so it would be good to indicate the PPDU type, to indicate that AID is not considered here.

Q: Do we have a link MAC address?

A: yes.

The document cannot be inserted in the draft as is, and requires harmonization with other proposals.

No more question.

1. **Way forward discussion**

Q: We have moved a little more text into the draft, the question is to know if we want to move in the last 10 minutes the 604 and 553 documents?

C: In the time we have I think we can only motion document that passed straw polls earlier.

Chair: I think we can direct out technical editor to provide a D0.3 and then we can continue working on 11-24/0604 and 11-24/0553.

Chair then request a motion to put the texts that was approved (passes a SP with good support) in the D0.3.

**Motion #41:** “Approve directing the Editor to create a Draft 0.3 with the texts that have been approved during this plenary and in earlier teleconferences.Specifically: 24/568r2, 24/150r5, 23/1664r7, 23/68r4”

**Motion #41** **Moved** by Po-Kai Huang and **Seconded** by Jerome Henry

Chair ask if there is any objection to approve by unanimous consent.

Someone object.

**Motion#41** is then run.

**Motion#41 result:** 26 Yes / 1 No /3 Abstain: Motion passes

Chair indicates that next session should work on doc 11-24/0604

No Other business.

1. Chair adjourned the meeting at 10:03 EDT