IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Minutes Mixed Mode Interim Session  11-15 September 2023 | | | | |
| Date: 2023-09-18 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Stephane Baron | Canon Research Center France | Cesson Sévigné, France |  | Stephane.baron@crf.canon.fr |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meeting that took place during the IEEE 802 Mixed Mode Interim Session 11-15 September 2023. The on-site location for the meeting was Atlanta, USA.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**1st slot. Monday 11 September 2023, 10:30 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron, Canon**

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

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

Chair calls meeting to order at 10:38 local time.

Agenda slide deck: [11-23-1361r1](https://mentor.ieee.org/802.11/dcn/23/11-23-1361-01-00bi-september-interim-tgbi-agenda.pptx):

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 11-23-1361r1**
   1. Further submissions added to the agenda

MLD discussion is still on going, so 1495r0 will be presented tomorrow

Chair ask if there is any opposition for this change. No answers.

Order of presentation modified accordingly.

* 1. Agenda as amended approved by unanimous consent (30 remote participants, 17 in-room)

1. **Administration**
   1. **Motion #33**

**Approve the minutes for:**

* **2023 July 802.11 Plenary: 11-23/1307r0,**
* **TGbi Teleconference: 11-23/1370r1 (10 August), 11-23/1532r0 (07 September)**

Moved: Stéphane Baron, Seconded: Po-kai Huang

Approved by unanimous consent (29 online and 17 local)

* 1. **Remaining meetings for this Interim session reminder by the chair:**

Chair indicates that discussion on MLD architecture support is scheduled for tomorrow’s session (09/13 PM2), and reminds that the group has to update the TGbi timeline according to our current progress.

New schedule is then as follow (indicating the major topic to address).

* Tuesday 09/12 PM2 -- MLD discussion
* Wednesday 09/13 PM2
* Thursday 09/14 PM1 -- Timeline update discussion

1. **Technical Presentations**
   1. **1497r0 – Proposals for PMKID Requirement– Po-Kai**

Presentation made by Po-Kai about requirement for PMKID requirements.

Presentation explicit how PMKID are generated each time a PTKSA is establish following mechanism already discussed in the past in the scope of past amendment and generally agreed.

Document then indicate direction for associated spec text drafting (to be done quickly is agreement is reached on this document).

**Questions:**

Q: For the FT part, please note that PTK can have a very long life, and you have potentially to update everything in the mobility domain. I would like to understand what is the intention here?

A: R1 key holder has to communicate with the R0 keyholder, and for FT you have a new R0 name.

Q: I try to figure out if a STA has to remember several R0 holder per key?

A: Only one, I think.

Q: I have a concern regarding the statement around EDP AP in this presentation. We may be breaking the mobility domain (ESS) by hiding things unless we are very cautious.

A: For the non-FT case the spec says nothing (not standardized) around key exchange in the ESS and we do not change it. So, I think we do not break anything.

C: Whether it is described or not, we should take care not breaking existing implementation.

Q: Can you provide pointer in the spec where key exchange is described?

A: I will try.

Q: On slide 7: editorial: can you please change the reference number 2, since this is a 2021 document. A: sorry about that.

C: I second previous answer, OKC implementation is not described in the spec, this is a de facto standard. So, I think what the author is proposing is enough.

A: Thank you.

Q: I try to understand the difference between FT case and non-FT case, can you elaborate a little?

A: PMKID can be used for both FT and non-FT cases, but for FT when you roam you have to use the R0 key holder name.

Q: KDK derived from PTK and is distributed after association, so how can you link KDK and PMK? In 11bi all can change including the R0 key holder, right?

A: There is no requirement to change the R0 key holder ID in 11bi.

Q: You are making this mobility domain specific. Can we have legacies in this domain?

A: For FT case yes, the domain is specific, but for non-FT case we can have legacies.

Q: So, there will be 2 mobility domains?

A: No, for legacies, R0 name will not change, and 11bi staff has to take care of updating correctly they’re info.

A: In the current spec (REVme D4.0, page 2864, line 24) it is said that the PMKID will not change, but do we know why? I think we need to address that in the scope of 11bi.

A: currently, this is for interoperability reason that the ID is not changed for the lifetime of this PMKSA.

C: If we can have alternative, it is ok, but for the moment we should stick with what is on the server except if we have other solutions.

A: (chat) We have "another approach" proposed for SAE Password IDs for REVme. So, there is an example if someone want to take a look at how HPKE(PMKID) could be used.

**No more questions.**

* 1. **Next meeting reminder**

**Chair call again for contribution and remind tomorrow objectives (MLD discussion)**

The Chair reminds next meeting date and time: Sept. 12th PM2.

**6.5** AOB:

no other business.

Chair recess at 11:52 local time.

**2nd slot. Tuesday 12 September 2023, 16:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron, Canon**

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

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

Chair calls meeting to order at 16:02 ET.

**Agenda slide deck**: [11-23/1361r3](https://mentor.ieee.org/802.11/dcn/23/11-23-1361-03-00bi-september-interim-tgbi-agenda.pptx)

1. Reminder to do attendance. Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.
2. Review of policies and procedures.

IEEE individual process slides were presented.

1. The chair mentioned the call for essential patents

No one responded to the call for essential patents

1. The chair covered the IEEE copyright and participation rules.

No questions

1. **Discussion of agenda 11-23-11361r3**
   1. Remaining Meetings reminder:
      * Wednesday PM2
      * Thursday PM1 – Timeline Update Discussion

Agenda is then reviewed:

no contribution uploaded yet, so the chair reminds the goal of today : discuss MLD architecture support for 11bi.

Approval of agenda by unanimous consent (23 participants on-line, 12 participants in the room).

1. **MLD and non-MLD discussion**

Chair presented slide 19 of the agenda summarizing the topic of the discussion, and the associated question:

* + A feature or all features could be optional for MLD and non-MLD
  + A feature or all features could be only applicable for MLD
  + Do we want to go feature by feature, or decide more broadly?

**Discussion:**

Chair indicates that this topic is important to start drafting spec text, so it is highly preferable to find an agreement on this topic.

**C:** I agree that we may not be able to make a blanket draft, and I prepared a document (23-11/1495r0) that is now in the queue on this topic**.**

A: Ok, so let see other people comments and then see your document.

C: we have a lot of signaling, and protected frames that can be common to non MLD and MLD, but some others may be much easier for MLD, like MAC address change. So, let’s separate the features that are non-MLD compatible and MLD compatible features.

1. **Technical Presentations**
   1. 23-11/1495r0 Discuss Requirements of MLD – Po-kai

Author presents his document that provides elements for the previous discussion on requirements of MLD.

The question is mainly to know if TGbi should mandate support of the MLD architecture.

Reminder of where the problem come from (slide 3) and especially the problem linked with the AAD.

AAD uses the MLD MAC address in MLD architecture, it is then easier to adapt it for feature requesting hardware change like RCM.

Q&A:

Q: I agree on a lot of things you mentioned, and I think MLD is the best idea, but I have a question:

Slide 7: MLD support will be mandatory in the future, but currently we have Wi-Fi 5 station for instance. How can this work?

A: in WFA, all chip vendors indicate support of MLD for high-end and low-end devices.

Q: I presented a contribution 11-23-0133 to make AAD swap easily based on the DS MAC. I think we can have same CCMP encapsulation as MLD using DS MAC instead of MLD MAC.

A: I agree that we need something for the MLD support for the AAD swap, but only the client needs DS MAC, and AP may not have DS\_MAC address. So, this is a one side process.

C: This is only for CPE, but you need to consider CPE client talking to a BPE.

Q: What is the point of implementing the first feature list (not RCM related), if we do not change the MAC address?

A: There is still a benefit. For instance, for roaming or probing, station can have an interest in anonymizing the frame exchanges by using encryption. So, we do not have nothing if we do not change the MAC address.

Q: Why MAC address change requires hardware change?

A: There is a document presented earlier and in reference (11-23/873r2)

C: I think MAC address, SN, or PN change can be done in Software.

A: Please, have a look at the reference I mentioned (11-23/873r2), since this is a problem that requires a long discussion that cannot occur now.

C: in 11-23-0133 I propose a minor change in the current non-MLD CCMP encapsulation that will allow changing the over the air MAC address for non-MLD with minor modifications.

C: I don’t think that MLD architecture solves all the problems for MAC address change, and I don’t think all the stations will be MLD in the future. This is why I propose the solution of 11-23-0133.

A: I agree that both MLD and non MLD requires changes. I know it is doable to use non-MLD MAC address but I think as previous commenter mention, that adoption will be faster using MLD architecture.

Q: Can you show a diagram to explain why MLD and non MLD are so different from the MAC address change. And we also need to consider BPE.

A: I agree but the point is that for CPE is only a one side change. A CPE AP will not need to implement the MAC address change.

Q: Is it the AP that needs to be at least Wi-Fi 7?

A: this is not what I mean.

C: maybe for the software part we can agree on the first straw poll.

C: I also support using the MLD as a new structure for make support of the 11bi.

Q: So, do you support that there are two groups of features, first group for MLD and non MLD stations, and second that is for MLD stations only?

A: yes.

Q: for list of features in slide 9, if you are not changing OTA MAC there is no concept of DS-MAC needed, right?

A: I agree, so I will indicate that this is probably better to indicate “when you roam and change your MAC address” there.

Q: I think this is a bad idea to split features between MLD and non MLD. Can we remove “and do not support STA MAC address” in the first straw poll?

A: I prefer to address the problem of MAC address change separately, and avoid confusion in this SP.

Q: MAC address change includes SN/PN and so on, so, maybe things are not clear enough. Second point is that we do not need to support the whole list here, so we can make it clear in the SP.

**SP#1**: requested by Po-Kai:

“Do you support the following:11bi devices that support any of the following features and do not support STA MAC address change and related features while associated can be MLD or non-MLD: (List of the feature is on the slide 9 of document 1495r1)”

Document containing the SP is uploaded (23-11/1495r1) before the SP is run.

**SP#1 Results**: 12Y / 1 N / 8A / 7 Need more info / 4 No answer

Chair request if anyone as another presentation ready for presentation.

No answer

Chair indicate that tomorrow meeting is not cancelled and call for contributions for this meeting.

1. **AoB**

No other business.

1. Chair adjourned the meeting at 17:25 ET.

**3rd slot. Wednesday 13 September 2023, 16:00 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron, Canon**

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

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

Agenda slide deck: [11-23-1361r4](https://mentor.ieee.org/802.11/dcn/23/11-23-1361-04-00bi-september-interim-tgbi-agenda.pptx):

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

1. The 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

No one responded to the call for essential patents

1. The chair covered the IEEE copyright and participation rules.
2. Remaining Meetings:

Thursday PM1 – Timeline Update Discussion

1. Agenda discussion

Chair indicates no new documents have been uploaded.

A document uploaded recently is then mentioned:

11-23-1628r0 MACc MACp proposal from Jerome Henry.

The author indicates that he prefers to present the document later to allow co-authors to be present.

Document to be presented Thursday September 14th.

A second document not uploaded yet is mentioned as pertinent for the MLD/ non-MLD discussion.

11-23-1623r0 Material for MLD Discussion proposed by Antonio.

Author indicates that if needed, the doc can be uploaded immediately.

Discussion on agenda

Chair ask if people have a preference to continue MLD non MLD discussion, or go to technical presentations

C: I think it would be nice to have a decision on the direction even if we do not have a full technical solution.

Decision is taken to continue the discussion on MLD non MLD theme.

The doc 11-23-1623r0 is then uploaded

Proposal to present 11-23-1623r0 as material for the discussion is approved and agenda modified accordingly.

Approval of agenda (as indicated in agenda 1361r5 slide 18) by unanimous consent (27 participants on-line, 12 participants in the room).

1. **Technical presentations:**
   1. 11-23-1623r0 Material for MLD Discussion – Antonio de la Oliva**:**

The presentation explains how the support of MAC address rotation can be done independently of the support of the MLD architecture.

The document especially describes a solution to use the DS MAC address for MPDU encryption/de-encryption. This proposed solution is presented as architecture agnostic.

Discussion:

Q: slide 14: You change the original proposal by using the DS MAC address but we decided not to exchange DS MAC, right?

A: The DS MAC can be exchanged in message 3 or 4 of the 4-way handshake and is then completely hidden. I am not proposing to have the DS MAC sent in clear.

Q: You claim that the PTK is derived from the DS MAC but this is not the case, the PTK is derived from MAC 1 in your slide.

A: OK I see your point on that.

C: On slide 8 you indicate DS MAC 1 and DS MAC 2, but if the AP do not implement BPE, this is a single side change.

A: I do not see this point.

Q: why is this presentation not in scope for 11bh?

A: 11bi address RCM while associated, not 11bh.

C: your presentation doesn’t say that.

A: I see, but RCM while associated is clearly in the scope of 11bi.

C: I think that if you reduce the scope to MLD only, you will do only half of the job. If you want to do so, you have to change the 11bi PAR.

A: This is why we separate between software features and hardware features. So 11bi will support both MLD or non-MLD anyway, the question is only on hardware features.

Q: I am looking for option 2 slide 11. What is the difference between option2 and 23-11/1495 proposal?

A: I am not forcing MLD compliant, just apply 11be CCMP to non MLD 11bi enabled STA.

C: I think your option2 is a subset of what 1495 propose, so I think this is just a question of definition what means MLD compliant for 11bi.

A: I agree to find a solution, but I don’t want to let out stations that are not MLD.

C: I just want to emphasis that we just discuss feature that is MAC address rotation, there are a lot of other features that doesn’t need to select between MLD and non MLD.

C: IMO, the major MAC hardware change is required to avoid mixing MPDU from old and new MAC address. So, we need separated buffers or something like that.

C: I think there is no discussion that 11bi MLD STA will support MAC address change while associated. The question is to know the difference between a single link MLD and a “normal” STA.

A: they are very similar since to add a queue you will push toward mechanism added to the MLD

C: regarding the scope MLD, whatever 11bi decides, please take care of your PAR.

A: The 23-11/1623 proposal would make station similar to MLD, but not be an MLD so we do the job twice.

A: I agree that at the end we may be closer to MLD but transmission without handling links that has nothing to do.

Then chair request a SP

**SP#2:** requested by TGbi chair:

“11bi devices that support STA MAC address change while associated shall support MLD?”

Discussion:

Q: when you mention non MLD, is it legacies prior 11be?

A: I thought 11be has MLD STAs and non MLD STA.

C: proposal is to indicate station that doesn’t support MLD.

Q: I am wondering if it would not be better to ask the reverse first?

**SP#2 text is then changed to :**

“Do you agree that TGbi will include a specific solution for OTA MAC address change for STAs that do not support MLO?”

**SP#2 results**: 10 Y / 17 N/ 7 Abstain /6 no answer

For completeness, TGbi chair run the other SP

**SP#3:** Requested by TGbi Chair:

“11bi devices that support STA MAC address change while associated shall support MLD?”

**SP#3 Results:** 22 Y / 4 N / 6 Abstain / 9 no answer

Discussion after the straw poll result.

Q: considering the result of the first SP, does it mean that we will have a solution in another group?

A: we do not say support 11be, but support MLO.

Q: The question is to know where to spent our energy. Do we continue discussing on MLD vs non-MLD or do we move on?

A: I agree this is the way to go even if we have to refine the scope.

C: All features except the MAC rotation will be implemented on any kind of devices.

C: I think for sake of progress, we have to forget the non-MLD and focus on MLD, right?

A: We also have to see at the WG level how they feel about the current direction

C: please do not rush on PAR modification, first go to the first letter ballot and see how is the technical solutions and the associated scope then decide if there is a PAR violation.

Chair reminds that we will come back on this question tomorrow during the last session.

Going back to the agenda, doc 11-23/851r2 is presented.

* 1. 11-23-0851r2 Proposed spec texts for action frame to request capabilities and operation parameters – Po-kai Huang

Second presentation after refinement of the non-MLO part that was the only remaining open comment for this document.

Q: On page 4 can you have only one table with options?

A: For advance reader no problem, but I want to avoid future questions from readers by making things very clear.

Q: This action frame is only for probe response, right?

A: This is not a probe response this is an additional action frame. The table indicates the elements as defined in probe response chapter, but this is not a probe request.

A: we define additional frames that can be encrypted and that contains everything you need, and was usually provided in a probe response.

Q: probe response has many elements that make non sense to be put in this action frame.

A: there is a requirement to reduce what is sent in probe before association, but those frames are post association frames, and may contain more info.

Q: There are some critical elements you cannot remove from the probe response

A: The table 9-67 will cover what is included or not included, in order to not repeat everything each time we use those elements.

No other question.

TGbi chair request a SP:

**SP#4:**

“Do you have any objection to pushing this text (11-23/851r2) into our first draft?”

**SP#4 results**: No objection and 1 abstention

**22 Future sessions schedule**

Chair indicates we need to discuss tomorrow on the timeline.

Quick recap on MLD non MLD and for the future sessions scheduling especially teleconferences.

**23 Chair indicate Recess at 17:56**

**4th slot. Thursday 14 September 2023, 13:30 local time.**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stephane Baron, Canon**

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

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

Agenda slide deck: [11-23-1361r6](https://mentor.ieee.org/802.11/dcn/23/11-23-1361-06-00bi-september-interim-tgbi-agenda.pptx):

Chair calls meeting to order at 13:32 local time.

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**

No one responded to the call for essential patents

1. **The chair covered the IEEE copyright and participation rules**.
2. **Agenda approval**:

Agenda as shown in 11-23-1361r6 page 18 is approved with unanimous consent (19 people 10 in the room)

**30 Teleconference discussion**:

Proposed teleconference planning:

* + Teleconference planning:
    - Continue to use Thursday 10amET every other week – more often?
    - Sept. 28, Oct. 12, Oct. 26, Nov. 9
    - Oct. 5, Oct. 19, Nov. 2 (if we want to meet more often)
  + Timeline adjustment

C: better granularity, every week, is a good idea and cancel it in advance if needed.

C: Oct 19th is not a good date since this is during WFA meeting and secretary will not be able to attend 11bi on Oct 19th.

Oct 19th is then cross out, and other meeting sessions are agreed.

**31 Timeline discussion**

Discussion:

C: people discuss around first letter ballot.

Chair propose optimistic date: Nov 2023.

C: It is more realistic to put January 2024

C: In addition, just a thought: There is a reasonable chance to be in parallel of a lot of letter ballot in November.

C: (chat) Better to set early as it would give incentive versus having people wait IMHO

TGbi chair then setup the initial letter ballot to January 2024, and adjust following milestones accordingly.

TGbi chair to publish agenda 1361r7 including resulting timeline as discussed

**32** Final MLD non-MLD review

TGbi chair display following summary as the result of the group past discussion:

* TGbi has several blocks of features: (list is not exhaustive, just illustrative)

CPE

Changing STA MAC during Association

Limited content pre-assoc messages

Protected/limited content mgmt. frames

AP identification (protected)

BPE

Beacon with encrypted/limited parameters

Obfuscated group frames

Changing AP and STA MAC during Assoc.

* + CPE features, other than MAC address change while associated, will be defined for MLD and non-MLD
  + CPE MAC Address change while associated will be defined for D0.1 assuming an MLD architecture
  + BPE features TBD, not expected in D0.1

Chair asked if everybody agreed on the presented summary.

Discussion:

Q: I am ok with this but I have a question around multiple source address and destination address. Is it also after D0.1?

A: If people as some draft text and we can get feedback, we can integrate it.

No more question.

Going back to the agenda, TGbi ask if there is any preference to present first.

C: I think 11-23-1628r0 should go first since this is new material.

**33 Technical presentations**

**33.1 11-23-1628r0** MACc MACp proposal – Jerome Henry

Jerome presents the document presenting an extension of the MAC address change mechanism that seems to meet current consensus in the group.

The proposal is that a single STA may support a set of active unicast MAC addresses instead of one currently.

Discussion:

C: changing the MAC also require having a different context for each MAC address (SN, PN, AID, etc.) so is it not that simple.

A: Agree that each MAC needs to have a set of parameters. It is the same as having 2 addresses by Stations.

Q: does some MAC address survive cross Epoch?

A: It would probably safer to change everything at once. But I do not have strong opinion.

Q: On slide 3: about tracking MAC addresses: here, what does the eave dropper will gather during this epoch, and for how long?

A: duration is not decided yet, let’s say around 5-10 minutes.

A: (chat) Agree with 10min (in that order of magnitude at least)

C: I think this is quite a very complicated implementation that will not provide that added value against tracking.

C: Transition period is time when retries and retransmissions will occur, so there is no reason to set a limit.

C: I think that having a pair of addresses is very easy to deal with it, but I do not see the reason of having a hard Epoch.

A: the signal will be sent by the AP and makes things difficult for eaves dropper to follow a single STA since everybody change at the same time.

C: regular Epoch is quite easy to determine for an eavesdropper, I don’t see the benefit of a hard Epoch limit.

A: I don’t have a strong opinion there, but if there is a station individual change there is a risk that a station changes every 5 seconds.

A: This can be negotiated upon association

Q: We already had SN, PN, discussion. If a STA has several MAC addresses, you need different obfuscation factors for each MAC address, and a traffic flow may be divided on several MAC addresses. This will make the work difficult to unscramble the eggs.

A: I agree with you this can be an issue.

C: About epoch: Ap may actually prepare everything in advance since the change occurs let say every 10minutes.

C: having more MAC addresses seems more difficult to track, but not sure that 2 or 3 MAC addresses will help. Having 10 or more, yes, but this is not practical. In addition, I think the group agrees on MAC address change requested by the STA.

A: Yes, this is a separate requirement (the STA requesting changing its MAC address change)

A: about computation cost, at AP side at least. I think this is not so expensive for the AP. I think this is more efficient to have more MAC address,

Q: Coming back to previous commenter discussion around Epoch. Can, predictable Epoch for eavesdroppers be turned into non regular Epoch duration?

A: I think this is a very good proposal to make Epoch more flexible.

Q: Do we discuss on AP side to change of its MAC address?

A: this is not what I have in mind.

Q: Do you think downlink will have this mechanism?

A: I do not have strong opinion on this point.

Q: do you think we should have different AID?

A: I think we need one AID per MAC address.

Q: So, what about the triggering that is based on AID?

A: Yes, an AP may use several AIDs to trigger a station.

Q: You say that more MAC addresses mean more privacy but what do you think?

A: I think than having several MAC addresses make it more difficult to track a station.

C: In the case of multiple links, so many MAC addresses will be handled by a single STA.

A: Yes, this is why I say we need a mechanism to negotiate the number of MAC addresses.

Q: For 3rd sub bullet of the 2nd bullet in slide 4: Do you see why we shouldn’t do this also for the AP?

A: I think we should not indicate to the station how to use those different MAC addresses. And same for the AP. But for the AP, we could have a resource issue.

Q: About MLD, each link has its own security context, so I don’t know if AP could support the increase of storage for all the security context. It is like having different stations.

A: We had some discussions to have key derivation not linked to the STA MAC to reduce the storage and complexity issue.

A: regarding the security association, if I follow yesterday discussion, the security context will be mapped to the DS MAC, so only one context.

C: I think having more complex epoch duration will make thing much more difficult for observer.

A: Yes I like this direction.

Q: do you indicate how AID are bound to the Mac address?

A: we need one AID per MAC so this limits the number of possible associated stations.

Q: Is the AID associated upon association?

A: I think we need a mechanism to change it.

A: About Aid change, there was another presentation 23-11-0336r1 that deal with this problem and discussion occurred at that time. One opinion is that it could be generated by the STA and corrected by the AP if needed, the other opinion is that this is typically AP’s role to assignee the AID.

A: About Aid, I think that, due to the number of stations, collision of AID is very likely, so we probably have to assign an AID, and I think the AP has to do that, but I agree that we have to discuss the details.

No more question:

SP is deferred to allow more discussion on this subject.

**33.2 11-23-1160r1** Proposed spec texts for encrypting (re)association request response – Po-kaiHuang

Second presentation of the document taking into account comments received;

Discussion:

Q: For the non MLD part to understand the process. Do you use the 4-way handshake?

A: There is no 4-way since we move it to the association frame.

Q: MLD MAC address is different from the DS MAC?

A: The DS MAC do not change so I think MLD MAC address and DS MAC should be different.

Q: Do you have to change the MAC address in the DS?

A: No, you will use another MLD MAC address when roaming but not change the DS MAC. We do not need it since this part is encrypted.

Q: When you receive a frame from the DS, the DA is set to the DS MAC, so what do you think we should do?

A: OTA is only the MLD MAC address, the AP translates and knows the link.

Q: For the non MLO part: page 6 authentication frame. I don’t think we need the “as defined in 12.5.2. CTR …”

A: If I don’t mention it then we are using TKIP or WEP, so this is why I indicated those references.

C: I also think I would actually remove this par also; this is not really needed.

A: Ok, I will remove it.

Q: Why did you just indicate just FT protocol instead of over the air and over the DS separately?

A: I see, I just want to avoid repeating things.

Q: A1 filtering is not indicated here?

A: this is out of scope of this document, but A1 filtering definitely needs to be clarified. Change of MAC address is something done on top of this. When you roam, you change the address simply, but while associated if you change your MAC address, you need to do additional things.

Q: On page 8 you indicate the usage of the DS MAC address right. I read this as AP take care of the DS MAC address, but I see nothing about STA, I would need more details.

A: OK.

Several additional editorial friendly amendments are proposed to clarify the text.

Author to create 1160r2 including the discussed modifications

No more question.

Author ask if it is possible to SP r2 now.

TGbi chair indicates it would be better to post r2 first.

**34 Back to the agenda,**

the agenda is exhausted.

**35AoB**

No other business.

**36 Chair adjourned the meeting at 15:22 local time**