IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes April 04th 2024 |
| Date: 2024-04-05 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Stéphane Baron | Canon | Cesson-Sévigné, France |  | Stephane.baron@crf.canon.fr |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meetings that took place Thursday April 04th.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 10:02 ET.

Agenda slide deck: [11-24-0646r1](https://mentor.ieee.org/802.11/dcn/24/11-24-0646-01-00bi-tgbi-telecon-agenda-apr-may.pptx):

1. Reminder to do attendance
2. The chair mentioned the call for essential patents

No one responded to the call for essential patents but there is a comment.

1. Review of policies and procedures.

IEEE individual process slides were presented.

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

No Questions

1. **Discussion of agenda 11-24-0646r1 (slide #14)**
	1. Discussion on agenda

No discussion

* 1. Adoption of agenda by unanimous consent (15 participants).
1. **Administrative**
	1. Upcoming teleconferences planning
* Apr 11th, 18th, 25th
* May 2nd, 9th

Call from the chair to indicate if people need a slot for presentation of a contribution.

1. **Technical presentations**
	1. [11-24/0645r0](https://mentor.ieee.org/802.11/dcn/24/11-24-0645-00-00bi-edp-epoch-setup-normative-text-for-11bi.docx) -- EDP Epoch Setup normative text for 11bi – Stéphane Baron

Document presented by Stéphane.

This document presents the spec text corresponding to previous concepts presentations and provides details of empty chapters in current D0.3.

* + 1. Discussion

C: I need more time to analyze the document.

A: Agree, this is just first presentation, no SP will be run today.

Q: What is the unit of the fields in the EDP Epoch setup parameters element?

A: This is open to discussion, but I think a multiple of the TU (for instance 50 x 1024us) can be a good compromise. allowing for instance interval between 50ms and 50 min.

Q: Can we have just a general formula, to compute the EDP Epoch start time, instead of two?

A: Yes, the second formula works at any time, the first formula was just an easy computation of the first EDP Epoch of the sequence. We can keep only the second one.

Q: Did you consider TBTT instead of TSF?

A: For MLD architecture, TSF is a better choice since TBTT are not synchronized among links. So which TBTT should we take? TSF is easier because 11be already provides TSF offsets per link so it is easy to compute equivalent TSF counter value on each link.

Q: Did you indicate the units of the fields in the IE?

A: No, this can be multiple of TU.

Q: For Group Epoch operation, I think “any management frames” is too broad.

A: Perhaps it can be reduced for Probe response or we can define a list of management frames.

Q: Are EDP Action frames individual or group?

A: In my mind those are unicast action frames.

Q: Is there any maximum bound for the range of the added random time?

A: We use a modulo Time Range field to maintain the pseudo random variation in a predetermined range. Exact allowable range can be discussed.

Q: What is the unit there?

A: Same as it is for Interval. Potentially TU.

Q: Can this pseudo random range be optional?

A: I think this is desirable to obfuscate the date of the new parameters application to increase the privacy, but put 0 for the range value, and there is no pseudo random variation.

C: for individual it is OK, but not sure it is useful for Group EDP mode.

Q: Can we exchange group info during association to immediately start privacy mechanism?

A: Yes, this is possible.

Q: Why a limited number of EDP Epoch? Infinite is enough, I think.

A: Here we indicate support of a number of EDP Epoch per sequence to support the one shot and infinite sequences. The limited number, is for stations eager to change the frequency of EDP Epoch frequently to make eavesdropper life more difficult.

C: I think the random variation will come naturally when a STA will have traffic to send, no need for artificial creation of a random variation.

A: It depends on scenario. Natural variation will only come for station that have no buffered traffic ready for transmission.

A: In case of heavily loaded network, lots of STA will have traffic waiting for transmission. Transmission using new parameters will occur immediately after the EDP Epoch start time. We need to make this start time less predictable, this is why the pseudo random variation of the EDP Epoch start time is made for.

Q: What happens if a STA have no data to transmit? The STA has to wake up at each change even if it has nothing to transmit. I think this is too complex

A: STA performs privacy mechanism only when it needs to wake up and not the contrary. A STA can then compute current parameters, but a STA do not need to wake up only for that.

C: I think MAC address based on TSF is good. Perhaps group EDP is not mandatory.

C: Update element format to be compliant by adding extension element.

A: OK.

C: You need capability bit(s) to indicate the support of EDP features. This is not described here.

A: Jerome already defined capability bits in its document. Need to merge with this doc.

C: About PRF, I suggest to think about length you need. Make it AKM dependent to avoid specifying number of bits we need.

Q: PTK\* and GTK\* (key derived from PTK/GTK) need to be precise to avoid confusion.

A: We could use KDK to build the PTK\*. I will provide more detail in next revision.

Q: Can we have multiple group EDP Epoch? How a STA can join a group?

A: This is not specified here, but different group is OK. We just need to add a Group ID in the Information Element.

* 1. [11-24/0637r0](https://mentor.ieee.org/802.11/dcn/24/11-24-0637-00-00bi-proposed-spec-texts-for-pmkid-requirement-follow-up.docx) -- Proposed spec texts for PMKID requirement follow up – Po-Kai

Document presented by Po-Kai.

Focus on PMKID computation part and addition of a section for PMKR0Name privacy

Author indicates this is the first presentation and he do not request a straw poll to let people digest the presentation.

The main proposal is to agree on the PMKR0Name computation formula.

* + 1. Discussion

Q: Regarding SNOUNCE in the formula. We are talking about several APs so the snounce is specific to a couple STA / AP, right?

A: Anonce and Snonce are connection dependent.

Q: So, the values doesn’t need to be exchanged?

A: There is an exchange between key holders.

Author ask for people to review and provide comments.

1. **AoB**

No other business.

1. Chair adjourned the meeting at 11:40 EDT.

**Attendance:**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbi | 4/4 | Ansley, Carol | Cox Communications Inc. |
| TGbi | 4/4 | baron, stephane | Canon Research Centre France |
| TGbi | 4/4 | Bredewoud, Albert | Broadcom Corporation |
| TGbi | 4/4 | Coffey, John | Realtek Semiconductor Corp. |
| TGbi | 4/4 | DeLaOlivaDelgado, Antonio | InterDigital, Inc. |
| TGbi | 4/4 | Fujimori, Yuki | Canon Research Centre France |
| TGbi | 4/4 | Henry, Jerome | Cisco Systems, Inc. |
| TGbi | 4/4 | Ho, Duncan | Qualcomm Incorporated |
| TGbi | 4/4 | Huang, Po-Kai | Intel |
| TGbi | 4/4 | Kneckt, Jarkko | Apple Inc. |
| TGbi | 4/4 | Li, Weiyi | Spreadtrum Communication USA, Inc |
| TGbi | 4/4 | Luo, Hui | Infineon Technologies |
| TGbi | 4/4 | Miwa, Shinya | Canon Research Centre France |
| TGbi | 4/4 | Mutgan, Okan | Nokia |
| TGbi | 4/4 | Nezou, Patrice | Canon Research Centre France |
| TGbi | 4/4 | Patwardhan, Gaurav | Hewlett Packard Enterprise |
| TGbi | 4/4 | Petrick, Albert | InterDigital |
| TGbi | 4/4 | Sevin, Julien | Canon Research Centre France |
| TGbi | 4/4 | Smith, Luther | Cable Television Laboratories Inc. (CableLabs) |