IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes 16 February 2023 |
| Date: 2023-02-23 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Sky Group/Comcast | Brussels, Belgium |  | amelia.ieee@andersdotter.cc |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meeting that took place on

16 February 2023 at 10:00 ET.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**Chair: Carol Ansley, Cox Communications**

**Secretary: Amelia Andersdotter, Comcast**

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

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

Chair calls meeting to order at 10:01 ET.

Agenda slide deck: [11-23-0224r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0224-00-00bi-february-march-telecon-agenda.pptx):

1. Reminder to do attendance
2. Review of policies and procedures.
	1. IEEE individual process slides were presented.
3. The chair mentioned the call for essential patents
	1. No one responded to the call for essential patents
4. The chair covered the IEEE copyright and participation rules.
	1. No questions

1. **Discussion of agenda 11-23-0224r0 (slide #16)**
	1. Adoption of agenda by unanimous consent (18 participants).
2. **Administrative**
	1. One more teleconference before the 802 Plenary in March.
3. **Technical presentations**
	1. **Mechanism of simultaneous changes to SN scrambler seed PN AID and TID** ([11-23-0166r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0166-00-00bi-mechanism-of-simultaneous-changes-to-sn-scrambler-seed-pn-aid-and-tid.pptx)), Chaoming Luo (OPPO)

	Presentation proposes obfuscation mechanisms for TID, AID and PN where-in one public version of these identifiers are transmitted over-the-air, and another hashed version containing the identifiers foreseen in the standard are kept private between AP and non-AP STA.

	**C:** The OTA identifiers would preserve the structure of the private identifiers.
	**C:** Resetting SN may cause problems in the transition phase between an old OTA-MAC and a new OTA-MAC. It may require flushing all the packets when there is a transition.
	**C:** This proposal would require changing up to 16 values at the same time, and this might in itself generate suspicion. A possible improvement is enabling a selection of values that can be reset, especially when some of the identifiers are persistent but not transmitted.
	**C:** Maybe resetting to zero is simpler than resetting to a random number.
	**C:** If a non-AP STA is already associated. it will be difficult to reset the sequence number. Obfuscation is desirable, but we should have the "true" values still rolling.
	**C:** Pre-assigning AIDs will be a scalability issue, we have to look at that.
	2. **Obfuscate SSID of BPE AP** ([11-23-0167r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0167-00-00bi-obfuscate-ssid-of-bpe-ap.pptx)), Chaoming Luo (OPPO)

	Presentation proposes a hash function to obfuscate the SSID of a BPE, so that BPE AP effectively maintain two SSIDs. BPE Clients would cache "true" SSIDs of BPA APs.

	**C:** It may not be possible to have a dependency on SAE password, since the OTA SSID would then get a unique value per user. This may also be a problem in the case multiple PSKs are used.
	**C:** Each SSID would have to be decoded with the random number that is included in same beacon or probe response. A random number would have to be transmitted before a first OTA SSID is transmitted.
	**C:** There is a risk that this would be confusing to legacy devices. It might be better to have separate scanning operations for BPE and non-BPE to help legacy devices.
	**Q:** Why is SSID part of the AP identification information?
	**A:** It was included in the discussion leading up to Requirement 18.
	**Q:** The idea is that two SSIDs map to the same BSS?
	**A:** Yes.
	3. **Varying PMKID and SAE password ID** ([11-23-0168r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0168-00-00bi-varying-pmkid-and-sae-password-id.pptx)), Chaoming Luo

	Presentation proposes to generate a new PMKID at each successful (re)association.

	**C:** This is related to 11-23-44r3 (Protected SAE password identifiers). This may already be solved by Rev-me taskgroup.
	**C:** Another relevant prior contribution is 11-22-1666r2. Using the PTK assumes re-doing the 4-way-handshake, and if you don't do the 4-way-handshake you don't get a new PMKID. This is resource intensive.
	C: The information that needs to change is not the password identifier, as such, but what is sent over the air.
	4. **Simple entropy metric for TGbi requirements** (11-23-0223r0), Amelia Andersdotter (Sky Group/Comcast)

	C: We will be encrypting a lot of the bits which should already account some of the things included in this metric.
	C: Some bits are not equally probable to be different from the others, so maybe an additional modification is necessary.
	C: We are looking at a time series in addition, where maybe the Cocktail Problem would be a good direction to look,
4. **AoB**
	1. No other business.
5. Chair adjourned the meeting at 11:52 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | Sky Group/Comcast |
| Ansley, Carol | Cox Communications Inc. |
| baron, stephane | Canon Research Centre France |
| DeLaOlivaDelgado, Antonio | InterDigital, Inc. |
| Harkins, Daniel | Hewlett Packard Enterprise (Aruba Networks) |
| Hawkes, Philip | Qualcomm Incorporated |
| Henry, Jerome | Cisco Systems, Inc. |
| Levy, Joseph | InterDigital, Inc. |
| Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| Malinen, Jouni | Qualcomm Technologies, Inc |
| McCann, Stephen | Huawei Technologies Co., Ltd |
| RISON, Mark | Samsung Cambridge Solution Centre |
| Sam, Harvey | Broadcom Corporation |
| Smith, Luther | Cable Television Laboratories Inc. (CableLabs) |
| Sun, Bo | Sanechips |