IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Teleconference Minutes 21 October 2021 | | | | |
| Date: 2021-11-01 | | | | |
| 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 on 21 October 2021 at 09:00 ET. Last 30 minutes notes kindly taken by Stephen McCann (Huawei).

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, self**

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

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

Chair calls meeting to order at 09:03 ET.

Agenda slide deck: 11-21-1638r2:

1. Reminder to do attendance
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.
   1. No questions
4. **Discussion of agenda 11-21-1638r2 (slide 16)**
   1. Request to add MAC Address Persistence (11-21-1715r0).
   2. Request to present document 11-21-1697r0 MAC Privacy and PMKSA caching as per reflector request earlier this week. Request for clarification on procedure for requesting agenda time.
   3. Adoption of agenda 11-21-1638r2 slide 16 as amended by unanimous consent.
5. **Administrative:** 
   1. Reminder: One more teleconference before plenary on 4 Nov at regular 9AM ET slot for one hour.
6. **Presentations.** 
   1. **Rotating MAC Address over the air (11-21/1539r0)**, Antonio de la Oliva (Interdigital)

**Discussion**

Q: The over the air-MAC could get rotated very quickly, but do you have proposals on how that would get negotiated in the network?

A: We could work on this.

Q: High-level this is interesting and useful to split network and over-the-air. On slide 5 you say that the network MAC would be used for association, but that would mean it's exposed at that time. Is that actually what you mean? Shouldn't it be always protected?

A: What we're saying is that the network MAC needs to be used for cryptographic encapsulation, that's basically it.

Q: In the figures on slides 6 and 7 you imply that CCMP will be handled a certain way. I don't like that, but we can deal with it later. There will be really big problems if you try to change contents in the header after the encapsulation for most implementations. High-level everything here is OK but we'll have to work on details to see what actually works.

A: I'll be fine to work on something together to find what works.

* 1. **MAC Address persistence within an ESS addition (11-21/1715r0)**, Thomas Derham (Broadcom)

**Discussion**

Q: Is this a new slide or a modification of an existing slide?

A: It's a modification.

**Straw Polls**

SP 1: **Do you agree updating “STA MAC persistence within an ESS” issue into TGbi proposed issues document (DCN 21-641)?**

Use-case/issue to be updated in issue tracking document.

* 1. **MAC Privacy and PMKSA caching (11-21/1697r1)**, Mike Montemurro (Huawei)

**Discussion**

C: Take a look at the issue tracking document and see how it relates to already existing issues.

C: The issue tracking document also has high-level references to possible solutions to the issues.

Q: There seems to be a discrepancy between slide 3 and the process for PMKID update on slide 7. Is there not a risk of hand-shakes getting out of step?

A: I don't think so. But we could look closer at this.

C: My memory is we already discussed briefly in md, but I don't think there are any similar issues already raised and I would include this being tracked by our group. But I also agree we need to find a way of updating ids and keys at the same time, and look for what is the best way of synchronising across STAs.

Q: What sort of enforcement will there be on legacy devices?

A: In 802.11aq there’s a statement about when SSID elements are placed into frames, information can be leaked.

C: I think it is also a problem that needs to be solved.

1. AoB
   1. None
2. Chair adjourned the meeting at 09:51 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | Sky UK Group |
| Ansley, Carol | Cox Communications Inc. |
| Bhandaru, Nehru | Broadcom Corporation |
| Carney, William | Sony Group Corporation |
| DeLaOlivaDelgado, Antonio | InterDigital, Inc. |
| Halasz, David | Morse Micro |
| Hamilton, Mark | Ruckus/CommScope |
| Hawkes, Philip | Qualcomm Incorporated |
| Henry, Jerome | Cisco Systems, Inc. |
| Hernandez, Marco | National Institute of Information and Communications Technology (NICT) |
| Hervieu, Lili | Cable Television Laboratories Inc. (CableLabs) |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Kain, Carl | USDOT; Noblis, Inc |
| Kneckt, Jarkko | Apple, Inc. |
| Lumbatis, Kurt | CommScope, Inc. |
| Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| Malinen, Jouni | Qualcomm Incorporated |
| McCann, Stephen | Huawei Technologies Co., Ltd |
| Montemurro, Michael | Huawei Technologies Co., Ltd |
| Petrick, Albert | InterDigital |
| RISON, Mark | Samsung Cambridge Solution Centre |
| Sevin, Julien | Canon Research Centre France |
| Smith, Graham | SRT Wireless |
| Yee, Peter | NSA-CSD |