IEEE P802.11
Wireless LANs

|  |
| --- |
| Telecon Minutes for REVmd CRC- June 17-19 2020 |
| Date: 2020-06-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jon Rosdahl | Qualcomm Technologies, Inc. | 10871 N 5750 WHighland, UT 84003 | +1-801-492-4023 | jrosdahl @ ieee.org |
| Michael Montemurro | BlackBerry | 4701 Tahoe Blvd, Mississauga, ON L4W 0B4 | +1 289-261-4183 | mmontemurro@blackberry.com  |

Abstract

Minutes for the 802.11md REVmd CRC Telecons for June 17 and 19, 2020.

R0: Minutes for June 17, 2020 – Thanks to Mike for helping with Minutes.

1. **IEEE 802.11md REVmd CRC Telecon Wednesday June 17, 2020 16:00-18:00 ET**
	1. **Called to order at 4:03pm** ET by the TG Chair Dorothy STANLEY (HPE)
	2. **Review Patent and Participation Policy**
		1. No Issues noted.
	3. **Attendance:** -please log with IMAT:
		1. About 12 attendees reported by WebEx

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | TGmd | 6/17 | Au, Kwok Shum | Huawei Technologies Co., Ltd |
|  | TGmd | 6/17 | Coffey, John | Realtek Semiconductor Corp. |
|  | TGmd | 6/17 | Derham, Thomas | Broadcom Corporation |
|  | TGmd | 6/17 | Goodall, David | Morse Micro |
|  | TGmd | 6/17 | Hamilton, Mark | Ruckus Wireless |
|  | TGmd | 6/17 | Levy, Joseph | InterDigital, Inc. |
|  | TGmd | 6/17 | Montemurro, Michael | BlackBerry |
|  | TGmd | 6/17 | NANDAGOPALAN, SAI SHANKAR | Cypress Semiconductor Corporation |
|  | TGmd | 6/17 | Qi, Emily | Intel Corporation |
|  | TGmd | 6/17 | RISON, Mark | Samsung Cambridge Solution Centre |
|  | TGmd | 6/17 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
|  | TGmd | 6/17 | Stanley, Dorothy | Hewlett Packard Enterprise |

* + 1. Missing from IMAT: None reported
	1. **Review Agenda**: 11-20/535r24:
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0535-24-000m-2020-april-july-teleconference-agendas.docx>
		2. **The draft agenda for the teleconferences is below:**

1.       Call to order, attendance, and patent policy

a.       **Patent Policy: Ways to inform IEEE:**

1. Cause an LOA to be submitted to the IEEE-SA (patcom@ieee.org); or
2. Provide the chair of this group with the identity of the holder(s) of any and all such claims as soon as possible; or
3. Speak up now and respond to this Call for Potentially Essential Patents

If anyone in this meeting is personally aware of the holder of any patent claims that are potentially essential to implementation of the proposed standard(s) under consideration by this group and that are not already the subject of an Accepted Letter of Assurance, please respond at this time by providing relevant information to the WG Chair

b.      Patent, Participation slides: See slides 5-12 in <https://mentor.ieee.org/802.11/dcn/20/11-20-0308-00-000m-2020-march-tgmd-agenda.pptx>

2.  Editor report – Emily QI/Edward AU

3.  Comment resolution:

1. **2020-06-17 Wednesday 4-6pm Eastern 2 hours**
	1. Mark HAMILTON CIDs – 11-20/338r8 –

<https://mentor.ieee.org/802.11/dcn/20/11-20-0338-08-000m-revmd-initial-sa-comments-assigned-to-hamilton.docx>

* 1. Jon Rosdahl - GEN CIDs

<https://mentor.ieee.org/802.11/dcn/20/11-20-0147-11-000m-sb1-revmd-gen-comments.xls>

4.       AOB

5. Adjourn

* + 1. Discussion of Agenda
			1. No comments on proposed agenda
		2. No objection to updated Agenda see R25
	1. **Editor Report** – Emily QI (Intel)
		1. No update since Friday’s report.
	2. **Review doc 11-20/338r8** – Mark HAMILTON (Ruckus/CommScope)
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0338-08-000m-revmd-initial-sa-comments-assigned-to-hamilton.docx>
		2. CID 4723 (MAC)
			1. Review status and history of the comment discussion.
			2. Review table 12-10.
			3. From discussion: AKMs 00-0F-AC:14-17 use AES-SIV
* There is no padding needed with AES-SIV.
* So, we now have wrapping algorithms other than “NIST AES Key Wrap”, and padding is confitional. The baseline text was wrong on this aspect. This is now a technical change/fix.
	+ - 1. Proposed Resolution: Revised. Change “encrypted GTK” to “wrapped GTK” (as requested by the commenter). Same thing at P2698.15 (in the description of the Authenticator state machine).

Similarly, replace “Encrypted” with “Wrapped” in Figures 4-32 and 4-33.

In 13.8.5 (P2748.59), change

“If a GTK, an IGTK or a BIGTK(#2116) are included, (#102)the Key field of the subelement shall be encrypted using KEK (#102)(when the negotiated AKM is 00-0F-AC:3, 00-0FAC:4, 00-0F-AC:9, or 00-0F-AC:13) or KEK2 (when the negotiated AKM is 00-0F-AC:16 or 00-0F-AC:17) and the NIST AES key wrap algorithm. The Key field shall be padded before encrypting if the key length is less than 16 octets or if it is not a multiple of 8.”

to

“If a GTK, an IGTK or a BIGTK are included, the Key field of the subelement shall be wrapped using KEK and/or KEK2 and the appropriate key wrap algorithm, as specified in Table 12-10.”

At P2668.7 and P2668.10, change “key-wrap” to “key wrap”.

* + - 1. Discussion: need to ensure editors identify 3 instances of changes in the last paragraph.
			2. Item to still resolve: 4-32 and 4-33 – difference in function listed 3 times vs listing the function with 3 parameters.
			3. Identification of where padding specified to ensure deleting the padding info is correct.
			4. Discussion on KEK2 vs KEK wrapping and if it is done twice or not.
			5. Table 12 has some issues that will need more homework.
			6. Comparing 4-31 and 4-32 are describing independent processes, so 4-32 is probably the one that needs to be changed.
			7. Discussion on how to describe KEK2 process and if it is defined in Table 12-10, so no more changes in text.
			8. More work needed – pull from Motion on Friday.
		1. CID 4221 (MAC)
			1. Review comment
			2. Discussed previously, reviewed the history.
			3. Proposed Resolution: Revised; Delete “valid” at 1618.41, as requested.

Also, replace “no valid TSF timestamp is present” with “no timestamp is present” at both P2199.63 and P2200.2.

* + - 1. Discussion on if there are more instances of “valid TSF timestamp”
			2. Suggestion that “valid” is not needed in all cases.
			3. Table 9-227 – discussion on if deleting “valid” is meaningful or not.
			4. Discussion on the use of values vs enumerated name/descriptions.
			5. Direction to change similar to “Statuks field indicating “Accept, timestamp present iin TIM Frames” “.
			6. More work to make the changes throughout.
		1. CID 4377 (MAC)
			1. Review Comment
			2. Review discussion history
			3. No objection to the bit numbering
			4. No objection to change 9-114 and 9-115.
			5. Proposed resolution: Revised; Proposed Resolution:

Subtract 1 from each of the bit positions in the Figures 9-12, 9-13, 9-16, 9-21, 9-687.

Subtract 4 from each of the bit positions in Figures 9-8, 9-338.

Subtract 8 from each of the bit positions in Figure 9-9.

Subtract 3 from each of the bit positions in Figure 9-17.

Subtract 9 from each of the bit positions in Figures 9-18, 9-19.

Subtract 18 from each of the bit positions in Figure 9-22.

Subtract 29 from each of the bit positions in Figure 9-559.

Subtract 34 from each of the bit positions in Figure 9-560.

Subtract 1 from each of the bit numberings in Figures 9-114 and 9-115.

Correct “B4” to “B0” in Figure 9-838.

Request the Editors to add a statement in the Editors Guide that all format figures shall number bits from B0.

Action ITEM: Request the Editors to add a statement in the Editors Guide that all format figures shall number bits from B0.

* + - 1. No objection - Ready for Motion.
		1. CID 4485 (MAC)
			1. Review comment.
			2. Review history of discussion.
			3. Still need to add a phrase for a convention for reserved fields.
			4. Proposed Text to add:

“Reserved field and subfield values are not used upon transmission.

NOTE—Should a future revision of this standard make use of such values, it is intended that steps be taken to ensure only devices compliant with this future revision are expected to receive and process them.”

* + - 1. Discussion on what happens when reserved fields or reserved values are received and what the action should be.
			2. Debate on the action of the reception of a reserved value.
			3. Discussion on the new text to add that covers the values.
			4. Proposed Resolution: CID 4485: Revised. Replace, at the cited location, “Setting this field to 0 indicates that the low rate TIM frame is not transmitted.” with “The value 0 is reserved.”

Add to the end of subclause 9.2.2:

* + - 1. “Reserved field and subfield values are not used upon transmission. Upon reception of a reserved field or subfield value, the behavior is undefined.”
			2. No objection – Mark Ready for Motion
		1. CID 4442 (MAC)
			1. Review Comment
			2. Review the context of the proposed change and description of “co-located”. Different higher layer entities will send synch to the lower MAC and have the indication passed through the SAP.
			3. This is just trying to clean up the language description the operation and behavior.
			4. Discussion of PPDU and MPDU vs Data Frame usage and what is being depicted.
			5. Proposed Resolution: CID 4442: Revised; Replace the second and third sentences with: “When the MAC transmits a Data frame with an Address 1 match, the MLME-HL-SYNC.indication shall occur when the last symbol of the PPDU carrying the Data frame is transmitted. When the MAC receives a Data frame with an Address 1 match, the MLME-HL-SYNC.indication shall occur when the last symbol of the PPDU carrying the matching Data frame is received.”
			6. No objection – Mark Ready for Motion
		2. CID 4418 (MAC)
			1. Review Comment
			2. Proposed Resolution: Accept
			3. Review summary of the changes.
			4. No objection – Mark Ready for Motion.
	1. **GEN Comments** – document 11-20/147r11 - Jon ROSDAHL (Qualcomm)
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0147-11-000m-sb1-revmd-gen-comments.xls> -
		2. These comments can be viewed in 11-20/147r11, but we are processing directly from the database today.
		3. CID 4170 (GEN)
			1. The proposed resolution is technically correct, but it would make existing implementations non-compliant.
			2. Some devices “work around the issue” by setting the probe delay to 0. However, probe delay cannot be set to 0. ProbeDelay is a local variable unique to the scanning procedure.
			3. A new MIB variable could be created to allow a probe delay of 0.
			4. This comment needs a submission and some discussion.
			5. Discussion on the proposed resolution, or to possibly create a new variable.
			6. Possible MIB variable to be added is one possible solution. If the MIB variable allows zero, then existing devices can use zero. The issue is not arriving at the new Channel and starting to transmit too early.
			7. ACTION ITEM: Menzo WENTINK to create a submission
			8. If no submission comes forward, the comment will need a rejection reason.
		4. CID 4169 (GEN)
			1. This comment is related to CID 4170.
			2. CID 4169 only has a proposed change to clause 11.8.9 but no changes to the primitives.
			3. The issue needs to be specified for legacy PHYs as well as new PHYs
			4. The resolution to CID 4170 should apply to CID 4169 as well.
		5. CID 4115 (GEN)
			1. Clause 11.18 in the proposed resolution would become Clause 11.17.
			2. There is agreement to moving the sub-clause but there isn’t agreement on the proposed destination for the sub-clause.
			3. The first chapter 10 clause dealing with RSNA is clause 10.25.
			4. SPP refers to Signaling and Payload Protected and has was added as part of 802.11n.
			5. The sub-clause should be moved to Clause 10 or Clause 12. Maybe the sub-clause should be a sub-clause of Clause 10.11.
			6. In Clause 11, there are a number of security procedures that are applied. For instance, Beacon Protection procedures are added to the MLME.
			7. A-MSDU does not belong in Clause 11.
			8. If there is a strong preference to move the sub-clause, it should be moved to after Clause 10.11. We could move it to Clause 10.11.2
			9. We could move the two paragraphs to the end of Clause 10.11.
			10. Proposed Resolution: CID 4115 (GEN) REVISED (GEN: 2020-06-17 21:53:23Z) Move the contents of 11.17 and place the contents at the end of clause 10.11 and delete the current 11.17 and renumber the remaining subclauses after it.
			11. No objection – Mark Ready for Motion
	2. **Review agenda for next call.**
	3. **Adjourn at 5:59pm**

**References:**

**July 17, 2020:**

1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0535-24-000m-2020-april-july-teleconference-agendas.docx>
2. <https://mentor.ieee.org/802.11/dcn/20/11-20-0308-00-000m-2020-march-tgmd-agenda.pptx>
3. <https://mentor.ieee.org/802.11/dcn/20/11-20-0338-08-000m-revmd-initial-sa-comments-assigned-to-hamilton.docx>
4. <https://mentor.ieee.org/802.11/dcn/20/11-20-0147-11-000m-sb1-revmd-gen-comments.xls>