IEEE P802.11
Wireless LANs

|  |
| --- |
|  Telecon Minutes for REVme - August 2022 |
| Date: 2022-08-08 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jon Rosdahl | Qualcomm Technology, Inc. | 10871 N 5750 WHighland, UT 84003 | +1 801 – 492 – 4023 | jrosdahl @ ieee . org |
|  |  |  |  |  |

Abstract

 Telecon Minutes for REVme - August 2022

Ro: August 8th Telecon.

1. **TGme (REVme) Telecon –Monday, August 8, 2022, at 10:00-12:00 ET**
	1. **Called to order** 10:07 am ET by the TG Chair, Michael MONTEMURRO (Huawei).
	2. **Introductions of other Officers present:**
		1. Vice Chair - Mark HAMILTON (Ruckus/CommScope)
		2. Vice Chair - Mark RISON (Samsung)
		3. Editor - Emily QI (Intel)
		4. Editor – Edward AU (Huawei)
		5. Secretary - Jon ROSDAHL (Qualcomm)
	3. **IMAT Reported attendance**

|  |  |  |
| --- | --- | --- |
|  | Name | Affiliation |
| 1 | Au, Kwok Shum | Huawei Technologies Co., Ltd |
| 2 | Coffey, John | Realtek Semiconductor Corp. |
| 3 | Hamilton, Mark | Ruckus Wireless |
| 4 | Levy, Joseph | InterDigital, Inc. |
| 5 | McCann, Stephen | Huawei Technologies Co., Ltd |
| 6 | Montemurro, Michael | Huawei Technologies Co., Ltd |
| 7 | Qi, Emily | Intel |
| 8 | RISON, Mark | Samsung Cambridge Solution Centre |
| 9 | Rosdahl, Jon | Qualcomm Technologies, Inc. |

* 1. **Review Patent Policy and Copyright policy and Participation Policies.**
		1. No issues were noted.
	2. **Review agenda**:11-22/1173r2:
		1. <https://mentor.ieee.org/802.11/dcn/22/11-22-1173-02-000m-july-august-teleconference-agenda.docx>
		2. Reviewed,
		3. No changes
		4. No objection to approval of agenda
	3. **CID SEC** Michael Montemurro (Huawei)
		1. CID 1922 (SEC)
			1. Review comment
			2. Review proposed changes
			3. Discussion on why this change is needed.
			4. Proposed Resolution: accepted
			5. No objection – Mark Ready for Motion
		2. CID 1766 (SEC)
			1. Review Comment
			2. Review adhoc notes describing the change to be made.
			3. Proposed resolution: CID 1766 (SEC): Revised. At 3186.6, insert the following paragraph (after the first paragraph):
			4. "NOTE---A Protected Dual of Public Action frame is protected by encryption if it is individually addressed and by a MIC if it is group addressed."
			5. No objection – Mark Ready for Motion
		3. CID 1765 (SEC)
			1. Review Comment
			2. Discuss the need for “should” vs “shall”.
			3. Discussion on the format of the sentence.
			4. Proposed Resolution: REVISED (SEC: 2022-08-08 14:34:03Z) - At 3186.7, insert the following paragraph:
			5. "When a Public Action frame is received, but a Protected Dual of Public Action frame should have been used, the frame should be discarded."
			6. No objection – Mark Ready for Motion
		4. CID 1733 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted
			3. No Objection – Mark Ready for Motion
		5. CID 2177 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted
			3. No Objection – Mark Ready for Motion
		6. CID 1591 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted
			3. No Objection – Mark Ready for Motion
		7. CID 1788 (SEC)
			1. Review Comment
			2. Similar to CID 1789 (SEC)
			3. Make the same resolution to both CIDs.
			4. Proposed Resolution for both CID 1788 and CID 1789 (SEC): REVISED (SEC: 2022-08-08 14:46:12Z) - At 3205.56, change

"Key Ack (bit 7) is set to 1 in messages from the Authenticator if an EAPOL-Key frame is required in response to this message and is 0 otherwise."

to

"Key Ack (bit 7) is set to 1 if sent by the Authenticator and is set to 0 otherwise."

* + - 1. No objection – Mark Ready for Motion
		1. CID 1832 (SEC)
			1. Review Comment
			2. Proposed Resolution: REVISED (SEC: 2022-08-08 14:48:26Z) - At 3206.36, change "pairwise temporal key" to "temporal key"
			3. No objection – Mark Ready for Motion
		2. CID 1578 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted
			3. No Objection – Mark Ready for Motion
		3. CID 1786 (SEC)
			1. Review Comment
			2. Discussion on the need for the NOTE.
			3. Proposed Resolution: REVISED (SEC: 2022-08-08 15:05:40Z) - At 3206.8, delete "(this should be before receiving message 3 of the 4-way handshake)"

After the cited paragraph, insert:

"NOTE -- The Secure bit is set to 1 in messages 3 and 4 of the 4-way handshake."

* + - 1. No Objection – Mark Ready for Motion
		1. CID 1839 (SEC)
			1. Review Comment
			2. Discussion on which entity is being described.
			3. There is a Set of resolutions in 11-22/0355 starting at CID 1273 that has changes to help clarify this area.
			4. For this CID, only the NOTE to be added is needed.
			5. Proposed Resolution: REVISED (SEC: 2022-08-08 15:17:16Z) - After the cited paragraph, insert the following note:

"NOTE---An EAPOL-Key request frame requests initiation of a 4-way handshake or group key handshake. An EAPOL-Start frame requests initiation of an EAP handshake."

* + - 1. No Objection – Mark Ready for Motion
		1. CID 1237 (SEC)
			1. Skip for now, need to check CID 1822.
		2. CID 1709 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted
			3. No Objection – Mark Ready for Motion
		3. CID 1822 (SEC) with CID 1237 (SEC)
			1. Review Comments
			2. See CID 1822's Ad Hoc notes for the combined discussion.
			3. Proposed Resolution for CID 1822 (SEC) and CID 1237 (SEC):

REVISED (SEC: 2022-08-08 15:26:04Z) - At 3207.10, change

"The Authenticator should use the key replay counter to identify invalid messages to silently discard."

To be:

"The Authenticator shall use the key replay counter to identify invalid messages."

At 3207.13, change "should also" to "shall also"

At 3207.16, change "field should not be updated" to "field shall not be updated"

At 3207.17, change

"In other words, the Supplicant never updates" to

"In other words, the Supplicant shall not update"

* + - 1. No Objection – Mark Ready for Motion
		1. CID 1568 (SEC) CID 1569 (SEC) and 1575 (SEC)
			1. Review comments
			2. Discussion on the proposed changes.
			3. Proposed Resolution for CID 1568 (SEC), CID 1569 (SEC) and CID 1575 (SEC):

REVISED (SEC: 2022-08-08 15:35:48Z) - At 3209.30 and 3209.33, change: "the GroupKey" to "key material (e.g. the GTK)"

At 3209.33. Change "the EAPOL-Key frames shall be ignored." to "the EAPOL-Key frame shall be ignored."

* + - 1. No Objection – Mark Ready for Motion
		1. CID 1825 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted
			3. No Objection – Mark Ready for Motion
		2. CID 1828 (SEC)
			1. Review Comment
			2. Proposed Resolution: REVISED (SEC: 2022-08-08 15:42:56Z) - At 3216.42, change
			3. Change "set in EAPOL-Key frames" to "set to 1 in EAPOL-Key frames"
			4. No objection – Mark Ready for Motion
		3. CID 1946 (SEC)
			1. Review Comment
			2. Discussion on the specifics of the proposed resolution.
			3. Proposed Resolution: REVISED (SEC: 2022-08-08 15:46:11Z) - At cited location, change:

"to establish an initial PTKSA, GTKSA, if management frame protection is enabled, an IGTKSA, (11ba)if beacon protection is enabled, a BIGTKSA(11ba), and if WUR frame protection is negotiated, a WIGTK, that is based on this protocol."

to

"to establish an initial set of security associations: PTKSA,

GTKSA, IGTKSA if management frame protection is enabled, BIGTKSA if beacon protection is enabled, and WIGTKSA if WUR frame protection is negotiated."

* + - 1. No objection – Mark Ready for Motion
		1. CID 1238 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted
			3. No objection – Mark Ready for Motion
		2. CID 1239 (SEC)
			1. Review Comment
			2. Proposed Resolution: REVISED (SEC: 2022-08-08 15:50:55Z) - At 3218.56, change:

"and Supplicant RSNE indicates OCVC capability, the Authenticator silently discards message 2 if any of the following are true:"

to

"and the Supplicant RSNE indicates OCVC capability, the Authenticator shall silently discard message 2 if any of the following are true:"

* + - 1. No objection – Mark Ready for Motion
		1. CID 1908 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted.
			3. No Objection – Mark Ready for Motion
		2. CID 1240 (SEC)
			1. Review Comment
			2. Proposed Resolution: Accepted.
			3. No Objection – Mark Ready for Motion
		3. CID 1827 (SEC)
			1. Review Comment
			2. Proposed Resolution: ACCEPTED (SEC: 2022-08-08 15:54:54Z)

Note to Editor, the proposed change is:

At 3220.1, Change

"MIC(KCK, EAPOL) or MIC(SKCK, EAPOL)"

to

"MIC(KCK, EAPOL)".

* + - 1. No Objection – Mark Ready for Motion
		1. CID 1242 (SEC)
			1. Review Comment
			2. Proposed Resolution: REVISED (SEC: 2022-08-08 15:58:26Z) -

At 3221.13, change

"and Authenticator RSNE indicates OCVC capability, the Supplicant silently discards message 3"

to

"and the Authenticator RSNE indicates OCVC capability, the Supplicant shall silently discard message 3"

* + - 1. No Objection – Mark Ready for Motion
	1. **Adjourned 11:59am ET**

**References:**

**August 8th:**

1. <https://mentor.ieee.org/802.11/dcn/22/11-22-1173-02-000m-july-august-teleconference-agenda.docx>