IEEE P802.11
Wireless LANs

|  |
| --- |
| Minutes for REVmd May and June 2018 telecons |
| Date: 2018-05-25 |
| 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 |
| Mark Hamilton | Ruckus/ARRIS | 350 W Java DrSunnyvale, CA 94089 | +1-303-818-8472 | mark.hamilton@arris.com |

Abstract

Minutes for REVmd 25th May and 1st, 15th and 22nd June 2018 telecons

R0 = REVmd May 25th Telecon

Teleconferences are subject to applicable policies and procedures, see below.

==================================================

•       IEEE Code of Ethics

–       <http://www.ieee.org/about/corporate/governance/p7-8.html>

•       IEEE Standards Association (IEEE-SA) Affiliation FAQ

–       <http://standards.ieee.org/faqs/affiliation.html>

•       Antitrust and Competition Policy

–       <http://standards.ieee.org/resources/antitrust-guidelines.pdf>

•       IEEE-SA Patent Policy

–       <http://standards.ieee.org/develop/policies/bylaws/sect6-7.html>

–       [https://development.standards.ieee.org/myproject/Public//mytools/mob/loa.pdf](http://standards.ieee.org/board/pat/pat-slideset.ppt)

–       <http://standards.ieee.org/board/pat/faq.pdf>

–       <http://standards.ieee.org/board/pat/pat-slideset.ppt>

•       IEEE 802 Working Group Policies &Procedures (29 Jul 2016)

–       <http://www.ieee802.org/PNP/approved/IEEE_802_WG_PandP_v19.pdf>

•       IEEE 802 LMSC Chair's Guidelines (Approved 09 Mar 2018)

–       <https://mentor.ieee.org/802-ec/dcn/17/ec-17-0120-26-0PNP-ieee-802-lmsc-chairs-guidelines.pdf>

•       Participation in IEEE 802 Meetings

–       <https://mentor.ieee.org/802-ec/dcn/16/ec-16-0180-05-00EC-ieee-802-participation-slide.pptx>

•       IEEE 802.11 WG OM: (Approved 10 Nov 2017)

–       <https://mentor.ieee.org/802.11/dcn/14/11-14-0629-21-0000-802-11-operations-manual.docx>

1. **May 25, 2018 REVmd Telecon – 802.11md**
	1. **Called to order at 10:03 ET** by the TG Chair Dorothy Stanley (HPE)
	2. Attendance:
		1. Dorothy Stanley (HPE)
		2. Ganesh Venkatesan (Intel)
		3. Chris Hansen (Peraso)
		4. Mark Hamilton (ARRIS/Ruckus)
		5. Emily Qi (Intel)
		6. Joseph Levy (InterDigital)
		7. Roger Marks (Huawei)
		8. Mike Montemurro (Blackberry)
		9. Sean Coffey (Realtek)
		10. Menzo Wentink (Qualcomm)
	3. **Reviewed Patent Policy** and Participation Policy
	4. **Review Agenda:**
		1. <https://mentor.ieee.org/802.11/dcn/18/11-18-1007-01-000m-tgmd-2018-may-june-teleconference-agendas.docx>

Draft agenda for the May 25th teleconference:

1.       Call to order, attendance, and patent policy

a.       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:**

                                                               i.      Either speak up now or

                                                             ii.      Provide the chair of this group with the identity of the holder(s) of any and all such claims as soon as possible or

                                                           iii.      Cause an LOA to be submitted

b.      <https://mentor.ieee.org/802-ec/dcn/16/ec-16-0180-05-00EC-ieee-802-participation-slide.pptx>

2.       Editor report – Emily QI

a.       Editor report document, <https://mentor.ieee.org/802.11/dcn/17/11-17-0920-09-000m-802-11revmd-editor-s-report.ppt>

b.      Comments received on LB 232 are here: <https://mentor.ieee.org/802.11/dcn/18/11-18-0611-03-000m-revmd-wg-ballot-comments.xls>

3.       Comment resolution.

 **2018-05-25**

* + - 1. Youhan KIM – CID 1374 (10 mins)
			2. Sigurd S 11-18-701 CIDs 1359 (10 mins)
			3. Roger MARKS – CID 1533 (10 mins)
			4. Mike MONTEMURRO - PHY CIDs 1552, 1324, 1264, 1188, 1004, 1552 , 11-18-0899 (80 mins)
		1. No objection to the proposed agenda that was in the 11-18/1007r1
		2. Also reviewed upcoming meeting plans, and adjusted to match presenters’ availability.
	1. **Editor Report – 11-17/920r9** - Emily Qi
		1. <https://mentor.ieee.org/802.11/dcn/17/11-17-0920-09-000m-802-11revmd-editor-s-report.ppt>
		2. Reviewed report
		3. Volunteers are helping with review of D1.1.
		4. CID 1486 (EDITOR) needs discussion. Will revisit later on this call.
	2. **Review Submission 11-18/949r3** – CID 1533 (MAC) - Roger MARKS:
		1. <https://mentor.ieee.org/802.11/dcn/18/11-18-0619-00-000m-revmd-editor2-lb232-comments.xlsx>
		2. This is a minor revision of document reviewed in Warsaw.
		3. CID 1533 (MAC) – changes to Neighbor Report
		4. Since Warsaw, in discussion with Mark RISON, added clarification that an SSID is “corresponding to” an AP.
		5. No comments, or concerns.
		6. CID 1533, Ready for motion. Incorporate changes as shown in 11-18-0949r3. These changes clarify the use of the FILS Discovery frame.
	3. **CID 1486 (EDITOR)** - Emily QI:
		1. Reviewed email exchange on CID 1486.
		2. Intention was for ACCEPTED on this comment. However, Editors have determined that implementation of the resolution has some ambiguity.
		3. 1. Is the change only meant to apply to the Measurement Request/Reply frames, and not (for example) Measurement Request/Reply element?
		4. 2. In 6.3.14 and 6.3.16, it may not work to add “Spectrum” to the primitives.
		5. 3. Other issues. For example, in 4.3.11.9, “a Measurement Request frame” is not “a Spectrum Measurement Request frame”
		6. Move comment to MAC.
		7. ACTION: Assign to Emily, for further work.
	4. **PHY Motion A-comment** tab - Mike MONTEMURRO:
		1. CID 1004 (PHY):
			1. Similarly is arguably incorrect here. It is not the 802.1X AS that should not expose the key, it is the Authenticator. Nothing wrong with the bullet, without the “Similarly”
			2. Maintain the ACCEPTED proposed resolution.
			3. Ready for Motion.
		2. CID 1264 (PHY):
			1. This was REJECTED, because we are not maintaining deprecated features such as TKIP.
			2. Comment from Mark RISON, that if we are keeping feature text, it should not be incorrect.
			3. Discussion about how clearly we indicate features that are deprecated, where the reader will see it. In this case, at the top of 12.2 (in 12.2.1) we stated that TKIP is deprecated.
			4. Maintain the REJECTED resolution.
			5. Ready for motion.
		3. CID 1552 (PHY):
			1. Mark RISON comment that an RSNE does not have a PMKID field. Also, don’t we need to say REVSIED (and not ACCEPTED) if any change is directed, no matter how trivial?
			2. The major issue seems to be the concern about an “PMKID field” within an RSNE.
			3. Reviewed P2506.1. This seems to use PMKID field.
			4. Reviewed the format definition for RSNE. There is a PMKID Count and PMKID List, which is a list of PMKIDs. It does seem that “PMKID field” is incorrect, even though there are other occurrences in the text.
			5. Suggest changing the new text here to “added in the PMKID List field”.
			6. Reviewed P2505.8. This is an example of the same problem in the existing text.
			7. Searched for other examples of “PMKID field”.
			8. P2416.27: Probably should be “PMKID List field includes one PMKID which is KeyName”
			9. This will take a lot of time to check all existing occurrences and make sure they are correctly appropriately.
			10. We can resolve this comment (CID 1552), per the above change. Leave the other occurrences
			11. REVISED. With the Proposed Change, with the change to “PMKID List field” (above).
			12. Ready for motion.
			13. ACTION: Mike MONTEMURRO to check into the other existing occurrences.
		4. CID 1188 (PHY):
			1. Mark RISON comments: This is another (perhaps) deprecated feature, and should not be maintained.
			2. This is not a deprecated feature, it is a valid frame and field, with a possible value that indicates reference to a deprecated item.
			3. Maintain the ACCEPTED resolution.
			4. Ready for Motion.
		5. CID 1324 (PHY):
			1. Reviewed the concern that terms with shared words included are ambiguous. Disagree that this creates an ambiguity. The definitions are clear.
			2. Maintain the REJECTED resolution.
			3. Ready for motion.
	5. **Review Sumission 11-18/0899r1** (<https://mentor.ieee.org/802.11/dcn/18/11-18-0899-01-000m-lb232-comment-resolutions-mmontemurro.doc>) – REVmd LB232 comment resolutions – Mike MONTEMURRO:
		1. CID 1228 (PHY):
			1. Reviewed comment.
			2. REVISED: At 3591.21, replace “Unsigned32” with “INTEGER”
			3. At 3601.44, replace “SYNTAX Unsigned32 (0..65535)” with “SYNTAX Integer32 (-255..255)”
			4. Ready for Motion.
		2. CID 1365 (PHY) CID 1366 (PHY):
			1. Reviewed comment and discussion.
			2. Disagree that concatenation is implied. The last argument (DataKDs) is meant to be a list.
			3. Now that we’re looking at nearby examples, the cases that say this argument is 0 (zero) is confusing. It should be an empty list in that case.
			4. It would be best to create a “list” notation, maybe using curly-braces, and clean up all uses.
			5. Noted that the next comment in this document (CID 1366) is similar.
			6. ACTION: Mike MONTEMURRO to create a submission making this change globally.
		3. CID 1019 (PHY):
			1. Isn’t there a real security issue here, because our medium is not reliable, so depending on having seen the frame before isn’t reliable?
			2. Not really.
			3. But, still agree it is too late to change this.
			4. REJECTED. The proposed change would make some existing implementations non-compliant.
			5. Ready for Motion.
		4. CID 1322 (PHY):
			1. Reviewed this with security experts, and think it is correct.
			2. There is an issue with the exact wording, though. Request EAPOL frames could have a different KeyReplay Counter sequence. We need to except that from the rule.
			3. Wordsmithed.
			4. REVISED. At the cited location change "On reception of message 4, the Authenticator verifies that the Key Replay Counter field value is one that it used on this 4-way handshake"

to

“On reception of message 4, the Authenticator verifies that the KeyReplay Counter field value is one that it used on this 4-way handshake and is strictly larger than that in any other EAPOL-Key frame that has the Request bit in the Key Information field set to 0 and that has been received during this session.”

* + - 1. Ready for Motion.
		1. CID 1341 (PHY):
			1. Consulted with security experts.
			2. REJECTED. It is not accurate to describe GCMP as being "excessively vulnerable to nonce reuse". GCMP, just like CCMP, has certain requirements that are specified in the standard. In particular, neither can be used in a manner that would allow transmitted to reuse the same nonce value with the same key. GCMP is the default cipher for 60 GHz STAs and it is also in the process of being deployed in new Suite B use cases. It is not appropriate to deprecate GCMP and leave these new uses without a not-deprecated cipher suite. GCMP, when implemented correctly per the current standard requirements, prevents nonce re-use.
			3. Ready for Motion.
		2. CID 1148 (PHY):
			1. Consulted with security experts.
			2. REJECTED. Such an AP is not compliant with the standard and should be fixed. There has been limited deployment of SAE in infrastructure BSSs so far, but there has been recent interoperability testing and this identified issue is being addressed at least in some implementations. There does not seem to be sufficient justification to relax the rules for EAPOL-Key protection based on this since it looks likely that implementations get fixed before larger scale deployment.
			3. Ready for Motion.
		3. CID 1539 (PHY):
			1. Consulted with security experts.
			2. ACCEPTED.
			3. Ready for Motion.
		4. CID 1538 (PHY):
			1. Consulted with security experts.
			2. Agree with the direction they suggested.
			3. One location got missed, though, at P2422.47.
			4. REVISED. At cited paragraph, delete “When using an AEAD cipher and having PTK, this subfield is set to 1.” At 2419.4, 2422.47 and 2428.23, change “Encrypted Key Data = 0” to “Encrypted Key Data = 1 when using an AEAD cipher or 0 otherwise”
			5. Ready for Motion.
		5. CID 1346 (PHY):
			1. Reviewed comment and Figure.
			2. Suggest to just replace the “floating A circle” with the words.
			3. Another suggestion to say this without the “floating A circle” as text below the figure.
			4. Looked at Figure 17-18. General agreement that this seems okay. There are more examples, later. Make the clause 15 Figure look like this.
			5. REVISED. Add an arrow from the higher-up floating A in a circle to the Switch to RX STATE box. This changes the cited Figure to align with Figure 17-18.
			6. Ready for Motion.
		6. CID 1393 (PHY):
			1. Reviewed comment.
			2. Probably fine. Need side-by-side comparison to be sure. Or, change editing instructions to list what is actually changed.
			3. Bring back next time.
	1. **Next call**: Next week, June 1, same time.
	2. **Adjourned 12:00pm ET**.
1. **REVmd Telecon June 1, 2018 10am -12pm ET**
	1. UPDATE STARTING HERE, ON JUNE 1

**References:**

May 25th Telecon:

1. <https://mentor.ieee.org/802.11/dcn/18/11-18-1007-01-000m-tgmd-2018-may-june-teleconference-agendas.docx>
2. <https://mentor.ieee.org/802-ec/dcn/16/ec-16-0180-05-00EC-ieee-802-participation-slide.pptx>
3. <https://mentor.ieee.org/802.11/dcn/17/11-17-0920-09-000m-802-11revmd-editor-s-report.ppt>
4. <https://mentor.ieee.org/802.11/dcn/18/11-18-0611-03-000m-revmd-wg-ballot-comments.xls>
5. <https://mentor.ieee.org/802.11/dcn/17/11-17-0920-09-000m-802-11revmd-editor-s-report.ppt>
6. <https://mentor.ieee.org/802.11/dcn/18/11-18-0619-00-000m-revmd-editor2-lb232-comments.xlsx>
7. <https://mentor.ieee.org/802.11/dcn/18/11-18-0899-01-000m-lb232-comment-resolutions-mmontemurro.doc>

June 1st Telecon: