IEEE P802.11
Wireless LANs

|  |
| --- |
| Telecon Minutes for REVmd CRC- April 1 and 3 2020 |
| Date: 2020-04-03 |
| 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 |
|  |  |  |  |  |

Abstract

Minutes for the 802.11md REVmd CRC Telecon April 1 and 3, 2020 –

R0: April 1 – 16:00-18:00 ET

R1: April 3 – 10:00-12:00 ET

1. **IEEE 802.11md REVmd CRC Telecon Wednesday April 01, 2020 16:00-18:00 ET**
	1. **Called to order at 4:03pm** by the TG Chair Dorothy STANLEY (HPE)
	2. **Review Patent and Participation Policy**
		1. No Issues noted.
	3. **Attendance:** -please log with IMAT:
		1. WebEx reported 14 on call
		2. IMAT Report
			1. Andersdotter, Amelia None - Self-funded
			2. Au, Kwok Shum Huawei Technologies Co., Ltd
			3. Coffey, John Realtek Semiconductor Corp.
			4. Derham, Thomas Broadcom Corporation
			5. Goodall, David Morse Micro
			6. Hamilton, Mark Ruckus Wireless
			7. Levy, Joseph InterDigital, Inc.
			8. Montemurro, Michael BlackBerry
			9. Qi, Emily Intel Corporation
			10. RISON, Mark Samsung Cambridge Solution Centre
			11. Rosdahl, Jon Qualcomm Technologies, Inc.
			12. Smith, Graham SR Technologies
			13. Stanley, Dorothy Hewlett Packard Enterprise
			14. Yu, Mao NXP Semiconductors
	4. **Review Agenda**: 11-20/535r0:
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0535-00-000m-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>

c. Adhoc meeting reminders:

April 21-23 Cambridge UK – Not in person; teleconference proposal is below.

2.       Editor report – Emily QI/Edward AU

3.       Comment resolution

1. **2020-04-01 Wednesday – 4:00-6pm Eastern \*\*\*\*\*Teleconference announced with 10 day notice\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*(London is +5)**
	1. Emily QI - <https://mentor.ieee.org/802.11/dcn/20/11-20-0141-15-000m-sa1-proposed-resolutions-for-editor-adhoc.doc> . CIDs 4800, 4587, 4375 – 20 minutes
	2. Mark RISON - CIDs **–** 60 minutes
2. Jon ROSDAHL – GEN CIDs – 30 minutes
**Teleconferences – week of April 20, approved ad-hoc meeting [assume 9 sessions in the ad-hoc, 4 sessions suggested below, recover other 5 via successive Wednesdays; could also extend duration of calls]**
	1. 2020-04-21 Tuesday 4-6pm Eastern 2 hours
	2. 2020-04-22 Wednesday 4-6pm Eastern 2 hours
	3. 2020-04-23 Thursday 4-6pm Eastern 2 hours
	4. 2020-04-24 Friday 10 am Eastern 2 hours
3. **Teleconferences from end April to July: use Weds/Fri schedule**
	1. 2020-04-29 Wednesday 4-6pm Eastern 2 hours
	2. 2020-05-01 Friday 10 am Eastern 2 hours
	3. 2020-05-06 Wednesday 4-6pm Eastern 2 hours
	4. 2020-05-08 Friday 10 am Eastern 2 hours
	5. 2020-05-13 Wednesday 4-6pm Eastern 2 hours
	6. 2020-05-15 Friday 10 am Eastern 2 hours
	7. 2020-05-20 Wednesday 4-6pm Eastern 2
	8. 2020-05-22 Friday 10 am Eastern 2 hours
	9. 2020-05-27 Wednesday 4-6pm Eastern 2 hours
	10. 2020-05-29 Friday 10 am Eastern 2 hours
	11. 2020-06-03 Wednesday 4-6pm Eastern 2 hours
	12. 2020-06-05 Friday 10 am Eastern 2 hours
	13. 2020-06-10 Wednesday 4-6pm Eastern 2 hours
	14. 2020-06-12 Friday 10 am Eastern 2 hours
	15. 2020-06-17 Wednesday 4-6pm Eastern 2 hours
	16. 2020-06-19 Friday 10 am Eastern 2 hours
	17. 2020-06-24 Wednesday 4-6pm Eastern 2 hours
	18. 2020-06-26 Friday 10 am Eastern 2 hours
	19. 2020-07-01 Wednesday 4-6pm Eastern 2 hours
	20. 2020-07-03 Friday 10 am Eastern 2 hours
	21. 2020-07-08 Wednesday 4-6pm Eastern 2 hours
	22. 2020-07-09 Friday 10 am Eastern 2 hours

 4.       AOB

* Review TGmd schedule –
* roughly 400 comments remaining;
* target D 4.0 in July? D5.0 to RevCom
* July/Aug: 15-day recirc D4.0
* Aug-Sept comment resolution D4.0
* Sept D5.0 WG approval
* Sept – D5.0 Recirc/Unchanged recirc
* 6 Oct – 802 EC Approval, Draft TGme PAR (next revision)
* 13 October – Draft to RevCom
* 2020 Dec RevCom/SASB

5. Adjourn

* + 1. No objection to the planned agenda:
	1. **Editor Report:** Emily QI
		1. Editors are still working on updating the draft.
	2. **Review doc 11-20/0141r16** Emily QI (Intel)
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0141-16-000m-sa1-proposed-resolutions-for-editor-adhoc.doc>
		2. CID 4587 (EDITOR)
			1. Review Comment
			2. Review submission discussion.
			3. Review proposed changes
			4. Proposed Resolution: Revised.

Lowercase "Neighbor report"(s) at 191.46, 1145.39, 3686.27.

Lowercase "Neighbor Report"(s) at 3912.60.

Change "neighbor report data" to "neighbor report" at 458.35.

Change "Neighbor Report Elements" to "Neighbor Report elements" at 1527.29, and "a Neighbor Report frame" to "a Neighbor Report Response frame" on next line.

Note to the commenter: neighbor report is not a measurement type of Table 9-125. Therefore, the rules won’t apply to neighbor report.

* + - 1. No Objection – Mark Ready for Motion
		1. CID 4375 (EDITOR) REVISIT
			1. Review comment
			2. Review submission discussion
			3. Review history of the changes related to this CID.
			4. The prior resolution from earlier in March would be replaced with the updated Resolution.
			5. Proposed Resolution: Revised.

Change "Integrity Group key” to "integrity group key" in clause 6, 3 instances.

Change ", or beacon integrity group temporal key" to ", or beacon protection key" in clause 6, 3 instances.

Change the title of 12.7.1.7 “Beacon integrity group temporal key (BIGTK) hierarchy” to “Beacon protection key hierarchy”.

At 1165.22 (in 9.4.2.47), Change “The GTK subelement contains the group temporal key” to “The GTK subelement contains the GTK”

In 9.6.13.20, make following changes:

Change “The GTK subelement contains the Group Key” to “The GTK subelement contains the GTK”, at 1610.15

Change “The IGTK subelement contains the Integrity GTK” to “The IGTK subelement contains the IGTK”, at 1610.45, 1166.5.

Change “The BIGTK subelement contains the beacon integrity group temporal” to “The BIGTK subelement contains the BIGTK”, at 1611.4.

Note to the commenter: In Clause 6, the context for this is "Defines whether this key is a group key, pairwise key, PeerKey, Integrity Group key, or beacon protection key" in the Description column. These are generic references to the types of keys that are being operated on with the particular MLME primitive. "Integrity group key" seems more consistent in this context when comparing to "group key" and "pairwise key". The same logic applies 12.7.1.5 . This subclause describes the key hierarchy for integrity group keys; not for a specific IGTK.

* + - 1. No Objection – Mark Ready for Motion – Replacing previous Resolution.
		1. CID 4800 (EDITOR) REVISIT
			1. Review Comment
			2. Review previous Resolution.
			3. Review reason for revisiting
			4. Discussion on the differences with co-located vs collocated vs colocated.
			5. Straw Poll: Prefer
				1. Option A: previous Resolution: Throughout the draft, replace “collocated” (254 occurrences) and “colocated” (2 occurences) with “co-located”.
				2. Option B:

No changes to “Co-Located BSSID”.  no change to “Co-located”

No changes to “collocated interference”.  no change to “collocated”

Replace 3 instances of “colocated” with either “collocated” or “co-located”.

At 1484.13: change to “The Co-Located BSSID List subelement is present when there is at least one other BSS that is co-located within the same physical device as the reporting BSS.”

At 3907.17: change to “supporting collocated interference reporting. The capability is disabled, otherwise."

At 3907.31: change to “support collocated interference reporting is enabled.”

* + - * 1. Resolution:

A:6 B:5 Abstain: 1

* + - 1. No clear consensus – we can proceed with what we had in the proposed resolution.
			2. Secretary to include Results of Straw Polls that got us to this point:
				1. From 11-20/0261r0 – Sunrise, FL:

Motion #161 –– Failed –

2.6.8.5 Proposed Resolution: Revised.

Change “co-located” to “colocated”, 13 instances.

Change “Co-Located” to “Colocated”, 22 instances.

Change “Co-located” to “Colocated”, 1 instance.

* + - * 1. From 11-20/262r1 – Telecon March 13:

2.7.2.7 Straw Poll: Can you accept the spelling of the word?

2.7.2.7.1 A: Colocated

2.7.2.7.2 B: Co-located

2.7.2.7.3 C: Collocated

2.7.2.7.4 You have Multiple options

2.7.2.7.5 Results: A: 5 B: 4 C: 3

2.7.2.8 Slight preference to one “l” and we then discussed usages.

2.7.2.9 Straw Poll: Do you prefer the spelling of this word?

2.7.2.9.1 A: Colocated

2.7.2.9.2 B: Co-located

2.7.2.9.3 Results: A: 1 B: 7

2.7.2.10 Proposed Resolution: Accept; Note to editor, add this exception to the Editor's Guidelines.

* + 1. A Motion on the Accept resolution will be presented for consideration in future.
	1. **Review doc 11-20/435r1** Mark RISON (Samsung)
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0435-01-000m-resolutions-for-some-comments-on-11md-d3-0-sb1.docx>
		2. CID 4499 (MAC) REVISIT
			1. Review Comment
			2. Review submission discussion.
			3. In 9.5.6 – suggest change isMaster to isController (5x).
			4. In 9.5.6 – suggest change “master of the data” to “controller of the data”.
			5. Review context in the Draft.
			6. Discussion on if PC terms should be avoided or not.
			7. Concern that Master-Slave terminology may creep back in if we allow Master to remain.
			8. Straw Poll: Support the direction of resolution proposed in 11-20/262r1:
				1. Results: Yes:2 No:5 Abstain: 4
			9. No support for this Resolution -- keep the existing resolution and restore to Mark Ready for Motion.
		3. CID 4591 (EDITOR)
			1. Review comment
			2. Review the submission discussion and proposed changes.
			3. Delete one set of proposed changes.
			4. Proposed Resolution: Revised; incorporate the proposed changes for CID 4591 in doc 11-20-435r2 <<https://mentor.ieee.org/802.11/dcn/20/11-20-0435-02-000m-resolutions-for-some-comments-on-11md-d3-0-sb1.docx>>
			5. No objection – Mark Ready for Motion.
		4. CID 4679 (EDITOR) REVISIT
			1. Review Comment
			2. Review submission discussion.
			3. Discussion on what should be in the frame description
			4. Motion #162: CID 4679 Resolution: REJECTED (EDITOR: 2020-02-20 10:30:19Z). Reason: The description of Address fields in 9.3.3 are needed as they are specific to Management frames.
			5. Discussion on the 3 alternatives presented.
			6. Alternative 1:
				1. Delete “For example, receiver address matching is always performed on the contents of the Address 1 field in received frames, and the receiver address of CTS and Ack frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.” in 9.2.4.3.1.
			7. Alternative 3:
				1. Change “For example, receiver address matching is always performed on the contents of the Address 1 field in received frames, and the receiver address of CTS and Ack frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.” in 9.2.4.3.1 to “Specifically, the Address 1 field in received frames always identifies the receiver(s) of the frame, and the Address 2 field in received frames, where present, always identifies the transmitter of the frame.”
			8. Straw Poll:
1. No change – current rejection
2. Alternate 1
3. Alternate 3
4. Abstain
	* + 1. Result: A:5 B: 3 C: 1 Abstain: 3
			2. Will retain the current rejection.
		1. CID 4689 (EDIOTR) REVISIT
			1. Review comment history
			2. Review submission Discussion.
			3. Motion #162 – CID 4689 Resolution: REJECTED (EDITOR: 2020-02-20 10:29:29Z). Reject Reason: In 9.4.3, subelements are within an element. In 9.6.7.37 and 9.6.7.38, subelements are within a field. Therefore, cannot change t o refer to 9.4.3 in 9.6.7.37 and 9.6.7.38.
			4. Straw Poll:
				1. Retain Rejection
				2. Update Resolution
				3. Abstain
			5. Results: A:6 B:4 C:2
			6. Will maintain the current resolution.
		2. CID 4809 (EDITOR) REVISIT
			1. Reviewed history
			2. Motion 167 CID 4809 resolution: Accept: “Delete "received" (and change "a" to "an" as appropriate) at P1589L40, P1590L53, P1592L56, P2180L1, P2482L30, and P2482L39.”
			3. Review proposed changes.
			4. All the changes were made, but there are some additional changes that need to be made.
			5. A separate motion will be made to incorporate the additional changes.
				1. The Text will be pulled from 11-20/435r2 and include in the motion text.
			6. We will not change the existing CID resolution.
			7. Concern that the changes make the statement much broader than originally intended.
			8. Discussion on Respond after a receipt.
			9. ACTION ITEM: Dorothy to send the Reflector for comment and feedback
	1. **GEN CIDS:**
		1. GEN comments on April 1, 2020 REVmd CRC telecon (Jon ROSDAHL (Qualcomm), from the database):
		2. CID 4765 (GEN):
			1. Update the resolution (prior to motion), to add in classes 128, 129 and 130, with the same change from “E-5” to “E-6”.
			2. No objections.
			3. Peter ECCLESINE has posted an updated document, 11-20/335r1 (<https://mentor.ieee.org/802.11/dcn/20/11-20-0335-01-000m-resolution-for-sa1-comment-4765.docx> >), with that addition.
			4. Updated the resolution. Revised. In Table E-4, in each of the circled entries, replace “E-5-” with “E-6-”. See doc 11-20/335r1: <<https://mentor.ieee.org/802.11/dcn/20/11-20-0335-01-000m-resolution-for-sa1-comment-4765.docx> >
			5. Ready for motion.
		3. CID 4114 (GEN):
			1. Proposed ACCEPTED (GEN: 2020-04-01 21:40:38Z).
			2. No objection.
			3. Ready for motion.
		4. CID 4005 (GEN):
			1. Consider accepting and changing the year of 802.11 to be 2016.
			2. Suggest just deleting the year.
			3. Noted that in Annex C, referenced must have the year. Editors fix these up at time of publication.
			4. Suggest we put in some sort of a “tag” so that these are easy to find, and nothing gets missed at publication.
			5. Suggest we just delete the references that are to 802.11 clauses. Most of the entries don’t have the REFERENCE, do we really need that?
			6. Is this REFERENCE really to the correct table?
			7. Action Item: Jon will work off-line with the Editors on a resolution.
	2. **Review Teleconference schedule**
		1. Review existing assignments
		2. Review proposed new telecons
		3. Propose to add Tuesday 4-21 and Thursday 4-23 to add to replace AdHoc that was cancelled.
	3. **Review TG Schedule**
* We had targeted May to be done. We may be lucky for July.
* Review TGmd schedule – roughly 400 comments remaining; target D 4.0 in July? D5.0 to Revcom
* July/Aug: 15-day recirc D4.0
* Aug-Sept comment resolution D4.0
* Sept D5.0 WG approval
* Sept – D5.0 Recirc/Unchanged recirc
* 6 Oct – 802 EC Approval, Draft TGme PAR (next revision)
* 13 October – Draft to RevCom
* 2020 Dec RevCom/SASB
	1. **Adjourned at 4:02pm**
1. **IEEE 802.11md REVmd CRC Telecon Friday April 03, 2020 10:00-12:00 ET**
	1. **Called to order at 8:05am** by the TG Chair Dorothy STANLEY (HPE)
	2. **Review Patent and Participation Policy**
		1. No Issues noted.
	3. **Attendance:** -please log with IMAT:
		1. Andersdotter, Amelia None - Self-funded
		2. Au, Kwok Shum Huawei Technologies Co., Ltd
		3. Bhandaru, Nehru Broadcom Corporation
		4. Derham, Thomas Broadcom Corporation
		5. Hamilton, Mark Ruckus Wireless
		6. Harkins, Daniel Aruba Networks, Inc.
		7. Inoue, Yasuhiko Nippon Telegraph and Telephone Corporation (NTT)
		8. Levy, Joseph InterDigital, Inc.
		9. Liu, Yong Apple, Inc.
		10. Malinen, Jouni Qualcomm Incorporated
		11. McCann, Stephen BlackBerry
		12. Montemurro, Michael BlackBerry
		13. RISON, Mark Samsung Cambridge Solution Centre
		14. Rosdahl, Jon Qualcomm Technologies, Inc.
		15. Smith, Graham SR Technologies
		16. Stanley, Dorothy Hewlett Packard Enterprise
		17. Wentink, Menzo Qualcomm Incorporated
		18. Yu, Mao NXP Semiconductors
	4. **Review Agenda: 11-20/535r0**

* + 1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0535-00-000m-2020-april-july-teleconference-agendas.docx>
		2. Agenda specific for today’s telecon:

b. 2020-04-03 Friday 10 am Eastern 2 hours \*\*\*\*\*Teleconference announced with 10 day notice\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* (London is +5)

1. Dan Harkins - <https://mentor.ieee.org/802.11/dcn/20/11-20-0351-00-000m-sae-sb1-resolutions.docx> and <https://mentor.ieee.org/802.11/dcn/20/11-20-0459-01-000m-internationalized-character-support.docx>, and <https://mentor.ieee.org/802.11/dcn/20/11-20-0543-00-000m-privacy-for-password-identifiers.docx> .
2. Edward Au: <https://mentor.ieee.org/802.11/dcn/20/11-20-0270-04-000m-resolutions-for-some-initial-sa-ballot-comments-on-11md-d3-0-part-ii.docx>
	* + 1. More requests were made and will be included in 11-20/535r1.
			2. Add 11-20/371r1 for Edward AU.
			3. No objection to plan as described (see 11-20/535r1) for today.
				1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0535-01-000m-2020-april-july-teleconference-agendas.docx>
	1. **Editor Report** – Emily QI (Intel)
	2. **Review doc 11-20/351r0** Dan Harkins (HPE)
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0351-00-000m-sae-sb1-resolutions.docx>
		2. CID 4667 (PHY)
			1. Review comment
			2. Proposed Resolution: REJECTED (PHY: 2020-04-03 14:22:51Z) - No problem has been identified and the cited table and paragraph provide useful information.
			3. No objection – Mark Ready for Motion
		3. CID 4668 (PHY)
			1. Review comment
			2. Similar issue noted with different proposed change as CID 4667.
			3. Discussion on if there is duplication of text and table.
			4. Discussion on what an appropriate rejection reason.
				1. Proposed rejection reason: "The normative requirement is specified in the paragraph and the content of the table are complementary, not contradictory. "
			5. Discussion on value of normative vs informative text in this section.
			6. "For example, the results of the above method for some defined groups ..."
			7. Straw Poll:
3. Reject
4. Modify the text adding “for example”
5. Abstain
	* + - 1. Results: a:9 b:5 c:4
			1. We will craft a rejection reason.
			2. Proposed Resolution: REJECTED (PHY: 2020-04-03 14:42:42Z) - The proposed change is not correct because z is determined by finding the number that satisfies the rules for all groups. They all use that formula, even the ones whose IANA-assigned values are listed in table 12-2.
			3. The normative requirement is specified in the paragraph and the content of the table are complementary, not contradictory. No problem has been identified and the cited table and paragraph provide very useful information to implementers.
			4. Mark ready for Motion –
		1. CID 4670 (PHY)
			1. Review comment
			2. Review discussion:
				1. Discussion: No problem has been identified. The operators that result in branching are explicitly called out due to them being so useful in doing side channel attacks. The entire algorithm must be done in constant time but calling out these special operators is useful information for implementers. Not only that but if explicitly calling out CSEL and CEQ “suggest that maybe other operations such as multiplication do not have to be in constant time” then calling them out explicitly in the proposed change would not really address the alleged issue.
			3. Discussion on if the claim of a problem was identified or not debated.
			4. Discussion included identifying the benefits of the existing text.
			5. Proposed Resolution: REJECTED (PHY: 2020-04-03 14:53:20Z) - No technical problem has been identified and explicit mention of operations that result in code branching as needing special attention is important information for implementers. CSEL and CEQ are functions that could result in branching, so they need to be explicitly identified.
			6. Mark Ready for Motion
		2. CID 4671 (PHY)
			1. Review Comment
			2. Review context locations.
				1. D3.0 – p2571 location
				2. D3.2 p2560.41 –
				3. "12.4.4.3.3 Direct Generation of the password element with FFC groups(M137)An SAE peer indicates support for direct hashing to obtain the FFC password element by setting the SAE hash-to-PWE bit"
			3. The proposed change is similar what is now in d3.2 by CID 4726.
			4. Discussion on if current version is in d3.2 is sufficient.
			5. Proposed Resolution: CID 4726: "REVISED (PHY: 2020-01-13 22:14:09Z) - Incorporate the changes given in https://mentor.ieee.org/802.11/dcn/19/11-19-2154-02-000m-sae-anti-clogging-token.docx which clarifies anti-clogging token usage with password identifiers."
			6. More Work needed to harmonize the proposed changes.
		3. CID 4698 (PHY)
			1. Review Comment
			2. Insufficient Detail rejection would be better resolution.
			3. Discussion on the value of “SAE exchange” or “FILS exchange”.
				1. Some suggest that “SAE exchange” could be changed as noted to “SAE authentication”, but “FILS exchange” seems to have more value.
			4. Discussion on the FILS change:
				1. from Mark RISON (Samsung) to everyone:
				2. Change “When FILS authentication is performed, the key confirmation is performed as part of the FILS exchange using association frames. Hence, no additional handshake is necessary(11ai).
				3. -> "When FILS authentication is performed, the key confirmation is performed as part of the exchange ofassociation frames. Hence, no additional handshake is necessary(11ai)."
			5. Jouni’s proposed resolution: CID 4698: REVISED. Replace "use in the SAE exchange" with "use in SAE authentication" in 9.4.1.42 (REVmd/D3.0 p941 l38).
			6. More work needed
	1. **Review doc 11-20/459r1 Dan** Harkins (HPE)
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0459-01-000m-internationalized-character-support.docx>,
		2. A motion for this document is scheduled for April 17th.
		3. Abstract: This submission proposes the use of character pre-processing methods in order to support internationalized character sets with usernames (password identifiers) and passwords
		4. Minor changes from r0 to r1.
		5. No objections have been noted. – ready for motion on April 17th.
	2. **Review doc 11-20/0543r0** Dan Harkins (HPE)
		1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0543-00-000m-privacy-for-password-identifiers.docx> .
		2. Abstract: This submission proposes a way to provide privacy protections to SAE password identifiers.

This scheme has the following properties:

* A passive attacker cannot determine a protected identity;
* Identifiers are protected against active attack insofar as SAE is resistant to active attack;
* A passive attacker cannot connect protected identities across SAE protocol runs to generate PII;
* Password identifiers can be arbitrarily padded to foil passive traffic analysis;
* Protected identities are secure under a birthday bound of 232 encryptions;
* An attacker cannot tamper with or substitute identifiers to connect distinct runs of SAE;
* An AP needs to only manage a single credential;
* APs in an ESS can share the single credential (in an out of band, out of scope manner);
* APs can use the same credential to protect all groups in the ESS that use password identifiers;
* Identities are protected against members of the same group;
* The interface for password identifiers on a STA is unchanged;
* The overhead is minimal—25 octets plus padding;
* Uses symmetric cryptography for speed and DOS resistance;
* Protected password identifiers in a mesh is supported.
	+ 1. CID 4731 (PHY)
			1. Review submission
			2. Discussion of the proposal vs some solution that may be more generic.
			3. Discussion on the inclusion of elements being included.
				1. The Password Identifier element is optionally present if the Status Code field is zero, 123, or 126, and the Protected Password Identifier element is not present.
				2. The Protected Password Identifier element is optionally present if the Status Code field is zero, 123, or 126, and the Password Identifier field is not present.
			4. Discussion on the size and length to time an identifier would be valid.
			5. More work is needed.
	1. **Review doc 11- 20/270r6** Edward AU
		1. Document <https://mentor.ieee.org/802.11/dcn/20/11-20-0270-06-000m-resolutions-for-some-initial-sa-ballot-comments-on-11md-d3-0-part-ii.docx>
		2. CID 4070 (EDITOR2)
			1. Review comment
			2. Review submission discussion
			3. Discussion on the improvement of the NOTE.
				1. Original:

NOTE – the VHT beamformee might therefore have to transmit an MPDU that is bigger than the VHT beamformee is capable of receiving

* + - * 1. The 2 options:
1. NOTE--The requirement that the VHT compressed beamforming feedback is transmitted in a single VHT Compressed Beamforming frame implies that the VHT beamformee might have to transmit an MPDU that is bigger than its receive capability.
2. NOTE--The requirement that the VHT compressed beamforming feedback is transmitted in a single VHT Compressed Beamforming frame might imply that the VHT beamformee transmits an MPDU that is bigger than its receive capability.
	* + 1. No objection to choosing Option 1
			2. Proposed resolution: Revised.

The VHT beamformee does not fragment if the Compressed Beamforming Report fits in the VHT beamformer’s maximum MPDU length capability. So if for example the Compressed Beamforming Report is 10 kB and the beamformer’s maximum MPDU length capability is 11 kB, then the beamformee does not fragment, even if the beamformee’s maximum MPDU length capability on receive is 4 kB (which one might think is also its max on transmit). This is the subtlety the NOTE is capturing.

1959.15 replace the NOTE with

NOTE--The requirement that the VHT compressed beamforming feedback is transmitted in a single VHT Compressed Beamforming frame implies that the VHT beamformee might have to transmit an MPDU that is bigger than its receive capability.

* + - 1. No objection – Mark Ready for Motion
		1. CID 4214 (EDITOR2)
			1. Review comment
			2. Review proposed changes.
			3. Discussion
			4. Proposed Resolution: Revised.

At 287.41 and 287.44, replace

“entity and IEEE 802.1X Authenticator/Supplicant unless” with

“entity, and IEEE 802.1X Authenticator or Supplicant, unless”.

At 283.3, 283.39, 286.4, and 286.38 (twice), replace

“802.1X Authenticator/Supplicant” with

“IEEE 802.1X Authenticator or Supplicant”.

At at 2669.30, replace

“Authenticator/Supplicant nonce” with

“Authenticator or Supplicant nonce, respectively”.

At 1382.32, replace

“Probe/Association Request frame” with

“Probe Request frame or Association Request frame”.

At 2763.55, replace

“Authentication-Confirm/Authentication-Ack frames (over the air) or FT Confirm/FT Ack frames (over the DS)” with

“Authentication-Confirm and Authentication-Ack frames (over the air) or FT Confirm and FT Ack frames (over the DS)”.

At 2837.25, replace

“during authentication/association” with

“during authentication and association”.

At 2669.23, replace

"Install/Not install" with

"indicates whether to install (1) or not install (0)"

* + - 1. No objection – Mark Ready for Motion
		1. CID 4072 (EDITOR2)
			1. Review comment
			2. Review proposed changes.
			3. Proposed resolution: Revised.

At 2059.60 in subclause 10.42.7, replace “BEAM\_TRACKING\_REQUEST parameter in the RXVECTOR set to Beam Track Requested” with “BEAM\_TRACKING\_REQUEST parameter in the RXVECTOR set to Beam Tracking Requested”.

At 2060.26 in subclause 10.42.7, replace “BEAM\_TRACKING\_REQUEST to beam tracking not requested” with “BEAM\_TRACKING\_REQUEST to Beam Tracking Not Requested”.

At 2060.31 in subclause 10.42.7, replace “BEAM\_TRACKING\_REQUEST parameter in the RXVECTOR equal to beam tracking not requested” with “BEAM\_TRACKING\_REQUEST parameter in the RXVECTOR equal to Beam Tracking Not Requested”.

At 2064.12 in subclause 10.42.9, replace “ENHANCED\_BEAM\_TRACKING\_REQUEST to enhanced beam tracking requested” with “ENHANCED\_BEAM\_TRACKING\_REQUEST to Enhanced Beam Tracking Requested”.

At 2064.15 in subclause 10.42.9, replace “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter shall be set to enhanced beam tracking not requested” with “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter shall be set to Enhanced Beam Tracking Not Requested”.

At 2064.20 in subclause 10.42.9, replace “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter in the RXVECTOR equal to enhanced beam tracking requested” with “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter in the RXVECTOR equal to Enhanced Beam Tracking Requested”.

At 2064.30 in subclause 10.42.9, replace “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter in the TXVECTOR to enhanced beam tracking requested” with “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter in the TXVECTOR to Enhanced Beam Tracking Requested”.

At 2064.54 in subclause 10.42.9, replace “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter in the TXVECTOR to enhanced beam tracking requested” with “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter in the TXVECTOR to Enhanced Beam Tracking Requested”.

At 2064.61 in subclause 10.42.9, replace “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter in the RXVECTOR equal to enhanced beam tracking requested” with “ENHANCED\_BEAM\_TRACKING\_REQUEST parameter in the RXVECTOR equal to Enhanced Beam Tracking Requested”.

At 3092.46 in Table 20-1, replace “Beam tracking requested or Beam tracking not requested” with “Beam Tracking Requested or Beam Tracking Not Requested”.

At 3459.31 in Table 24-1, replace “Beam tracking requested or beam tracking not requested” with “Beam Tracking Requested or Beam Tracking Not Requested”.

At 3459.49 in Table 24-1, replace “Enhanced beam tracking requested or enhanced beam tracking not requested” with “Enhanced Beam Tracking Requested or Enhanced Beam Tracking Not Requested”.

At 3488.64 in Table 25-1, replace “Beam tracking requested or Beam tracking not requested” with “Beam Tracking Requested or Beam Tracking Not Requested”.

At 3130.53 and 3130.60, remove “the” from “the PPDU Type”.

* + - 1. Discussion on the capitulation, hyphens and underscore useage.
			2. This will need more work.
			3. ACTION ITEM: Edward to update and post to reflector for feedback.
			4. Will bring back.
	1. **Adjourned 12:01pm**

**References:**

**April 1:**

1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0308-00-000m-2020-march-tgmd-agenda.pptx>
2. <https://mentor.ieee.org/802.11/dcn/20/11-20-0535-00-000m-2020-april-july-teleconference-agendas.docx>
3. <https://mentor.ieee.org/802.11/dcn/20/11-20-0141-16-000m-sa1-proposed-resolutions-for-editor-adhoc.doc>
4. <https://mentor.ieee.org/802.11/dcn/20/11-20-0435-01-000m-resolutions-for-some-comments-on-11md-d3-0-sb1.docx>
5. <https://mentor.ieee.org/802.11/dcn/20/11-20-0435-02-000m-resolutions-for-some-comments-on-11md-d3-0-sb1.docx>
6. <https://mentor.ieee.org/802.11/dcn/20/11-20-0335-01-000m-resolution-for-sa1-comment-4765.docx>

**April 3:**

1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0535-00-000m-2020-april-july-teleconference-agendas.docx>
2. <https://mentor.ieee.org/802.11/dcn/20/11-20-0535-01-000m-2020-april-july-teleconference-agendas.docx>
3. <https://mentor.ieee.org/802.11/dcn/20/11-20-0351-00-000m-sae-sb1-resolutions.docx>
4. <https://mentor.ieee.org/802.11/dcn/20/11-20-0459-01-000m-internationalized-character-support.docx>
5. <https://mentor.ieee.org/802.11/dcn/20/11-20-0543-00-000m-privacy-for-password-identifiers.docx>
6. <https://mentor.ieee.org/802.11/dcn/20/11-20-0270-06-000m-resolutions-for-some-initial-sa-ballot-comments-on-11md-d3-0-part-ii.docx>