IEEE P802.11
Wireless LANs

|  |
| --- |
| Some LB 253 CRs |
| Date: March 3 2021 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | nehru.bhandaru@broadcom.com |

Abstract

This document contains discussion and proposed resolutions for the following LB 253 comments on TGaz Draft 3.0:

5018, 5019, 5030, 5031, 5085, 5086, 5144, 5263, 5268, 5276, 5292, 5299, 5300, 5301, 5302, 5303, 5304,

5305, 5306, 5307, 5308, 5337, 5338, 5339. 5340, 5357, 5358, 5359, 5360, 5362, 5363, 5370, 5371, 5372, 5374, 5394, 5398, 5401, 5403, 5445, 5453, 5455, and 5456.

**Revision Notes**

R0 – initial version

R1 – update based on TGaz call 02/24/2021

R2 – further updates after TGaz calls – additional CIDs.

R3 – Update to Class 1a frames based on feedback

R4 – update based on TGaz call 03/03/2021

**References**

[1] IEEE P802.11-REVmdTM/D5.0, September 2020

[2] IEEE P802.11az™/3.0 January 2021

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause/Page** | **Comment** | **Proposed Change** | **Resolution** |
| **5018** | 9.4.2.303, p85.12 | Need to include a case (field value) for FILS shared key With PFS as it seems to be missing option? | As per comment | Resolution: RejectPASN already provides PFS (see 12.12 in [2]). There is no value in supporting FILS shared key w/PFS. |
| **5019** | 9.4.2.303, p85.23-25 | Section 9 cannot have normative text hence change the text 'Comeback After subfield may be 0 indicating that the operation may be retried with the Cookie of non-zero length that shall be present. Comeback After subfield shall not be present (i.e. zero octets) in PASN authentication frames from a non-AP STA" | Modify the text to read 'Comeback After subfield 0 indicates that the operation can be retried with the Cookie of non-zero length. Comeback After subfield is not be present (i.e. zero octets) in PASN authentication frames from a non-AP STA.Also, add normative text in section 11.3.5.1 (General) with corresponding normative text. | Resolution: ReviseAgree with the commentor on the first point. There is already normative text for the second issue – but it is missing for PASN authentication frame 1TGaz Editor: Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5030** | 11.3.3, p109.0611.3.4 | Add the word 'unicast; before Protected in texts '...Protected Fine Timing frames... and ....Protected Dual of Public Action frames... | As per comment. | Resolution: ReviseAgree with the commentor. However Unicast is already present before Protected Dual of ..TGaz Editor: Change “Protected Fine Timing frames” to “Unicast Protected Fine Timing frames” |
| **5031** | 11.3.5, p111.40 | Change 'must' to 'shall' in the sentence | As per comment. | Resolution: AcceptAgree with the commentor. To associate or reassociate, a STA is required to perform non-PASN authentication. |
| **5085** | 12.6.7, p198.03 | Delete text 'When establishing an RSNA in an MBSS, PASN authentication shall not be used.' as it is not clear why we're limiting the use of PASN in Multi-BSS case? | As per comment | Resolution: RejectMBSS is a Mesh BSS and not Multi-BSS. Mesh BSS already has mechanisms for establishing security association (PTKSA) using AMPE and PASN does not add any new functionality. See discussion. |
| **5086** | 12.12.3.112.12.3.212.12.5pages:205209210212lines: 13-1518-20222629-3023 & 31 | We need to include an explicit PASN failure termination message to clarify the text behaviors such as:>If the processing fails, the AP may return an appropriate status in theStatus Code field (9.4.1.9) of the frame without including additional information or silently dropthe frame.>Otherwise, it may return an appropriate status in the Status code field (9.4.1.9) of the frame or silently drop the frame.>Otherwise the STA shall terminate the PASN authentication protocol exchange.>the AP shall terminate the PASN authentication.>If the AP terminated the PASN authentication silently or by sending a failure Status Code to the non-AP STA, other than a temporary refusal, it shall delete all of the PASN authentication state.>a failure indication, PASN authentication shall be abandoned | As per comment | Resolution: ReviseAgree with commentor in principle except for 12.12.3.1 which is a generic section. See discussions for suggested modifications to provide a specific status code in other contexts.TGaz Editor: Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5263** | 4.5.4.2, p23.37 | The intent of baseline text is lost by the addition made in P802.11az. The baseline text reads "An RSNA might support SAE authentication, FILS authentication, or both(11ai)." P802.11az D3.0 added an additional authentication method PASN Authentication. But the addition of the new authentication method has resulted in the removal of the possibility of an implementation supporting both SAE and FILS authentication. | Preserve the original intent of the baseline text. | Resolution: ReviseAgree in principle with the commentor.TGaz Editor: Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5268** | 9.4.2.118, p60.15-16 | Contradictory statements in the description of MIC element -- the introductory statement in P802.11REVmd D5.0 states "The MIC element provides message integrity to mesh peering Management frames. The format of the MIC element is shown in Figure 9-535 (MIC element format).". The description of the MIC field in the MIC element in P802.11az D3.0 states "In other frames, the MIC field is of variable length, depending on the context that specifies the computation of the MIC." If MIC element only provides message integrity check for mesh peering management frames, how can or whu would other frames include a MIC element? | Render statements in baseline consistent with changes to 9.4.2.118 in 802.11az D3.0. i.e., modify the introductory statement in Clause 9.4.2.118 to allow inclusion of MIC element in frames other than Mesh Peering management frames. Or some change to fix the contradiction. | Resolution: ReviseAlthough ‘other frames’ are understood from the context and clause 9 does not specify normative behavior it would not hurt to clarify the introductory sentence.TGaz Editor: Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5276** | 10.3.2.14.3, p104.13 | Does the term 'Protected Fine Timing action frame" include protected LMR? Table 9.535 seems to indicate so. However table 10-5 calls them out as different. | If Protected Fine Timing Frame includes protected LMR, remove calling out 'public action LMR' from table 10-5 and 10-6. Otherwise fix Table 9-535. | Resolution: RejectTable 9-535 includes protected LMR. Public Action LMR is a different frame. Sequence spaces indicated by tables 10-5 and 10-6 apply to both protected LMR and the Public Action LMR. Table 9-535 does not say anything about public action frames. |
| **5299** | 11.3, p108.7 | Do not change the style and content of State 1, the style must match the style and content of the other states. The style is a description of the STAs the state applies to followed by a sentence of the status of that state. "Unauthenticated and unassociated". | Remove the proposed change and return the text to the baseline text in REVmdD5.0. | Resolution: ReviseAgree in principle with the commentor. TGaz draft may have changed the style and some text inadvertently. This comment was marked technical although seems editorial.TGaz Editor: Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5300** | 11.3, p108.10 | State 1a should be in the same style as the other states. This text should identify the STAs this state applies to. | Replace the text describing State 1a with:- State 1a: Authenticated for non-DMG STAs and for DMG STAs that have performed PASN Authentication (12.12). Unassociated. | Resolution: ReviseAgree in principle with commentor except the initial part is replaced with suggested text and trailing explanatory text is still keptTGaz Editor: Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5301** | 11.3, p108.11 | The statement of the purpose of state 1a, should be provided as a note, it is not a requirement. Also robust management frames are MSDUs, so these STA do wish to exchange robust management frames, just not non-robust management frames and data frames. | Replace the text: "This state is used by STAs that wish to perform secure ranging but do not wish to exchange MSDUs."With: "Note: state 1a is used by STAs that wish to perform secure ranging and only exchange robust management frames." | Resolution: ReviseAgree in principle with commentor that the purpose could be placed in a note. State1a may also use non-robust management frames also. Clarified the note.TGaz Editor: Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5302** | 11.3.2 p109.1 | State 1a as described in figure 11-16 is unclear. 1) PASN Authenticated is not a defined term. Define the term or simply state Authenticated by PASN authentication. 2) protected Class 2 Frames is not defined. Hence this state is not well defined. | replace: "PASN Authenticated"With: "Authenticated by PASN"Replace: "Robust Unicast Class 2 Frames"With: "Class 1a Frames"Note: Class 1a Frames must be defined in clause 11.3.3. Suggest adding a.i) Class 1a frames and a list of the allowed frames. Defining these frames will clearly identify which frames are protected Class 2 Frames. | Resolution: ReviseAgree with the commentor on the first point. However, migration to Class 1a frames is also the subject of CID 5303 and can be considered in that context. protected Class 2 frames are listed in the list of Class 2 frames ... “Protected Class 2 frames comprising...”TGaz Editor: Please change the phrase ‘PASN Authenticated’ to “Authenticated by PASN” in figure 11-16 |
| **5303** | 11.3.3, p109.11 | There is no need to modify b) Class 2 frames. Instead add a.i) Class 1a frames and move the allowed frames under this heading. As there is no longer any changes to Class 2 frames, there is no need for changes to references to Class 2 frame in this clause or other clause. | Remove the changes to Class 2 frames and insert the above b) Class 2 Frames:"a.i) Class 1a frames 1) Management frames i) Disauthentication ii) Unicast SA Query (11.13) iii) Protected Dual of Public Action frames (9.6.10) iv) Protected Fine Timing frames (9.6.34)"Additionally, remove all changes to text regarding Class 2 frames, as the definition of Class 2 frames is not changed so there is no need to make the changes. (e.g. at 127.16, etc.) | Resolution: reviseAgree with the commentor. Frames in an Infrastructure BSS when PTKSA from PASN exists could be classified as Class 1a frames – that would avoid changing other classes.TGaz Editor: Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5304** | 11.3.3, p112.13 | Why is disassociation not allowed in State 1a? If the STA received a disassociation frame, it should be interpreted as a deauthentication frame. | Remove the statement about Disassociation is not allowed in State 1a. | Resolution: ReviseState 1a is an 802.11 authenticated state. Disassociation is a Class 2 frame that is not useful in State 1a (and State 1) – “In State 1, only Class 1 frames are allowed” ([1] p2218.7). There does not seem to be a rationale or a precedent to treat disassociation frame as a deauthentication frame – e.g., 11.3.5.6 Non-AP and non-PCP STA disassociation initiation procedures.However, the statement re: Disassociation being not allowed in State 1a can be removed – as it will have no effect.TGaz Editor: The revision is the same as that for CID 5359 which removes the sentence. No further action is needed. |
| **5305** | 12.12.4, p190.9 | The statement of RSNA establishment is not in the style or form of the base line. Please align with the baseline style. | Replace: "g) When an RSNA capable STA uses PASN authentication, an RSNA capable the STA's SME establishes an RSNA as described in 12.12 (Pre-Association Security Negotiation)."With: g) If an RSNA uses PASN authentication, an RSNA capable the STA establishes an RSNA as described in 12.12 (Pre-Association Security Negotiation). | Resolution: Accept |
| **5306** | 9.6.34.1, p104.1 | P802.11az defines "A protected Location Measurement Report" frame as one of the Protected Fine Timing Frame Category frames. However, this frame is defined to be carried in Action No Ack frame which is not a robust Management frame in the current baseline. Consequently, this frame would not be protected. This is clearly not the intention here, so it looks like Action No Ack frames would need to be defined to be robust Management frames for this protection mechanism to be available for the protected LMR. | Add the following definition to 3.2:'robust Action No Ack frame: An Action No Ack frame with a category value specified in 9.4.1.11 (Action field) (Table 9-51 (Category values)) with Yes in the Robust column.'In 12.2.7, replace 'The robust Management frames are Disassociation, Deauthentication, and robust Action frames.Action frames specified with "No" in the "Robust" column of Table 9-51 (Category values) are not robust Management frames and shall not be protected.'with:'The robust Management frames are Disassociation, Deauthentication, robust Action frames, and robust Action No Ack frames.Action frames and Action No Ack frames specified with "No" in the "Robust" column of Table 9-51 (Category values) are not robust Management frames and shall not be protected.'In 12.6.19, replace all five instances of "robust Action frames" with "robust Action frames and robust Action No Ack frames". | Resolution: Accept |
| **5307** | 11.21.6.3.4, p132.5 | Use of the protected variants of the frames is noted in a "shall use" statement, but there is no explicitly specified rules on how to address not protected frames in that "shall use" case. Taken into account the history of known security vulnerabilities, it would be helpful to have a clear shall requirement on the received discarding unexpected unprotected frames. | Replace "When Management Frame Protection is negotiated for TB and Non-TB Ranging negotiation, a STA shall use Protected Fine Timing Action frames for FTMR frames,Fine Timing Measurement frames, and Location Measurement Report frames." with "When Management Frame Protection is negotiated for TB and Non-TB Ranging negotiation, a STA shall use Protected Fine Timing Action frames for FTMR frames,Fine Timing Measurement frames, and Location Measurement Report frames and shall discard received unprotected variants of these frames." | Resolution: ReviseTGaz Editor: Change as followsReplaceWhen Management Frame Protection is negotiated for TB and Non-TB Ranging negotiation, a STA shall use Protected Fine Timing Action frames for FTMR frames,Fine Timing Measurement frames, and Location Measurement Report frames.withWhen Management Frame Protection is negotiated for TB and Non-TB Ranging, a STA shall* use Protected Fine Timing Action frames for FTMR frames, Fine Timing Measurement frames, and Location Measurement Report frames for ranging negotiation and measurement
* discard unprotected variants of these frames upon reception.
 |
| **5308** | 12.12.5, p211.33 | PASN introduces a new use case for SAE. P802.11az/D3.0 does not place any constraints on which PWE derivation method can be used or give any guidance on how to select that. Since this is a new use case, we should promote use of the newer H2E method and disallow use of the older hunting-and-pecking loop since this use case does not need to have backwards compatibility with old (pre-PASN) STAs. | Add the following sentence to the end of the first paragraph in 12.12.5: "When SAE is used with PASN authentication, the direct hashing technique described in 12.4.4.2.3 and 12.4.4.3.3 shall be used." | Resolution: ReviseAgree with the commentor. The older Hunt & Peck method would be slower and some devices in the field might not implement it correctly.TGaz Editor: Add the following sentence to the end of first paragraph of 12.12.5 (PASN authentication with SAE)When SAE is used with PASN authentication, the direct hashing technique described in 12.4.4.2.3 (Hash-to-curve generation of the password element with ECC groups) or 12.4.4.3.3 (Direct Generation of the password element with FFC groups ) shall be used. A PASN capable AP shall set SAE hash-to-element bit to 1in the Extended RSN Capabilities field of the RSNXE included in its Beacon, Probe Response, and second PASN authentication frames. A non-AP STA initiating PASN authentication shall set SAE hash-to-element bit to 1 in the Extended RSN Capabilities field of the RSNXE in the first PASN authentication frame. |
| **5358** | 11.3.4.3, p111.15 | Isn't a state transition missing? It is possible to go from State 1a to State 2 by using a non-PASN authentication, right? Also, "PASN authentication was not used" is a bit confusing, because it doesn't say 'used when?' | Change "if it was in State 1" to "if it was in State 1 or State 1a", and change "when PASN authentication procedure was not used" to "and this authentication exchange is not for a PASN authentication" | Resolution: ReviseAgree in principle with the commentor on the first part. The case for when PASN authentication procedure was used is in the next sentence “The state for the originating STA shall be set to State 1a if it was in State 1” TGaz Editor: ReplaceThe state for the originating STA shall be set to State 2 if it was in State 1 (#1403) when PASN authentication procedure was not used.withThe state for the originating STA shall be set to State 2 if it was in State 1 (#1403) or state 1a when PASN authentication procedure was not used. |
| **5359** | 11.3.4.3, p112.13 | Disassociation can happen at any time, because it is easily possible to get out of synch with the peer's state machine. So, it cannot be disallowed in State 1a. There's no real reason to disallow it, anyway. | Delete "Disassociation is not allowed in State 1a." | Resolution: Accept |
| **5360**  | 111.39 | Not allowing reassociation when in states 3 or 4 is an incorrect change to the baseline. Reassociation to the currently associated AP is explicitly allowed. I'm not sure why this paragraph was added, anyway - it seems to be to clarify that before a STA can perform association from State 1a it must first perform non-PASN authentication and move to State 2. But, the same is true, and always has been, for State 1, and not explicity described in text. The state machine already shows this clearly. | Delete this paragraph. | Resolution: ReviseAgree in principle with the commentor. This is intended to cover State 1a behavior. Suggest keeping the clarification.TGaz Editor replace the paragraph on page 111 lines 39-41 with the following.Association and reassociation are not allowed in State 1 and State 1a. In order to associate or reassociate, a STA in State 1 or State 1a must perform a IEEE Standard 802.11 non-PASN authentication or FILS authentication and transition to State 2. |
| **5362**  | 12.6.10.2, p198.12 | PASN authentication, while establishing RSNA authentication, is not sufficient to open the 802.1X port. | Add a modification to this baseline clause, with the statement that "PASN authentication does not open the 802.1X port". | Resolution: ReviseAgree it would be useful although there is no statement about PASN opening up 802.1x port.TGaz Editor: Add the following to the end of 12.6.10.1 (note p198.12 refers to the 12.6.10.1 in TGaz 3.0)NOTE—A STA does not open 802.1X port(s) upon successful PASN authentication. |
| **5363**  | 12.12, p203.9 | It seems that PASN establishes a PTKSA. But, then the following security negotiations (if the STA associates) will also establish a (different?) PTKSA. How do these 2 PTKSAs relate? Is there really only one superset PTKSA with both security contexts included? When are each of the PTKSAs deleted? | Add discussion of this PASN PTKSA as compared to an PTKSA derived from other RSNA PTKSA establishment. Also add clarification in 12.6.18 that specifies how and when the PASN PTKSA is terminated. | Resolution: RejectAgree that the spec needs to specify PTKSA lifetime. The lifetime is specified in 12.6.1.1.6 (PTKSA) to be minimum of PMKSA and PASN negotiated timeout (See TIE element in PASN negotiation). There is exactly one PTKSA (see 12.6.1.1.6). That PTKSA including PASN established PTKSA is deleted when non-AP STA associates (p2224.20 [1]) and when association is successful on the AP (p2232.1 bullet j in [1]) |
| **5370**  | 12.12.3.2, p210.3 | A general best security practice is to discard frames that fail MIC validation, rather than terminate negotiation in progress - to protect against trivial DOS attacks. PASN negotiation should continue and ignore messages w/ invalid MIC. The current 802.11 draft (5.0, for e.g.) has such protections for various other exchanges - p2602.40 (BIP MIC processing), p2611.21 (GCM MIC processing), p2577.50 (SAE confirm processing), p2666.20(4-way M2 processing on Authenticator) | Replace the sentences that deal with MIC failures by adding an exception to MIC failure handling.p210.3If the validation fails, the non-AP STA shall terminate the PASN authentication protocol except if the MIC verification fails, the frame is discarded with no additional action. Otherwise the STA begins the construction the third PASN frame as followsp210.26For the third PASN frame, if validation fails, or Base AKM processing indicates an error, the AP shall terminate the PASN authentication except if the MIC verification fails, the frame is discarded with no additional action.. | Resolution: ReviseAgree with the commentor to follow best practices on handling MIC failures**TGaz Editor:** Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5371** | C.3, p259.42 | Typo 'dot11II2RLMRFeedbackPolicy' - should dot11I2RLMRFeedbackPolicy | Fix the typo | Resolution: Accept |
| **5372** | 9.4.2.241, p68.22 | Protection of Range Negotiation and Measurement Management Frames Required field is set depending on MIB variable dot11RSTARequiresPMFActivated that is specified to apply only for pre-association ranging. For the associated case, MFP protection for ranging is determined based on RSN security context - see p132.3 11az d3.0 - and the 'Protection of Range Negotiation and Measurement Management Frames Required' setting does not apply. | Clarify the draft by renaming 'Protection of Range Negotiation and Measurement Management Frames Required' to 'Unassociated Protection of Range Negotiation and Measurement Management Frames Required'; perhaps introduce an abbreviation URNM-MFPR for this and replace 'Protection of Range Negotiation and Measurement Management Frames Required' in the draft with the abbreviation | Resolution: ReviseAgree with the commentor. Some clarification and an abbreviation would help.**TGaz Editor change as follows****Insert in 3.2 Definitions specific to IEEE 802.11 the following abbreviation****Unassociated Range Negotiation and Measurement Management Frame Protection Required (URNM-MFPR ) :** A security policy that specifies whether ranging frames are required to be protected without association.**Replace in draft the following phrases with the abbreviation URNM-MFPR (Table 9-321, p121.24, p121.26, p123.29, p131.8)**Protection of Range Measurement Management Frames Required Protection of Range Negotiation and Measurement Management Frames Required |
| **5374**  | 12.12, p203.2 | OCI element needs to be included in PASN negotiation to prevent channel based MITM attacks | Add OCI element to PASN messages 1 and 2. Possible changes to p203.31, 207.14 (add OCI to M1), 207.22 (verify OCI in M1),209.9 (add OCI to M2), 209.22 (verify OCI in M2). Note that although M1 is not MIC protected, the MIC for M3 covers the body of M1 and hence the OCI element integrity can be trusted. | Resolution: ReviseAgree in principle with the commentor. OCI improves the security of PASN by preventing channel based MITM attacks**TGaz Editor:** Please make changes as specified in https://mentor.ieee.org/802.11/dcn/20/11-21-0291-04-00az-lb-253-crs-a.docx |
| **5394**  | 11.21.6.3.3, p131.9 | security context? I think we normally refer to a security association. And normally by its acronym (e.g., PTKSA) | Identify and replace with the correct term | Resolution: ReviseAgree.**TGaz Editor: please replace the phrase ‘security context’ with ‘PTKSA’** |
| **5398**  | 11.21.6.4.5.2,p161.2 | In Figure 11-37o, the Note1 appears next to LTF\_GEN\_SAC3, however the explanation of the Note declares to use LTF\_GEN\_SAC1 or LTF\_GEN\_SAC2. In no other place the LTF\_GEN\_SAC3 is explained | Clarify the meaning of the LTF\_GEN\_SAC3 or remove it | Resolution: ReviseLTF\_GEN\_SAC3 is the generation SAC for the next measurement or current measurement (just like LTF\_GEN\_SAC2) – it is for illustration only. However the NOTE—next to LTF\_GEN\_SAC3 is confusing. Propose to remove the phrase ‘See NOTE 1’ from the figure – the reader can read the note without additional instruction.**TGaz Editor: please remove the phrase ‘See NOTE 1’ from the figure (the note itself is however retained)** |
| **5401**  | 11.21.6.3.6, p133.13 | There is no such a frame "Protected Dual of the Fine Timing Measurement Request" defined in the draft. Same about "Protected Dual of the Fine Timing Measurement frame" | Align the frames with the "Protected Fine Timing" category | Resolution: ReviseAgree**TGaz Editor: please replace the two instances of ‘Protected Dual of the Fine Timing Measurement Request frame’ in 11.21.6.3.6 Negotiation for Secure EDMG TRN in EDCA based Ranging measurement exchange****with ‘Protected Fine Timing Measurement Request frame’** |
| **5403**  | 11.21.6.4.5.2 | "...Fine Timing Measurement frame..." Protected Fine Timing frames of unique category and action fields are defined in 9.6.34.1. The frames are: protected Fine Timing Measurement Request, protected Fine Timing Measurement, and protected Location Measurement Report. The correct names of the frames shall be referred when the frames are used. | Replace by the correct names (protected Fine Timing Measurement Request, protected Fine Timing Measurement, and protected Location Measurement Report) in all relevant appearances. | **Resolution: Revise**Agree in principle.**TGaz Editor: please add the word ‘protected to the sentence as shown below.**The first LTF Generation SAC and its associated Secure LTF Counter (#**2289**) parameters are carried in an initial protected Fine Timing Measurement frame, and a protected Location Measurement Report frame. |
| **5445** | 9.4.2.299, p80.21 | "(#2289) The LTF Generation SAC field is a nonzero value associated with Secure LTF Counter(#2289) carried in the same Secure LTF Parameters element and validates the randomized LTF sequence; see 11.21.6.3.4 (Negotiation for Secure LTF in the TB and Non-TB Ranging measurement exchange). This field is present in the initial protected Fine Timing Measurement frame, the R2I protected Location Measurement Report frame and is reserved otherwise. (#3627, #3902)" "LTF Generation SAC" is not used by the revised secure LTF mechanism in 11az\_D3.0. | Delete "LTF Generation SAC" field from the Figure 9-788 and all the related text throughout the spec, and use only "Ranging Management SAC" where appropriate. | Resolution: RejectThe Generation SAC was (prior to TGaz 3.0) never used to derive anything as the SAC can be independently derived on both ISTA and RSTA and still is not– it’s primary purpose is to cross check that the derived keys are correct ahead of the actual measurement – at which point the measurement need not be attempted if there is mismatch. The usage of LTF generation SAC and range measurement SAC is also akin and symmetric like the dialog and follow up tokens use in non-secure TB and NTB ranging. |
| **5455**  | 11.21.6.4.5.4.1, 171.8 | Figure 11-37s, for itf-iv construction, there is no text descripting the "block-counter" updating frequency. | Please add description or reference for block-counter used for itf-iv construction, and specify how frequently it's updated. | Resolution: rejectp170.21 has the statement ‘The counter is incremented by 1 each time an AES block is output by the generator. The figure is illustrative only‘ |
| **5456** | 11.21.6.4.5.4.2, 172.8 | Figure 11-37t, for itf-iv construction, there is no text descripting the "block-counter" updating frequency. | Please add description or reference for block-counter used for itf-iv construction, and specify how frequently it's updated. | Resolution: rejectp170.21 has the statement ‘The counter is incremented by 1 each time an AES block is output by the generator. The figure is illustrative only |
| **5144** | 12.2.4, p190.15 | Change marks missing from the text in P190L15-16. | underline the text starting from "PASN Authentication" to the end of the paragraph. | Resolution: Accept |
| **5292** | 12.12.9, p215.24 | "and thus be": this looks as if a word is missing. | Change "and thus be" to "and thus may be". | Resolution: Accept |
| **5337** | 12.5.3.4, p193.25 | "9.6.xx" must be "9.6.34". | Please fix this typo. | Resolution: Accept |
| **5338, 5339, 5340** | 12.12.3.2, p207.6, p209.1, p210.12 | "FILS Wrapped Data element" should be "Wrapped Data element" according to other modifications made in D3.0. | Please remove"FILS". | Resolution: Accept |
| **5453** | 12.12.11, p191.22 | "A pseudo-random key (PRK) is generated using the hash function accepting IKM and salt as inputs. See RFC 5869 section 2.2." The hash function to generate PRK is undefined. | Please add that : "The hash function to be employed to generate the PRK is SHA-256." | Resolution: RejectThe text at p191.18 states “The hash function to be employed in HKDF is SHA-256.” and per RFC 5869 2.2 referenced above p191.22, PRK is derived using the hash function |

**CID 5018 - Discussion**

PASN already provides PFS because of the ephemeral key exchange and uses the shared secret derived from the exchange in PMKSA and PTKSA derivation(s). The PMKSA derived along with PASN shall not be used as PMKSA for a subsequent association ([2] p211.25). Consequently, there is no value in supporting FILS shared key with PFS explicitly.

**CID 5019 - Discussion**

Agree with the commentor.

The normative is already present in § **12.12.3.2 PASN Frame Construction and Processing** that describes the construction of PASN auth frame 3 from non-AP STA. The proposed change is to add to PASN auth frame 1 construction also.

For PASN auth frame 3 p210.9

“Public Key information and Comeback Info fields shall not be present. The Control field in the element is set appropriately to indicate the presence or absence of fields in the element.”

**CID 5019 - Proposed Changes**

**Tgaz Editor: Modify § 9.4.2.303, p85.22 the following in TGaz Draft as follows**

where the Comeback After subfield is time in TUs after which the non-AP STA is requested to retry the PASN authentication. Comeback After subfield ~~may be 0 indicating~~ is set to 0 to indicate that the operation ~~may~~ can be retried with the Cookie of non-zero length ~~that shall be present~~ in the Cookie subfield. Comeback After subfield is ~~shall~~ not ~~be~~ present (i.e. zero octets) in PASN authentication frames from a non-AP STA.

**Tgaz Editor: Modify § 12.12.3.2 PASN Frame Construction and Processing, p207.2 the following in TGaz Draft as follows**

— Including 9.4.2.303 (PASN Parameters Element) with the wrapped data format, chosen finite cyclic group ID, and the ephemeral public key. Comeback field ~~information included and~~ ~~is~~ shall either be absent or set to the cookie length and the cookie received from the AP if the authentication is being retried; Comeback After subfield shall not be present in the Comeback field. The Control field in the element is set appropriately to indicate the presence or absence of fields in the element.

**CID 5085 – Discussion**

Mesh peering is like an association, and PTK (MTK) establishment in MBSS is already specified in § 14.5 (AMPE) of the base 802.11 spec [1] – it works with SAE or AP Peer Key protocol. So PASN does not add any new functionality to an MBSS.

From [1]

**mesh basic service set (MBSS):** A basic service set (BSS) that forms a self-contained network of mesh

stations (STAs) that use the same mesh profile. An MBSS contains zero or more mesh gates, and can be

formed from mesh STAs that are not in direct communication.

4.3.21.5.4 Mesh security

In an MBSS, mesh link security protocols are used to authenticate a pair of mesh STAs and to establish

session keys between them. Mesh authentication protocols establish a shared, common pairwise master key

(PMK), and authenticate a peer mesh STA. The authenticated mesh peering exchange protocol relies on the

existence of the PMK between the two mesh STAs to establish an authenticated peering and derive session

keys. The details of mesh security are described in 12.4 (Authentication using a password), 14.3.3 (Mesh

authentication), 14.5 (Authenticated mesh peering exchange (AMPE)), and 14.6 (Mesh group key

handshake).

**CID 5086 – Discussion**

§ 12.12.3.1 is a generic description with more details of frame construction and processing specified later in § 12.12.3.2 PASN Frame Construction and Processing and § 12.12.5 PASN authentication with SAE

As part of CID 5370 (related MIC validation) changes are made to return a status code if MIC validation is successful (or there is no MIC).

There are some cases where improvements can be made, although in general the processing section indicates the status code to be returned. These include

p210.29

If the AP terminated the PASN authentication silently or by sending a failure Status Code to the non-AP STA, other than a temporary refusal, it shall delete all of the PASN authentication state.

This is after the processing is complete. Nothing else can be done other than cleaning up.

p212.5

The AP upon receiving the first PASN frame, delivers the frame to SAE for processing via the SAE parent process managed by the SME. If the PASN authentication process receives, from the SAE protocol instance, a failure indication, PASN authentication shall be abandoned.

Here perhaps one could return a status to PASN from SAE – using a status code – such as BASE\_AKM\_FAILURE

p212.23

The non-AP STA upon receiving the second PASN frame, delivers the Commit and Confirm messages from the AP to the SAE protocol instance. If the PASN authentication process receives, from the SAE protocol instance, a failure indication, PASN authentication shall be abandoned. Otherwise PASN authentication process receives an Authentication frame with a Confirm message (12.4.7.5 Encoding and decoding of SAE Confirm messages) as the SAE protocol instance transitions to the Confirmed state followed by a transition to the Accepted state (Since it has 26 received both the Commit and Confirm messages from the peer).

The non-AP STA sets the Wrapped Data in the third PASN frame to be the Authentication frame 28 body with a Confirm message. The AP upon receiving the third PASN frame, delivers the 29 Authentication frame from the Wrapped Data to the SAE protocol instance. Either the instance accepts the frame and transitions to the Accepted state or PASN authentication shall be abandoned and the SAE protocol instance destroyed.

p212.21

The non-AP STA upon receiving the second PASN frame, delivers the Commit and Confirm messages from the AP to the SAE protocol instance. If the PASN authentication process receives, from the SAE protocol instance, a failure indication, PASN authentication shall be abandoned.

p207.31

— Verifies (#1751) the public key as specified in 5.6.2.3 of NIST SP 800-56A R2. If 31 verification fails, the AP shall terminate PASN authentication protocol.

Here perhaps one could return a status perhaps invalid public key – FILS also does this – simply says AP may

terminate the authentication exchange.

p210.29

If the AP terminated the PASN authentication silently or by sending a failure Status Code to the non-AP STA, other than a temporary refusal, it shall delete all of the PASN authentication state.

Following changes can help

1. p207.31 – upon public key validation failures, add an invalid public key status code and return it
2. p207.30 – return invalid params if PASN parameters are invalid
3. terminate after returning a failure status for PASN frame 1

I am not sure if it makes sense to return a status to AP if validation of PASN frame 2 fails – for certain validation such as mismatched/malformed AKMs in RNSE, bad public key, missing PMK frame 3 cannot be constructed. If the MIC is wrong AP will discard the frame anyway. So I believe the PASN should be terminated on non-AP STA and terminated on AP upon implementation specific timeout.

\*\* The resolution/proposed changes need more work\*\*

**TGaz Editor: Add the status code to Table 9-50 Status Codes**

***Insert (append) the row shown below at the end of Table 9-50—Status Codes* *before the final reserved range.***

|  |  |  |
| --- | --- | --- |
| **Status Code** | **Name** | **Meaning** |
| ANA-invalid-pub-key | INVALID\_PUBLIC\_KEY | Public key format is invalid |
| ANA-pasn-base-akm-failure | PASN\_BASE\_AKM\_FAILED | Failure from Base AKM processing during PASN |

**TGaz Editor: in § 12.12.3.2 PASN Frame Construction and Processing, add the following sentence after the paragraph p207.30**

If the validation fails, unless a processing status of REFUSED\_TEMPORARILY is being returned, the processing status is set to INVALID\_PARAMETERS.

**TGaz Editor: in § 12.12.3.2 PASN Frame Construction and Processing, replace the sentence after the paragraph p207.332**

If verification fails, the AP shall terminate PASN authentication protocol.

**with**

If verification fails, the processing status is set to INVALID\_PUBLIC\_KEY.

**TGaz Editor: in § 12.12.3.2 PASN Frame Construction and Processing, p208.4 replace the processing status**

REFUSED

**with**

PASN\_BASE\_AKM\_FAILED

**TGaz Editor: in § 12.12.3.2 PASN Frame Construction and Processing, replace following sentence p209.12**

Once the processing complete, the AP sends the second PASN frame to the non-AP STA.

**with**

Once the processing complete, the AP sends the second PASN frame to the non-AP STA. If the processing status returned in the frame was not SUCCESS, the AP shall terminate PASN authentication protocol.

**CID 5263 – Discussion**

Base text in [1]

An RSNA might support SAE authentication, FILS authentication, or both(11ai). An RSNA also supports

authentication based on IEEE Std 802.1X-2010, or preshared keys (PSKs) after Open System

authentication. IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one

another. This standard does not specify an EAP method that is mandatory to implement. See 12.6.5 (RSNA

policy selection in an IBSS(#59)) for a description of the IEEE 802.1X authentication and PSK usage within

an IEEE 802.11 IBSS.

**CID 5263 - Proposed Changes**

**Tgaz Editor: Replace the following paragraph at p23.36 of TGaz draft**

An RSNA might support SAE authentication, FILS authentication, or PASN authentication ~~both~~(802.11 REVmd 3.0). An RSNA also supports authentication based on IEEE Std 802.1X-2010, or preshared keys (PSKs) after Open System authentication.

**with**

An RSNA might support one or more of SAE authentication, FILS authentication, or PASN authentication ~~both~~(802.11 REVmd 3.0) methods. An RSNA also supports authentication based on IEEE Std 802.1X-2010, or preshared keys (PSKs) after Open System authentication.

**CID 5268 - Discussion**

See summary table.

Make it applicable to any management frames. Existing changes in TGaz draft specifies that current behavior for this MIC to be 16 octets in mesh peering frames for compatibility and variable in others.

**CID 5268 - Proposed Changes**

**Tgaz Editor: Add the following to TGaz Draft**

***Change in 9.4.2.118 MIC Element as follows – p1288.9. – REVmd 5.0***

9.4.2.118 MIC element

The MIC element provides message integrity to ~~mesh peering~~ Management frames. The format of the MIC element is shown in Figure 9-535 (MIC element format).

**CID 5299 – Discussion**

This change is mainly related to style, but the comment was marked as technical. Also “;” before Unauthenticated – in 11md D5.0 [1] it is a “.”. We don’t intend to change it.

**CIDs 5299, 5300, 5301 – Proposed changes**

**Tgaz Editor: Replace in TGaz Draft the corresponding text as follows § 11.3 p108.7**

**11.3 STA authentication and association**

***Change “11.3.1 State Variables” by adding another description to the bulleted list as follows: (#2222)***

— *State 1*: Initial start state for non-DMG STAs and for DMG STAs that perform IEEE 802.11

authentication. Unauthenticated and unassociated.

— *State 1a*: Authenticated for non-DMG STAs and for DMG STAs that have performed PASN Authentication (12.12). Unassociated. Association is not possible from this state without non-PASN IEEE 802.11 Authentication. Note: This state is used by STAs that wish to exchange robust management frames e.g., perform secure ranging, but do not wish to exchange data frames.

(#**3520**) (#3132)

**CID 5303 – Discussion**

Comment:

There is no need to modify b) Class 2 frames. Instead add a.i) Class 1a frames and move the allowed frames under this heading. As there is no longer any changes to Class 2 frames, there is no need for changes to references to Class 2 frame in this clause or other clause.

Suggestion:

Remove the changes to Class 2 frames and insert the above b) Class 2 Frames:

"a.i) Class 1a frames

 1) Management frames

 i) Disauthentication

 ii) Unicast SA Query (11.13)

 iii) Protected Dual of Public Action frames (9.6.10)

 iv) Protected Fine Timing frames (9.6.34)"

Additionally, remove all changes to text regarding Class 2 frames, as the definition of Class 2 frames is not changed so there is no need to make the changes. (e.g. at 127.16, etc.)

Can a frame be in multiple classes – protected fine timing frames are possible in State 1a and State 4

Class 1a frames – Protected SA Query, Protected Fine Timing, and Protected Dual of Public Action frames.

State 1a – allows Class 1 and Class 1a frames

State 4 should also allow these frames – Figure 11-16 State 4 needs to change to include Class 1a frames

Class 2 frames are used in authenticated state.

Class 1a requires additional rules about what to do with them in states 2, 3 and 4.

Generally speaking, it’s probably worth changing this area since the semantics become clearer – and the change itself doesn’t really change the semantics. Without PASN PTKSA there is no change to frame classification or filtering – like before.

Update in R3:

Feedback from Jouni:

“What are the use cases, e.g., for DSE, eCSA, GAS, and QMF policy updates? I guess I could think of a potential use for protected GAS, but what about the other ones? Do they really make sense without an association? I'm a bit worried about potential security issues and implementation bugs coming from a change that would allow clearly specific-to-association frames from being allowed in a state that does not have association.”

I agree being conservative would be best for 11az as this is not really needed in for ranging - and this could be revisited in 11me or another TG perhaps – like KDK was re-used in 11ba. Removing protected dual of pub action frames from Class 1a.

**TGaz Editor: In Figure 11-16 p109 replace the phrase in State 1a**

”Class 1, and protected Class 2 Frames”

**with**

“Class 1, and Class 1a Frames”

**TGaz Editor: In § 11.3.3 Frame Filtering based on STA state, replaces lines 5-7 with the following**

A STA shall not transmit Class 2 frames unless in State 2 or State 3 or State 4. In State 1a, A STA shall not transmit frames other than Class 1 and Class 1a frames.

**TGaz Editor: In § 11.3.3 Frame Filtering based on STA state add the following**

***Add Class 1a frames as follows after Class 1 frames and renumber bullets for Class 2 and Class 3 frames to be c) and d):***

b) Class 1a frames

In an infrastructure BSS when PTKSA from PASN authentication exists.

 1) Protected Fine Timing frames (9.6.34)

 2) Unicast SA Query (11.13)

**TGaz Editor: In § 11.3.3 Frame Filtering based on STA remove bullet iv) on page 110 line 4 in Class 2 frames – the bullet relates to PASN frames which are now moved to Class 1a**

**CID 5370 – Discussion**

**CID 5370 – Proposed changes**

**TGaz Editor: replace the following in 12.12.3.2 PASN Frame Construction and Processing p210.3 in non-AP STA PASN frame 2 receive processing**

If the validation fails, the non-AP STA shall terminate the PASN authentication protocol.

Otherwise the STA begins...

**with**

If MIC validation fails, the non-AP STA shall discard the frame and terminate the processing of the frame with no further effect.

If other validation fails, the STA begins the construction the third PASN frame as follows

— 9.4.1.1 (Authentication Algorithm Number field) set to 7 (PASN Authentication)

— 9.4.1.2 (Authentication Transaction Sequence Number field) set to 3

— Status code indicating the failure

— 9.4.2.118 (A MIC element) with MIC computed as specified in 12.12.8 (MIC computation for PASN third frame)

Otherwise, the STA begins...

**TGaz Editor: replace the following in 12.12.3.2 PASN Frame Construction and Processing p210.26 in AP PASN frame 3 receive processing**

For the third PASN frame, if validation fails, or Base AKM processing indicates an error, the AP shall terminate the PASN authentication. Otherwise the AP installs the temporal key derived using MLME-SETKEYS.request primitive to install the new key.

**with**

For the third PASN frame, if the MIC validation fails, the AP shall discard the frame and terminate the processing of the frame with no further effect. If other validation fails, or Base AKM processing indicates an error, the AP shall terminate the PASN authentication. If the validation was successful, the AP installs the temporal key derived using MLME-SETKEYS.request primitive to install the new key.

**CID 5374 – Discussion**

**CID 5374 – Proposed changes**

**TGaz Editor: Add the status code to Table 9-50 Status Codes to indicate missing OCI mismatch**

***Insert (append) the row shown below at the end of Table 9-50—Status Codes* *before the final reserved range.***

|  |  |  |
| --- | --- | --- |
| **Status Code** | **Name** | **Meaning** |
| ANA-missing-oci | OCI\_MISMATCH | OCI does not match received channel information |

**TGaz Editor: Add the following bullet in 12.12.3.2 PASN Frame Construction and Processing after p207.14, before p209.10, and before p210.15, so that the OCI element is included in each of the PASN frames**

— Including an OCI Element containing an OCI element as defined in 9.4.2.236 (OCI element)

**TGaz Editor: Add the following bullet in 12.12.3.2 PASN Frame Construction and Processing after p208.4, before p210.1, and before p210.21 to validate the OCI element is included in each of the frames**

— Validates that an OCI element is present and the Channel information in the element matches current operating channel parameters (see 12.2.9 (Requirements for Operating Channel Validation)). Otherwise, if there is a mismatch, processing status is set to OCI\_MISMATCH

**TGaz Editor: Change the following statement requiring OCVC capability for PASN STAs after p206.1, and p208.23 in 12.12.3.2 PASN Frame Construction and Processing**

— MFPC and MFPR (see 9.4.2.24.4 RSN capabilities) in the RSN capabilities field are set to 22 1

**to**

— OCVC, MFPC and MFPR (see 9.4.2.24.4 RSN capabilities) in the RSN capabilities field are set to 1

**CID 5455 – Discussion**

Options are

1. Keep the LTF generation SAC for cross checking and early detection of key mismatch
2. Convert the field into a reserved field
3. Remove the field