IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbh SA Ballot misc CIDs | | | | |
| Date: 2024 - May | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Misc CIDs.

3008, 3010, 3022, 3026, 3027, 3029, 3028, 3036, 3072, 3084, 3091, 3092, 3093, 3098, 3099, 3100, 3106, 3107, 3109, 3110, 3142, 3149, 3151, 3161, 3172, 3173, 3180, 3187, 3188, 3192, 3199, 3209

Note: Document 24/884 (Mark Hamilton) was referenced for all these CIDs. In many cases the resolution is that proposed by or based upon Mark Hamilton’s comments/suggestions in that document.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3008 | 17.9 | 3.2 | "device identification (ID): [device ID] An ID that a network can provide to a non-access-point (non-AP) station (STA) to allow the non-AP STA to identify itself to a known network at a future time.[84, 65]". Surely it is to the same network? | Replace cited with "device identification (ID): [device ID] An ID that a network can provide to a non-access-point (non-AP) station (STA) to allow the non-AP STA to identify itself to a known that same network at a future time." | Typo in suggested text.  See also CID 3028  Revise  At 17.9 to read:  **“device identifier (ID):** [device ID] An ID provided by an access point (AP) in an ESS to a non-access point (non-AP)  station (STA) to allow the non-AP STA to identify itself to that same ESS at a future time.” |
| 3028 | 17.9 | 3.2 | "identification" is an action or process. So one would expect that the "device identification" definition be about an action or process (which it is not). "Identification" would not normally be abbreviated as ID. Expanding it in the definition makes it read "An identification that a network can provide.." making it sound like a thing (not an action). | Change the term to "device identifier".  Change the definition to "A value provided by an AP to a non-AP STA, that if returned by the non-AP STA to the AP in a future association, allows the AP or another AP in the ESS to identify the non-AP STA."  Update the "measurement identifier" term along similar lines. | See also 3008  Present definition:  **device identification (ID):** [device ID] An ID that a network can provide to a non-access point (non-AP)  station (STA) to allow the non-AP STA to identify itself to a known network at a future time”  Unclear what changes are proposed for Measurement ID, so no changes proposed.  Revise  At 17.9 to read:  **device identifier (ID):** [device ID] An ID provided by an access point (AP) in an ESS to a non-access point (non-AP)  station (STA) to allow the non-AP STA to identify itself to that same ESS at a future time” |
| 3084 | 17.9 | 3.2 | The text "device identification (ID): [device ID]” implies that “ID” is an abbreviation for “identification”. However, “ID” does not seem to be in the abbreviation list of the base standard. Also, on P17L17, "measurement identifier (ID): [measurement ID]” implies that “ID” is an abbreviation for “identifier". | Specify that “ID” is an abbreviation for ‘identifier” and adjust these two definitions accordingly. | See CID 3028  Revise  At 17.9 to read:  **device identifier (ID):** [device ID] An ID provided by an access point (AP) in an ESS to a non-access point (non-AP)  station (STA) to allow the non-AP STA to identify itself to that same ESS at a future time” |
| 3142 | 17.9 | 3.2 | "a device ID" is not defined. CID 105's resolution claims "device ID" is defined in 3.2, but 3.2 defines "device identification" not "device identifier" | I'm not sure whether we're allowed to have a single term expand to two things. If we are, then extend the definition of "device ID" to cover "device identifier" too | Revise  At 17.9 to read:  **device identifier (ID):** [device ID] An ID provided by an access point (AP) in an ESS to a non-access point (non-AP)  station (STA) to allow the non-AP STA to identify itself to that same ESS at a future time” |
| 3010 | 29.6 | 9.4.2.309 | "The PASN Encrypted Data element contains an Encrypted Data field to be encrypted by the KEK." Is it encrypted or not? It says "to be encrypted", so this data is not encrypted which is also clear from Table 9-417c. Hence the term "encrypted data" is misleading, it is data that will be encrypted, or "data for encryption". | Replace "Encrypted" with "Encryption" at the following locations 29.3, 29.6, 29.10 (in Figure 9-1072d), 29.15, 29.20, 29.21, 29.26, 29.44. | Revise  At 29.6, change  "The PASN Encrypted Data element contains an Encrypted Data field to be encrypted by the KEK."  to  "The PASN Encrypted Data element contains encrypted data included in PASN authentication."  At 29.20, change  "The Encrypted Data field contains one or more subelements."  to  "The Encrypted Data field contains one or more subelements encrypted by the KEK (see 12.2.13)." |
| 3161 | 29.6 | 9.4.2.316 | The PASN Encrypted Data element contains an Encrypted Data field to be encrypted by the KEK" -- I don't understand what the future tense is about here. On the air it has been encrypted | Change to "The PASN Encrypted Data element contains an Encrypted Data field encrypted with the KEK" | Revise  At 29.6, change  "The PASN Encrypted Data element contains an Encrypted Data field to be encrypted by the KEK."  to  "The PASN Encrypted Data element contains encrypted data included in PASN authentication."  At 29.20, change  "The Encrypted Data field contains one or more subelements."  to  "The Encrypted Data field contains one or more subelements encrypted by the KEK (see 12.2.13)." |
| 3072 | 29.3 | 9.4.2.319 | Given that this encrypted data element could be used for other purposes in the future, let's drop the PASN | Change "PASN Encrypted Data element" to "Encrypted Data element" throughout. Locations are: 24.26, 24.38, 29.3, 29.15, 29.21, 29.26, 29.44, 39.37, 39.41, 39.58, 44.25, 44.26, 44.27, 44.32, 44.33, 44.34, 44.60, 44.61, 44.52, 44.64 | Rejected.  The current use is specifically only within the context of PASN authentiation, per 12.2.13. To generalize this to be just any sort of encrypted data is confusing, as there are already a number of other fields that carry encypted data in other contexts (such as 4-way handshake messages, and CCMP and GCMP general data encryption). |
| 3022 | 23.6 | 9.3.3.5 | According the rule defined in 4.5.3.4, Reassociation procedure can be used for a STA to change its associaton attributes with the same AP. That's, the STA should disconnect from one AP, and then reassociate with the same AP due to association attributes changing reason. In that case, 11bh identifier also can be used. | change "Association" to "Re(association)" to cover the case mentioned above, and do the same change in other propreciated place as well. | Rejected.  1) Reassocation does not involve "disconnect from one AP", in any scenario. The whole point is that the assocation is "moved" from one AP to another within the ESS, or the assocaiton has \_some\_ attributes changed with the same AP.  2) But, the rules for MAC address usage state explicitly that changing the MAC address during the entire lifetime of an assocation (across any/all APs) is \_not\_ allowed, and is not one of those "some" attributes that can be changed. |
| 3026 | 28.27 | 9.4.2.317 | "contains one of the values"; well of course it does, but the table is not just a list of values, it assigns meaning to those values. | Change the sentence at 28.24 to read "The IRM Status field is present if the element is sent to a non-AP STA and otherwise not present" (so that we have one statement on presence or absence).  Change the statement at 28.26 to read "The IRM Status field is defined in Table 9-417b"  For consistency, change the statement at 28.44 and 28.47 to "The IRM field is present if the element is sent to an AP and otherwise not present." and "The IRM field contains a MAC address.", respectively. | Revised  At 28.24 to read  “When the element is sent to an AP, the IRM Status field is not present.”  Change the statement at 28.26 to read: “When the element is sent from an AP, the IRM Status field is defined in Table 9-417b" |
| 3027 | 17.13 | 3.2 | "can be used" defines ability but ability is not what the definition is for. The definition is mixing behavior (what the non-AP STA does with the IRM) with what the IRM itself is. | Change the definition to "A MAC address that with high probability uniquely identifies a non-AP STA." It might be useful to add "The IRM is not sent in the clear so that the non-AP STA identity is protected." (or similar statement on purpose). | The definition in full is: *A MAC address that can be used by*  *a non-access point (non-AP) station (STA) to identify itself to a network*.”  Agree that “can be used” is an ability and “uniquely identifies”, is correct but so does the designated MAC. However the IRM is sent in the clear for the identification but the new IRM is provided encrypted.  Revise  At 17.13 definition for IRM to read:  *“A random local MAC address provided by a non-access point (non-AP) station (STA)*  *to identify itself to a network*.”  NOTE Please also see CID 3085 and CID 3088 |
| 3029 | 18.15 | 4.5.4.10 | "can" defines ability; "might" more appropriate here. It is not clear why one identifier is "provided" and the other "used". The second sentence seems unnecessary since the mechanisms are introduced in the context of "mitigate this sort of traffic analysis". | Change the first sentence to "Such a STA, might identify itself to the AP (and only the AP) by providing to the AP a device ID previously allocated to the non-AP STA by the network and/or by using as its MAC address the IRM provided by the non-AP STA to the network in the previous association." and remove the second sentence | Cited  *“Such a STA, upon reconnecting to a*  *network, can provide either a device ID previously provided by the network or can use an identifiable*  *random MAC address (IRM) the STA previously provided to the network or both.”*  Reject  “can” means “has the ability to”, and is defined in our spec. “Might” is external to our spec. This is introductory. The second sentence mentions the network recognizing the STA, which is an important distinction and the raison d’etre for TGbh.  "Provide" is for device ID, because the device ID is embedded in the protocol, but the STA is "using" MAC addresses (not providing them), so the IRM as an TA is a "use". |
| 3036 | 18.15 | 4.5.4.10 | Change from 'STA' to 'non-AP STA' in this paragraph for the newly added text. A separate comment to be submitted to REVme for the baseline text. | as in comment | Revise  At 18.15, 18.14 and 18.20  Change “a STA” to “a non-AP STA” |
| 3091 | 39.21 | 12.2.12.2 | As mentioned in the comment targeted to P38L27, the concept of “initial” should be generalized. | Revise accordingly. | Cited  *In the case of an initial association to an AP in an ESS*,  At 38.27 we have  *When associating or authenticating using PASN for the first time to an ESS*  Revised  At 39.20 delete Note 2.  And insert following text:  “When associating for the first time or authenticating using  PASN for the first time to any AP in an ESS, the AP sets the IRM status field to 1 indicating Not Recognized. In this case, the non-AP STA shall ignore that setting and continue to associate or authenticate using  PASN.”  At 39.20 insert new Note 2:  “Note 2 - A STA might delete a stored IRM at any point in time for implementation specific reasons” |
| 3092 | 39.21 | 12.2.12.2 | The text “would ignore that” is non-normative, which is appropriate given its location within a note. But is there a normative statement elsewhere specifying this behavior? | Revise accordingly. | *Cited text*  *NOTE 2—In the case of an initial association to an AP in an ESS, the AP indicates that the non-AP STA is not*  *recognized, but the non-AP STA would ignore that.*  Reflector discussion showed support for adding note on a STA deleting IRMs similar to device ID.  Revised  At 39.20 delete Note 2.  And insert following text:  “When associating for the first time or authenticating using  PASN for the first time to any AP in an ESS, the AP sets the IRM status field to 1 indicating Not Recognized. In this case, the non-AP STA shall ignore that setting and continue to associate or authenticate using  PASN.”  At 39.20 insert new Note 2:  “Note 2 - A STA might delete a stored IRM at any point in time for implementation specific reasons” |
| 3093 | 39.32 | 12.2.12.2 | The text “ought to” is not typically used in IEEE standard. It appears to be intended to mean “should”. Such text should be within a normative paragraph, not in a note. Also, consider the overlap with P38L29 ("Each time the non-AP STA associates with an AP in an ESS, it may provide a new IRM to the AP during association.”), which uses the very weak word “may". | Revise accordingl; e.g., change NOTE 3 to: "Changing the IRM in each assocaition or PASN preassociation conttributes to privacy enhancement." | Revised  Delete Note 3 and add  “A non-AP STA should change the IRM at each association or PASN  Preassociation.” |
| 3098 | 52.32 | AF.4 | Use of normative language ("should") in an informative clause. | change to:  A new opaque identifier is generated with a pad length that differs from the pad length of the previously wrapped identifier. | Accept |
| 3099 | 51.25 | AF.1 | Use of normative language in an informative clause ("may"). | "This annex provides an example scheme for generating opaque identifiers suitable for use in the Device ID field of the Device ID element" | Accept |
| 3100 | 48.64 | B | Normative language ("may") in a footnote (which are informative).  Yes, this one is all over 802 standards. Sign. Here's the same suggestion I've made to other groups for other standards. | change to: "  Copyright release for PICS proforma: Users of this standard are granted permission to freely reproduce the PICS proforma in this annex so that it can be  used for its intended purpose. Permission is further granted to publish the completed PICS. | Reject  This is baseline text and the commenter is recommended to take it up with 11me. |
| 3106 | 45.17 | 12.13.7 | This "or" is ambiguous. | Change the phrase to "the AKMP is neither PASN AKMP nor PAS with defined key wrap AKMP" | Revised  At 45.17  Change  “if the AKMP is other than PASN AKMP or PASN with defined key wrap AKMP”  to  “if the AKMP is neither PASN AKMP nor PASN with defined key wrap AKMP” |
| 3107 | 45.41 | 12.13.7 | Should this "and" be an "or", so the condition applies when dot11KEKPASNActivated is false? | Change "and" to "or" | Po Kai provided the resolution. Reference approved document 24/0044r8  Revised  At cited location, sentence to read:  “When dot11KEKPASNActivated is false or when dot11KEKPASNActivated is true and the KEK in PASN field in the RSNXE from the peer is 0, PTK is composed of the Key Confirmation Key (KCK), Temperal Key (TK) and the Key Derivation Key (KDK which are derived as follows:” |
| 3109 | 46.10 | 12.13.7 | "The Key ID in the PTKSA (see 12.6.1.1.6 (PTKSA)) resulting from PASN authentication shall be 3 0." It's either 3 or 0. | The correct text will need to be taken from the next REVme update (this is wrong in the baseline), and kept in synch. | Reject  Baseline text.  Commenter does not identify a change. |
| 3110 | 39.57 | 12.2.13 | This text is not explicit about how many 0x00 octets are required. | Replace "zero or more 0x00 octets" with "a number of 0x00 octets such that the length of the Encrypted Data field is at least 16 octets and a muiltple of 8 octets. | Reject  This text is aligned with similar text in the baseline. |
| 3149 | 51.30 | AF.1 | It is not clear what "distinct ESSs" are. CID 187 rejected a change to "multiple ESSes" on the basis that "You can't know whether you have multiple objects unless you have a way of identifying distinct--i.e. recognizably different--instances of said object." | Add a definition of ESS distinctiveness | Rejected.  1) This is an informative annex, so there's a limit to how much effort to put into technical fine details. 2) 802.11 ARC SC has spent considerable time wrestling with how to define unique ESSs, with little success. |
| 3151 |  | 9.3.3 | Shouldn't the order numbers depend on the baseline? | Ensure no duplication or gaps | Rejected.  No problem is identified in the comment. |
| 3171 | 43.32 | 12.13.2 | "the AP with dot11KEKPASNActivated equal to true" is confusing | Change to "an AP that has dot11... equal to true" | Reject  Similar wording is present in the baseline |
| 3172 | 45.18 | 12.13.7 | "if the Base AKMP is PASN AKMP or PASN with defined key wrap" should be +" AKMP" | As it says in the comment | Revised  Add “AKMP” at end of cited phrase to read:  “Otherwise, if the Base AKMP is PASN  AKMP or PASN with defined key wrap AKMP” |
| 3173 | 44.59 | 12.13.3.2 | "ncluding a PASN Encrypted Data element and an IRM element as defined in 9.4.2.314 (IRM element) in the PASN Encrypted Data element" makes no sense: why would PASN Encrypted Data element be included in a PASN Encrypted Data element? | Delete "a PASN Encrypted Data element and" | Revise  At cited location change to:  “If dot11IRMActivated is true, including an IRM subelement, as defined in  9.4.2.317 (IRM element), in a PASN Encrypted Data element, if required per the procedure in 12.2.12.2  (Identifiable random MAC address (IRM) operation.”  At 44.25  “If dot11DeviceIDActivated is true, including a Device ID subelement as defined in 9.4.2.316 (Device ID element) in a PASN Encrypted Data element, if  required per the procedure in 12.2.12.1 (Device ID mechanism)”  At 44.31  “If dot11IRMActivated is true, including an IRM subelement, as defined in  9.4.2.317 (IRM element), in a PASN Encrypted Data element, if required per the procedure in 12.2.12.2  (Identifiable random MAC address (IRM) operation.” |
| 3180 | 46.50 | 12.13.7 | "The Key ID in the PTKSA (see 12.6.1.1.6 (PTKSA)) resulting from PASN authentication shall be 0.[184]" -- isn't this incompatible with extended key IDs for individually addressed Data frames? | Clarify | Resolved by Jouni,  Note to Editor: At 46.9 the “ 3” should be deleted. It is baseline text, but it is incorrect and PASN will set the PTKSA Key ID to 0 in all cases.  Reject  PASN being “incompatible” with extended key IDs, yes, that is correct and expected. PASN is for cases where there is no long term association and no mechanism is defined for rekeying the TK (from PTK). As such, there is no case under which there would be need to be able to indicate or use Key ID 1 since only a single TK is ever derived for the full duration of the security association coming from PASN authentication. |
| 3187 | 52.15 | AF.3 | "All APs in an ESS use the same tweak length for all opaque identifiers which are generated and parsed." -- how is this achieved? | Change to "All APs in an ESS need to use the same tweak length for all opaque identifiers that are generated and parsed." (uses definition of "need to" from REVme) | Accept.  (Note, the change from "which" to "that" is already done in the REVme baseline (the comment quotes the baseline incorrectly). |
| 3188 | 52.23 | AF.3 | " If so, the unwrapped identity is passed up to the protocol using the scheme with an indication of success." -- and if not? | Presumably " the protocol using the opaque device identifier fails" | Revised.  Add a sentence, "If not, the protocol using the opaque device identifier is notified of the failure and no identifier is passed up." |
| 3192 | 30.29 | 9.6.36.1 | "These frames are identified by the single octet IRM Action field, which follows immediately after the Category field." duplicates the figure and should be "An IRM Action field, in the field immediately after the Category field, differentiates the formats.". Baseline Subclause 1.4 talks of "references in this standard to a “<name> frame”, where <name> corresponds to an Action frame subtype identified by the octet immediately after the Category field (the <something> Action field identified in the subclauses of 9.6 (Action frame format details))"  I accept that there are some "in the octet immediately after the Category field"s in 9.6 but I don't think we should make it any worse | As it says in the comment | This text was copied from a baseline example, but the commenter says this is not the best example.  slight change proposed.  Revise  Change cited text at 30.29 to  “An IRM Action field, immediately after the Category field, differentiates the meanings." |
| 3199 | 42.50  51.58? | AF.2 | How is n determined at both sides / negotiated? | Add a NOTE to explain that the non-AP STA does not need to know n, since it does not parse the opaque identifier, it merely passes it on to another AP | At 51.58 the variable n is first mentioned but it is not defined at all at that point. It is not until line 64 that we discover that n is length of tweak.  However  Reject  At 51.38 we have  “To a non-AP STA they are indistinguishable from a random string and have no significance”  Hence it is clear that the non-AP STA knows nothing about opaque IDs. To the non-AP STA it is simply an ID and it does not know if it is opaque or not. |
| 3209 | 51.2 | C.3 | "at the STA" seems superfluous (and not used for dot11DeviceIDActivated) | Delete the cited text | Revise  At 60.54  Replace  “This attribute, when true at a non-AP STA, indicates support for IRM operation at the STA.[21] This attribute, when true at an AP indicates  that the AP supports IRM.”  With  “This attribute, when true, indicates support for IRM operation.” |