IEEE P802.11
Wireless LANs

|  |
| --- |
| CID Resolutions IRM - 1  |
| Date: 2023 - July |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Proposed resolutions on D1.0 related to IRM scheme.

2,3,4,5,6,7,15,17,21,22,23,25,28,37,38,49,51,57,58,59,60,61,62,64,65,66,67,68,69,70,81,

114,128,135,137,140,148,149,164,168,169,193,196,197,198,207,208,214,224,240,294

Rev 1, small edits

Rev 2, added CIDs 56, 89,100,101,102,108,109,147,156,194

Rev 3, edited CIDs 7, 21, 114 to alternative of adding a note.

Rev 4, added edited text for appropriate CIDs at end of document.

Rev 5, moved similar comments next to each other. Added text at end to clarify edits and ease discussions.

REV 6 completed moving like CIDs together. Updated TG comments and proposals.

REV 7 resolved CID 23. More work on CIDs 135, 224.

REV 8 added error code for different IRM/Device ID, (CID 135, 224), resolved 38, 49, 102, 56. Deleted CIDs on status code removal (resolved by Jay).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed | Resolution |
| 2 | 33 | 12 | "If the AP recognizes the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to 1 and the IRM field is reserved". Status field 0 is recognized, so change the "1" to "0" or change to "recognized" | Change" IRM element is set to 1" to "IRM element is set to "recognized"" | Looking at 11me D 3.0 , the theme appears to be "set to 1 to indicate that…". REVISED At 33.12 Change "is set to 1" to "is set to 0 to indicate that the AP recognizes the IRM"(see edits at end of this document) |
| 3 | 33 | 12 | "...and the IRM field is reserved." In device ID we used a "zero-length". Propose the same here. | Change "...and the IRM field is reserved" to "and has a zero-length IRM field? | ACCEPT(see edits at end of this document) |
| 4 | 33 | 12 | "If the AP does not recognize the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to 0 and the IRM field is reserved." Unrecogniozed is setting 1, but better to jyst set to "unrecognized". Also use "zero-length" IRM field. | Change cited text to "If the AP does not recognize the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to "not recognized" and has a zero-length IRM field" | REVISEDAt 33.12, Change cited text to "If the AP does not recognize the IRM, the IRM Status field of the IRM KDE or IRM element is set to 1 to indicate that AP does not recognize the IRM, and has a zero-length IRM field"(see edits at end of this document) |
| 149 | 33 | 12 | According to description on clause 9, the IRM Status field is set to 0 to indicate "recognized". | Replace "1" with "0" at P33L12, "0" with "1" at P33L13. | Yes, comment is correct. See CIDs 2, 3,4REVISED At 33.12 Change "is set to 1" to "is set to 0 to indicate that the AP recognizes the IRM"At 33.12, Change to "If the AP does not recognize the IRM, the IRM Status field of the IRM KDE or IRM element is set to 1 to indicate that AP does not recognize the IRM, and has a zero-length IRM field" |
| 197 | 33 | 12 | "the IRM Status field of the IRM KDE or IRM element is set to 1" not clear | Change to "... is set to indicate <whatever>". Ditto below | See 2,3,4, 149REVISED At 33.12 Change "is set to 1" to "is set to 0 to indicate that the AP recognizes the IRM"At 33.12, Change to "If the AP does not recognize the IRM, the IRM Status field of the IRM KDE or IRM element is set to 1 to indicate that AP does not recognize the IRM, and has a zero-length IRM field" |
| 5 | 33 | 14 | "The non-AP STA, on receipt of an IRM Status field of value 1 may either continue to associate to the AP or disassociate." Change "value 1" to "set to "not recognized"" | Change "IRM Status field of value 1" to "IRM Status field set to "not recognized"" | REVISEDAt 33.14, Change "IRM Status field of value 1" to "IRM Status field of value 1, indicating the AP has not recognized the IRM, "(see edits at end of this document) |
| 294 | 28 | 33 | The description is unlear. | Suggest to modify this sentence as follows:"...Indicates the IRM has been recognized by the AP..""...Indicates the IRM has not been recognized by the AP.." | REJECTComment is correct, butTable is correct, 0 = recognized, 1 = not recognized. Text has it wrong, See CIDs 2,3,4,5 where the text is corrected. |
| 6 | 34 | 26 | The IRM Status field and IRM field in the IRM KDE format have been defined in the IRM element (9.4.2.307b). be | Simplify the definition of IRM Status field and IRM field by referring to the IRM element (9.4.2.307b) | REVISEDAt 34.26 Replace "The IRM Status field indicates the current status of the IRM." with "The IRM Status field is defined in 9.4.2.307b (IRM element)" and delete lines 28-52. (Accepted CID 37)(see edits at end of this document) |
| 37 | 34 | 26 | In order to avoid duplicate sepc text make a reference to 9.5.2.307b (IRM element) similar to the previous Device ID Status field | Please replace "The IRM Status field indicates the current status of the IRM." with "The IRM Status field is defined in 9.4.2.307b (IRM element)" and delete lines 28-52. | ACCEPT(see also CID 6)(see edits at end of this document) |
| 207 | 34 | 25 | This is the exact same IRM Status field as in C9, no? | Just refer to that, as for the Device ID Status field above | REVISEDReplace "The IRM Status field indicates the current status of the IRM." with "The IRM Status field is defined in 9.4.2.307b (IRM element)" and delete lines 28-52. (See also CID 37)(see edits at end of this document) |
| 7 | 33 | 20 | Since the IRM is locally generated at the non-AP STAs, there are chances that two or more non-AP STAs may generate the same address. AP needs to ensure that conflicts are avoided. | Add mechanisms at AP to ensure that IRM conflicts are avoided. | Need 8,388,608 for 50% chance of collision. 375 for10^-9 chance of collision.(see also CIDs 21, 114) REJECT or add a NOTE? The chance of duplication is the same as for the random and changing MAC addresses. A mechanism may be possible but the TG feels that the chance of duplication is so low that the special case is not required to added in TGbh. ALTERNATIVE At 33.24 add“NOTE: IRM addresses are typically generated with the same algorithm used to generate the Randomized Changing MAC addresses.”ALTERNATIVEAdd “Duplicate” to the Status Field.(Also CIDs 21, 114) |
| 21 | 32 | 54 | the colision issue may happened when non-AP STA may allocate a new IRM MAC address to the AP.AP need the deauth the non-AP STA if the non-AP STA allocate a new IRM that is already allocated by another non-AP STA, and it still be valid. And the de-authentication carrying the reason code of IRM collision | add the solution to address the IRM collision issue. | (see also 7, 114) Add NOTEOR REJECT The chance of duplication is the same as for the random and changing MAC addresses. A mechanism may be possible but the TG feels that the chance of duplication is so low that the special case is not required to added in TGbh.  |
| 114 | 32 | 37 | IRM is a (non-AP) STA-generated identifier. There is a possibility that more than one non-AP STA(s) can choose the same IRM, leading to "ID collision".The non-AP STA should know when ID collision happens so that it can choose another IRM. | Add a mechanism for IRM to inform non-AP STA about the "ID collision" | (see CID 7)ADD NOTE or REJECT. The chance of duplication is the same as for the random and changing MAC addresses. A mechanism may be possible but the TG feels that the chance of duplication is so low that the special case is not required to added in TGbh.  |
| 22 | 30 | 21 | IRM is the abbreviation of "identifiable random MAC address",suppose we need to remove the deplicated words"MAC address" after IRM | change "IRM MAC adress" to "IRM" | Yes IRM = Identifiable Random MAC addressREVISEDAt following locations replace “IRM MAC address” with "IRM": 30.21, 32.47, 32.48, 32.49, 32.54, 32.57, 32.62, 32.63, 33.1, 33.11, 33.13, 33.21, 33.26, 33.31, 33.36, 33.37At 33.4 replace “IRM MAC” with “IRM” See also CIDS 25, 51, 168, 169, 193 |
| 25 | 32 | 47 | replace "IRM MAC address" with "IRM" | as the comments, in line 47,line 48, line 49 and other place | REVISEDAt following locations replace “IRM MAC address” with "IRM": 30.21, 32.47, 32.48, 32.49, 32.54, 32.57, 32.62, 32.63, 33.1, 33.11, 33.13, 33.21, 33.26, 33.31, 33.36, 33.37At 33.4 replace “IRM MAC” with “IRM”  |
| 51 |  |  | The term IRM is being used to refer to the mechanism and the identifier. Also, the acronym is sometimes used as a prefix for MAC address, which is already present in the acronym (IRM MAC address == identifiable random MAC address MAC address). See 33.37, 33.25, 33.21, 33.11. | Choose a term for the mechanism (e.g., IRM mechanism or IRM operation) and a separate term for the identifier (e.g., IRM -- no "MAC address") | Do not think there is any need to add “IRM operation” or such. No reference is provided where there may be a problem REVISEDAt following locations replace “IRM MAC address” with "IRM": 30.21, 32.47, 32.48, 32.49, 32.54, 32.57, 32.62, 32.63, 33.1, 33.11, 33.13, 33.21, 33.26, 33.31, 33.36, 33.37At 33.4 replace “IRM MAC” with “IRM”  |
| 168 |  |  | "IRM" already stands for identifiable random MAC address so "IRM MAC address" is pleonastic | Delete " MAC address" after "IRM" (~19x) | REVISEDAt following locations replace “IRM MAC address” with "IRM": 30.21, 32.47, 32.48, 32.49, 32.54, 32.57, 32.62, 32.63, 33.1, 33.11, 33.13, 33.21, 33.26, 33.31, 33.36, 33.37At 33.4 replace “IRM MAC” with “IRM”  |
| 169 | 19 | 19 | "IRM" is a noun abbreviation | Change to "When using an IRM..." Similarly at line 24 ... and in many other places | Wrong reference. Think it is 30.19“When using IRM, a non-AP STA may…”Commenter wants to sayAt 30.19 Replace “When “When using an IRM…”Similarly at 30.24 “Device ID and an IRM may be used together.”It reads fine. We didn’t say “A Device ID and an IRM may be used together.”REJECT |
| 23 | 30 | 24 | it's not clear how Device ID and IRM used together. | give some clarification on how the two schemes used together, e.g. How the AP identify the STA when the frame sent by STA carries two identifiers. | (see also CID 135) The two schemes are independent. Add Note at 30.25 REVISEDAdd at 30.25 NOTE: Device ID and IRM are independent schemes that allow an AP to recognize a non-AP STA prior to association and identify it during association respectively. The device ID is allocated by an AP, and the IRM is selected by a non-AP STA. If an AP and a non-AP STA both support both IRM and device ID, the non-AP STA might provide both an IRM and a device ID. |
| 135 | 30 | 24 | It is not clear how IRM and Device ID can be used together. Is it possible that STA sometimes uses Device ID and other times uses IRM?What if the IRM and Device ID match to different devices? | Remove possibility to use IRM and Device ID at the same time, or specify all the details related to simultaneous use of these protocols. | REVISEDAdd at 30.25 see CID 23 NOTE: Device ID and IRM are independent schemes that allow an AP to recognize a non-AP STA prior to association and identify it during association respectively. The device ID is allocated by an AP, and the IRM is selected by a non-AP STA. If an AP and a non-AP STA both support both IRM and device ID, the non-AP STA might provide both an IRM and a device ID.Also, incorporate the changes identified as CIDs 135, 224 this document 23/1245 |
| 224 | 19 | 29 | Both IRM and Device ID can be used simultaneously, what happens if each of them identifies a different STA? | This applies to all the document. Need to clarify what happens when there is a collision | REVISEDincorporate the changes identified as CIDs 135, 224 this document 23/1245 |
| 38 | 36 | 48 | Incorrect reference | Please replace "Figure 9.4.2.307b" with "9.4.2.307b (IRM element)" | ACCEPT |
| 49 | 30 | 8 | This subclause needs to 1) describe the problem the mechanisms are addressing. 2) introduce the mechanisms. Improvements to the current text to achieve these goals are provided. Some specific problems with the text are as follows: The "user" in the second sentence is ambiguous. Is this the person using the device that contains the non-AP STA or is this the network operator? The description in the second paragraph applies to both mechanisms, however, since it is using "device ID" it appears intended for only one of the mechanisms. There seems to be a distinction that "device ID" is purely used with association while "IRM" is used with association and PASN authentication (which is contradicted later in the detailed description). | For all but the first sentence, replace with the following:This presents a problem for the network in that it is unable to identify a non-AP STA that previously associated and is not able to apply cached information from that previous association to the current association. The two mechanisms defined in 12.2.11 alleviate this problem."The first mechanism, referred to as the device ID mechanism, has the AP provide an identifier to the non-AP STA during association or PASN authentication that the non-AP STA can then report back to the AP during a future association or PASN authentication. The second mechanism, referred to as the IRM mechanism, has the non-AP STA provide a random MAC address (different from the address it is using) to the AP during association or PASN authentication and then use that MAC address for the next association or PASN authentication.The two mechanisms are not mutual exclusive and may be used simultaneously. | REVISED**At Page 30.8 replace entire text in 12.2.11 with following** “To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address (see 4.5.4.10 (MAC privacy enhancements)).This presents a problem for the network in that it is unable to identify a non-AP STA that previously associated and is not able to apply cached information from that previous association to the current association. The two mechanisms defined in 12.2.11 alleviate this problem.The first mechanism, referred to as device ID, has the AP provide an identifier to the non-AP STA during association or PASN authentication that the non-AP STA can then report back to the AP during a future association or PASN authentication. The second mechanism, referred to as IRM, has the non-AP STA provide a random MAC address (different from the address it is using) to the AP during association or PASN authentication and then use that MAC address for the next association or PASN authentication.The two mechanisms device ID and IRM, may be used concurrently.” |
| 102 | 30 | 24 | What does "may be used together" | Change "Device ID and IRM may be used together" to "Device ID and IRM may be used concurrently" | **Not to editor: same resolution as CID 49****Note to Commenter: the change is accepted but the clause was revised in its entirety. The term “concurrently” is used.**REVISED**At Page 30.8 replace entire text in 12.2.11 with following** “To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address (see 4.5.4.10 (MAC privacy enhancements)).This presents a problem for the network in that it is unable to identify a non-AP STA that previously associated and is not able to apply cached information from that previous association to the current association. The two mechanisms defined in 12.2.11 alleviate this problem.The first mechanism, referred to as device ID, has the AP provide an identifier to the non-AP STA during association or PASN authentication that the non-AP STA can then report back to the AP during a future association or PASN authentication. The second mechanism, referred to as IRM, has the non-AP STA provide a random MAC address (different from the address it is using) to the AP during association or PASN authentication and then use that MAC address for the next association or PASN authentication.The two mechanisms device ID and IRM, may be used concurrently.” |
| 56 | 30 | 19 | The non-AP STA does not 'provide' a random MAC to the AP, this seems to say that the AP gets its MAC from the STA. | Replace with "a non-AP STA, when it associates with an AP or when it performs PASN authentication, may communicate to the AP the value of a new IRM MAC address. | REVISED**At Page 30.8 replace entire text in 12.2.11 with following** “To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address (see 4.5.4.10 (MAC privacy enhancements)).This presents a problem for the network in that it is unable to identify a non-AP STA that previously associated and is not able to apply cached information from that previous association to the current association. The two mechanisms defined in 12.2.11 alleviate this problem.The first mechanism, referred to as device ID, has the AP provide an identifier to the non-AP STA during association or PASN authentication that the non-AP STA can then report back to the AP during a future association or PASN authentication. The second mechanism, referred to as IRM, has the non-AP STA provide a random MAC address (different from the address it is using) to the AP during association or PASN authentication and then use that MAC address for the next association or PASN authentication.The two mechanisms device ID and IRM, may be used concurrently.” |
| 57 | 32 | 47 | The term 'provide' is misleading, it seems to indicate that the STA gives to the AP the MAC that the AP is expected to use. | Replace with "Each time the non-AP STA associates with an AP/ESS, it shares the value of t new IRM MAC address with the AP/ESS, during the RSN association". | Note: Consider CIDs 58-62, 193 and then return to this one.**See Discussion at Page 23**REJECTText makes it clear that it is the STA that uses the IRM. “provide” is a reasonable verb to use. See also CIDS, 58-62, 193. |
| 58 | 32 | 54 | The term 'allocate' is confusing, it seems to indicates that the intention is for the AP to use that MAC as its own, or that the STA will see the AP with that MAC address. | Replace with "the non-AP STA may indicate to the AP the value of a new IRM MAC address" | **See Discussion at Page 23** REVISEDAt 32.54 “When associating to an AP that advertises support for IRM, the non-AP STA may provide a new IRM to the AP” |
| 59 | 32 | 57 | The term 'allocate' is confusing, it seems to indicates that the intention is for the AP to use that MAC as its own, or that the STA will see the AP with that MAC address. | Replace with "the non-AP STA may indicate to the AP the value of a new IRM MAC address" | **See Discussion at Page 23** REVISEDAt 32.57 “When using PASN, the non-AP STA may provide a new IRM to the AP by including the IRM element” |
| 60 | 33 | 26 | The term 'allocated' is confusing, it seems to indicates that the intention is for the AP to use that MAC as its own, or that the STA will see the AP with that MAC address. | Replace with "... as the TA to the AP with which that IRM MAC was previously shared" | **See Discussion at Page 23** REVISEDAt 33.26 “When a non-AP STA sends an Authentication Request using an IRM as the TA to the AP that was provided that address.” |
| 61 | 33 | 29 | The term 'allocated' is confusing, it seems to indicates that the intention is for the AP to use that MAC as its own, or that the STA will see the AP with that MAC address. | Replace with "...for an AP or ESS with which that IRM MAC address was previously shared" | See Discussion at Page 23 REVISEDAt 33.29 “an AP or ESS that was provided that address, such that the AP may identify the non-AP STA” |
| 62 | 33 | 31 | The term 'allocated' is confusing, it seems to indicates that the intention is for the AP to use that MAC as its own, or that the STA will see the AP with that MAC address. | Replace with "a non-AP STA that has previously shared an IRM MAC address with an AP/ESS may use that address..." | See Discussion at Page 23 REVISEDAt 33.31 “non-AP STA that has provided an IRM to an AP/ESS, may use that address” |
| 193 | 32 | 53 | "may allocate a new IRM MACaddress to the AP" -- I don't think the address is allocated to the AP | Change to "may allocate a new IRM for use with the AP". Ditto next sentence. Ditto at 33.25 | See Discussion at Page 23 REVISEDAt 32.53 “When a non-AP STA sends an Authentication Request using an IRM as the TA to the AP that was provided that address”At 33.26 “When a non-AP STA sends an Authentication Request using an IRM as the TA to the AP that was provided that address” |
| 65 | 33 | 4 | This should not be a note (informative); it should be normative and a recommendation. Also, it might not be necessary to generate a new MAC address with each association, especially if they occur within a short time from each other. | Replace the note with a normative statement:Because the MAC address is exposed to third parties during and post association, the non-AP STA should generate a new MAC address either periodically or with each association. | NOTE 1—Allocating a new IRM MAC during each association or PASN preassociation ensures that the non-AP STAwill use a different TA for the next association or PASN preassociation, and hence that non-AP STA is unidentifiable toa third party.Leave as Note or make text?REJECTConcerns behavior of the STA which is better suited to a Note. Also, introducing idea that MAC address can change periodically rather than each association is open ended and not recommended at all. |
| 66 | 32 | 60 | This statement is a repeat of ones at 28.20 and 34.28 and unnecessary | Delete the statement. | “The IRM Status field in the IRM KDE or IRM element is reserved when transmitted by the non-AP STA.” True, maybe 3 times is too much, Inclined to ACCEPT |
| 194 | 32 | 59 | "The IRM Status field in the IRM KDE or IRM element is reserved when transmitted by the non-AP STA." duplicates C9 | Delete | See also CID 66ACCEPT |
| 67 | 33 | 8 | This needs to be a conditional statement (if this and this then this). | Change to "If a non-AP STA indicates support for the IRM mechanism in a (Re-)Association Request frame and the AP indicates support for the IRM mechanism in the corresponding (Re-)Association Response frame, then the AP shall include an IRM KDE in message 3 of the 4-way handshake, or, if using FILS authentication, in the Association Response frame. | Presently “When a non-AP STA that advertises support for IRM associates to an AP that advertises support for IRM, the AP shall include an IRM KDE in message 3 of the 4-way handshake or, when using FILS authentication,including an IRM element in the Association Response frame.”REJECTNot convinced the suggested text is better. Main difference is that proposed text expands the ‘advertising/indicating support’ but this is detailed in text later. |
| 68 | 32 | 62 | It is not necessary to state this; it is implied by the statements for OTA operation. This is essentially a statement about implementation. | Delete the statement that begins: "The non-AP STA should store..." | Text is “The non-AP STA should store the newly allocated IRM MAC address as an identifier for use with that AP/ESSand the AP/ESS should store that IRM MAC address as an identifier for that non-AP STA”Inclined to REJECT The idea is to make sure that the AP must remember the IRM list. Is it obvious - maybeAlternative is to make it a NOTE? But prefer REJECTThe idea is to make sure that the AP and STA remember the IRM list, (same with Device IDs) otherwise the schems do not work. Is it obvious - maybe, but no harm done. |
| 69 | 33 | 21 | Inappropriate reference: 12.2.10 does not describe how a MAC address is constructed from the locally administered address space. Since this paragraph is essentially repeating information in 12.2.10 make a statement about conformance to 12.2.10 instead. | A non-AP STA that uses the IRM mechanism also supports the requirements for MAC privacy enhancement defined in 12.2.10. It might also be better to move this statement earlier in this section. | Text is “An IRM MAC address is a 48-bit address that is constructed from the locally administered address space (see12.2.10).”Needs discussion on whether we need to reference (12.2.10) or is “locally administered address space” enough? REVISEDAt 33.20 Delete “(see 12.2.10)” |
| 70 | 17 | 9 | The term "identifiable random MAC address" does not accurately describe its purpose. It is generated randomly, but there is nothing inherently identifiable about it. It would be better to describe it as an address for future use. | Use a term that better describes the purpose. For example, "Future MAC address (FMA)" | Could use MAAD "MAC Address Designation" if preferred? Not a fan of FMA. IRM has been used for a long time now.REJECTThe IRM is random, and it is identifiable because the AP was given it in advance.  |
| 81 | 32 | 56 | The sentence says "..., including the IRM element in the Association Response frame."Should it be Association Request? | Change Association Response to Association Request. | ACCEPT |
| 147 | 32 | 56 | I think "the Association Response frame" should be replaced with "the Association Request frame" because the frame seems to be transmitted by the non-AP STA. | As in comment | ACCEPT (see also CID 81) |
| 108 | 32 | 43 | The amendment cannot enforce a normative requirement on a configuration of an ESS. | Remove "APs in a givenESS shall set this field to the same value."At 30.36, add "NOTE -- The IRM Active field should be confiigured consistently throughout the ESS." | ACCEPT |
| 109 | 33 | 8 | "When a non-AP STA advertises support..." non-APs do not advertise support, they negotiate support. | Change "When a non-AP STA that advertises support for IRM associates ..." to "When a non-AP STA that negotiates support for IRM, by setting the IRM Active field to 1 in the Extended RSN Capabilities field, associates ..." | REJECTThere is no negotiation taking place. The non-AP STA decides to make active or not. |
| 128 | 32 | 37 | IRM as defined in this clause, appears to repeat exisiting non-AP STA behaviour that was introduced by 802.11aq. A non-AP STA can already allocate a new MAC address every time it wishes to (re)associate, so I don't see what is new here. Furthermore, the exisiting behaviour is reinforced by NOTE 3 (P33L35). | Remove clause 12.2.11.2. | REJECT No it does not repeat 11aq. The non-AP STA provides a new MAC Address (IRM) **in advance.** It is new. |
| 137 | 28 | 43 | IRM currently defines only one MAC address for a STA. The use of authentication MAC addresses could help and relax STA associations with the network. | Please allow IRM to configure multiple addresses for the STA. | **Needs discussion**. IRM can easily allocate more than one MAC address. Address 1 used ONLY for probes, and address 2 used ONLY for associaition. Does add another level of privacy but increases length of the KDE. |
| 140 | 30 | 21 | Please clarify the random generation procedure of the IRM MAC addresses such that a returningnon-AP STA cannot be identified by a third party from the TA it is using. | Indicate how the IRM MAC addresses are generated | Do we need more than at 30.19? And 33.22? Maybe at 32.33 "A non-AP STA should generate the IRM MAC addresses on a random basis", become a "shall"? Could add "random" in a few more places to be very clear. Either REVISED At 32.47 change "new IRM", to "new random IRM" ?REJECT30.19 and 33.22 both refer to random generation. No need to say it again. |
| 148 | 33 | 11 | AP's behavior is unclear a little."If the AP recognizes the IRM MAC address, ..." what is the IRM to be recognized should be described. Is it the IRM used as the TA? | Propose to change"If the AP recognizes the IRM MAC address, "to"If the AP recognizes the IRM used as the TA in the received frame(s) from the non-AP STA, ..." | REVISEDThe previous sentence makes it clear where the IRM is, i.e., in the IRM KDE in msg 3 of 4-way HS.At 33.11 Change “If the AP recognizes the IRM MAC address” to “If the AP recognizes the IRM in the IRM KDE,”(see edits at end of this document) |
| 164 | 28 | 41 | "The IRM field is a 48 bit MAC address" -- figure already shows it's 48 bits | Delete "48 bit". Also at 34.49. Also delete "48-bit" at 33.20. Change a to an where necessary | ACCEPT |
| 156 | 18 | 18 | "but protects theinformation from third parties" -- not clear which information this is, or how it is protected. Also not clear what the subject is (device ID? MAC address?) | Clarify | Same text as agreed for CID 240.(see edits at end of this document)  |
| 240 | 18 | 18 | The general description is awkwardly phrased and hard to parse. | Change: "Such a STA, when reconnecting to a network, can exchange a device ID that allows the network to recognize the device and/or use a MAC address that it previously provided to the network, but protects the information from third parties."To: "Such a STA, may provide a device ID when (re)connecting to a network and/or use a MAC address known to the network (an IRM) that to allows the network to recognize the device, while continuing to mitigate the abilities of third parties to do traffic analysis." | See also CID 156 Inclined to ACCEPTBut probably needs word-smithing(see edits at end of this document) |
| 196 | 33 | 8 | "When a non-AP STA that advertises support for IRM associates to an AP that advertises support for IRM, theAP shall include an IRM KDE in message 3 of the 4-way handshake or, when using FILS authentication,including an IRM element in the Association Response frame. " -- already stated a few lines above | Delete | ACCEPT |
| 198 | 33 | 12 | "and the IRM field is reserved." already stated in C9 | Delete. Also at line 14 | REJECTTrue it is a repeat, but it does fit here in that it describes the process.  |
| 208 | 34 | 64 | "IRM KDE is a KDE containing IRM MAC addresses." -- it can only contain one | Change to "IRM KDE is a KDE containing an IRM." | ACCEPT |
| 214 | 35 | 29 | The IRM KDE can't be mandatory | Change "{IRM KDE}" to "{} or {IRM KDE}" | ACCEPT |

**CIDs 135, 224 -** What if the IRM and Device ID match to different devices?

At 27.57 add new line to Table 9.322aq

|  |  |  |
| --- | --- | --- |
| Device ID Status | Name | Meaning |
| 0 | Recognized | Indicates the device ID was recognized by the AP. |
| 1 | Not Recognized | Indicates the device ID was not recognized by the AP. |
| 2 | No agreement | Device ID does not correspond with IRM |
| 3-255 | Reserved |  |

Add at 31.29

“If a non-AP STA associates or PASN authenticates with an IRM and also provides a device ID that the AP does not recognize as corresponding to that non-AP STA, then the AP shall set Device ID status to 2 indicating “No agreement.”

At 28.57 add new line to Table 9.322ar

|  |  |  |
| --- | --- | --- |
| IRM Status | Name | Meaning |
| 0 | Recognized | Indicates the IRM was recognized by the AP. |
| 1 | Not Recognized | Indicates the IRM was not recognized by the AP. |
| 2 | No agreement | IRM does not correspond with Device ID |
| 3-255 | Reserved |  |

Add at 33.16

“If a non-AP STA associates or PASN authenticates with an IRM and also provides a device ID that the AP does not recognize as corresponding to that non-AP STA, then the AP shall set IRM status to 2 indicating “No agreement.”

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**CID 49 (reprinted here to aid word smithing:**

30.8

**ORIGINAL:**

To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address (see 4.5.4.10 (MAC privacy enhancements)). For some services, however, it may be desired by the user that the non-AP STA is identified by an AP and network services.

An AP may provide a device ID to a non-AP STA to allow any AP in the AP’s ESS to recognize the non-AP STA when it returns to that ESS even if the non-AP STA changes its MAC address. The non-AP STA may provide that device ID to any AP in the same ESS upon a new association. Exchanges of the device ID are protected from third parties.

When using IRM, a non-AP STA may provide a random MAC address to an AP either when it associates or when it performs PASN authentication. The non-AP STA may then use that IRM MAC address as its TA when it returns to the ESS or AP such that the non-AP STA may be identified pre-association.

Device ID and IRM may be used together.

**PROPOSED**To mitigate tracking and traffic analysis, a non-AP STA may randomly change its MAC address (see 4.5.4.10 (MAC privacy enhancements)).

This presents a problem for the network in that it is unable to identify a non-AP STA that previously associated and is not able to apply cached information from that previous association to the current association. The two mechanisms defined in 12.2.11 alleviate this problem.

The first mechanism, referred to as ~~the~~ device ID ~~mechanism~~, has the AP provide an identifier to the non-AP STA during association or PASN authentication that the non-AP STA can then report back to the AP during a future association or PASN authentication. The second mechanism, referred to as ~~the~~ IRM ~~mechanism~~, has the non-AP STA provide a random MAC address (different from the address it is using) to the AP during association or PASN authentication and then use that MAC address for the next association or PASN authentication.

The two mechanisms ~~are not mutual exclusive and~~, device ID and IRM, may be used ~~simultaneously~~ concurrently.

As per CID 102

The two mechanisms ~~are not mutual exclusive and~~, device ID and IRM, may be used ~~simultaneously~~ concurrently.

NOTE: Why I prefer ‘concurrently”.

“Concurrent” is about two activities overlapping in duration.

“Simultaneously” refers to things happening at the same instant, that share a connection.

**CID 240, 156**

**18.18**

Change: "Such a STA, when reconnecting to a network, can exchange a device ID that allows the network to recognize the device and/or use a MAC address that it previously provided to the network, but protects the information from third parties."

To: "Such a STA, may provide a device ID when (re)connecting to a network and/or use a MAC address known to the network (an IRM) that to allows the network to recognize the device, while continuing to mitigate the abilities of third parties to do traffic analysis."

Proposal

Such a STA, when reconnecting to a network, can exchange a device ID that allows the network to recognize the device and/or use a MAC address (IRM) that it previously provided to the network, ~~but protects the information from third parties~~ while continuing to mitigate the abilities of third parties to do traffic analysis.

CIDS 2,3,4,5, 149, 197

33.8

When a non-AP STA that advertises support for IRM associates to an AP that advertises support for IRM, the AP shall include an IRM KDE in message 3 of the 4-way handshake or, when using FILS authentication, including an IRM element in the Association Response frame. If the AP recognizes the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to ~~1~~ 0 to indicate that the AP recognizes the IRM and ~~the IRM field is reserved~~ has a zero length IRM field. If the AP does not recognize the IRM MAC address, the IRM Status field of the IRM KDE or IRM element is set to ~~0~~ 1 to indicate that AP does not recognize the IRM and ~~the IRM field is reserved~~ has a zero length IRM field. The non-AP STA, on receipt of an IRM Status field of value 1, indicating the AP has not recognized the IRM, may either continue to associate to the AP or disassociate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CID 6, 37, 207

34.26

The IRM Status field ~~indicates the current status of the IRM.~~is defined in 9.4.2.307b (IRM elemtent).

~~When sent from a non-AP STA to an AP, the IRM Status field is reserved.~~

~~When sent from an AP to a non-AP STA, the IRM Status field contains one of the following values as~~

~~defined in Table 12-11a (IRM Status field values).~~

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CID 148

33.11

If the AP recognizes the IRM ~~MAC address~~ in the IRM KDE, the IRM Status field of the IRM KDE or IRM element is set to …

DISCUSSION ON ALLOCATE< SHARE< INDICATE etc.

(Note: “IRM MAC address” has been changed to “IRM”

**My recommendation** – Stick to “provides”, seems pretty clear. “Allocates” is probably wrong as the identity is for the STA, and “shares” is not much better.

CID 57 32.47 REJECT (keep original)

Each time the non-AP STA associates with an AP/ESS, it provides a new IRM to the AP/ESS during the RSN association.

“Each time the non-AP STA associates with an AP/ESS, it shares the value of a new IRM to the AP/ESS during the RSN association”

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CID 58 32.54 REVISE

“When associating to an AP that advertises support for IRM, the non-AP STA may allocate a new IRM to the AP”

“When associating to an AP that advertises support for IRM, the non-AP STA may indicate to the AP the value of a new IRM.”

(CID 193) When associating to an AP that advertises support for IRM, the non-AP STA may allocate a new IRM for use with the AP

**Proposed**

“When associating to an AP that advertises support for IRM, the non-AP STA may provide a new IRM to the AP”

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_CID 59 32.57

When using PASN, the non-AP STA may allocate a new IRM to the AP by including the IRM element

When using PASN, the non-AP STA may indicate to the AP the value of a new IRM by including the IRM element

**Proposed**

When using PASN, the non-AP STA may provide a new IRM to the AP by including the IRM element

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CID 60 33.26

When a non-AP STA sends an Authentication Request using an IRM as the TA to the AP that was allocated that address,

When a non-AP STA sends an Authentication Request using an IRM as the TA to the AP with which that IRM was previously shared,

(CID 193) When a non-AP STA sends an Authentication Request using an IRM as the TA for use with the AP,

**Proposed**

When a non-AP STA sends an Authentication Request using an IRM as the TA to the AP that was provided that address,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CID 61 33.29

an AP or ESS that was allocated that address, such that the AP may identify the non-AP STA

an AP or ESS with which that IRM was previously shared, such that the AP may identify the non-AP STA

**Proposed**

an AP or ESS that was provided that address, such that the AP may identify the non-AP STA

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CID 62 33.31

non-AP STA that has allocated an IRM to an AP/ESS, may use that address

non-AP STA that has previously shared an IRM with an AP/ESS, may use that address

**Proposed**

non-AP STA that has provided an IRM to an AP/ESS, may use that address

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_