IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbh SA Ballot 2 Technical CIDs | | | | |
| Date: 2024 - July | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

Technical CIDs

4011, 4013, 4014 4018, 4020, 4023, 4029, 4030, 4034, 4035, 4039, 4043, 4044, 4045, 4047,~~4054, 4055~~, 4060, 4062, 4063, 4064, 4067,4068, 4069,4070, 4073, 4085, 4086, 4087, 4088, 4089, 4090, 4091, 4092, 4093, 4101, 4111, 4114

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4011 | RISON, Mark | 52 | AF.1 | 35 | It is not clear what "distinct ESSs" are. CID 3149 admits that "802.11 ARC SC has spent considerable time wrestling with how to define unique ESSs, with little success." | Change to "multiple ESSs" | The intention is that there is enough randomness that the same opaque identifier is not used for different ESSs  ACCEPT. . |
| 4013 | RISON, Mark | 28 | 9.4.2.19.7 | 13 | "The Measurement ID element has the format defined in Figure 9-1074c (Measurement ID element format). When the Measurement ID element is included in a Beacon request, it requests the responding STA include the provided Measurement ID element in the Probe Request frames the STA transmits.[3005, 3153]" still seems to confuse the element and the subelement, and the fact that it's the payload you carry in the probereq, not the subelement per se | As it says in the comment | REJECT - True, the Measurement ID element has a subelement Measurement ID. BUT As per P25.63, the Measurement ID element is included in the Probe Request frame. Hence this is correct. |
| 4014 | RISON, Mark | 30 | 9.4.2.317 | 25 | "When the element is sent from an AP, the IRM Status field is defined in Table 9-417b (IRM Status field values).[3026]" -- not clear what it's set to otherwise | Add a sentence "When the IRM element is sent to an AP, the IRM Status field is not present." as for Device ID | REJECT Two lines above cite, is the sentence requested. |
| 4018 | RISON, Mark | 31 | 9.4.2.319 | 17 | "The Encrypted Data field contains one or more elements encrypted by the KEK" -- subelements, given the end of the para | Change "elements" to "subelements" | REVISE incorporate the changes in 24/1316r2 |
| 4020 | RISON, Mark | 47 | 12.13.8 | 2 | "the Encrypted Data field in the Encrypted Data element" should be "… in the PASN Encrypted Data element" | As it says in the comment | ACCEPT |
| 4023 | RISON, Mark | 44 | 12.13.2 | 29 | "the AP with dot11KEKPASNActivated equal to true" -- not clear what "the AP" refers back to here | Change to "an AP…" | ACCEPT |
| 4029 | RISON, Mark | 30 | 9.4.2.318 | 48 | Like the Device ID element, the Measurement ID element should be extensible | As it says in the comment | REJECTED The element currently does not include a length field for the Measurement ID value. The scope is limited and it is considered there is limited to no value in making it extensible. |
| 4030 | RISON, Mark |  | 9.3.3 |  | It is not clear why FILS has to be activated to be able to use DID | In 9.3.3.5/6, after the table add a "NOTE---Device ID and IRM elements are not included if dot11FILSActivated is not true because they are instead carried in the 4-way handshake." | REJECT The use of the DID in FILS is extensively covered in clause 12 that clearly states the coupling referred to. No need to also add that in clause 9. |
| 4034 | RISON, Mark | 39 | 12.2.13.2 | 59 | "The non-AP STA may also use that IRM as its TA for any Probe Request frames, directed or broadcast, public Action frames, Authentication frames, and (Re)Association frames that it may transmit when it intends to be identified." -- the modals seem wrong | Change to "The non-AP STA shall also use that IRM as its TA for any Probe Request frames, directed or broadcast, public Action frames, Authentication frames, and (Re)Association frames that it transmits when it intends to be identified." | ACCEPT |
| 4035 | RISON, Mark |  | C.3 |  | dot11DeviceIDActivated is "the device ID mechanism is supported" but dot11IRMActivated is "the STA supports IRM operation". Either both should be active, or both should be passive | As it says in the comment | REVISE At P52.1 change “indicates that the STA supports IRM operation" to "indicates that the IRM mechanism is supported." |
| 4039 | RISON, Mark | 40 | 12.2.13.2 | 34 | "If the AP recognizes the IRM used as the TA in the received frame(s) from the non-AP STA, the AP shall set the IRM Status field of the IRM KDE or IRM element to Recognized and the IRM field is not present. If the AP does not recognize the IRM, the AP shall set the IRM Status field of the IRM KDE or IRM element to Not Recognized and the IRM field is not present. " -- the IRM field absence is already specified in Clause 9 (and it reads wrong anyway) | Change to "If the AP recognizes the IRM used as the TA in the received frame(s) from the non-AP STA, the AP shall set the IRM Status field of the IRM KDE or IRM element to indicate Recognized. If the AP does not recognize the IRM, the AP shall set the IRM Status field of the IRM KDE or IRM element to indicate Not Recognized. " -- the IRM field absence is already specified in Clause 9 | REVISE  At 40.35 delete “and the IRM field is not present”  Note to commentor: the main text is subject to changes from other CIDs. |
| 4043 | RISON, Mark | 38 | 12.2.13.1 | 56 | Per the resolution of CID 3200, "a new shared identity" should be "a new shared identity state" | As it says in the comment | ACCEPT |
| 4044 | RISON, Mark | 39 | 12.2.13.2 | 20 | "The RSNXE with the IRM Support field equal to 1" -- this is already stated in the previous sentence | Delete "with the IRM Support field equal to 1" | REVISE  At 39.19 Change cited para to read  “A non-AP STA that has dot11IRMActivated equal to true indicates that the IRM mechanism is supported by setting the IRM Support field to 1 in the Extended RSN Capabilities field in the RSNXE  in either the (Re)Association Request frames or the first PASN frame that  it sends to an AP that advertises support for the IRM mechanism.” |
| 4045 | RISON, Mark | 39 | 12.2.13.2 | 20 | "The RSNXE […] is present in either (Re)Association Request frames or the first PASN frame that it sends to an AP that advertises support for the IRM mechanism." -- doesn't this duplicate Clause 9? | Delete the cited text | REVISE  At 39.19 Change cited para to read  “A non-AP STA that has dot11IRMActivated equal to true indicates that the IRM mechanism is supported by setting the IRM Support field to 1 in the Extended RSN Capabilities field in the RSNXE  in either the (Re)Association Request frames or the first PASN frame that  it sends to an AP that advertises support for the IRM mechanism.” |
| 4047 | RISON, Mark | 17 | 3.2 |  | Some of the definitions are in terms of a "network", others are in terms of an "ESS" or APs therein. The same term should be used for all | As it says in the comment | REVISED  At 19.15 change "..to identify itself to a network" to "to indentify itself to an extended service set (ESS)" |
| ~~4054~~ | ~~RISON, Mark~~ | ~~31~~ | ~~9.4.2.319~~ | ~~18~~ | ~~"The element format is defined in 9.4.3" well, no, 9.4.3 is about the subelement format~~ | ~~Refer to 9.4.2.1. instead~~ | ~~ACCEPT~~ |
| ~~4055~~ | ~~RISON, Mark~~ | ~~31~~ | ~~9.4.2.319~~ | ~~18~~ | ~~"subelement" has been changed to "element", but the rest of the para continues to refer to subelements~~ | ~~Revert the change~~ | ~~The text seems to be editor instructions. Needs sorting~~ |
| 4060 | RISON, Mark | 37 | 12.2.13.1 | 38 | "the AP shall provide both a device ID and a PASN ID using the procedure described below: 1) When using FILS authentication and the non-AP STA did not provide a device ID in the Device ID element in the Association Request frame, the AP shall provide a device ID in the Device ID ele-ment and a PASN ID in the PASN ID element in the Association Response frame. 2) When not using PASN or FILS authentication and the non-AP STA didn’t provide a device ID in the Device ID KDE in message 2 of the 4-way handshake, the AP shall provide a device ID in the Device ID KDE and a PASN ID in the PASN ID KDE in message 3 of the 4-way handshake." -- this is missing the cases of using PASN but not FILS, and the cases where the non-AP STA did provide a DID. Similarly for non-AP STA behaviour at the bottom of the page, and AP again on the next page | As it says in the comment | REVISE  Incorporate changes in 24/1301r3    . |
| 4062 | RISON, Mark | 38 | 12.2.13.1 | 11 | "The value of PASN ID shall be random" -- it's just the ID that is random | Delete "value of " | ACCEPT |
| 4063 | RISON, Mark | 44 | 12.7.6.4 | 1 | "Additionally, may include a Device ID KDE and optionally a PASN ID KDE subject to the conditions in 12.2.13.1 (Device ID)." -- the "optionally" is already covered by the "may" | Delete "optionally" | REVISE  Change to "Additionally, may include a Device ID KDE, subject to the conditions in 12.2.13.1 (Device ID)." and "Additionally, may include a PASN ID KDE."  (see 4064) |
| 4064 | RISON, Mark | 44 | 12.7.6.4 | 1 | "Additionally, may include a Device ID KDE and optionally a PASN ID KDE subject to the conditions in 12.2.13.1 (Device ID)." -- the "optionally" is already covered by the "may" | Change to "Additionally, may include a Device ID KDE, subject to the conditions in 12.2.13.1 (Device ID)." and "Additionally, may include a PASN ID KDE." | ACCEPT |
| 4067 | RISON, Mark | 46 | 12.13.8 | 47 | "When dot11KEKPASNActivated is false or when dot11KEKPASNActivated is true and the KEK In PASN field in the RSNXE from the peer is 0" -- MIB attribute might be absent. Also precedence could be clearer | Change to "When dot11KEKPASNActivated is not true, or when dot11KEKPASNActivated is true and the KEK In PASN field in the RSNXE from the peer is 0" | ACCEPT |
| 4068 | RISON, Mark | 47 | 12.13.8 | 21 | "Extended Capabilities" should be "Extended RSN Capabilities field" | As it says in the comment | ACCEPT |
| 4069 | RISON, Mark | 47 | 12.13.11 | 39 | "To encrypt the Encrypted Data field of the PASN Encrypted Data element, the KEK, as derived from the PTK (see 12.13.8 (PTKSA derivation with PASN authentication)), shall be used with the negotiated key wrap algorithm to encrypt the Encrypted Data field of the PASN Encrypted Data element." is of the form "To do X, do Y to do X" | Change to "The KEK, as derived …" | ACCEPT  Note to editor:  At 47.39 delete “To encrypt the Encrypted Data field of the PASN Encrypted Data element,” and capitalize “The” |
| 4070 | RISON, Mark | 47 | 12.13.11 | 54 | "If the Encrypted Data field uses an AEAD cipher, the Encrypted Data field shall not be padded and the AAD for the encipherment operation shall not be used and the number of AAD components is zero. " not dlear -- the number of AAD components where, in what context? | As it says in the comment | Not sure what to change. |
| 4073 | RISON, Mark |  | AG |  | It is not clear what a "FILS Association Request" is. Ditto "FILS Association Response" | Refer to a specific frame type | REVISED  Delete "FILS" x2 (already done elsewhere) |
| 4085 | RISON, Mark |  | AG |  | "AP/ESS" -- well, which is it? (5x) | I think ESS is probably better | REVISED,  At 54.34 change "AP/ESS" to “ESS”. |
| 4086 | Hamilton, Mark | 22 | 6.5.7.3.2 | 37 | In MLME-ASSOCIATE.response and .confirm this is not the best wording: "Specifies the device ID (or PASN ID) for the requesting STA." It is really providing a "next time" device ID or PASN ID, not "the ID for the STA" (now), but the "ID the STA should use next time". Same thing in 9.3.3.6 for the Association Response frame carrying (FILS only) Device ID or PASN ID. | At the cited locations (MLME-ASSOCIATE.response and .confirm), change "the Device ID [or PASN ID] for the requesting STA" to "a new Device ID [or PASN ID] for the associating STA". | ACCEPT |
| 4087 | Hamilton, Mark | 22 | 6.5.7.3.2 | 48 | We need the PASN ID to be delivered by the MLME-ASSOCIATE indication and confirm. Otherwise, how does the RXr of the info get it to match with a later PASN activity? | Add PASN ID (matching the .request and .response) to the MLME-ASSOCIATE.confirm and .indication primitives. | ACCEPT  or  REVISE  Incorporate changes in 24/1301r3 |
| 4088 | Hamilton, Mark | 25 | 9.3.3.5 | 25 | The PASN ID provided in the MLME-ASSOCIATE.request needs to be carried in the Association Request frame. | Add PASN ID (matching the Association Response frame) to the Association Request frame. | REJECT  The STA will never include a PASN ID in an Association request, only in a PASN frame. The AP may however provide a PASN ID as well as a device ID in the initial association case. |
| 4089 | Hamilton, Mark | 45 | 12.13.3.2 | 34 | The non-AP STA can only expect/require the PASN Encrypted Data element if it knows the AP has device ID (or IRM) activiated. Otherwise, we break legacy PASN interopability. | Change cited text to, "If dot11DeviceIDActivated is true and the PASN frame is from an AP that indicated support for the device ID mechanism in its Beacon or Probe Response frame(s), it validates ...". Same thing at P45.41 (with "incidated support for the IRM mechanism"). Then, again, same things at P45.59 and P46.1. | ACCEPT |
| 4090 | Hamilton, Mark | 46 | 12.13.8 | 47 | "When dot11KEKPASNActivated is false or when dot11KEKPASNActivated is true and the KEK In PASN field in the RSNXE from the peer is 0,": the "is false" needs to be "is not true" per the implied "or is not present" trick (see REVme 1.4). | Change "When dot11KEKPASNActivated is false" to "When dot11KEKPASNActivated is not true" | ACCEPT  (done elsewhere CID 4067) |
| 4091 | Hamilton, Mark | 41 | 12.2.13.2 | 6 | Its called "PASN authentication". | Change "PASN preassociation" to "PASN authentication" | ACCEPT |
| 4092 | Yang, Jay | 37 | 12.2.13.1 | 37 | [on the behalf of Yan Li]non-AP STA may not perform PASN authentication in the future,which may wast resource to store the PASN ID if AP provides PASN ID in the initial connection by default As the comment | as the comments. | REJECT  True, the PASN ID may never be used, but the STA does not indicate if PASN supported to the AP, so AP cannot know whether to provide PASN ID or not. Note that the AP only provides the PASN ID if the AP supports PASN. |
| 4093 | Smith, Graham | 19 | 3.2 | 23 | PASN ID. It is transient so say so | Insert "transient" before "device ID" | It then matches the transient Measurement ID just above it  ACCEPT |
| 4101 | Levy, Joseph | 36 | 12.2.13 | 29 | There is no such MIB variable as dot11PrivacyActivated, the variable is dot11MACPrivacyActivated. Also, the statement "MAC privacy enhancements are required in order to use the device ID mechanism or the IRM mechanism. A non-AP-STA shall set dot11PrivacyActivated equal to true to use either of these mechanisms." while "correct" is not very clear, as it is not apparent that the MAC privacy enhancements relate to the MAC privacy enhancements in clause 12.2.11. | Replace "MAC privacy enhancements are required in order to use the device ID mechanism or the IRM mechanism. A non-AP-STA shall set dot11PrivacyActivated equal to true to use either of these mechanisms." With:  "The device ID mechanism and the IRM mechanism require that the Non-AP STA supports the MAC privacy enhancements in 12.2.11."  And move the requirement that dot11MACPrivacyActivated is true to the 12.2.13.1 two locations (37.1, 37.12) as shown below: replace : "A non-AP STA that has dot11DeviceIDActivated equal to true ..." With: "A non-AP STA that has dot11MACPrivacyActivated and dot11DeviceIDActivated equal to true ..." And in 12.2.13.2 two locations (39.19 and 39.40) as shown below replace: "A non-AP STA that has dot11IRMActivated equal to true ..." With: "A non-AP STA that has dot11MACPrivacyActivated and dot11IRMActivated equal to true ..." | ACCEPT? |
| 4111 | Sun, Li-Hsiang | 41 | 12.7.2 | 48 | Similar to the device ID element, there should be text saying the Device ID status is not present when sent by non-AP STA, and must be present when sent by AP | as in comment | REJECT.  It is covered by the reference to 9.4.2.316. Do we repeat that here? |
| 4114 | Sun, Li-Hsiang | 20 | 4.5.4.10 | 23 | Not clear what the definition of "shared identity state" is Baseline 12.2.12 does not seem to have the definition of "shared identity state" On p36 L13, is "cached information" the synonym of "shared identity state"? | Define "shared identity state" in clause 3.2 | REJECT  12.2.13 has “apply cached information (shared identity state)”  This is considered sufficient description. |