IEEE P802.11
Wireless LANs

|  |
| --- |
| D1.0 CIDs in clauses 10.71.3 |
| Date: 2025-07-03 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |

Abstract

Abstract

This submission proposes resolution of comments received against the following sections of TGbi Draft 1.0:

* 10.71.3 (Establishing frame anonymization parameter sets),

We propose draft specification text for TGbi draft D1.3.

Resolved CIDs (14): 95, 317, 318, 354, 562, 563, 565, 566, 568, 570, 573, 816, 1069, 1070

Open CIDs (2): 564, 567

Revisions:

* Rev 0: Initial version of the document.

**Background**

Overview of noteworthy changes

* Reorganization of the order of some text
* Adjusting terms and acronyms to align with resolution of CID #223 in 25/1100

Note that there the authors have further changes to 10.71.3 which are provided in in 25/1100.

| **CID** | **Commenter** | **Clause** | **Page.Line** | **Doc** | **Comment** | **Proposed Change** | **Done** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1069 | Philip Hawkes | 10.71.3  | 81.36 |   | The mechanisms for obtaining frame anonymization parameters is spread acrss clauses 10.71.3, 10.71.4 and 10.71.7. This is inconvenient. | For convenience, aggregate all sections on establishing/assigning parameters used in frame anonymization into this section.Create clause 10.71.3.1 with heading "Frame anonymization and AID", and move the contents of D1.0 10.71.7 to this clause. D1.0 clause 10.71.7 is then no longer needed.Create clause10.71.3.2 with heading "Establishing CPE FA parameter sets", and move the contents of D1.0 10.71.3 to this clause.Create clause 10.71.3.3 with heading "Establishing BPE FA parameter sets", and move the contents of D1.0 10.71.4 to this clause. D1.0 clause 10.71.4 is then no longer needed. | **Rev** | **Reject****Discussion:** Not sure it is worth the effort |
| 816 | John Wullert | 10.71.3  | 81.44 |   | The text would be clearer if the description of how the EDP FA block is generated immediately follows the requirement that it is generated. (Note: The order in clause 10.71.4 is in line with the change proposed here.) | Break this sentence into two. The first sentence is "The EDP CPE frame anonymization parameters for a given EDP epoch shall be generated (by the CPE nonAP MLD and CPE AP MLD) by computing a single pseudorandom EDP FA block." This should then be followed by the content from lines 1-20 on page 82. Then the second sentence is "The EDP FA block is partitioned intothe set of EDP CPE frame anonymization parameters as follows:" which is followed by the existing bullet list and subsequent tables. | **Acc** | **Revised****Discussion:** Agreed in principle. Propose deleting lines 45-47, moving bulle be deleted.**Changes**:**P81 lines 44-64**Delete this text.**P82 line 21**Insert new text:“The non-AP MLD and the AP MLD shall extract the CPE MHA parameters from CPE MHA block as follows:**“**This change also addresses the resolution of CIDs: #95, #573, #1070**P82 line 22.**Copy the bullet list from P81 lines 48-64 to here, after applying applying CID #1070 to p81 lines 51-53. |
| 95 | Graham Smith | 10.71.3  | 81.45 |   | "The EDP CPE frame anonymization parameters for a given EDP epoch shall be generated (by the CPE non-AP MLD and CPE AP MLD) by computing a single pseudorandom EDP FA block..." In general the passive tense is not best | Replace cited text with "The CPE non-AP MLD and the CPE AP MLD shall generate the EDP CPE frame anonymization parameters for a given EDP epoch by computing a single pseudorandom EDP FA block..." | **Rev** | **Revised****Discussion**: Agreed in principle. This text is deleted by CID #816.However, this active tense should be applied at p82 line 1 and the new line introduced at p82 line 21 in CID #816. Also note that the “CPE” Prefix for non-AP MLD and AP MLD is not required, as per resolution to CID #130 in 25/1100.**Change:****P82 line 01:** Replace“For a given EDP epoch, the EDP FA block shall be generated as:”with“For a given EDP epoch, the non-AP MLD and the AP MLD shall generate a CPE MHA block as:“This change also addresses the following CIDs: #573, #1070**P82 line 21**:See new line proposed in CID #816 |
| 1070 | Philip Hawkes | 10.71.3  | 81.46 |   | This block is used only forCPE frame anonymization, so the name "EDP FA block" is ambiguous. | Here, and throughout this section, replace "EDP FA Block" with "EDP CPE FA Block" to align with 10.71.4 | **Rev** | **Revised****Discussion**: For the bullet list in p81 lines 48-64: (moved elsewhere by CID #816) the text “from EDP FA block” is redundant – delete these words in the bullet list. Elsewhere Recommend replace “EDP FA block” with “CPE MHA block”. Insert “the” when missing, as per CID #562**Changes**:**p81 lines 48-64**: (moved elsewhere by CID #816)Delete 6 occurrences of “from EDP FA Block” in the list (excluding table captions).*Note: This change also addresses the following CIDs: #573***p83 lines 16**: (moved elsewhere by CID #568)Delete “from EDP FA Block”*Note: This change also addresses the following CIDs: #573***Otherwise**: replace “EDP FA Block” with “CPE MHA block” or “the CPE MHA block”.*Note: This change also addresses the following CIDs: #562, #573* |
| 562 | Mark RISON | 10.71.3  | 81.48 |   | "from EDP FA block" missing article (multiple instances) | As it says in the comment | **Rev** | **Revised****Discussion:** Agree in principle. Resolved as part of CID #1070 |
| 573 | Mark RISON | 10.71.3  | 82.03 |  | It's inconsistent for it to be "EDP FA Block" for CPE but "EDP\_BPE\_FA\_block" for BPE | As it says in the comment | **Rev** | **Revised****Discussion:** Agree in principle. Resolved as part of CID #1070 |
| 570 | Mark RISON | 10.71.3  | 82.09 |  | "which is partitioned" should be "that is partitioned" (American English) | As it says in the comment | **Acc** | **Accepted** |
| 563 | Mark RISON | 10.71.3  | 82.19 |   | "a EDP" should be "an EDP" | As it says in the comment | **Rej** | **Rejected**The text is updated by CID #1070 from “EDP” to “CPE”, and “a CPE” is correct. |
| 564 | Mark RISON | 10.71.3  | 82.23 |   | Font of first row differs from other rows in Table 10-40a and Table 10-40b | Make consistent |  | **OPEN**Unsure what difference is. |
| 565 | Mark RISON | 10.71.3  | 82.35 |   | "Reserved" in Table 10-40b is confusing because these bits will not necessarily be 0 | As it says in the comment | **Rev** | **Revised****Discussion**: Agree in principle.**Change**: Replace “Reserved” with "Not used" in Table 10-40b, Table 10-40c and Table 10-40f |
| 568 | Mark RISON | 10.71.3  | 83.10 |   | There are lots of 10-40 tables, but only 10-40b has an explanatino of its use | Explain how each of the other tables is used too | **Rev** | **Revised****Discussion**: Agree in principle.Most 10-40 tables do not need additional explanation because the bits extracted from EDP CPE FA Block are used directly as the offset values.Table10-40b has additional explanation because the MAC address is not just the bits extracted from the EDP CPE FA Block – the Local/Global bit and Individual/Group bit need to be set correctly.It makes more sends to append this text with the item currently at p81 line 52 starting “EDP\_STA\_address values shall be extracted from…”- noting that this text is moved elsewhere by CID #816.**Changes**:**p81 lines 51-53** (Prior to moving the bullet list to p82, line 22) replace this bullet with“— The EDP\_STA\_address value for a given link ID shall be the MAC address defined as follows: (#354)—The Local/Global bit shall be set to value 0, local address. —The Individual/Group bit is set to value 0, individual address. —The remaining 46 bits are extracted according to Table 10-40b (Extracting EDP\_STA\_address values from EDP FA Block)., (#573, #1070)Note: This change incorporates changes for the following CIDs: #354, #573, #1070**p83 line 10 - line 18**: Delete this text. |
| 354 | Carol Ansley | 10.71.3  | 83.10 |   | Change "the" to "a" | Change to "the EDP\_STA\_address for a given Link ID shall be a MAC address..." | **Acc** | **Accept**Note: This text is moved elsewhere by CID #568 |
| 566 | Mark RISON | 10.71.3  | 83.10 |   | "Link ID" should be "link ID" | As it says in the comment | **Rev** | **Revised**In addition to the identified change, “Link ID” is changed to “link ID” 15 times in Table 10-40b.Instruction to the editor: apply changes referenced with tag: #566 |
| 567 | Mark RISON | 10.71.3  | 83.16 |   | "-- The remaining 46 bits are extracted from EDP FA block according to Table 10-40b (ExtractingEDP\_STA\_address values from EDP FA Block)." -- I can imagine no end of interop issues due to endianness etc. interpretations | Be much clearer on the endianness and bit order, and give an example |  | **OPEN** Still thinking about how to resolve this. I am open to suggestions! |
| 317 | Michael Grigat | 10.71.3  | 83.57 |   | End value not correct "1104:1151" in Table 10-40d | Change to "1104:1152" | **Rev** | **Revised****Discussion**: The text “1104:1151” in p83 line 57 is correct.The text “1153:1199” in p83 line 59 is incorrect.**Changes**:**p83 line 59**: Replace “1153:1199” with “1152:1199”  |
| 318 | Michael Grigat | 10.71.3  | 84.38 |   | Start value "35:45" in Table 10-40f is same as end value in left column "34:35" | Change value range to "36:45" | **Acc** | **Accept** |

**Proposed spec text:**

***TGbi editor: Apply the following changes to the text to clause 10.71.3 (Establishing frame anonymization parameter sets), starting at p81, line 45***

* (#816) (#816)
* (#816)
* (#816)
* (#816)
* (#816)
* (#816)

For a given EDP epoch, the non-AP MLD and the AP MLD shall generate an CPEblock as: (#95, #573, #1070)

CPE MHAblock =*KDF*-*Hash*-*Length*( KDK, "EDP CPE MHA block", n) (#573, #1070)

where

CPE MHA block is the block of bits that is partitioned into the sets of all possible values for each CPE MHA parameter (#223[25/1100], #570, #573, #1070)

KDF-*Hash*-*Length* is the key derivation function as defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-190 (AKM suite selectors))

KDK is the Key Derivation Key

n is the current number of the EDP epoch in the EDP epoch sequence as defined in 10.71.2.4 (EDP Epoch Start Time Computation)

*Length* is the total number of bits to derive. A total of 1728 bits are derived for a CPE MHA block. (#573, #1070)

The non-AP MLD and the AP MLD shall extract the CPE MHA parameters from CPE MHA block as follows: (#95, #573, #816, #1070)

* (#573, #816, #1070)
* The for a given link ID shall be the MAC address defined as follows: (#354,#568, #816)
* The Local/Global bit shall be set to value 0, local address. (#568)
* The Individual/Group bit is set to value 0, individual address. (#568)
* The remaining 46 bits are extracted according to Table 10-40b (Extracting EDP\_STA\_address values from EDP FA Block). (#568, #573, #1070)
* (#573, #816, #1070)
* (#573, #816, #1070))
* (#573, #816, #1070)
* (#573, #816, #1070)
* Extracting EDP\_PN\_offset values from the CPE MHA block

(#562, #573, #1070)

|  |  |
| --- | --- |
| 48-bit sub-block of the CPE MHAblock (#562,#573, #1070) | Value |
| 0:47 | EDP\_PN\_offset for frames transmitted by non-AP MLD |
| 48:95 | EDP\_PN\_offset for frames transmitted by AP MLD |

* Extracting EDP\_STA\_address values from the CPE MHA block

(#562, #573, #1070)

|  |  |  |
| --- | --- | --- |
| 48-bit sub-block of the CPE MHA) block (#562,#573, #1070) | Sub-block Bits [0:45] | Sub-block Bits [46:47] |
| 96:143 | EDP\_STA\_address [0:45] for link ID(#566) 0  | Not used(#565) |
| 144:191 | EDP\_STA\_address [0:45] for link ID(#566) 1 | Not used(#565) |
| 192:239 | EDP\_STA\_address [0:45] for link ID(#566) 2 | Not used(#565) |
| 240:287 | EDP\_STA\_address [0:45] for link ID(#566) 3 | Not used(#565) |
| 288:335 | EDP\_STA\_address [0:45] for link ID(#566) 4 | Not used(#565) |
| 336:383 | EDP\_STA\_address [0:45] for link ID(#566) 5 | Not used(#565) |
| 384:431 | EDP\_STA\_address [0:45] for link ID (#566) 6 | Not used(#565) |
| 432:479 | EDP\_STA\_address [0:45] for link ID(#566) 7 | Not used(#565) |
| 480:527 | EDP\_STA\_address [0:45] for link ID(#566) 8 | Not used(#565) |
| 528:575 | EDP\_STA\_address [0:45] for link ID(#566) 9 | Not used(#565) |
| 576:623 | EDP\_STA\_address [0:45] for link ID(#566) 10 | Not used(#565) |
| 624:671 | EDP\_STA\_address [0:45] for link ID(#566) 11 | Not used(#565) |
| 672:719 | EDP\_STA\_address [0:45] for link ID(#566) 12 | Not used(#565) |
| 720:767 | EDP\_STA\_address [0:45] for link ID(#566) 13 | Not used(#565) |
| 768:815 | EDP\_STA\_address [0:45] for link IDv 14 | Not used(#565) |

 (#568) (#568) (#568) (#568)

* Extracting EDP\_SN\_offset values for SNS1 and SNS 10 from the CPE MHA block

(#562, #573, #1070)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 48-bit sub-block of the CPE MHAblock (#562,#573, #1070) | Sub-block Bits [0:11] | Sub-block Bits [12:23] | Sub-block Bits [24:35] | Sub-block Bits [36:47] |
| 816:863 | EDP\_SN\_offset value(#TBD) for SNS1 in frames transmitted by non-AP MLD | Not used(#565) | EDP\_SN\_offset value(#TBD) for SNS10 in frames transmitted by non-AP MLD | EDP\_SN\_offset value(#TBD) for SNS10 in frames transmitted by AP MLD |

* Extracting EDP\_SN\_offset values for SNS3 from the CPE MHA block

(#562, #573, #1070)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 48-bit sub-block of the CPE MHAblock (#562,#573, #1070) | Sub-block Bits [0:11] | Sub-block Bits [12:23] | Sub-block Bits [24:35] | Sub-block Bits [36:47] |
| EDP\_SN\_offset values for SNS3 for frames transmitted by the non-AP MLD |
| 864:911 | Value for TID 0 | Value for TID 1 | Value for TID 2 | Value for TID3 |
| 912:959 | Value for TID 4 | Value for TID 5 | Value for TID 6 | Value for TID 7 |
| 960:1007 | Value for TID 8 | Value for TID 9 | Value for TID 10 | Value for TID 11 |
| 1008:1055 | Value for TID 12 | Value for TID 13 | Value for TID 14 | Value for TID 15 |
| EDP\_SN\_offset values for SNS3 for frames transmitted by the AP MLD |
| 1056:1103 | Value for TID 0 | Value for TID 1 | Value for TID 2 | Value for TID3 |
| 1104:1151 | Value for TID 4 | Value for TID 5 | Value for TID 6 | Value for TID 7 |
| 1152:1199 (#317) | Value for TID 8 | Value for TID 9 | Value for TID 10 | Value for TID 11 |
| 1200:1247 | Value for TID 12 | Value for TID 13 | Value for TID 14 | Value for TID 15 |

* Extracting EDP\_SN\_offset values for SNS9 from the CPE MHA block

(#562, #573, #1070)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 48-bit sub-block of the CPE MHAblock (#562,#573, #1070) | Sub-block Bits [0:11] | Sub-block Bits [12:23] | Sub-block Bits [24:35] | Sub-block Bits [36:47] |
| EDP\_SN\_offset values for SNS9 for frames transmitted by the non-AP MLD |
| 1248:1295 | Value for TID 0 | Value for TID 1 | Value for TID 2 | Value for TID3 |
| 1296:1343 | Value for TID 4 | Value for TID 5 | Value for TID 6 | Value for TID 7 |
| 1344:1391 | Value for TID 8 | Value for TID 9 | Value for TID 10 | Value for TID 11 |
| 1392:1439 | Value for TID 12 | Value for TID 13 | Value for TID 14 | Value for TID 15 |
| EDP\_SN\_offset values for SNS9 for frames transmitted by the AP MLD |
| 1440:1487 | Value for TID 0 | Value for TID 1 | Value for TID 2 | Value for TID3 |
| 1488:1535 | Value for TID 4 | Value for TID 5 | Value for TID 6 | Value for TID 7 |
| 1536:1583 | Value for TID 8 | Value for TID 9 | Value for TID 10 | Value for TID 11 |
| 1584:1631 | Value for TID 12 | Value for TID 13 | Value for TID 14 | Value for TID 15 |

* Extracting EDP\_SN\_offset values for SNS12 from the CPE MHA block

(#562, #573, #1070)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 48-bit sub-block of the CPE MHAblock (#562,#573, #1070) | Sub-block Bits [0:11] | Sub-block Bits [12:23] | Sub-block Bits [24:35] | Sub-block Bits [36:47] |
| 0:9 | 10:11 | 12:21 | 22:23 | 24:33 | 34:35 | 36:45 (#318) | 46:47 |
| EDP\_SN\_offset values for SNS12 for frames transmitted by the non-AP MLD |  |
| 1632:1679 | Value for ACI 0 | Not used(#565) | Value for ACI 1 | Not used(#565) | Value for ACI 2 | Not used(#565) | Value for ACI 3 | Not used(#565) |
| EDP\_SN\_offset values for SNS12 for frames transmitted by the AP MLD |  |
| 1680:1727 | Value for ACI 0 | Not used(#565) | Value for ACI 1 | Not used(#565) | Value for ACI 2 | Not used(#565) | Value for ACI 3 | Not used(#565) |