IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| D1.0 CIDs in clauses 10.71.3 | | | | |
| Date: 2025-07-28 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |

Abstract

This submission proposes resolution of comments received against the following sections of TGbi Draft 1.0 (see [1]):

* 10.71.3 (Establishing frame anonymization parameter sets),

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

Resolved CIDs (15): 95, 317, 318, 354, 562, 563, 564, 565, 566, 568, 570, 573, 816, 1069, 1070

Revisions:

* Rev 00: Initial version of the document.
* Rev 01: Applied CID #354 correctly. (a different contribution was mistakenly uploaded for this version)
* Rev 02: Identical to Rev 01.
* Rev 03:
  + Updates from 2025-07-09 ad hoc session,
  + CID #562, #565, #566, #568, #573 are also valid for 10.71.4. Applied corresponding changes to 10.71.4, with the intent of keeping 10.71.3 and 10.71.4 aligned.
  + Update to Length definition added by CID #575 in 25/1107r1.

**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
* Alignment of 10.71.3 and 10.71.4.

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

| **CID** | **Commenter** | **Clause** | **Page. Line** | **Comment** | **Proposed Change** | **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. | **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 into the set of EDP CPE frame anonymization parameters as follows:" which is followed by the existing bullet list and subsequent tables. | **Revised**  **Discussion:** Agreed in principle.  **Changes**: Instructions to Editor: Apply the changes in this document identified by tag: “#816” |
| 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..." | **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.  **Changes:** Instructions to Editor: Apply the changes in this document identified by tag: “#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 | **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, replace “EDP FA block” with “CPE\_MHA\_block” (in 10.71.3) or “BPE\_MHA\_block” (in 10.71.4).  **Changes**: Instructions to Editor: Apply the changes in this document identified by tag: “#1070” |
| 562 | Mark RISON | 10.71.3 | 81.48 | "from EDP FA block" missing article (multiple instances) | As it says in the comment | **Revised** **Discussion:** Agree in principle.  **Changes**: Instructions to Editor: Apply the changes in this document identified by tag: “#562” |
| 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 | **Revised**  **Discussion:** Agree in principle. Replace “EDP FA block” with “CPE\_MHA\_block” (in 10.71.3). Replace “EDP FA block” and “EDP\_BPE\_FA\_block” with “BPE\_MHA\_block” (in 10.71.4).  **Changes**: Instructions to Editor: Apply the changes in this document identified by tag: “#573” |
| 570 | Mark RISON | 10.71.3 | 82.09 | "which is partitioned" should be "that is partitioned" (American English) | As it says in the comment | **Accepted** |
| 563 | Mark RISON | 10.71.3 | 82.19 | "a EDP" should be "an EDP" | As it says in the comment | **Revised**  **Discussion:** Agree in principle. However, the text is updated by CID #1070 from “EDP” to “CPE”, and “a CPE” is correct.  **Changes:**:None |
| 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 | **Revised**  Editor to fix font in Table 10-40a and Table 10-40b |
| 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 | **Revised** **Discussion**: Agree in principle. Replace all occurences of “Reserved” in tables in 10.71.3 and 10.71.4 with "Not used"  **Change**: Instructions to Editor: Apply the changes in this document identified by tag: “#565” |
| 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 | **Revised** **Discussion**: Agree in principle. Update corresponding text in 10.71.4 to align with the new text in 10.71.3.  **Change**: Instructions to Editor: Apply the changes in this document identified by tag: “#568” |
| 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..." | **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 | **Revised**  **Discussion**: In addition to the identified change, “Link ID” is changed to “link ID” 15 times in Table 10-40b and 15 times in corresponding Table 10-40h of 10.71.4.  **Changes**: Instruction to the editor: apply changes referenced with tag: #566 |
| 317 | Michael Grigat | 10.71.3 | 83.57 | End value not correct "1104:1151" in Table 10-40d | Change to "1104:1152" | **Revised**  **Discussion**:  The text “1104:1151” in p83 line 57 is correct.  The text “1153:1199” in p83 line 59 is incorrect.  **Changes**:Instruction to the editor: apply changes referenced with tag: #318 |
| 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" | **Accept** |
| 575 | Mark RISON | 10.71.4 | 85.02 | Length is undefined | Define it (as for CPE) | **Accepted** |

**Proposed spec changes:**

***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 each EDP epoch of the EDP group to which a non-AP MLD is assigned, the non-AP MLD and the AP MLD shall generate a CPE\_MHA\_block as: (#95, #573, #1070)

CPE\_MHA\_block =*KDF*-*Hash*-*Length*( KDK, "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 (#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 shown in the following tables: (#95, #573, #816, #1070)

* Table 10-40a (Extracting EDP\_PN\_offset values from EDP FA Block). (#816)
* Table 10-40b (Extracting EDP\_STA\_address values from EDP FA Block). (#816)
* Table 10-40c (Extracting EDP\_SN\_offset values for SNS1 and SNS 10 from EDP FA Block). (#816)
* Table 10-40d (Extracting EDP\_SN\_offset values for SNS3 from EDP FA Block). (#816)
* Table 10-40e (Extracting EDP\_SN\_offset values for SNS9 from EDP FA Block). (#816)
* Table 10-40f (Extracting EDP\_SN\_offset values for SNS12 from EDP FA Block). (#816)
* Extracting EDP\_PN\_offset values from the CPE\_MHA\_block

(#562, #573, #1070)

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

NOTE—Only 46 bits of each EDP\_STA\_address are extracted from the CPE\_MHA\_block. The generation of the full 48-bit EDP\_STA\_address is defined in 10.71.5.4 (Addressing). (#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\_MHA\_block (#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(#565) for SNS1 in frames transmitted by  non-AP MLD | Not used(#565) | EDP\_SN\_offset value(#565) for SNS10 in frames transmitted by  non-AP MLD | EDP\_SN\_offset value(#565) 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\_MHA\_block (#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\_MHA\_block (#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\_MHA\_block (#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) |

* Establishing BPE frame anonymization parameter sets

All associated BPE non-AP MLDs and the BPE AP MLD shall generate EDP BPE frame anonymization parameters for a given EDP epoch by computing a single pseudorandom EDP BPE FA block which is partitioned into a set of EDP BP frame anonymization parameters according to the following tables.

For a given EDP epoch, the BPE\_MHA\_block shall be generated as: (#573)

BPE\_MHA\_block = KDF-*Hash*-*Length* (PGTK, " BPE\_MHA\_block ", n), (#573)

where

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))

PGTK is the Privacy Group Transient 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 960 bits are derived for a

BPE MHA block. (#575, #573)

The BPE offsets for the Group PN, SNS1 DL, SNS11 DL and Timestamp together with the anonymized BPE AP link addresses are created from the BPE\_MHA\_block. The offsets and the AP link addresses have static assignments within the BPE\_MHA\_block as shown in the Tables below. (#573)

* Extracting EDP\_PN\_offset values from the BPE\_MHA\_block

(#562, #573)

|  |  |
| --- | --- |
| 48-bit sub-block of the BPE\_MHA\_block (#562, #573) | Value |
| 0:47 | EDP\_Group\_PN\_offset |

* Extracting EDP\_AP\_address values from the BPE\_MHA\_block

(#562, #573)

|  |  |  |
| --- | --- | --- |
| 48-bit sub-block of the BPE\_MHA\_block (#562, #573) | Sub-block Bits [0:45] | Sub-block  Bits [46:47] |
| 48:95 | EDP\_AP\_address [0:45] for link ID 0 (#566) | Not used (#565) |
| 96:143 | EDP\_AP\_address [0:45] for link ID 1 (#566) | Not used (#565) |
| 144:191 | EDP\_AP\_address [0:45] for link ID 2 (#566) | Not used (#565) |
| 192:239 | EDP\_AP\_address [0:45] for link ID 3 (#566) | Not used (#565) |
| 240:287 | EDP\_AP\_address [0:45] for link ID 4 (#566) | Not used (#565) |
| 288:335 | EDP\_AP\_address [0:45] for link ID 5 (#566) | Not used (#565) |
| 336:383 | EDP\_AP\_address [0:45] for link ID 6 (#566) | Not used (#565) |
| 384:431 | EDP\_AP\_address [0:45] for link ID 7 (#566) | Not used (#565) |
| 432:479 | EDP\_AP\_address [0:45] for link ID 8 (#566) | Not used (#565) |
| 480:527 | EDP\_AP\_address [0:45] for link ID 9 (#566) | Not used (#565) |
| 528:575 | EDP\_AP\_address [0:45] for link ID 10 (#566) | Not used (#565) |
| 576:623 | EDP\_AP\_address [0:45] for link ID 11 (#566) | Not used (#565) |
| 624:671 | EDP\_AP\_address [0:45] for link ID 12 (#566) | Not used (#565) |
| 672:719 | EDP\_AP\_address [0:45] for link ID 13 (#566) | Not used (#565) |
| 720:767 | EDP\_AP\_address [0:45] for link ID 14 (#566) | Not used (#565) |

(#568)NOTE—Only 46 bits of each EDP\_AP\_address are extracted from the CPE\_MHA\_block. The generation of the full 48-bit EDP\_AP\_address is defined in 10.71.5.4 (Addressing). (#568)

* Extracting EDP\_Group\_Anonymization\_Offset from the BPE\_MHA\_block

(#562, #573)

|  |  |  |
| --- | --- | --- |
| 48-bit sub-block of the BPE\_MHA\_block (#562, #573) | Sub-block Bits [0:45] | Sub-block Bits [46:47] |
| 768:815 | EDP\_Group\_Anonymization\_Offset | Not used (#565) |

* Extracting EDP\_SN\_offset values for SN1 and SNS 11 from the BPE\_MHA\_block

(#562, #573)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 48-bit sub-block of the BPE\_MHA\_block (#562, #573) | 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 SNS1 | | EDP\_SN\_offset values for SNS11 | |
| 816:863 | Not used (#565) | Value for frames transmitted by  AP MLD | Not used (#565) | Value for frames transmitted by  AP MLD |

* Extracting Timestamp Offset from the BPE\_MHA\_block

(#562, #573)

|  |  |  |
| --- | --- | --- |
| 48-bit sub-block of the BPE\_MHA\_block (#562, #573) | Sub-block Bits [0:63] | Sub-block Bits [64:95] |
| 864:959 | Timestamp offset | Not used (#565) |

**References:**

[1] <https://mentor.ieee.org/802.11/dcn/25/11-25-0286-09-00bi-ieee-802-11bi-lb288-comments.xlsx>