IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Editorial Comments Part II | | | | |
| Date: 2025-05-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel Corporation |  |  | po-kai.huang@intel.com |

Abstract

This submission proposes resolutions for multiple comments related to TGbi D1.0 with the following CIDs:

27, 80, 81, 90, 115, 116, 117, 118, 285, 316,

330, 346, 347, 348, 353, 355, 535, 536, 538, 543,

544, 546, 547, 549, 550, 551, 552, 553, 764, 807,

871, 905, 969, 1061, 1064, 1065, 995

378, 381, 395, 722, 723, 724, 726, 728, 898, 899,

900, 901, 992

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision for CID 547. Add 378, 381, 395, 722, 723, 724, 726, 728, 898, 899, 900, 901, 992.
* Rev 2: Add CID 995

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 27 | 9.4.1.83 | 48.50 | "The First Epoch TSF Start Time filed contains", Typo, "filed" should be "field" | At cited location Repace "filed" with "field" | Accepted - |
| 80 | 10.71.2.4 | 79.60 | "...Epoch number Offset..." Capitilize "Number" | At cited location change to "Epoch Number Offset" | Revised –  When refer to Epoch Number Offset field, then all words are captialized. When refers to value, then none of them need to be captailized.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 80 |
| 81 | 10.71.2.4 | 79.59 | "First planned Epoch Start" Capitalize Planned" also incorrect name, it is First Planned Epoch TSF Start Time | At cited location "First Planned Epoch TSF Start" | Revised –  The indicated field is named First Epoch TSF Start Time. We unify the description of the value to be first epoch TSF start time.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 81 |
| 90 | 10.71.2.4 | 80.65 | "new EDP Epoch applies at the end of this TXOP" "apply" not "applies" | At cited location replace "applies" with "apply" | Accepted - |
| 115 | 10.71.2.4 | 79.59 | Inconsistent field name. | Change to: an EDP element including the First Epoch TSF Start Time field based on the TSF of the link, the Epoch Interval field, and the Epoch Number Offset field set to the next epoch number of the EDP epoch sequence of the EDP group assigned to the non-AP STA. | Revised –  The indicated field is named First Epoch TSF Start Time. We unify the description of the value to be first epoch TSF start time.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 81 |
| 116 | 10.71.2.4 | 80.01 | Inconsistent variable name. | Change to: -- Store the first epoch TSF start time, the epoch interval, and set its epoch number for this epoch to the value of the received Epoch Number Offset field for that link. -- Constructs the corresponding the first epoch TSF start time of its other links according to the formula: | Revised –  The indicated field is named First Epoch TSF Start Time. We unify the description of the value to be first epoch TSF start time.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 81 |
| 117 | 10.71.2.3 | 79.27 | "Group Enhanced Privacy element" is not defined, assume it should be "EDP element". | Change to: EDP element | Accepted - |
| 118 | 10.71.2.3 | 79.27 | "EDP epoch setting action response frame" is not defined, assume it should be "EDP Epoch Response frame" | Change to: EDP Epoch Response frame | Accepted - |
| 285 | 10.71.2.4 | 79.60 | Epoch number Offset --> Epoch Number Offset | As in comment | Revised –  When refer to Epoch Number Offset field, then all words are captialized. When refers to value, then none of them need to be captailized.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 80 |
| 316 | 10.71.2.4 | 79.59 | non-consistent usage of Upper/lower character "First planned Epoch Start time" | check consistent writing in the following text (lines 1,4,49 on page 80) | Revised –  The indicated field is named First Epoch TSF Start Time. We unify the description of the value to be first epoch TSF start time.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 81 |
| 330 | 10.71.2.4 | 80.04 | grammar problem - "STA shall: Constructs" | Change to "Construct" | Accepted - |
| 346 | 10.71.2.4 | 80.04 | Wrong verb tense - "STA shall constructs" | Change to Construct | Accepted - |
| 347 | 10.71.2.4 | 80.65 | Wrong verb tense - "parameters applies" | Change to "apply" | Accepted - |
| 348 | 10.71.2.4 | 80.31 | Parameter n should be in italics | several uses on this page, all should be italicized | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 348 |
| 353 | 10.71.3 | 82.16 | Parameter n should be in italics | several uses on this page, all should be italicized | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 348 |
| 355 | 10.71.2.4 | 85.10 | Parameter n should be in italics | Used on this page and previous one, all should be italicized | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 348 |
| 535 | 10.71.2.3 | 0.00 | " EDP Epoch" should be " EDP epoch" since not name of field etc. | Fix at line 8 and 10 and 36, 37, 40 | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 535 |
| 536 | 10.71.2.3 | 78.11 | ", shall" spurious comma | Delete comma | Accepted - |
| 538 | 10.71.2.3 | 79.26 | "EDP epoch setting action response frame" -- use the actual name of the frame | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 118 |
| 543 | 10.71.2.4 | 79.58 | "including the First planned Epoch Start time based on the TSF of the link, the epoch interval, and the Epoch number Offset " is full of case horror. Ditto next page "First planned epoch start time, the epoch interval, and set its epoch number for this Epoch to the value of the received Epoch number offset for that link." and "First planned epoch start time of its other links " and "= First epoch TSF start time of the receiving link + TSF Offset " | Lowercase everything except "TSF" | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 80 and 81 |
| 544 | 10.71.2.4 | 80.23 | Use minuses not hyphens for maths | As it says in the comment | Accepted - |
| 546 | 10.71.2.4 | 80.36 | "Epoch number Offset field of EDP Epoch Settings Field" -- case and article horror | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 546 |
| 547 | 10.71.2.4 | 80.47 | "Length is the number of bits to derive. 16-bits are derived for IT" -- weird hyphen. Anyway if it's fixed there's no need to waffle. Also at 82.18 | Change to "Length is 16" | Revised –  We simply do editorial change to fix the hyphen.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 547 |
| 549 | 10.71.2.4 | 80.54 | "Time Range field, of " spurious comma | As it says in the comment | Revised –  Delete the comma.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 549 |
| 550 | 10.71.2.4 | 80.57 | "PGTK (for Privacy GTK) " -- parenthesis unclear | Delete the parenthesis | Revised –  Delete “(PGTK)”  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 550 |
| 551 | 10.71.2.4 | 80.65 | "EDP Epoch applies" case and grammar horror | Change to "EDP epoch apply" | Accepted - |
| 552 | 10.71.2.3 | 78.06 | "EDP epoch transitions operations" should be "EDP epoch transition operations" | As it says in the comment | Accepted - |
| 553 | 10.71.2.3 | 79.57 | "or an (Re)Association Request frame" should be "or a (Re)Association Request frame" | As it says in the comment | Accepted - |
| 764 | 10.71.2.4 | 80.31 | There are some sentences without a period at their end in lines 31-60. | Please put commas under a unified rule. | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 764 |
| 807 | 10.71.2.4 | 80.04 | The word "Constructs" should be "Construct" | Change to "Construct" | Accepted - |
| 871 | 10.71.2.3 | 79.28 | Please replace "Epoch Interval Duration field" with "Epoch interval field" | As in comment | Revised –  Agree in principle with the commenter. Add instructions to do global change.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 871 |
| 905 | 10.71.2.4 | 79.60 | Epoch number Offset --> Epoch Number Offset | As in comment | Revised –  When refer to Epoch Number Offset field, then all words are captialized. When refers to value, then none of them need to be captailized.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 80 |
| 969 | 10.71.2.3 | 78.12 | Spurious comma before "shall". | Remove the comma. | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 536 |
| 1061 | 10.71.2.4 | 80.52 | I think "First Epoch TSF Start Time" should be "First Planned Epoch TSF Start Time" | Replace "First Epoch TSF Start Time" with "First Planned Epoch TSF Start Time" | Revised –  The indicated field is named First Epoch TSF Start time. We unify the name to be first epoch TSF start time.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 81 |
| 1064 | 10.71.2.4 | 80.57 | "(for Privacy GTK)" is unnecessary | Delete Identified text. | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 550 |
| 1065 | 10.71.2.4 | 80.65 | I believe "this TXOP" is ambiguous | reaplce identified text with "that TXOP" | Accepted - |
| 995 | 9.4.1.83 | 47.9 | In 10.71.2.4, this "First Epoch TSF Start Time" is called "First Planned Epoch TSF Start Time". Inconsistent terminology. | Update "First Epoch TSF Start Time" to "First Planned Epoch TSF Start Time" here, elsewhere in this clause, and in 10.71.2.4 | Revised –  The indicated field is currently First Epoch TSF Start time. The word “planned” is not necessary, so the proposed resolution keeps the shorter field name. We unify the description to be first epoch TSF start time.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 81 |
| 378 | 4.2.5 | 23.46 | "PASN and EDPKE authentication allows" should be "PASN and EDPKE authentication allow" | As it says in the comment | Revised –  Agree in principle with the commenter.  This is already fixed in D1.1. |
| 381 | 4.2.5 | 24.07 | "PASN authentication or EDPKE authentication are" should either be "PASN authentication or EDPKE authentication is" or "PASN authentication and EDPKE authentication are" | Change "are" back to "is", since next sentence uses "it" not "they" | Revised –  Agree in principle with the commenter.  D1.1 use “PASN authentication or EDPKE authentication is” |
| 395 |  |  | EDKPE should be EDPKE (4x) | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 395 |
| 722 | 12.16.9.3.1 | 133.25 | "AP(for" missing space | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 722 |
| 723 | 12.16.9.3.1 | 133.25 | "between EDPKE capable non-AP MLD" missing article | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 723 |
| 724 | 12.16.9.3.1 | 133.45 | "-- EDPKE AKMP is used instead of PASN AKMP." missing articles | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 724 |
| 726 | 12.16.9.3.1 | 133.62 | "MIC Computation" should be "MIC computation" | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 726 |
| 728 | 12.16.9.3.2 | 133.52 | "For MLO, the first Authentication frame can be sent on any of the non-AP STA affiliated with the non-AP  MLD" -- frames are not sent "on" STAs | Change "on" to "by" | Accepted - |
| 898 | 6.5.5.3.2 | 29.03 | Fix the typo "EDKPE" to "EDPKE". | As in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 395 |
| 899 | 6.5.5.4.2 | 30.03 | Fix the typo "EDKPE" to "EDPKE". | As in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 395 |
| 900 | 6.5.5.5.2 | 31.03 | Fix the typo "EDKPE" to "EDPKE". | As in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 395 |
| 901 | 12.16.9.1 | 133.04 | Fix the typo "EDKPE" to "EDPKE". | As in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in the latest version of 11-25/0891 under all headings that include CID 395 |
| 992 | 3.4 | 22.58 | The term "enhanced data privacy key exchange" is not defined | Add a definition in clause 3.2 | Rejected –  EDPKE is described in 12.16.9.1 General as “Enhanced Data Privacy Key Exchange (EDPKE) is an RSNA authentication protocol that uses the PASN  procedures (see 12.12 (Preassociation security negotiation)) with the following differences:”. It is not necessary to have every feature defined in 3.4 with basically the same description in 12.16.9.1. |

**TGbi Editor: *Modify 9.4.1.84 as follows: (track change on)***

* EDP Epoch Settings field

The EDP Epoch Settings field includes the information regarding the parameters of an epoch.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | EDP Epoch Settings Control | Group ID | Epoch Interval | First Epoch TSF Start Time | Epoch Number Offset | Time Range | Epochs Remaining | Minimum Epoch Pacing Parameters |
| Bits: | 16 | 0 or 8 | 16 | 0 or 64 | 0 or 8 | 0 or 16 | 0 or 16 | 0 or 16 |

|  |  |  |
| --- | --- | --- |
|  | Number Of Participating Affiliated STAs | AID Storage Size |
| Bits: | 0 or 8 or 16 or 24 | 0 or 16 |

* EDP Epoch Settings field format

The EDP Epoch Settings field contains the EDP epoch parameters of an EDP epoch sequence for the non-AP MLD.

The Group ID field signals an identifier of the EDP group. The value 0 indicates the default group. The value 255 is reserved.

The EDP Epoch Settings Control is defined as follows:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Group ID Present | First Epoch TSF Start Time  Present | Time Range  Present | Epochs Remaining  Present | Participating Affiliated STAs Count Present | Participating Affiliated STAs Percentage Present | Minimum Epoch Pacing Parameters  Present | AID Storage Size Present |
| Bits: | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

|  |  |
| --- | --- |
|  | Reserved |
| Bits: | 8 |

* EDP Epoch Settings Control field format

Each of the bits of the EDP Epoch Settings Control field indicate the presence of the corresponding field in the EDP Epoch Settings field when set to 1 and its absence when set to 0.

The Epoch Interval field is defined as follows:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Epoch Interval Unit | Epoch Interval Length | Reserved |
| Bits: | 3 | 11 | 2 |

* Epoch Interval field format

The Epoch Interval Length field contains the length of the EDP epoch, expressed in Epoch Interval Units, shown in Table 9-129s (Epoch Interval Units and epoch durations). Epoch Interval Length value 0 is reserved.

|  |  |  |
| --- | --- | --- |
| Epoch Interval Unit field value | Epoch Interval Unit | Max Epoch Duration (approx.) |
| 0 | 1000 s | 23 d 16 h 36 min 40 s |
| 1 | 1 s | 34 min 7 s |
| 2-7 | Reserved | N/A |

* Epoch Interval Units and epoch durations

The First Epoch TSF Start Time field(#27) contains the first epoch TSF start time, which is(#81) value of the TSF timer of the receiving link at the start time of the first EDP epoch of the sequence (EDP epoch number = epoch number offset(#80)).

The Epoch Number Offset(#80) field value contains the epoch number offset(#80) between the AP epoch number and the non-AP STA epoch number (see 10.71.2.4 (EDP Epoch Start Time Computation)).

The Minimum Epoch Pacing field signals the minimum epoch duration value that the non-AP MLD can support. The format of the Minimum Epoch Pacing element is the same as the Epoch Interval field.

The Time Range field contains the range of values, expressed in Epoch Interval Units as defined in Table 9-129s (Epoch Interval Units and epoch durations), used by the AP and each non-AP stations member of the EDP group to determine a random delay added to the EDP epoch planned start time (PlannedTSFStartTime) as defined in 10.71.2.4 (EDP Epoch Start Time Computation).

The Epochs Remaining field indicates the number of EDP epochs(#535) left in the sequence after the current epoch finishes, except 255, which means that the sequence duration is unlimited.

The Number of Participating Affiliated STAs field is optional. When present, the field signals an indication of the number of affiliated STAs currently participating to this group EDP epoch on the current link.

|  |  |  |
| --- | --- | --- |
|  | Participating Affiliated STAs Count | Participating Affiliated STAs Percentage |
| Octets: | 2 | 1 |

* Number of Participating Affiliated STAs field format

The Participating Affiliated STAs Count field represents an indication of the number of affiliated STAs participating in the signaled group on the link. The Participating Affiliated STAs Percentage field, with values in the range of 0 to 100, represents an indication of the percentage of the associated affiliated STAs participating to the signalled group on the link. Values 101-255 are reserved.

When transmitted by a CPE AP, the AID Storage Size field indicates the minimum number of AID values required by a CPE non-AP MLD to be allowed to join in the EDP group.

When transmitted by a CPE non-AP MLD, the AID Storage Size field indicates the number of AID values that the non-AP MLD can store.

**TGbi Editor: *Modify 10.71.2.3 as follows: (track change on)***

* EDP epoch transition(#552) operations

Each EDP epoch(#535) starts with a transition period.

During the transition period of an EDP epoch(#535), the EDP parameters assigned to a non-AP MLD during the preceding EDP epoch(#536) shall remain valid only for the following operations:

* Retransmission of a frame.
* Reception of a retransmitted frame.
* Frame acknowledgement.

A transition period terminates at the end of a transition timeout interval or before the end of the transition timeout interval, after the completion of the successful transmissions or retransmissions initiated during the preceding EDP epoch, whichever comes first.



* Example of EDP epoch(#535) timeline

Figure 10-166a (Example of EDP Epoch timeline) shows an example EDP epoch sequence of consecutive EDP epochs with their associated EDP epoch start times tn and transition period tpn.

An overview of the group EDP epoch is shown in Figure 10-166b (Overview of group EDP epoch).



* Overview of group EDP epoch

The next epoch boundary is derived (as described in 10.71.2.4 (EDP Epoch Start Time Computation)) from the value of the first epoch TSF start time defined in the EDP Epoch Settings field of the EDP(#117) element of the (Re)Association Response frame or the EDP Epoch Response(#118) frame. The Epoch Interval (#871) field of the same fields and frames defines the interval of the following Group EDP epochs sequence.

A CPE non-AP MLD belonging to an EDP group and the CPE AP MLD may calculate the new OTA values to be used for the non-AP MLD in the next group EDP epoch.

At the start of the new group EDP epoch, the new anonymization parameters are used to anonymize the selected OTA fields of all new individual frames transmitted during the epoch.

To account for clock drifts, the CPE non-AP MLD and CPE AP MLD shall begin to accept individually addressed frames that use the new anonymization parameters for a dot11EDPEpochStartTimeMargin before the start of the new epoch. The CPE non-AP MLD and CPE AP MLD shall accept individually addressed frames with the old anonymization parameters for dot11EDPEpochTransitionTime after the start of the new epoch. The rules of 10.71.2.1 (General) apply for frame retransmissions and acknowledgments.

**TGbi Editor: *change variable n in 10.71.2.4 to italic (#348)***

**TGbi Editor: *change “Epoch Interval Duration field” to “Epoch Interval field” (#871)***

**TGbi Editor: *Modify 10.71.2.4 as follows: (track change on)***

* EDP Epoch Start Time Computation

To avoid an easy determination of the epoch start time by an eavesdropper in a link, the start time of each EDP epoch in a link is determined by introducing a pseudo random variation around a planned start time occurring at a regular interval.

Upon reception on a link of an EDP Epoch Request frame or a(#553) (Re)Association Request frame, the AP may send in response to the requesting non-AP STA, an EDP element including the first epoch TSF start(#81) time based on the TSF of the link, the epoch interval, and the Epoch Number Offset field(#80) set to the next epoch number of the EDP epoch sequence of the EDP group assigned to the non-AP STA.

Upon reception of an EDP Epoch Response frame, or of a (Re)Association Response frame containing an EDP element on a link, the non-AP STA of a non-AP MLD shall:

* Store the first epoch TSF start time(#81), the epoch interval, and set its epoch number for this epoch(#80) to the value of the received epoch number offset(#80) for that link.
* Construct(#330) the corresponding first epoch TSF(#81) start time of its other links according to the formula:

First (#81)epoch TSF start time of another link= First epoch TSF start time of the receiving link + TSF Offset value between the other link and the receiving link

NOTE 1—the TSF Offset value is the value received in the latest Basic Multi-Link element exchange.

At any point of time, for a given link, for any EDP epoch number n (n > 0) in an EDP epoch sequence, the link TSF timer value corresponding to the start time of the EDP epoch number n is called EpochTSFStartTime(n) and is computed according to the formula:

EpochTSFStartTime(n) = PlannedTSFStartTime(n) for the link + ΔIT

with

PlannedTSFStartTime(n) = FirstPlannedEpochTSFStartTime + (n - EpochNumberOffset) × EpochInterval

ΔIT = int (KDF-*Hash*-*Length*(PGTK, "ERCM", n)) mod TimeRange

and where

n is a 2 bytes value in little endian order of the current number of

the EDP epoch in the EDP epoch sequence.

PlannedTSFStartTime(n) is the TSF timer value of the link corresponding to the start

time of the EDP epoch number n in the EDP epoch sequence.

EpochNumberOffset is the value indicated in the Epoch Number Offset(#80) field of the(#546) EDP

Epoch Settings Field.(#764)

EpochInterval is the value in TU corresponding to the Epoch Interval

Duration field of the EDP Epoch Settings field.(#764)

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 9-190 (AKM suite selectors)) .(#764)

*Length* is the number of bits to derive. 16(#547)bits are derived for ΔIT. (#547)

FirstPlannedEpochTSFStartTime is the value of the first (#81)epoch TSF start time,

computed upon reception of an EDP element by the STA based

on the First Epoch TSF Start Time value of the EDP element of

the received EDP Epoch Settings Field.(#764)

TimeRange is the value in TU corresponding to the Time Range field(#549) of

the EDP Epoch Settings field.(#764)

PGTK(#550) is the cryptographic key assigned by an EDP AP MLD that is

used to manage the group EDP epoch, distributed to the EDP

non-AP MLDs associated with the EDP AP MLD.(#764)

If the start time of an EDP epoch occurs during an ongoing TXOP, the FA parameters corresponding to the new EDP epoch(#535) apply(#90) at the end of that(#1065) TXOP.

**TGbi Editor: *Modify 6.5 as follows: (track change on)***

* MLME SAP primitives
* Authenticate
* MLME-AUTHENTICATE.confirm
* Semantics of the service primitive

***Modify MLME-AUTHENTICATE.confirm and the table as follows (not all lines shown):***

The primitive parameters are as follows:

MLME-AUTHENTICATE.confirm(

....

Content of 802.1X Authentication frame,

Content of EDPKE Authentication frame,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| ..... | ..... | ..... | ..... |
| AuthenticationType | Enumeration | OPEN\_SYSTEM, SHARED\_KEY FAST\_BSS\_TRANSITION, SAE, FILS\_SHARED KEY\_WITHOUT\_PFS, FILS\_SHARED\_KEY\_WITH\_PFS, FILS\_PUBLIC\_KEY, PASN, 802\_1X, EDPKE | Specifies the type of authentication algorithm that was used during the authentication process. This value matches the AuthenticationType parameter specified in the corresponding MLME-AUTHENTICATE.request primitive. |
| ..... | ..... | ..... | ..... |
| Content of 802.1X Authentication frame | Sequence of elements and fields | As defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames), 12.16.8.2 (IEEE 802.1X),  9.4.1.82 (Encapsulation Length field), 9.4.1.83 (Encapsulation field), 9.4.2.295 (AKM Suite Selector element), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.188 (FILS Nonce element), 9.4.2.312 (Diffie-Hellman Parameter element). | The set of elements and fields to be included in 802.1X Authentication frames. Present if AuthenticationType indicates 802\_1X and dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated is true, otherwise not present. |
| Content of EDPKE(#395) Authentication frame | Sequence of elements and fields | As defined in 12.16.9.3.2 (EDPKE Frame Construction and Processing), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.47 (Timeout Interval element) | The set of elements and fields to be included in EDPKE Authentication frames. Present if AuthenticationType indicates EDPKE and dot11EDPKEActivated is true, otherwise not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.24 (Vendor Specific element) | Zero or more elements. |

* MLME-AUTHENTICATE.indication
* Semantics of the service primitive

***Modify MLME-AUTHENTICATE.indication and the table as follows (not all lines shown):***

The primitive parameters are as follows:

MLME-AUTHENTICATE.indication(

....

Content of 802.1X Authentication frame,

Content of EDPKE Authentication frame,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| ..... | ..... | ..... | ..... |
| AuthenticationType | Enumeration | OPEN\_SYSTEM, SHARED\_KEY, FAST\_BSS\_ TRANSITION, SAE, FILS\_SHARED\_KEY\_WITHOUT\_PFS, FILS\_SHARED\_KEY\_WITH\_PFS, FILS\_PUBLIC\_KEY, PASN, 802\_1X, EDPKE | Specifies the type of authentication algorithm that was used during the authentication process. |
| ..... | ..... | ..... | ..... |
| Content of 802.1X Authentication frame | Sequence of elements and fields | As defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames), 12.16.8.2 (IEEE 802.1X),  9.4.1.82 (Encapsulation Length field), 9.4.1.83 (Encapsulation field), 9.4.2.295 (AKM Suite Selector element), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.188 (FILS Nonce element), 9.4.2.312 (Diffie-Hellman Parameter element). | The set of elements and fields to be included in 802.1X Authentication frames. Present if AuthenticationType indicates 802\_1X and dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated is true, otherwise not present. |
| Content of EDPKE(#395) Authentication frame | Sequence of elements and fields | As defined in 12.16.9.3.2 (EDPKE Frame Construction and Processing), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.47 (Timeout Interval element) | The set of elements and fields to be included in EDPKE Authentication frames. Present if AuthenticationType indicates EDPKE and dot11EDPKEActivated is true, otherwise not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.24 (Vendor Specific element) | Zero or more elements. |

* MLME-AUTHENTICATE.response
* Semantics of the service primitive

***Modify MLME-AUTHENTICATE.response and the table as follows (not all lines shown):***

The primitive parameters are as follows:

MLME-AUTHENTICATE.response(

....

Content of 802.1X Authentication frame,

Content of EDPKE Authentication frame,

VendorSpecificInfo  
)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| ..... | ..... | ..... | ..... |
| Content of 802.1X Authentication frame | Sequence of elements and fields | As defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames), 12.16.8.2 (IEEE 802.1X),  9.4.1.82 (Encapsulation Length field), 9.4.1.83 (Encapsulation field), 9.4.2.295 (AKM Suite Selector element), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.188 (FILS Nonce element), 9.4.2.312 (Diffie-Hellman Parameter element). | The set of elements and fields to be included in 802.1X Authentication frames. Present if AuthenticationType indicates 802\_1X and dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated is true, otherwise not present. |
| Content of EDPKE(#395) Authentication frame | Sequence of elements and fields | As defined in 12.16.9.3.2 (EDPKE Frame Construction and Processing), 9.4.2.23 (RSNE), 9.4.2.240 (RSNXE), 9.4.2.186 (Wrapped Data element), 9.4.2.305 (PASN Parameters element), 9.4.2.47 (Timeout Interval element) | The set of elements and fields to be included in EDPKE Authentication frames. Present if AuthenticationType indicates EDPKE and dot11EDPKEActivated is true, otherwise not present. |
| VendorSpecificInfo | A set of elements | As defined in 9.4.2.24 (Vendor Specific element) | Zero or more elements. |

**TGbi Editor: *Modify 12.16.9 as follows: (track change on)***

* Enhanced Data Privacy Key Exchange
* General

If dot11EDPKEActivated is true, then dot11EDPReAssociationFrameEncryptionSupportActivated and dot11KEKPASNActivated are set to true.

Enhanced Data Privacy Key Exchange (EDPKE) is an RSNA authentication protocol that uses the PASN procedures (see 12.12 (Preassociation security negotiation)) with the following differences:

* SAE AKMP 00-0F-AC:8 or 00-0F-AC:24 can be used as the Base AKMP.
* When there is no Base AKMP, EDPKE(#395) is not used.
* The three Authentication frames have the Authentication Algorithm Number field set to 9 (EDPKE Authentication).
* The generated PTK is used as the initial PTK once associated.
* Discovery of an EDPKE capable AP

An AP indicates it is capable of performing EDPKE authentication by including the EDPKE AKMP as part of the RSNE included in Beacon and Probe Response frames. When the EDPKE AKMP is advertised, the AP shall also include at least one additional AKMP in the RSNE.

* Key establishment with EDPKE authentication
* Overview

This subclause defines the procedures for establishing a PTKSA and the corresponding shared keys between an EDPKE capable STA and an EDPKE(#723) AP (#722)(for non-MLO) as well as between an(#723) EDPKE capable non-AP MLD and an EDPKE capable(#723) AP MLD (for MLO). The same procedures as specified in 12.12.3.1 (Overview) are used with the following differences:

* The three Authentication frames have the Authentication Algorithm Number field set to 9 (EDPKE Authentication).
* The EDPKE AKMP is used instead of the PASN AKMP.(#724)
* The RSNE indicates EDPKE instead of PASN.
* For MLO, the PMKSA association is between the AP MLD and the non-AP MLD.
* EDPKE Frame Construction and Processing

The same procedures as specified in 12.12.3.2 (PASN Frame Construction and Processing) are used with the following differences:

* The three Authentication frames have the Authentication Algorithm Number field set to 9 (EDPKE Authentication).
* EDPKE AKMP is used instead of PASN AKMP.
* The RSNE indicates EDPKE instead of PASN.
* The PTK is generated as specified in 12.16.9.3.4 (PTKSA derivation and MIC Computation with EDPKE authentication).

For MLO, the first Authentication frame can be sent by(#728) any of the non-AP STA affiliated with the non-AP MLD. The RA field of an Authentication frame in response to an Authentication frame from the peer shall be set to the TA field of the Authentication frame from the peer.

* EDPKE authentication with SAE

The same procedures as specified in 12.13.5 (PASN authentication with SAE) are used.

* PTKSA derivation and MIC computation(#726) with EDPKE authentication

The same procedures as specified in 12.13.8 (PTKSA derivation with PASN authentication) are used.

For MLO, the following modifications shall be used:

* The AP MLD MAC address is used instead of the BSSID.
* The non-AP MLD MAC address is used instead of the SPA.

The same procedures as specified in 12.13.9.2 (MIC computation for third PASN frame) are used. For MLO, the following modifications shall be used for HMAC-HASH computation:

* The AP MLD MAC address is used instead of the BSSID.
* The non-AP MLD MAC address is used instead of the SPA.

The Key ID in the PTKSA (see 12.6.1.1.6 (PTKSA)) resulting from EDPKE authentication shall be 0.

NOTE 1—In order to ensure KEK derivation, the KEK In PASN field in the RSNXE from the peer STA is set to 1 (see 12.13.8 (PTKSA derivation with PASN authentication).