IEEE P802.11
Wireless LANs

|  |
| --- |
| Frame Anonymization (FA) and EDP Epoch operation |
| Date: 2023-01-30 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Philip Hawkes | Qualcomm |  |  | phawkes@qti.qualcomm.com |
| Duncan Ho |  |  |  |
| Jouni Malinen |  |  |  |
| George Cherian |  |  |  |
| Stephane Baron | Canon |  |  | Stephane.baron@crf.canon.fr |
| Julien Sevin |  |  |  |
| Patrice Nezou |  |  |  |

Abstract

We propose the draft specification for the following requirements in contribution “11-23-0892-03-00bi-requirements-and-issues-tracking” for TGbi draft D0.1.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Requirement** | **Issue**  | **Status** |
| 7 | 11bi shall define a mechanism for a CPE Client to initiate changing its own OTA MAC Address used with a CPE AP in Associate STA State 4 without any loss of connection. | MAC address change while associated | Discussions underway |
| 9 | Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP to change the transmitted SN and the scrambler seed on downlink and uplink to uncorrelated new values in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated | Discussions underway |
| 10 | Edited to: 11bi shall define a mechanism for a CPE Client and CPE AP to change the transmitted PN on downlink and uplink to uncorrelated new values in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed. | MAC address change while associated | Discussions underway |
| 11 | 11bi shall define a mechanism for a CPE Client and CPE AP to change the CPE Client’s AID to an uncorrelated new value in Associate STA State 4, without any loss of connection when the OTA MAC address of the CPE Client is changed | MAC address change while associated | Discussions underway |

*Notes:*

* *Requirement 13 (11bi shall define or reuse a mechanism for CPE Clients and CPE APs to protect the SA/DA values from exposure OTA to 3rd parties) is expected to use a different mechanism which will be introduced separately.*

Revisions:

* Rev 0: Initial version of the document, formed by merging
	+ “11-23-2098-03-00bi-frame-anonymization-fa-normative-text-for-11bi.docx” (reviewed text and skeleton) and
	+ “11-24-0079-02-00bi-edp-epoch-operation-normative-text-for-11bi.docx” (reviewed text).

Editorial enhancements noted in comments.

* Rev 1: Incorporating offline feedback.

**High level summary of the changes:**

The text addresses EDP epoch operation and CPE features only – leaving open the option of introducing BPE features in the future.

**Key to highlighting:**

* Yellow highlighting: identifies instructions to the TGbi editor.
* Blue highlighting: identifies items that may need addressing in the future.

**Proposed spec text:**

The baseline for this text is 802.11 REVme D4.1.

***TGbi editor: Add new definition to Subclause 3.2 (Definitions specific to IEEE Std 802.11):***

**enhanced data privacy (EDP) epoch:** [EDP epoch] time window in which a set of EDP parameters remain constant.

**Enhanced data privacy (EDP) epoch reference interval**: [EDP epoch reference interval] Fixed reference duration between the start times of two successive EDP epochs in an EDP epoch sequence.

**enhanced data privacy (EDP) epoch parameters:** [EDP epoch parameters] set of parameters characterizing an EDP epoch.

**enhanced data privacy (EDP) parameter**: [EDP epoch parameter] CPE or BPE parameter.

**enhanced data privacy (EDP) epoch sequence**: [EDP epoch sequence]one or more successive EDP epochs characterized by a starting time determined using same EDP Epoch parameters.

**frame anonymization**: [FA] MLO mechanisms mitigating against presence monitoring using unencrypted fields in beacon frames and individually addressed frames.

**frame anonymization parameter set**: [FA parameter set] set of parameters used in frame anonymization mechanisms.

**group enhanced data privacy (EDP) epoch**: [group EDP epoch] time window in which each non-AP MLD of a set of non-AP MLDs applies a set of EDP parameters that is valid for the duration of that group EDP epoch.

**individual enhanced data privacy (EDP) epoch:** [individual EDP epoch] time window in which a single non-AP MLD applies a set of EDP parameters that is valid for the duration of that individual EDP epoch.

**over-the-air sequence number**: [OSN] value transmitted in an individually addressed MPDU header in the place of the sequence number as part of frame anonymization.

**over-the-air packet number**: [OPN] value transmitted in an individually addressed CCMP header or GCMP header in the place of the packet number as part of frame anonymization.

**presence monitoring**: determining the ongoing presence of non-AP MLDs associated to an AP MLD

***TGbi editor: Add new acronyms to Subclause 3.4 (Acronyms and abbreviations)as follows:***

FA frame anonymization

OSN over-the-airsequence number

OPN over-the-airpacket number

***TGbi editor: Add new Subclause 10.y (EDP Epoch operation) under clause 10.x.2 (MAC sublayer functional description) with the heading formats adjusted properly as follows:***

# 10.y EDP Epoch operation

## 10.y.1 Introduction

An EDP Epoch is a time window in which a set of EDP parameters remain constant. EDP Epoch operation is an EDP feature that is valid when MLO is supported.

An EDP Epoch is either an Individual EDP Epoch or a Group EDP Epoch:

* An Individual EDP Epoch sequence request is initiated by a non-AP MLD and the associated AP MLD shall send a response. The EDP Epoch parameters of an individual EDP Epoch are negotiated by a non-AP MLD with its associated AP MLD as defined in subclause 10.y.2.1 individual EDP Epoch negotiation. The non-AP MLD applies the negotiated EDP Epoch parameters, of the Individual EDP Epoch, to determine corresponding EDP Epoch sequence of one or more EDP Epoch start times.
* A Group EDP Epoch sequence is initiated by an AP MLD by advertising the EDP Epoch parameters to a set of non-AP MLDs as defined in subclause 10.y.2.2 Group EDP Epoch advertisement. Each non-AP MLD of the set of non-AP MLDs applies the advertised EDP Epoch parameters of the Group EDP Epoch to determine the same EDP Epoch sequence of one or more EDP Epoch start times.

At any given time, an AP MLD has at most one EDP Epoch assigned to a given associated non-AP MLD.

A non-AP MLD has at most one EDP Epoch.

## 10.y.2 EDP Epoch setup

EDP Epoch may be one-time or periodic and there are two types of EDP Epoch – Group EDP Epoch and Individual EDP Epoch.

### 10.y.2.1 Group EDP Epoch

TBD: This section describes the mechanism, for an AP MLD to provide same EDP Epoch parameter set to one or more of its associated non-AP STA.

### 10.y.2.2 Individual EDP Epoch negotiation

TBD: This section describes the usage of dedicated protected Action frames during an individual EDP Epoch negotiation process, to negotiate the EDP Epoch parameter set between a non-AP MLD and its associated AP MLD.

## 10.y.3 Determination of EDP Epoch parameters value

TBD: EDP Epoch parameters correspond to a set of parameters used to determine the start time of an EDP Epoch based on a fixed EDP Epoch Reference Interval with a limited pseudo random variation.

The process to setup the EDP parameters value is defined in subclause 10.y.2.1 or 10.y.2.2.

***TGbi editor: Add new subclause 10.x (Frame anonymization) under clause 10 (MAC sublayer functional description) as follows:***

# 10.x Frame anonymization

## 10.x.1 Introduction

Some unencrypted fields in beacon frames and individually addressed frames contain values that facilitate *presence monitoring*, determining the continued presence of a non-AP MLD even if the long-term identity of the non-AP MLD cannot be determined. Presence monitoring can be a threat to privacy of the user of the non-AP MLD. User privacy can be improved by shortening the presence-monitoring time-windows. It is possible to limit presence-monitoring time-windows by doing (re)association as defined in 11.3. However, (re)association results in leaving State 4 and introduces a loss in connectivity that could create a negative user experience. <The paragraph is currently focused on presence monitoring of non-AP MLDs only. To accommodate BPE, the paragraph can be updated to cover presence monitoring of AP also.>

Frame anonymization (FA) is an EDP feature available when MLO is supported.

The unencrypted fields that facilitate presence monitoring of a non-AP MLD are:

* AID of associated non-AP MLDs.
* Address 1 (on the downlink) and Address 2 (on the uplink) that contains the MAC address of the affiliated STA of the non-AP MLD on the link on which the frame is transmitted. <To accommodate BPE, the paragraph can be generalized to cover BSSID as well>
* Sequence Number (SN).
* Packet Number (PN).

FA enables restricting presence-monitoring time-windows to portions of a single association (that is, without leaving State 4). These time-windows are the EDP Epochs described in subclause 10.y (EDP Epoch operations). A new *frame anonymization parameter set (FA parameter set)* is established between the AP MLD and non-AP MLD for each new EDP Epoch of the non-AP MLD as described in 10.x.2 (Establishing FA parameter sets). An FA parameter set includes the following:

* *FA AID*: new random value to be used as the non-AP MLD AID. The FA AID is selected by the AP MLD using implementation-specific means.
* *FA STA MAC*: new random values for the affiliated STA MAC address randomization for each set link. <To accommodate BPE, the paragraph can be generalized to cover FA BSSID or similar>
* *FA SN offsets*: new random values for use in SN anonymization are generated for each supported sequence number space of the AP MLD and each supported sequence number space of the non-AP MLD, see Table 10-5 (Transmitter sequence number spaces).
* *FA* *PN offsets*: new random values for use in PN anonymization are generated for the PN assigned by the AP MLD and the PN assigned by the non-AP MLD.

FA provides the following functions:

* **AID randomization:** The FA AID is used directly wherever AID is currently used.
* **Affiliated STA MAC address randomization**. For each link, the FA STA MAC address is used directly in MAC header creation at the transmitter. These addresses are also used in the MAC header processing at the receiver: e.g., in address filtering. <To accommodate BPE, the paragraph can be generalized to cover FA BSSID or similar>
* **SN/PN anonymization**: The transmitter applies the FA SN offset and FA PN offset to the SN and PN values to produce over-the-air values which can be safely transmitted in the clear while maintaining anonymity. The transmitted values appear to do a random “jump” to a new starting value, and then continue incrementing from the new starting value. The intended receiver transforms the over-the-air values back to the original values of SN and PN.

NOTE—The following list clarifies the scope of attacks which FA mitigates:

* FA mitigates against presence monitoring across multiple FA epochs.
* FA does not mitigate against presence monitoring within a single FA epoch.
* FA does not mitigate identifying frames transmitted from a single MLD within a single FA epoch.
* FA does not mitigate using traffic analysis using known transmission behavior of upper layer protocols for presence monitoring across multiple FA epochs.

<Further introductory text on transitioning between EDP epochs might be appropriate here>

## 10.x.2 Establishing frame anonymization parameter sets

1. This subclause describes how an AP MLD and associated non-AP MLD establish the FA parameter set for each EDP epoch for the non-AP MLD.
2. The non-AP MLD and AP MLD establishe the EDP epochs used for frame anonymization as described in 10.y (EDP epoch operation).
3. Details for establishing the FA parameter set for a given EDP epoch are TBD.

## 10.x.3 Frame anonymization and transmitting functions

1. This subclause describes the changes to transmitting functions when frame anonymization is enabled.

**SN/PN anonymization**: Details are TBD.

**Frame header creation**: Details are TBD.

## 10.x.4 Frame anonymization and receiving functions

1. This subclause describes the changes to receiving functions when frame anonymization is enabled.

**Address filtering**: Details are TBD.

**SN/PN de-anonymization**: Details are TBD.

## 10.x.5 Frame anonymization and AID

This subclause describes the changes to the use of AID when frame anonymization is enabled. Details are TBD.

## 10.x.6 Frame anonymization, TXOP and retransmissions

This subclause describes the considerations for TXOP and retransmissions when frame anonymization is enabled. Details are TBD.