IEEE P802.11
Wireless LANs

|  |
| --- |
| D1.0 CIDs on frame anonymization definitions and introductions  |
| Date: 2025-07-02 |
| 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:

* 3.2 (Definitions specific to IEEE 802.11)
* 4.5.4.10a (Enhanced Data Privacy (EDP) enhancements)
* 10.71.1 (Introduction)

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

Resolved CIDs (21): 65, 66, 67, 322, 336, 376, 511, 513, 924, 925, 926, 938, 958, 959, 989, 1025, 1027, 1028, 1029, 1030, 1039

Revisions:

* Rev 00: Initial version of the document. Addressed 10.71.1 (Introduction) only.
* Rev 01: Smaller set of self-contained CIDs but now spread across
	+ 3.2 (Definitions specific to IEEE 802.11)
	+ 4.5.4.10a (Enhanced Data Privacy (EDP) enhancements)
	+ 10.71.1 (Introduction)
* Rev 02:
	+ Removed changes for CID #515 (moved to a separate contribution)
	+ Updated existing text shown for 4.5.4.10a (Enhanced Data Privacy (EDP) enhancements) to D1.2 text.
	+ Added resolution of #958
	+ Added resolution of some related rejected CIDs.
* Rev 03: Added CID #65 to the resolved CID(s) list (I had neglected to add it earlier)..

**Background**

Overview of noteworthy changes

* Improvements to definitions (3.2).:
	+ Removing definition of “presence monitoring”. This is sometimes replaced with “to determine the long-term presence of a person at a location, even if the identity of the person cannot be determined” or a shortened version of this text.
	+ Updates to definition of “frame anonymization”
* Removing motivation for “frame anonymization” from 10.71.1 and adding an improved motivation in 4.5.4.10a.
* Clarifying the objective of frame anonymization in 10.71.1

Note that there the authors have further changes to 4.5.4.10a and 10.71.1 in 25/1100.

| **CID** | **Commenter** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- |
| 924 | Robert Stacey | 3.2 | 21.61 | The first part (about MLO) seems superfluous since it is implied by the type of recipient. Also, it is better to define what it is and then how it is applied, rather than how it is applied and then what it is. | Change to "An EDP mechanism that mitigates against the use of unencrypted fields for presence monitoring in frames sent to or sent by a non-AP MLD." | **Revised**Changes: Replace“A multi-link operation (MLO) enhanced data privacy (EDP) mechanism for frames transmitted by or intended for reception by an associated non-AP multi-link device (MLD), mitigating…”with"An EDP mechanism for multi-link devices (MLDs), that mitigates…”“ |
| 322 | Carol Ansley | 3.2 | 21.63 | "Mitigating against" is poor wording | Remove "against", "mitigating" already means reducing the impact of. | **Accepted** |
| 925 | Robert Stacey | 3.2 | 22.01 | This kind of definition is totally useless since it just repeats the words in the term itself. | Delete the definition for "frame anonymization parameter set" | **Accepted** |
| 376 | Mark RISON | 3.2 | 22.26 | "Determining the ongoing presence of non-access point (non-AP) multi-link devices" -- it is not clear what "ongoing presence" means | Delete "ongoing " | **Rejected****Rationale**: This definition is deleted by CID #926 |
| 926 | Robert Stacey | 3.2 | 22.26 | The definition of "presence monitoring" seems unnecessary. Misleading actually. Essentially, this definition applies a very narrow meaning (MLO-only) to something that should have broader meaning. The term is only used on 10.71 and thus a local definition would suffice.However, even a local definition seems unnecessary; the way the term is used 10.71 is generic enough that it does not need defining. | Delete this definition. If you wish to keep it apply the meaning more narrowly: e.g., "MLO-based presence monitoring" | **Revised****Discussion**: Deleting this term seems appropriate. - It seems inappropriate to define a term for something that is being prevented. “presence monitoring”- Several CIDs relate to confusion over this term and its definition.- "Presence Detection" is related to Wi-Fi Sensing– we should avoid confusion with that feature.-recommend replacing with text along the lines of "a third party determining the long-term presence of a person"**Changes**:**p21 line 64** Replace “against the use of unencrypted fields for presence monitoring”with“the privacy threat posed by values that are (a) assigned to an MLD, (b) remain static or predictable, and (c) transmitted in unencrypted fields and elements”**p22 line 26** Delete definition(Use of “presence monitoring” in 10.71.1 updated by CID #959)  |
| 989 | Philip Hawkes | 3.2 | 22.26 | This definition implies presences monitoring applies only to a non-AP MLD, but presence monitoring of an AP MLD is the rationale for BPE features too, | Replace "non-access point (non-AP) multi-link devices (MLDs) associated to an AP MLD." with "multi-link devices (MLDS)" | **Rejected****Rationale**: This definition is deleted by CID #926 |
| 65 | Graham Smith | 10.71.1 | 75.18 | Frame anonymization has one aim, to counter "presence monitoring". It is not obvious what this is (i.e., how does it work such that a third party finds it useeful) or how effective FA is. The counter is simply to change the STAs parameters every now and then. Was any presentation given on how often the changes are needed in order to be effective, (1 day, 1 hour, 1 minute, 1 second?) or indeed what presence monitoring actually achieves (STAs are using random MACs)? Also, how many associated STAs are required to make FA effective (10, 100, 1000)? FA is a lot of work, and no indication is given as to how it really helps or what the criteria are. To convince me that this is useful, I would need to see an Annex at the least as to how it works and the criteria required for it to work | Either add an Annex or add text to introduction that shows the crtieria (e.g., min or max time slots, and number of assciated STAs) required that prove that FA is useful or delete the whole thing. | **Rejected****Rationale:** FA provides a range of parameters to provide a range of choices implementers and users. Recommendations on those parameters are best left to industry organizations, not 802.11.  |
| 958 | Robert Stacey | 10.71.1 | 75.20 | Historically, we have interpreted "Introduction" to imply "informative". I don't necessarily agree with this, but that is the reason we use "General" and not "Introduction". | Change "Introduction" to "General" (since this subclause clearly has normative requirements). | **Accepted** |
| 938 | Srinivas Kandala | 10.71.1 | 75.26 | Based on the description here I am unable to comprehend how this presence monitoring (likely by some nebulous actor) is accomplished. Can you describe how this threat would develop? I agree that presence monitoring is a threat, but I could not figure out how one can get there. Unless this can be clarified and explained adequately I cannot be sure what problem this amendment is attempting to solve | Please clarify, preferably in clause 4 | **Revised**Discussion: Agreed in principle**Changes:****P24 line 61: (4.5.4.10a)**Insert new text as a new paragraph after “…secured connection.”(see inline text)(This change incorporates resolutions from the following CIDs: #66, #67, #959, #1030)**P75 line 24.** Append the following sentence to the paragraph“The objective of FA is that, for the set of values assigned to an MLD that are transmitted in unencrypted fields and elements, those values remain static or predictable only within configurable time windows called EDP Epochs.“**P75 line 26 to line 51**: Delete paragraphs |
| 959 | Robert Stacey | 10.71.1 | 75.26 | The purpose should be stated upfront and more clearly. Then get into the means. | Change to "Frame anonymization helps minimize presence monitoring. Presence monitoring is the determination by a third party that a person is present at a location over a period of time even if the identity of the person cannot be determined. With frame anonymization unencrypted fields in a frame are periodically changed so that the long term presence of the sender cannot easily be determine." | **Revised****Discussion**: Agreed in principle. Replace “presence monitoring “ with “a third party determining the long-term presence of a person at a location, even if the identity of the person cannot be determined”or a shortened version where appropriate.**Changes****P24 line 61: (4.5.4.10a)**Account for this CID In new text introduced by CID #938.**P76, line 9 to line 17**: Replace note with normal text“The following list clarifies the scope of attacks that FA mitigates:— FA mitigates (#336) third parties determining the presence of a person presence monitoring across multiple FA epochs. — FA does not mitigate (#336) third parties determining the presence of a person 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 (#1039) third parties determining the presence of a person across multiple FA epochs via traffic analysis using known transmission behavior of upper layer protocols.“(This change incorporates changes from the following CIDS: #336, #1039) |
| 1025 | Philip Hawkes | 10.71.1 | 75.26 | FA provides CPE features which apply to group addressed frames, in addition to the frames identified here. | Replace "Beacon frames and individuallyaddressed frames" with "frames" | **Rejected** The identified text is updated by CID #938. The resulting text which no longer refers to frames, so the present CID no longer applies.. |
| 66 | Graham Smith | 10.71.1 | 75.31 | "It is possible to limit presence monitoring..." I think this would be better as a NOTE. Not sure also "by doing (re)association" is correct. Reassociation uses the same MAC address. | At cited location, make the final 2 sentences a NOTE. Also at 75.32 replace "by doing (re) association" with "by performing a new assocation" and at 75.34 delete "(re)"; and at 75.34 replace "could" with "might". | **Revised****Discussion**: Agreed in principle.**Changes**: This CID is addressed as part of the resolution of CID #938 in 4.5.4.10a.  |
| 511 | Mark RISON | 10.71.1 | 75.31 | "It is possible to limit presence moni-toring time windows by doing (re)association as defined in 11.3 (Authentication and association). However, (re)association results in leaving State 4 and introduces a loss in connectivity that could create a negative user experience. " sounds like a NOTE | Prepend "NOTE---" | **Revised****Discussion**: Agreed in principle. Address by moving text to 4.5.4.10a, as proposed by CID #938.**Changes**: This CID is addressed as part of the resolution of CID #938 in 4.5.4.10a.  |
| 1027 | Philip Hawkes | 10.71.1 | 75.32 | "doing" is an imprecise verb for this situation. | Replace "doing" with "performing" | **Rejected** This text has been modified by CID 938. The change is no longer applicable. |
| 1028 | Philip Hawkes | 10.71.1 | 75.32 | There is not a clear indiication of what is "leaving State 4". | Replace "leaving State 4" with "the non-AP MLD leaving State 4". | **Rejected** This text has been deleted as part of by CID 938. The change is no longer applicable. |
| 1029 | Philip Hawkes | 10.71.1 | 75.37 | This list applies to individual addressed frames only | Replace "The encrypted fields and elements..." with "The encrypted fields and elements of individually addressed frames..." | **Rejected****Discussion:** The changes proposed in CID #1030 no longer identifies the type of frame. of unencrypted fields and elements. This comment is no longer valid  |
| 1030 | Philip Hawkes | 10.71.1 | 75.44 | Lines 37-43 identified unencrypted fields and elements that facilitate presence monitoring of a non-AP MLD. Text is needed that identifies unencrypted fields and elements that facilitate presence monitoring of an AP MLD. | Insert the following text at line 44:"The unencrypted fields and elements that facilitate presence monitoring of an AP MLD are:--For all frames: Address 2 (on the downlink) and Address 1 (on the uplink).--For group addressed frames: Address 1 (on the downlink), Sequence Number (SN), Packet Number (PN).--For Beacon frames: Timestamp." | **Revised****Discussion**: It is simpler if this introduction provides an informative list of example unencrypted fields and elements without referring to the type of frame, and without providing the details for processing those fields and elements. Incorporated into resolution of CID #938 in 4.5.4.10a.**Change**(4.5.4.10a.)Include the following text as part of the new text added by CID #938 in 4.5.4.10a.“Examples of values in unencrypted fields and elements that contain static or predictable values assigned to the transmitter or receiver include: transmitter address (TA), receiver address (RA); sequence number (SN); packet number (PN); timestamp; association identifier (AID) and fields and elements derived from the AID.“ |
| 67 | Graham Smith | 10.71.1 | 75.46 | "FA enables restricting presence monitoring time windows..." It does not enable it, it actually does it. Suggest a rewrite of this para. | Replace cited paragraph with "FA defines time windows, known as EDP epochs, during a single association such that the parameters of unencrypted fields and elements are used for restricted time periods. In each EDP epoch, new parameter sets are used. EDP epoch operation is described in 10.71.2. The establishment of the FA new parameter set is described in 10.71.3" | **Revised****Discussion**: Agreed in principle. Addressed as part of the text proposed by CID #938.**Changes**: This CID is addressed as part of the resolution of CID #938 in 4.5.4.10a. |
| 513 | Mark RISON | 10.71.1 | 75.46 | "presence monitoring time windows" should be "presence-monitoring time windows" now that the prohibition on using hyphens has been rescinded | As it says in the comment | **Rejected** This text has been deleted as part of by CID #938. The change is no longer applicable. |
| 336 | Carol Ansley | 10.71.1 | 76.11 | "Mitigating against" is poor wording | Remove "against", "mitigating" already means reducing the impact of. | **Accept** |
| 1039 | Philip Hawkes | 10.71.1 | 76.15 | "mitigate using traffic analysis using" sounds awkward with two occurences of the word "using". | Replace with "mitigate traffic analysis using" | **Accept** |

**Proposed spec text:**

***TGbi editor: Apply the following changes to the following definitions in 3.2 (Definitions specific to IEEE 802.11). The baseline for this text is Draft P802.11bi\_D1.2.***

**frame anonymization:** [FA] An enhanced data privacy (EDP) mechanism for multi-link devices (MLDs), that mitigates the privacy threat posed by values that are (a) assigned to an MLD, (b) remain static or predictable, and (c) transmitted in unencrypted fields and elements. (#322, #924, #926)

 (#925)**…**

 (#926)

***TGbi editor: Apply the following changes to 4.5.4.10a (Enhanced Data Privacy (EDP) enhancements). The baseline for this text is Draft P802.11bi\_D1.2.***

* **Enhanced Data Privacy (EDP) enhancements**

Third parties observing the wireless medium might seek to track device locations and device activity. Using EDP features, a STA or MLD can modify the amount of information disclosed in several ways. Using EDP client privacy enhancements (CPE), a non-AP STA or non-AP MLD can modify the content of messages sent before and during association to reduce the opportunity to fingerprint the non-AP STA or non-AP MLD through its messages outside of a secured connection.(#383, #384)

Additional threats exist even after a secured connection is established. When values are (a) assigned to an 802.11 device, (b) static or predictable and (c) transmitted in unencrypted fields and elements, then those values can be used by a third-party observer to determine the long-term presence of a person at a location, even if the identity of the person cannot be determined. Without appropriate mitigations, the values transmitted in these unencrypted fields and elements remain static or predictable until a new association is performed, even when other EDP features are enabled. (#66, #938, #959)

Examples of values in unencrypted fields and elements that contain static or predictable values assigned to the transmitter or receiver include: transmitter address (TA), receiver address (RA); sequence number (SN); packet number (PN); timestamp; association identifier (AID) and fields and elements derived from the AID. A third-party observer can monitor these values and, as long as the values remain static or predictable, the third-party observer can determine that the corresponding 802.11 device continues to be present at that location. In some cases, the location could be fixed (relative to the ground) while in other cases the location could be in motion, e.g. the device is moving, or the AP is installed in a vehicle and both the AP and the device are moving. (#938, #1030)

Frame anonymization, available when MLO is enabled, improves user privacy by restricting the time windows within which unencrypted fields and elements remain static or predictable, thereby increasing the effort required for a third party to determine the long-term presence of the person. The time windows, called EDP epochs, can be relatively short in duration when compared to the typical lifetime of an association. (#67, #511, #938, #959)

A non-AP MLD supporting CPE frame anonymization can change the MAC address(es) and other fields used in communications by its affiliated STAs during an association. (#881, #304, #771, #297)

***TGbi editor: Apply the following changes to 10.71.1 (Introduction). The baseline for this text is Draft P802.11bi\_D1.2.***

* **General(#958)**

Frame anonymization (FA) is an EDP CPE feature available when MLO is supported and DS MAC address is supported. The objective of FA is to mitigate the privacy threat posed by values that (when FA is disabled) are (a) assigned to an MLD, (b) remain static or predictable, and (c) transmitted in unencrypted fields and elements. FA encrypts some such values, e.g., transmitting MSDU(s) in an A-MSDU to protect SA and DA. FA transforms other values into “over-the-air” values that remain static or predictable only within configurable time windows called EDP Epochs, e.g., using temporary MAC addresses. (#938, #959)

(#938) (#938) (#938)

***TGbi editor: Apply the following changes start p76 line 9. The baseline for this text is Draft P802.11bi\_D1.2.***

The following list clarifies the scope of attacks that FA mitigates: (#959)

* FA mitigates third parties determining the presence of a person across multiple FA epochs. (#336, #959)
* FA does not mitigate third parties determining the presence of a person within a single FA epoch. (#336, #959)
* FA does not mitigate identifying frames transmitted from a single MLD within a single FA epoch.
* FA does not mitigate third parties determining the presence of a person across multiple FA epochs via traffic analysis using known transmission behavior of upper layer protocols . (#959, #1039)