IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 12.16.7 comments |
| Date: 2025-03-25 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission resolves the following CIDs:

178, 919, 967, 917, 269, 270, 687, 918

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the discussion during the meeting
* Rev 2: Revision for CID 967 and 269
* Rev 3: Revision for CID 967 and 269 based on the discussion during the teleconference call. Changes are marked with green.

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 D1.0 Draft. This introduction is not part of the adopted material.

Editing instructions formatted like this are intended to be copied into the TGbi D1.0 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** |
| 178 | 127.15 | 12.16.7 | Good to specify that support of PMKID privacy is uniform across the ESS. This is needed for the FT case anyway. | As in comment | Rejected – We already have the following requirement for FT.“APs in the same mobility domain shall set the PMKSA Caching Privacy Support field in the RSNXE to the same value.” |
| 967 | 127.29 | 12.16.7.1 | It would be good to state how a new PMKID is to be generated instead of just noting that the AP delivers the PMKID to be used next time. Surely the expectation here is that the new PMKID is not something that 3rd parties could use to track the STA. | At P127 L29, replace"the EDP AP shall deliver the PMKID for the identified PMKSA to be used next time"'with"the EDP AP shall generate a random new PMKID for the identified PMKSA and deliver the generated PMKID to be used next time".At P127 L35, replace"the EDP AP MLD shall deliver the PMKID for the identified PMKSA to be used next time"'with"the EDP AP MLD shall generate a random new PMKID for the identified PMKSA and deliver the generated PMKID to be used next time". | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0535 under all headings that include CID 269 |
| 269 | 130.14 | 12.16.7.1 | The PMKID anonymization mechanism shall include input from the non-AP MLD. | Pleasedefine a PMKID anonymization mechanism that uses input from a STA. | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0535 under all headings that include CID 269 |
| 270 | 130.14 | 12.16.7.1 | The AP assigned PMKID can be delivered only in encrypted (Re)Association frame. There are signaling flows that may not transmit protected (re)association frames. | Please defne anonymization mechanism in which the STA may calculate the anonymized PMKID or allow anonymized PMKID delivery in a protected management frame. | Rejected –All the existing flows use PMKID will follow a (re)association frames exchange. |
| 687 | 128.19 | 12.16.7.2 | "The R0KH may then deliver the latest PMKR0Name to other R1KHs with corresponding PMK-R1 SA in the same mobility domain. The R1KH of the target FTR may also retrieve the latest PMKR0Name from the R0KH." -- shouldn't these be "shall"s? | As it says in the comment | Rejected –We provide two alternatives and either one can be used. It is not required to do both. It is also not required to do it right away. R1KH can connect R0KH when receiving the PMKR0Name as well see 13.5.2 Over-the-air FT protocol authentication in an RSN. |
| 919 | 127.13 | 12.16.7 | For MLO, it is not clear how AP identifies real STA link MAC address if the STA link MAC address is randomized only for PMKID/PMKR0Name indicated frame. | Fix the issues. Will follow up with a contribution. | Revised – When STA connects to a new AP, the random STA MAC address is used through the connection until after association with the potential EPOCH mechanism to do further change. However, after checking with the commenter, the question is about to identify the STA in the DS during roaming, which is done using DS MAC address. We revise the note to clarify this point.TGbi editor to make the changes shown in the latest version of 11-25/0535 under all headings that include CID 919 |
| 917 | 127.41 | 12.16.7.1 | For a different PMKID to ensure privacy, non-AP MLD address in Multi-Link IE also needs to be randomized in auth frames. As a result, tracking cannot be done on the non-AP MLD MAC address. | Fix the issues. Will follow up with a contribution. | Revised – It is possible to randomize MLD MAC address per 11be spec. See 12.2.11 Requirements for support of MAC privacy enhancements.However, after checking with the commenter, the question is about to identify the STA/MLD in the DS during roaming, which is done using DS MAC address. TGbi editor to make the changes shown in the latest version of 11-25/0535 under all headings that include CID 919 |
| 918 | 128.11 | 12.16.7.2 | For a different PMKR0Name to ensure privacy, non-AP MLD address in Multi-Link IE also needs to be randomized in auth frames. As a result, tracking cannot be done on the non-AP MLD MAC address. | Fix the issues. Will follow up with a contribution. | Revised –It is possible to randomize MLD MAC address per 11be spec. See 12.2.11 Requirements for support of MAC privacy enhancements.However, after checking with the commenter, the question is about to identify the STA/MLD in the DS during roaming, which is done using DS MAC address. TGbi editor to make the changes shown in the latest version of 11-25/0535 under all headings that include CID 919 |

***Discussion:***

***Proposal:***

**TGbi Editor: *Instruction: Modify 9.4.2.188 as follows***

* ~~FILS~~ Nonce element

The ~~FILS~~ Nonce element is used for exchanging an additional source of randomness in an~~the FILS~~ authentication exchange or an encrypted (Re)Association Request/Response frame exchange(#269). The format of the ~~FILS~~ Nonce element is shown in Figure 9-767 (FILS Nonce element format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | ~~FILS~~ Nonce |
| Octets: | 1 | 1 | 1 | 16 |
| * ~~FILS~~ Nonce element format
 |

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The ~~FILS~~ Nonce field contains randomly generated data.

**TGbi Editor: *Instruction: Modify 12.16.7 as follows***

* PMKSA caching privacy

This subclause defines rules for PMKSA caching privacy such that the identifier related to PMKSA caching can be changed after using the identifier to establish a PTKSA, thus, cannot be used for tracking.

* A STA that sets the PMKSA Caching Privacy Support field in the RSNXE to 1 shall set the (Re)Association Frame Encryption Support field in the RSNXE to 1. PMKID privacy

After the indicated PMKID in an RSNE identifies a cached PMKSA (see 12.6.8.3 (Cached PMKSAs and RSNA key management)), and a PTKSA is established using the identified PMKSA,

* For non-MLO, if the EDP non-AP STA and the EDP AP set the PMKSA Caching Privacy Support field in the RSNXE to 1,
* The EDP non-AP STA shall include the Nonce element in the (Re)Association Request frame. (#269)
* The EDP AP shall include the Nonce element in the (Re)Association Response frame. (#269)
* Both the EDP non-AP STA and the EDP AP shall change the PMKID for the identified PMKSA to be used next time.(#269)
* For MLO, if the EDP non-AP STA(s) affiliated with an EDP non-AP MLD and the EDP AP(s) affiliated with an EDP AP MLD set the PMKSA Caching Privacy Support field in the RSNXE to 1,
* The EDP non-AP MLD shall include the Nonce element in the (Re)Association Request frame. (#269)
* The EDP AP MLD shall include the Nonce element in the (Re)Association Response frame. (#269)
* Both the EDP non-AP MLD and the EDP AP MLD shall change the PMKID for the identified PMKSA to be used next time(#269).(#175)

NOTE 1—For MLO, all STAs affiliated with an MLD set the RSNXE to the same value.

The PMKID shall be changed as:

 PMKID = Truncate-128(Hash(“PMK Name” || PMKIDANonce || PMKIDSNonce))

where:

 Hash is the hash algorithm from the key derivation type (see

 Table 9-190 (AKM suite selectors)) for each AKM

 PMKIDANonce is the Authenticator nonce indicated in the Nonce element in the (Re)Association Response frame used to compute the changed PMKID.

 PMKIDSNonce is the Supplicant nonce indicated in the Nonce element in the (Re)Association Request frame used to compute the changed PMKID.

(#269)

NOTE 2—For a different PMKID indicating in a frame to ensure privacy, the MAC address in the TA and the MLD MAC address (if present) in the Frame Body field need to be randomized to .avoid tracking based on the MAC address. During BSS transition, the DS MAC address can remain the same to preserve the mapping to the DS.(#919)

**TGbi Editor: *Instruction: Modify 9.3.3.5 as follows:***

* Association Request frame format

***Insert new rows to Table 9-64 (Association Request frame body) in numeric order (not all lines shown):***

* revme D7.0 up to 60, 11bh D6.0 up to 61-62, 11be D7.0 63-65, 11bk D5.0 no addition, 11bf D8.0 66-69
* Association Request frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 70 | DS MAC Address | The DS MAC Address element is present if the Association Request frame is encrypted, dot11DSMACAddressActivated is true, and the peer indicates support for DS MAC Address in the RSNXE; otherwise, it is not present.(#160) |
| 71 | EDP | The EDP element is present if the Association Request frame is encrypted and dot11EDPGroupEpochActivated is true; otherwise, it is not present. This element carries the desired parameters of the Epoch to be joined by the sending STA. |
| 72 | Mobility domain | An MDE is present in an Association Request frame ifdot11FastBSSTransitionActivated is true, encryption of the Association Request frame is used, and if the frame is beingsent to an AP that advertised its FT capability in the MDE in itsBeacon or Probe Response frame (i.e., AP also hasdot11FastBSSTransitionActivated equal to true).(#176, #Ed) |
| 73 | Fast BSS Transition | An FTE is present in an Association Request frame ifdot11FastBSSTransitionActivated is true, encryption of the Association Request frame is used, anddot11RSNAAuthenticationSuiteSelected is equal to an AKM suiteselector value for which the Authentication type column indicatesFT authentication. See Table 9-190 (AKM suite selectors) (i.e.,part of a fast BSS transition in an RSN).(#176, #Ed)  |
| 74 | Nonce | The Nonce element is optionally present as defined in 12.16.7.1 (PMKID privacy); otherwise, it is not present. (#269) |

**TGbi Editor: *Instruction: Modify 9.3.3.6 as follows:***

* Association Response frame format

***Change rows in Table 9-65 (Association Response frame body) as follows (not all lines shown):***

* revme D7.0 up to 77, 11bh D6.0 up to 78-80, 11be D7.0 81-86, 11bk D5.0 no addition, 11bf D8.0 87-90
* Association Response frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 10 | RSN | The RSNE is present if dot11FILSActivated is true or if performing OWE or if the Association Response frame is encrypted; otherwise, it is not present.(#402)  |
| ... |  |  |
| 38 | Key Delivery | The Key Delivery element is present if dot11FILSActivated is true or if the Association Response frame is encrypted; otherwise, it is not present.(#402) |
| ... |  |  |
| 91 | EDP | The EDP element carrying configuration and EDP Group ID(#1012) for the assigned group EDP epoch(#1012). This element is present if the Association Response frame is encrypted and dot11EDPGroupEpochActivated is true; otherwise, it is not present. |
| 92 | Nonce | The Nonce element is optionally present as defined in 12.16.7.1 (PMKID privacy); otherwise, it is not present. (#269) |

**TGbi Editor: *Instruction: Modify 9.3.3.7 as follows:***

* Reassociation Request frame format

***Insert new rows to Table 9-66 (Reassociation Request frame body) in numeric order (not all lines shown):***

* revme D7.0 up to 64, 11bh D6.0 no addition, 11be D7.0 65-67, 11bk D5.0 no addition, 11bf D8.0 68-71
* Reassociation Request frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 72 | DS MAC Address | The DS MAC Address element is present if the Reassociation Request frame is encrypted, dot11DSMACAddressActivated is true, and the peer indicates support for DS MAC Address in the RSNXE; otherwise, it is not present.(#160) |
| 73 | EDP | The EDP element is present if the Reassociation Request frame is encrypted and dot11EDPGroupEpochActivated is true; otherwise, it is not present. This element carries the desired parameters of the Epoch to be joined by the sending STA. |
| 74 | Nonce | The Nonce element is optionally present as defined in 12.16.7.1 (PMKID privacy); otherwise, it is not present. (#269) |

**TGbi Editor: *Instruction: Modify 9.3.3.8 as follows:***

* Reassociation Response frame format

***Change rows in Table 9-67 (Reassociation Response frame body) as follows (not all lines shown):***

* revme D7.0 up to 80, 11bh D6.0 no addition, 11be D7.0 81-86, 11bk D5.0 no addition, 11bf D8.0 87-90
* Reassociation Response frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 10 | RSN | An RSNE is present in a Reassociation Response frame if dot11FastBSSTransitionActivated is true, dot11RSNAActivated is true, and this frame is a response to a Reassociation Request frame that contained an FTE (i.e., part of a fast BSS transition in an RSN)~~;~~, or if dot11FILSActivated is true~~;~~, or ifperforming OWE, or if the Reassociation Response frame is encrypted. Otherwise, it is not present.(#Ed, #400)  |
| ... |  |  |
| 41 | Key Delivery | The Key Delivery element is present if dot11FILSActivated is true and FILS authentication is used or if the Reassociation Response frame is encrypted; otherwise, it is not present.(#402)  |
| ... |  |  |
| 91 | EDP | The EDP element carrying configuration and EDP Group ID(#1012) for the assigned group EDP(#1012) epoch. This element is present if the Ressociation Response frame is encrypted and dot11EDPGroupEpochActivated is true; otherwise, it is not present. |
| 92 | Nonce | The Nonce element is optionally present as defined in 12.16.7.1 (PMKID privacy); otherwise, it is not present. (#269) |