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

178, 919, 917, 270, 687, 918

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the discussion during the meeting

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 11-25/0536 under all headings that include CID 967 |
| 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. Note that the current proposal is adopted to avoid the hassle of specifying the formula. We add a requirement but does not specify the formula. TGbi editor to make the changes shown in the latest version of 11-25/0536 under all headings that include CID 269HMAC-SHA256 (Anonce, Snonce) => no Nonce in EDPKESTA random value AP random value  |
| 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 11-25/0536 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 11-25/0536 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 11-25/0536 under all headings that include CID 919 |

***Discussion:***

***Proposal:***

**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 AP shall generate a new random PMKID for the identified PMKSA and deliver the generated PMKID(#967) to be used next time to the non-AP STA in the PMKID KDE included in the Key Delivery element of the encrypted (Re)Association Response frame. The EDP AP shall use a random input form the EDP non-AP STA (ex. SNonce or Diffie-Hellman parameter) to generate the new random PMKID. The formula to generate the new random PMKID is out of the scope of this standard.(#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 AP MLD shall generate a new random PMKID for the identified PMKSA and deliver the generated PMKID(#967) to be used next time to the non-AP MLD in the PMKID KDE included in the Key Delivery element of the encrypted (Re)Association Response frame.(#175) The EDP AP MLD shall use a random input form the EDP non-AP MLD (ex. SNonce or Diffie-Hellman parameter) to generate the new random PMKID. The formula to generate the new random PMKID is out of the scope of this standard.(#269)

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

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)

* PMKR0Name privacy

APs in the same mobility domain shall set the PMKSA Caching Privacy Support field in the RSNXE to the same value.

If both an FTO and a target FTR set the PMKSA Caching Privacy Support field in the RSNXE to 1, after the target FTR uses the indicated PMKR0Name to identify the PMK-R1 (see 13.8.1 (Overview)), and a PTKSA is established using the identified PMK-R1,

* the R1KH of the target FTR shall send the latest ANonce and SNonce to the R0KH and
* both the S0KH of the FTO and the R0KH shall recompute the PMKR0Name.

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

The PMKR0Name shall be recomputed as follows:

 PMKR0Name = Truncate-128(HMAC-Hash( XXKey, "FT-R0N" || ANonce || SNonce))

where:(#686)

 Hash is the hash algorithm from the key derivation type (see Table 9-190 (AKM suite selectors)) for each AKM

 "FT-R0N" is treated as an ASCII string

 XXKey is defined in 12.7.1.6.3 PMK-R0

 ANonce is the Authenticator nonce used when the current PTKSA was established

 SNonce is the Supplicant nonce used when the current PTKSA was established

NOTE 2—For a different PMKR0Name 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 in the frame indicating the PMKR0Name 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)

NOTE 3—PMKR1Name is still derived based on the indicated PMKR0Name with the same formula defined in 12.7.1.6.4 (PMK-R1) for the first time and PMKR1Name once derived is not recomputed because the Reassociation Request and Response frame that carry PMKR1Name are encrypted.

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.