IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi Proposed bug fix for PMKID generation |
| Date: 2025-1-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Duncan Ho | Qualcomm Technologies Incorporated | 5665 Morehouse DrSan Diego, CA 92121 | (858) 845-3214 | dho@qti.qualcomm.com |

Abstract

This submission proposes a bug fix for PMKID generation.

Revisions:

* Rev 0: Initial version of the document.

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 D0.6 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D0.7 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.***

**Discussion:**

Currently PMKID generation requires the ANonce and SNonce. See section 12.16.7.1.

* **PMKID privacy**

[…]

The PMKID shall be recomputed as:

 PMKID = Truncate-128(HMAC-Hash(Keyname, "PMK Name" || ANonce || SNonce))

However, the EDPKE frame exchange does not use ANonce and SNonce but they use “A-Ephemeral Pub” and “S-Ephemeral Pub” instead. Therefore, the ANonce and SNonce in PMKID generation should be replaced by those ephemeral keys.

**Proposed text change:**

Modify section 12.16.7.1 ss follows:

* **PMKID privacy**

After the indicated PMKID in an RSNE(#1466) 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, both the EDP non-AP STA and the EDP AP shall recompute the PMKID for the identified PMKSA to be used next time.
* For MLO, if the EDP non-AP STA(s)(#1467, #Ed) affiliated with an EDP non-AP MLD and the(#1467) EDP AP(s)(#Ed) affiliated with an EDP AP MLD set the PMKSA Caching Privacy Support field in the RSNXE to 1, both the EDP non-AP MLD and the EDP AP MLD shall recompute the PMKID for the identified PMKSA to be used next time.

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

The PMKID shall be recomputed as:

 PMKID = Truncate-128(HMAC-Hash(Keyname, "PMK Name" || ANonce || SNonce))

where:

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

 Table 9-190 (AKM suiteselec tors)) for each AKM

 Keyname is the key stored as PMK or MPMK in the PMKSA (see 12.6.1.1.2 (PMKSA))

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

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

If EPDKE authentication is used, the ANonce shall be replaced by the Ephemeral Public Key carried in the second Authentication frame of the EPDKE frame exchange (see 12.12.3.2 (PASN Frame Construction and Processing)) and the SNonce shall be replaced by the Ephemeral Public Key carried in the first Authentication frame of the EPDKE frame exchange.

TBD for recalculating the PMKID for Suite B AKMs.

NOTE 2—For a different PMKID to ensure privacy, the SPA needs to be randomized in the frame indicating the PMKID to identify the cached PMKSA. As a result, tracking cannot be done on the MAC address.(#1468)