IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D0.4 CR for 1145 |
| Date: 2024-11-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission proposes resolutions for the following CIDs:

1145

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 D0.6 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** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 1145 | Po-Kai Huang | 12.14.6.1 | 79.13 | Need to address the TBD for Suite B. If there are concerns for violating Suite B requirement (AKM 11 and 12), then we may want to continue disallow recomputation for suite B. "When the negotiated AKM uses PMKID derivation with (#3744)PTK-KCK as a parameter as defined in 12.7.1.3 (Pairwise key hierarchy), the PMKID derived from the PTK-KCK during the initial 4-way handshake is not changed during the lifetime of this PMKSA " | As in comment | Revised – Check with the people relevant to the texts of no change for PMKID. There are comments that there are no fundamental security issues to change PMKID for suite B AKM, but there is a preference to continue to use PTK-KCK to derive PMKID to avoid exposure of PMK. Propose to remove the TBD sentence and revise the texts along this line of technical thinking.TGbi editor to make the changes shown in 11-24/1927r0 under all headings that include CID 1145 |

**Discussion:**

**Proposed Texts: (#1145)**

**TGbi Editor: *Instruction: Modify 12.14.6.1 as shown below***

* 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—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 suite selectors)) for each AKM

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

 (PMKSA)) except when AKM is 00-0F-AC:11 or 00-0F-AC:12 and is

 PTK-KCK of the latest established PTKSA using the identified PMKSA

 when AKM is 00-0F-AC:11 or 00-0F-AC:12. (#1145)

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

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

(#1145)

NOTE—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)