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.
* Rev 1: Revision based on the offline discussion

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. 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 have PMKID to be used next time without exposure of PMK.To have the unified approach, the preferred solution is to deliver PMKID to be used next time reusing existing PMKID KDE.TGbi editor to make the changes shown in 11-24/1927r1 under all headings that include CID 1145 |

**Discussion:**

**Proposed Texts: (#1145)**

**TGbi Editor: *Instruction: Modify 12.16.7.1 as shown below***

12.16.7 PMKSA caching privacy

This subclause defines rules for(#1465) 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(#1488) Support field in the RSNXE to 1.

* + - 1. 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, the EDP AP shall deliver the PMKID for the identified PMKSA 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.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, the EDP AP MLD shall deliver the PMKID for the identified PMKSA 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.

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

(#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)

**TGbi Editor: *Instruction: Modify 9.4.2.23.5 as shown below***

**9.4.2.23.5 PMKID**

***Change third and fourth paragraph (not all shown) as follows:***

A PMKID in the PMKID List field can refer to

1. The PMKID of a cached PMKSA that has been obtained through preauthentication with the target AP
2. The PMKID of a cached PMKSA from an EAP, FILS, or SAE authentication
3. The PMKID of a PMKSA derived from a PSK for the target AP

ca) If PMKSA caching privacy is used, the changed PMKID(#1225)

**TGbi Editor: *Instruction: Modify 12.6.1.1.2 as shown below***

**12.6.1.1.2 PMKSA**

***Change the third paragraph (not all lines shown) as follows:***

A PMKSA association is bidirectional. In other words, both parties use the information in the security association

for both sending and receiving. The PMKSA is used to create the PTKSA. PMKSAs have a certain

lifetime. The PMKSA consists of the following:

— PMKID that identifies the security association.

* If PMKSA caching privacy is not used, PMKID as defined in 12.7.1.3 (Pairwise key hierarchy) or 12.7.1.6.3 (PMK-R0).
* If PMKSA caching privacy is used, changed PMKID as defined in 12.16.7.1 (PMKID privacy).(#1225)