IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Suite B PMKID | | | | |
| Date: 2018-11-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

The way PMKID is derived for Suite B AKMs is somewhat inconvenient since KCK is used as an input parameter and that means PMKID cannot be generated before going through PTK derivation, i.e., 4-way handshake. In addition to the that extra complexity during creation of the PMKSA, the standard is not very clear on whether the PMKID of the PMKSA might change whenever deriving a new KCK. It would be simpler to clearly define the PMKID to never change for the PMKSA and just point the first KCK to be used whenever using the PMKSA.

There have been some interoperability issues in this area that resulted in PMKSA caching not working due to different interpretations on which PMKID is used. This contribution proposes changes to REVmd/D1.6 to make this Suite B PMKID use defined explicitly in the standard in hope to minimize risk of such interoperability issues. It would be good to get this included in REVmd since Wi-Fi Alliance has already launched a certification program that uses these Suite B AKMs.

**Proposed changes to REVmd/D1.6:**

*Modify 12.6.1.1.2 as shown (note that change tracking does not show the two paragraph breaks added to split this single paragraph into three):*

* PMKSA

When the PMKSA is the result of a successful IEEE 802.1X authentication, it is derived from the EAP authentication and authorization parameters provided by the AS. When the PMKSA is the result of a successful SAE authentication, it is generated as a result of the successful completion of the SAE exchange.

The PMKSA is created by the Supplicant’s SME when the EAP authentication or FILS authentication completes successfully or the PSK is configured. The PMKSA is created by the Authenticator’s SME when the PMK is created from the keying information transferred from the AS in an IEEE 802.1X authentication exchange, when the FILS authentication completes successfully, when the SAE exchange successfully completes, or when the PSK is configured. When the negotiated AKM uses PMKID derivation with KCK as a parameter as defined in 12.7.1.3 (Pairwise key hierarchy), the PMKID derived from the KCK during the initial 4-way handshake is not changed during the lifetime of this PMKSA.

The PMKSA is used to create the PTKSA. PMKSAs have a certain lifetime. The PMKSA consists of the following: