IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| FILS IKM for FT | | | | |
| Date: 2015-05-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

P802.11ai/D4.0 cleaned up some of the key derivation clauses and ended up removing IKM (intermediate keying material?) without updating other parts of the document where IKM is still used in case of FT key hierarchy. This document proposed changes to bring back the IKM definition to fix the FT case.

CID 7266 addresses one of the IKM occurrences by replacing it with PMK in 11.6.1.7.1. However, that change does not cover a figure in that clause or the other occurrences of IKM in Clause 12. The additional changes proposed in this document could be used to amend that comment’s resolution.

### Proposed changes

**11.6.1.7 FT key hierarchy**

**11.6.1.7.1 Overview**

*Replace “IKM” with “PMK” in Figure 11-31—FT key hierarchy at an Authenticator*

**12.2.2 Authenticator key holders**

*Change as follows:*

The R0KH and R1KH are responsible for the derivation of keys in the FT key hierarchy. For fast BSS transition, the functions of the IEEE Std 802.1X Authenticator are distributed among the R0KH and R1KHs.

The R0KH interacts with the IEEE Std 802.1X Authenticator to receive the MSK resulting from an EAP authentication. The R1KH interacts with the IEEE Std 802.1X Authenticator to open the Controlled Port. Both the R0KH and R1KH interactions with the IEEE Std 802.1X Authenticator occur within the SME.

The R0KH derives the PMK-R0 for use in the mobility domain utilizing the MSK (when the AKM negotiated is 00-0F-AC:3), the PSK (when the AKM negotiated is 00-0F-AC:4) or the PMK (when the AKM negotiated is 00-0F-AC:9, 00-0F-AC:16, or 00-0F-AC:17). The R0KH shall be responsible for deriving a PMK-R1 for each R1KH within the mobility domain.

**12.2.3 Supplicant key holders**

*Change as follows:*

The S0KH and S1KH are responsible for the derivation of keys in the FT key hierarchy. The S0KH and S1KH are entities that are assumed to physically reside in the Supplicant.

The S0KH interacts with the IEEE Std 802.1X functional block (see Figure 4-18 (Portion of the ISO/IEC basic reference model covered in this standard) in 4.9 (Reference Model) to receive the MSK resulting from  an EAP authentication or the PMK resulting from a FILS authentication. The S1KH interacts with 802.1X to  open the Controlled Port. Both the S0KH and S1KH interactions with 802.1X occur within the SME of a STA.

The S0KH derives the PMK-R0 for use in the mobility domain utilizing the MSK (when the AKM negotiated is 00-0F-AC:3), the PSK (when the AKM negotiated is 00-0F-AC:4) or the PMK (when the  AKM negotiated is 00-0F-AC:9, 00-0F-AC:16, or 00-0F-AC:17).

**12.2.4 FT initial domain association over FILS in an RSN**

*Change as follows:*

Upon successful completion of FILS authentication request processing, the R0KH on the AP uses the PMK (see 11.11.2.4.2) to establish key hierarchy. If a key hierarchy already exists for this STA belonging to the same mobility domain (i.e., having the same MDID), the R0KH shall delete the existing PMK-R0 security association and PMK-R1 security associations. It then calculates the PMK-R0, PMKR0Name, and PMK-R1 and makes the PMK-R1 available to the R1KH of the AP that the STA is associated to.