IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key names with FT using SHA-384 | | | | |
| Date: 2018-06-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

IEEE Std 802.11ac-2013 added new AKM suite selectors 00-0F-AC:11 (802.1X, SHA-256), 00-0F-AC:12 (802.1X, SHA-384), and 00-0F-AC:13 (FT, SHA-384) for Suite B compliant options for RSN. Suite B was replaced with CNSA Suite which maintains only the SHA-384 based combinations. The previously defined AKM suite selector 00-0F-AC:12 covers this need with 802.1X/EAP authentication, but the definition of the AKM suite selector 00-0F-AC:13 apparently missed couple of changes to be consistent with algorithm use. In particular, AKM 00-0F-AC:13 did not modify PMKID derivation rules (it ends up defaulting to using SHA-1 now) and PMKR0Name/PMKR1Name derivation (uses SHA-256).

To follow the requirements of the CNSA Suite, these key naming definitions for 00-0F-AC:13 would need to be replaced with consistent use of SHA-384 through all operations. There has been no known (at least to the author) deployments of devices with AKM 00-0F-AC:13 support, so it looks justifiable to address this undesired inconsistency now in REVmd before need for deployment arises. A similar fix was done for PMKID derivation with FILS in REVmd/D1.0. The only known (to the author) implementation of AKM 00-0F-AC:13 is already using the proposed changes to meet the CNSA Suite requirements.

This contribution proposes changes to REVmd/D1.0 to address the identified issues. There is no CID for this change in the D1.0 letter ballot since the issue was discovered during an implementation effort after that ballot closed.

**12.7.1.3 Pairwise key hierarchy**

*Change REVmd/D1.0 page 2399 line 54 as shown:*

When the negotiated AKM is 00-0F-AC:13, 00-0F-AC:15 or 00-0F-AC:17, and the PMK identifier is defined as

PMKID = Truncate-128(HMAC-SHA-384(PMK, "PMK Name" || AA || SPA))

**12.7.1.6.3 PMK-R0**

*Change REVmd/D1.0 page 2404 lines 21-27 as shown:*

The PMK-R0 is referenced and named as follows:

PMKR0Name = Truncate-128(Hash("FT-R0N" || PMK-R0Name-Salt))

where

— Hash is the hash algorithm identified by the AKM suite selector (see Table 9-144 (AKM suite selectors)).

— "FT-R0N" is treated as an ASCII string.

**12.7.1.6.4 PMK-R1**

*Change REVmd/D1.0 page 2404 lines 53-61 as shown:*

The PMK-R1 is referenced and named as follows:

PMKR1Name = Truncate-128(Hash("FT-R1N" || PMKR0Name || R1KH-ID || S1KH-ID))

where

— Hash is the hash algorithm identified by the AKM suite selector (see Table 9-144 (AKM suite selectors)).

— "FT-R1N" is treated as an ASCII string.