IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Modifications for FT with FILS Association |
| Date: 2014-07-14 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Soo Bum LeeGeorge CherianSantosh AbrahamJouni Malinen | Qualcomm | 5775 Morehouse Dr., San Diego, CA 92121 | +1 858 651 6645 | gcherian@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposes modifications to allow FT association with FILS

* General description
* Overview of the services
* Access control and data confidentiality services

.

***Change sub Clause 4.5.4.8 a****s follows*

4.5.4.8 Fast BSS transition

The FT mechanism defines a means for a STA to set up security and QoS parameters prior to reassociation

to a new AP. This mechanism allows time-consuming operations to be removed from the time-critical

reassociation process within a mobility domain. When the FILS authentication is used during a handover across mobility domains, the overhead incurred during the FT initial mobility domain association in a RSN is further reduced.

* Frame formats
* Management frame body components

**8.4.2 Information Elements**

**8.4.2.24 RSNE**

* AKM suites

***Insert new row in Table 8-101 as shown, adjusting numbers appropriately:***

|  |
| --- |
| * AKM suite selectors
 |
| OUI | Suite type |  | Meaning |  |
| Authentication type | Key management type | Key derivation type |
| 00-0F-AC | <ANA-3> | FT authentication over FILS with SHA-256 and GCM-128 | FT over FILS key management as defined in 11.6.1.7 | Defined in  11.6.1.7.2 |
| 00-0F-AC | <ANA-4> | FT authentication over FILS with SHA-384 and GCM-256 | FT over FILS key management as defined in 11.6.1.7 | Defined in  11.6.1.7.2 |

* Security
* Keys and key distribution

11.6.1 Key hierarchy

**11.6.1.7 FT key hierarchy**

***Change clause 11.6.1.7.1 as follows:*** [14/0341r5]

**11.6.1.7.1 Overview**

This subclause describes the FT key hierarchy and its supporting architecture. The FT key hierarchy is

designed to allow a STA to make fast BSS transitions between APs without the need to perform an SAE or

IEEE 802.1X authentication at every AP within the mobility domain.

The FT key hierarchy can be used with SAE, IEEE 802.1X authentication, PSK authentication, or FILS authentication.

The FT key hierarchy shown in Figure 11-27 consists of three levels whose keys are derived using the key

derivation function (KDF) described in 11.6.1.7.2 as follows:

a) PMK-R0 – the first-level key of the FT key hierarchy. This key is derived as a function of the master

session key (MSK) or PSK. It is stored by the PMK-R0 key holders, R0KH and S0KH.

b) PMK-R1 – the second-level key of the FT key hierarchy. This key is mutually derived by the S0KH

and R0KH.

c) PTK – the third-level key of the FT key hierarchy that defines the IEEE 802.11 and IEEE 802.1X

protection keys. The PTK is mutually derived by the PMK-R1 key holders, R1KH and S1KH.

As shown in Figure 11-27, the R0KH computes the PMK-R0 from the key obtained from SAE

authentication (for the purposes of FT this key is identified as the Master PMK, or MPMK), from the PSK,

from the MSK resulting (per IETF RFC 3748-2004 [B38] ) from a successful IEEE 802.1X authentication

between the AS and the Supplicant or from the rMSK resulting from a successful FILS authentication. Upon a successful authentication, the R0KH shall delete any prior

PMK-R0 security association for this mobility domain pertaining to this S0KH. The R0KH shall also delete

all PMK-R1 security associations derived from that prior PMK-R0 security association.

***Change Figure 11-31 to the following***



**Figure 11-31 – FT key hierarchy at an Authenticator**

***Change clause 11.6.1.7.3 as follows***

**11.6.1.7.3 PMK-R0**

The first-level key in the FT key hierarchy, PMK-R0, is derived using the KDF defined in 11.6.1.7.2. The

PMK-R0 is the first level 256-bit keying material used to derive the next level keys (PMK-R1s):

R0-Key-Data = KDF-384(XXKey, "FT-R0", SSIDlength || SSID || MDID || R0KHlength || R0KH-ID

|| S0KH-ID)

PMK-R0 = L(R0-Key-Data, 0, 256)

PMK-R0Name-Salt = L(R0-Key-Data, 256, 128)

where

— KDF-384 is the KDF as defined in 11.6.1.7.2 used to generate a key of length 384 bits.

— L(-) is defined in 11.6.1.

— If the AKM negotiated is 00-0F-AC:3, then XXKey shall be the second 256 bits of the MSK (which

is derived from the IEEE 802.1X authentication), i.e., XXKey = L(MSK, 256, 256). If the AKM

negotiated is 00-0F-AC:4, then XXKey shall be the PSK. If the AKM negotiated is 00-0F-AC:9, then XXKey shall be the MPMK generated as the result of SAE authentication. If the AKM negotiated is 00-0F-AC:<ANA-3> or 00-0F-AC:<ANA-4> , then XXKey shall be the second 256bits of rMSK (which is derived from EAP-RP).

***Insert new sub-Clause after sub-Clause 11.11 as follows:***

**11.A1-1 FT initial domain association over FILS in an RSN**

A STA indicates its support for the FT procedures by including the MDE in the Authentication Request frame and indicates its support of security in the RSNE. To establish FT key hierarchy, the AP responds by including the FTE, MDE, and RSNE in the Authentication Response frame. At the end of the sequence, the IEEE 802.1X Controlled Port is opened, and the FT key hierarchy has been established. The message flow is shown in Figure 11-AI-1

When authentication is used for the FT initial domain association in an RSN, the FT initial domain association procedures performed during association request and response messages (see 12.4.2) is performed during the authentication frame exchanges; and the FT initial domain association procedures performed during FT 4-way handshake message 2 and message 3 (see 12.4.2) is performed during the FILS association frame exchanges as shown in Figure 12-3.

To establish FT key hierarchy, the STA shall send an Authentication Request frame to the AP that includes the MDE. The contents of the MDE shall be the values advertised by the AP in its Beacon or Probe Response frames. Additionally, the STA includes its security capabilities in the RSNE.

If the contents of the MDE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the Authentication Request frame with status code 54 (i.e., Invalid MDE). If an MDE is present in the Authentication Request frame and the contents of the RSNE do not indicate a negotiated AKM of Fast BSS Transition over FILS (suite type 00-0F-AC:<ANA-3> or 00-0F-AC:<ANA-4>), the AP shall reject the Authentication Request frame with status code 43 (i.e., Invalid AKMP).

After performing EAP-RP with an authentication server, the R0KH on the AP receives the rMSK and authorization attributes. 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 with which the STA is associated.

Then, the AP shall construct an Authentication Response frame. The Authentication Response frame shall contain an MDE, with contents as presented in Beacon and Probe Response frames. The FTE shall include the key holder identities of the AP, the R0KH-ID and R1KH-ID, set to the values of dot11FTR0KeyHolderID and dot11FTR1KeyHolderID, respectively. The FTE shall have a MIC element count of zero (i.e., no MIC present) and have ANonce, SNonce, and MIC fields set to 0.

The S1KH on STA provides the PMKR1Name in the PMKID field of the RSNE to be included in the Association Request Frame. The PMKR1Name shall be as calculated by the S1KH according to the procedures of 11.6.1.7.4; all other fields of the RSNE shall be identical to the RSNE present in the Authentication Request frame. The S1KH shall provide the FTE and MDE; the FTE and MDE shall be the same as those provided in the AP’s Authentication Response frame.

Finally, the R1KH provides the PMKR1Name in the PMKID field of the RSNE to be included in Association Response frame. The PMKR1Name shall be as calculated by the R1KH according to the procedures of 11.6.1.7.4 and shall be the same as the PMKR1Name in the FILS Association Request frame; all other fields of the RSNE shall be identical to the RSNE present in the Beacon or Probe Response frames. The R1KH shall also provide the FTE, the MDE, the reassociation deadline timeout in the TIE[ReassociationDeadline], and the PTK key lifetime in the TIE[KeyLifetime]. The FTE and MDE shall be the same as in the Authentication Response frame. The reassociation deadline shall be set to the minimum of dot11FTReassociationDeadline and the key lifetime.

***Insert new figure as follows***



**Figure 11-AI-1—FT initial mobility domain association using FILS authentication in an RSN**

**12. Fast BSS transition**

**12.2 Overview**

***Change clause 12.2.2 as shown***

**12.2.2 Authenticator key holders**

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 802.1X Authenticator are distributed among the R0KH and R1KHs.

The R0KH interacts with the IEEE 802.1X Authenticator to receive the MSK resulting from an EAP

Authentication or the rMSK resulting from an EAP reauthentication (i.e., EAP-RP). The R1KH interacts with the IEEE 802.1X Authenticator to open the Controlled Port. Both the R0KH and R1KH interactions with the IEEE 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) or the rMSK (when the AKM negotiated is 00-0F-AC:<ANA-3> or 00-0F-AC:<ANA-4>). The R0KH shall be responsible for deriving a PMK-R1 for each R1KH

within the mobility domain.

**12.2.3 Supplicant key holders**

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 802.1X functional block (see Figure 4-14 in 4.9) to receive the MSK

resulting from an EAP authentication or the rMSK resulting from an EAP reauthentication. 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) or the rMSK resulting from an EAP reauthentication.

 [14/0341r5]

[14/0341r5][CID 2716]

[14/183r0]