IEEE P802.11
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| FT AKM for PASN |
| Date: 2025-05-21 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel  |  |  | po-kai.huang@intel.com |
| Ido Ouzieli |  |  | ido.ouzieli@intel.com |
| Johannes Berg |  |  | johannes.berg@intel.com |
| Ilan Peer |  |  | ilan.peer@intel.com |
|  |  |  |  |  |

 |

Abstract

This submission propose several clarifications for FT used under PASN and proposes to add AKM 9 and 25 to PASN.

**Revision History:**

R0: Initial version.

R1: Revision to clarify FT AKMP based on the feedback during the F2F meeting

## Discussion:

**Topic 1:**

PASN can use AKM 00-0F-AC: [3, 4, 13, 19, 22] as the base AKMP for FT.

***12.13.6 PASN authentication with FT***

*This subclause specifies aspects of PASN authentication when one of (#7033)AKM 00-0F-AC: [3, 4, 13, 19, 22] is used as the (#7185)base AKMP.*









Under FT key hierarchy, PTKSA is generally derived under PMK-R1. However, the current PTK derivication of PASN simply refers to PMK, which can not represent PMK-R1 under 12.7.1.6.1 Overview of FT key hierarchy. Note that in 12.7.1.6.1, we have PMK-R0 derived from MPMK (ex PMK from SAE, MSK from 802.1X), PMK-R1 derivied from PMK-R0, and PTK derived from PMK-R1. As a result, the terminology “PMK” is not accurate for FT. We propose to clarify that PMK-R1 is used under PASN with FT AKM to derive PTKSA.

**Topic 2:**

FTE currently includes ANonce, SNonce based on 13.8.2. In PASN, the PTK derviation does not involve SNonce and ANonce, so the two fields are not used. We propose to clarify that ANonce and SNonce is not used under PASN with FT AKM to derive PTKSA.

**Topic 3:**

AKM 9 and AKM 25 is currently not listed under PASN for FT.

***12.13.6 PASN authentication with FT***

*This subclause specifies aspects of PASN authentication when one of (#7033)AKM 00-0F-AC: [3, 4, 13, 19, 22] is used as the (#7185)base AKMP.*





We note that SAE defined in clause 12.4 can have AKM 9 and 25 as well. Once a STA uses AKM 9 and 25 in FT initial domain association, then the STA should be able to use AKM 9 and 25 in current PASN. As a result, we propose to allow AKM 9 and 25 in PASN FT.

**Reference:**

Currently, when used with FT, PASN relies on the FT key hierarchy establsiehd via initial domain association to compute PTKSA like other PASN protocol.

*When used with FT, PASN authentication is an RSNA protocol, and relies on the FT key hierarchy already being established via the FT initial mobility domain association (13.4.2 (FT initial mobility domain association in an RSN)). PASN protocol messages carry the PMKR0Name, and the PASN PTKSA is established like any other base AKMP.*

The PTKSA derivation of PAN is shown below.

*PTK = KDF-HASH-NNN (PMK, “PASN PTK Derivation”, SPA || BSSID || DHss)*

*where*

*PMK (#7185)is the pairwise master key for the base AKMP if the AKMP is other than*

*PASN AKMP; see 9.4.2.23.3 (AKM suites). Otherwise, if the base AKMP is*

*PASN AKMP, that is, the PASN PTKSA is being setup without mutual*

*authentication in a non-RSN, the PMK shall be set to the string “PMKz” padded*

*with 28 0s.*

*NOTE—The PMK for the derivation can come from a cached PMKSA for the AKMP or*

*from the PMKSA established with PASN by tunneling Wrapped Data or Authentication*

*frames.*

To do PASN with FT, Wrapped Data element is included in the first and second message to follow first and second message of 13.8.2.

*The Wrapped Data element shall be optionally present in the (#8118)first PASN frame. When the Wrapped Data element is not present, the authentication is non-FT PASN. When present, the authentication is FT PASN. The Wrapped Data element shall contain a set of elements that include RSNE (9.4.2.23 (RSNE)), MDE (9.4.2.45 (MDE(#1776))), and FTE (9.4.2.46 (FTE(#1776))) as specified for the first message of the FT authentication sequence (13.8.2 (FT authentication sequence: contents of first message)). The Wrapped Data element shall be optionally present in the second PASN frames but shall be present if the Wrapped Data element was present in the first PASN frame. When present it shall contain a set of elements that include the RSNE (9.4.2.23 (RSNE)), the MDE (9.4.2.45 (MDE(#1776))), and the FTE (9.4.2.46 (FTE(#1776))) as specified for the second message of the FT authentication sequence (13.8.3 (FT authentication sequence: contents of second message)).*

## Proposed Text:

**12.13.6 PASN authentication with FT**

This subclause specifies aspects of PASN authentication when one of AKM 00-0F-AC: [3, 4, 9, 13, 19, 22, 25] is used as the base AKMP.(#3)

When used with FT, PASN authentication is an RSNA protocol, and relies on the FT key hierarchy already being established via the FT initial mobility domain association (13.4.2 (FT initial mobility domain association in an RSN)). PASN protocol messages carry the PMKR0Name, and the PASN PTKSA is established like any other base AKMP.

The Wrapped Data element shall be optionally present in the (#8118)first PASN frame. When the

Wrapped Data element is not present, the authentication is non-FT PASN. When present, the authentication is FT PASN. The Wrapped Data element shall contain a set of elements that include RSNE (9.4.2.23 (RSNE)), MDE (9.4.2.45 (MDE(#1776))), and FTE (9.4.2.46 (FTE(#1776))) as specified for the first message of the FT authentication sequence (13.8.2 (FT authentication sequence: contents of first message)). The Wrapped Data element shall be optionally present in the second PASN frames but shall be present if the Wrapped Data element was present in the first PASN frame. When present it shall contain a set of elements that include the RSNE (9.4.2.23 (RSNE)), the MDE (9.4.2.45 (MDE(#1776))), and the FTE (9.4.2.46 (FTE(#1776))) as specified for the second message of the FT authentication sequence (13.8.3 (FT authentication sequence: contents of second message)). The Wrapped Data element shall be absent in the third PASN frame. The elements in the Wrapped Data element are used for additional validation FT security parameters as being used in PASN authentication.

NOTE – The ANonce or SNonce included in the FTE of the first PASN frame or the second PASN frame is not used in the PTKSA derivation. See 12.13.8.(#2)

**12.13.8 PTKSA derivation with PASN authentication**

For PTKSA key derivation, the inputs to the PRF are defined by the following formula. (#1)

PTK = KDF-HASH-NNN (PASN-PMK(#1), “PASN PTK Derivation”, SPA || BSSID || DHss)

where

PASN-PMK (#7185) is the pairwise master key for the base AKMP if the base AKMP is other than

PASN AKMP or the Authentication type column for the base AKMP does not indicate FT authentication (see 9.4.2.23.3 (AKM suites)). If the Authentication type column (see Table 9-190 (AKM suite selectors)) for the base AKMP indicate FT authentication, then the PASN-PMK is the PMK-R1. If the base AKMP is PASN AKMP, that is, the PASN PTKSA is being setup without mutual authentication in a non-RSN, the PASN-PMK shall be set to the string “PMKz” padded with 28 0s. (#1)

NOTE—The PASN-PMK(#1) for the derivation can come from a cached PMKSA for the AKMP or from the PMKSA established with PASN by tunneling Wrapped Data or Authentication frames.

(…existing texts…)