IEEE P802.11
Wireless LANs

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

|  |
| --- |
| CR for CIDs 7095, 7096 |
| Date: 2024-05-02 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry | Cisco Systems |  |  | jerhenry@cisco.com  |
| Stephen Orr | Cisco Systems |  |  | sorr@cisco.com  |
| Nehru Bhandaru | Broadcom |  |  | nehru.bhandaru@broadcom.com  |
| Thomas Derham | Broadcom |  |  | thomas.derham@broadcom.com  |
|  |  |  |  |  |

 |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11-REVme D5.0:

7095, 7096

**Revision History:**

R0: Initial version.

# CIDs 7095, 7096

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** |
| 7095 | 12.13.6 | 3164.62 | Add text to clarify the procedure. | PASN Authentication with FT is not precise on how the second AP validates the MDE and PMKR0Name, "Like any other Based AKMP" only covers the PTKSA, not the STA parameters validation. |
| 7096 | 12.13.6 | 3164.62 |  | PASN Authentication with FT may build on FT where a RSNA is used, or not. The second case is not described. |

## Discussion:

Agree that FT has specific requirements that include, for the AP, reaching out to the PMKR0Name, and for the STA to signal the PMKR0 identity. The text needs to clarify the scenarios, as bundling all cases into a single paragraph causes confusion.

## Proposed Resolution: CID 7095, 7096

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for corresponding CIDs

**TGme Editor: *Instruction: Modify 12.13.6 as shown below***

**12.13.6 PASN authentication with FT**

This subclause specifies aspects of PASN authentication when one of FT AKMPs 00-0F-AC: [3, 4, 13, 19] is used as the Base AKMP.

PASN authentication, when used with FT and as an RSNA protocol, relies on 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 FT PMKR~~1~~0Name and PMKR0Name~~as the PMKID~~, and the PASN PTKSA is established like any other Base AKMP.

Wrapped Data shall be optionally present in PASN first frame. When Wrapped Data is not present, the authentication is non-FT PASN. When present, Wrapped Data ~~it~~ 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 FT authentication sequence (13.8.2 (FT authentication sequence: contents of first message)). Wrapped Data shall be optionally present in the second PASN frames but shall be present if Wrapped Data was present in the first PASN frame. When present it 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 second message of FT authentication sequence (13.8.2 (FT authentication sequence: contents of ~~first~~ second message)). Wrapped Data shall be absent in the third PASN frame. The elements in the Wrapped Data are used for additional validation FT security parameters as being used in PASN authentication.

PASN authentication, when used with FT and when not an RSNA protocol, does not rely on FT key hierarchy already being established. Wrapped Data shall be optionally present in PASN first frame for PASN FT initial mobility domain authentication. When Wrapped Data is not present, the authentication is non-FT PASN. When Wrapped Data is present, it 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 FT authentication sequence (13.8.2 (FT authentication sequence: contents of first message)). Wrapped Data shall be optionally present in the second PASN frames but shall be present if Wrapped Data was present in the first PASN frame. When present it 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 second message of FT authentication sequence (13.8.2 (FT authentication sequence: contents of second message)). Wrapped Data shall be absent in the third PASN frame.

Wrapped Data shall be optionally present in PASN first frame for PASN FT over-the-air protocol. When present it 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))). The PMKR0Name shall be set to Null. Wrapped Data shall be optionally present in the second PASN frames but shall be present if Wrapped Data was present in the first PASN frame. When present it 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))) . The PMKR0Name shall be set to Null. Wrapped Data shall be absent in the third PASN frame. Authentication to the target AP is successful if the target AP receives the PASN third frame within the Rassociation Deadline Time.

The FT Request, during the Over-the-DS FT protocol includes the FTO, TargetAP, RSNE, MDE, and FTE (13.5.3). The FTO is the MAC address that the STA intends to use with the TargetAP. The PMKR0Name is set to Null. The SNonce is the public ephemeral key (12.13.3.2). The FT Response includes the FTO, the TargetAP, the RSNE, the MDE, and the FTE (13.5.3). The PMKR0Name is set to Null. The ANonce is the target AP public ephemeral key (12.13.3.2). PASN FT Authentication to the target AP is successful if the target AP receives the PASN third frame within the Rassociation Deadline Time.