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.

R1: better wording after review.

R2: editorial improvements

# 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 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 FT PMKR~~1~~0Name and PMKR0Name~~as the PMKID~~, and the PASN PTKSA is established like any other Base AKMP.

The Wrapped Data element shall be optionally present in PASN first 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 ~~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 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 frame~~s~~ 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.~~2~~3 (FT authentication sequence: contents of ~~first~~ 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.

PASN authentication, when used with FT and when not as an RSNA protocol, does not rely on FT key hierarchy already being established. The Wrapped Data element shall be present in the PASN first frame and the PASN second frame for PASN FT initial mobility domain authentication. The Wrapped Data element shall be absent in the third PASN frame.

The Wrapped Data element shall be present in the PASN first frame for PASN FT over-the-air protocol, and contain the RSNE, the MDE, and the FTE. In the RSNE, the PMKR0Name shall be set to Null. In the second PASN frame, the Wrapped Data element shall contain the RSNE, the MDE, and the FTE. In the RSNE, the PMKR0Name shall be set to Null. The Wrapped Data element 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 reassociation deadline time.

The FT Request, during the Over-the-DS PASN FT protocol shall include the FTO, TargetAP, RSNE, MDE, and FTE. The FTO shall be the MAC address that the STA intends to use with the TargetAP. In the RSNE, the PMKR0Name shall be set to Null. In the FTE, the SNonce shall be the public ephemeral key (12.13.3.2). The FT Response shall include the FTO, the TargetAP, the RSNE, the MDE, and the FTE (13.5.3). The PMKR0Name shall be set to Null. In the FTE, the ANonce shall be 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 reassociation deadline time.