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

R3: clearer solution

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

The Wrapped Data element shall be optionally present in the 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.

**TGme Editor: *Instruction: Please insert the following clause after 12.13.6 and renumber following clauses accordingly:***

12.13.7 Tunneled PASN

Tunneled PASN allows a STA to perform ephemeral key exchanges with a target AP through another AP with which a PASN session is established, and where both APs advertise the same SSID (non-FT case) and the same mobility domain (FT case). The APs advertize this possibility by setting the Tunneled PASN Capability bit in the Extended Capability field. The STA establishes a PASN session with the first AP. The STA then shall send to the first AP a PASN first frame that includes the Tunneled PASN element. The Tunneled PASN element shall contain the address that the STA intends to use with the target AP, and the BSSID of the target AP’s BSS. The ephemeral key passed in the PASN first frame shall be the key that the STA intends to use with the target AP.

The PASN second frame shall include the Tunneled PASN element with the STA address and the the BSSID of the target AP’s BSS. The ephemeral key passed in the PASN second frame shall be the key provided by the target AP. The TIE shall be present with Timeout Interval Type field set to 1.

Authentication to the target AP is successful if the target AP receives the PASN third frame within the time indicated by the Timeout Interval Value field.

**TGme Editor: *Instruction: Please insert the following clause at the end of clause 9.4.2:***

9.4.2.xx. Tunneled PASN element

The Tunneled PASN element is present in tunneled PASN frames (12.13.17). The format of the Tunneled PASN element is shown in Figure XX.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension  | STA Address | Target AP Address |
| Octets:  | 1 | 1 | 1 | 6 | 6 |

## Figure -XX Tunneled PASN element

The Element ID, Length and Element ID Extension fields are defined in 9.4.2.1 (General).

The STA address is the address that the STA intends to use with the target AP. The Target AP Address is the BSSID of the BSS of the AP with which the STA performs tunneled PASN.

**TGme Editor: *Instruction: Please insert the following line at the end of table 9-70:***

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| <ANA> | Tunneled PASN element | A Tunneled PASN element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames).  |

**TGme Editor: *Instruction: Please modify table 9-71 as follows:***

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication algorithm  | Authentication transaction sequence number  | Status Code(#3326)  | Presence of fields and elements from order 4 onward  |
| PASN Authentication(11a z)  | 1  | Reserved  | RSNE is present.RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.PASN Parameters element is present.Timeout Interval element may be present.Wrapped Data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved.Fragment element may be present if any of the elements are fragmented. Tunneled PASN element may be present. |
| PASN Authentication(11a z)  | 2  | Status  | RSNE is present and PASN Parameters element is present if Status Code field is 0.RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero. Timeout Interval element may be present.Wrapped data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved and Status Code field is 0.MIC element is present.Fragment element may be present if any of the elements are fragmented and Status Code field is 0. Tunneled PASN element may be present. |

**TGme Editor: *Instruction: Please insert the following line at the end of table 9-130:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element  | Element ID  | Element ID Extension  | Extensible  | Fragmentable  |
| Tunneled PASN element (see 9.4.2.xx, Tunneled PASN element) | <ANA> | <ANA> | Yes | No |

**TGme Editor: *Instruction: Please insert the following line at the end of table 9-192:***

|  |  |  |
| --- | --- | --- |
| Bit | Information | Notes |
| <ANA> | Tunneled PASN Support | Set to 1 to indicate that the AP supports the tunneled PASN feature |
| 106-n | Reserved  |  |