IEEE P802.11
Wireless LANs

|  |
| --- |
| LB282 CR for CID237 |
| Date: 2024-01-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Okan Mutgan | Nokia |  |  | okan.mutgan@nokia-sbell.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions and discussions for CID237 on 802.11bh D2.0:

R0. Initial Version.

R1. Modified the discussion and some typos.

R2. Added CID177 for the comment resolution.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed Change | Resolution |
| 237 | 37 | 44 | P33L56 mentions "...if using PASN authentication, the AP shall include an IRM element in the second PASN frame."Second PASN frame does not contain IRM element. | Add IRM element to the second PASN frame. | REVISED. |
| 177 | 38 | 14 | "-- If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as defined in 9.4.2.311 (Device ID element)" -- not consistent with the previous wording | Append ", if required per the procedure in 12.2.12.1 (Device ID mechanism)" | REVISED |

**Discussion**

IRM element has two fields: “IRM Status” and “IRM” field.

In PASN,

third PASN frame contains only “IRM” field (to assign a new IRM)

second PASN frame contains “IRM Status” field (to indicate the current IRM’s status - recognized/not recognized).

P33L56 (in 12.2.12.2 Identifiable random MAC address (IRM) operation) mentions to send IRM IE in second PASN frame as follows (**bolded sentence**):

“A non-AP STA indicates support for the IRM mechanism in a (Re-)Association Request frame and the AP indicates support for the IRM mechanism in the corresponding (Re-)Association Response frame. If a non-AP STA indicates support for the IRM mechanism in an Association Request frame and the AP indicates support for the IRM mechanism in the corresponding Association Response frame, then the AP shall include an IRM KDE in message 3 of the 4-way handshake or, if using FILS authentication, the AP shall include an IRM element in the Association Response frame or **if using PASN authentication, the AP shall include an IRM element in the second PASN frame.**”

However, “12.13.3.2 PASN frame construction and processing” section does not define IRM element for second PASN frame. Therefore, add IRM element to second PASN frame in this section.

Besides, “12.13.3.2 PASN frame construction and processing” in D2.0 includes device ID element in third PASN frame. Since device ID element does not exist in third PASN frame, it should be deleted.

NOTE: since PASN frame construction is changed based on document number 11-24-0044rx, the change should apply to that document.

**Proposed Changes**

**CID237, CID177**

*Modify the following sentences in 11/24-0044rx:*

**12.13.3 Key establishment with PSN authentication 12.13.3.2 PASN frame construction and processing**

***Add the following text as shown at the end of the list that begins: “The first PASN authentication frame (see 9.3.3.11) of the exchange is constructed as follows:”***

— If dot11DeviceIDActivated is true, including a Device ID element ~~containing a device identifier~~ as

defined in 9.4.2.311 (Device ID element), if required per the procedure in 12.2.12.1 (Device ID mechanism).

***Add the following text as shown in the list that begins: “***— Derives the PTKSA; see 12.13.7.***”***

* If dot11RSNAOperatingChannelValidationActivated is true, including an OCI Element containing

an OCI element as defined in 9.4.2.236 (OCI element), if dot11RSNAOperatingChannelValidationActivated is true.

* If dot11DeviceIDActivated is true, including a PASN Encrypted Data element and a Device ID subelement ~~containing a device identifier~~ as defined in 9.4.2.311 (Device ID element) in the PASN Encrypted Data element, if required per the procedure in 12.2.12.1 (Device ID mechanism). The PASN Encrypted Data element shall be encrypted as defined in 12.2.12.3 (Encryption Encrytped Data element in PASN). (#210)
* If dot11IRMActivated is true, including a PASN Encrypted Data element and a IRM subelement as defined in 9.4.2.312 (IRM element) in the PASN Encrypted Data element, if required per the procedure in 12.2.12.2 (Identifiable random MAC address (IRM) operation). The PASN Encrypted Data element shall be encrypted as defined in 12.2.12.3 (Encryption of PASN Encrypted Data element in PASN).
* A MIC element (9.4.2.118) with MIC computed as specified in 12.13.8.1.

***Add the following text as shown in the list that begins: “Otherwise the STA begins the constructions of the third PASN frame as follows:”***

* If dot11RSNAOperatingChannelValidationActivated is true, including an OCI Element containing an OCI element as defined in 9.4.2.236 (OCI element).
* ~~If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as defined in 9.4.2.311 (Device ID element).~~
* If dot11IRMActivated is true, including a PASN Encrypted Data element and a IRM subelement ~~containing an IRM~~ as defined in 9.4.2.312 (IRM element) in the PASN Encrypted Data element, if required ~~the STA so chooses,~~ per the procedure in 12.2.12.2 (Identifiable random MAC address (IRM) operation). The PASN Encrypted Data element shall be encrypted as defined in 12.2.12.3 (Encryption of PASN Encrypted Data element in PASN). (#210)
* A MIC element (9.4.2.117) with MIC computed as specified in 12.13.8.2.