IEEE P802.11
Wireless LANs

|  |
| --- |
| LB274 CID Resolutions  |
| Date: 2023-07-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Okan Mutgan | Nokia |  |  | okan.mutgan@nokia-sbell.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions and discussions for the following CIDs on 802.11bh D1.0:

82, 83, 84, 85, 86, 87, 111, 112, 113

R0. Initial Version

aa

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed Change | Resolution |
| 82 | 30 | 53 | The sentence says "3) When not using FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake."The sentence should say "When not using FILS or PASN authentication, ..." | Change the sentence to:3) When not using PASN or FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake. | ACCEPT |
| 83 | 30 | 58 | The sentence says"... the non-AP STA has not previously associated or using PASN ..."It should be "used PASN" because this sentence talks about the first interaction, so non-AP STA has not used PASN before. | Change "using PASN" to "used PASN" | ACCEPT |
| 84 | 30 | 6 | The details of encrypting IRM element in PASN frame 3 and device ID element in PASN frame 2 is missing.. | Add the details of encrypting IRM element in PASN frame 3 and device ID element in PASN frame 2 | Needs further submission. |
| 85 | 36 | 30 | This sentence talks about sending device ID IE encrypted in the second PASN frame (from AP to non-AP STA).In this case, device ID IE should be encrypted.This sentence does not mention encryption. | Change the sentence to:If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as defined in (9.4.2.296a Device ID element), if any. The Device ID element shall be encrypted with the chosen cipher suite. | ACCEPT |
| 86 | 36 | 44 | This subsection talks about the third PASN frame.In the third PASN frame, only IRM element is sent encrypted.No Device ID is sent in the third PASN frame. | Remove this sentence in this subsection:If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as definedin 9.4.2.307a (Device ID element). | ACCEPT |
| 87 | 36 | 48 | This statement talks about sending IRM Element encrypted in the third PASN frame.The cipher suite (AES-128-CMAC) is strictly specified in this statement.It is better not to mention a specific cipher suite. | Change"The IRM element shall be encrypted with the cipher suite of AES-128-CMAC."to"The IRM element shall be encrypted with the chosen cipher suite." | ACCEPT |
| 111 | 30 | 6 | D1.0 does not address some of the scenarios such as TDLS. | If applicable, add support for IRM and/or device ID in TDLS. | Needs durther discussion. |
| 112 | 30 | 6 | In FILS, device ID IE and IRM IE is exchanged in (Re)Association Request and Response.The intention is to send device ID IE and IRM IE encrypted in "FILS Encrypted Data" in (Re)Association Request and Response.No text describes this.(It seems possible to send device ID IE/IRM IE unencrpyted like a normal IE) | Add an explanation to state clearly that device ID IE and IRM IE encrypted in "FILS Encrypted Data" in (Re)Association Request and Response. | ACCEPT |
| 113 | 33 | 37 | for IRM in PASN, AP does not send any IRM IE (or any way) to inform non-AP STA about the identification result (IRM success/fail) | Add a mechanism for IRM in PASN to inform non-AP STA about the identification result (IRM success/fail) | Needs further discussion. |
|  |  |  |  |  |  |

**Proposed Changes**

**1) CID82**

30.53

Original:

3) When not using FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.

Proposed:

3) When not using PASN or FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.

**2) CID83**

30.58

Original:

A non-AP STA that is associating with any AP in an ESS or that is using PASN with any AP in an ESS, when Device ID is active for both the non-AP STA and the AP and the non-AP STA has not previously associated or using PASN with any AP in the ESS, shall not send a device ID in the non-AP STA Identity frame.

Proposed:

A non-AP STA that is associating with any AP in an ESS or that is used PASN with any AP in an ESS, when Device ID is active for both the non-AP STA and the AP and the non-AP STA has not previously associated or using PASN with any AP in the ESS, shall not send a device ID in the non-AP STA Identity frame.

**3) CID85**

36.30

Original:

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

defined in 9.4.2.307a (Device ID element), if any.

Proposed:

If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as defined in (9.4.2.296a Device ID element), if any. The Device ID element shall be encrypted with the chosen cipher suite.

**4) CID86**

36.44

Original:

— If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as defined in 9.4.2.307a (Device ID element).

—If dot11IRMActivated is true, including a IRM element containing an IRM as defined in Figure 9.4.2.307b (IRM element), if any. The IRM element shall be encrypted with the cipher suite of AES-128-CMAC.

Proposed:

—If dot11IRMActivated is true, including a IRM element containing an IRM as defined in Figure 9.4.2.307b (IRM element), if any. The IRM element shall be encrypted with the cipher suite of AES-128-CMAC.

**5) CID87**

36.48

Original:

—If dot11IRMActivated is true, including a IRM element containing an IRM as defined in Figure 9.4.2.307b (IRM element), if any. The IRM element shall be encrypted with the cipher suite of AES-128-CMAC.

Proposed:

—If dot11IRMActivated is true, including a IRM element containing an IRM as defined in Figure 9.4.2.307b (IRM element), if any. The IRM element shall be encrypted with the chosen cipher suite.

**6) CID112**

30.43

Original:

2) When using FILS authentication in the Device ID element in the (Re)Association Request frame.

Proposed:

2) When using FILS authentication in the Device ID element in the (Re)Association Request frame (as part of FILS Encrypted Data).

30.52

Original:

2) When using FILS authentication in the Device ID element in the (Re)Association Response frame.

Proposed:

2) When using FILS authentication in the Device ID element in the (Re)Association Response frame. (as part of FILS Encrypted Data).

32.54

Original:

When associating to an AP that advertises support for IRM, the non-AP STA may allocate a new IRM MAC address to the AP by including an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication, including the IRM element in the Association Response frame.

Proposed:

When associating to an AP that advertises support for IRM, the non-AP STA may allocate a new IRM MAC address to the AP by including an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication, including the IRM element in the Association Response frame (as part of FILS Encrypted Data).

33.8

Original:

When a non-AP STA that advertises support for IRM associates to an AP that advertises support for IRM, the AP shall include an IRM KDE in message 3 of the 4-way handshake or, when using FILS authentication, including an IRM element in the Association Response frame.

Proposed:

When a non-AP STA that advertises support for IRM associates to an AP that advertises support for IRM, the AP shall include an IRM KDE in message 3 of the 4-way handshake or, when using FILS authentication, including an IRM element in the Association Response frame (as part of FILS Encrypted Data).