IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA CR for CID3132 | | | | |
| Date: 2024-05-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Okan Mutgan | Nokia |  |  | okan.mutgan@nokia.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions and discussions for CID3132 on 802.11bh SA ballot:

R0. Initial Version.

R1. Text modifications.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed Change | Resolution |
| 3132 | 39 | 38 | """Section 12.2.13 Encryption of the Encrypted Data field in the PASN Encrypted Data element in  PASN seems to fit under the PASN subclause better (12.13 Preassociation security negotiation).  Move this subsection to PASN subclause (12.13 Preassociation security negotiation) and add a different subsection or note here simply saying that  """"When using PASN authentication, device ID element and IRM element should be carried in the Encrypted Data field of the PASN Encrypted Data element shall be  encrypted in the second PASN frame (if present) and in the third PASN frame (if present), as defined in 12.13.X Encryption of the Encrypted Data field in the PASN Encrypted Data element in  PASN""""""" | As in comment. | REVISED. |

**Discussion**

802.11bh D4.0 defines to encrypt device ID IE and IRM IE in the of payload PASN frame 2 and PASN frame 3 as PASN Encrypted Data element in subsection (see 12.2.13 Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN). This subsection can be applicable to other IEs in other groups in the future. Currently, 12.2.13 is under 12.12. Therefore, this document suggests to move subsection 12.2.13 Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN under PASN section (12.13).

|  |  |
| --- | --- |
| This is the current situation: | This is a more ideal situation (baseline: Revme 5.0): |

**Proposed Changes (Baseline 802.11Revme D5.0):**

**CID3132**

1. *Move the whole subsection “12.2.13 Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN” under “12.13 Preassociation security negotiation” and make the changes as follows:*

12.13 Preassociation security negotiation

…

12.13.1 General

…

12.13.9 Comeback cookies

…

12.13.10 *Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN*

~~When using PASN authentication,~~ the Encrypted Data field of the PASN Encrypted Data element shall be encrypted in the second PASN frame (if present) and in the third PASN frame (if present).

To encrypt the Encrypted Data field of the PASN Encrypted Data, the KEK shall be used, as derived as part of the PTK (see 12.13.7 (PTKSA derivation with PASN authentication)), with the negotiated key wrap algorithm (see Table 12-11 (Integrity and key wrap algorithms)).

If the size of the Encrypted Data field is larger than 254 octets, then the Encrypted Data field shall be encrypted first, then element fragmentation as defined in 10.28.11 (Element fragmentation) shall be performed.

If the Encrypted Data field uses the NIST AES key wrap, then the Encrypted Data field shall be padded before encrypting if the length of the Encrypted Data field is nonzero and less than 16 octets, or if it is not a multiple of 8 octets. The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received PASN Encrypted Data element, the receiver shall ignore this trailing padding.

If the Encrypted Data field uses an AEAD cipher, the Encrypted Data field shall not be padded and the AAD for the encipherment operation shall not be used and the number of AAD components is zero.

1. *Add the following note in* *12.2.12.1 Device ID mechanism as follows:*

When a non-AP STA receives a frame that contains a Device ID Status field in a Device ID KDE or Device ID (sub)element equal to 1, indicating Not Recognized, it shall assume that no shared identity state exists with the AP or ESS (as per the concepts of 12.2.12 (Identifying a non-AP STA with changing MAC address)).

NOTE - When using PASN authentication, the Device ID subelement is included in the the Encrypted Data field of the PASN Encrypted Data element (see 12.13.10 Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN)

1. *Add the following note in* *12.2.12.2 Identifiable random MAC address (IRM) operation as follows:*

NOTE 3—To enhance STA privacy, a non-AP STA ought to change its IRM in each association or PASN preassociation.

NOTE - When using PASN authentication, the IRM subelement is included in the the Encrypted Data field of the PASN Encrypted Data element (see 12.13.10 Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN)

1. *Modify the following sentences in 12.2.12.2 Identifiable random MAC address (IRM) as follows:*

*Original sentences:*

— the AP shall include an IRM KDE in message 3 of the 4-way handshake if executing a 4-way handshake.

— the AP shall include an IRM element in the Association Response frame if using FILS authentication.

— the AP shall include an IRM element in the second PASN frame if using PASN authentication.

If the AP recognizes the IRM used as the TA in the received frame(s) from the non-AP STA, the IRM Status field of the IRM KDE or IRM element is set to indicate Recognized and the IRM field is not present. If the AP does not recognize the IRM, the IRM Status field of the IRM KDE or IRM element is set to indicate Not recognized and the IRM field is not present. The non-AP STA, on receipt of an IRM Status field of value 1, indicating that the AP has not recognized the IRM, may either continue to associate or authenticate using PASN to the AP and optionally provide a new IRM in an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication optionally provide an IRM element in the Association Request frame, or when using PASN authentication optionally provide an IRM element in the third PASN frame, else disassociate/deauthenticate. An AP may set an IRM status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state.

Revised sentences:

— the AP shall include an IRM KDE in message 3 of the 4-way handshake if executing a 4-way handshake.

— the AP shall include an IRM element in the Association Response frame if using FILS authentication.

— the AP shall include an IRM subelement in the second PASN frame if using PASN authentication.

If the AP recognizes the IRM used as the TA in the received frame(s) from the non-AP STA, the IRM Status field of the IRM KDE or IRM (sub)element is set to indicate Recognized and the IRM field is not present. If the AP does not recognize the IRM, the IRM Status field of the IRM KDE or IRM (sub)element is set to indicate Not recognized and the IRM field is not present. The non-AP STA, on receipt of an IRM Status field of value 1, indicating that the AP has not recognized the IRM, may either continue to associate or authenticate using PASN to the AP and optionally provide a new IRM in an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication optionally provide an IRM element in the Association Request frame, or when using PASN authentication optionally provide an IRM subelement in the third PASN frame, else disassociate/deauthenticate. An AP may set an IRM status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state.

1. *Modify the following sentences in 12.13.3.2 PASN frame construction and processing as follows:*

*Original sentences:*

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 dot11RSNAOperatingChannelValidation-Activated is true.

— If dot11DeviceIDActivated is true, including a PASN Encrypted Data element and a Device ID subelement as defined in 9.4.2.316 (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 12.2.13 (Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN).

— if dot11IRMActivated is true, including a PASN Encrypted Data element and an IRM subelement as defined in 9.4.2.317 (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 12.2.13 (Encryption of the Encrypted Data field in the 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 construction 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 dot11IRMActivated is true, including a PASN Encrypted Data element and an IRM element as defined in 9.4.2.317 (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 12.2.13 (Encryption of the Encrypted Data field in the PASN Encrypted Data

element in PASN).

*Revised sentences:*

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 dot11RSNAOperatingChannelValidation-Activated is true.

— If dot11DeviceIDActivated is true, including a PASN Encrypted Data element and a Device ID subelement as defined in 9.4.2.316 (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 12.13.10 (Encryption of the Encrypted Data field in the PASN Encrypted Data element in PASN).

— if dot11IRMActivated is true, including a PASN Encrypted Data element and an IRM subelement as defined in 9.4.2.317 (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 12.13.10 (Encryption of the Encrypted Data field in the 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 construction 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 dot11IRMActivated is true, including a PASN Encrypted Data element and an IRM subelement as defined in 9.4.2.317 (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 12.13.10 (Encryption of the Encrypted Data field in the PASN Encrypted Data

element in PASN).