IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA CR for some CIDs | | | | |
| Date: 2024-07-14 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Okan Mutgan | Nokia |  |  | okan.mutgan@nokia.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions and discussions for CID4000 and CID4001 on 802.11bh SA ballot:

R0. Initial Version.

R1. Added PASN ID text for Authentication Frame 1 for PASN.

R2. Further text modification.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed Change | Resolution |
| 4000 | 56 | 22 | [On behalf of Yan Li]In the first part of figure AG-2, association response is not cipher text, because the PMKSA and PTKSA can't be generated until the EAP exchange and 4-HS complete.Therefore, the device ID and PASN ID can not be carried in the assoc response. | remove EAP exchange and 4-HS from the first part and optionally add clarification for the type of FILS auth(Public key with PFS) for auth frame of the first part | REVISED. |
| 4001 | 54 | 21 | Example text and figures for FILS do not match the current FILS procedure, therefore, need modifications. | Modify the text and figures for FILS (both for device ID and IRM) to match FILS procedure. | REVISED. |

**Discussion**

FILS has three modes:

1.shared key with PFS 2.shared key without PFS 3.public key with PFS

For mode 1 or 2,

in the initial connection, non-AP STA goes to 4-way HS and EAP. Assoc req/resp is not encrypted. Device ID/IRM can be (should be) carried in 4-way HS.

In later connection, non-AP STA does not go to 4-way HS and EAP. Assoc req/resp is encrypted. Device ID/IRM can be (should be) carried in Assoc req/resp.

For mode 3,

non-AP STA never goes to 4-way HS and EAP. Assoc req/resp is always encrypted. Device ID/IRM can be (should be) carried in Assoc req/resp.

In this regard, Figure AG-2—Example of device ID exchange in FILS and Figure AG-5—Example of IRM exchange in FILS are not consistent with any of the modes and explanation in 12.2.13 Identifying a non-AP STA with changing MAC address.



Figure AG-2—Example of device ID exchange in FILS



Figure AG-5—Example of IRM exchange in FILS

More specifically:

If mode 1 or mode 2 is referred, in the initial connection, device ID/IRM should be exchanged during 4-way Handshake (as opposed to Assoc Req/Resp in the figures).

If mode 3 is referred, in the initial connection, there should not be 4-way Handshake messages.

Therefore, this document suggests,

* Refer to mode 3 in these examples
* Remove 4-way Handshake and EAP messages from the figure
* Keep device ID/IRM exchange in Assoc Req/Resp

**Proposed Changes**

**CID3131**

*Modify the following sentences and replace Figure AG-2—Example of device ID exchange in FILS and Figure AG-5—Example of IRM exchange in FILS in Annex AG Examples of device ID and IRM usage:*

Figure AG-2 shows an example of a device ID exchange when a non-AP STA associates to APs (AP-1 and AP-2 belonging to the same ESS) using FILS public key with PFS.

… After the FILS authentication frame exchange, the non-AP STA indicates its activation of device ID by setting the Device ID Active field in the RSNXE to 1 in the Association Request.

… (Notice the device ID activation from AP-2 via Association Response frame as well).

*To Editor: Figure AG-2—Example of device ID exchange in FILS should be replaced with the following figure*



Figure AG-5 shows an example of an IRM exchange when a non-AP STA associates to APs (AP-1 and AP-2 belonging to the same ESS) using FILS public key with PFS.

*To Editor: Figure AG-5—Example of IRM exchange in FILS should be replaced with the following figure*



*Change the following row in Table 9-71 (Presence of fields and elements in Authentication frames) as*

*shown (header row shown for convenience)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication**  **algorithm** | **Authentication**  **transaction**  **sequence number** | **Status Code** | **Presence of fields and elements**  **indicated as conditional in Table 9-70**  **(Authentication frame body)** |
| PASN  Authentication | 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 ID element is optionally present. |
| PASN  Authentication | 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.  PASN Encrypted Data element is optionally  present.  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. |
| PASN  Authentication | 3 | Status | PASN Parameters element is present if Status Code  field is 0.  Wrapped Data element is present if wrapped data  format in PASN Parameters element is nonzero and  not reserved; and Status Code field is 0.  PASN Encrypted Data element is optionally  present.  MIC element is present.  Fragment element may be present if any of the  elements are fragmented and Status Code field is 0. |