IEEE P802.11
Wireless LANs

|  |
| --- |
| SA CR for CID3131 |
| 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 CID3131 on 802.11bh SA ballot:

R0. Initial Version.

R1. Some modification

* Multiple APs added to the examples (covering ESS)
* “IE” removed
* PASN frame re-named
* Relevant text modified
* KEK activation is removed (since KEK is more relevant to PASN rather than RCM)
* Informative text format added
* Device ID and IRM exchange together added

R2. PASN ID added.

R3. Modified text and figures for PASN ID.

R4. Further modifications on the figures and text.

R5. A small modification on AX.3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed Change | Resolution |
| 3131 | 37 | 42 | Draw example figures of the signaling for IRM and device ID, preferably each mechanism with identifier recognized or not recognized. (Previous letter ballot consists of several comments that are not completely clear about the signaling procedures) | As in comment. | REVISED. |

**Discussion**

This is the current figure of device ID exchange in PASN:



This document proposes additional figures and also some modification for the current figure 12-0a.

**Proposed Changes**

**CID3131**

*Add the following sentence in 12.2.12 Identifying a non-AP STA with changing MAC address:*

The two mechanisms, device ID and IRM, both allow the network to recognize the STA while mitigating the abilities of third parties to do traffic analysis and tracking of the non-AP STA.

The two mechanisms, device ID and IRM, may be used concurrently.

Annex AX provides illustrative examples of the usage of device ID and IRM.

*Remove the following paragraph and Figure 12-0a—Example of device ID exchanges in PASN:*

Figure 12-0a (Example of device ID exchanges in PASN) shows an example of a device ID exchange in

PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS

containing AP1 and AP2. The non-AP STA with a MAC address of MAC1 first initiates the connection with AP1 by sending the first PASN frame with the Device ID Active field in the RSNXE set to 1. Upon receiving the first PASN frame, AP1 assigns a device ID (devID1) and sends it to the non-AP STA in the second PASN frame. The non-AP STA then continues to establish an FTM session with AP1. When the non-AP STA with a MAC address of MAC2 (non-AP STA changing its MAC from MAC1 to MAC2) performs PASN with AP2 to establish another FTM session, the non-AP STA sends previously assigned device ID (devID1) to AP2 in the first PASN frame. Upon receiving the device ID (devID1) in first PASN frame, AP2 assigns another device ID (devID2) and sends it to the non-AP STA in the second PASN frame. The non-AP STA then proceeds to establish the FTM session. Similarly, when the non-AP STA with a MAC address of MAC3 returns to AP1, it sends the previously assigned device ID (devID2) and is assigned another device ID (devID3) that will be used in the subsequent PASN for another FTM session.



*Create Annex AX and put the following text and figures as follows:*

**Annex AX
(informative) Examples of device ID and IRM usage**

**AX.1 – Examples of device ID usage**

Figure AX-1 shows an example of a device ID exchange when a non-AP STA authenticates and associates to APs (AP-1 and AP-2 belonging to the same ESS) using the 4 way handshake. The AP-1 and AP-2 advertise their support of device ID in the RSNXE in Beacons and Probe Responses. The non-AP STA with a MAC address of MAC1 initiates the first connection with AP-1, i.e., the non-AP STA does not have a device ID for that AP/ESS). After the 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. Similarly, the AP-1 indicates its activation of device ID by setting the Device ID Active field in the RSNXE to 1 in Association Response. In 4-way Handshake Message 3, the AP-1 includes a device ID KDE and PASN ID KDE and assigns a device ID (devID) and a PASN ID(pasnID1) to the non-AP STA. Non-AP STA, AP-1, and AP-2 store devID and pasnID1.

Later the non-AP STA terminates the connection with the AP-1.

The non-AP STA then returns to that same ESS using a different MAC address (MAC2), again indicating activation of device ID in the Association Request/Response frame exchange. The non-AP STA then provides the previously assigned device ID (devID) to AP-2 in a device ID KDE in 4-way Handshake Message 2. The AP-2 identifies the non-AP STA from the device ID (devID) despite the non-AP STA using a randomized MAC address (MAC2). The AP-2 then sends a device ID KDE in 4-way Handshake Message 3 with the Status field set to 0 indicating that the device ID has been recognized.

The AP-2 does not allocate a new device ID in the device ID KDE sent in 4-way Handshake Message 3, implying that the same device ID(devID) will be used subsequently.



Figure AX-1 – Example of device ID exchange in 4-way Handshake

Figure AX-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. The AP-1 and AP-2 advertise their support of device ID in the RSNXE in Beacons and Probe Responses. The non-AP STA with a MAC address of MAC1 initiates the first connection with AP-1, i.e., the non-AP STA does not have a device ID for that AP/ESS. After the 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. Similarly, the AP-1 indicates its activation of device ID by setting the Device ID Active field in the RSNXE to 1 in the FILS Association Response. In the FILS Association Response, the AP-1 includes Device ID element and PASN ID elementand assigns a device ID (devID1) and a PASN ID (pasnID1) to the non-AP STA. Non-AP STA, AP-1, and AP-2 store devID1 and pasnID1.

Later the non-AP STA terminates the connection with the AP-1.

The non-AP STA then returns to that same ESS using a different MAC (MAC2), non-AP STA again indicating activation of device ID in the Association Request. The non-AP STA then provides the previously assigned device ID (devID1) to AP-2 in a Device ID element in the FILS Association Request. Because of devID1, The AP-2 identifies the non-AP STA from the device ID (devID1) despite the non-AP STA using a randomized MAC address (MAC2). The AP-2 then sends a device ID element in the FILS Association Response with the Status field set to 0 indicating that the device ID has been recognized. (Notice the device ID activation from AP-2 via Association Response frame as well).

In the Figure AX-2, the AP-2 optionally allocates a new device ID (devID2) and a PASN ID (pasnID2) in the device ID element and in the PASN ID element sent in the FILS Association Response.



Figure AX-2 – Example of device ID exchange in FILS

Figure AX-3 shows an example of a device ID and PASN ID exchange in PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS containing AP-1 and AP-2. AP-1 and AP-2 advertise their support of device ID in the RSNXE in Beacons and Probe Responses. The non-AP STA with a MAC address of MAC1 first initiates the connection with AP-1 by sending the first PASN frame with the Device ID Active field in the RSNXE set to 1 and without a PASN ID. Upon receiving the first PASN frame, AP1 indicates its activation of device ID by setting the Device ID Active field and PASN ID Active in the RSNXE to 1. AP-1 then assigns a device ID (devID) and a PASN ID (pasnID1), and sends them to the non-AP STA in the Device ID field in the Device ID subelement and in the PASN ID field in the PASN ID subelement in the PASN Ecrypted Data element in the second PASN frame. Non-AP STA, AP-1 and AP-2 store devID and pasnID1. The non-AP STA then continues to establish an FTM session with AP-1. When the non-AP STA, now using a MAC address of MAC2 (non-AP STA changing its MAC from MAC1 to MAC2), performs PASN with AP-2 to establish another FTM session, the non-AP STA sends the previously assigned PASN ID (pasnID1) to AP-2 in the PASN ID field in an PASN ID element in the first PASN frame. AP-2 identifies the non-AP STA from the PASN ID (pasnID1) despite the non-AP STA using a randomized MAC address (MAC2). Upon receiving the PASN ID (pasnID1) in first PASN frame, AP-2 sends a PASN ID subelement in the PASN Ecrypted Data element in the second PASN frame with the PASN ID status field set to 0, indicating that the PASN ID has been recognized. AP-2 then assigns another PASN ID (pasnID2) and sends it to the non-AP STA in the PASN ID field in the PASN ID subelement included in the PASN Ecrypted Data element in the second PASN frame. The non-AP STA then proceeds to establish the FTM session. Similarly, when the non-AP STA with a MAC address of MAC3 returns to AP-1, it sends the previously assigned PASN ID (pasnID2) and is assigned another PASN ID (pasnID3) that will be used in the subsequent PASN for another FTM session.



Figure AX-3 – Example of device ID and PASN ID exchange in PASN

**AX.2 – Examples of IRM usage**

Figure AX-4 shows an example of a IRM exchange when a non-AP STA authenticates and associates to APs (AP-1 and AP-2 belonging to the same ESS) using the 4 way handshake. The AP-1 and AP-2 advertis their support of IRM in the RSNXE in Beacons and Probe Responses. The non-AP STA with a MAC address of MAC1 initiates a first connection with the AP-1, i.e., the non-AP STA has not previously provided an IRM to that AP/ESS. After the authentication frame exchange, the non-AP STA indicates its activation of IRM via by setting the IRM Active field in the RSNXE to 1 in the Association Request. Similarly, the AP-1 indicates its activation of IRM by setting IRM Active field in the RSNXE to 1 in the Association Response. In 4-way Handshake Message 4, the non-AP STA includes an IRM KDE and provides an IRM (IRM1) to the AP-1. The non-AP STA, AP-1, and AP-2 store that IRM (IRM1). Later the non-AP STA terminates the connection with the AP-1.

When non-AP STA returns to that same ESS, the non-AP STA uses IRM1 as its MAC address. The AP-2 identifies the non-AP STA from the stored IRM1. The AP-2 then sends an IRM KDE in 4-way Handshake Message 3 with the Status field set to 0 indicating that the IRM has been recognized. The non-AP STA then provides another IRM (IRM2) to the AP-2 in an IRM KDE in 4-way Handshake Message 4.



Figure AX-4 – Example of IRM exchange in 4-way Handshake

Figure AX-5 shows an example of a IRM exchange when a non-AP STA associates to APs (AP-1 and AP-2 belonging to the same ESS) using FILS. The AP-1 and AP-2 advertise their support of IRM in the RSNXE in Beacons or Probe Responses. The non-AP STA with a MAC address of MAC1 initiates a first connection with AP-1 i.e., the non-AP STA has not previously provided an IRM to that AP/ESS. After the FILS authentication frame exchange, the non-AP STA indicates its activation of IRM by setting the IRM Active field in the RSNXE to 1 in the FILS Association Request. In Association Request, non-AP STA assigns an IRM (IRM1) to itself in IRM element. AP-1 also indicates its activation of IRM by setting the IRM Active field in the RSNXE to 1 in the FILS Association Response. The non-AP STA, AP-1, and AP-2 store IRM1. Later the non-AP STA terminates the connection with the AP-1.

When non-AP STA returns to that same ESS, the non-AP STA uses IRM1 as its MAC address. The AP-2 identifies the non-AP STA from the stored IRM1. The AP-2 then sends an IRM element in the Association Response with the Status field set to 0 indicating that the IRM has been recognized. The non-AP STA also provides another IRM (IRM2) to the AP-2 in an IRM element in FILS Association Request.



Figure AX-5 – Example of IRM exchange in FILS

Figure AX-6 shows an example of a IRM exchange in PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS containing AP-1 and AP-2. AP-1 and AP-2 advertise their support of IRM in the RSNXE in Beacons and Probe Responses. The non-AP STA with a MAC address of MAC1 first initiates the connection with AP-1 by sending the first PASN frame with the IRM Active field in the RSNXE set to 1. Upon receiving the first PASN frame, AP-1 indicates its activation of IRM by setting the IRM Active field in the RSNXE to 1. In the third PASN frame, the non-AP STA provides an IRM (IRM1) to AP-1 sending it to AP1 in the IRM field in an IRM subelement in the PASN Ecrypted Data element. The non-AP STA, AP-1 and AP-2 store IRM1. The non-AP STA then continues to establish an FTM session with AP-1. When the non-AP STA performs PASN with AP-2 to establish another FTM session, the non-AP STA uses IRM1 as its MAC address. AP-2 identifies the non-AP STA from the stored IRM1. Upon receiving IRM1 in first PASN frame, AP-2 may send an IRM subelement in the PASN Ecrypted Data element in the second PASN frame with the IRM status field set to 0, indicating that the IRM has been recognized. The non-AP STA then provides another IRM (IRM2) to AP-2 in the IRMfield in an IRM subelement in PASN Ecrypted Data element in the third PASN frame. Similarly, when the non-AP STA returns to AP-1, it uses the previously assigned IRM (IRM2) as its MAC address and provides another IRM (IRM3) that will be used in the subsequent PASN for another FTM session.



Figure AX-6 – Example of IRM exchange in PASN

**AX.3 – Example of device ID and IRM usage**

Figure AX-7 shows an example of a simultaneous exchange of device ID and IRM in 4-way Handshake for APs (AP-1 and AP-2 belonging to the same ESS). The AP-1 and AP-2 advertise their support of device ID and IRM in the RSNXE in Beacons and Probe Responses. The non-AP STA with a MAC address of MAC1 initiates the first connection with AP-1, i.e., the non-AP STA does not have a device ID and IRM for that AP/ESS. After the authentication frame exchange, the non-AP STA indicates its activation of device ID and IRM by setting the Device ID Active field and IRM Active field in the RSNXE to 1 in the Association Request. Similarly, the AP-1 indicates its activation of device ID and IRM by setting the Device ID Active field and and IRM Active field in the RSNXE to 1 in Association Response. In 4-way Handshake Message 3, the AP-1 includes a device ID KDE and PASN KDE and assigns a device ID (devID) and pasn ID (pasnID1) to the non-AP STA. In 4-way Handshake Message 4, the non-AP STA includes an IRM KDE and provides an IRM (IRM1) to the AP-1. The non-AP STA, AP-1, and AP-2 store devID, pasnID1, and IRM1.

Later the non-AP STA terminates the connection with the AP-1.

When non-AP STA returns to that same ESS, the non-AP STA uses IRM1 as its MAC address. The AP-2 identifies the non-AP STA from the stored IRM1. The AP-2 then sends an IRM KDE in 4-way Handshake Message 3 with the Status field set to 0 indicating that the IRM has been recognized. The non-AP STA then provides another IRM (IRM2) to the AP-2 in an IRM KDE in 4-way Handshake Message 4. Also, the non-AP STA exchanges device ID (devID) in 4-way Handshake Message 3 and 4.

Later the non-AP STA terminates the connection with the AP-2.

When non-AP STA returns to that same ESS, the non-AP STA uses IRM2 as its MAC address. The AP-2 identifies the non-AP STA from the stored IRM2. The AP-2 then sends an IRM KDE in 4-way Handshake Message 3 with the Status field set to 0 indicating that the IRM has been recognized. Also, the non-AP STA exchanges device ID (devID) in 4-way Handshake Message 3 and 4.



Figure AX-7 – Example of device ID exchange and IRM exchange in 4-way Handshake