IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bh D0.2 CR for device ID in PASN |
| Date: 2023-4-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Okan Mutgan | Nokia |  |  | okan.mutgan@nokia-sbell.com |
| Jay Yang | Nokia |  |  | zhijie.yang@nokia-sbell.com |

Abstract

This submission proposes resolutions for device ID support for PASN in P802.11bh/D0.2:

Revisions:

Rev 0: Initial version of the document.

Rev 1: Modification based on the previous discussion (reduced to one option where device ID is exchanged in Auth Msg2 and Auth Msg3 encrypted)

Rev 2: Modification based on 22/1329r17 and 23/0129r4.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbh D0.2 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbh D0.2 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbh Editor: Editing instructions preceded by “TGbh Editor” are instructions to the TGbh editor to modify existing material in the TGbh draft. As a result of adopting the changes, the TGbh editor will execute the instructions rather than copy them to the TGbh Draft.***

**Discussion**

Based on the previous discussion, to support PASN use case, this document proposes that AP/ESS and non-AP STA should exchange device ID encrypted in PASN authentication:

- AP/ESS should assign device ID to non-AP STA encrypted in Auth Msg2

- non-AP STA should use the assigned device ID encrypted in Auth Msg3

Note:

1) Device ID IE encryption is possible for PASN Authentication Msg2 and Authentication Msg3

2) To fully cover the use case, encypted device ID should be exchanged

- for each FTM session and

- for each return to the same ESS

Example Scenario:

Non-AP STA is assigned unique Device ID in each Auth Msg2.

Non-AP STA uses different MAC addresses (MAC1, MAC2, MAC3, MAC4) for each FTM session session and for each returning to the same ESS (AP1 & AP2), and uses previously assigned Device ID in each Auth Msg3.

Device ID is encrypted differently in each PASN Auth Msg2 and Auth Msg3, so no exposing it to third parties (see green color for third party exposure).



**Proposed Text**(Proposed text modifications are based on Draft 11bh 0.2 and 802.11az-2022)

***TGbh editor:******Modify the subclause 12.2.11 Device ID indication*** *as follows:*

Note to Editor: This text is taken from of 22/1329r17 and 23/0129r4 therefore, the proposed text is based on these documents.

 **12.2.11 Device ID indication**

A non-AP STA indicates activation of device ID for a particular ESS by setting the Device ID Active field to 1 in the Extended RSN Capabilities field (see 9.4.2.241 - RSNExtension Element) in (Re)Association Request frames sent to any AP in the ESS. An AP indicates activation of Device ID by setting the Device ID Active field to 1 in the Extended RSN Capabilities field in Beacon, (Re)Association Response, and Probe Response frames. All APs in a given ESS shall set this field to the same value.

A STA shall not send a device ID to any STA that does not indicate Device ID is active.

A non-AP STA shall send a device ID when required by the procedures described below via the following frames (known as “non-AP STA Identity frames”):

1. When using FILS authentication in the Device ID element in the (Re)Association Request frame.
2. When not using FILS authentication in the Device ID KDE in message 2 of the 4 way handshake.
3. When using PASN authentication in the Device ID element in the third PASN Authentication frame.

An AP shall send a device ID when required by the procedures described below via the following frames (known as “AP Identity frames”):

1. When using FILS authentication in the Device ID element in the (Re)Association Response frame.
2. When not using FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.
3. When using PASN authentication in the Device ID element in the second PASN Authentication frame.

A non-AP STA that is associating with any AP in an ESS or that 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 used PASN with any AP in the ESS, shall not send a device ID in the non-AP STA Identity frame. Similarly, if the non-AP STA is associating with any AP in an ESS or that using PASN with any AP in an ESS, when Device ID is active for both the non-AP STA and the AP but the non-AP STA no longer has a device ID for that ESS for implementation-specific reasons (for example, configuration changes have lost the device ID, or sufficient time has passed since the last association to the ESS so that the device ID has been deleted), then the non-AP STA shall not send a device ID in the non-AP STA Identity frame.

A non-AP STA that is associating or using PASN with any AP in an ESS with Device ID active for both the non-AP STA and the AP and the non-AP STA has a saved device ID for the ESS shall send the most recently received device ID for that ESS in the non-AP STA Identity frame.

When an AP with Device ID active receives a non-AP STA Identity frame from a non-AP STA with Device ID active and the received device ID is recognized, the AP shall perform one of the following actions:

1. Send a zero-length device ID and set Identifier Status to “Recognized” in the appropriate AP Identity frame.
2. Assign a new device ID to the non-AP STA, send the device ID, and set Identifier Status to “Recognized” in the appropriate AP Identity frame.

When a non-AP STA receives an AP Identity frame with Identifier Status equal to “Recognized” it can proceed with the assumption that the shared identity state with the AP or ESS (as per the concepts of 12.2.10) is now bound to the non-AP STA’s current MAC address.

When a non-AP STA receives an AP Identity frame with the Identifier Status equal to “Not Recognized”, it must assume that no shared identity state exists with the AP or ESS (as per the concepts of 12.2.10) and the non-AP STA must (re)establish any desired, shared identity state per the procedures previously described.

***TGbh editor: Modify the subclause 12.12.3.2 PASN Frame Construction and Processing*** *as follows:*

**12.12.3.2 PASN Frame Construction and Processing**

**The AP begins the construction the second PASN frame** as follows:

— 9.4.1.1 (Authentication Algorithm Number field) set to 7 (PASN Authentication)

— 9.4.1.2 (Authentication Transaction Sequence Number field) set to 2

— Status code indicating the processing status

…..

— Optionally including 9.4.2.48 (Timeout Interval element (TIE)) with Timeout Interval 18 Value set to dot11RSNAConfigPASNPTKSATimeout and Timeout Interval Type set to 2 (key lifetime interval).

— Including RSNXE (9.4.2.241 RSN Extension Element (RSNXE)) that is advertised in AP’s Beacon and Probe Response frames, if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.

— 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 — 9.4.2.118 (A MIC element) with MIC computed as specified in 12.12.8.1 (MIC computation for PASN second frame.

— If dot11DeviceIDActivated is true, including a Device ID element contains a device identifier as defined in (9.4.2.296a Device ID element). The Device ID element shall be encrypted with the cipher suite of AES-128-CMAC.

— 9.4.2.118 (A MIC element) with MIC computed as specified in 12.12.8.1 (MIC computation for PASN second frame)

**Otherwise the STA begins the construction the third PASN frame** as follows:

— 9.4.1.1 (Authentication Algorithm Number field) set to 7 (PASN Authentication)

— 9.4.1.2 (Authentication Transaction Sequence Number field) set to 3

— Status code indicating success

….

— 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 contains a device identifier as defined in (9.4.2.296a Device ID element), if any. The Device ID element shall be encrypted with the cipher suite of AES-128-CMAC.

— 9.4.2.118 (A MIC element) with MIC computed as specified in 12.12.8 (MIC computation for PASN third frame)