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 the following CIDs in P802.11bh/D0.2:

CID19 and CID20

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)

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.***

 **Comments:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Comment** | **Proposed Change** | **Resolution** |
| 19 | Jonathan Segev | It is not clear how the Device ID mechanism supports unassociated PASN operation.the PASN operation is required to support management procedure that do not requiredata transfer, examples are FTM and 11ba. | Add support for Device ID in PASN. |   |
| 20 | Jonathan Segev | The mechanism for device ID should be such that to a single network a devicewith an on going unassociated session should be identifiable as single deviceto the network (ESS).an example of such operation is the need to two way report for FTM;The client STA reports measurement conducted to each individual AP while themultiple outstanding FTM sessions are in progress, the NW is able to associate the measurement frommultiple sessions to be attributed to a single client and thus can identify client location.This client may not be associated to the network. | Add a functionality that allows a device to be identified to the ESS as a single entity. |  |

**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 and CID, 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:*

 **12.2.11 Device ID indication**

When using FILS authentication, the non-AP STA sends the identifier, if it has one and opts-in to using it, in the Association Request frame and the AP sends a new identifier in the Association Response frame.

When using FT, the non-AP STA sends the identifier, if it has one and opts-in to using it, during the initial mobility domain association the EAPOL-Key message 2/4 and the AP sends a new identifier in the EAPOL-Key message 3/4; the identifier or a new identifier are not exchanged during the FT protocol reassociations within the same ESS.

When using PASN authentication, the non-AP STA sends the *identifier*, if it has one and opts-in to using it, in the third PASN frame and the AP sends a new *identifier* in the second PASN frame.

For other cases, the non-APSTA sends the identifier, if it has one and opts-in to using it, during the initial 4-way handshake in the EAPOL-Key message 2/4 and the AP sends a new identifier in the EAPOL-Key message 3/4.

***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). And the Device ID element shall be encrypted.

— 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. And the Device ID element shall be encrypted.

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