IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11bh D0.2 CR for device ID in PASN | | | | |
| Date: 2022-10-25 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Okan Mutgan | Nokia |  |  |  |
| Jay Yang | Nokia |  |  |  |

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.

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 require data 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 device  with an on going unassociated session should be identifiable as single device  to 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 the  multiple outstanding FTM sessions are in progress, the NW is able to associate the measurement from  multiple 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**

The current P802.11bh/D0.2 assigns/provides device ID as a Device ID IE in Association request/response frames for FILS or as a Device ID KDE otherwise.  
PASN for un-associated non-AP STA only exchanges three authentication frames, and never goes into Association and 4-way handshake frame exchange. Therefore, un-associated non-AP STA in PASN does not obtain Device ID.  
To mitigate this problem, this resolution proposes to exchange device ID in PASN Authentication frames.

**Proposed Text**(Proposed text modifications are based on Draft 11bh 0.2 and Draft 11az 7.0)

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

**Option 1:**

**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 first 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.

**Option 2:  
  
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:*

**Option 1:**

**12.12.3.2 PASN Frame Construction and Processing**

**The first PASN Authentication frame** (see 9.3.3.11 (Authentication frame format)) of the exchange is constructed 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 1;

— Including the constructed RSN

— Including 9.4.2.303 (PASN Parameters Element) with the wrapped data format, chosen 3 finite cyclic group ID, and the ephemeral public key. Comeback field shall either be absent 4 or set to the cookie length and the cookie received from the AP if the authentication is 5 being retried. Comeback After subfield shall not be present in the Comeback field. The 6 Control field in the element is set appropriately to indicate the presence or absence of fields 7 in the element.

— Including 9.4.2.187 (FILS Wrapped Data Element) corresponding to Base AKMP data, if any. This element may be fragmented using mechanism specified in 10.28.11 (Element fragmentation) as necessary;

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

— Including RSNXE (9.4.2.241 RSN Extension Element (RSNXE)) 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 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 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

— 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)

**Option 2:**

**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)