IEEE P802.11
Wireless LANs

|  |
| --- |
| STA generated Device ID |
| Date: 2022-01-21 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposes a minimal P802.11bh mechanism for a non-AP STA to be able to optionally provide the AP an arbitrary identifier using existing frames and encryption functionality to protect the exchange from third parties. The arbitrary identifier could be the globally unique MAC address of the non-AP STA (i.e., an opt-in mechanism for the non-AP STA to tell the network its persistent MAC address to restore functionality that was prevented by the need to randomize and frequently change the over-the-air MAC addresss) or a semi-persistent per-ESS identifier generated by the non-AP STA (i.e., an opt-in mechanism with a smaller scope and duration to enable the authorized network to recognize and track the non-AP STA across multiple sessions).

# Discussion

This mechanism assumes that RSN is used. If authentication is not needed, OWE can be used to allow this mechanism to be used with RSN. The non-AP STA is in control of when to send its identifier and what is encoded in that identifier. For some use cases, this identifier could be the globally unique MAC address of the STA. For some other cases, it might be a random value generated for connections to the specific ESS. For the identifier to be useful, the value should be selected in a manner that is likely to result in a unique value between the STAs connected to the ESS at the same time.

When using FILS authentication, the identifier is sent in the (Re)Association Request frame. When using FT, the identifier is sent during the initial mobility domain association EAPOL-Key msg 4/4, but not during the FT protocol reassociations within the same ESS. For other cases, the identifier is sent during the initial 4-way handshake EAPOL-Key msg 4/4.

The new extended capability bit is used to decide when the Device ID can be sent. In theory, this might not be needed, but taken into account past issues with RSN extensions with deployed devices, it feels better to do this to not surprise the AP with the new KDE in EAPOL-Key msg 4/4 which previously did not normally contain anything in the Key Data field.

# Proposed text changes

*Note to editor: Text changes are shown against REVme/D1.0.*

* Association Request frame format

*Add a new row into Table 9-62 (Association Request frame body) as shown below:*

|  |
| --- |
| * Association Request frame body
 |
| Order | Information | Notes |
| ... | ... | ... |
| 57 | WUR Mode | The WUR Mode element is optionally present when dot11WUROptionImplemented is true; otherwise, it is not present. |
| 58 | Device ID | The Device ID element is optionally present when using FILS authentication; otherwise, it is not present. |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

* Reassociation Request frame format

*Add a new row into Table 9-64 (Reassociation Request frame body) as shown below:*

|  |
| --- |
| * Reassociation Request frame body
 |
| Order | Information | Notes |
| ... | ... | ... |
| 61 | WUR Mode | The WUR Mode element is optionally present when dot11WUROptionImplemented is true; otherwise, it is not present. |
| 62 | Device ID | The Device ID element is optionally present when using FILS authentication; otherwise, it is not present. |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

* Elements
* General

*Add a new row into Table 9-128 (Eelement IDs) as shown below:*

|  |
| --- |
| * Element IDs
 |
| Element | Element ID | Element ID Extension | Extensible | Fragmentable |
| ... | ... | ... | ... | ... |
| Anti-Clogging Token Container (see 9.4.2.247 (Anti-Clogging Token Container element)) | 255 | 93 | No | No |
| Device ID (see 9.4.2.x (Device ID element) | 255 | <ANA> | No | No |
| Reserved | 255 | 94–255 |  |  |
| NOTE—See 10.28.6 (Element parsing) on the parsing of elements. |

* Extended Capabilities element

*Add a new row into Table 9-190 (Extended Capabilities field) as shown below:*

|  |
| --- |
| * Extended Capabilities field
 |
| Bit | Information | Notes |
| ... | ... | ... |
| 89 | TWT Parameters Range Support | Set to 1 to indicate support for reception of a TWT Setup frame that contains two TWT elements (see 10.47.9 (TWT parameter ranges)); otherwise, set to 0. |
| <ANA> | Device ID Support | Set to 1 to indicate support for Device ID indication; otherwise, set to 0. |
| 88, 90–*n* | Reserved |  |

9.4.2.296 Device ID element

*Add a new subclause after 9.4.2.295 (i.e., at the end of the 9.4.2 subclauses):*

The Device ID element contains a device identifier. The format of the Device ID element is shown in Figure 9-1002a (Device ID element format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | Device ID |
| Octets: | 1 | 1 | 1 | variable |
| Figure 9-1002a—Device ID element format |

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The Device ID corresponds to the arbitrary identifier for the STA sending this element.

12.2.11 Device ID indication

*Add a new subclause after 12.2.10 (i.e.,immediately before 12.3):*

A non-AP STA may provide its persistent or semi-persistent identifier to the AP when using RSN. For some use cases, this identifier might be the globally unique MAC address of the STA. For some other cases, it might be a random value generated for connections to the specific ESS. For the identifier to be useful, the value should be selected in a manner that is likely to result in a unique value between the STAs connected to the ESS at the same time.

When using FILS authentication, the identifier is sent in the (Re)Association Request frame. When using FT, the identifier is sent during the initial mobility domain association EAPOL-Key msg 4/4, but not during the FT protocol reassociations within the same ESS. For other cases, the identifier is sent during the initial 4-way handshake EAPOL-Key msg 4/4.

The non-AP STA may send the Device ID element or the Device ID KDE if the AP indicates support for Device ID in the Extended Capabilities element. Otherwise, the non-AP STA shall not send the Devicde ID element or the Device ID KDE.

* EAPOL-Key frames

*Add a new row into Table 12-10 (KDE selectors) as shown below:*

|  |
| --- |
| * KDE selectors
 |
| OUI | Data type | Meaning |
| 00-0F-AC | 0 | Reserved |
| ... | ... | ... |
| 00-0F-AC | 15 | WIGTK KDE |
| 00-0F-AC | <ANA> | Device ID KDE |
| 00-0F-AC | 16–255 | Reserved |
| Other OUI or CID | Any | Vendor specific |

*Add the following description of the new KDE at the end of 12.7.2 (P3212 L55) as shown below:*

|  |
| --- |
| * WIGTK KDE
 |

The WIPN corresponds to the WIPN value that was used for computing the MIC in the last protected broadcast or group addressed WUR Wake-up frame and it is used by the receiver as the initial value for the BIP replay counter for the WIGTK.

The format of the Device ID KDE is shown in Figure 12-48a (Device ID KDE format).

|  |  |
| --- | --- |
|  | Device ID |
| Octets: | variable |

Figure 12-48a—Device ID KDE format

The Device ID corresponds to the arbitrary identifier for the STA sending this KDE.

NOTE—A globally unique MAC address or a per-ESS persistent identifier for the STA might be used as the Device ID.

* EAPOL-Key frame notation

*Modify 12.7.4 (P3215 L25) as shown below:*

 OCI KDE is a KDE containing operating channel information

 Device ID KDE is a KDE containing device identifier

 RSNXE is described in 9.4.2.241 (RSN Extension element (RSNXE))

 PMKID identifies the PMKSA selected by the Authenticator

 “{a} or {b}” means that exactly one of either {a} or {b} is present as the {Key Data}

* 4-way handshake
* General

*Modify 12.7.6.1 as shown below:*

RSNA defines a protocol using EAPOL-Key frames called the *4-way handshake*. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:

Message 1: Authenticator ® Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,{} or {PMKID})

Message 2: Supplicant ® Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,{RSNE} or {RSNE, OCI KDE} or {RSNE, RSNXE} or {RSNE, OCI KDE, RSNXE})

Message 3: Authenticator®Supplicant:
EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,{RSNE,GTK[N]} or
{RSNE, GTK[N], OCI KDE} or {RSNE, GTK[N], RSNXE} or
{RSNE, GTK[N], OCI KDE, RSNXE})

Message 4: Supplicant ® Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{} or {Device ID KDE}).

* 4-way handshake message 4

*Modify 12.7.6.5 (P3221 L17 and L32) as shown below:*

Message 2 uses the following values for each of the EAPOL-Key frame fields:

Descriptor Type **=** N – see 12.7.2 (EAPOL-Key frames)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other cases 0 – same as message 1

Key Type = 1 (Pairwise) – same as message 1

Reserved = 0

Install = 0

Key Ack = 0

Key MIC = 0 when using an AEAD cipher or 1 otherwise

Secure = 0 – same as message 1

Error = 0 – same as message 1

Request = 0 – same as message 1

Encrypted Key Data = 1 when using an AEAD cipher or if the Device ID KDE is included, or 0 otherwise

Reserved = 0 – unused by this protocol version

Key Length = 0

Key Replay Counter = *n* – to let the Authenticator or initiator STA know to which message 1 this corresponds

Key Nonce = SNonce

EAPOL-Key IV = 0

Key RSC = 0

Key MIC = Not present when using an AEAD cipher; otherwise, MIC(KCK, EAPOL) – MIC computed over the body of this EAPOL-Key frame with the Key MIC field first initialized to 0

Key Data Length = length of Key Data field in octets

Key Data =

— May include Device ID KDE

— May include one or more vendor specific KDEs and/or Vendor Specific elements