802.11bi Draft Specification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed spec texts for encrypting (re)association request response | | | | |
| Date: 2023-07-09 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission proposes spec text based on the following passed requirement.

Part I:

11bi shall define a mechanism for a CPE Client and CPE AP to protect the (Re)Association Request/Response.

11bi shall define a mechanism to protect the Frame Body field of the (Re)Association Request frame

11bi shall define a mechanism to protect the Frame Body field of the (Re)Association Response frame

Part II:

11bi shall define a mechanism for a CPE Client and CPE AP to establish the CPE Client’s DS MAC Address without the CPE Client’s DS MAC Address being transmitted in the clear.

11bi shall define a mechanism to carry the DS MAC address of a 11bi non-AP STA or an 11bi non-AP MLD in a protected (Re)association Request frame (and any other TBD protected management frames) from the 11bi non-AP STA to a 11bi AP or from the 11bi non-AP MLD to a 11bi AP MLD.

11bi shall define a mechanism to randomize over the air MAC address of the 11bi non-AP STA or 11bi non-AP MLD (carried in Address 1 field or Address 2 field of the MAC header) during BSS transition.

11bi shall define a mechanism for a CPE Client to change its own OTA MAC Address when reassociating from a CPE AP to another CPE AP.

Revision History:

* Rev 0: Initial version of the document
* Rev 1: Revision based on the comments received during the first presentation. Changes are marked with green

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

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

**Discussion:**

There are several requirements related to protect the frame body of (re)association request/response. Since we have the requirement to establish keys from authentication exchange, which is the difficult part, once the key is established and pairwise cipher is chosen, we can directly use the key and pairwise cipher to encrypt the (re)association request/response.

*11bi shall define a mechanism for a CPE Client and CPE AP to establish keys from an Authentication exchange which can then be used to protect the (Re)Association Request/Response.*

After the (re)association request/response is protected, the DS MAC address can then directly be included in the Frame Body field of the (re)association request and the over-the-air MAC address can then be randomized during BSS transition.

We propose texts only for the basic part, which can then be combined with the proposal for establishing key and choosing pairwise cipher using authentication frame.

**Proposed Texts:**

**TGbi Editor: *Instruction: Insert new rows in Table 9-363 in 9.4.2.241 RSNXE as shown below***

9.4.2.241 RSNXE

|  |  |  |
| --- | --- | --- |
| * **Extended RSN Capabilities field** | | |
| **Bit** | **Information** | **Notes** |
| <ANA> | Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support | A EDP STA sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield to 1 if dot11EDPEncryptionOfTheFrameBodyFieldOfTheReAssociation RequestResponseFrameSupportActivated is true. Otherwise, this subfield is set to 0. See 12.13.x (Encryption of the Frame Body Field of the (Re)Association Request/Response frame). |

**TGbi Editor: *Instruction: Insert new clauses in 9.4.2 Elements as shown below***

9.4.2 Elements

9.4.2.x DS MAC Address element

The DS MAC Address element is used by a non-AP STA that is not affiliated with a non-AP MLD or a non-AP MLD to provide the DS MAC address to the AP or a non-AP MLD, respectively, to be used for the DS mapping.

The format of the DS MAC Address element is shown in **Error! Reference source not found.**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | DS MAC Address |
| Octets: | 1 | 1 | 1 | 6 |

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

The DS MAC Address field indicates the DS MAC address.

**TGbi Editor: *Instruction: Modify 9.3.3.5 as shown below (track change on)***

* **Association Request frame format**

The frame body of an Association Request frame contains the information shown in **Association Request frame body**.

|  |  |  |
| --- | --- | --- |
| * **Association Request frame body** | | |
| **Order** | **Information** | **Notes** |
| …(existing elements)…. | | |
| <ANA> | DS MAC Address | The DS MAC Address element is present when Association Request frame is encrypted; otherwise, it is not present. |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

**TGbi Editor: *Instruction: Modify 9.3.3.6 as shown below (track change on)***

* **Association Response frame format**

The frame body of an Association Response frame contains the information shown in **Association Response frame body**.

|  |  |  |
| --- | --- | --- |
| * **Association Response frame body** | | |
| **Order** | **Information** | **Notes** |
| …(existing elements)…. | | |
| 10 | RSN | The RSNE is present if dot11FILSActivated is true or if dot11FILSActivated is false and the Association Response frame is encrypted; otherwise not present. |
| …(existing elements)…. | | |
| 38 | Key Delivery | The Key Delivery element is present if dot11FILSActivated is true or if dot11FILSActivated is false and the Association Response frame is encrypted; otherwise not present. |
| …(existing elements)…. | | |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

**TGbi Editor: *Instruction: Modify 9.3.3.7 as shown below (track change on)***

* **Reassociation Request frame format**

The frame body of a Reassociation Request frame contains the information shown in **Reassociation Request frame body**.

|  |  |  |
| --- | --- | --- |
| * **Reassociation Request frame body** | | |
| **Order** | **Information** | **Notes** |
| …(existing elements)…. | | |
| <ANA> | DS MAC Address | The DS MAC Address element is present when Reassociation Request frame is encrypted; otherwise, it is not present. |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

**TGbi Editor: *Instruction: Modify 9.3.3.8 as shown below (track change on)***

* **Reassociation Response frame format**

The frame body of a Reassociation Response frame contains the information shown in **Reassociation Response frame body**.

|  |  |  |
| --- | --- | --- |
| * **Reassociation Response frame body** | | |
| **Order** | **Information** | **Notes** |
| …(existing elements)…. | | |
| 10 | RSN | An RSNE is present in a Reassociation Response frame if dot11FastBSSTransitionActivated is true, dot11RSNAActivated is true, and this frame is a response to a Reassociation Request frame that contained an FTE (i.e., part of a fast BSS transition in an RSN); or if dot11FILSActivated is true or if dot11FILSActivated is false and the Reassociation Response frame is encrypted. Otherwise, not present. |
| …(existing elements)…. | | |
| 41 | Key Delivery | The Key Delivery element is present if dot11FILSActivated is true and FILS authentication is used or if dot11FILSActivated is false and the Reassociation Response frame is encrypted; otherwise not present. |
| …(existing elements)…. | | |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

**TGbi Editor: *Instruction: Insert 12.13.x Protection of (Re)Association Request/Response frame as shown below***

**12.13 Client Privacy Enhancement**

**12.13.x Encryption of the Frame Body Field of the (Re)Association Request/Response Frame**

This subclause defines rules to encrypt the Frame Body field of the (Re)Association Request/Response frame and include DS MAC Address element in the encrypted (Re)Association Request frame.

**12.13.x.1 non-MLO**

An EDP non-AP STA that sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1 may indicate a pairwise cipher, establish PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP that sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1.

An EDP non-AP STA may randomize over-the-air MAC address during BSS transition if the BSS transition procedure uses encrypted (Re)Association Request frame to carry the DS MAC Address element.

After a pairwise cipher is indicated by the EDP non-AP STA and a temporal key (TK) is derived during Authentication frame exchange between the EDP non-AP STA and an EDP AP, then the EDP non-AP STA shall encrypt the (Re)Association Request frame transmitted to the EDP AP using the TK and the indicated pairwise cipher in the Authentication frame exchange as defined in 12.5.2 CTR with CBC-MAC protocol (CCMP) or 12.5.4 GCM protocol (GCMP).

The EDP non-AP STA shall include the DS MAC Address element in the (Re)Association Request frame to indicate the DS MAC address to be used by the EDP AP for the mapping to the DS.

The EDP AP shall decrypt the (Re)Association Request frame received from the EDP non-AP STA using the TK and the indicated pairwise cipher in the Authentication frame exchange as defined in 12.5.2 CTR with CBC-MAC protocol (CCMP) or 12.5.4 GCM protocol (GCMP). If the decryption fails, then the association exchange fails and the EDP AP shall reject the association.

The EDP AP shall encrypt the (Re)Association Response frame transmitted to the EDP non-AP STA in response to the (Re)Association Request frame using the TK and the indicated pairwise cipher in the Authentication frame exchange as defined in 12.5.2 CTR with CBC-MAC protocol (CCMP) or 12.5.4 GCM protocol (GCMP).

The EDP AP shall include the Key delivery element in the (Re)Association Response frame if all the following conditions are satisfied:

* FILS authentication is not used
* Over-the-air FT protocol is not used
* Over-the-DS FT protocol is not used

If the Key delivery element is included in the (Re)Association Response frame, the EDP AP shall construct a Key Delivery element indicating the current GTK PN in the RSC subfield, with the GTK KDE, with the IGTK KDE if management frame protection is enabled, with the BIGTK KDE if beacon protection is enabled, with WIGTK KDE if WUR frame protection is enabled.

The EDP non-AP STA shall decrypt the (Re)Association Response frame received from the EDP AP using the TK and the indicated pairwise cipher in the Authentication frame exchange as defined in 12.5.2 CTR with CBC-MAC protocol (CCMP) or 12.5.4 GCM protocol (GCMP). If the decryption fails, then the association exchange fails.

On successful (re)association,

* the EDP AP and the EDP non-AP STA shall transition to State 4 (as defined in 11.3 (STA authentication and association)) to enable Data frame transmission.
* the EDP non-AP STA shall process the Key Delivery element in the (Re)Association Response frame if present.
* The EDP AP shall process the DS MAC Address element and use the indicated DS MAC address to establish EDP non-AP STA to EDP AP mapping to the DS
* The EDP non-AP STA installs the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and WIGTK and WIGTK RSC if present in the Key Delivery element and dot11RSNAWURFrameProtectionActivated is true.

On failed (re)association, established PTKSA shall be irretrievably deleted.

**12.13.x.2 MLO**

A non-AP MLD that sets the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1 may indicate a pairwise cipher, establish PTKSA, and drive a temporal key (TK) through Authentication frame exchange with an EDP AP MLD if APs affiliated with the EDP AP MLD set the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1.

NOTE - For MLO, all STAs affiliated with an MLD set the RSNXE to the same value.

An EDP non-AP MLD may randomize over-the-air MAC address during BSS transition if the BSS transition procedure uses encrypted (Re)Association Request frame to carry the DS MAC Address element.

After a pairwise cipher is indicated by the EDP non-AP MLD and a TK is derived during Authentication frame exchange between the EDP non-AP MLD and an EDP AP MLD, then the EDP non-AP MLD shall encrypt the (Re)Association Request frame transmitted to the EDP AP MLD using the TK and the indicated pairwise cipher in the Authentication frame exchange as defined in 12.5.2 CTR with CBC-MAC protocol (CCMP) or 12.5.4 GCM protocol (GCMP).

The (Re)Association Request frame shall:

* Have the value of the Address 1 field equal to the value of the Address 1 field of the Authentication frame used by the non-AP MLD to establish PTKSA
* Have the value of the Address 2 field equal to the value of the Address 2 field of the Authentication frame used by the non-AP MLD to establish PTKSA
* Include the DS MAC Address element in the (Re)Association Request frame to indicate the DS MAC address to be used by the EDP AP MLD for the mapping to the DS.

The EDP AP MLD shall decrypt the (Re)Association Request frame received from the EDP non-AP MLD using the TK and the indicated pairwise cipher in the Authentication frame exchange as defined in 12.5.2 CTR with CBC-MAC protocol (CCMP) or 12.5.4 GCM protocol (GCMP). If the decryption fails, then the association exchange fails and the EDP AP MLD shall reject the association.

The EDP AP MLD shall encrypt the transmitted (Re)Association Response frame transmitted to the EDP non-AP MLD in response to the (Re)Association Request frame using the TK and the indicated pairwise cipher in the Authentication frame exchange as defined in 12.5.2 CTR with CBC-MAC protocol (CCMP) or 12.5.4 GCM protocol (GCMP)

The EDP AP MLD shall include the Key Delivery element into the (Re)Association Response frame if all the following conditions are satisfied:

* FILS authentication is not used
* Over-the-air FT protocol is not used
* Over-the-DS FT protocol is not used

If the Key delivery element is included in the (Re)Association Response frame, the EDP AP MLD shall construct a Key Delivery element with the RSC field set to 0, with the MLO GTK KDE for each setup link, with the MLO IGTK KDE for each setup link if management frame protection is negotiated, with the MLO BIGTK KDE for each setup link if beacon protection is enabled.

The EDP non-AP MLD shall decrypt the (Re)Association Response frame received from the EDP AP MLD using the TK and the indicated pairwise cipher in the Authentication frame exchange as defined in 12.5.2 CTR with CBC-MAC protocol (CCMP) or 12.5.4 GCM protocol (GCMP). If the decryption fails, then the association exchange fails.

On successful (re)association,

* the EDP AP MLD and the EDP non-AP MLD shall transition to State 4 (as defined in 11.3 (STA authentication and association)) to enable Data frame transmission.
* the EDP non-AP MLD shall process the Key Delivery element in the (Re)Association Response frame if present.
* The EDP AP MLD shall process the DS MAC Address element and use the indicated DS MAC address to establish EDP non-AP MLD to EDP AP MLD mapping to the DS
* The EDP non-AP MLD installs the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true.

On failed (re)association, established PTKSA shall be irretrievably deleted.