IEEE P802.11
Wireless LANs

|  |
| --- |
| CR for Miscellaneous CIDs |
| Date: 2025-06-30 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel Corporation |  |  | po-kai.huang@intel.com |

Abstract

This submission proposes resolutions for multiple comments related to TGbi D1.0 with the following CIDs:

* 946, 182

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 TGbi Draft. This introduction is not part of the adopted material.

***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 existing 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.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 946 | 3.2 | 21.16 | DS MAC address is an inaccurate term | DS MAC address is not accurate since that MAC address will be transmitted beyond the DS. Also DS is a virtual concept. Perhaps rename it to "LAN MAC address" or "Network MAC address". It would be the MAC address asigned to an IP stack. | Rejected –The connection of the MAC address to higher layer routing is described in the spec through association and DS mapping. Once the address used for DS mppaing is clarified, it will be used outside of the 802.11 automatically. Hence, even if the name is DS MAC address, it does not prevent the address to be used externally. Similar to the STA MAC address and MLD MAC address naming used for DS before 11bi, which does not have any LAN or Network naming.LAN MAC address and network address does not connect with the 802.11 DS concept directly to differentiate with the STA MAC address and MLD MAC address. MLD is also a virtual concept, but we define MLD MAC address. *To deliver an MSDU within an ESS via the DS, the DS needs to know which AP within the ESS to deliver**the MSDU to(#4387), so that the MSDU might ultimately be delivered to the addressed IEEE 802.11 STA.**This information is provided to the DS by the concept of association. Association is necessary, but not**sufficient, to support BSS-transition mobility. Association is sufficient to support no-transition mobility.**Association is one of the services in the DSS.**For a non-GLK STA, the act of becoming associated invokes the association service, which provides the**STA to AP mapping to the DS. How the information provided by the association service is stored and**managed within the DS is not specified by this standard.* |
| 182 | 12.11 | 117.01 | The privacy issues with FILS are not addressed in this draft | Come up with a scheme to protect the FILS Public Key Element which sends either a certificate or a raw public key, both of which allow for 3rd party tracking. | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/1092 under all headings that include CID 182 |

***Discussion: FILS public key authentication***

The commenter refers to FILS public key element used during FILS public key authentication.

*The FILS Public Key element is present if dot11FILSActivated is true and FILS Public Key authentication is used; otherwise not present.*

FILS public key element is currently after FILS Session element in (re)association requet/response frame and is encrypted by AEAD.

*The plaintext passed to the AEAD algorithm is the data that would follow the FILS Session element in an unencrypted frame body. The output of the AEAD algorithm becomes the data that follows the FILS Session element in the encrypted and authenticated (Re)Association Request frame.*

As a result, passive attacker can not decrypt the AEAD and track the public key or certificate of the FILS Originator. However, an active attacker may perform MITM attack since the PTK-KEK is derived purely by DH exchange in the first two authentication frames and is only confirmed during the (Re)Association Request/Response exchange using the exchanged public key.



*The first authentication frame provides Diffie-Hellman parameter and Nonce from the FILS Originator.*

*The second authentication frame provides Diffie-Hellman parameter and Nonce from the FILS Responder.*

*Both the FILS Originator and the FILS responder compute PTKSA*

*PMK = HMAC-Hash(SNonce || ANonce, DHss)*

*PTK = PRF-X(PMK, “FILS PTK Derivation”, SPA || AA || SNonce || ANonce [ || DHss ])*

If the group wants to address the active attack, then the proposal is to move the key confirmation in (Re)Assocaition Response to the second authentication frame and use the AEAD encryption such that the client can confirm before sending its own public key in the (Re)Association Request frame.

***Proposal: (#182)***

**TGbi Editor: *Modify 12.16.8 as follows***

**12.16.8 Key derivation with Authentication frame exchange**

12.16.8.4 FILS Authentication

If a FILSO and a FILSR (see 12.11 (Authentication for FILS)) set the (Re)Association Frame Encryption Support field

in the RSNXE to 1, then the FILSO and FILSR shall perform FILS authentication with PFS.

If FILS public key authentication is used, the FILSR shall include the FILS Public Key and the FILS Key Confirmation element after the FILS Session element in the Authentication frame rather than the (Re)Association Response frame.

The Authentication frame sent by FILSR shall be encrypted using the AEAD algorithm as defined in 12.11.2.7 (AEAD cipher mode for FILS) with the PTK-KEK as the key. The AAD used with the AEAD algorithm for the Authenticaiton frame consists of the following data passed as separate components in the following order:

* FILSO’s MAC address
* FILSR’s MAC address (i.e., BSSID of the AP’s BSS or, for MLO, AP MLD’s MAC address)
* FILSO’s nonce
* FILSR’s nonce
* The contents of the Authentication frame from the Authentication Algorithm Number field (inclusive)

to the (#482)FILS Session element (inclusive)

The plaintext passed to the AEAD algorithm is the data that would follow the FILS Session element in an unencrypted frame body. The output of the AEAD algorithm becomes the data that follows the FILS Session element in the encrypted and authenticated Authentication frame. The output of the algorithm is as specified in IETF RFC 5116. The resulting Authentication frame shall be transmitted to the FILSO.

The FILSO decrypts and verifies the received Authenticaiton frame with the AEAD algorithm as defined in this subclause above with the PTK-KEK as the key. The AAD is reconstructed as defined in this subclause above and is passed with the cipher text of the received

frame to the AEAD decryption operation.

If the output from the AEAD decryption operation returns failure, the authentication exchange fails. If the output does not return failure, the output plaintext replaces the cipher text as portion of the frame body that follows the FILS Session element and processing of the received frame continues by checking the value of the FILS Key Confirmation element as defined in 12.11.2.6.3 ((Re)Association Response for FILS key confirmation). If any of these verifications related to the FILS Key Confirmation element fail, authentication fails.

**TGbi Editor: *Modify 9.3.3.6 as follows***

* Association Response frame format

***Change rows in Table 9-65 (Association Response frame body) as follows (not all lines shown):***

* revme D7.0 up to 77, 11bh D6.0 up to 78-80, 11be D7.0 81-86, 11bk D5.0 no addition, 11bf D8.0 87-90
* Association Response frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 10 | RSN | The RSNE is present if dot11FILSActivated is true or if performing OWE or if the Association Response frame is encrypted; otherwise, it is not present.(#402)  |
| ... |  |  |
| 34 | FILS Public Key | The FILS Public Key element is present if dot11FILSActivated istrue, the Association Response frame is not encrypted using TK, and FILS Public Key authentication is used; otherwise notpresent. |
| 35 | FILS Key Confirmation | The FILS Key Confirmation element is present ifdot11FILSActivated is true, the Association Response frame is not encrypted using TK when FILS Public Key authentication is used, and FILS authentication is used;otherwise not present. |
| ... |  |  |
| 38 | Key Delivery | The Key Delivery element is present if dot11FILSActivated is true or if the Association Response frame is encrypted; otherwise, it is not present.(#402) |
| ... |  |  |
| 91 | EDP | The EDP element carrying configuration and EDP Group ID(#1012) for the assigned group EDP epoch(#1012). This element is present if the Association Response frame is encrypted and dot11EDPGroupEpochActivated is true; otherwise, it is not present. |

TGbi Editor: *Modify 9.3.3.8 as follows*

* Reassociation Response frame format

***Change rows in Table 9-67 (Reassociation Response frame body) as follows (not all lines shown):***

* revme D7.0 up to 80, 11bh D6.0 no addition, 11be D7.0 81-86, 11bk D5.0 no addition, 11bf D8.0 87-90
* Reassociation Response frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 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 ifperforming OWE, or if the Reassociation Response frame is encrypted. Otherwise, it is not present.(#Ed, #400)  |
| … |  |  |
| 37 | FILS Public Key | The FILS Public Key element is present if dot11FILSActivated istrue, the Reassociation Response frame is not encrypted using TK, and FILS Public Key authentication is used; otherwise notpresent. |
| 38 | FILS Key Confirmation | The FILS Key Confirmation element is present ifdot11FILSActivated is true, the Association Response frame is not encrypted using TK when FILS Public Key authentication is used, and FILS authentication is used;otherwise not present. |
| ... |  |  |
| 41 | Key Delivery | The Key Delivery element is present if dot11FILSActivated is true and FILS authentication is used or if the Reassociation Response frame is encrypted; otherwise, it is not present.(#402)  |
| ... |  |  |
| 91 | EDP | The EDP element carrying configuration and EDP Group ID(#1012) for the assigned group EDP(#1012) epoch. This element is present if the Ressociation Response frame is encrypted and dot11EDPGroupEpochActivated is true; otherwise, it is not present. |

TGbi Editor: *Modify 9.3.3.11 as follows*

* Authentication frame format
* revme D7.0 up to order 27, 11bh D6.0 no addition, 11be D7.0 up to order 28, 11bk D5.0 no addition, 11bf D8.0 no addition

***Change Table 9-71 (Presence of fields and elements in Authentication frames) and insert new rows at the end of Table 9-71 (Presence of fields and elements in Authentication frames) as follows (not all lines shown):***

* Presence of fields and elements in Authentication frames

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication algorithm | Authentication transaction sequence number | Status code | Presence of fields and elementsindicated as conditional in Table 9-70 (Authentication frame body) |
| FT | 1 | Reserved | The MDE is present. The FTE and RSNE(s) are present if dot11RSNAActivated is true.The RSNXE is present if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.The Diffie-Hellman Parameter element is optionally present as defined in 12.16.8.1 (FT protocol(#176)).(#409) |
| FT | 2 | Not REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | The MDE is present if the Status Code field is 0. The FTE and RSNE(s) are present if the Status Code field is 0 and dot11RSNAActivated is true.The Diffie-Hellman Parameter element is optionally present as defined in 12.16.8.1 (FT protocol(#176)).(#409) |
| .... |  |  |  |
| FILS Shared Keyauthenticationwithout PFS | 1 | Reserved | The RSNE is present.The MDE is present if the FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present.The FILS Session element is present.The Wrapped Data element is present. |
| FILS Shared Keyauthenticationwithout PFS | 2 | Status | The RSNE is present.The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present if the Status Code field is 0.The FILS Session element is present if the Status Code field is 0.The Wrapped Data element is present if the Status Code field is 0.The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Requestframe. |
| FILS Shared Keyauthentication with PFS | 1 | Reserved | The Finite Cyclic Group field is present.The FFE field is present.The RSNE is present.The MDE is present if the FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present.The FILS Session element is present.The Wrapped Data element is present. |
| FILS Shared Keyauthentication withPFS | 2 | Status | The Finite Cyclic Group field is present if the Status Code field is 0.The FFE field is present if the Status Code field is 0.The RSNE is present.The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present if the Status Code field is 0.The FILS Session element is present if the Status Code field is 0.The Wrapped Data element is present if the Status Code field is 0.The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |
| FILS Public Keyauthentication | 1 | Reserved  | The Finite Cyclic Group field is present.The FFE field is present.The RSNE is present.The MDE is present if the FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present.The FILS Session element is present. |
| FILS Public Keyauthentication | 2 | Status | The Finite Cyclic Group field is present if the Status Code field is 0.The FFE field is present if the Status Code field is 0.The RSNE is present.The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present if the Status Code field is 0.The FILS Session element is present if the Status Code field is 0.The FILS Public Key element is present if the Status Code field is 0 and the encryption of (Re)Association Request/Response frame exchange using TK is used.The FILS Key Confirmation element is present if the Status Code field is 0 and the encryption of (Re)Association Request/Response frame exchange using TK is used.The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |

**TGbi Editor: *Modify 12.16.6 as follows***

**12.16.6 (Re)Association Request/Response Frame Encryption**

**12.16.6.1 Non-MLO procedure**

(…existing texts…)

If the FT protocol is used, then the EDP non-AP STA shall not calculate the MIC for the MIC field of the FTE in the Reassociation Request frame. The length of the MIC field of the FTE in the Reassociation Request frame shall be 0 (i.e., the MIC Length subfield of the MIC Control field of the FTE is set to 3). The Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

If the FILS authentication protocol is used, then the EDP non-AP STA shall not encrypt the (Re)Association Request frame using the AEAD algorithm as described in 12.11.2.6.2 (Re)Association Request for FILS key confirmation.

(…existing texts…)

If the FT protocol is used, then the EDP AP shall not wrap the Key field of the subelements in the FTE in the

Reassociation Response frame and shall not calculate the MIC for the MIC field of the FTE in the Reassociation

Response frame. The length of the MIC field of the FTE in the Reassociation Response frame shall be

0 (i.e., the MIC Length subfield of the MIC Control field of the FTE is set to 3). The Element Count subfield

of the MIC Control field of the FTE shall be set to 0.(#915)

If the FILS authentication protocol is used, then the EDP AP shall not encrypt the (Re)Association Response frame using the AEAD algorithm as described in 12.11.2.6.3 (Re)Association Response for FILS key confirmation.

**12.16.6.2 MLO procedure**

(…existing texts…)

If the FT protocol is used, then the EDP non-AP MLD shall not calculate the MIC for the MIC field of the

FTE in the Reassociation Request frame. The length of the MIC field of the FTE in the Reassociation

Request frame shall be 0 (i.e., the MIC Length subfield of the MIC Control field of the FTE is set to 3). The

Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

If the FILS authentication protocol is used, then the EDP non-AP MLD shall not encrypt the (Re)Association Request frame using the AEAD algorithm as described in 12.11.2.6.2 (Re)Association Request for FILS key confirmation.

(…existing texts…)

If the FT protocol is used, then the EDP AP MLD shall not wrap the Key field of the subelements in the FTE

in the Reassociation Response frame and shall not calculate the MIC for the MIC field of the FTE. The

length of the MIC field shall be 0 (i.e., the MIC Length subfield of the MIC Control field of the FTE is set to

3). The Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

If the FILS authentication protocol is used, then the EDP AP MLD shall not encrypt the (Re)Association Response frame using the AEAD algorithm as described in 12.11.2.6.3 (Re)Association Response for FILS key confirmation.

(…existing texts…)