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.
* Rev 1: Revison based on the discussion during the teleconference call.

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. FILS public key element is already encrypted in (re)association request currently with AEAD. Under 11bi, it will be encrypted with PMF. Hence, 3rd party can not track the encrypted FILS public key element. 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. The resolution only clarifies that in 11bi, we use PMF to encrypt the (re)association request/response rather than AEAD.



*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 ])*

***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.

**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…)