IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | SB CR for Miscellaneous CIDs | | | | | | Date: 2024-03-08 | | | | | | Author(s): | | | | | | Name | Affiliation | Address | Phone | email | | Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11-REVme D5.0:

7041, 7042, 7043, 7044, 7026, 7070, 7045,

7046, 7047, 7048, 7049, 7050

**Revision History:**

R0: Initial version.

R1: Add CID 7026 and 7070

R2: Fix editorial errors of the abstract.

R3: Revision based on discussion during the meeting. Table 7049, 7050.

R4: Revision 7050 based on offline discussion.

R5: Revision 7049 based on Mark’s comment to resolve instances of “management frame protection is not used (2x)”, ”management frame protection is not in use (4x)”, and “management frame protection is used (1x)”

R6: Clarify under scenario of association or reassociation where there are management frame protection negotiation for existing association or new association that management frame protectin in use means management frame protection is negoatied for the existing association

R7: Another revison for 7049 to clarify scenarios.

R8: Revision for 7049 based on discussion during teleconference call.

# CID 7041, 7042, 7043, 7044, 7026, 7070, 7045

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** |
| 7041 | 9.3.3.11 | 769.56 | [Po-Kai] In Table 9-71 RSNXE is not present in message 1 and message 3, 4, but Table 13-1 specifies that RSNXE is in message 1 and message 3 and 4 | Add "The RSNXE is present as defined in Table 13-1" to message 1, 3, and 4. |
| 7042 | 9.3.3.11 | 767.47 | [Po-Kai] In Table 9-70, RSNXE is not included, but RSNXE is included in authentication frame for PASN and FT. | Add RSNXE to the Table 9-70. For the order, RSNXE is in clause 9.4.2.240, so roughter after password identifier (9.4.2.215) and before rejected groups (9.4.2.245). Hence, suggest to add after order 21 as order 22 for RSNXE |
| 7043 | 9.3.3.11 | 769.56 | [Po-Kai] Title of Table 9-71 is presence of fields and elements in authentication frames, but vendor specific element is never specified. | Add "The vendor specific element is optionally present" in every column of "Presence of fields and elements from order 4 onward" |
| 7044 | 9.3.3.11 | 767.47 | [Po-Kai] FILS Wrapped Data element should be renamed as Wrapped Data element per 11az change. | Change all instances of "FILS Wrapped Data" to "Wrapped Data" in the spec. There is a total of 12 instances. |
| 7026 | 9.4.2.186 | 1323.54 | IEEE Std 802.11az-2022 renamed FILS Wrapped Data element to Wrapped Data element, but did not change all locations in the standard. Multiple instances of the old name remains in REVme/D5.0. This applies to the FILS Wrapped Data field as well. | At P769 L6, replace "FILS Wrapped Data" with "Wrapped Data" (twice). At P771 L28, L42, and L64, replace "FILS Wrapped Data element" with "Wrapped Data element" (three times). At P772 L20, replace "FILS Wrapped Data element" with "Wrapped Data element". At P893 L13, replace "FILS Wrapped Data" with "Wrapped Data". At P1323 L54, delete Editor's Note about this renaming. At P3140 L36, L38, and L41, replace "FILS Wrapped Data element" with "Wrapped Data element" (three times). At P3142 L2 and L45, replace "FILS Wrapped Data field" with "Wrapped Data field" (twice). |
| 7070 | 9.4.2.186 | 1323.54 | 11az work item - 11az asks to change instances of “FILS Wrapped Data” to “Wrapped Data” as appropriate in the next revision of IEEE Std 802.11. A submission is required | as in comment. |
| 7045 | 9.3.3.11 | 767.47 | [Po-Kai] In Table 9-70, MIC element is not included, but MIC element is included in authentication frame for PASN as described in Table 9-71. | Add MIC element to Table 9-70 likely after vendor specific element to be at the end. |

## Discussion:

None

## Proposed Resolution: CID 7041, 7042, 7043, 7044, 7045

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for corresponding CID in 11-24/0528r3

## Proposed Resolution: CID 7026, 7070

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for CID 7044 in 11-24/0528r3

## Proposed Text Update: CID 7041, 7042, 7043, 7044, 7045

*TGme editor: Modify Clause 9.3.3.11 as follows (track change on):*

* Authentication frame format

The frame body of an Authentication frame contains the information shown in Table 9-70 (Authentication frame body). FT authentication is used when FT support is advertised by the AP and dot11FastBSSTransitionActivated is true in the STA. SAE authentication is used when dot11MeshActiveAuthenticationProtocol is sae (1). FILS authentication is used if support for FILS authentication is advertised by the AP and dot11FILSActivated is true in the STA.

|  |  |  |
| --- | --- | --- |
| * Authentication frame body | | |
| Order | Information | Notes |
| 1 | Authentication algorithm number |  |
| 2 | Authentication transaction sequence number |  |
| 3 | Status Code(#3326) | The status code information is reserved in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 4 | Finite Cyclic Group | An unsigned integer indicating a finite cyclic group as described in 9.4.1.40 (Finite Cyclic Group field). This is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 5 | Anti-Clogging Token | A random bit string used for anti-clogging purposes as described in 12.4.6 (Anti-clogging tokens). This is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 6 | Send-Confirm | A binary encoding of an integer used for anti-replay purposes as described in 12.4.7.4 (Encoding and decoding of SAE Confirm messages). This is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 7 | Scalar | An unsigned integer encoded as described in 12.4.7.3 (Encoding and decoding of SAE Commit messages). This is present only in cer-tain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 8 | FFE(#312) | An element in a finite field encoded as described in 12.4.7.3 (Encoding and decoding of SAE Commit messages). This is present only in cer-tain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 9 | Confirm | An unsigned integer encoded as described in 12.4.7.4 (Encoding and decoding of SAE Confirm messages). This is present only in cer-tain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 10(#3056) | RSN | An RSNE is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 11(#3056) | Mobility Domain | An MDE is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 12(#3056) | Fast BSS Transition | An FTE is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 13(#3056) | Timeout Interval (reassociation deadline) | A TIE containing the reassociation deadline interval is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 14(#3056) | RIC | A resource information container, containing a variable number of elements, is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 15(#3056) | Multi-band | The Multi-band element is optionally present if dot11MultibandImplemented is true. |
| 16(#3056) | Neighbor Report | One or more Neighbor Report elements are present only in cer-tain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 17(#3056) | FILS Nonce | The FILS Nonce element is present in FILS Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 18(#3056) | FILS Session | The FILS Session element is present in FILS Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 19(#3056) | (#7044)Wrapped Data | The (#7044)Wrapped Data element is present in FILS Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 20(#3056) | Association Delay Info | The Association Delay Info element is present in FILS Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 21(#3056) | Password Identifier | The Password Identifier element is optionally present in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 22 | RSNXE | The RSNXE is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames)(#7042) |
| 23(#3056) (#7042) | Rejected Groups | The Rejected Groups element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 24(#3056) (#7042) | Anti-Clogging Token Container | The Anti-Clogging Token Container element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 25(M67)(#3056) (#7042) | AKM Suite Selector | The AKM Suite Selector element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 26(11az) (#7042) | PASN Parameters | A PASN element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| Last-1(#7045) | Vendor Specific | One or more Vendor Specific elements are optionally present. (#7045) |
| Last(#7045) | MIC(#7045) | A MIC element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). (#7045) |

|  |  |  |  |
| --- | --- | --- | --- |
| * Presence of fields and elements in Authentication frames | | | |
| Authentication algorithm | Authentication transaction sequence number | Status Code(#3326) | Presence of fields and elements  indicated as conditional in Table 9-70 (#7043) |
| Open System | 1 | Reserved | Not present |
| Open System | 2 | Not REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | Not present |
| Open System | 2 | REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | One or more Neighbor Report element(s) is present. |
| (#3056)FT | 1 | Reserved | The (#1776)MDE is present.  The (#1776)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.(#7041) |
| FT | 2 | Not REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | The (#1776)MDE is present if the Status Code field is 0.  The (#1776)FTE and RSNE(s) are present if the Status Code field is 0 and dot11RSNAActivated is true. |
| FT | 2 | REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | One or more Neighbor Report element(s) is present. |
| FT | 3 | Reserved | The (#1776)MDE is present.  The (#1776)FTE and RSNE(s) are present if dot11RSNAActivated is true.  The RIC element is optionally present. |
| FT | 4 | Any | The (#1776)MDE is present if the Status Code field is 0.  The (#1776)FTE and RSNE(s) are present if dot11RSNAActivated is true.  The RIC element is optionally present if the Status Code field is 0.  The TIE (reassociation deadline) is present if a RIC element is present. |
| SAE | 1 | Any | The Scalar field is present if the Status Code field is zero or 126.  The FFE field is present if the Status Code field is zero or 126.  When the hunting-and-pecking method is used to drive the PWE, the Anti-Clogging Token field is present if the Status Code field is ANTI\_CLOGGING\_TOKEN\_REQUIRED or if the Authentication frame is in response to a previous rejection with the Status Code field equal to ANTI\_CLOGGING\_TOKEN\_REQUIRED.  The Finite Cyclic Group field is present if the Status Code field is zero, ANTI\_CLOGGING\_TOKEN\_REQUIRED, 77 or 126.  The Password Identifier element is optionally present if the Status Code field is zero, 123 or 126.  (#288)If the Status Code field is 126, the Rejected Groups element is conditionally present as described in 12.4.7.3 (Encoding and decoding of SAE Commit messages); otherwise the Rejected Groups element is not present. When the hash-to-element method is used to derive the PWE, the Anti-Clogging Token Container element is present if the Status Code field is ANTI\_CLOGGING\_TOKEN\_REQUIRED or if the Authentication frame is in response to a previous rejection with the Status Code field equal to ANTI\_CLOGGING\_TOKEN\_REQUIRED.  (M67)The AKM Suite Selector element is present if (#3266)the intended AKM is 00-0F-AC:24 or 00-0F-AC:25 (see 12.4.5.3 (Construction of an SAE Commit message) and 12.4.5.4 (Processing of a peer’s SAE Commit message)); otherwise, it is not present. |
| SAE | 2 | Not REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | The Send-Confirm field is present.  The Confirm field is present. |
| SAE | 2 | REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | One or more Neighbor Report element(s) are present |
| FILS Shared Key authentication without 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 (#7044)Wrapped Data element is present. |
| FILS Shared Key authentication without 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 (#7044)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 Shared Key authentication 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 (#7044)Wrapped Data element is present. |
| FILS Shared Key authentication with PFS | 2 | Status | The Finite Cyclic Group field(#313) 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 (#7044)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 Key authentication | 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 Key authentication | 2 | Status | The Finite Cyclic Group field(#313) 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 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. |
| PASN Authentication(11az) | 1 | Reserved | RSNE is present.  RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.  PASN Parameters element is present.  Timeout Interval element may be present.  Wrapped Data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved.  Fragment element may be present if any of the elements are fragmented. |
| PASN Authentication(11az) | 2 | Status | RSNE is present and PASN Parameters element is present if Status Code field is 0.  RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.  Timeout Interval element may be present.  Wrapped data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved and Status Code field is 0.  MIC element is present.  Fragment element may be present if any of the elements are fragmented and Status Code field is 0. |
| PASN Authentication(11az) | 3 | Status | PASN Parameters element is present if Status Code field is 0.  Wrapped data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved; and Status Code field is 0.  MIC element is present.  Fragment element may be present if any of the elements are fragmented and Status Code field is 0. |

*TGme editor: Modify Clause 13.8.1 as follows (track change on):*

13.8.1 Overview

(..existing texts…)

Regardless of the transport mechanism, the information contained in the FT authentication sequence consists of the set of elements shown in Table 13-1 (FT authentication elements).

|  |  |  |
| --- | --- | --- |
| * FT authentication elements | | |
| Information | Presence in Authentication Sequence messages | Description |
| RSN | The RSNE is present if dot11RSNAActivated is true; otherwise not present.(#3400) | 9.4.2.23 (RSNE) |
| Mobility Domain | The (#1776)MDE is present. | 9.4.2.45 (MDE(#1776)) |
| Fast BSS Transition | The (#1776)FTE is present if dot11RSNAActivated is true. | 9.4.2.46 (FTE(#1776)) |
| Timeout Interval (reassociation deadline) | The (#1776)TIE is optionally present in the fourth message of the sequence if dot11RSNAActivated is not true. | 9.4.2.47 (TIE(#1776)) |
| RIC | The (#1776)RDE is optionally present in the third and fourth messages. | 9.4.2.48 (RDE(#1776)) |
| RSNXE | (#6301)(#4070)The RSNXE is present in the first message if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.  (#6301)The RSNXE is present in the third message if an RSNXE is present in a Beacon or Probe Response frame that the FTO has received from the target AP and the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.  (#6301)The RSNXE is present in the fourth message if an RSNXE was present in the third message and the target AP set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.  (#6301)Otherwise, the RSNXE is not(#7041) present. | 9.4.2.240 (RSNXE(#1776)) |

(..existing texts…)

*TGme editor: Modify Clause 4.10.3.6.2 as follows (track change on):*

**4.10.3.6.2 AKM operations using FILS Shared Key authentication**

A non-AP STA and a trusted third party (TTP) using FILS Shared Key authentication verify mutual possession of a shared key (rRK) (as defined in IETF RFC 5295 and IETF RFC 6696) using Extensible Authentication Protocol (EAP) reauthentication protocol (EAP-RP) signaling. EAP-RP signaling is encapsulated using (#7044)wrapped data in an Authentication frame as shown in Figure 4-35 (FILS authentication using TTP). A valid rRK is derived using a prior full authentication using the full EAP as defined in 4.10.3.2 (AKM operations with AS). This rRK can be used for multiple runs of EAP-RP authentications as specified in IETF RFC 5295 and IETF RFC 6696.

(…existing texts…)

*TGme editor: Modify Clause 9.4.2.186 as follows (track change on):*

**9.4.2.186 (11az)Wrapped Data element**

(…existing texts…)

(#7044)

*TGme editor: Modify Clause 9.4.2.1 as follows (track change on):*

* General

(…existing texts…)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * Element IDs | | | | |
| Element | Element ID | Element ID Extension | Extensible | Fragmentable |
| (…existing entries…) |  |  |  |  |
| (#7044)Wrapped Data (see 9.4.2.186((11az)Wrapped Data element))) | 255 | 8 | No | Yes |
| (…existing entries…) |  |  |  |  |

(…existing texts…)

*TGme editor: Modify Clause 12.11.2.3.1 as follows (track change on):*

**12.11.2.3.1 Overview**

(…existing texts…)

EAP-RP signaling as defined in IETF RFC 5295 and IETF RFC 6696 is used to validate the mutual possession of rRK between the STA and the TTP. EAP-RP signaling is encapsulated using a (#7044)Wrapped Data element in the Authentication frame. The AP unwraps the encapsulated EAP-RP packet received from the STA in the (#7044)Wrapped Data element and forwards the EAP-RP packet to the TTP using a transport that is out of scope of this standard. When the AP receives an EAP-RP packet from the TTP, the AP forwards the packet to the STA by encapsulating the EAP-RP packet in the (#7044)Wrapped Data element of the Authentication frame.

(…existing texts…)

*TGme editor: Modify Clause 12.11.2.3.2 as follows (track change on):*

**12.11.2.3.2 Non-AP STA construction of Authentication frame**

(…existing texts…)

The STA then constructs an Authentication frame with the Authentication algorithm number set to 4 (FILS Shared Key authentication without PFS) or 5 (FILS Shared Key authentication with PFS) (see 9.4.1.1 (Authentication Algorithm Number field)) depending on whether PFS is used, and the Authentication transaction sequence number set to 1. The random nonce shall be encoded in the FILS Nonce element (see 9.4.2.188 (FILS Nonce element)). If a list of PMKSA identifiers was generated, it shall be used to construct the PMKID List field in (#6299)the RSNE. The random FILS Session shall be encoded in the FILS Session element (see 9.4.2.178 (FILS Session element)). The EAP-Initiate/Reauth packet, if generated, shall be copied into the (#7044)Wrapped Data field (see 9.4.2.186 ((11az)Wrapped Data element)). If PFS is desired, the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 9.4.1.40 (Finite Cyclic Group field)) and the ephemeral public key shall be encoded in the FFE field (see 9.4.1.38 (FFE field)) according to the element to (#1288)octet string conversion in 12.4.7.2.4 (Element to octet string conversion).

(…existing texts…)

*TGme editor: Modify Clause 12.11.2.3.3 as follows (track change on):*

**12.11.2.3.3 AP processing of Authentication frame**

(…existing texts…)

3) If an EAP-Initiate/Reauth packet is included and PMKSA caching is not used, the AP shall

extract the (#2043)data needed from the (#7044)Wrapped Data field (see 9.4.2.186

((11az)Wrapped Data element)) and shall forward it to the Authentication Server. When applicable, the AP communicates with the Authentication Server using the same protocols it uses when authenticating with EAP. Suitable protocols include, but are not limited to, remote authentication dial-in user service RADIUS (as specified in IETF RFC 2865 [B33]) and Diameter (as specified in IETF RFC 6942).

(…existing texts…)

*TGme editor: Modify Clause 12.11.2.3.4 as follows (track change on):*

**12.11.2.3.4 AP construction of Authentication frame**

(…existing texts…)

Otherwise, the AP shall generate its own nonce and construct an Authentication frame for the STA. The AP shall copy the FILS Session element from the Authentication frame sent by the non-AP STA to this response Authentication frame. If PMKSA caching is not used, this frame shall contain the (#7044)wrapped data that encapsulates (#330)the EAP-Finish/Reauth packet received from the Authentication Server. In addition, if PFS is used, the FFE field of the Authentication frame sent by the AP contains the AP’s ephemeral public key. In this frame, the AP shall set the Authentication algorithm number to 4 or 5 depending on whether PFS is used, and the Authentication sequence number to 2. If PMKSA caching is used, the AP indicates the selected PMKID in the PMKID List.

(…existing texts…)

# CID 7046, 7047, 7048, 7049, 7050

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** |
| 7046 | 12.13.3.1 | 3157.05 | [Po-Kai] Figure 12-59 can have some improvmenet. First, ephemeral pub is in PASN parameters element. Should have them in PASN Parameters like "PASN Parameters (S-Ephemeral Pub)". Second Algorithm number is the first in the frame based on Table 9-70 rather than transaction sequence number. Third, Base AKMP Data-1 is in Wrapped Data element. Finally, maybe good to have then in order based on Table 9-70. | Fix Figure 12-59 as in comments. |
| 7047 | 12.6.3 | 3054.52 | [Po-Kai] There is some confusion on the terms "management frame protection is enabled" vs "management frame protection is negotaited" vs MFP is used. Based on Bit 7 description in 9.4.2.23.4 RSN capabilities, "enabled" means MFPC is 1. In Note 1 of "12.6.17 Protection of robust Management frames", "managmenet frame protection is negotiated" means both STAs set MFPC to 1. But then Table 12-5 suddenly has a column with title "MFP used?" and that is pretty confusing on the meaning. Similar consdieration for Table 12-6. Then we have description like "(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#6149)(#199)) and the (#6149)value of the MFPC bit in the RSNE transmitted by the TDLS initiator STA in the TDLS Setup Request frame to determine if a TDLS direct link is allowed, and if so whether management frame protection is enabled", which does not align with the word "used" and should mean "negotiated". | Change "MFP used" to "MFP negotiated" in Table 12-5 and Table 12-6. Change "...f a TDLS direct link is allowed, and if so whether management frame protection is enabled. " to "f a TDLS direct link is allowed, and if so whether management frame protection is negotiated. " Commenter is willing to submit a contribution to fix related issues. |
| 7048 | 12.7.6.1 | 3101.56 | [Po-Kai] There is some confusion on the terms "management frame protection is enabled" vs "management frame protection is negotaited" vs MFP is used. Based on Bit 7 description in 9.4.2.23.4 RSN capabilities, "enabled" means MFPC is 1. In Note 1 of "12.6.17 Protection of robust Management frames", "managmenet frame protection is negotiated" means both STAs set MFPC to 1. However, page 3101 says,"IGTKSA if management frame protection is enabled" and page 3106 says "and if management frame protection is negotiated, the IGTK KDE, " Then we have "When management frame protection is enabled, a non-AP STA’s SME creates an IGTKSA when it receives a valid message 3 of the 4-way handshake or FT 4-way handshake, the Reassociation Response frame of the fast BSS transition protocol with a status code indicating success" in 12.6.1.1.9. For non-AP STA, creating IGTKSA when AP has MFPC set to 0 does not make sense. so the sentence in 12.6.1.1.9 needs to be negoatied. As a result, 3101 should also be management frame is negotiated. | Fix as suggested in comments. Commenter is willing to submit a contribution to fix related issues. |
| 7049 | 11.3.4.5 | 2548.22 | [Po-Kai] There is some confusion on the terms "management frame protection is enabled" vs "management frame protection is negotaited" vs "management frame protection is in use". Based on Bit 7 description in 9.4.2.23.4 RSN capabilities, "enabled" means MFPC is 1. In Note 1 of "12.6.17 Protection of robust Management frames", "managmenet frame protection is negotiated" means both STAs set MFPC to 1. "Management frame protection is in use" should be replaced with "managmeent frame protection is negotiated." | Replace all instances of "Management frame protection is in use" with "managmeent frame protection is negotiated". Commenter is willing to submit a contribution to fix related issues. |
| 7050 | 12.2.7 | 2973.10 | [Po-Kai] It is subtle that robust management frame is defined specifically as "The robust Management frames are Disassociation, Deauthentication, robust Action frames, and robust Action No Ack frames." It does not include all the managmeent frame. However, definition in 3.2 says "robust management frame(#4340): A Management frame that is eligible for protection.". Therefore, Beacon frame based on the definition is a robust managment frame when it is eligible for protection, but it contradicts with the definition in 12.2.7 Requirements for management frame protection | Change the defiintion of robust management frame in 3.2 as "robust management frame(#4340): A Management frame as defined in 12.2.7 that is eligible for protection." In 4.5.4.9 change "Robust Management frames are a set of Management frames that can be protected by the management frame protection service." to "Robust Management frames are a set of Management frames that can be protected by the management frame protection service as defined in 12.2.7." |

## Discussion:

None

## Proposed Resolution: CID 7046, 7047, 7048

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for CID in 11-24/0528r3

## Proposed Resolution: CID 7049, 7050

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for CID in 11-24/0528r8

## Proposed Text Update: CID 7046, 7047, 7048, 7049, 7050

*TGme editor: Modify Clause 12.11.2.3.4 as follows (track change on):*

**12.13.3.1 Overview**

(…existing texts…)

(#7046)

(#7046)

(…existing texts…)

*TGme editor: Modify Clause 12.6.3 as follows (track change on):*

* RSNA policy selection in an infrastructure BSS

The requirements in this subclause apply to a STA when dot11RSNAActivated is true.

(#1688)An AP advertises the available RSNA policies in an infrastructure BSS.

RSNA policy selection in an infrastructure BSS utilizes the normal IEEE 802.11 association procedure. RSNA policy selection is performed by the associating STA. The STA does this by including an RSNE (11ba), and if WUR frame protection is enabled, an RSNXE with the Protected WUR Frame Support subfield equal to 1 in its (re)association requests(#199)(#1562).

In an RSN, an AP shall not associate with pre-RSNA STAs, i.e., with STAs that fail to include the RSNE in the (Re)Association Request frame.

An SME initiating an association shall insert an RSNE into its (Re)Association Request via the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive, when the targeted AP indicates RSNA support. The initiating STA’s RSNE shall include one authentication and pairwise cipher suite from among those advertised by the targeted AP in its Beacon and Probe Response frames. It shall also -specify the (#6020)group data cipher suite and group management cipher suite (if present) specified by the targeted AP. If at least one RSNE field from the AP’s RSNE fails to overlap with any value the STA supports, the STA shall decline to associate with that AP. An HT STA shall eliminate TKIP as a choice for the pairwise cipher suite if CCMP-128 or CCMP-256 is advertised by the AP or if the AP included an HT Capabilities element in its Beacon and Probe Response frames. The elimination of TKIP as a choice for the pairwise cipher suite may result in a lack of overlap of the remaining pairwise cipher suite choices, in which case the STA shall decline to create an RSNA(#4025) with that AP.

If an AP receives a (Re)Association Request frame that includes an RSNE and if it chooses to accept the association as a secure association, then it shall use the authentication and pairwise cipher suites in the (Re)Association Request frame, unless the AP includes an optional second RSNE in message 3 of the 4-way handshake. If the second RSNE is supplied in message 3, then the pairwise cipher suite used by the security association, if established, shall be the pairwise cipher from the second RSNE.

In order to accommodate local security policy, a STA may choose not to associate with an AP that does not support any pairwise cipher suites. An AP may indicate that it does not support any pairwise keys by advertising 00-0F-AC:0 (Use group data cipher suite(#6020)) as the pairwise cipher suite selector.

NOTE—When an ESS uses PSKs, STAs negotiate a pairwise cipher. However, any STA in the ESS can derive the pairwise keys of any other that uses the same PSK by capturing the first two messages of the 4-way handshake. This provides malicious insiders with the ability to eavesdrop as well as the ability to establish a man-in-the-middle attack.

An AP and a non-AP STA shall use Table 12-5 (Robust management frame selection in an infrastructure BSS(#587)) and the values of the MFPC and MFPR subfields(#211) advertised in the RSNEs to determine if they may associate, and if so whether management frame protection is enabled.(#587) If either STA does not advertise an RSNE or does not advertise an RSN Capabilities field in an RSNE, this shall be treated as if its MFPC and MFPR bits were 0. A STA in an infrastructure BSS shall, outside the context of TDLS, set the MFPC subfield(#211) to 1 if dot11RSNAProtectedManagementFramesActivated is true and to 0 otherwise, and set the MFPR subfield(#211) to 1 if dot11RSNAUnprotectedManagementFramesAllowed is false and to 0 otherwise. dot11RSNAProtectedManagementFramesActivated shall be true if dot11RSNAUnprotectedManagementFramesAllowed is false.(#199)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| * Robust management frame selection in an infrastructure BSS(#587) | | | | | | |
| Non-AP STA MFPC | Non-AP  STA MFPR | Non-AP STA action | AP MFPC | AP MFPR | AP action | MFP negotiated(#7047)? |
| 0 | 0 | The STA may associate with the AP | 0 | 0 | The AP may accept associations from the STA | No |
| 1 | 0 | The STA may associate with the AP | 0 | 0 | The AP may accept associations from the STA | No |
| 0 | 0 | The STA may associate with the AP | 1 | 0 | The AP may accept associations from the STA | No |
| 1 | 0 or 1 | The STA may associate with the AP | 1 | 0 or 1 | The AP may accept associations from the STA | Yes |
| 1 | 1 | The STA shall not associate with the AP | 0 | 0 | N/A | N/A |
| 0 | 0 | The STA shall not associate with the AP (see NOTE) | 1 | 1 | The AP shall reject associations from the STA with the Status Code ROBUST\_MANAGEMENT\_POLICY\_VIOLATION | N/A |
| 0 | 1 | The STA shall not use this combination |  |  |  | N/A |
|  |  |  | 0 | 1 | The AP shall not use this combination | N/A |
| NOTE—STAs conformant with a previous revision of this standard might not ascribe a meaning to the MFPC and MFPR subfields. | | | | | | |

(#199)TDLS STAs shall use Table 12-6 (Robust management frame selection between TDLS STAs(#6149)(#199)) and the (#6149)value of the MFPC bit in the RSNE transmitted by the TDLS initiator STA in the TDLS Setup Request frame to determine if a TDLS direct link is allowed, and if so whether management frame protection is negotiated(#7047). A TDLS STA should, in the context of TDLS, set the MFPC bit to 1 if dot11RSNAProtectedManagementFramesActivated is true, and shall set it to 0 unless dot11RSNAProtectedManagementFramesActivated is true.

(#6149)NOTE—The MFPR bit from the TDLS initiator STA is ignored by the TDLS responder STA, and (if a TDLS Discovery Response frame is sent) the MFPC and MFPR bits from the TDLS responder STA are ignored by the TDLS initiator STA, except that a TDLS initiator STA might set its MFPC bit to 0 if the MFPC bit from the TDLS responder STA is 0.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * Robust management frame selection between TDLS STAs(#6149)(#199) | | | | |
| TDLS initiator STA MFPC | TDLS responder STA MFPC (might not be transmitted) | TDLS initiator STA action | TDLS responder STA action | MFP negotiated(#7047)? |
| 0 | 1 | The TDLS initiator STA may establish a TDLS direct link with the TDLS responder STA | The TDLS responder STA may establish a TDLS direct link with the TDLS initiator STA (see NOTE 1) | No |
| 0 | 0 | The TDLS responder STA may establish a TDLS direct link with the TDLS initiator STA |
| 1 | 1 | Yes |
| 1 | 0 | See NOTE 2 | The TDLS responder STA should reject attempts by the TDLS initiator STA to establish a TDLS direct link with the Status Code ROBUST\_MANAGEMENT\_POLICY\_VIOLATION (see Note 3) | N/A |
| NOTE 1—If the TDLS responder requires MFP, it can cause the TDLS direct link establishment to fail by using the Status Code ROBUST\_MANAGEMENT\_POLICY\_VIOLATION in the TDLS Setup Response frame.  NOTE 2—If a TDLS initiator STA has performed TDLS discovery and determined that the TDLS responder STA is not MFPC, it might, if it trusts the authenticity of the TDLS Discovery Response frame, avoid this situation, i.e., it might set its MFPC bit to 0 and not use MFP.  NOTE 3—Any subsequent attempt to use robust Management frame (e.g., ADDBA Request frames) will fail. | | | | |

*TGme editor: Modify Clause 12.7.6.1 as follows (track change on):*

**12.7.6.1 General**

(….existing texts…)

The FT initial mobility domain association uses the FT 4-way handshake (#1946)to establish an initial set of security associations: PTKSA, GTKSA, IGTKSA if management frame protection is negotiated(#7048), BIGTKSA(11ba) if beacon protection is enabled, and WIGTKSA if WUR frame protection is negotiated. The FT 4-way handshake protocol is described in 13.4 (FT initial mobility domain association).

(….existing texts…)

*TGme editor: Modify Clause 12.6.1.1.9 as follows (track change on):*

**12.6.1.1.9 IGTKSA**

When management frame protection is negotiated(#7048), a non-AP STA’s SME creates an IGTKSA when it receives a valid message 3 of the 4-way handshake or FT 4-way handshake, the Reassociation Response frame of the fast BSS transition protocol with a status code indicating success, a Mesh Peering Open Message of the Authenticated Mesh Peering Exchange (AMPE) protocol, a valid message 1 of the group key handshake, or the (Re)Association Response frame of FILS authentication with a status code indicating success. The Authenticator’s SME creates an IGTKSA when it establishes or changes the IGTK with all STAs to which it has a valid PTKSA or mesh PTKSA(#240). An IGTKSA has the same lifetime as the BSS, unless superseded.

(….existing texts…)

*TGme editor: Modify Clause 11.3.4.5 as follows (track change on):*

**11.3.4.5 Deauthentication—destination STA**

(….existing texts…)

a) If management frame protection was not negotiated when the PTKSA(s) were created, or if

management frame protection was negotiated when the PTKSA(s) were created (#7049) and the frame is not discarded per management frame protection processing, the MLME shall issue an MLME-DEAUTHENTICATE.indication primitive to inform the SME of the deauthentication, and set the state for the originating STA to State 1.

(….existing texts…)

*TGme editor: Modify Clause 11.3.5.2 as follows (track change on):*

**11.3.5.2 Non-AP and non-PCP STA association initiation procedures**

(….existing texts…)

(#2128)NOTE—Any MSDU fragments from the AP or PCP, and if management frame protection was negotiated for the existing association (#7049), any MMPDU fragments from the AP or PCP, are discarded at this point (see 12.6.12 (RSNA key management in an infrastructure BSS)), since fragments are required to be encrypted with the same key (see 10.5 (MSDU, (11ax)AMSDU, and MMPDU defragmentation)).

*TGme editor: Modify Clause 11.3.5.3 as follows (track change on):*

**11.3.5.3 AP or PCP association receipt procedures**

(….existing texts…)

p) If the ResultCode in the MLME-ASSOCIATE.response primitive is not SUCCESS and

management frame protection was negotiated for the existing association(#7049) the state for the STA shall be left unchanged. If the

ResultCode is not SUCCESS and management frame protection was not negotiated for the existing association (#7049) the state for the STA

shall be set to State 3 if it was State 4.

(#2128)NOTE 5—Any MSDU fragments from the STA, and if management frame protection was negotiated for the existing association (#7049), any MMPDU fragments from the STA, are discarded at this point (see 12.6.12 (RSNA key management in an infrastructure BSS)), since fragments are required to be encrypted with the same key (see 10.5 (MSDU, (11ax)A-MSDU, and MMPDU defragmentation)).

(….existing texts…)

*TGme editor: Modify Clause 11.3.5.4 as follows (track change on):*

**11.3.5.4 Non-AP and non-PCP STA reassociation initiation procedures**

(….existing texts…)

(#2128)NOTE—Per item 6) in the first list under c) any MSDU fragments in the reassembly buffers, and if management frame protection was negotiated for the existing association (#7049), any MMPDU fragments, have been discarded. This is important since fragments are required to be encrypted with the same key (see 10.5 (MSDU, (11ax)A-MSDU, and MMPDU defragmentation)).

*TGme editor: Modify Clause 11.3.5.4 as follows (track change on):*

**11.3.5.5 AP or PCP reassociation receipt procedures**

(….existing texts…)

k) If (#1699)management frame protection was not negotiated for the existing association (#7049), or the ResultCode in the MLMEREASSOCIATE.response primitive is SUCCESS and the reassociation is not part of a fast BSS

transition, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA(11ba),

(#3344)WIGTKSA, WTKSA, and TPKSA (including temporal keys)(#205) held for

communication with the STA by using the MLME-DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)).

(….existing texts…)

n) If the ResultCode in the MLME-REASSOCIATE.response primitive is not SUCCESS and

management frame protection was negotiated for the existing association (#7049) the state for the STA shall be left unchanged. If the ResultCode is not SUCCESS, management frame protection was not negotiated for the existing association (#7049), and the reassociation is part of a fast BSS transition, the state for the STA shall be left unchanged. If the ResultCode is not SUCCESS, management frame protection was not negotiated for the existing association (#7049), the reassociation is not part of a fast BSS transition, and the state for the STA was State 3 or State 4, the state for the STA shall be set to State

2 if the reassociation is for the same AP, or to State 3 otherwise.(#1699)

(….existing texts…)

(#2128)NOTE 4—Per 11.3.5.4 (Non-AP and non-PCP STA reassociation initiation procedures) item 6) in the first list under c) any MSDU fragments in the reassembly buffers, and if management frame protection was negotiated for the existing association (#7049), any MMPDU fragments, have been discarded. This is important since fragments are required to be encrypted with the same key (see 10.5 (MSDU, (11ax)A-MSDU, and MMPDU defragmentation)).

*TGme editor: Modify Clause 11.3.5.7 as follows (track change on):*

**11.3.5.7 Non-AP and non-PCP STA disassociation receipt procedure**

Upon receipt of a Disassociation frame from an AP or PCP for which the state is State 3 or State 4, if management frame protection was not negotiated when the PTKSA(s) were created, or if management frame protection was negotiated when the PTKSA(s) were created (#7049) and the frame is not discarded per management frame protection processing, a non-AP and non-PCP STA shall disassociate from the AP or PCP using the following procedure:

(….existing texts…)

*TGme editor: Modify Clause 11.3.5.9 as follows (track change on):*

**11.3.5.9 AP or PCP disassociation receipt procedure**

Upon receipt of a Disassociation frame from a STA for which the state is State 3 or State 4, if management frame protection was not negotiated when the PTKSA(s) were created, or if management frame protection was negotiated when the PTKSA(s) were created (#7049) and the frame is not discarded per management frame protection processing, the AP or PCP shall disassociate the STA using the following procedure:

(….existing texts…)

*TGme editor: Modify Clause 11.20.4 as follows (track change on):*

**11.20.4 TDLS direct link establishment**

(….existing texts…)

(#201)Subsequent to the successful completion of the TPK handshake, all Data frames transmitted on the TDLS direct link, and all Management frames if management frame protection was negotiated(#7049), shall be protected using the TPKSA, per the procedures defined in Clause 12 (Security).

(….existing texts…)

*TGme editor: Modify Clause 12.6.12 as follows (track change on):*

**12.6.12 RSNA key management in an infrastructure BSS**

(….existing texts…)

The Supplicant and Authenticator signal the completion of key management by utilizing the MLMESETKEYS.request primitive to configure the agreed-upon temporal pairwise key into the IEEE 802.11 MAC and by calling the MLME-SETPROTECTION.request primitive to enable its use. (#2128)Any MSDU fragments previously received under the corresponding (#3493)key ID shall be discarded at this point. If management frame protection was negotiated for the current association(#7049), any MMPDU fragments previously received under the corresponding (#3493)key ID shall be discarded at this point.

(….existing texts…)

*TGme editor: Modify Clause 12.6.19 as follows (track change on):*

**12.6.19 RSNA rekeying**

(….existing texts…)

When both ends of the link support extended (#3493)key IDs for individually addressed frames, it is possible to install the new PTKSA without data loss, provided the new PTKSA uses a different (#3493)key ID from the old PTKSA. Data loss might occur if the same (#3493)key ID is used because it is not possible to precisely coordinate (due to software processing delays) when the new key is used for transmit at one end and when it is applied to receive at the other end. If a different (#3493)key ID is used for the new PTKSA, then provided the new key is installed at the receive side prior to its first use at the transmit side there is no need for precise coordination. During the transition, received MPDUs(#3243) are unambiguously identified using the (#3493)key ID as belonging to either the old or new PTKSA. (#2128)The same (#3493)key ID shall be used for all fragments of a given MSDU. If management frame protection was negotiated for the current association (#7049), the same (#3493)key ID shall be used for all fragments of a given MMPDU.

(….existing texts…)

*TGme editor: Modify Clause 14.7.3 as follows (track change on):*

**14.7.3 Mesh Group Key Inform frame construction and processing**

Mesh Group Key Inform frame shall be constructed as follows:

(…existing texts…)

* If management frame protection is enabled(#7049), the IGTKdata field shall be present and shall contain

the data for the IGTK from IGTK source. The components of the IGTKdata are specified in 14.6.4 (Distribution of group keys in an MBSS(#1521)).

(…existing texts…)

*TGme editor: Modify Clause 9.6.13.20 as follows (track change on):*

**9.6.13.20 WNM Sleep Mode Response frame format**

(…existing texts…)

The Key Data Length field is the length of the Key Data field. If (#1722)management frame protection was not negotiated for the current association (#7049), this field is 0.

The Key Data field contains zero or more subelements that provide the current GTK, IGTK and BIGTK to the STA. The format of these subelements is shown in Figure 9-1286 (WNM Sleep Mode GTK subelement format), Figure 9-1287 (WNM Sleep Mode IGTK subelement format), and Figure 9-1288 (WNM Sleep Mode BIGTK subelement format).(#155) The subelement IDs for these subelements are defined in Table 9- 540 (Optional subelement IDs for WNM Sleep Mode parameters). When management frame protection was not negotiated for the current association (#7049), the Key Data field is not present.

(…existing texts…)

*TGme editor: Modify Clause 3.2 as follows (track change on):*

**3.2 Definitions specific to IEEE Std 802.11**

**robust management frame(#4340):** A Management frame that is in the subset of Management frames that are eligible for management frame protection. See 12.2.7 (Requirements for management frame protection).

NOTE—A Beacon frame is eligible for beacon protection, not management frame protection. (#7050)

*TGme editor: Modify Clause 4.5.4.9 as follows (track change on):*

**4.5.4.9 Management frame protection**

Robust Management frames are a subset of Management frames that can be protected by the management frame protection service (see 12.2.7 (Requirements for management frame protection) for a list of the robust Management frames). (#7050)

(….existing texts…)