IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11bi EDPKE comments (LB288) |
| Date: July, 2025 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Duncan Ho | Qualcomm Technologies, Inc | 5665 Morehouse Dr, San Diego CA 92131 USA | +1 (858) 845-3214 | dho@qti.qualcomm.com |

Abstract

This document contains the proposed resolution of the following CIDs received for TGbi LB288:

890, 168, 170, 171, 172, 179, 180, 293, 294, 295, 296, 413, 414, 720, 725, 727, 729, 730, 731, 732, 916, 142, 721

**Revision information**

**Introduction**

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. The abstract, revision information, introduction, explanation of the proposed changes and references sections are 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).***

Details of the CIDs and proposed resolution:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **Pg/Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 890 | Julien Sevin | 10.71.3 | 82.15 | The generation and distribution of the KDK are not defined | Please define the generation and distribution of the KDK | **Revised**Agreed in principle. For easier long-term maintenance, consolidate the requirements of KDK and WTK derivation in a single place - 12.6.1.1.6 (PTKSA) and refer to it when needed in other places of the spec.**TGbi editor to make the changes shown in** **the latest version of 11-25/1003 marked CID 890.** Notethetext changes are based on REVme D7.0. |
| 168 | Po-Kai Huang | 4.5.4.2 | 23.47 | "PASN and EDPKE authenticationallows for the protection of Management frames without association by establishing a PTKSA using authenticationframes." This sentence may be confusing because EDPKE does go to association eventually. Perhaps, a way to clarify is to have a separate sentence "EDPKE authenticationallows for the protection of (Re)Association Request/Response frame by establishing a PTKSA using authenticationframes." | As in comment | **Revised –**Agree in principle with the commenter.**TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 168** |
| 170 | Po-Kai Huang | 12.16.9.1 | 132.65 | Perhaps adding a note to clarify that we need KEK in PASN because PTK-KEK is used for group key handshake that may be used later even if PTK-KEK is not used in EDPKE frame exchange. | As in comment | **Revised**Agreed in principle. Add the following note: "The PTK-KEK derived in PASN will be used for group key handshake after association even if PTK-KEK is not used in EDPKE frame exchange".**TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 170** |
| 171 | Po-Kai Huang | 12.16.9.3.1 | 133.27 | The reference should be "12.13.3.1 (Overview)" rather than "12.12.3.1 (Overview)". | As in comment | **Accepted** |
| 172 | Po-Kai Huang | 12.16.9.3.2 | 133.40 | in RSNE construction of 12.13.3.2, we have "Group Data Cipher Suite and Group Management Cipher Suite set to 00-0F-AC:7, indicating thatgroup addressed traffic is not allowed." Since we will do association afterwards under EDPKE, this rule should not be followed. As a result, we should also list this as a difference. Based on baseline, just indicate group cipher of the BSS | As in comment | **Revised**Agreed in principle. Add the a bullet at the end of the bullet list to exclude the rule**TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 172** |
| 179 | Po-Kai Huang | 12.16.9.3.1 | 133.32 | "-- EDPKE AKMP is used instead of PASN AKMP. -- The RSNE indicates EDPKE instead of PASN." The two bullets needs to be deleted. The algorithm number is EDPKE, but the base AKMP is whatever AKMP we use and does not include PASN AKMP or EDPKE AKMP as defined in 12.16.9.1 General | As in comment | **Accepted** |
| 180 | Po-Kai Huang | 12.16.9.3.2 | 133.46 | -- EDPKE AKMP is used instead of PASN AKMP. -- The RSNE indicates EDPKE instead of PASN. The two bullets needs to be deleted. The algorithm number is EDPKE, but the base AKMP is whatever AKMP we use and does not include PASN AKMP or EDPKE AKMP as defined in 12.16.9.1 General | As in comment | **Accepted** |
| 293 | Jay Yang | 12.16.9.3.2 | 133.52 | not sure whether the 2-authentication and 3-authentication frame are exchanged on the same link or a different links? | please add some texts to say "the 2nd authentication frame and 3rd authentication frame shall be exchanged on the same link as the first authentication frame" | **Revised**Agreed in principle. **TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 293** |
| 294 | Jay Yang | 12.16.9.3.2 | 133.52 | add the text to clarify the 2nd Authentication frame will be sent by the coreponding AP affliciated with AP MLD. Otherwise, the 2nd Authentication frame will be sent by the AP if we follow the baseline rule. | "add the following text ""the second Authentication frame will be sent on correponding AP affiliated with the AP | **Revised**Agreed in principle. **TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 293** |
| 295 | Jay Yang | 12.16.9.3.2 | 133.52 | add some text to clarify the RA field and TA field are the affiliciated non-AP or affiliciated AP MAC address. | as the comments | **Revised**Agreed in principle. Note that addressing is described in general in 35.3.2 MLD addressing. **TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 293** |
| 296 | Jay Yang | 12.16.9.3.4 | 134.09 | the MLD MAC address should be included in basic ML element in the three authentication frames. | as the comments | **Revised**Agreed in principle. We add a note. Note that this is already the case due to **Table 9-70—Authentication frame body revision in 11be “The Basic Multi-Link element is present if dot11MultiLinkActi-vated is true and the frame exchange is with a peer STA that is affiliated with an MLD. Otherwise, it is not present.”** and 35.3.5.4 Basic Multi-Link element usage in the context of ML (Re)Setup, Authentication, and FT Action frame exchanges between two MLDs “A STA affiliated with an MLD shall include a Basic Multi-Link element in an Authentication frame or FT action frame that it transmits with the following rules:—the STA shall include the MLD MAC address of the MLD with which the STA is affiliated in the Common Info field of the element—the STA shall set all subfields in the Presence Bitmap subfield of the Multi-Link Control field of the element to 0—the STA shall not include the Link Info field of the element.”**TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 296**  |
| 413 | Mark RISON | 9.3.3.11 | 42.57 | "wrapped data format in PASN Parameters element" -- not clear what field this is referring to | Refer to an actual field name | **Revised**Agreed in principle.Replace "wrapped data format" with "Wrapped Data Format field".**TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 413** |
| 414 | Mark RISON | 9.3.3.11 | 43.05 | "RSNE is present and PASN Parameterselement is present if Status Code field is 0." is ambiguous as to scope of "if" | 414 | **Revised**Agreed in principle. Replace "RSNE is present and PASN Parameters element is present if Status Code field is 0." with "RSNE is present if Status Code field is 0. PASN Parameters element is present if Status Code field is 0.".**TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 414** |
| 720 | Mark RISON | 12.16.9.1 | 132.63 | "If dot11EDPKEActivated is true, then dot11EDPReAssociationFrameEncryptionSupportActivated and dot11KEKPASNActivated are set to true. " is too wishy-washy | Change "are" to "shall be" | **Accepted** |
| 725 | Mark RISON | 12.16.9.3.1 | 133.47 | "-- The RSNE indicates EDPKE instead of PASN." -- indicates where? If in the AKM list, then the previous bullet already says this | Delete the cited text | **Accepted** |
| 727 | Mark RISON |  | 0.00 | I think the convention is to use normal case for headings, not Uppercase the Key Words | E.g. "EDPKE Frame Construction and Processing" should be just "EDPKE frame construction and processing" | **Revised –**Agree in principle with the commenter. **TGbi editor to make the changes shown in the latest version of 11-25/1003 under all headings that include CID 727** |
| 729 | Mark RISON | 12.16.9.3.2 | 133.53 | "The RA field of an Authentication frame in response to an Authentication frame from the peer shall be set to the TA field of the Authentication frame from the peer. " -- by definition a response is to the peer | Delete "from the peer" 2x | **Accepted** |
| 730 | Mark RISON | 12.16.9.3.2 | 133.65 | "The same procedures as specified in 12.13.8 (PTKSA derivation with PASN authentication) are used." is followed by "the following modifications shall be used:". Similarly at 134.6 | Change to "The same procedures as specified in 12.13.8 (PTKSA derivation with PASN authentication) shall be used, except that for MLO:" and then use "shall be used" instead of "is used" in the bullets | **Accepted** |
| 731 | Mark RISON | 12.16.9.3.2 | 134.07 | "HMAC-HASH computation" -- not clear what this is, even less with the uppercase HASH | As it says in the comment | **Rejected**The "HMAC-HASH" is defined in the 12.13.9.2 (MIC computation for 3rd PASN frame). |
| 732 | Mark RISON | 12.16.9.3.2 | 134.14 | "NOTE 1--In order to ensure KEK derivation, the KEK In PASN field in the RSNXE from the peer STA is set to 1 (see 12.13.8 (PTKSA derivation with PASN authentication)." -- is this a new requirement? If so delete NOTE--- | As it says in the comment | **Accepted** |
| 916 | Duncan Ho | 12.16.9.2 | 133.12 | It is not clear if the combination of EDPK capable but not (re)Assoc encryption capable is allowed. | Clarify in the spec whether such combination is allowed. Will follow up with a contribution. | **Revised**Agreed in principle. Resolved by resolution of CID720. |
| 142 | Nehru Bhandaru | 11.3.2 | 99.30 | I have talked briefly about this before with other members, I am okay with EDPKE as its own 802.11 authentication method, for a good reason, that is close to PASN but concerned with it going from state 1 to 2 with state 2 to 4 with encrypted association. This means that no protected class 1 frames are possible with EDPKE; one has to do PASN for that. It's possible that EDPKE could transition to state 1a, get pre-association security and the encrypted association goes from state 1a to state 4. | Allow state transiton 1->1a with EDPKE and 1a->4 with EDPKE | **Rejected**We create EDPKE specially because we want to separate with PASN unassociated operation. Allow 1a to 4 is basically allowing PASN state to go to state 4. But EDPKE/PASN is not enough to do state 4 alone, we need (re)association request/response anyway. EDPKE is possible to move to state 2. Then we need (re)association request/response to go to state 4. |
| 721 | Mark RISON | 12.16.9.2 | 133.16 | "When the EDPKE AKMP is advertised, the AP shall also include at least one additional AKMP in the RSNE." -- why? Why can't the AP do EDPKE and nothing else? | Delete the cited text | **Rejected**This is because EDPKE AKMP is a wrapper AKM like PASN AKM. We need SAE AKM inside for authentication. This is there because we reuse the PASN design. |

**TGbi Editor: *Instruction: Modify 12.6.9.1 as follows***

* General

If dot11EDPKEActivated is true, then dot11EDPReAssociationFrameEncryptionSupportActivated and dot11KEKPASNActivated shall be(#720) set to true.

Enhanced Data Privacy Key Exchange (EDPKE) is an RSNA authentication protocol that uses the PASN procedures (see 12.12 (Preassociation security negotiation)) with the following differences:

* SAE AKMP 00-0F-AC:8, 00-0F-AC:9, 00-0F-AC:24, or 00-0F-AC:25 can be used as the Base AKMP.(#176)
* When there is no Base AKMP, EDPKE(#395) is not used.
* The three Authentication frames have the Authentication Algorithm Number field set to 9 (EDPKE Authentication).
* The generated PTK is used as the initial PTK once associated.

NOTE - The PTK-KEK derived in PASN will be used for group key handshake after association even if PTK-KEK is not used in EDPKE frame exchange.(#170)

**TGbi Editor: *Instruction: Modify 12.16.9.3.1 as follows***

* Overview

This subclause defines the procedures for establishing a PTKSA and the corresponding shared keys between an EDPKE capable STA and an EDPKE(#723) AP(#722) (for non-MLO) as well as between an(#723) EDPKE capable non-AP MLD and an EDPKE capable(#723) AP MLD (for MLO). The same procedures as specified in 12.13.3.1(#171) (Overview) are used with the following differences:

* The three Authentication frames have the Authentication Algorithm Number field set to 9 (EDPKE Authentication).
* (#179)(#179)For MLO, the PMKSA association is between the AP MLD and the non-AP MLD.

**TGbi Editor: *Instruction: Modify 12.16.9.3.2 as follows***

* EDPKE frame construction and processing(#727)

The same procedures as specified in 12.12.3.2 (PASN Frame Construction and Processing) are used with the following differences:

* The three Authentication frames have the Authentication Algorithm Number field set to 9 (EDPKE Authentication).
* (#180)(#180)The PTK is generated as specified in 12.16.9.3.4 (PTKSA derivation and MIC computation(#726) with EDPKE authentication).
* The requirement of group addressed traffic not allowed in PASN, i.e., setting the Group Data Cipher Suite and the Group Management Cipher Suite to 00-0F-AC:7, does not apply for EDPKE.(#172)
* The requirement of setting MFPR to 1 in the RSN Capabilities field does not apply for EDPKE.(#172)
* The requirement of setting No Pairwise bit to 0 in the RSNE does not apply for EDPKE.(#172)

NOTE – In RSN Capabilities field, there is no No Pairwise bit. (See 9.4.2.23.4 (RSN capabilities))

For MLO, the first Authentication frame can be sent by(#728) any of the non-AP STA affiliated with the non-AP MLD. The RA field of the second(#293) Authentication frame in response to the firstAuthentication(#293) frame (#729)shall be set to the TA field of the Authentication frame(#729). The RA field of the third Authentication frame in response to the second Authentication frame shall be set to the TA field of the Authentication frame. (#293)

**TGbi Editor: *Instruction: Modify 12.16.9.3.2 as follows***

* PTKSA derivation and MIC computation(#726) with EDPKE authentication

The same procedures as specified in 12.13.8 (PTKSA derivation with PASN authentication) shall be used except that for MLO: (#730).

* (#730)The AP MLD MAC address shall be used instead of the BSSID. (#730)
* The non-AP MLD MAC address shall be used instead of the SPA. (#730)

The same procedures as specified in 12.13.9.2 (MIC computation for third PASN frame) are used. For MLO, the following modifications shall be used for HMAC-HASH computation:

* The AP MLD MAC address is used instead of the BSSID.
* The non-AP MLD MAC address is used instead of the SPA.

The Key ID in the PTKSA (see 12.6.1.1.6 (PTKSA)) resulting from EDPKE authentication shall be 0.

In order to ensure KEK derivation, the KEK In PASN field in the RSNXE from the peer STA is set to 1 (see 12.13.8 (PTKSA derivation with PASN authentication).(#732)

**NOTE1 -** The MLD MAC address corresponding to the affiliated STA that transmits the Authentication frame is included in the Basic Multi-link element in the three Authentication frames. See 35.3.5.4 (Basic Multi-Link element usage in the context of ML (Re)Setup, Authentication, and FT Action frame exchanges between two MLDs).(#296)

**TGbi Editor: *Instruction: 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

***Modify Table 9-70 (Authentication frame body) as follows (not all lines shown):***

* Authentication frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 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 certain Authentication frames as defined in Presence of fields and elements in Authentication frames. |
| 9a | Encapsulation Length | This field indicates the number of octets in the Encapsulation field as described in 9.4.1.82 (Encapsulation Length field). This is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames).(#408, #404, #406, #405)  |
| 9b | Encapsulation | This field is used to carry an EAPOL PDU as described in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames). This is present only when the Encapsulation Length field is nonzero.(#408)  |
| ... |  |  |
| 17 | ~~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). |
| ... |  |  |
| 25 | PASN Parameters | A PASN Parameters element is present only in certain Authentication framesas defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| ... |  |  |
| 29 | Diffie-Hellman Parameter | A Diffie-Hellman Parameter element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |

***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 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. |
| .... |  |  |  |
| IEEE 802.1X authentication | 1 | Reserved  | The Encapsulation Length field is present.The Encapsulation field is present only when the Encapsulation Length field is nonzero.The AKM Suite Selector element is optionally present as defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames).The RSNE is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The RSNXE is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The Nonce element is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The Diffie-Hellman Parameter element is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The MDE is optionally present as defined in 12.16.8.3 (FT initial mobility domain association(#176)).(#176, #Ed) |
| IEEE 802.1X authentication | 2 | SUCCESS | The Encapsulation Length field is present.The Encapsulation field is present only when the Encapsulation Length field is nonzero.The AKM Suite Selector element is optionally present as defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames).The RSNE is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The Nonce element is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The Diffie-Hellman Parameter element is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The MDE is optionally present as defined in 12.16.8.3 (FT initial mobility domain association(#176)).(#176, #Ed)The FTE is optionally present as defined in 12.16.8.3 (FT initial mobility domain association(#176)).(#176, #Ed) |
| IEEE 802.1X authentication | 2 | Not SUCCESS | The Encapsulation Length field is present.The Encapsulation field is present only when the Encapsulation Length field is nonzero. |
| IEEE 802.1X authentication | > =3(#410) | Status | The Encapsulation Length field is present.The Encapsulation field is present only when the Encapsulation Length field is nonzero. |
| EDPKE authentication | 1 | Reserved | The RSNE is present.The RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.The MDE is present if the Base AKMP is 00-0F-AC:9 or 00-0F-AC:25.(#176, #Ed)The PASN Parameters element is present.The Timeout Interval element is optionally present.(#411)The Wrapped Data element is present if the Wrapped Data Format field(#413) in the PASN Parameters element is nonzero and not reserved.(#Ed) |
| EDPKE authentication | 2 | Status | RSNE is present if Status Code field is 0. PASN Parameters element is present if Status Code field is 0.(#414)The RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.The MDE and the FTE are present if the Base AKMP is 00-0F-AC:9 or 00-0F-AC:25.(#176, #Ed)The Timeout Interval element is optionally present.(#411)The Wrapped Data element is present if Wrapped Data Format field(#413)in the PASN Parameters element is nonzero and not reserved and the Status Code field is 0.The MIC element is present.(#Ed) |
| EDPKE authentication | 3 | Status | The PASN Parameters element is present if Status Code field is 0.The Wrapped Data element is present if Wrapped Data Format field(#413)in the PASN Parameters element is nonzero and not reserved; and the Status Code field is 0.The MIC element is present.(#Ed) |

**TGbi Editor: *Instruction: Modify 4.5.4.2 as follows***

**4.5.4.2 Authentication**

***Change the third, fourth, sixth paragraph as follows:***

IEEE Std 802.11 defines the following ~~five~~ IEEE 802.11 authentication methods: ~~Open System authentication, FT authentication, simultaneous authentication of equals (SAE), FILS authentication, and preassociation security negotiation (PASN) authentication~~

* Open System authentication admits any STA to the DS.
* FT authentication relies on keys derived during the initial mobility domain association to authenticate the stations as defined in Clause 13 (Fast BSS transition).
* SAE authentication uses finite field cryptography to prove knowledge of a shared password.
* IEEE 802.1X authentication uses EAP to authenticate STAs and the AS with one another.
* FILS authentication allows for faster connection to the network for FILS non-AP STAs by providing authentication, association, and key confirmation information in an efficient number of frame exchanges (see 4.10.3.6 (AKM operations using FILS authentication)).
* PASN (#168)authentication allow~~s~~ for the protection of Management frames without association by establishing a PTKSA using authentication frames.
* EDPKE authentication allows for the protection of (Re)Association Request/Response frame by establishing a PTKSA using authentication frames.(#168)

The IEEE 802.11 authentication mechanism also allows definition of new authentication methods, or any combination of these authentication methods.(#10) (#168)

**Text to be adopted (for CID 890) begins here.**

4.10.3.2 AKM operations with AS

***TGbi editor: Please modify the 2nd paragraph of 4.10.3.2 as follows:***

A 4-way handshake or FT 4-way handshake utilizing (#1836)EAPOL-Key PDUs is initiated by the

Authenticator to do the following:

— Confirm that a live peer holds the PMK.

— Confirm that the PMK is current.

— In the case of fast BSS transition, derive PMK-R0s and PMK-R1s.

— Derive a fresh pairwise transient key (PTK) from the PMK or, in the case of fast BSS transition, from the PMK-R1. The derived PTK includes the key derivation key (KDK) under the conditions defined in 12.6.1.1.6 (PTKSA).

—Derive a fresh WTK from the KDK(11ba) under the conditions defined in 12.6.1.1.6 (PTKSA).

— Install the pairwise encryption and integrity keys, and the WTK.(11ba), if derived.

— Transport the group (#1349)keys and sequence number from Authenticator to Supplicant and install the (#1349)group keys and sequence number in the STA and, if not already installed, in the AP.

— Verify that the RSN capabilities negotiated are valid as defined in 9.4.2.23.4 (RSN capabilities).

— Confirm the cipher suite selection.12.6.1.1.6 PTKSA

***TGbi editor: Please modify the 5th paragraph of 12.6.1.1.6 as follows:***

The PTKSA consists of the following:

— PTK(11ba), where the PTK includes the KDK only when any of the following is true:

* WUR frame protection is negotiated.
* dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support capability in its RSNXE (see 9.4.2.240 (RSNXE)).
* Frame anonymization is negotiated (see 10.71 (Frame anonymization))(11bi).

— Pairwise cipher suite selector(11ba), and when WUR frame protection is negotiated, the cipher suite selector 00-0F-AC:6 (BIP-CMAC-128) for individually addressed WUR Wake-up frames

— (#4109)Supplicant MAC address, depending on the negotiated AKMP(#271)(#3266)

— (#4109)Authenticator MAC address, depending on the negotiated (#3266)AKMP(#271)

— Key ID

— If FT key hierarchy is used,

— R1KH-ID

— S1KH-ID

— PTKName

— (11ba)If WUR frame protection is negotiated,

— WTK

12.7.1.3 Pairwise key hierarchy

***TGbi editor: Please modify the 2nd paragraph of 12.7.1.3 as follows:***

The PTK is partitioned into (#3744)PTK-KCK, PTK-KEK, (11ba)a temporal key, and a KDK, if derived under the conditions defined in 12.6.1.1.6 (PTKSA).

12.7.1.6.5 PTK

***TGbi editor: Please modify the 2nd paragraph of 12.7.1.6.5 as follows:***

Using the KDF defined in 12.7.1.6.2 (Key derivation function (KDF)), the PTK derivation is as follows:

(#478)PTK = KDF-Hash-Length(PMK-R1, “FT-PTK”, SNonce || ANonce || BSSID || STA-ADDR)

where

(#478)KDF-Hash-Length is the key derivation function as defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-190 (AKM suite selectors))

PMK-R1 is the key that is shared between the S1KH and the R1KH

SNonce is a 256-bit random bit string contributed by the S1KH

ANonce is a 256-bit random bit string contributed by the R1KH

STA-ADDR is the non-AP STA’s MAC address

BSSID is the BSSID of the target AP’s BSS

Length(#3686) is the total number of bits to derive, i.e., number of bits of the PTK. The length is dependent on the negotiated cipher suites and (#3266)AKMP as defined by Table 12-8 (Cipher suite key lengths(#1083)(#3532)) in 12.7.2 (EAPOL-Key frames) and Table 12-11 (Integrity and key wrap algorithms(#3244)) in 12.7.3 (EAPOL-Key PDU construction and processing)(11ba), and whether a KDK is derived (see 12.6.1.1.6 (PTKSA) for the conditions of derivation of KDK).

12.7.6.2 4-way handshake message 1

***TGbi editor: Please modify the 2nd paragraph of 12.7.6.2 as follows:***

Processing for PTK generation is as follows:

The Authenticator sends message 1 to the Supplicant at the end of a successful IEEE 802.1X authentication, after (re)association completes for a STA that has authenticated with SAE or for which PSK authentication is negotiated(#3434), when a cached PMKSA is used, or after a STA requests a new key. On reception of message 1, the Supplicant determines whether the Key Replay Counter field value has been used before with the current PMKSA. If the Key Replay Counter field value is less than or equal to the current local value, the Supplicant discards the message. Otherwise, the Supplicant:

a) Generates a new nonce SNonce, if no SNonce has yet been generated for this 4-way handshake. The same SNonce is reused within this 4-way handshake until a valid message 3 has been received.(#6483)

b) Derives PTK,.

c) Constructs message 2.

13.2 Key holders

13.2.1 Introduction

***TGbi editor: Please add the following after the last paragraph of 13.2.1:***

The derived PTK includes a Key derivation key (KDK) under the conditions described in 12.6.1.1.6 (PTKSA).13.2.2 Authenticator key holders

***TGbi editor: Please modify the 4th paragraph of 13.2.2 as follows:***

The R1KH and S1KH each derive the PTK(11ba). If WUR frame protection is negotiated, the R1KH and S1KH each derive a WTK from the KDK, which is part of the derived PTK.

13.2.3 Supplicant key holders

***TGbi editor: Please modify the 4th paragraph of 13.2.3 as follows:***

The S1KH shall derive the PTK mutually with the R1KH(11ba)t. If WUR frame protection is negotiated, the S1KH shall derive a WTK from the KDK, which is part of the derived PTK.

**Text to be adopted (for CID 890) ends here.**