**IEEE P802.11
Wireless LANs**

|  |
| --- |
| **Normative text for EDMG FAA** |
| **Date**: 2016-12-06 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Rob Sun | Huawei Technologies Co., Ltd.  | Suite 400, 303 Terry Fox Drive, Kanata, Ontario K2K 3J1  | +1 613 2871948  | Rob.sun@huawei.com  |

**Abstract**

The submission provides normative text based on the ideas presented in 11-16-0354-01-00 which satisfy the requirements of SFD

**Notice:** This document has been prepared to assist IEEE 802.11. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

**Release:** The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.11.

**Patent Policy and Procedures:** The contributor is familiar with the IEEE 802 Patent Policy and Procedures <[http:// ieee802.org/guides/bylaws/sb-bylaws.pdf](#_blank)>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <stuart@ok-brit.com> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.11 Working Group. **If you have questions, contact the IEEE Patent Committee Administrator at <**patcom@ieee.org**>**.

***Insert the following definition into 3.1:***

***Modify section 4.5.4.2 as indicated and highlighted:***

4.5.4.2 Authentication

.

IEEE Std 802.11 defines another additional 802.11 authentication methods to complement the existing IEEE 802.11 authentication mechanisms, specifically the DMG/EDMG Fast Authentication and Association, a.k.a EDMG FAA. The EDMG FAA method are defined in this version of the specification. The FAA authentication exchange is utilized with the Non-TTP (Trust Third Party) and the authentication is processed between at the EDMG PCP/AP and the EDMG STA at some scenarios where the round trip of authentication and association timing is extremely crucial for the link setup. In order to expedite the authentication and association process, the exchange of the authentication is piggybacked with other management frames during discovery and association. An EDMG STA that discovers an EDMG FAA-capable PCP/AP through the FAA indication bit may begin the Fast Authentication and Association protocol and perform mutual authentication using the pre-shared credentials. Otherwise the STA may perform full EAP authentication via IEEE 802.1X authentication. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods. Between the PCP/AP and the STA, they may have multiple preshared keys in order to increase the security functions, and they will proceed with the Key ID to indicate the appropriate preshared key for the instance of the FAA authentication.

An RSNA shall support DMG/EDMG Fast Authentication and Association Protocol. An RSNA which supports FAA authentication based on IEEE Std 802.1X-2004, and the preshared keys (PSKs) within the PBSS. IEEE 802.1X authentication may also utilize the EAP to authenticate DMG/EDMG STAs and the PCP/AP with one another.

***Modify section 4.5.4.3 as indicated and highlighted:***

* Deauthentication

The deauthentication service is invoked when the FAA is to be terminated..

In an RSN PBSS, Open System authentication is optional, but a STA is required to recognize Deauthentication frames. Deauthentication results in the IEEE 802.1X Controlled Port for that STA being disabled and deletes the PTKSA.

***Create section 4.10.3.4a***

**4.10.3.4a AKM operations using FAA authentication**

It is assumed that the PCP/AP, functioning as the authenticator has a pre-shared credentials, i.e the pre-shared keys with DMG/EDMG STA.

The following operations are carried out when FAA authentication is used with preshared keys:

1. The STA discovers the AP’s policy through passive monitoring of Beacon frames or through active probing or through announcement frames or other means. If a FAA-capable STA discovers that the AP supports FAA authentication, the STA and AP proceed to FAA authentication
2. The PCP/AP initiates FAA authentication by sending a FAA Authentication IE with the authentication information. The FAA authentication IE and other informations are carried within the DMG Beacons and broadcasted to the EDMG STA. Upon receiving the DMG Beacon, if applicable, the EDMG STA should responds through the 802.11 association requests frame in which the FAA authentication information element are embedded within the authentication IE.
3. The PCP/AP which receives a association request from the EDMG STA shall respond to the STA with an Association response frame with FAA information. The STA and AP generate a PTK, and the KEK, KCK and TK as a result of this exchange. The FAA authentication is complete at this step and the generated pairwise keys are used to encrypt and decrypt the data frames afterwards. This exchange provides proof-of-possession of the PMK which is assigned the value of the pre-shared key and enables the creation of a PTKSA and further establish the
4. The EDMG STA can optionally send a response frame to the AP within either management frame or data frame to acknowledge the receipt of the association response frame which completes the FAA authentication. This exchange provides the proof of the completion of the authentication from both parties and the further establishment of the data communication



 **Figure —FAA Authentication**

***Create section 4.10.3.4b***

**4.10.3.4b AKM operations using FAA authentication with Key ID**

It is assumed that the PCP/AP, functioning as the authenticator has multiple pre-shared credentials, i.e the pre-shared keys with DMG/EDMG STA, the usage of the pre-shared key shall be indicated by the key ID during the exchange of the authentication information.

The following operations are carried out when FAA authentication is used with pre-shared keys:

1. The STA discovers the AP’s policy through passive monitoring of Beacon frames or through active probing or through announcement frame or other means. If a FAA-capable STA discovers that the AP supports FAA authentication, the STA and AP proceed to FAA authentication
2. The PCP/AP initiates FAA authentication by sending a FAA Authentication IE with the authentication information. The FAA authentication IE and other informations are carried within the DMG Beacons and broadcasted to the EDMG STA. When the PCP/AP chooses to authenticate with the EDMG STA with a particular pre-shared key with key ID as indicated within the authentication IE. Upon receiving the DMG Beacon, if applicable , the EDMG STA should responds through the 802.11 association requests frame in which the FAA authentication information element are embedded within the authentication IE. At the state of message exchange, the EDMG STA starts the generation of the PTK based on the pre-shared key as indicated by the key ID. If the key ID is not valid, the EDMG STA shall start the de-authentication process
3. The PCP/AP which receives a association request from the EDMG STA shall respond to the STA with an Association response frame with FAA information. The STA and AP generate a PTK, and the KEK, KCK and TK as a result of this exchange. The FAA authentication is complete at this step and the generated pairwise keys are used to encrypt and decrypt the data frames afterwards. This exchange provides proof-of-possession of the PMK which is assigned the value of the pre-shared key and enables the creation of a PTKSA and further establish the
4. The EDMG STA can optionally send a response frame to the AP within either management frame or data frame to acknowledge the receipt of the association response frame which completes the FAA authentication. This exchange provides the proof of the completion of the authentication from both parties and the further establishment of the data communication

 

 ***Figure <ANA-X>***

***Modify section 9.4.2.25.4 as indicated and hightlighted:***

**9.4.2.25.4 RSN capabilities**

The FAA capability is indicated through the RSN Capabilities field indicates requested or advertised capabilities at the bit position of B14. If the RSN Capabilities field is not present, the default value of 0 is used for all of the capability subfields.

The length of the RSN Capabilities field is 2 octets. The format of the RSN Capabilities field is as illustrate.



Bit 14: EDMG Fast Authentication and Association (FAA) capability. A PCP/AP sets this bit to 1 to indicate that it is FAA capable and another FAA authentication IE will be appended to the management frame. If PCP/AP sets this bit to 0 which is non-FAA capable.

Bit 15: Reserved. The remaining of the RSN capability field are reserved.

***Create section 9.4.2.176 as indicated:***

9.4.2.176 EDMG FAA Authentication IE

When a PCP/AP sets the EDMG FAA capability bit to 1, the PCP/AP shall append the EDMG Authentication IE into the frame which carries the information for the FAA authentication.

The format of the EDMG FAA Authentication IE is defined in figure <xxxxx>



Figure <ANA-1> EDMG FAA Authentication Information Element

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

The structure of the EDMG Auth Options subfield within the EDMG Auth Options field is defined in figure <xxxxx>



The encoding of the Association Authentication type subfield (B0-B1) within the EDMG Auth Options field is defined as following table <xxxx>

|  |  |
| --- | --- |
| B0B1 | Definition |
|  00 |  Reserved |
|  01 |  EDMG PBSS Fast Association/Authentication with PSK |
|  10 | EDMG PBSS Fast re-association/ re-authentication with PSK |
|  11 | EDMG association/authentication using other frames than 802.11 association/authentication frames |

The encoding of the handshake subfield (B2-B3) within the EDMG Auth Option field is defined as following table <xxxx>

|  |  |
| --- | --- |
| B2B3 | Definition |
| 00 | Message #1 (Within the DMG Beacon or other frames) |
| 01 | Message #2( Within the 802.11 (re) Association Request Frame) |
| 10 | Message #3 (Within the 802.11 (re) Association Response Frame) |
| 11 | Message #4 (Not used if B0::B1= 01 and 10) |

The Key ID Usage indication bit (B4) is set to indicate whether the EDMG FAA authentication is configured to authenticate the peer based on the pre-shared key indicated by the Key ID which is both pre-known to the PCP/AP and the EDMG STA.

The Key ID initiator subfield (B4) within the EDMG Auth Options field is to indicate the originator of the Key ID, the encoding of the Key ID subfield is defined as following table <xxxx>

|  |  |
| --- | --- |
| B4 |  Definition |
| 0 | PCP/AP as Key ID initiator |
| 1 | EDMG STA as key ID initiator |

B5-B7 are reserved, the rest of the EDMG Auth Options subfields are reserved.

The Key ID field within the EDMG Authentication IE is 1 octet and the encoding of this field is based on the Key ID usage indication bit (B4) within the EDMG Auth Options. If the Key ID usage indication bit is set to be 0, then the Key ID field shall be set all 0’s. Otherwise, the Key ID field shall be set to the value of the Key ID associated with the Key.

The Nonce field within the EDMG Authentication IE is 32 octets long and it’s defined to carry the Nonce value which is input into the FAA authentication protocol and for the generation of the PTK keying materials. The generation of the Nonce is based on the mechanism specified in 12.7.5

The MIC field within the EDMG Authentication IE is 2 octets, The MIC field contains a message integrity code calculated over the EDMG Authentication IE

***Modify section 9.4.2.25.3 as indicated and highlighted:***

* + - * 1. AKM suites

The AKM Suite List field contains a series of AKM suite selectors contained in the RSN element. In the EDMG PBSS, AKM suite selector for the FAA authentication shall be specified as the following AKM suite selector.

Each AKM suite selector specifies an AKMP. Table 8-101 gives the AKM suite selectors defined by this -standard. An AKM suite selector has the format shown in Figure 8-187.

|  |
| --- |
| * Table 9-133 -- AKM suite selectors
 |
| OUI | Suite type | Meaning |
| Authentication type | Key management type | Key derivation type  |
| 00-0F-AC | <ANA-14> | EDMG FAA | FAA key management as defined in 12.12 | Defined in 12.12 |
| Other | Any | Reserved | Reserved | Reserved |

***Modify section 11.5.1.1.2 as indicated:***

* PMKSA

When the PMKSA is the result of a successful EDMG FAA authentication, it is generated as a result of the successful completion of the EDMG FAA exchange. This security association is bidirectional. In other words, both parties use the information in the security association for both sending and receiving. The PMKSA is created by the Supplicant’s SME when the FAA with preshared key (PSK) completes successfully. The PMKSA is created by the Authenticator’s SME when the PMK assigned to the value of the PSK, The PMKSA is used to create the PTKSA. PMKSAs are cached for up to their lifetimes.

***Create section 12.12 and its component subsections***

**12.12 Authentication for EDMG FAA authentication and association**

The EDMG FAA Authentication protocol authenticates EDMG STAs to each other, with TTP is optionally supported. The authentication exchange can optionally be performed with PFS. The result of the EDMG FAA authentication and association protocol is a PTKSA. EDMG FAA authentication and association is an RSNA authentication protocol.

**12.12.1 Assumptions on EDMG FAA authentication and association**

The security of EDMG FAA authentication and association depends on the following assumptions:

1. If dot11RSNAEnabled is true, and if the RSNA is based on IEEE 802.1X AKM in PBSS.
2. No TTP (Trust Third Party) Auth Server required.
3. No other DMG STA in the proximity
4. Both PCP/AP and EDMG STA shares the common Shared Secret (PSK) cryptographically secure (NIST SP800-97) PSK is the Authentication Key ( at least 128bits)
5. The 1st message of 4 way handshake is now piggybacked over DMG beacon from PCP/AP. The EDMG FAA Capability Bit and EDMG FAA Authentication IE could be appended to the DMG Beacon, or Announcement or Probe Response Frames.
6. The 4th message of 4 way handshake is omitted in order to save flight time which traditionally is deployed for key confirmation purpose.

**12.12.2 EDMG FAA Authentication protocol**

The EDMG STA and the PCP/AP communicate using the EDMG FAA authentication IE carried over management frames during discovery and association phase,i.e the DMG Beacon, association request/response frames, to perform key establishment and 802.11 association frames to perform key confirmation.

After exchanging EDMG FAA authentication IE, the STA and AP derive from the pre-shared key which will be used to derive a set of secret keys that are authenticated after exchanging 802.11 association frames.

**12.12.2.1 Discovery with FILS Authentication**

An PCP/AP indicates that it is capable of performing EDMG FAA Authentication by constructing a EDMG FAA-capable Beacon or Announcement frame. The EDMG FAA-capable 802.11 Beacons or Announcement frame shall contain an AKM indicating support for FAA Authentication.

A EDMG STA that discovers a EDMG FAA-capable AP that supports the EDMG FAA authentication with the pre-shared key may begin the EDMG FAA Authentication protocol to the AP and construct the security association of the PMKSA and derive the subsequent keying materials including the PTK.

**12.12.2.2 Key Establishment with EDMG FAA Authentication**

A FILS-capable STA and AP establish a shared key by exchanging Authentication frames. The specific contents of the Authentication frame depend on the particular authentication technique—whether a TTP is being used or whether digital signatures are being used—and whether PFS is obtained in the exchange or not.

**12.12.2.2.2 EDMG FAA Key Establishment**

The PCP/AP constructs a DMG Beacon frame with the Authentication algorithm number set to <ANA-X> within the RSNE and sets the EDMG FAA capability to 1. The PCP/AP generates the random nonce which shall be encoded as the nonce field within the EDMG FAA authentication IE (see 9.4.2.176). The PCP/AP shall transmit the DMG Beacon frame to the EDMG STA.

Upon receiving the DMG Beacon frame from the PCP/AP. The DMG STA shall choose an random Nonce and processes the DMG Beacon frame. First, if the PCP/AP indicates it’s desired to use the preshared key from associated with the Key ID within the EDMG FAA authentication IE, the EDMG STA shall first check if the Key ID is the valid, the process of validation of the key ID field is out of the scope of this specification, then the EDMG STA will construct the PTKSA and corresponding security keys based on the pre-shared key associated with the Key ID. The EDMG STA shall respond with an 802.11 association request frame. Second, if the PCP/AP indicates that it’s desired to use the pre-shared key without the key ID indicated within the EDMG FAA authentication IE, the the EDMG STA will construct the PTKSA and corresponding security keys (see 12.7.12 ) based on the pre-shared key associated with the Key ID. The EDMG STA shall respond with an 802.11 association request frame with the attachment of the EDMG Authentication IE. Third, if the EDMG STA encounters any error or unexpected conditions, i.e the Key ID is not found, the EDMG STA shall not responded with 802.11 association request frame and terminate any intermediate security association.

At the second handshake message though the 802.11 association request, the PCP/AP shall be able to construct the PTKSA and the corresponding security keys based on the received Nonce and the Nonce it generated during the 1st handshake through the DMG beacon frame, and other security parameters. The PCP/AP then constructs an 802.11 association response frame with the EDMG Authentication IE and transmit to the EDMG STA.

The EDMG STA may optionally choose to acknowledge the PCP/AP with an FAA authentication Ack frame which is to complete the FAA authentication process. The FAA authentication Ack frame can be transmitted during ATI or DTI by a management frame (see xxx)

**12.7.12 Key Derivation with FAA Authentication**

Key derivation with EDMG FAA Authentication uses the KDF from section 12.7.1.7.2 to produce three keys, a key encryption key (KEK), a confirmation key (KCK), and a traffic key (TK). The inputs to the KDF are the two 16 octet nonces produced by the STA and AP, a constant label, the preshared key (PSK), and the key ID as the octet string if the Key ID is indicated. The length of the KEK shall be 128 bits, and the KCK shall be 128 bits, and therefore the output from the KDF shall be 512+TK\_bits, where TK\_bits is determined from table 11-4.

KEK | KCK | TK = KDF-X ( PSK, “EDMG Key Generation”, Min(MAC\_s, MAC\_a)||Max(MAC\_s, MAC\_a)||Min(SNonce, ANonce)|| Max(SNonce, ANonce))

Where X is 512+TK\_bits from table 11-4, the PSK is the preshared key, the Key ID is the octe string represents the Key ID if used, the MAC\_s is the MAC address of the EDMG STA to represent its identity and the MAC\_a is the MAC address of the PCP/AP to represent its identity, the SNonce is the 16 bit random Nonce generated and transmitted from the EDMG STA and the ANonce is the 16 bit random Nonce generated and transmitted from the PCP/AP .

If the Key ID is preferred, the Key derivation is constructed as following:

 KEK | KCK | TK = KDF-X(PSK, “EDMG Key Generation”, Key ID||Min(MAC\_s, MAC\_a)||Max(MAC\_s, MAC\_a)||Min(SNonce,ANonce)|| Max(SNonce, ANonce))

Where X is 512+TK\_bits, the PSK is the preshared key, the Key ID is the octe string represents the Key ID if used, the MAC\_s is the MAC address of the EDMG STA to represent its identity and the MAC\_a is the MAC address of the PCP/AP to represent its identity, the SNonce is the random Nonce generated and transmitted from the EDMG STA and the ANonce is the random Nonce generated and transmitted from the PCP/AP .