IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution to Comments | | | | |
| Date: 2018-06-11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Rob Sun | Huawei Technologies, Canada | Suite 400, 303 Terry Fox drive,  Kanata, On | +1 613 2781948 | Rob.sun@huawei.com |
| Yan Xin | Huawei Technologies, Canada |  |  | Yan.xin@huawei.com |

Abstract

This document presents suggested proposal towards CID 1064, 1067, 1180, 1289, 1437, 1438, 1440, 1441, 1442, 1443, 1444, 1446, 1552, 1640, 1658, 1659, 1660, 1661, 1728, 1729, 1862, 1869, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2198, 2199

***Modify the following definition into 10.3.1 as highlighted in red texts:***

* STA authentication and association

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause Number(C)** | **Comment** | **Proposed Change** | **Resolution** |
| 1064 | 12.12.3.3.2 | The dictionary definition of NONCE is "(of a word or expression) coined for or used on one occasion." and its use in cryptography relies on this property. The NONCE cannot be reused or the protocol is insecure. In 12.12.3.3.2 it says the EDMG FAA capable AP constructs a beacon that advertises the NONCE. For the NONCE to be used only once it would require changing the value of the NONCE in the beacon before every beacon is sent. | Fix FAA authentication so the nonce is never used twice or more. Add a note that it must be changed every beacon period. If this isn't feasible then remove FAA authentication. | Revised |
| 1067 | 4.5.4.2 | The paragraph gives brief description of each features that are cited in the first sentence. As EDMG FAA is also added, it's description should be added at the end of the paragraph. | Add one sentence for brief description of EDMG FAA at the end of the paragraph. | Revised |
| 1180 | 4.5.4.2 | The PAR says nothing about 802.11ay providing new security mechanisms. The changes related to the FAA are outside the scope of the project. | Consider carefully whether existing mechanisms (e.g. FILS, SAE) can meet the perceived needs of 802.11ay. If so, use them. If not, then make a PAR modification to include a new authentication mechanism.    If the FAA mechanism is retained, the TG will need to consult with WG officers to determine how its new security mechanisms will receive appropriate review by security experts. | Rejected 1) The FAA was introduced to fit for Usage scenario 1 of USR (Ultra Short Range) whereby the DMG Beacon is i) directional ii) within 10cm iii) The downloading is within 1 sec. 2) A fast authentication procedure needs to be help the scenario. It wouldn't work with SAE, as SAE is a slow Password/PSK based authentication, and it will not help the DMG/EDMG in UC #1 time budget. 3) For FILS, There is no mechanism delivering the key handshake in the beacon frames which is different. |
| 1289 | 12.12.3.4.1 | The cited paragraph states that the "FAA Authentication element" is transmitted from an AP or PCP possibly within a DMG Beacon or Announce frame to initiate FAA authentication. However, the FAA Authentication element contains a Nonce (Figure 55), which should not be broadcast by an AP or PCP to initiate an authentication exchange. | The FAA authentication process needs to be modified to replace the Nonce with a parameter that changes for each transaction with each STA, not for all STAs. | Revised |
| 1437 | 12 | The requirement that "No other DMG STA in the proximity" is unreasonable. How can this possibly be met? | Delete FAA or Revise FAA to not need this requirement | Rejected 1) In 11ay UC, Ultra Short Range is for the case where the devices is close proximity with the AP (<10cm) 2) The EDMG FAA is strictly to fit for this use case |
| 1438 | 12 | "RSNA is based on IEEE 802.1X AKM." is not precise. | Delete the cited text or rephrase to indicate the specific AKMs used. | Revised |
| 1440 | 12.12 | FAA is susceptible to dictionary attack. Merely saying a PSK is an SP800-97 PSK is insufficient, the important thing is not the size of the PSK but the number of possible values the PSK can take. Note that SP800-97 recommends against 802.11ai PSK mode because of the difficulty in securely distributing the PSK. The whole scheme collapses unless there's a way to securely distribute PSKs, which there is not. | Use SAE instead. SAE uses 802.11 Authentication frames which DMG STAs do not use. So then they should use them. If it is completely impossible to use 802.11 Authentication frames then SAE should be collapsed into a 3-message exchange using the "(Re)Association Request, (Re)Association Response, and FAA Authentication Ack." This would necessitate making the FAA Authentication Ack mandatory. Alternately, SAE could be one using special action frames for (E)DMGs. | Rejected 1) The FAA was introduced to fit for Usage scenario 1 of USR (Ultra Short Range) whereby the DMG Beacon is i) directional ii) within 10cm iii) The downloading is within 1 sec. 2) A fast authentication procedure needs to be help the scenario. It wouldn't work with SAE, as SAE is a slow Password/PSK based authentication, and it will not help the DMG/EDMG in UC #1 time budget. 3) For FILS, There is no mechanism delivering the key handshake in the beacon frames which is different. 4) SP800-97 still allows the usage of PSK as long as the PSK entropy is sufficient to meet the security requirements |
| 1441 | 12.7 | FAA generates a PMKSA but no PMK. It generates a PTK but no PTKSA | Use the RSN key hierarchy properly. | Rejected In 12.6.1.1.2, line 21-22, states the PMK is equal to the value of PSK |
| 1442 | 12.7 | FAA generates a KCK and KEK but never seems to use them. There cannot be any proof of possession of the PSK if there is no use of these keys derived from it. Since FAA merely takes a PSK and plumbs a TK to encrypt the air it would be much more efficient and even faster (the Very Fast Authentication and Association Protocol--VFAA) if you were to just specify that TKs be distributed instead of PSKs. | Use SAE instead. It properly does authentication based on proof-of-possession of the PSK. It generates a shared secret as the PMK. If FAA doesn't want to do any additional handshaking then it can take that PMK and just run it through a KDF to get a TK. | Rejected 1) The FAA was introduced to fit for Usage scenario 1 of USR (Ultra Short Range) whereby the DMG Beacon is i) directional ii) within 10cm iii) The downloading is within 1 sec. 2) A fast authentication procedure needs to be help the scenario. It wouldn't work with SAE, as SAE is a slow Password/PSK based authentication, and it will not help the DMG/EDMG in UC #1 time budget. 3) For FILS, There is no mechanism delivering the key handshake in the beacon frames which is different. 4) SP800-97 still allows the usage of PSK as long as the PSK entropy is sufficient to meet the security requirements |
| 1443 | 4.5.4.2 | "An RSNA which supports FAA authentication is based on IEEE Std 802.1X-2004, and the preshared keys (PSKs)." Are both 802.1X and PSK used at the same time? The most recent version of 802,1X is 2010. Is it intentional to go back and require the prior version? FAA with 802.1X is not defined. | Refer to the latest version of the relevant standard, IEEE Std 802.1X-2010. Define operation with 802.1X or delete refernces to it. | Revised.  Note to the commenter: the references are deleted. |
| 1444 | 12.12.3.4.1 | The handshaking for FAA begins with a beacon which is broadcast by the PCP/AP. This frame contains the Anonce which is put into the KDF. But if two DMG STAs both receive the same beacon, a distinct possibility, after discovering the PCP/AP then the Anonce will be the same for two different sessions. This is a problem because the security of the 4-way handshake, from which it look like FAA has borrowed, is based on the nonces being randomly generated, unique, and ephemeral for each 4-way handshake. If you reuse a nonce you adversely affect the security of the handshake. It seems FAA can very easily reuse a nonce. | Stop using a broadcast frame from the PCP/AP to initiate the handshake. Replace FAA with SAE and collapse the exchange into "(Re)Association Request, (Re)Association Response, and FAA Authentication Ack", use special DMG action frames to transmit SAE, or just require DMG STAs to use 802.11 Authentication frames now if they want to implement FAA. | Rejected 1) Due to the nature of usage for EDMG FAA which is essentially point to point for UC #1. It's safe to use in this case. 2) SAE is a slow process of the password/psk based, very computational intensive. it's not fit for the usage of UC #1.  3) With the clarification of the ANonce and SNonce usage per connection in section 12.12.3.3.2, it would relieve the concern. |
| 1446 | 4.5.4.2 | "The FAA authentication exchange is utilized with a non trusted third party (TPP)" | What are the 3 entities involved? The STA isn't a third party. Delete the cited text. | Revised . |
| 1552 | 4.5.4.2 | "IEEE Std 802.11 defines the following four IEEE 802.11 authentication methods: Open System 5 authentication, Shared Key authentication, FT authentication, and simultaneous authentication of equals 6 (SAE) and EDMG fast authentication and association (FAA)."    FILS autentication is not referred here. It is not clear FILS authentication can be used with 802.11ay. | Clarify the relationship between 802.11ay and 802.11ai FILS authentication. | Rejected IEEE 802.11ai FILS authentication doesn't fit in the message protocol flow with FAA. The first authentication message is piggybacked over the DMG beacon message while the FILS starts with IEEE 802.11 authentication message. |
| 1640 | 12.12 | The FAA construction with a fixed PSK and PTK derivation using ANonce/SNonce does not look particularly secure. Why is that added here? The existing PSK mechanism in 4-way handshake is already known to be problematic with weak passwords and same would apply for this new FAA design, so it would depend on some unspecified mechanism for pre-configuring cryptographically secure PSKs. What would that provisioning mechanism be? Why is FAA needed in the first place? SAE should be used if passwords-style authentication without EAP is desired (or alternatively, FILS public key authentication if this could use public keys instead of PSKs).    Would FAA be allowed for any STA, including operations in 2.4 and 5 GHz bands? | Remove FAA from P802.11ay or more clearly describe when it can (and more importantly, cannot be used) and how a secure PSK is going to be provisioned. | Rejected 1) The EDMG FAA was introduced in the paragraph of 4.5.4.2 with defintion. 2) The PSK geneation algorithm is out of scope but recommended to follow the NIST SP800-92 as specified in 12.12  3) EDMG FAA only applies to the 11ad/11ay devices |
| 1658 | 12.12.2 | Does the requirement of "No other DMG STA in the proximity" greatly limit the use of FAA? If yes, probably better to put some guidance/descriptive language in the usage scenrios. | Please clarify | Revised |
| 1659 | 12.7.12 | There is no KeyID used in line 10-11 | Please clarify | Rejected 1) In 12.7.12, there are two KDF function being defined. The first Key generation function is performed without the Key ID. 2) The second KDF function is performed with the use of Key ID |
| 1660 | 12.12.3.3.2 | At the beginning, it is said the pre-shared key without Key ID, but later at the end of the sentence, the pre-shared key assoicated with the Key ID is mentioned. Really confusing. Is it editorial issue or ? | Please clarify | Rejected The paragraph states that on line 16 that if both parties are desired to use the PSK with key ID. And on paragraph 20, on a second case, whereas both parties intend not to use the key ID. At later part of the, the Key ID (line 24) was mentioned for an exmple of exception handling. |
| 1661 | 12.12 | DMG does not support authenication as indicated in the 11ad Spec, what does it mean in 11ay or even in FAA authentication? Meanwhile, it seems "no RSNA required" or "4-way handshake is successful" is the condition for transition from state 2 to state 4. Does it mean after association, 4-way handshake is a must to unblock the 802.1X controlled ports instead of the newly defined new FAA? It is very confusing. | Please clarify | Revised |
| 1728 | 4.5.4.2 | Confusing wording. Is this saying that the TTP is not required (it is optional), so FAA can be done without a TTP? Or this just a typo, and it is (incorrectly) saying that FAA is done with a TTP (the "non" should be deleted) - in which case that's not entirely correct, because the TTP is optional? | Clarify | Revised |
| 1729 | 4.5.4.2 | What does this paragraph add, after the much more specific discussion just above (other than the date on 802.1X)? | Delete this paragraph. Add the "-2004" date to the earlier 802.1X reference (line 21). | Revised the paragrah is to add the definition of the EDMG FAA protocol and the usage. |
| 1862 | 4.5.4.2 | EDMG AP used in multiple instances in draft and not defined | Add definition in clause 3.0 Definitions | Rejected This is not the philosophy used in the 802.11 spec. For example, there is no definition (in section 3) for HT AP or VHT AP. |
| 1869 | 12.7.12 | SNonce and ANonce are 16 bit random values. The text doesn't call out that the SNonce and ANonce are to be used only once in a session and not repeated on future sessions. | Add Note in the security clause that a Snonce and Anonce are to be used once per session.  TGay may discuss this with REVmd | Revised |
| 2011 | 12.7.2 | If FAA is defining a new Key Derivation protocol it should be a new AKM. | Define a new AKM for FAA and include it in the RSN AKM table in Section 9. Update Section 12 as appropriate. | Rejected The AKM for FAA has been defined in section 9.4.2.23.3 |
| 2012 | 12.12.2 | Shared secrets are subject to dictionary attacks. IEEE 802.11 already includes SAE. Any new "shared secret" security protocol for IEEE 802.11 should be based on SAE. | Adjust FAA to be based on SAE and make the approprate changes in Clause 12. | Rejected 1) The FAA was introduced to fit for Usage scenario 1 of USR (Ultra Short Range) whereby the DMG Beacon is i) directional ii) within 10cm iii) The downloading is within 1 sec. 2) A fast authentication procedure needs to be help the scenario. It wouldn't work with SAE, as SAE is a slow Password/PSK based authentication, and it will not help the DMG/EDMG in UC #1 time budget. 3) For FILS, There is no mechanism delivering the key handshake in the beacon frames which is different. 4) SP800-97 still allows the usage of PSK as long as the PSK entropy is sufficient to meet the security requirements |
| 2013 | 12.12.2 | Anonce usage is bad. Furthermore authentication protocols that use Nonces are transactional (to ensure that Nonces are not reused). | Remove the Anonce from DMG Beacons and update the protocol as appropriate. If the desire is to piggyback the FAA security protocol on top of Authentication/Association frames, it would be much better to initiate the protocol on the STA side. So the SNonce is transmitted first. The FT protocol could be used as a model for this. If the FAA protocol is desired, the EDMG STA would have to support transmission and reception of IEEE 802.11 Authentication frames, or an Action frame to confirm completion for the key derivation after the IEEE 802.11 Association exchange. | Revised |
| 2014 | 12.12.2 | One issue with eliminating the 4th message of the 4-way handshake is that the peer STA does not know whether the security association has been confirmed/completed. | Adjust FAA to piggyback on top of Authentication and Association frames (they need to be transmitted in any case). Use the FT protocol as a model. (i.e. the non-AP/non-DMG STA initiates the protocol. That also eliminates the need to transmit Nonces in Beacons/Probe Responses). | Rejected 1) The fouth message is to add the key confirmation, however it's not cryptographically nessassry, i.e the WiMAX PKM protocol is 3 way handshake. 2) The FT protocol is not suitable for the authentication requirement here. |
| 2015 | 9.4.2.256 | It looks to me that this conveys a combination of protocol mode and key derivation mechanism. This looks like an AKM protocol. | Define new AKM(s) for FAA and include them in the RSNE | Rejected The AKM for FAA has been defined in section 9.4.2.23.3 |
| 2016 | 12.12.3.2.1 | "Authentication" frames? What Authentication frames. Is this referring to IEEE 802.11 Authentication frames? | Define the IEEE 802.11 frame that is transmitting information. | Revised |
| 2017 | 12.7.12 | I'm still not exactly sure what EDMG FAA Authenticaiton protocol is. The KDF in the referenced clause looks to refer to the FT protocol KDF. However its not clear which RSN AKM is used for this protocol. | Define a proper AKM for this and completely define how this protocol works and what frames and elements are used to transmit information. | Rejected The AKM for FAA has been defined in section 9.4.2.23.3 |
| 2198 | 4.5.4.2 | There is no description of EDMG FAA, all of the other authentication methods provide a description of what they are. Add a description of EDMG FAA including a reference to the clause where it is defined. | Add a description of EDMG FAA | Revised |
| 2199 | 4.5.4.3 | EDMG FAA is a type of authentication, just as Open System, Shared Key and SAE are. So placing EDMG FAA after the word authentication changes the intent of the sentence, EDMG FAA should simply be added to the list of authentication types. | Change the sentence to read:  "The deauthentication service is invoked when an existing Open System, Shared Key, SAE, or EDMG FAA authentication is to be terminated." | Accepted |

***Discussion:***

CID 1064, 1289, 1869 and 2013 are similar in nature which requires to properly define the one time usage of the ANonce and SNonce during the FAA handshake, the proposals have been revised in the following changes.

CIDs 1067, 1438, 1443, 1446, 1658, 1659, 1660, 1661, 1728, 1729, 2198, 1437, 2016 and 2199 require to add more clarification and remove some of the confusions during the description of the EDMG FAA protocol. Most of the proposed solution have been accepted and reflected in the following changes.

CIDs 1440, 1441, 1442, 1444, 1552, 1640, 2011, 2012, 2014 and 2015 require the modification of the EDMG FAA protocol to be in line with SAE protocol, or to define the new AKM for EDMG FAA, or reuse the FILS authentication protocol, or to reuse the FT protocol. The EDMG FAA protocol is designed for the 60Ghz 11ad/ay devices which are deployed for the USR (Ultra Short Range) applications, the USR use case requires <10cm in distance and the whole connectivity timing is within 0.6sec in accordance with the 11ay Usage Scenario document 11-15/0625. The SAE protocol is good with Password/PSK based authentication, however it usually comparably slow and computational intensive, hence it’s not fit for the time budge of the USR case.

CID 1180 states that 11ay PAR doesn’t contain the security requirements, however the FAA is a solution for the USR use case and it’s in line with the MAC layer enhancement requirements within the 11ay PAR.

CID 1862 requests the definition of the EDMG AP in clause 3, however it’s not in line with 802.11 convention, similiarly, there is no definition in clause 3 for HT AP and VHT AP.

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

***(Red for addition, Yellow for deletion)***

***(CID 1067, 1443, 1446, 1728, 1729, 2198)***

~~An RSNA might support EDMG FAA.~~ The FAA authentication exchange is ~~utilized with a non trusted third party (TPP) and~~ the authentication protocol that can be performed between an EDMG PCP or EDMG AP and the EDMG STA when the duration of authentication and association is crucial for the link setup, such as the Ultra Short Range usage scenario, whereby the distance is very short (<10cm) and the communication duration is very short (<600ms). 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 FAA-capable EDMG STA that discovers an FAA-capable EDMG PCP or EDMG AP can begin the fast authentication and association protocol and perform mutual authentication using the pre-shared credentials. Otherwise, the EDMG STA may perform full EAP authentication via IEEE 802.1X-2010 authentication or other type of AKM authentication mechanisms, such as SAE. Between an EDMG PCP or an EDMG AP and the EDMG STA there can be 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.

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

***(CID 2199)***

* Deauthentication

The deauthentication service is invoked when an existing Open System, Shared Key, ~~or~~ SAE authentication, ~~or~~ EDMG FAA is to be terminated

***Modify section 12.12.1 as indicated and highlighted:***

***(CID 1438)***

The EDMG FAA authentication protocol authenticates between the EDMG PCP or EDMG AP, and the EDMG STAs ~~to each other, with TTP being 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.

***Modify section 12.12.2 as indicated and highlighted:***

***(CID 1658, 1661, 2012, 2013)***

***12.12.2 ~~Assumptions~~ Requirements on EDMG FAA authentication and association***

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

* dot11RSNAEnabled is true.
* ~~RSNA is based on IEEE 802.1X AKM.~~
* ~~No TTP (Trust Third Party) Auth Server.~~
* No other DMG STA ~~in the proximity~~ in the EDMG PCP or EDMG AP’s antenna discovery coverage (i.e the Ultra Short Range Usage Scenarios)
* Both EDMG PCP or EDMG AP and non-PCP and non-AP EDMG STA share the common Shared Secret (PSK). Cryptographically secure (NIST SP800-97) PSK is the Authentication Key (at least 128bits).
* The 1st message of 4 way handshake is piggybacked onto DMG Beacon frames transmitted by an EDMG PCP or EDMG AP. The FAA Capable field and FAA Authentication element can be appended to DMG Beacon, ANonce ~~Announce~~ or Probe Response frames.
* The 4th message of 4 way handshake is omitted in order to save flight time which traditionally is deployed for key confirmation purpose.

***Modify section 12.12.3.3.1 as indicated and highlighted:***

***(CID 2016)***

An EDMG FAA-capable STA and AP or PCP establish a shared key by exchanging IEEE 802.11 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 7the exchange or not.~~

***Modify section 12.12.3.3.2 as indicated and highlighted:***

***(CID 1064, 1289, 1869, 2013)***

An EDMG PCP or EDMG AP that is EDMG FAA capable constructs a DMG Beacon frame with the Authentication algorithm number set to <ANA-X> within the RSNE and sets the FAA Capable field to 1. The PCP or AP generates the random nonce which shall be encoded as the Nonce field within the FAA Authentication element (see 9.4.2.256). In EDMG FAA protocol, the EDMG PCP or the EDMG AP shall only use the ANonce once within each broadcasting DMG Beacon transmission and for each FAA authentication and association.

Upon receiving a DMG Beacon frame from the PCP/AP, an EDMG STA chooses a random Nonce and processes the DMG Beacon frame, in EDMG FAA protocol, the EDMG STA shall only use the SNonce once for each FAA authencation and association. First, if the PCP or AP indicates desire to use the preshared key associated with the Key ID within the FAA Authentication element, 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 constructs 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 or AP indicates desire to use the pre-shared key without the key ID indicated within the FAA Authentication element, the EDMG STA constructs 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 Association Request frame including the FAA Authentication element. Third, if the EDMG STA encounters any error or unexpected conditions, e.g., the Key ID is not found, the EDMG STA shall not respond with an Association Request frame and shall terminate any intermediate security association.