IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution to Comments : CID 135,136,137,144 | | | | |
| Date: 2017-06-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Rob Sun | Huawei Technology | Suite 400, 303 Terry Fox drive,  Kanata, On | +1 613 2781948 | Rob.sun@huawei.com |
|  |  |  |  |  |

Abstract

This document presents suggested proposal towards CID 135,136,137,144 for .11ay D0.3

***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** |
| 135 | 4.10.3.6 | Much of the text in this sub clause reads as normative. | Move normative text elsewhere, such as in clause 11 | Revised |
| 136 | 4.10.3.6 | Resolve the editor comment regarding the last bullet item | As noted | Revised |
| 137 | 4.10.3.7 | Much of the text in this sub clause reads as normative. | Move normative text elsewhere, such as in clause 11 | Revised |
| 144 | 9.4.2.256 | How is this done? Need to specify | As noted | Revised |

***Discussion:***

Both CID 135, 137 suggested moving the respective sub clauses to the clause 11 since they both are normative text. The revised resolution is to define the AKM operation for FAA authentication protocol within the clause 12 which seems more appropriate.

CID 136 points out the purpose of FAA Authentication Ack at the end of FAA handshake is unclear. The original design purpose is to fully Ack the reception of the 802.11 Association Resp frame with the Authentication IE and matching the 802.11 the 4th message of the 802.11 4 way handshakes. After examining the FAA protocol, the optional FAA authentication Ack doesn’t provide security enhancements. Hence the revised resolution is to remove the optional FAA authentication Ack from the protocol. There are also relevant sub clauses need to be changed.

CID 144 requires the clarification of the MIC field within EDMG FAA Authentication IE. The revised resolution provides the definition.

**Proposed Resolution:**

***Modify Sub clause 9.4.2.256 with the highlight***

9.4.2.256 EDMG FAA Authentication IE

***Modify Figure 43 with the highlighted Change***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | EDMG Auth Options | Key ID | Nonce | MIC |

Octets: 1 1 1 1 1 32 ~~2~~ 16

**Figure 43 —FAA Authentication element format**

***Modify the text at line 30 as:***

The MIC field within the EDMG Authentication IE is 16 octets, The MIC field contains a message integrity code calculated over the EDMG FAA Authentication ~~IE~~ element. The MIC value is 128 bits and calculated with KCK and the AES-128-CMAC algorithm. The AES-128-CMAC is defined by NIST SP 800-38B and also found in IETF RFC 4493.

***Create Sub clause 12.12.3.4***

**12.12.3.4 AKM operations using FAA authentication**

*Create Sub clause 12.12.3.4.1 and move 4.10.3.6 with highlighted modifications to this sub clause, and then remove 4.10.3.6.*

### 12.12.3.4.1 AKM operation using FAA authentication without Key ID

It is assumed that an EDMG PCP or EDMG AP, functioning as the authenticator, has a pre-shared credential, i.e., a pre-shared key with an EDMG STA.

The following operations, depicted in Figure 1, are carried out when FAA authentication is used with pre-shared key:

* The STA discovers the AP’s or PCP’s policy through passive monitoring of DMG Beacon or Announce frames, through active probing or other means. If an FAA-capable EDMG STA discovers that the EDMG AP or EDMG PCP supports FAA authentication, the STA and the AP or PCP, respectively, can proceed to FAA authentication.
* The PCP or AP initiates FAA authentication by sending a FAA Authentication element with the authentication information. The FAA authentication element is carried within DMG Beacon, Announce or Probe Response frames and broadcasted to the STA. Upon receiving the DMG Beacon, the EDMG STA can initiate the 802.11 association procedure and transmit the FAA Authentication element.
* The PCP or AP which receives an Association Request from the EDMG STA responds to the STA with an Association Response frame with FAA information. The STA and the AP or PCP 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 establishment of the data communication.
* ~~The EDMG STA can optionally send a response frame to the AP or PCP 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 without Key ID**

*Create Sub clause 12.12.3.4.2 and move 4.10.3.7 with highlighted modifications to this sub clause, and then remove 4.10.3.7*

### 12.12.3.4.2 AKM operations using FAA authentication with Key ID

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

The following operations, depicted in Figure 2, are carried out when FAA authentication is used with pre-shared keys:

* The STA discovers the AP’s or PCP’s policy through passive monitoring of DMG Beacon or Announce frames, through active probing or other means. If an FAA-capable EDMG STA discovers that the EDMG AP or EDMG PCP supports FAA authentication, the STA and the AP or PCP, respecticely, can proceed to FAA authentication.
* - The PCP or AP initiates FAA authentication by sending a FAA Authentication element with the authentication information. The FAA authentication element is carried within DMG Beacon, Announce or Probe Response frames and broadcasted to the STA.
* - Upon receiving the DMG Beacon, the EDMG STA can initiate the 802.11 association procedure and transmit the FAA Authentication element. The PCP or AP can choose to authenticate with the EDMG STA with a particular pre-shared key and specify the key ID within the FAA Authentication element. 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 starts the de-authentication process.
* - The PCP or AP which receives an Association Request from the EDMG STA responds to the STA with an Association Response frame with FAA information. The STA and the AP or PCP 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 establishment of the data communication.
* ~~The EDMG STA can optionally send a response frame to the AP or PCP 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 with Key ID**

***Modify* *sub clause 12.12.3.3.2 by removing text between line 31 and 33***

**12.12.3.3.2 EDMG FAA Key Establishment**

~~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)~~

SP~~:~~

Do you agree to adopt the comment resolutions to CID 135,136,137,144 as proposed in doc: IEEE 802.11-17/xxxxr0?