IEEE P802.11 Wireless LANs

|  |
| --- |
| Proposed Optimized RSN Information Encoding in FILS Discovery Frame  |
| Date: 2014-1-3 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Lei Wang | self |  | 1 858 205 7286 | leiw@billeigean.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes an optimized RSN information encoding in FILS Discovery frame, as a proposed resolution to a comment submitted to IEEE 802.11 Working Group Technical Letter Ballot 198 for 802.11ai Draft 1.0.

# Introduction

As a response to IEEE 802.11 Working Group Technical Letter Ballot 198 for 802.11ai Draft 1.0 [Ref-3], the following comment is submitted:

***Comment****: line 16 on page 64, Section 8.5.8.35*

*The RSNE is used in FD frame to support the 11ai STA that needs to use full EAP, e.g., without valid rRk for EAP-RP. However, the size of the RSNE is relatively large, e.g., 22 to 40 bytes based on the examples given in 802.11mc/D1.5, while the size of all the other content items in FD frame is typically about 33 to 45 bytes. As the FD frame is designed to be transmitted between Beacon frames in order to facilitate a fast AP/Network discovery, the size of FD frame needs to be small, therefore, possible optimizations on the RSN information provisioning in FD frame should be explored.*

This contribution proposes a resolution to the above comment.

# Conventions

In this contribution, the proposed 802.11ai Specification Document text will be presented as modifications to the TGai draft specification 802.11ai/D1.1 [Ref-4]. The following format conventions are used:

1. The new added text is marked as blue underline text;
2. The deleted text is marked as ~~red strikethrough text~~;
3. The unchanged baseline standard text stays in black text in the context of proposed TGai specification text;
4. The editorial instruction is marked as *italic text highlighted by Yellow*;
5. Any other text, e.g., discussions, proposed motions, etc., is in black text, but not in the context of proposed TGai specification text.

# Discussions

Based on Table 8-221f in Section 8.5.8.35 in TGai Draft Specification, 802.11ai/D1.0 [Ref-3], the FILS Discovery frame contains an optional element, RSNE, to carry RSN information for FILS STAs that may not able to use FILS authentication schemes, e.g., no valid rRK for EAP-RP, instead, a full EAP is needed as described in Section 11.11.2.2.1 of 802.11ai/D1.0 [Ref-3].

The size of RSNE could be up to 257 octets, including the EID and Length fields. There are five samples of RSNE elements provided in Section 8.4.2.24 in 802.11mc/D1.5 [Ref-2], whose sizes are 22, 22, 20, 40, and 28 bytes, including the EID field and Length field, respectively.

Based on the FD frame format shown in Table 8-221f in Section 8.5.8.35 in TGai Draft Specification, 802.11ai/D1.0 [Ref-3], the typical sizes of all the content items other than RSNE are about 33 bytes to 45 bytes. Therefore, the RSNE’s size is relatively large in the FD frame.

This contribution proposes an optimized encoding to provide RSN information in FD frame, as shown in Figure 1 below.



1. **Proposed RSN Information Field in FD Frame**

Similarly, the proposed RSN information field is an optional field in FD frame, and its presence is indicated by an 1-bit presence indicator in the FD frame control field.

Note that the proposed RSN information field has a single Pairwise suite and a single AKM suite unlike the RSNE defined in 802.11mc/D1.5 [Ref-2] that allows a list of suites for each. This is based on the consideration that practically an AP will use one Pairwise Cipher Suite and one AKM Suite at any time, although it may support multiple. Therefore, it should be sufficient for AP to advertise what is actually in use in FD frames. In addition, all the sample RSNE elements given in 802.11mc/D1.5 [Ref-2] do not have multiple Pairewise Cipher Suites or multiple AKM Suites. The proposed RSN information field, similar to the RSNE defined in 802.11mc/D1.5 [Ref-2], has a single Group Data Cipher Suite and a single Group Management Cipher Suite selector.

In addition to limiting the number of Pairwise Cipher Suites and the number of AKM suites, the proposed RSN information field uses an optimized 4-bit code to identify each of the Group Data Cipher, Pairwise Cipher, AKM, and Group Management Suites, instead of a 4-octet code in the RSNE as defined in 802.11mc/D1.5 [Ref-2] .

The detailed text specifying the above proposed RSN information field in FD frame is provided in Section 4 of this contribution.

# Proposed 802.11ai Specification Text

The following proposed 802.11ai Specification Document text will be presented as modifications to the TGai draft specification 802.11ai/D1.1 [Ref-4].

*Instructions to Editor: in line 61 page 64, Section 8.5.8.35, in Table 8-221f, change the row of “RSNE” to the following:*

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 10 | RSN~~E~~ Information | ~~The RSNE, as specified in 8.4.2.27, is optionally present in FD frame generated by STAs that have dot11RSNAActivated equal to true.~~An optional field in the FD frame. Its presence is indicated by an 1-bit RSN Presence Indicator in the FD Frame Control. The format of the 4-octet FD RSN information field is shown in Figure <ANA-11ai-a> (Format of the FD RSN Information field). |

*Instructions to Editor: in line 30 page 65, Section 8.5.8.35, change Figure 8-502l* *to the following:*



**Figure 8-502l—FD Frame Control field format**

*Instructions to Editor: in line 47 page 65, Section 8.5.8.35, insert the following text:*

The RSN Information presence indicator is 1 bit in length. If it is set to 1, it indicates the RSN information field is present in the FD frame; otherwise, it indicates the RSN information field is not present in the FD frame.

*Instructions to Editor: in line 27 page 68, Section 8.5.8.35, insert the following text:*

The FD RSN Information field contains the RSN information, including: RSN capability, an authentication suite selector, a pairwise cipher suite selector, a group data cipher suite selector, and a group management cipher suite selector. Its length is 4 bytes. Its format is defined in Figure <ANA-11ai-a>.



**Figure <ANA-11ai-a> Format of the FD RSN Information Field**

The FD RSN information field contains a 2-octet RSN Capability subfield, as specified in Figure 8-217 in Section 8.4.2.24.4.

The FD RSN information field also contains three 4-bit Cipher Suite Selectors, including, one 4-bit Group Data Cipher Suite selector, one 4-bit Group Management Cipher Suite selector, and one 4-bit Pairwise Cipher Suite Selector. Each 4-bit Cipher Suite selector is a 4-bit code identifying a Cipher Suite Type as specified in Table 8-111. The definition of the 4-bit Cipher Suite Selectors is shown in Table <ANA-ai-3>.

**Table ANA-ai-3 Cipher Suite Selector Definitions**

|  |  |
| --- | --- |
| **Cipher Suite Selector (4 bits)** | **Cipher Suite Type** |
| 0 to 8 | Cipher Suite Type 0 to 8, in Table 8-111 |
| 9 – 13 | Reserved |
| 14 | Vendor Specific |
| 15 | no cipher suite selected |

The RSN Information field contains one 4-bit AKM Suite Selector. A 4-bit Cipher Suite selector is a 4-bit code identifying a AKM Suite Type as specified in Table 8-113. The definition of the 4-bit AKM Suite Selectors is shown in Table <ANA-ai-4>.

**Table <ANA-ai-4> AKM Suite Selector Definitions**

|  |  |
| --- | --- |
| **AKM Suite Selector (4 bits)** | **AKM Suite Type** |
| 0 to 10 | AKM Suite Type 0 to 10, in Table 8-113. |
| 11 to 13 | Reserved |
| 14 | Vendor Specific |
| 15 | no AKM suite selected |

# References:

1. IEEE Std 802.11 – 2012
2. IEEE Std 802.11mc/D1.5
3. IEEE Std 802.11ai/D1.0
4. IEEE Std 802.11ai/D1.1