IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed 802.11ai Specification Text for the Security Field in FILS Discovery Frame | | | | |
| Date:2013-01-05 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Lei Wang | InterDigital Communications | 781 Third Ave., King of Prussia, PA 19406 | 1 858 205 7286 | leiw@billeigean.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes the 802.11ai specification text for the security field in FILS Discovery Frame, based on the accepted features and functionalities in the 802.11ai Specification Framework Document (SFD), i.e., Section 6.3.1, in 12/0151r14[Ref-1], and also based on the relevant text in the TGai draft specification 802.11ai/D0.2 [Ref-3] .

# Introduction

To facilitate a fast initial link setup, high-level descriptions about passive scanning enhancement related features/functionalities have been accepted in 802.11ai Specification Framework Document (SFD), 12/0151r14 .

In previous TGai meetings, some text for the passive scanning enhancement related features / functionalities has been accepted to the 802.11ai draft specification document, 802.11ai/D0.2 [Ref-3], including the FILS Discovery (FD) frame contents with the security field. However, the definition of the security field in FD frame is missing.

To complete the FD frame definition, this contribution proposes detailed text for TGai Specification Document, to define the Security field in FD frame.

# Conventions

In this contribution, the proposed 802.11ai Specification Document text will be presented as modifications to the TGai draft specification 802.11ai/D0.2 [Ref-3]. 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. The quoted TGai SFD text is marked as *green italic text*; and
6. Any other text, e.g., discussions, proposed motions, etc., is in black text, but not in the context of proposed TGai specification text.

# Background

Based on Table 8-221g in Section 8.5.8.34 in TGai Draft Specification, 802.11ai/D0.2 [Ref-3], the FILS Discovery frame contains an optional field, FD Security, to carry security related information for a fast initial link setup.

There were multiple contributions submitted to TGai in previous meetings, among which the contribution, 12/1238r1 [Ref-4], was the most recent proposal that included all the updates from the previous discussions. In 12/1238r1 [Ref-4], the following was proposed for the FD Security field:

* 1. Design a fixed-size new Security field in FD frame, e.g., 4 bytes;
  2. Use the RSNE as defined in Section 8.4.2.27 in 802.11-2012 as starting point; and consider changes to make it smaller in size, e.g.,
     + Re-design the RSN Capabilities subfield to reflect its practical uses and 11ai specific considerations;
     + Limit the numbers of Pairwise suites and AKM suites, e.g., 2 for each
     + Introduce 4-bit codes to identify Cipher Suites and AKM Suites
     + Remove PMKID count and PMLID list
  3. Add some new info items, e.g.,
     + Security capability indicators for FILS authentication methods support, e.g.,
       - FILS Fast-EAP based authentication
       - FILS EAP-RP based authentication
       - FILS Non-EAP Fast authentication
       - FILS Fast Authentication without 3rd-party
  4. Use a 1-bit indicator in the FD frame control field to indicate the presence of the Security info item in the FD frame.
  5. In addition, a detailed FD Security field encoding is proposed as shown in the figure below.



1. **Proposed FD Security Field**

In this contribution, further detailed text is provided to specify the FD Security field, based on the above proposal presented in contribution, 12/1238r1 [Ref-4].

# 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/D0.2 [Ref-3].

*Instructions to Editor: append the following text at the end of Section 8.5.8.34, i.e., line 65 on page 35 in the TGai draft specification 802.11ai/D0.2 :*

The FD Security field contains the security information related to the data communications with the BSS of the AP STA transmitting the FD frame. Its length is 4 bytes. Its format is defined in Figure 8—460q.



**Figure 8-460q Format of the FD Security Field**

The FD Security field contains four 4-bit Cipher Suite Selectors, including, one 4-bit Group Data Cipher Suite selector, one 4-bit Group Management Cipher Suite selector, and two 4-bit Pairwise Cipher Suite Selectors. Each 4-bit Cipher Suite selector is a 4-bit code identifying a Cipher Suite Type as specified in Table 8-99. The definition of the 4-bit Cipher Suite Selectors is shown in Table 8-ai-3.

**Table 8-ai-3 Cipher Suite Selector Definitions**

|  |  |
| --- | --- |
| **Cipher Suite Selector (4 bits)** | **Cipher Suite Type** |
| 0b0000 – 0b0111 | Cipher Suite Type 0 to 7, in Table 8-99 |
| 0b1000 – 1101 | Reserved |
| 0b1110 | Vendor Specific |
| 0b1111 | no cipher suite selected |

The FD Security field contains two 4-bit AKM Suite Selectors. Each 4-bit Cipher Suite selector is a 4-bit code identifying a AKM Suite Type as specified in Table 8-101. The definition of the 4-bit AKM Suite Selectors is shown in Table 8-ai-4.

**Table 8-ai-4 AKM Suite Selector Definitions**

|  |  |
| --- | --- |
| **AKM Suite Selector (4 bits)** | **AKM Suite Type** |
| 0b0000 – 0b1001 | Cipher Suite Type 0 to 9, in Table 8-101. |
| 0b1010 – 1101 | Reserved |
| 0b1110 | Vendor Specific |
| 0b1111 | no AKM suite selected |

The FD Security field contains eight 1-bit security capability subfields, from bit 24 to bit 31. The subfields, Pre-Authentication (bit 24), Management Frame Protection required (bit 25), and Management Frame Protection Capable (bit 30), have the same meaning and set to equivalent bits as in the RSN capabilities field as specified in Section 8.4.2.27.4.

The subfield FILS Fast EAP (bit 26) is set to 1 if the FILS Fast EAP is supported, otherwise, set to 0.

The subfield FILS EAP-RP (bit 27) is set to 1 if the FILS EAP-RP is supported, otherwise, set to 0.

The subfield FILS Non-EAP (bit 28) is set to 1 if the FILS Non-EAP is supported, otherwise, set to 0.

The subfield FILS Authentication Without Third Party (bit 29) is set to 1 if the FILS Authentication Without Third Party is supported, otherwise, set to 0.

The subfield FILS Perfect Forward Secrecy (bit 31) is set to 1 if the FILS FILS Perfect Forward Secrecy is supported, otherwise, set to 0.

# Straw-Polls and Motions

The following lists the draft straw-polls and motions that are intended to present to the TGai Group in next Face-to-Face meeting.

**Motion-1:** Include the text proposed in Section 4 of this contribution (13/0010), i.e., defining the Security field for the FD frame, into the TGai Draft Specification Document (D0.2).

Yes: \_\_\_\_\_\_\_\_\_\_\_\_; No: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; Abstain: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Move:

Second:

# References:

1. 11-12-0151-14-00ai-Proposed-Specification-Framework-Document.docx
2. IEEE Std 802.11 – 2012
3. IEEE Std 802.11ai/D0.2
4. 11-12-1238-01-00ai-FD-Frame-capability-security-neighbor-info