IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Clarifications for FILS Session Identifier | | | | |
| Date: 2013-09-10 | | | | |
| 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 clarifications for FILS session identifier, 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, the following comment is submitted:

***Comment****: line 32 on page 44, Section 8.4.2.182*

*Multiple questions about the session identifier:*

1. *in what domain is the session identifier unique? Per BSS/AP or per STA? Note that an AP may have multiple non-AP STAs in progress of doing FILS authentication; and a non-AP STA may initiate FILS authentication with multiple APs, based on the paragraph in line 1 page 97. But, there should be no reason for a non-AP STA to initiate multiple FILS authentication sessions with the same AP.*
2. *what's the purpose of using the session identifier? prevent errors from multiple interleaving FILS authentication sessions between the same STA and AP? How? for example, what will an AP do if it receives an Authentication request with the same session ID at an on-going authentication session for the same STA?*
3. *The FILS session IEs are used in authentication frames and association frames. What value of FILS session identifier does an AP use in the Authentication response and Association response? Does the STA use the same session identifier in Association request as the one used in authentication request?.*

This contribution proposes a resolution to the above comment.

# Conventions

In this contribution, the proposed 802.11ai Specification Document text will be presented as changes to the current TGai draft specification, 11ai/D1.0[Ref-2]. 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*; and
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 of the Proposed Resolution

Two possible resolutions are discussed here:

1. Add the necessary specifications to complete the description about how to use FILS Authentication Session Identifier to enforce one FILS authentication session at a time between an AP and an non-AP STA. In other words, multiple simultaneous FILS authentication sessions are not allowed between an AP and a STA.
2. simply remove the FILS Session IE, under the assumption that it won’t happen multiple simultaneous FILS authentications between an AP and a STA.

The rest of this contribution will focus on the option 1) above, considering it needs much more work than option 2). The proposed resolution for option 1) is summarized as follows:

1. FILS session identifier is unique in the domain of a pair of an AP and a non-AP STA;
2. An FILS session is defined as entire message exchange process for FILS authentication, i.e., from Authentication request to Association response (for Key confirmation). Therefore, one FILS session identifier is used in all the messages of the same session. It is chosen by the non-AP STA that initiates the FILS authentication procedure by sending Authentication request.
3. If AP receives an Authentication request frame from a non-AP STA with the different FILS session identifier from the identifier of the on-going FILS authentication session with the same non-AP STA, then the AP shall terminate the previous authentication session, and use the information provided in the newly received authentication frame to start a new FILS authentication process at AP.
4. If AP receives an Authentication request frame from a non-AP STA with the same FILS session identifier as the identifier of the on-going FILS authentication session with the same non-AP STA, then the AP shall ignore the newly received Authentication request frame.
5. If AP receives an Association request frame from a non-AP STA with the different FILS session identifier from the identifier of the on-going FILS authentication session with the same non-AP STA, the FILS authentication session shall be deemed a failure.
6. If STA receives an Authentication Response or an Association Response from the AP with a different FILS session identifier from the identifier of the most-recent in-progress FILS authentication session with the same AP, the FILS authentication session shall be deemed a failure.

The detailed changes needed for above proposed resolution are described in Section 4 of this contribution.

# Proposed Changes to 802.11ai/D1.0 Specification Text

*Instructions to Editor: replace the paragraph in line 32 page 44 with the following text.*

The FILS Session element is used for conveying the identifier that uniquely identifies an in-progress FILS authentication session between an AP and a non-AP STA. The format of the FILS Session element is shown in Figure 8-401da (FILS Session element format).

*Instructions to Editor: insert the following text in line 46 page 44.*

An FILS authentication session includes message exchanges for key establishment using Authentication frames and key confirmation using Association Request and Response frames. The FILS Authentication session identifier is chosen randomly by the non-AP STA when it constructs an FILS authentication frame with Authentication transaction sequence number equal to 1 (Authentication Request). The same session identifier shall be used in the FILS Session elements in Authentication Response (Authentication frame with Authentication transaction sequence number equal to 2), Association Request, and Association Response frames of the same FILS authentication session.

*Instructions to Editor: change the paragraph in line 36 page 100 as follows:*

The STA then constructs an Authentication frame with the Authentication algorithm number set to <ANA-1> and the Authentication transaction sequence number set to one (1). The FILS Session element shall be set to indicate the FILS session identifier chosen by the STA (see 8.4.2.182), the ~~The~~ STA's FILS Identity shall be indicated using the FILS Identity element (see 8.4.2.179), the random nonce shall be encoded in the FILS nonce field (see 8.4.1.55), the FILS authentication type shall be set to indicate the specific type of FILS authentication, and the EAP-Initiate/Re-auth packet shall be copied into the FILS authentication wrapped data field (see 8.4.2.188). If PFS is desired, the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42) and the ephemeral public key shall be encoded in the Element field (see 8.4.1.40) according to the element to octet-string conversion in 11.3.7.2.4.

*Instructions to Editor: insert the following text in line 48 page 100:*

The AP shall first check if there is an existing FILS authentication session with the requesting STA. If so, the AP shall take the following actions, otherwise the AP shall proceed the processing of the received Authentication request.

1. The AP shall ignore the received Authentication request, if it contains the same FILS session identifier in the FILS Session element as the existing FILS authentication session;
2. Otherwise, the AP shall terminate the existing FILS authentication session and start a new session based on the newly received Authentication request.

*Instructions to Editor: change the sentence in line 14 page 101 as follows:*

In this frame, the AP shall set the Authentication sequence number to (2), and include the FILS Session element with the same FILS session identifier as in the most-recent received Authentication request from the same non-AP STA.

*Instructions to Editor: change the paragraph in line 28 page 101 as follows:*

* 1. If the received Authentication frame does not include the Authentication algorithm number set to <ANA-1>, or if the received Authentication frame contains a different FILS session identifier in the FILS Session element from that sent by the STA in the Authentication request, or if the received Authentication frame does not include an EAP-Finish/Re-auth packet, then the STA shall abandon the FILS authentication

*Instructions to Editor: change the paragraph in line 10 page 102 as follows:*

The STA then constructs an 802.11 authentication frame with the Authentication algorithm number set to <ANA-1> and the Authentication transaction sequence number set to one (1). The FILS Session element shall be set to indicate the FILS session identifier chosen by the STA (see 8.4.2.182), the ~~The~~ STA's FILS Identity shall be indicated using the FILS Identity element (see 8.4.2.180), the random nonce shall be encoded in the FILS nonce field (see 8.4.1.55), the FILS authentication type shall be set to indicate FILS authentication without a trusted third party (2), the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42), and the STA's public key shall be encoded into the Element field (see 8.4.1.40) according to the element to octet-string conversion in 11.3.7.2.4.

*Instructions to Editor: insert the following text in line 22 page 102:*

The AP shall first check if there is an existing FILS authentication session with the requesting STA. If so, the AP shall take the following actions, otherwise the AP shall proceed the processing of the received Authentication request.

1. The AP shall ignore the received Authentication request, if it contains the same FILS session identifier in the FILS Session element as the existing FILS authentication session;
2. Otherwise, the AP shall terminate the existing FILS authentication session and start a new session based on the newly received Authentication request.

*Instructions to Editor: change the paragraph in line 36 page 102 as follows:*

The AP then shall choose a random nonce, and random, ephemeral private key, and then use the agreedupon group's scalar-op (see 11.3.4.1) with its private key to generate its ephemeral public key. The AP then constructs an 802.11 authentication frame with the Authentication algorithm number set to <ANA-1>, the Authentication transaction sequence number set to two (2), and the FILS authentication type to indicate FILS authentication without a trusted third party (2). The AP's identity shall be indicated using the FILS Identity element (see 8.4.2.179), its random nonce shall be encoded in) the FILS nonce field (see 8.4.1.55), the finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42), and the AP's public key shall be encoded in the Element field (see 8.4.1.40) according to the element to octet-string conversion in 11.3.7.2.4. The FILS Session element shall be included with the same FILS session identifier as in the most-recent received Authentication request from the same non-AP STA. The AP shall transmit the 802.11 authentication frame to the STA. The AP may choose to derive the Diffie-Hellman shared secret, ss, at this point or it may choose to delay those computations until Key Confirmation (see 11.11.2.4). If it chooses to derive ss at this point, the AP shall use the STA's ephemeral public key and its private key with the chosen group's scalar-op to derive ss, and the AP shall then perform Key Derivation (see 11.11.2.3).

*Instructions to Editor: change the paragraph in line 53 page 102 as follows:*

The STA processes the AP's 802.11 authentication frame. First, it checks if the received Authentication frame contains the same FILS session identifier in the FILS Session element from that sent by the STA in the Authentication request. If not, the STA shall terminate the authentication exchange. Then, it ensures that the finite cyclic group in the AP's response matches the group selected by the STA. If they differ, the STA shall terminate the authentication exchange. If they match, the STA shall verify the validity of the AP's public key.

*Instructions to Editor: insert the following paragraph in line 50 page 103:*

The STA shall include an FILS Session element in the Association Request frame and set the FILS session identifier to the same as the value used in the Authentication frame of the same FILS authentication session.

*Instructions to Editor: change the paragraph in line 55 page 104 as follows:*

If the output from 11.11.2.6 returns a failure, authentication shall be deemed a failure. If the output returns plaintext, the Key-Auth from the decrypted Association Response frame shall be checked. If it is incorrect, authentication shall be deemed a failure. If the FILS session identifier does not match the session identifier that the AP has for the STA, the authentication shall be deemed a failure. If authentication is deemed a failure, the KCK2, KEK2, KCK, KEK, and TK shall be irretrievably destroyed. If authentication is not deemed a failure, the AP shall check the Key-Auth field in the Key Confirmation element.

*Instructions to Editor: change the paragraph in line 10 page 105 as follows:*

If authentication is a failure, the KCK2, KEK2, KCK, KEK, and TK shall be irretrievably destroyed. Otherwise, the AP shall then construct an 802.11 associate response frame confirming the selected ciphersuite and the FILS AKM, and containing the FILS KDE Container, and its own Key-Auth. The FILS Session element shall be included in the Association Response frame with setting the FILS session identifier to the same value used in the Association Request frame of the same FILS authentication session.

*Instructions to Editor: change the paragraph in line 13 page 106 as follows:*

If the output from 11.11.2.6 returns failure, authentication shall be deemed a failure. If the output returns plaintext, the Key-Auth from the decrypted Authentication frame shall be checked. If it is incorrect, authentication shall be deemed a failure. If the FILS session identifier does not match the session identifier that the STA has with the AP, the authentication shall be deemed a failure. If authentication is deemed a failure, the KCK2, KEK2, KCK, KEK, and TK shall be irretrievably destroyed. If authentication is not deemed a failure, the AP shall check the Key-Auth field in the Key Confirmation element.

# References

1. IEEE Std 802.11mc/D1.5
2. IEEE Std 802.11ai/D1.0