IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed Resolution for Authentication Frame Format |
| Date: 2016-01-19 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | hmorioka@src-soft.com |

Abstract

This document describes proposed resolution for Authentication frame format.

Addressed CIDs are:

10031, 10032, 10081, 10118, 10087, 10072

Baseline document is 11-16/0120r1 applied to Draft P802.11ai D6.3 and REVmc D4.0.

## Comments

## CID10031 (8.3.3.11, P50L27)

Comment:

RSNE, MDE and FTE are located before fields in FILS Authentication frame. It conflicts with the sentence "The frame body consists of the fields followed by the elements defined for each management frame subtype." in clause 8.3.3.1.

Proposed Change:

In Table 8-35, move RSNE, MDE and FTE after FILS Nonce. Renumber the order field apropriately.

## CID10032 (8.3.3.11, P50L27)

Comment:

The Finite Cyclic Group field and the Element field are located before the FILS Authentication Type field. But the presence of the Finite Cyclic Group field and the Element field is depend on FILS Authentication type. So the FILS Authentication frame can not be parsed.

Proposed Change:

"Option 1:

Move FILS Authentication field before Finite Cyclic Group field in Table 8-35.

Option 2:

Remove ""FILS Authentication field"".

Details are following.

In clause 8.4.1.1,

Replace ""Authentication algorithm number = 4: FILS authentication"" with ""Authentication algorithm number = 4: FILS authentication using a shared key and without PFS"".

Add ""Authentication algorithm number = 5: FILS authentication using a shared key and with PFS"" and ""Authentication algorithm number = 6: FILS authentication using a public key and with PFS"".

Remove ""FILS Authentication Type"" from Table 8-35 and 8-36.

Change references to the FILS Authentication Type field to the Authentication Algorithm Number field.

Remove clause 8.4.1.57.

Replace ""The STA then constructs an Authentication frame with the Authentication algorithm number set to 4 (FILS authentication) (see 8.4.1.1 (Authentication Algorithm Number field)) and the Authentication transaction sequence number set to 1.""

with ""The STA then constructs an Authentication frame with the Authentication algorithm number set to 4 (FILS authentication using a shared key and without PFS) or 5 (FILS authentication using a shared key and with PFS) (see 8.4.1.1 (Authentication Algorithm Number field)) depending on whether PFS is used and the Authentication transaction sequence number set to 1.""

on P146L12 in clause 11.11.2.3.2.

Remove ""and the FILS Authentication Type field shall be set to one of the FILS shared key authentication as defined in Table 8-73a (Values of FILS Authentication Type field) depending on whether PFS is used."" on P146L16 in clause 11.11.2.3.2.

Replace ""The Authentication algorithm number is set to 4"" with ""The Authentication algorithm number is set to 6"" on P149L8 and P149L49 in clause 11.11.2.4.

Remove ""FILS Authentication Type field indicates FILS public key authentication (2)."" on P149L12 in clause 11.11.2.4.

Remove ""The FILS Authentication Type field is set to 2, indicating FILS public key authentication."" on P149L52 in clause 11.11.2.4.

Remove ""(see Table 8-73a (Values of FILS Authentication Type filed))"" on P10L40 in clause 4.10.36.1.

Remove ""8.4.1.57 (FILS Authentication Type field)"" on P162L18 in Annex B.4.27."

## CID10081 (8.3.3.11, P50L27)

Comment:

"The way Authentication frame information mixes information elements and fields that are not elements is quite inconvenient to parse. Even though the base standard may seem to have such design in Table 8-35 , that mix does not show up in practice due to the way FT and SAE designs do not include all the fields, However, the P802.11ai additions make this pretty messy for the FILS cases. FILS would first use elements like RSNE followed by some existing non-elements from SAE like Finite Cyclic Group which would then be followed by some additional new non-elements and finally new elements. While that would, at least in theory, be parseable, this makes it more difficult to use a generic information element parser design which works with most other management frames (i.e., non-elements first followed by information elements).

With FILS design, this is even worse due to the Finite Cyclic Group and Element field (non-elements) being optionally present and that optionally depending on the value of the FILS Authentication Type field which is after this optional fields. It does not look like the AP is going to be able to parse this frame unambiguously due to that design.

At minimum, the fields would need to be re-ordered in the FILS Authentication case so that FILS Authentication Type field is before the optional Finite Cyclic Group field. However, it would likely be more convenient if all these fields were converted to information elements for the FILS case so that there would be only one segment of non-element fields followed by information elements."

Proposed Change:

Add a new information element to convery the information of FILS Authentication Type, FILS Nonce, Finite Cyclic Group, and Element non-elements (with the last two being optionally present subfields of the element based on FILS Authentication Type value).

## Discussion

1. Fix the order of non-element fields and elements

On existing standard, “Finite Cyclic Group filed”, “Anti-Clogging Token filed”, “Send-Confirm field”, “Scalar field” and “Element field” those are non-element fields located **after** elements, are only used by SAE. FILS authentication is the first case to use both RSNE, MDE and the SAE fields.

Should this issue be resolved by REVmc? (If so, we cannot progress until the issue is resolved.)

1. Authentication Type and the fields depend on Authentication Type

Authentication type information have to locate before the fields depend on it to parse the frame.

Why do we need Authentication type field separately from the Authentication Algorithm Number field?

1. New fields or new element

At first, we should re-use the existing fields and elements. So we should use “Finite Cyclic Group field” and “Element field” as existing. But these fields’ presences depend on FILS Authentication Type. So FILS Authentication Type information has to locate before “Finite Cyclic Group field”. This means FILS Authentication information have to be a **field** if we need a separate field.

The FILS Nonce can be an element.

## Resolution Policy

1. Re-order SAE fields before elements.
2. Remove FILS Authentication Type field.
3. Add Authentication algorithm numbers to the Authentication Algorithm number field.
4. Replace FILS Nonce field with FILS Nonce element.

## Resolution text

# ~~Red text with strike-out:~~ Remove from the TGai draft.

Blue text with underline: Add to the TGai draft. The text in the draft will be “Blue text with underline”.

Green text with underline: Add to the TGai draft with underline. The text in the draft will be “Green text with underline”. This is an additional modification to the baseline.

~~Green text with strike-out:~~ Add to the TGai draft with strike-out. The text in the draft will be “~~Green text with strike-out~~”. This is an additional modification to the baseline.

~~Green text with strike-out and yellow background:~~ Add strike-out to the existing text in the TGai draft. The text in the draft will be “~~Green text with strike-out and yellow background~~”.

***Red Italic bold text with underline and yellow background:*** Instruction to the editor.

**[White number(s) with bracket and black background]:** Resolution item(s) as following:

1. Re-order SAE fields before elements.
2. Remove FILS Authentication Type field.
3. Add Authentication algorithm numbers to the Authentication Algorithm number field.
4. Replace FILS Nonce field with FILS Nonce element.
5. Remove PMKID List element. [CID10118]
6. Parameter clean-up in clause 6.3.5. [CID10072]
7. Add indication for FILS shared key authentication with PFS. [CID0087, 10183]

## 4.10.3.6.1 General

# *Remove the reference “(see Table 8-73a (Values of FILS Authentication Type field))” at the end of the 2nd paragraph.*

Three FILS authentication methods are defined: (1) FILS shared key authentication performed without perfect forward security (PFS), (2) FILS shared key authentication performed with PFS, and (3) FILS public

key authentication with PFS ~~(see Table 8-73a (Values of FILS Authentication Type field))~~. **[2]**

## 6.3.5.2 MLME-AUTHENTICATE.request

### 6.3.5.2.2 Semantics of the service primitive

# *Modify as following:* [3, 5, 6]

MLME-AUTHENTICATE.request(

PeerSTAAddress,

AuthenticationType,

AuthenticateFailureTimeout,

Content of FT Authentication elements,

Content of SAE Authentication frame,

Multi-band local,

Multi-band peer,

~~FILSWrappedData,~~

~~PMKIDList,~~

Content of FILS Authentication frame,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| ~~FILSWrappedData~~ | ~~As defined in 8.4.2.183 (FILS Wrapped Data element)~~ | ~~As defined in 8.4.2.183 (FILS Wrapped Data element)~~ | ~~Data used by the FILS authentication algorithm. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.~~ |
| ~~PMDIDList~~ | ~~As defined in 8.4.2.185 (PMKID List element)~~ | ~~As defined in 8.4.2.185 (PMKID List element)~~ | ~~Data used by the FILS authentication algorithm. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.~~ |
| AuthenticationType | Enumeration | OPEN\_SYSTEM, SHARED\_KEY, FAST\_BSS\_TRANSITION, SAE, FILS\_SHARED\_KEY\_WITHOUT\_PFS, FILS\_SHARED\_KEY\_WITH\_PFS, FILS\_PUBLIC\_KEY | Specifies the type of authentication algorithm to use during the authentication process. |
| Content of FILS Authentication frame | Sequence of elements and fields | As defined in 8.4.1.42 (Finite Cyclic Group field), 8.4.1.40 (Element field), 8.4.2.24 (RSNE), 8.4.2.175 (FILS Session element), 8.4.2.183 (FILS Wrapped Data element), and 8.4.2.xxx (FILS Nonce element) | The set of elements and fields to be included in the first message of the FILS authentication sequence, as described in 11.11 (Authentication for FILS). Present if AuthenticationType indicates FILS shared key authentication without PFS, FILS shared key authentication with PFS or FILS public key authentication; otherwise not present. |

## 6.3.5.3 MLME-AUTHENTICATE.confirm

### 6.3.5.3.2 Semantics of the service primitive

# *Modify as following:* [3, 5, 6]

MLME-AUTHENTICATE.confirm(

PeerSTAAddress,

AuthenticationType,

ResultCode,

Content of FT Authentication elements,

Content of SAE Authentication frame,

Multi-band local,

Multi-band peer,

~~FILSWrappedData,~~

~~PMKIDList,~~

~~AssociationDelayInfo,~~

Content of FILS Authentication frame,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| ~~FILSWrappedData~~ | ~~As defined in 8.4.2.183 (FILS Wrapped Data element)~~ | ~~As defined in 8.4.2.183 (FILS Wrapped Data element)~~ | ~~Data used by the FILS authentication algorithm. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.~~ |
| ~~PMDIDList~~ | ~~As defined in 8.4.2.185 (PMKID List element)~~ | ~~As defined in 8.4.2.185 (PMKID List element)~~ | ~~Data used by the FILS authentication algorithm. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.~~ |
| ~~AssociationDelayInfo~~ | ~~Integer~~ | ~~As defined in 8.4.2.171 (Association Delay Info element)~~ | ~~Minimum association response timeout (in TU) that the non-AP STA sets to the value given by dot11AssociationRespon- seTimeOut.~~ |
| AuthenticationType | Enumeration | OPEN\_SYSTEM, SHARED\_KEY, FAST\_BSS\_TRANSITION, SAE, FILS\_SHARED\_KEY\_WITHOUT\_PFS, FILS\_SHARED\_KEY\_WITH\_PFS, FILS\_PUBLIC\_KEY | Specifies the type of authentication algorithm to use during the authentication process. |
| Content of FILS Authentication frame | Sequence of elements and fields | As defined in 8.4.1.42 (Finite Cyclic Group field), 8.4.1.40 (Element field), 8.4.2.24 (RSNE), 8.4.2.171 (Association Delay Info element), 8.4.2.175 (FILS Session element), 8.4.2.183 (FILS Wrapped Data element), and 8.4.2.xxx (FILS Nonce element) | The set of elements and fields to be included in the second message of the FILS authentication sequence, as described in 11.11 (Authentication for FILS). Present if AuthenticationType indicates FILS shared key authentication without PFS, FILS shared key authentication with PFS or FILS public key authentication; otherwise not present. |

## 6.3.5.4 MLME-AUTHENTICATE.indication

### 6.3.5.4.2 Semantics of the service primitive

# *Modify as following:* [3, 5, 6]

MLME-AUTHENTICATE.indication(

PeerSTAAddress,

AuthenticationType,

AuthenticateFailureTimeout,

Content of FT Authentication elements,

Content of SAE Authentication frame,

Multi-band local,

Multi-band peer,

~~FILSWrappedData,~~

~~PMKIDList,~~

Content of FILS Authentication frame,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| ~~FILSWrappedData~~ | ~~As defined in 8.4.2.183 (FILS Wrapped Data element)~~ | ~~As defined in 8.4.2.183 (FILS Wrapped Data element)~~ | ~~Data used by the FILS authentication algorithm. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.~~ |
| ~~PMDIDList~~ | ~~As defined in 8.4.2.185 (PMKID List element)~~ | ~~As defined in 8.4.2.185 (PMKID List element)~~ | ~~Data used by the FILS authentication algorithm. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.~~ |
| AuthenticationType | Enumeration | OPEN\_SYSTEM, SHARED\_KEY, FAST\_BSS\_TRANSITION, SAE, FILS\_SHARED\_KEY\_WITHOUT\_PFS, FILS\_SHARED\_KEY\_WITH\_PFS, FILS\_PUBLIC\_KEY | Specifies the type of authentication algorithm to use during the authentication process. |
| Content of FILS Authentication frame | Sequence of elements and fields | As defined in 8.4.1.42 (Finite Cyclic Group field), 8.4.1.40 (Element field), 8.4.2.24 (RSNE), 8.4.2.175 (FILS Session element), 8.4.2.183 (FILS Wrapped Data element), and 8.4.2.xxx (FILS Nonce element) | The set of elements and fields to be included in the first message of the FILS authentication sequence, as described in 11.11 (Authentication for FILS). Present if AuthenticationType indicates FILS shared key authentication without PFS, FILS shared key authentication with PFS or FILS public key authentication; otherwise not present. |

## 6.3.5.5 MLME-AUTHENTICATE.response

### 6.3.5.5.2 Semantics of the service primitive

# *Modify as following:* [3, 5, 6]

MLME-AUTHENTICATE.response(

PeerSTAAddress,

AuthenticationType,

ResultCode,

Content of FT Authentication elements,

Content of SAE Authentication frame,

Multi-band local,

Multi-band peer,

~~FILSWrappedData,~~

~~PMKIDList,~~

~~AssociationDelayInfo,~~

Content of FILS Authentication frame,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| ~~FILSWrappedData~~ | ~~As defined in 8.4.2.183 (FILS Wrapped Data element)~~ | ~~As defined in 8.4.2.183 (FILS Wrapped Data element)~~ | ~~Data used by the FILS authentication algorithm. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.~~ |
| ~~PMDIDList~~ | ~~As defined in 8.4.2.185 (PMKID List element)~~ | ~~As defined in 8.4.2.185 (PMKID List element)~~ | ~~Data used by the FILS authentication algorithm. This parameter is optionally present if dot11FILSActivated is true; otherwise not present.~~ |
| ~~AssociationDelayInfo~~ | ~~Integer~~ | ~~As defined in 8.4.2.171 (Association Delay Info element)~~ | ~~Minimum association response timeout (in TU) that the non-AP STA sets to the value given by dot11AssociationRespon- seTimeOut.~~ |
| AuthenticationType | Enumeration | OPEN\_SYSTEM, SHARED\_KEY, FAST\_BSS\_TRANSITION, SAE, FILS\_SHARED\_KEY\_WITHOUT\_PFS, FILS\_SHARED\_KEY\_WITH\_PFS, FILS\_PUBLIC\_KEY | Specifies the type of authentication algorithm to use during the authentication process. |
| Content of FILS Authentication frame | Sequence of elements and fields | As defined in 8.4.1.42 (Finite Cyclic Group field), 8.4.1.40 (Element field), 8.4.2.24 (RSNE), 8.4.2.171 (Association Delay Info element), 8.4.2.175 (FILS Session element), 8.4.2.183 (FILS Wrapped Data element), and 8.4.2.xxx (FILS Nonce element) | The set of elements and fields to be included in the second message of the FILS authentication sequence, as described in 11.11 (Authentication for FILS). Present if AuthenticationType indicates FILS shared key authentication without PFS, FILS shared key authentication with PFS or FILS public key authentication; otherwise not present. |

## 8.3.3.11 Authentication frame format

# *Modify Table 8-35 as following (baseline: REVmc D5.0):* [1, 2, 4, 5]

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 4 | Finite Cyclic Group | An unsigned integer indicating a finite cyclic group as described in 11.3.4 (Finite cyclic groups). This is present in SAE Authentication frames and FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| 5 | Anti-Clogging Token | A random bit-string used for anti-clogging purposes as described in 11.3.6 (Anti-clogging tokens). This is present in SAE Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| 6 | Send-Confirm | A binary encoding of an integer used for anti-replay purposes as described in 11.3.7.5 (Encoding and decoding of SAE Confirm messages). This is present in SAE Authentication frames as defined in  Table 8-36 (Presence of fields and elements in Authentication frames). |
| 7 | Scalar | An unsigned integer encoded as described in 11.3.7.4 (Encoding and decoding of SAE Commit messages). This is present in SAE (#99)Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| 8 | Element | A field element from a finite field encoded as described in 11.3.7.4 (Encoding and decoding of SAE Commit messages). This is present in SAE Authentication frames and FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| 9 | Confirm | An unsigned integer encoded as described in 11.3.7.5 (Encoding and decoding of SAE Confirm messages). This is present in SAE Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~4~~10 | Challenge text | The challenge text element is present only in certain Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~5~~11 | RSN | The RSNE is present in the FT Authentication frames and FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~6~~12 | Mobility Domain | The MDE is present in the FT Authentication frames and FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~7~~13 | Fast BSS Transition | An FTE is present in the FT Authentication frames and FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames).~~.~~ |
| ~~8~~14 | Timeout Interval (reassociation deadline) | A TIE containing the reassociation deadline interval is present in the FT Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~9~~15 | RIC | A resource information container, containing a variable number of elements, is present in the FT Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~10~~ | ~~Finite Cyclic Group~~ | ~~An unsigned integer indicating a finite cyclic group as described in 11.3.4 (Finite cyclic groups). This is present in SAE Authentication and FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). .~~~~An unsigned integer indicating a finite cyclic group as described in 11.3.4 (Finite cyclic groups). This is present in SAE Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames).~~ |
| ~~11~~ | ~~Anti-Clogging Token~~ | ~~A random bit-string used for anti-clogging purposes as described in 11.3.6 (Anti-clogging tokens). This is present in SAE Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames).~~ |
| ~~12~~ | ~~Send-Confirm~~ | ~~A binary encoding of an integer used for anti-replay purposes as described in 11.3.7.5 (Encoding and decoding of SAE Confirm messages). This is present in SAE Authentication frames as defined in  Table 8-36 (Presence of fields and elements in Authentication frames).~~ |
| ~~13~~ | ~~Scalar~~ | ~~An unsigned integer encoded as described in 11.3.7.4 (Encoding and decoding of SAE Commit messages). This is present in SAE Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames).~~ |
| ~~14~~ | ~~Element~~ | ~~A field element from a finite field encoded as described in 12.4.7.4 (Encoding and decoding of SAE Commit messages). This is present in SAE Authentication frames as defined in Table 9-36 (Presence of fields and elements in Authentication frames).~~~~A field element from a finite field encoded as described in 11.3.7.4 (Encoding and decoding of SAE Commit messages). This is present in SAE Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames).~~ |
| ~~15~~ | ~~Confirm~~ | ~~An unsigned integer encoded as described in 11.3.7.5 (Encoding and decoding of SAE Confirm messages). This is present in SAE Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames).~~ |
| ~~18~~ | ~~FILS Authentication Type~~ | ~~The FILS Authentication Type field is present in FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames).~~ |
| ~~19~~18 | FILS Nonce | The FILS Nonce ~~field~~ element is present in FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~20~~ | ~~PMKID List~~ | ~~The PMKID List element is present in FILS Authentication frames as defined in Table 9-36 (Presence of fields and elements in Authentication frames).~~ |
| ~~21~~19 | FILS Session ~~element~~ | The FILS Session ~~field~~ element is present in FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~22~~20 | FILS Wrapped Data | The FILS Wrapped Data element is present in FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |
| ~~23~~21 | Association Delay Info | The Association Delay Info element is present in FILS Authentication frames as defined in Table 8-36 (Presence of fields and elements in Authentication frames). |

# *Modify Table 8-36 as following:* [2, 3, 4, 5]

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication algorithm** | **Authentication transaction sequence no.** | **Status code** | **Presence of fields 4-2~~3~~1** |
| FILS shared key authentication without PFS | 1 | Reserved | ~~The FILS Session element is present.~~~~The FILS Authentication Type field is present.~~ ~~The FILS Nonce field is present.~~~~The RSNE is present.~~~~The FILS Wrapped Data element is present if FILS shared key authentication is used.~~~~The Finite Cyclic Group field is present if Status is 0 and the FILS Authentication Type field indicates PFS or if FILS pub- lic key authentication is used.~~~~The Element field is present if Status is 0 and the FILS Authentication Type field indicates PFS or if FILS public key authentication is used.~~~~The PMKID List element is present if the STA is asserting cached PMKs.~~~~The MDE is present if the FILS authentication is used for FT initial mobility domain association.~~The RSNE is present.The Mobility Domain element is present if the FILS authentication is used for FT initial mobility domain association.The FILS Nonce element is present.The FILS Session element is present.The FILS Wrapped Data element is present. |
| FILS shared key authentication without PFS | 2 | Status | ~~The FILS Session element is present.~~ ~~The RSNE is present.~~~~The FILS Authentication Type is present if Status Code field is 0.~~~~The FILS Nonce is present if Status Code field is 0.~~~~The FILS Wrapped Data element is present if Status Code field is 0 and FILS shared key authentication is used.~~~~The Finite Cyclic Group is present if Status is 0 and the FILS Authentication Type field indicates PFS or if FILS public key authentication is used.~~~~The Element field is present if Status is 0 and the FILS Authentication Type field indicates PFS or if FILS public key authentication is used.~~~~The PMKID List element is present if the AP agrees to per- form PMKSA caching.~~~~The Association Delay Info element is present if Status is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame.~~~~The MDE and FTE are present if Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.~~The RSNE is present.The Mobility Domain element and the Fast BSS Transition element are present if Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The FILS Nonce element is present if Status Code field is 0.The FILS Session element is present if Status Code field is 0.The FILS Wrapped Data element is present if Status Code field is 0.The Association Delay Info element is present if Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |
| FILS shared key authentication with PFS | 1 | Reserved | The Finite Cyclic Group field is present.The Element field is present.The RSNE is present.The Mobility Domain element is present if the FILS authentication is used for FT initial mobility domain association.The FILS Nonce element is present.The FILS Session element is present.The FILS Wrapped Data element is present. |
| FILS shared key authentication with PFS | 2 | Status | The Finite Cyclic Group is present if Status is 0.The Element field is present if Status is 0.The RSNE is present.The Mobility Domain element and the Fast BSS Transition element are present if Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The FILS Nonce element is present if Status Code field is 0.The FILS Session element is present if Status Code field is 0.The FILS Wrapped Data element is present if Status Code field is 0.The Association Delay Info element is present if Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |
| FILS public key authentication | 1 | Reserved | The Finite Cyclic Group field is present.The Element field is present.The RSNE is present.The Mobility Domain element is present if the FILS authentication is used for FT initial mobility domain association.The FILS Nonce element is present.The FILS Session element is present. |
| FILS public key authentication | 2 | Status | The Finite Cyclic Group is present if Status is 0.The Element field is present if Status is 0.The RSNE is present.The Mobility Domain element and the Fast BSS Transition element are present if Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The FILS Nonce element is present if Status Code field is 0.The FILS Session element is present if Status Code field is 0.The Association Delay Info element is present if Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |

## 8.4.1.1 Authentication Algorithm Number field

# *Add Authentication algorithm number definitions as following:* [3]

 Authentication algorithm number = 0: Open System

 Authentication algorithm number = 1: Shared Key

 Authentication algorithm number = 2: Fast BSS Transition

 Authentication algorithm number = 3: Simultaneous Authentication of Equals (SAE)

 Authentication algorithm number = 4: FILS shared key authentication without PFS

 Authentication algorithm number = <ANA1>: FILS shared key authentication with PFS

 Authentication algorithm number = <ANA2>: FILS public key authentication

 Authentication algorithm number = 65535: vendor specific use

# *Remove subclause 8.4.1.57 (FILS Authentication Type field) and 8.4.1.58 (FILS Nonce field):* [2, 4]

## 8.4.2.1 General

# *Remove “PMKID List” row from the Table 8-74.* [5]

# *Add the following row at the end of Table 8-74:* [4]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| FILS Nonce (see 8.4.2.xxx (FILS Nonce element)) | 255 | <ANA> |  | No |

# *Modify subclause 8.4.2.178 (FILS Indication element) as following (based on D6.3 + 11-16/120r1):* [7]

## 8.4.2.178 FILS Indication element

The FILS Information field provides information on the presence of the following optional fields in the FILS Indication element and the capability of the FILS shared key authentication with PFS. The format of the FILS Information field is shown in Figure 8-577l (FILS Information field definition).

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 | B2 | B3 | B5 | B6 | B7 | B8 | B9 | B10 | B~~9~~ 11 | B15 |
|  | Number of Public Key Identifiers | Number of Realm Identifiers | FILS IP Address Configuration | Cache Identifier Included | HESSID Included | FILS Shared Key Authentication without PFS Supported | FILS Shared Key Authentication with PFS Supported | Reserved |
| Bits: | 3 | 3 | 1 | 1 | 1 | 1 | 1 | ~~7~~5 |

**Figure 8-577l—FILS Information field definition**

# *Add the following text before Figure 8-577m (D6.3 P65L52, after HESSID description):* [7]

An AP sets the FILS Shared Key Authentication without PFS Supported bit to 1 if the AP supports FILS shred key authentication without PFS and is set to 0 otherwise. An AP sets the FILS Shared Key Authentication with PFS Supported bit to 1 if the AP supports FILS shared key authentication with PFS and is set to 0 otherwise.

# *Remove subclause 8.4.2.185 (PMKID List element).* [5]

# *Add the following subclause after 8.4.2.184:* [4]

## 8.4.2.xxx FILS Nonce element

The FILS Nonce element is used for exchanging an additional source of randomness in the FILS authentication exchange. The format of the FILS Nonce element is shown in Figure 9-xxx (FILS Nonce element format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | FILS Nonce |
| Octets: | 1 | 1 | 1 | 16 |

**Figure 8-xxx – FILS Nonce element format**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The FILS Nonce field contains randomly generated data.

## 11.11.2.2 Discovery of a FILS capable AP

# *Modify the 1st sentence of the 3rd paragraph as following (D6.3 P140L50):* [7]

An AP indicates support for FILS shared key authentication without PFS by setting the FILS Shared Key Authentication without PFS Supported bit to 1 in the FILS Information field of the FILS Indication element. An AP indicates support for FILS shared key authentication with PFS by setting the FILS Shared Key Authentication with PFS Supported bit to 1 in the FILS Information field of the FILS Indication element. An AP may ~~advertising~~ advertise between zero and seven realms using ~~a Domain Information~~ the Realm Identifier subfield(s) of the FILS Indication element that is part of Beacon, Probe Response, and FILS Discovery frames.

## 11.11.2.3.2 Non-AP STA construction of Authentication frame

# *Modify the 3rd paragraph as following (D6.3 P142L27):* [2, 3, 4, 5]

The STA then constructs an Authentication frame with the Authentication algorithm number set to 4 (FILS shared key authentication without PFS) or <ANA1> (FILS shared key authentication with PFS) (see 8.4.1.1 (Authentication Algorithm Number field)) depending on whether PFS is used, and the Authentication transaction sequence number set to 1. The random nonce shall be encoded in the FILS Nonce ~~field (see 8.4.1.58 (FILS Nonce field))~~ element (see 8.4.2.xxx (FILS Nonce element))~~, and the FILS Authentication Type field shall be set to one of the FILS shared key authentication as defined in Table 8-73a (Values of FILS Authentication Type field) depending on whether PFS is used~~. If a list of PMKSA identifiers was generated, it shall be used to construct the PMKID List ~~elements~~ field in RSNE. The EAP-Initiate/Re-auth packet, if generated, shall be copied into the FILS Wrapped Data field (see 8.4.2.183 (FILS Wrapped Data element)). If PFS is desired, the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)) and the ephemeral public key shall be encoded in the Element field (see 8.4.1.40 (Element field)) according to the element to octet-string conversion in 11.3.7.2.4 (Element to octet string conversion).

## 11.11.2.3.3 AP processing of Authentication frame

# *Modify the first sentence as following (D6.3 P142L49):* [3]

Upon reception of the Authentication frame with the Authentication algorithm number equal to 4 or <ANA1>, the AP shall do the following procedure:

# *Modify the list item b) as following (D6.3 P142L54):* [3]

b) If the indicated finite cyclic group in the received FILS Authentication frame is not supported, the AP shall respond with an Authentication frame with the Authentication algorithm number set to ~~4~~ <ANA1> (FILS shared key authentication with PFS) (see 8.4.1.1 (Authentication Algorithm Number field)) and the Status Code field set to 77 (Authentication is rejected because the offered finite cyclic group is not supported) and shall terminate the exchange.

# *Modify the list item c) as following (D6.3 P142L61):* [3, 5]

c) The AP shall check whether PMKSA caching is being attempted by the presence of the PMKID List ~~element~~ field in RSNE.

1) If the PMKID List ~~element~~ field is present in RSNE, the AP checks whether any PMKSA identifier offered in the PMKID List matches an identifier for a cached PMKSA. If so, the AP selects a PMKID that matches and continues the FILS shared key authentication protocol using the PMK from the identified PMKSA.

2) If a PMKID List ~~element~~ field is not present in RSNE or if no PMKSA identifier offered in the PMKID list matches any identifier for a cached PMKSA, the AP checks whether an EAP-Initiate/Re-auth packet was included. If not, the AP shall respond with an Authentication frame with the Authentication algorithm number set to ~~1~~4 or <ANA1> depending on whether PFS is used, and the Status Code field set to 53 (invalid PMKID) and shall terminate the exchange.

# *Modify the 2nd paragraph as following (D6.3 P143L19)):* [3]

If PFS is being used, the AP shall also generate an ephemeral private key and perform the group’s scalar-op (see 11.3.4.1 (General)) to produce its own ephemeral public key. The AP may delay the generation of its ephemeral public/private key pair until after receiving a response from the Authentication Server, if applicable. The Authentication Server processes the EAP-Initiate/Re-auth packet as specified in IETF RFC 6696 and returns an EAP-Finish/Re-auth packet to the AP. In the case of successful authentication by the Authentication Server, the Authentication Server returns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet. If the Authentication Server responds with a failure indication, then the AP shall produce an Authentication frame with the Authentication Algorithm Number field set to ~~“Fast Initial Link Setup authentication” 1~~4 (FILS shared key authentication without PFS) or <ANA1> (FILS shared key authentication with PFS) (see 8.4.1.1 (Authentication Algorithm Number field)) depending on whether PFS is used, and the Status Code field set to 15 (Authentication rejected because of challenge failure). In the case of successful authentication by the Authentication Server, the Authentication Server returns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet and processing terminates.

## 11.11.2.3.4 AP construction of Authentication frame

# *Modify the 2nd paragraph as following (D6.3 P143L51)):* [3]

Otherwise, the AP shall generate its own nonce and construct an Authentication frame for the STA. This frame shall contain the FILS wrapped data that encapsulates EAP-Finish/Re-auth packet received from the Authentication Server. In addition, if PFS is used, the Element field of the Authentication frame sent by the AP contains the AP’s ephemeral public key. In this frame, the AP shall set the Authentication algorithm number to 4 or <ANA1> depending on whether PFS is used, and the Authentication sequence number to 2.

## 11.11.2.3.5 Non-AP STA processing of Authentication frame

# *Modify the list item a) as following (D6.3 P144L11)):* [3]

1. If the received Authentication frame does not include the Authentication Algorithm Number equal to 4 (FILS shared key authentication without PFS) or <ANA1> (FILS shared key authentication with PFS) (see 8.4.1.1 (Authentication Algorithm Number field)), or if PMKSA caching was attempted and the received Authentication frame includes a PMKID that does not match a PMKID in the Authentication frame sent by the STA; or if the received Authentication frame doesn’t include either a PMKID or an EAP-Finish/Re-auth packet, the STA shall abandon FILS authentication.

## 11.11.2.4 Key establishment with FILS public key authentication

# *Modify the list item 3) as following (D6.3 P145L16):* [2, 3, 4]

3) Constructs an Authentication frame (see 8.3.3.11 (Authentication frame format)) as follows:

1. The Authentication algorithm number is set to ~~4~~<ANA2> (FILS public key authentication) (see 8.4.1.1 (Authentication Algorithm Number field)) and the Authentication transaction sequence number is set to 1.
2. The random nonce is encoded in the FILS Nonce ~~field~~ element (see ~~8.4.1.58~~ 8.4.2.xxx (FILS Nonce ~~field~~ element)).
3. ~~FILS Authentication Type field indicates FILS public key authentication (2).~~

~~d)~~c) The chosen finite cyclic group is encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)).

~~e)~~d) The STA’s public key is encoded into the Element field (see 8.4.1.40 (Element field)) according to the element to octet-string conversion in 11.3.7.2.4 (Element to octet string conversion).

# *Modify the list item 2) (P149L47) as following (D6.3 P145L59):* [2, 3, 4]

2) Constructs an Authentication frame (see 8.3.3.11 (Authentication frame format)) as follows:

1. The Authentication algorithm number is set to ~~4~~<ANA2> (FILS public key authentication) (see 8.4.1.1 (Authentication Algorithm Number field)) and the Authentication transaction sequence number is set to 2.
2. ~~The FILS Authentication Type field is set to 2, indicating FILS public key authentication.~~

~~c)~~b) The random nonce is encoded in the FILS Nonce ~~field~~ element (see ~~8.4.1.58~~ 8.4.2.xxx (FILS Nonce ~~field~~ element)).

~~d)~~c) The finite cyclic group is encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)).

~~e)~~d) The AP’s public key is encoded in the Element field (see 8.4.1.40 (Element field)) according to the element to octet-string conversion in 11.3.7.2.4 (Element to octet string conversion).

## B.4.27 FILS features

# *Modify the row for “FILS4” as following:* [2, 4]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Protocol Capability** | **References** | **Status** | **Support** |
| FILS4 | FILS authentication | 11.11 (Authentication for FILS)~~8.4.1.57 (FILS Authentication Type field)~~8.4 (Management and Extension frame body components)~~8.4.1.58 (FILS Nonce field)~~8.4.2.174 (FILS Key Confirmation element) 8.4.2.175 (FILS Session element)8.4.2.178 (FILS Indication element)8.4.2.xxx (FILS Nonce element) | (CF1 OR CF2.1) AND CF32: M | Yes No N/A  |

## C.3 MIB Detail

# *Add the following modification to the C.3 (MIB Details) at P164L6:* [3]

*-- Editor Note: Modify the dot11AuthenticationAlgorithm as following:*

dot11AuthenticationAlgorithm OBJECT-TYPE

 SYNTAX INTEGER {

 openSystem(1),

 sharedKey(2),

 fastBSSTransition(3),

 simultaneousAuthEquals(4) ~~}~~,

 FILSSharedKeyWithoutPFS(<ANA>),

 FILSSharedKeyWithPFS(<ANA>),

 FILSPublicKey(<ANA>)}

 MAX-ACCESS read-only

 STATUS current

 DESCRIPTION

 "This is a control variable.

 It is written by an external management entity.

 Changes take effect as soon as practical in the implementation.

 This attribute is the authentication algorithm described by this entry in the table. The following values can be used here

 Value = 1: Open system

 Value = 2: Shared key

 Value = 3: Fast BSS transition (FT)

 Value = 4: Simultaneous authentication of equals (SAE)

 Value = <ANA>: FILS shared key authentication without PFS

 Value = <ANA>: FILS shared key authentication with PFS

 Value = <ANA>: FILS public key authentication

 A given value shall not be used more than once"

 ::= { dot11AuthenticationAlgorithmsEntry 2 }