IEEE P802.11
Wireless LANs

|  |
| --- |
| Certificate-Based Authentication Protocol for IEEE 802.11 TGai |
| Date: 2012-11-05 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | Toronto ON | +1 415 690-7363+1 647 867-5658Skype: rstruik | rstruik.ext@gmail.com |

Abstract

This document presents suggested text to define how to implement FILS authentication using a certificate-based authenticated key agreement scheme. Suggested text is relative to 802.11-2012.

NOTE:

The scheme proposed complies with adopted motions within 802.11ai to-date.

ACKNOWLEDGEMENT:

Thanks to Dan Harkins for gracefully suggesting me to reuse his original 11/1488r0 submission, on which the initial version of this document (12/0052r0) was based.

REVISION NOTES:

* R04 provides textual changes resulting from the Palm Springs meeting and consultation of TGai stakeholders. Document pretty well aligns with 12/1172r0, but introduces some changes to make sure it satisfies feedback received from TGai community to best of ability and allows easy integration/unification with other proposals currently on the table.
* R03 adds note as to compliance with TGai motions so far (no update to 802.11-2011 yet [still pending – will end up with R04, once I have Word version hereof]).
* R02 cleans up some change markers, so as to improve readability (no other changes)
* R01 adds a note (NOTE-2) to Section 11.9a.2.2, so as to tackle the scenario where STA and AP do have certificates, but at least one of these cannot verify the other’s certificate (this is public-key authentication scheme (d) in 11/1408r05). NOTE: The scenario where they can verify each other’s certificate is public-key authentication scheme (a) in 11/1408r05.

IMPORTANT NOTE:

This document contains some specification text related to non-certificate based key agreement schemes. These remnants of 12/1172r0 were left in, so as to facilitate unification with other submissions (notably the sequel of 1045rx series.

***Insert the following reference into 2:***

FIPS PUB 186-3 Digital Signature Algorithm (DSS)

IETF RFC 3279 – Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

IETF RFC 5295, Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK), August 2008

IETF RFC 6696, EAP Extensions for EAP Re-authentication Protocol (ERP), July 2012

IETF RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

RFC 5480 **-** ECC Subject Public Key Information, March 2009

RFC 6090 **-** Fundamental Elliptic Curve Cryptography Algorithms, February 2011

FIPS Pub 180-3

NIST SP 800-38A

NIST SP 800-56A

NIST SP 800-56C

NIST SP 800-108

NIST SP 800-57A

NIST SP 800-133A

***Insert the following definition into 3.1:***

**3.1 Definitions**

**EAP Reauthentication Protocol (EAP-RP):** A protocol, using the EAP framework, allowing single-round-trip reauthentication with an Authentication Server following an initial EAP authentication.

**Trusted Third Party (TTP):** a non-STA entity that maintains a security association with both a non-AP STA and an AP.

**Perfect Forward Secrecy (PFS)**: a security property such that loss of secrecy of a long-lived secret does not compromise the security of past sessions.

**Certificate Authority (CA)**: entity that vouches for the binding between a device’s identity, its public key, and associated keying material (such as key validity period, key usage, etc.).

***Modify section 4.5.4.2 as indicated:***

* Authentication

IEEE 802.11 authentication operates at the link level between IEEE 802.11 STAs. IEEE Std 802.11 does not provide either end-to-end (message origin to message destination) or user-to-user authentication.

IEEE Std 802.11 attempts to control LAN access via the authentication service. IEEE 802.11 authentication is an SS. This service may be used by all STAs to establish their identity to STAs with which they communicate, in both ESS and IBSS networks. If a mutually acceptable level of authentication has not been established between two STAs, an association is not(#1421) established.

IEEE Std 802.11 defines five802.11(#12858) authentication methods: Open System authentication, Shared Key authentication, FT authentication(11r), simultaneous authentication of equals (SAE), and FILS authentication.(11s) Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. FT authentication relies on keys derived during the initial mobility domain association to authenticate the (#1112)stations as defined in Clause 12 (Fast BSS transition).(11r) SAE authentication uses finite field cryptography to prove knowledge of a shared password.(11s) Three FILS methods are defined in this version of the specification: (1) the FILS authentication exchange using a TTP is performed without PFS, (2) the FILS authentication exchange using a TTP is performed with PFS, (3) The FILS authentication exchange without a TTP and with PFS (Refer to table 8.4.2.42b). When a trusted third party is used for FILS authentication, then EAP-RP as defined in [IETF RFC 5295/6696] shall be used. When a trusted third party is used for FILS authentication A STA that discovers a FILS-capable AP that claims a trusted relationship with a mutually-trusted third party it may begin the FILS Authentication protocol to the AP and perform mutual authentication using the trusted third party only if the STA and trusted third party already share a valid rRK, as defined in [IETF RFC 6696] (see section 11.9a.2.1); otherwise the STA may perform full EAP authentication via IEEE 802.1X authentication. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

An RSNA might support SAE authentication and/or FILS authentication.(11s) An RSNA also supports authentication based on IEEE Std 802.1X-2004, or preshared keys (PSKs) after Open System authentication(11s). IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another. This standard does not specify an EAP method that is mandatory to implement. See 11.5.5 (RSNA policy selection in an IBSS and for DLS) for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS.

In an RSNA, IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port.

Either SAE authentication, FILS authentication or(11s) the Open System 802.11 authentication algorithm is used in RSNs based on infrastructure BSS and IBSS, although Open System 802.11 authentication is optional in an RSN based on an IBSS. SAE authentication is used in an MBSS.(11s) RSNA disallows the use of Shared Key 802.11 authentication.(#12858)

***Modify section 4.5.4.3 as indicated:***(11s)

* Deauthentication

The deauthentication service is invoked when an existing Open System, Shared Key, SAE(11s) or FILS authentication is to be terminated. Deauthentication is an SS.

When the deauthentication service is terminating SAE authentication any PTKSA, GTKSA, mesh TKSA, or mesh GTKSA related to this SAE authentication is destroyed. If PMK caching is not enabled, deauthentication also destroys any PMKSA created as a result of this successful SAE authentication.(11s)

In an ESS, because authentication is a prerequisite for association, the act of deauthentication causes(#1421) the STA to be disassociated. The deauthentication service may be invoked by either authenticated party (non-AP STA or AP). Deauthentication is not a request; it is a notification. The association at the transmitting STA is terminated when the STA sends a deauthentication notice to an associated STA. Deauthentication, and if associated, disassociation can not be refused by the receiving STA except when management frame protection(#12241) is negotiated and the message integrity check fails.(11w)

In an RSN ESS, Open System 802.11(#12858) authentication is required. In an RSN ESS, deauthentication results in termination of any association for the deauthenticated STA. It also results in the IEEE 802.1X Controlled Port for that STA being disabled and deletes the pairwise transient key security association (PTKSA). The deauthentication notification is provided to IEEE Std 802.1X-2004 via the MAC layer.

In an RSNA, deauthentication also destroys any related pairwise transient key security association(PTKSA)(11w), group temporal key security association (GTKSA), station-to-station link (STSL) master key security association (SMKSA), STSL transient key security association (STKSA), and integrity group temporal key security association (IGTKSA)(11w) that exist in the STA and, if applicable, closes the associated IEEE 802.1X Controlled Port. If pairwise master key (PMK) caching is not enabled, deauthentication also destroys the pairwise master key security association (PMKSA) from which the deleted PTKSA was derived.

In an RSN IBSS, Open System authentication is optional, but a STA is required to recognize Deauthentication frames. Deauthentication results in the IEEE 802.1X Controlled Port for that STA being disabled and deletes the PTKSA.

***Create section 4.10.3.4a***

**4.10.3.4a AKM operations using FILS authentication and a trusted third party**

It is assumed that the authenticator has a secure channel with the trusted third party in a manner outside the scope of this standard.

The following operations (see Figure <ANA-0>) are carried out when FILS authentication is used with a trusted third party:

1. The STA discovers the AP’s policy through passive monitoring of Beacon frames or through active probing. If a FILS-capable STA discovers that the AP supports FILS authentication and the identity of the trusted third party is known (and trusted) by the STA, the STA and AP proceed to FILS authentication
2. The STA initiates FILS authentication by sending an Authentication frame with the FILS information to the AP. The AP forwards the FILS Authentication information to the trusted 3rd party. Upon receiving a response from the trusted 3rd party, the AP responds to the STA with an Authentication frame with FILS information. The STA and AP generate a PMK as a result of this exchange. Exchange of messages (method, procedure, format and content) between AP/Authenticator and the trusted 3rd party is out of scope of this specification.
3. The STA sends an Association Request frame to the AP and receives a Association Response frame from the AP. This exchange provides proof-of-possession of the PMK and enables the creation of a PTKSA and further establishment of FILS state

IEEE 802.11 Probe Request ReRequest

STA/Supplicant

AP/Authenticator

Trusted 3rd Party

IEEE 802.11 Probe Response ReRequest

IEEE 802.11 Authentication

 FILS Authentication Request

 FILS Authentication Response

IEEE 802.11 Authentication

IEEE 802.11 Association Request

IEEE 802.11 Association Response

 **Figure <ANA-0>—FILS Authentication**

***Create section 4.10.3.4b***

**4.10.3.4b AKM operations using FILS authentication without an online trusted third party**

It is assumed that both STAs using FILS have obtained a public key certificate from a Certificate Authority and that each STA is capable of verifying this certificate during execution of the FILS authentication scheme. The manner by which these certificates are obtained is outside the scope of this standard.

The following operations are carried out when FILS authentication is used with a trusted third party:

1. The STA discovers the AP’s policy through passive monitoring of Beacon frames or through active probing. If a FILS-capable STA discovers that the AP supports FILS authentication and the identity of the trusted third party is known (and trusted) by the STA, the STA and AP proceed to FILS authentication
2. The STA initiates FILS authentication by sending a Authentication frame to the AP, after which the AP responds with a Authentication frame. The STA and AP generate a PMK as a result of this exchange.
3. The STA sends an Association Request frame to the AP and receives a Association Response frame from the AP. This exchange provides proof-of-possession of the PMK and enables the creation of a PTKSA and further establishment of FILS state.

***Modify section 6.3.5.2 as indicated:***

(11s)

**6.3.5.2 MLME-AUTHENTICATE.request**

**6.3.5.2.1 Function**

This primitive requests authentication with a specified peer MAC entity.

**6.3.5.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-AUTHENTICATE.request(

PeerSTAAddress,

AuthenticationType,

AuthenticateFailureTimeout,

Content of FT Authentication elements,

Content of SAE Authentication Frame,

FILS wrapped data,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Type**  | **Valid range**  | **Description** |
| PeerSTAAddress | MACAddress | Any valid individual MAC address | Specifies the address of the peer MAC entity with which to perform the authentication process. |
| AuthenticationType | Enumeration | OPEN\_SYSTEM,SHARED\_KEY,FAST\_BSS\_TRANSITION,SAE,FILS | Specifies the type of authentication algorithm to use during the authentication process. |
| AuthenticationFailureTimeout | Integer | 1 | Specifies a time limit (in TU) after which the authentication procedure is terminated. |
| Content of FT Authentication elements | Sequence of elements | As defined in 12.8 | The set of elements to be included in the first message of the FT authentication sequence, as described in 12.8.2. Present only if dot11FastBSSTransitionActivated is true. |
| Content of SAE Authentication Frame | Sequence of elements and fields | As defined in 8.4.1.37, 8.4.1.38, 8.4.1.39, 8.4.1.40b, 8.4.1.41, and 8.4.1.42 | The set of elements and fields to be included in the SAE Commit Message or SAE Confirm Message. Present only if AuthenticationType indicates SAE authentication. |
| FILS wrapped data | Sequence of elements and fields | As defined in 8.4.1.42a | The FILS wrapped data field is used for the STA and AP to communicate data used by the FILS authentication algorithm |
| VendorSpecificInfo | A set of elements | As defined in 8.4.2.28 | Zero or more elements. |

**6.3.5.3.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-AUTHENTICATE.confirm(

PeerSTAAddress,

AuthenticationType,

ResultCode,

Content of FT Authentication elements,

Content of SAE Authentication Frame,

FILS wrapped data,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Type**  | **Valid range**  | **Description** |
| PeerSTAAddress | MACAddress | Any valid individual MAC address | Specifies the address of the peer MAC entity with which to perform the authentication process. |
| AuthenticationType | Enumeration | OPEN\_SYSTEM,SHARED\_KEY,FAST\_BSS\_TRANSITION,SAE,FILS | Specifies the type of authentication algorithm to use during the authentication process. |
| ResultCode | Enumeration | SUCCESS, REFUSED,ANTI-CLOGGINGTOKEN REQUIRED,FINITE CYCLIC GROUPNOT SUPPORTED,AUTHENTICATIONREJECTED | Indicates the result of the MLMEAUTHENTICATE.request primitive. |
| Content of FT Authentication elements | Sequence of elements | As defined in 12.8 (FTauthentication sequence) | The set of elements included in the second message of the FT authentication sequence, as described in 12.8.3 (FT authentication sequence: contents of second message). Present only if dot11FastBSSTransitionActivated is true. |
| Content of SAE Authentication Frame | Sequence of elements and fields | As defined in 8.4.1.37(Send-Confirm field),8.4.1.38 (Anti-CloggingToken field), 8.4.1.39 (Scalarfield), 8.4.1.40 (Elementfield), 8.4.1.41 (Confirmfield), and 8.4.1.42 (FiniteCyclic Group field) | The set of elements and fields to be included in the SAE Commit Message or SAE Confirm Message. Present only if AuthenticationType indicates SAE authentication. |
| FILS wrapped data | Sequence of elements and fields | As defined in 8.4.1.42a | The FILS wrapped data field is used for the STA and AP to communicate data used by the FILS authentication algorithm |
| VendorSpecificInfo | A set of elements | As defined in 8.4.2.28 | Zero or more elements. |

**6.3.5.4.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-AUTHENTICATE.indication(

PeerSTAAddress,

AuthenticationType,

Content of FT Authentication elements,

Content of SAE Authentication Frame,

FILS wrapped data,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Type**  | **Valid range**  | **Description** |
| PeerSTAAddress | MACAddress | Any valid individual MAC address | Specifies the address of the peer MAC entity with which the authentication relationship was established. |
| AuthenticationType | Enumeration | OPEN\_SYSTEM,SHARED\_KEY,FAST\_BSS\_TRANSITION,SAE,FILS | Specifies the type of authentication algorithm that was used during the authentication process. |
| Content of FT Authentication elements | Sequence of elements | As defined in 12.8 | The set of elements to be included in the first message of the FT authentication sequence, as described in 12.8.2. Present only if dot11FastBSSTransitionActivated is true. |
| Content of SAE Authentication Frame | Sequence of elements and fields | As defined in 8.4.1.37, 8.4.1.38, 8.4.1.39, 8.4.1.40, 8.4.1.41, and 8.4.1.42 | The set of elements to be included in the SAE Commit Message or SAE Confirm Message. Present only if AuthenticationType indicates SAE authentication. |
| FILS wrapped data | Sequence of elements and fields | As defined in 8.4.1.42a | The FILS wrapped data field is used for the STA and AP to communicate data used by the FILS authentication algorithm |
| VendorSpecificInfo | A set of elements | As defined in 8.4.2.28 | Zero or more elements. |

**6.3.5.5.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-AUTHENTICATE.response(

PeerSTAAddress,

ResultCode,

Content of FT Authentication elements,

Content of SAE Authentication Frame,

FILS wrapped data,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Type**  | **Valid range**  | **Description** |
| PeerSTAAddress | MACAddress | Any valid individual MAC address | Specifies the address of the peer MAC entity from which the authentication request was received. |
| ResultCode | Enumeration | SUCCESS,REFUSED, ANTICLOGGINGTOKENREQUIRED,FINITE CYCLICGROUP NOT SUPPORTED,AUTHENTICATIONREJECTED | Indicates the result response to the authentication request from the peer MAC entity. |
| Content of FT Authentication elements | Sequence of elements | As defined in 12.8 | The set of elements to be included in the first message of the FT authentication sequence, as described in 12.8.2. Present only if dot11FastBSSTransitionActivated is true. |
| Content of SAE Authentication Frame | Sequence of elements and fields | As defined in 8.4.1.37, 8.4.1.38, 8.4.1.39, 8.4.1.40, 8.4.1.41, and 8.4.1.42 | The set of elements to be included in the SAE Commit Message or SAE Confirm Message. Present only if AuthenticationType indicates SAE authentication. |
| FILS wrapped data | Sequence of elements and fields | As defined in 8.4.1.42a | The FILS wrapped data field is used for the STA and AP to communicate data used by the FILS authentication algorithm |
| VendorSpecificInfo | A set of elements | As defined in 8.4.2.28 | Zero or more elements. |

***Modify table 8-22 in section 8.3.3.5 by inserting a new orders 8-10, incrementing the orders of subsequent rows:***

|  |
| --- |
| Table 8-22—Association Request frame body |
| Order | Information | Notes |
| 8 | FILS session | The FS IE is an identifier for the FILS session  |
| 9 | FILS signature | An octet string indicating a signature used during key confirmation and device authentication of FILS authentication.  |
| 10 | FILS Key Confirmation | A field that performs a cryptographic proof of authentication for the FILS Authentication protocol. Present if FILS authentication is used. |
| Last | Vendor Specific | One or more vendor-specific (#1684)elements are optionally present(#29). These (#1684)elements follow all other (#1684)elements(#1221). |

***Modify table 8-23 in section 8.3.3.6 by inserting a new order 6-9, and incrementing the orders of subsequent rows:***

|  |
| --- |
| Table 8-23—Association Response frame body |
| Order | Information | Notes |
| 6 | FILS session | The FS IE is an identifier for the FILS session  |
| 7 | FILS signature | An octet string indicating a signature used during key confirmation and device authentication of FILS authentication.  |
| 8 | FILS Key Confirmation | A field that performs a cryptographic proof of authentication for the FILS Authentication protocol |
| 9 | FILS KDE Container | A field that contains the KDE information. |
| Last | Vendor Specific | One or more vendor-specific (#1684)elements are optionally present(#29). These (#1684)elements follow all other (#1684)elements(#1221). |

***Modify section 8.3.3.11 as indicated:***

* Authentication frame format

The  frame  body of a management frame of subtype Authentication contains the information shown in **Error! Reference source not found.**. (#29)FT authentication is used when FT support is advertised by the AP and dot11FastBSSTransitionActivated(#1005) is(#1217) true(#1535) in the (#1112)STA.(11r) SAE authentication is used when dot11MeshActiveAuthenticationProtocol is sae (1).(11s)      FILS authentication is used when support for FILS authentication is advertised by the AP and dot11FILSAuthenticationActivated is true in the STA.

|  |
| --- |
| Table 8-28-- Authentication frame body |
| Order | Information | Notes |
| 16 | FILS session | The FS IE is an identifier for the FILS session  |
| 17(11s) | FILS identity | The FI IE identity of a STA performing FILS authentication |
| 18 | FILS authentication type | The FA field is an indicator of the type of FILS authentication a particular session will perform |
| <ANA-6b> | FILS ephemeral key | The FN IE is an ephemeral public key used by the FILS authentication protocol. |
| <ANA-7a> | FILS session | The FS IE is an identifier for the FILS session  |
| <ANA-7b> | FILS certificate  | The device certificate used by the FILS authentication protocol. |
| 19 | FILS nonce | The FN IE is a random, or pseudo-random, octet string used by the FILS authentication protocol. |
| 20 | FILS wrapped data | An encrypted and authenticated series of fields used for FILS authentication. |
| Last | Vendor Specific | One or more vendor-specific (#1684)elements are optionally present(#29). These (#1684)elements follow all other (#1684)elements(#1221). |

|  |
| --- |
| Table 8-29-- Presence of fields and(11s) elements in Authentication frames(11r)  |
| Authentication algorithm | Authentication transaction sequence no. | Status code | Presence of fields 4-15 (11r)(11s) |
| FILS(11s) | 1 | Status | FILS identity is presentFILS authentication type is present.FILS nonce is present. FILS ephemeral public key is presentFILS certificate is presentFILS wrapped data is present if FILS authentication uses a TTP. Finite cyclic group is present if FA type field indicates PFS.Element is present if FA type field indicates PFS. |
| FILS(11s) | 2 | Status | FILS identity is present if Status is zero.FILS authentication type is present if Status is zero.FILS nonce is present if Status is zero. FILS ephemeral public key is present if Status is zero.FILS certificate is present if Status is zero.FILS wrapped data is present if Status is zero and a TTP is used. Finite cyclic group is present if FA type field indicates PFS.Element is present if FA type field indicates PFS. |

***Modify section 8.4.1.1 as indicated:***

* Authentication Algorithm Number field

The Authentication Algorithm Number field indicates a single authentication algorithm. The length of the Authentication Algorithm Number field is 2 octets. The Authentication Algorithm Number field is illustrated in **Error! Reference source not found.**. The following values are defined for authentication algorithm number:

Authentication algorithm number = 0: Open System

Authentication algorithm number = 1: Shared Key

Authentication algorithm number = 2: Fast BSS Transition(11r)

Authentication algorithm number = 3: simultaneous authentication of equals (SAE)

Authentication algorithm number = <ANA-1>: Fast Initial Link Setup authentication (11s)

Authentication algorithm number = 65 535: Vendor specific use

NOTE—The use of this value implies that a Vendor Specific element(Ed) is included with more information.(#10081)

All other values of authentication algorithm number are reserved.

***Create section 8.4.1.40b, 8.4.1.40c, 8.4.1.42a, 8.4.1.42b, and 8.4.1.42c***

**8.4.1.40b FILS public key field**

The FILS public key field is used with FILS authentication to communicate a representation of an ephemeral public key as specified in 11.3. See Figure <ANA-2b> FILS element field. The format shall be compliant with NIST specifications and conventions in PKIX formats specified in RFC 5480.

|  |  |
| --- | --- |
|  | Element |
| Octets: | Variable |
| * Figure <ANA-2b> FILS public key field (11s)
 |

**8.4.1.40c FILS certificate field**

The FILS certificate field is used by the STA and AP to communicate their respective public-key certificate used by the FILS authentication algorithm. See figure <ANA-2c> FILS certificate.

|  |  |
| --- | --- |
|  | FILS certificate |
| Octets: | variable |
| * Figure <ANA-2c> FILS- (11s)certificate
 |

**8.4.1.42a FILS wrapped data field**

The FILS wrapped data field is used for the STA and AP to communicate data used by the FILS authentication algorithm. See figure <ANA-2> FILS wrapped data.

|  |  |
| --- | --- |
|  | FILS wrapped data |
| Octets: | variable |
| * Figure <ANA-2> FILS-wrapped data(11s)
 |

**8.4.2.42b FILS authentication type field**

The FILS authentication type field is used for indicating the type of FILS authentication exchange, either with PFS or without PFS. The format of the FILS authentication field is shown in Figure <ANA-3>.

|  |  |
| --- | --- |
|  | FILS authentication type |
| Octets: | 1 |

**Figure <ANA-3>-- FILS authentication type format**

The value of the FILS authentication type is taken from table <ANA-4>.

|  |  |
| --- | --- |
|  Value |  Description |
|  0 | The FILS authentication exchange using a TTP is performed without PFS. |
|  1 | The FILS authentication exchange using a TTP is performed with PFS. |
|  2 | The FILS authentication exchange without a TTP and with PFS. |
|  3-255 | Reserved. |

|  |
| --- |
| **Table <ANA-4>-- Values of FILS authentication type(#1248)** |

**8.4.2.42c FILS nonce field**

The FILS nonce field is used for exchanging an additional source of randomness to the FILS authentication exchange. The nonce data shall be 16 octets and shall be chosen in a random manner. The format of the FILS nonce field is shown in Figure <ANA-5> FILS nonce field.

|  |  |
| --- | --- |
|  | FILS nonce |
| Octets: | 16 |

**Figure <ANA-5>-- FILS nonce field format**

***Create sections 8.4.2.121a, 8.4.2.121b, 8.4.2.121c, 8.2.4.121e, 8.2.4.121f , 8.2.4.121g as indicated:***

**8.4.2.121a FILS Identity element**

The FILS identity element is used for conveying an identity to use with the FILS authentication protocol (see 11.9a). The FILS identity element is included in Beacon and Probe Response frames by APs that support FILS authentication and is included in Authentication frames sent by STAs to initiate the FILS authentication protocol. The format of the FILS identity element is shown in Figure <ANA-6> FILS identity element.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | ID type | FILS identity |
| Octets: | 1 | 1 | 1 | variable |
|  | **Figure <ANA-6>-- FILS identity element format(#1248)** |

The ID type subfield is set as follows:

* 0: Reserved
* 1: Trusted Third Party identity
* 2: STA identity

When using a trusted third party for authentication, the semantics of the FILS identity depend on the ID type as well as the namespace used by the Trusted Third Party to identify itself and entities with which it has a trusted relationship; they are therefore out of scope of this specification. When authenticating without a trusted third party, the ID type subfield shall be 2 (STA identity) for both the STA and AP, and the contents of the FILS identity field shall be an X.500 distinguished name (DN) that identifies either a certified or an uncertified public key.

*Editorial note RS – it is to be advised that the name space of device taken to be MAC address, so as to facilitate cert issuance at device manufacturing.*

**8.4.2.121b FILS Key Confirmation element**

The FILS Key Confirmation element is used to convey a cryptographic proof of authentication between a STA and an AP. The format of the FILS Key Confirmation element is shown in Figure <ANA-7> FILS Key Confirmation.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Element ID | Length | FILS Auth |
| Octets: | 1 | 1 | variable |
|  | **Figure <ANA-7>-- FILS Key Confirmation element format(#1248)** |

The FILS Auth field contains the cryptographic proof-of-possession information (see 11.9a.2.4b).

**8.4.2.121c FILS KDE container element**

The FILS KDE container element is used to communicate one or more KDEs in a FILS authentication exchange. The FILS KDE container may contain one or more KDEs. The format of the FILS KDE container element is shown in Figure <ANA-8> FILS KDE container element.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | One or more entries |
|  | Element ID | Length | KDE(s) |
| Octets: | 1 | 1 | Variable |
| **Figure <ANA-8>-- FILS KDE container element format (#1248)** |

The Length field of the FILS KDE container specifies the total number of octets of all the KDEs. The encoding of the KDE field is defined in Table 11-6 (KDE) of 11.6.2 (EAPOL-Key frames) of this specification.

**8.4.2.121e FILS session element**

The FILS session element is used for conveying the (unique) identifier of an in-progress FILS authentication protocol. The session identifier is chosen randomly by the non-AP STA in the FILS authentication protocol. The format of the FILS session element is shown in Figure <ANA-10> FILS session element.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Element ID | Length | FILS session |
| Octets: | 1 | 1 | 8 |
| **Figure <ANA-10>-- FILS session element format(#1248)** |

**8.4.2.121f FILS public key element**

The FILS public key element is used to communicate the device’s (certified) public-key for use with the FILS authentication exchange. The format of the FILS certificate element is shown in Figure <ANA-11> FILS certificate element.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length |  Key Type |  FILS public key |
| Octets: | 1 | 1 | 1 | variable |
|  | **Figure <ANA-11>-- FILS public key element format(#1248)** |

Where the Key Type subfield is as follows:

* 0: Reserved
* 1: An X.509v3 certificate encoded according to RFC 5280.
* 2: A manual certificate encoded according to RFC 5280, but without signature field.
* 3: A raw public key encoded according to RFC 5480
* 4: A raw public key encoded according to RFC 3279
* 5: Vendor specific

*Editorial note: “manual certificate” format shall be the same as PKIX format, except for absence of signature over “to-be-signed data” fields.*

**8.4.2.121g FILS signature element**

The FILS signature element is used to authenticate the device’s ephemeral public key via a signature produced using the device’s static public key. The signature data shall have variable length and shall be compliant with the FIPS Pub 186-2 format.The format of the FILS signature element is shown in Figure <ANA-5b> FILS signature element.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Element ID | Length |  FILS signature |
| Octets: | 1 | 1 | variable |
| **Figure <ANA-5b>-- FILS signature element format(#1248)** |

***Modify section 8.4.2.27.3 as indicated:***

* AKM suites

The AKM Suite Count field indicates the number of AKM suite selectors that are contained in the AKM Suite List field.

The AKM Suite List field contains a series of AKM suite selectors contained in the RSN (#1684)element. In an IBSS(#13085) only a single AKM suite selector may be specified because STAs in an IBSS (#10287)use the same AKM suite and because there is no mechanism to negotiate the AKMP in an IBSS (see 11.5.5).

Each AKM suite selector specifies an AKMP. gives the AKM suite selectors defined by this -standard. An AKM suite selector has the format shown in **Error! Reference source not found.**.(#11242)

|  |
| --- |
| * Table 8-101-- AKM suite selectors
 |
| OUI | Suite type | Meaning |
| Authentication type | Key management type | Key derivation type (11w) |
| 00-0F-AC | <ANA-12> | FILS | FILS key management as defined in 11.9a  | Defined in 11.9.a |
| 00-0F-AC | <ANA-12 > +1 –255  | Reserved | Reserved | Reserved |
| Vendor OUI | Any | Vendor-specific | Vendor-specific | Vendor-specific |
| Other | Any | Reserved | Reserved | Reserved |

***Modify section 10.3.2.2 as indicated:***

* + - 1. Authentication—originating STA

Upon receipt of an MLME-AUTHENTICATE.request primitive, the originating STA(#3097) shall authenticate with the indicated STA using the following procedure:(11r)

* If the STA is in an IBSS the SME shall delete any PTKSA and temporal keys held for communication with the indicated(#11069) STA by using the MLME-DELETEKEYS.request primitive (see 11.5.12 (RSNA security association termination)).(#10600)
* (#1342)The STA(#10600) shall execute one of the following:(11r)
* For the Open System or Shared Key authentication algorithm, the authentication mechanism described in 11.2.3.2 (Open System authentication) or 11.2.3.3 (Shared Key authentication), respectively.(11r)
* For the FT authentication algorithm in an ESS, the authentication mechanism described in 12.5 (FT Protocol), or, if resource requests are included, 12.6 (FT Resource Request Protocol).(#10600)(11r)
* For SAE authentication in an ESS, IBSS, or MBSS, the authentication mechanism described in 11.3 (Authentication using a password).(11s)

4) For FILS authentication in an ESS, the authentication mechanism described in 11.9a (FILS Authentication).

* If the authentication was successful within the AuthenticateFailureTimeout(#1342), the state(#1342) for the indicated STA shall be set to State 2 if it was State 1; the state shall remain unchanged if it(Ed) was other than State 1.(#10600)
* The MLME(#1342) shall issue an MLME-AUTHENTICATE.confirm primitive to inform the SME of the result of the authentication.

***Modify section 10.3.2.3 as indicated:***

* Authentication—destination STA

Upon receipt of an Authentication frame with authentication transaction sequence number equal to 1, the destination STA(#3097) shall authenticate with the originating(#1342) STA using the following procedure:

1. If FILS authentication is being used in an ESS, the MLME shall issue an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request, including the FILS authentication element, and the SME shall execute the procedure described in 11.9a (Authentication for fast link setup)

***Modify section 11.5.1.1.1 and 11.5.1.1.2 as indicated:***

* Security association definitions
* General(#2119)

IEEE Std 802.11 uses the notion of a security association to describe secure operation. Secure communications are possible only within the context of a security association, as this is the context providing the state—cryptographic keys, counters, sequence spaces, etc.—needed for correct operation of the IEEE 802.11 cipher suites.

A security association is a set of policy(ies) and key(s) used to protect information. The information in the security association is stored by each party of the security association, needs to(#10380) be consistent among all parties, and needs to(#10380) have an identity. The identity is a compact name of the key and other bits of security association information to fit into a table index or an MPDU. The following types of security associations are supported by an RSN STA(11w):

* PMKSA: A result of a successful IEEE 802.lX exchange, SAE authentication, FILS authenticaiton,(11s) preshared PMK information, or PMK cached via some other mechanism.
* PMKSA

When the PMKSA is the result of a successful IEEE 802.1X authentication, it is derived from the EAP authentication and authorization parameters provided by the AS. When the PMKSA is the result of a successful SAE authentication, it is generated as a result of the successful completion of the SAE exchange.(11s) When the PMKSA is the result of a successful FILS authentication, it is generated as a result of the successful completion of the FILS authentication protocol. This security association is bidirectional. In other words, both parties use the information in the security association for both sending and receiving. The PMKSA is created by the Supplicant’s SME when the EAP authentication, or FILS authentication completes successfully or the PSK is configured. The PMKSA is created by the Authenticator’s SME when the PMK is created from the keying information transferred from the AS, when IEEE 802.1X authentication is utilized, or when the SAE exchange or FILS authentication exchange successfully completes(11s) or the PSK is configured. The PMKSA is used to create the PTKSA. PMKSAs are cached for up to their lifetimes. The PMKSA consists of the following elements:

***Modify section 11.5.1.3.2 as indicated:***

* Security association in an ESS

In an ESS there are two cases:

* Initial contact between the STA and the ESS
* Roaming by the STA within the ESS

A STA and AP establish an initial security association via the following steps:

* The STA selects an authorized ESS by selecting among APs that advertise an appropriate SSID and FILS capabilities.
* The STA then performs(11s) IEEE 802.11(11s) authentication followed by association to the chosen AP. Confirmation(11s) of security parameters takes place during association. A STA performing IEEE 802.1X authentication uses Open System authentication. A STA performing secure password-based, or PSK, authentication uses SAE authentication.(11s) A STA performing authentication for fast initial link set-up performs FILS authentication.

NOTE 1—It is possible for more than one PMKSA to exist. As an example, a second PMKSA might(#10381) come into existence through PMKSA caching. A STA might leave the ESS and flush its cache. Before its PMKSA expires in the AP’s cache, the STA returns to the ESS and establishes a second PMKSA from the AP’s perspective.

NOTE 2—An attack altering the security parameters is(#10369) detected by the key derivation procedure.

NOTE 3—IEEE 802.11 Open System authentication provides no security, but is included to maintain backward compatibility with the IEEE 802.11 state machine (see 10.3 (STA authentication and association)).

* SAE authentication and FILS authentication provide mutual authentication and derivation of a PMK. If Open System authentication is chosen instead,(11s) the (#3098)Authenticator or the (#3098)Supplicant initiates IEEE 802.1X authentication. The EAP method used by IEEE Std 802.1X-2004(#10369) needs to support mutual authentication, as the STA needs assurance that the AP is a legitimate AP.

NOTE 1—Prior to the completion of IEEE 802.1X authentication and the installation of keys, the IEEE 802.1X Controlled Port in the AP blocks(#10369) all data frames. The IEEE 802.1X Controlled Port returns to the unauthorized state and blocks all data frames before invocation of an MLME-DELETEKEYS.request primitive. The IEEE 802.1X Uncontrolled Port allows IEEE 802.1X frames to pass between the Supplicant and Authenticator. Although IEEE Std 802.1X-2004 does not require a Supplicant Controlled Port, this standard assumes that the Supplicant has a Controlled Port in order to provide the needed level of security. Supplicants without a Controlled Port compromise RSN security and are not(#10382) used.

NOTE 2—Any secure network cannot support promiscuous association, e.g., an unsecured operation of IEEE Std 802.11. A trust relationship is needed(#10383) between the STA and the AS of the targeted SSID prior to association and secure operation, in order for the association to be trustworthy. The reason is that an attacker can deploy a rogue AP just as easily as a legitimate network provider can deploy a legitimate AP, so some sort of prior relationship is necessary to establish credentials between the ESS and the STA.

* The last step is key management. The authentication process, whether SAE authentication or FILS authentication utilizing IEEE 802.11 authentication frames or IEEE 802.1X authentication utilizing data frames post association, creates cryptographic keys shared between the cryptographic endpoints—the AP and STA,(11s) or the IEEE 802.1X AS and the STA, when using SAE/FILS or IEEE 802.1X, respectively. When using IEEE 802.1X(11s) the AS transfers these keys to the AP, and the AP and STA uses one of the key confirmation handshakes, e.g., the 4-Way Handshake or FT 4-Way Handshake,(#1038) to complete security association establishment. When using SAE authentication there is no AS and therefore no key transfer; the 4-way Handshake is performed directly between the AP and STA.(11s) The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow normal data traffic and protected (#13074)robust management frames(11w). FILS authentication performs key confirmation as part of the exchange and no additional handshake is necessary.

When FT is not enabled, a STA roaming within an ESS establishes a new PMKSA by one of the four(11s) schemes:(#1039)

* In the case of (re)association followed by IEEE 802.1X or PSK authentication, the STA repeats the same actions as for an initial contact association, but its Supplicant also deletes the PTKSA when it roams from the old AP. The (#3098)Supplicant also deletes the PTKSA when it disassociates/deauthenticates from all BSSIDs in the ESS.
* In the case of SAE authentication followed by (re)association, the STA repeats the same actions as for initial contact association, but the non-AP STA also deletes the PTKSA when it roams from the old AP. Note that a STA can take advantage of the fact that it can perform SAE authentication to multiple APs while maintaining a single association with one AP, and then use any of the PMKSAs created during authentication to effect a fast BSS transition.(11s)
* In the case of FILS authentication, the STA repeats the same actions as for initial contact and authentication. Note that a STA can take advantage of the fact that it can initiate FILS authentication to multiple APs while maintaining a single association with one AP, and finalize the FILS authentication with one AP.

***Modify section 11.5.9.1 as indicated:***

11.5.9 RSNA authentication in an ESS

11.5.9.1 General(#28)

When establishing an RSNA in a non-FT environment or during an FT initial mobility domain association,(#1040) a STA shall use IEEE 802.11 SAE authentication, FILS authentication or(11s) Open System authentication prior to -(re)association.

SAE authentication is initiated when a STA’s MLME-SCAN.confirm primitive finds another AP within the current ESS that advertises support for SAE in its RSN element.

FILS authentication is initiated when a STA’s MLME-SCAN.confirm primitive finds an AP that advertises support for FILS in its RSN element and indicates support for a trusted third party known to the STA.(11s)

IEEE 802.1X authentication is initiated by any one of the following mechanisms:

* If a STA negotiates to use IEEE 802.1X authentication during (re)association, the STA’s management entity may(#12694) respond to the MLME-ASSOCIATE.confirm (or indication) primitive by requesting the (#3098)Supplicant (or (#3098)Authenticator) to initiate IEEE 802.1X authentication. Thus, in this case, authentication is driven by the STA’s decision to associate and the AP’s decision to accept the association.
* If a STA’s MLME-SCAN.confirm primitive finds another AP within the current ESS, a STA may signal its Supplicant to use IEEE Std 802.1X-2004 to preauthenticate with that AP.

NOTE—A roaming STA’s IEEE 802.1X Supplicant can(#1520) initiate preauthentication by sending an EAPOL-Start message via its old AP, through the DS, to a new AP.

* If a STA receives an IEEE 802.1X message, it delivers this to its Supplicant or Authenticator, which may initiate a new IEEE 802.1X authentication.

***Modify section 11.5.12 as indicated:***

* + 1. RSNA key management in an ESS

When the IEEE 802.1X authentication completes successfully, this standard assumes that the STA’s IEEE 802.1X Supplicant and the IEEE 802.1X AS (#10369)share a secret, called a PMK. In a non-FT environment, the(#1042) AS transfers the PMK, within the MSK, to the AP, using a technique that is outside the scope of this standard; the derivation of the PMK from the MSK is EAP-method-specific. With the PMK in place, the AP initiates a key -confirmation handshake with the STA. The key confirmation handshake sets the IEEE 802.1X state variable portValid (as described in IEEE Std 802.1X-2004) to TRUE.

When SAE authentication completes, both STAs share a PMK. With this PMK in place, the AP initiates the key confirmation handshake with the STA.

Key confirmation is part of the FILS authentication exchange and no further handshakes are needed to satisfy key management requirements in an ESS.(11s)

When FILS authentication is not used, the key confirmation handshake is implemented by the 4-Way Handshake. The purposes of the 4-Way Handshake are as follows:

* Confirm the existence of the PMK at the peer.
* Ensure that the security association keys are fresh.
* Synchronize the installation of temporal keys into the MAC.
* Transfer the GTK from the Authenticator to the Supplicant.
* Confirm the selection of cipher suites.

NOTE 1—It is possible to forge message 1 of the 4-Way Handshake.(#12703) However, the forgery attempt is(#10369) detected in the -failure of the 4-Way Handshake.

NOTE 2—Neither the AP nor the STA can use the PMK for any purpose but the one specified herein without compromising the key. If the AP uses it for another purpose, then the STA can masquerade as the AP; similarly if the STA reuses the PMK in another context, then the AP can masquerade as the STA.

***Create section 11.9a and its component subsections***

**11.9a Authentication for Fast Initial Link Set-up**

STAs, both AP STAs and non-AP STAs, who share a means of authentication—either mutual trust of a third party, or based on trust in a known entity that certified the other party’s public keys—may use that shared trust to mutually authenticate and derive a shared key in a more efficient manner than using IEEE 802.1X.

The FILS Authentication protocol authenticates STAs to each other, optionally using a TTP. The authentication exchange can optionally be performed with PFS. When a TTP is not used, PFS shall be used. When the FILS authentication protocol is performed with PFS, the STA and AP derive ephemeral public and private keys with respect to a particular set of domain parameters that define a finite cyclic group and then exchange public keys. When an online trusted third party is not used, the FILS Authentication protocol executes an ephemeral Diffie-Hellman key agreement scheme, where the Diffie-Hellman exponents are signed by each communicating party, thus obviating the need for online involvement of a third party. The STA and AP each derive ephemeral public and private keys with respect to a particular set of domain parameters that define a finite cyclic group and then exchange the resulting ephemeral public keys. Authentication and key establishment shall be obtained by the STA and AP themselves.. In either case, the result of the FILS Authentication protocol is a PTKSA. FILS Authentication is an RSNA authentication protocol.

**11.9a.1 Assumptions on FILS Authentication**

The security of FILS authentication depends on the following assumptions:

* Communication between the STAs and the trusted third party, when applicable, is protected with a secure deterministic authenticated encryption function.
* When using a TTP, each STA shares a symmetric key (or keys) with the trusted third party that is (are) capable of being used with ERP; when not using a TTP, each STA shall have a means to trust the public key of the other STA. When not using an online TTP, each STA shall have a device certificate that is issued by a Certificate Authority that is trusted by the other STA or shall have another means to verify the authenticity of the public key of the other STA.
* When PFS is used, a finite cyclic group is negotiated for which solving the discrete logarithm problem is computationally infeasible. This shall be a group with at least 80-bits of cryptographic bit strength and should be a group with 128-bit of cryptographic bit strength.
* When PFS is used, both the STA and AP have at least one finite cyclic group from the dot11RSNAConfigDLCGroupTable in common.
* When not using an online TTP, both the STA and AP shall support the prime curve P-256 specified in FIPS 186-3 and ECDSA using this curve and the SHA-256 as hash function defined by FIPS 180-2. Each device may support other finite cyclic groups, as long as these meet the minimum cryptographic bit strength requirement of having at least 80-bit cryptographic bit strength.

All FILS Association frames shall be encrypted and authenticated (see 11.9a.2.5 and 11.9a.2.6).

**11.9a.2 FILS Authentication protocol**

The STA and the AP communicate using Authentication frames to perform key establishment and 802.11 association frames to perform key confirmation and mutual entity authentication.

After exchanging Authentication frames, the STA and AP derive a shared and secret key which will be used to derive a set of secret keys that are authenticated via the exchange of 802.11 association frames. This provides for mutual key confirmation and entity authentication between both parties.

When a trusted third party is used for FILS authentication, then EAP-RP as defined in [IETF RFC 5295/6696] shall be used. With FILS authentication without TTP, mutual device authentication is realized via the exchange by either party of a digital signature over the communicated ephemeral keys and verification hereof by the other party.

**11.9a.2.1 Discovery with FILS Authentication**

An AP indicates that it is capable of performing FILS Authentication by constructing a FILS-capable Beacon or Probe response. FILS-capable 802.11 Beacons or Probe responses shall contain an AKM suite element indicating support for FILS Authentication as well as FILS Identity IEs indicating the identity of the AP and, when applicable, the identity(-ies) of the trusted third party(-ies) with whom the AP maintains a relationship.

A STA that discovers a FILS-capable AP that claims a trusted relationship with a mutually-trusted third party may begin the FILS Authentication protocol to the AP and perform mutual authentication using the trusted third party only if the STA and trusted third party already share a valid rRK, as defined in [IETF RFC 6696]. A STA that discovers a FILS-capable AP that advertises an identity for which the STA has a trusted public key may begin the FILS Authentication protocol to the AP and perform mutual authentication using trusted public keys.

**11.9a.2.2 Key Establishment with FILS Authentication**

A FILS-capable STA and AP establish a shared key by exchanging Authentication frames. The specific contents of the Authentication frame depend on the particular authentication technique—whether a TTP is being used or whether digital signatures are being used—and whether PFS is obtained in the exchange or not.

**11.9a.2.2.2b FILS Key Establishment without trusted third party**

A FILS-capable STA and AP establish a shared key by exchanging Authentication frames that include ephemeral keys contributed by either party and which are used to compute a shared Diffie-Hellman key.

The STA selects a finite cyclic group to be used with FILS key establishment (see 11.9a.2.6b). It then generates an ephemeral public-private key pair corresponding to this group, according to the procedure specified in Section 5.6.1 of NIST SP 800-56a (for the specific finite field group chosen).

The STA shall construct a nascent Authentication Request frame, with the Authentication algorithm number set to <ANA-1>, with the Authentication transaction sequence number set to one (1), with the Finite Cyclic Group field set to the selected finite cyclic group (see 8.4.1.42), with the FILS Identity element indicating the STA’s FILS Identity (see 8.4.2.121a), with the FILS Public Key element field indicating the just generated ephemeral public key (see 8.4.1.40b), with the FILS Certificate element indicating the device’s public-key certificate (see 8.4.2.40c), with the FILS session element indicating the the FILS session identifier (see 8.3.3.11), and with the FILS authentication type indicating FILS authentication without a trusted third party (2).

The STA shall transmit the resulting 802.11 Authentication frame to the AP.

Upon receipt of the Authentication Request frame, the AP determines whether the indicated finite cyclic group is supported. If not, it shall respond with an Authentication Response frame with the status code of 77 (“Authentication is rejected because the offered finite cyclic group is not supported”) and terminate the FILS authentication protocol.

If the finite cyclic group is acceptable, the AP shall verify the validity of the STA’s ephemeral public key according to the procedure described in Section 5.6.2.3 of NIST SP 800-56a (for the indicated finite field group). If public key validation fails, the AP shall reject the received frame and FILS authentication shall fail.

The AP may decide to reject the received Authentication Request frame based on criteria that are outside the scope of the standard. If so, it shall generate an Authentication Response frame with the status code of TBD (“Authentication rejected”) and terminate the FILS authentication protocol.

NOTE 1– Upon receipt of the Authentication Request frame from the STA, the AP may exchange information with a third device, e.g., so as to assist in authorization decisions regarding admission of STA to the network. These communications, however, are outside scope of the FILS authentication protocol and the standard, since involving authorization, rather than authentication, messaging. Similarly, any state updates by the AP that solely depend on return messaging by such a third device are outside scope of the FILS protocol and the standard. This is motivated by the observation that, from the STA’s perspective, the mechanism by which the AP arrives at authorization decisions is unknown (i.e., it has no way of verifying whether these took place using localized knowledge only or would also involve intelligence as part of the network infrastructure). As a final note, authorization decisions as to which services a device may perform on the network may very well depend on details of higher-layer protocols that cannot be vetted at the network level.

NOTE 2 – Upon receipt of the Authentication Request frame from the STA, the AP may determine that it cannot verify the certificate of STA, since it was signed by a Certificate Authority that is unknown to AP. In that case, AP may exchange information with a third device, so as to get this third device to vouch for the authenticity of STA’s public key or so as to get a “compatible” certificate itself. In this scenario, involvement of the third party would assist in successful authentication. Even so, whether or not the AP involves a third party in this certificate translation or in certificate verification is unknown to STA.

Otherwise, the AP shall generate an ephemeral public-private key pair corresponding to the same finite cyclic group indicated with the received Authentication Request frame, according to the same procedure used by STA, i.e., as specified in Section 5.6.1 of NIST SP 800-56a (for the specific finite field group chosen).

Subsequently, the AP shall construct an Authentication Response frame similar in format to the Authentication Request frame just received, but now including its own FILS identity, its own ephemeral public key, and its own device certificate, and with no setting the Authentication transaction sequence number to two (2).

AP shall transmit the resulting Authentication Response frame to the STA.

AP may now compute the shared Diffie-Hellman key using the Diffie-Hellman primitive specified in Section 5.7.1 of NIST SP 800-56A (for the specific finite field group chosen) and then derive related keying material (see 11.9a.2.3b). Alternatively, it may choose to delay these operations till it receives an Association Request frame from the STA, for which processing depends on access to this derived keying material (see 11.9a.2.4b).

Upon receipt of the Authentication Response frame, the STA determines whether the indicated finite cyclic group and the session identifier both match the corresponding values it sent to AP. Moreover, it shall check that the FILS identifier of the AP corresponds to the AP it sent the Authentication Request frame to. If there is a mismatch, the STA shall terminate the FILS authentication protocol. Otherwise, STA shall verify the validity of AP’s ephemeral public key according to the procedure described in Section 5.6.2.3 of NIST SP 800-56a (for the indicated finite field group). If public key validation fails, the STA shall reject the frame and FILS authentication shall fail.

Similar to the AP, the STA may decide to reject the received Authentication Response frame based on criteria that are outside the scope of the standard. If so, it shall terminate the FILS authentication protocol.

Otherwise, STA shall now compute the shared Diffie-Hellman key using the Diffie-Hellman primitive specified in Section 5.7.1 of NIST SP 800-56A (for the specific finite field group chosen) and then derive related keying material (see 11.9a.2.3b). The STA shall then initiate key confirmation (see 11.9a.2.4b).

**11.9a.2.3b Key Derivation with FILS Authentication without trusted third party**

Key derivation with FILS Authentication uses the “Extraction-then-Expansion” key derivation procedure to produce three keys: a key confirmation key (KCK), a key encryption key (KEK), and a traffic key (TK*).* The KCK is a 256-bit key and is used for key confirmation between STA and AP (see 11.9a.2.4b). The KEK is a 128-bit key and is used for enciphering/deciphering of so-called “piggy-backed” information that may be communicated along the key confirmation flows of the key agreement protocol (see 11.9a.2.5b). The key TK is a key of bit-length TK\_bits, where TK\_bits is determined from Table 11-4, and is used for securing subsequent 802.11 traffic.

Note RS: The “Extraction-then-Expansion” key derivation procedure specified below complies with the provisions in NIST SP 800-56a (Clause 5.8.2) and its referenced specifications NIST SP 800-56C (Section 5) and NIST SP 800-108 (Section 5.1).

The “Extraction-then-Expansion” key derivation procedure consists of the following three steps (in order):

Step 1: Key Extraction

Compute the string KeyDerivationKey as KeyDerivationKey:=HMAC-SHA256(Salt, Z), where the string Z is the output of the Diffie-Hellman primitive specified in Section 5.7.1 of NIST SP 800-56A and where the string Salt is the right-concatenation of the x-coordinate of the ephemeral key EphKeySTA and the x-coordinate of the ephemeral key EphKeyAP contributed by STA and AP, respectively, during key establishment (see 11.9a.2.2.2b).

Step 2: Key Expansion

Compute the string DerivedKeyingMaterial, which is the output of the “KDF using CTR” construct specified in Section 5.1 of NIST SP 800-108, with as fixed parameters r=32 and h=256, and instantiated with as inputs the key derivation key computed in the key extraction step above, with as Label the (fixed) string “FILS Key Derivation”, with as Context field the right-concatenation of the certificate fields CertSTA and CertAP of STA and AP, respectively, and with as parameter L the integer 384 + TK\_bits.

Step 3: Key Partitioning

Parse the string DerivedKeyingMaterial as DerivedKeyingMaterial =: KCK | KEK | TK, where KCK is a 256-bit key and where KEK is a 128-bit key.

**11.9a.2.4b Key Confirmation with FILS Authentication without trusted third party**

Upon the completion of FILS key establishment (11.9a.2.2.2) and key derivation (11.9a.2.3b), the STA and AP evidence possession of the established shared key to each other and authenticate each other by exchanging Association frames. Along these key confirmation and authentication messages, additional so-called “piggy-backed” information is exchanged in enciphered format. The keys used for key confirmation and enciphering are the keys KCK and KEK. Entity authentication is provided using digital signatures provided by STA and AP.

For the AP, transfer of “piggy-backed” information in the Association Response frame includes the transfer of any necessary KDEs to the STA, via the inclusion of one or more KDEs using the FILS KDE container. The format and the rules for transferring the KDE shall follow section 11.6.2 (EAPOL Key Frames).

The STA shall construct a nascent 802.11 Associate Request frame indicating its selected cipher-suite and the FILS AKM, with FILS session identifier Sid set to the value used during key establishment (see 11.9a.2.2.2), with the Key Confirmation element constructed as follows:

 Key-Confirm-STA = HMAC-SHA256(KCK, “Const\_STA” | STA-MAC | AP-BSSID | EphKeySTA |

 EphKeyAP | FILS-Sid | ADTextDataSTA | CTextDataSTA),

where the string Const\_STA is the fixed string “KC\_2\_U”, where EphKeySTA and EphKeyAP are the ephemeral public keys contributed by STA and AP in their respective key establishment messages, where ADTextDataSTA and CTextDataSTA indicate additional “piggy-backed” data after securing by STA (see 11.9a.2.5b),

and with as Signature element the digital signature generated by STA using the private key corresponding to the public key contained in STA’s device certificate indicated in the 802.11 Authenticate Request frame, constructed as follows:

Signature-STA = Sign-STA (EphKeySTA | FILS-ID STA | FILS-Sid),

according to the signature generation procedures detailed for the scheme for the finite field group used by STA.

The STA shall transmit the resulting 802.11 Associate Request frame to the AP.

The AP shall verify the correctness of the Key Confirmation element included with the received 802.11 Associate Request frame by re-computing this value itself, but now with its own key KCK and its own version of all other data elements. If this verification fails, FILS Authentication shall fail and the keys KCK, KEK, TK and shared secret shall be irretrievably destroyed.

The AP shall decipher the “piggy backed data” (see 11.9a.2.5b). Subsequently, the AP shall verify STA’s certificate included with the received 802.11 Authenticate Request frame and the signature element Signature-STA included with the received 802.11 Associate Request frame, including policy checks (as in RFC5480) and checking that the certificate’s Subject field of the public key corresponds to the FILS-ID STA Identifier. This verification may be carried out prior to constructing the 802.11 Associate Response frame or delayed (so as to allow for offline processing). In either case, if verification fails, FILS authentication shall fail and the keys KCK, KEK, TK and shared secret shall be irretrievably destroyed. If deciphering is not deemed a failure and all verification steps succeed, FILS authentication shall succeed and AP shall use the TK generated in 11.9a.2.3b with the cipher that was indicated by the cipher-suite in the Associate Request frame. AP shall irretrievably destroy the ephemeral private key used during the execution of the FILS authentication protocol and shall similarly destroy the keys KCK, KEK, and the shared Diffie-Hellman key.

If authentication is not deemed a failure, the AP shall construct a nascent 802.11 Associate Response frame confirming the selected cipher-suite, the FILS AKM, and FILS session identifier Sid, but now with the role of STA and AP reversed and using its own KCK and KEK keys and its own private key to construct it own key confirmation element, its own signature, and its own secured “piggy-backed” data. Thus, the Key Confirmation element shall be constructed as follows:

 Key-Confirm-AP = HMAC-SHA256(KCK, “Const\_AP” | AP-BSSID | STA-MAC | EphKeyAP |

 EphKeySTA | FILS-Sid | ADTextDataAP | CTextDataAP),

where the string Const\_AP is the fixed string “KC\_2\_V”, where EphKeySTA and EphKeyAP are the ephemeral public keys contributed by STA and AP in their respective key establishment messages, where ADTextDataAP and CTextDataAP indicate additional “piggy-backed” data after securing by AP (see 11.9a.2.5b),

and with as Signature element the digital signature generated by AP using the private key corresponding to the public key contained in AP’s device certificate indicated in the 802.11 Authenticate Response frame, constructed as follows:

Signature-AP = Sign-AP (EphKeyAP | FILS-ID AP | FILS-Sid),

according to the signature generation procedures detailed for the scheme for the finite field group used by AP.

The AP shall transmit the 802.11 Associate Response frame to the STA.

The STA shall verify the correctness of the received Key Confirmation element included with the received 802.11 Associate Response frame by re-computing this value itself, but now with its own key KCK and its own version of all other data elements. Subsequently, the STA shall verify AP’s certificate included with the received 802.11 Authentication Response frame and the signature element Sign-AP included with the 802.11 Associate Response frame, including policy checks (as in RFC5480) and checking that the certificate’s Subject field of the public key corresponds to the FILS-ID AP Identifier. If any verification fails, FILS Authentication shall fail and the keys KCK, KEK, TK and shared secret shall be irretrievably destroyed.

The STA shall decipher the “piggy-backed data” (see 11.9a.2.5b). If deciphering is not deemed a failure and all verification steps succeed, FILS authentication shall succeed and STA shall use the TK generated in 11.9a.2.3b with the cipher that was indicated by the cipher-suite in the Associate Request and Response frames.

Both the STA and AP shall irretrievably destroy the ephemeral private key used during the execution of the FILS authentication protocol and shall similarly destroy the keys KCK, KEK, and the shared Diffie-Hellman key.

**11.9a.2.5b Enciphering and Deciphering of “piggy-backed” information with FILS Authentication without trusted third party**

The input ADTextData field shall be the contents of the Associate Request frame (for STA) or Associate Response frame (for AP) from the capability element (inclusive) to the FILS signature element (inclusive).

Note RS: so, this does not include the Key Confirmation element.

Enciphering:

AES-CTR mode (as specified with NIST SP 800-38A) shall be used to secure the “piggy-backed information” MTextData in the 802.11 Associate Request frame (for enciphering by STA) or in the 802.11 Associate Response frame (for enciphering by AP), with the following instantiation:

* The key shall be the KEK (see 11.9a.2.3b);
* The plaintext MTextData shall be the contents of the Associate Request frame (for enciphering by STA) or that of the Associate Response frame (for enciphering by AP) that follow the FILS signature and FILS key confirmation elements;
* The counter to be used with the AES-CTR mode shall be set to

a) For enciphering by STA: use counter values 0, 1, 2, 3 (increment for each AES-128 block);

b) For enciphering by AP: use as counter values the one-complement of 0, 1,2, 3, ... (decrement for each AES-128 block).

The ciphertext CTextData resulting from this operation shall substitute the corresponding input string MTextData in the corresponding frame.

Deciphering:

AES-CTR mode (as specified with NIST SP 800-38A) shall be used to unsecure the “piggy-backed information” CTextData in the 802.11 Associate Request frame (for deciphering by AP) or in the 802.11 Associate Response frame (for deciphering by STA), with the following instantiation:

* The key shall be the KEK (see 11.9a.2.3b);
* The ciphertext CTextData shall be the contents of the received Associate Request frame (for deciphering by AP) or of the received Associate Response frame (for deciphering by STA) that follow the FILS signature and FILS key confirmation elements;
* The counter to be used with the AES-CTR mode shall be set to

a) for deciphering by AP: use counter values 0, 1, 2, 3 (increment for each AES-128 block);

b) for deciphering by STA: use as counter values the one-complement of 0, 1,2, 3, ... (decrement for each AES-128 block).

* The plaintext MTextData resulting from this operation shall substitute the corresponding input string CTextData in the corresponding frame.

**11.9a.2.6b Finite cyclic groups to be used with FILS authentication without trusted third party**

FILS key establishment may use any finite cyclic group from the dot11RSNConfigDLCGroup table, with the following stipulations:

* Groups with less than 80-bit cryptographic bit strength shall not be used;
* Each device shall support the elliptic curve P-256 (for interoperability reasons)
* FILS key establishment without trusted third party shall use digital signature based on the same group used for Diffie-Hellman key agreement. The cryptographic bit strength of the hash function used with digital signatures used with a group shall have at least the cryptographic bit strength as that of the group.
* FILS key establishment without trusted third party shall support the use of ECDH based on P-256 curve and ECDSA based on this curve and the hash function SHA-256. It may support other choices, provided the overall cryptographic bit strength is at least 80-bits crypto strength.

**References:**

**Motion-1:** To authorize the Editor to incorporate the text changes proposed in contribution 11-12-0052r4 (*11-12-0052-04-00ai-fils-authentication with certified public keys*) to the draft TGai Draft Specification Document.

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