**IEEE P802.11
Wireless LANs**

|  |
| --- |
| **Normative text for FILS** |
| **Date**: 2012-01-16 |
| Author(s): |
| Name | Company | Address | Phone | email |
| George Cherian | Qualcomm | 5775 Morehouse Dr., San Diego, CA | 8586516645 | gcherian@qualcomm.com |
| Santosh Abraham | Qualcomm Inc | 5775 Morehouse Dr., San Diego, CA | 858 651 6107 | sabraham@qualcomm.com |
| Jouni Malinen | Qualcomm Inc | Hermiankatu 6-8 DTampere, Finland |  | jouni@qca.qualcomm.com |
| Hitoshi MORIOKA  | Allied Telesis R&D Center.  | 2-14-38 Tenjin, Chuo-ku, Fukuoka 810-0001 JAPAN  | +81-92-771-7630  | hmorioka@root-hq.com  |
| Hiroshi Mano  | Allied Telesis R&D Center.  | 7-21-11 Nishi-Gotanda, Shinagawa-ku, Tokyo 141-0031 JAPAN  | +81-3-5719-7630  | hmano@root-hq.com  |
| Mark RISON  | CSR  | Cambridge Business Park, Cowley Road, Cambridge CB4 0WZ UK  | +44-1223-692000  | Mark.Rison@csr.com  |
| Marc Emmelmann  | Fraunhofer FOKUS  | Kaiserin-Augusta-Alle 31 10589 Berlin Germany  | +49-30-3463-7268  | emmelmann@ieee.org  |
| Ping Fang  | Huawei Technologies Co., Ltd.  | Bldg 7, Vision Software Park, Road Gaoxin Sourth 9, Nanshan District, Shenzhen, Guangdong, China, 518057  | +86 755 36835101  | ping.fang@huawei.com  |
| Zhiming Ding  | Huawei Technologies Co., Ltd.  | Bldg 7, Vision Software Park, Road Gaoxin Sourth 9, Nanshan District, Shenzhen, Guangdong, China, 518057  | +86 755 36835837   | dingzhiming@huawei.com  |
| Phillip Barber | Huawei Technologies Co., Ltd.  | 1700 Alma Rd, Ste 500Plano, Texas 75075 USA  | +1 972-509-5599  | pbarber@huawei.com  |
| Rob Sun  | Huawei Technologies Co., Ltd.  | Suite 400, 303 Terry Fox Drive, Kanata, Ontario K2K 3J1  | +1 613 2871948  | Rob.sun@huawei.com  |
| Chengyan Feng Bo Sun  | ZTE Corporation  |  |  | feng.chengyan@zte.com.cn sun.bo1@zte.com.cn  |

**Abstract**

The submission provides normative text based on the ideas presented in 11/1160/r5.

* **Concurrent Authentication with IP address Assignment**
	+ Allows protection (integrity check & encryption) for IP address assignment message
		- based on STA choice
* **Use of EAP**
	+ Optimized EAP authentication to setup the EAP-RP context when EAP-RP context is not setup or expired
	+ EAP-RP based authentication during subsequent link setup
	+ Builds on existing EAP framework in 802.1X security architecture
* **RSNA security**
	+ The proposal meets the RSNA security requirement

**2. Normative references**

**Notice:** This document has been prepared to assist IEEE 802.11. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

**Release:** The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.11.

**Patent Policy and Procedures:** The contributor is familiar with the IEEE 802 Patent Policy and Procedures <[http:// ieee802.org/guides/bylaws/sb-bylaws.pdf](#_blank)>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <stuart@ok-brit.com> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.11 Working Group. **If you have questions, contact the IEEE Patent Committee Administrator at <**patcom@ieee.org**>**.

The following referenced documents are indispensable for the application of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

*Instructions to Editor: Add the following definition as shown underlined*

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

IETF RFC 5296, EAP Extensions for EAP Re-authentication Protocol (ERP), V. Narayanan, August 2008

**3.1 Definitions**

[Add the following definitions]

*Instructions to Editor: Add the following definition as shown underlined*

**concurrent IP address assignment**: An IP address assignment procedure that takes place concurrently with FILS authentication process.

[…]

*Instructions to Editor: Add the following subclauses to clause 4.5*

**4.5.x Fast Initial Link Setup (FILS)**

This subclause summarizes the fast initial link setup (FILS) operation. FILS setup reduces typical initial link setup time by concurrently performing the EAP based authentication, association, EAPOL Key exchange and IP address assignment procedure. Also, additional message saving for EAPOL Key exchange is obtained by sending ANonce in the beacon or Probe Response.

**4.5.x.1 Fast Initial Link Setup Authentication Procedure**

FILS uses EAP based authentication. Each instance of FILS consists of one of the following two cases

1. FILS context is not setup on the non-AP STA. FILS context consists of a valid rRK, rIK & EMSK/DSRK that are created as part of a EAP authentication for EAP-RP (see [IETF RFC 5295] and [IETF RFC 5296]). EAP authentication is performed either using Optimized EAP procedure (see clause 10.3.x.1) or IEEE 802.1X-2004. EAP authentication messages are sent using Authentication frames and Association request/Association Response frames.
2. When FILS context is setup on the STA, an EAP-RP based authentication is performed as specified in [IETF RFC 5295] and [IETF RFC 5296]. The EAP-RP authentication messages are sent using Association Request/Association Response frames.

**4.5.x.3 EAPOL Key Exchange for FILS**

At an AP where dot11MngmtOptionsFILSActivated is true, the EAPOL key exchange procedure is optimized by the following:

* AP sends ANonce using probe response or beacon instead of sending a separate EAPOL key message that carries ANonce as described in the step-1 of EAPOL key exchange. Or the AP encapsulates the first message of EAPOL key exchange which carries ANonce together with the first EAP-Request of any EAP method into the first Authentication frame in case EAP-RP can not be used.
* STA does not send an ‘EAPOL Key confirmation’ message since MAC layer acknowledgement provides the confirmation of delivery of the step-3 of EAPOL Key frame.

**4.5.x.4 IP Address Assignment Procedure for FILS**

Concurrent IP Address assignment with association is achieved by sending IP address request and response messages in Association Request and Association frames. If IP address assignment server doesn’t respond within a certain period, then the AP may send Association Response frame with indication of IP configuration unavailable/pending.

**4.5.x.3 Fast Initial Link Setup Association Procedure**

FILS uses Association Request and Association Response frames to transport authentication and IP address assignment messages between STA and the AP.

**4.10.3.1 General**

*Instructions to Editor: Change the following section as shown below*

This subclause summarizes the system setup and operation of an RSN, in three cases: when a password or PSK is used during IEEE 802.11 authentication, when an IEEE 802.1X AS is used after Open System authentication, and when a PSK is used after Open System authentication. For an ESS, the AP includes an Authenticator, and each associated STA includes a Supplicant. The operation for FILS is shown in section 4.5.x.

**6.3.5 Authenticate**

**6.3.5.2 MLME-AUTHENTICATE.request**

**6.3.5.2.1 Function**

**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,

Content of FILS Authentication Frame,

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,FAST\_INITIAL\_LINK\_SETUP | 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, 8.4.1.40, 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. |
| Content of FILS Authentication Frame | Sequence of elements and fields | *TBD* | *TBD* |
| 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,

Content of FILS Authentication Frame,

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,FAST\_INITIAL\_LINK\_SETUP | 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. |
| Content of FILS Authentication Frame | Sequence of elements and fields | *TBD* | *TBD* |
| 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,

Content of FILS Authentication Frame,

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. |
| Content of FILS Authentication Frame | Sequence of elements and fields | *TBD* | *TBD* |
| VendorSpecificInfo | A set of elements | As defined in 8.4.2.28 | Zero or more elements. |

**6.3.7 Associate**

**6.3.7.2 MLME-ASSOCIATE.request**

**6.3.7.2.2 Semantics of the service primitive**

*Instructions to Editor: Change the clause as shown underlined*

The primitive parameters are as follows:

MLME-ASSOCIATE.request(

PeerSTAAddress,

AssociateFailureTimeout,

CapabilityInformation,

ListenInterval,

Supported Channels,

RSN,

QoSCapability,

Content of FT Authentication elements,

SupportedOperatingClasses,

HT Capabilities,

Extended Capabilities,

20/40 BSS Coexistence,

QoSTrafficCapability,

TIMBroadcastRequest,

EmergencyServices,

FILSAuthMessage,

ULAddrAssigmentReq,

FILSKeyExchangeMessage,

VendorSpecificInfo

)

*Instructions to Editor: Add the following rows to the table in Clause 6.3.7.2.2*

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| FILSAuthMessage | Upper Layer Message Transport element | As defined in 8.4.2.ai4 | FILS Authentication Message |
| ULAddrAssigmentReq | Upper Layer Message Transport element | As defined in 8.4.2.ai4 | Upper Layer IP addresss assignment request Message |
| FILSKeyExchangeMessage | Upper Layer Message Transport element | As defined in 8.4.2.ai4 | FILS Key Exchange message |

[…]

**8.3.3.2 Beacon frame format**

The frame body of a management frame of subtype Beacon contains the information shown in Table 8-20

(Beacon frame body).

*Instructions to Editor: Add two rows to Table 8-20 as follows*

**Table 8-20—Beacon frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| … | … | … |
| 55 | Mesh ChannelSwitch Parameters | The Mesh Channel Switch Parameters element is optionally present when dot11MeshActivated is true and either Channel Switch Announcement element or Extended Channel Switch Announcement element is present. |
| ANA | ANonce | The ANonce element may be present when Fast Initial Link Setup field of Extended Capabilities element is set to 1. |
| … |  |  |

[…]

**8.3.3.5 Association Request frame format**

The frame body of a management frame of subtype Association Request contains the information shown in

Table 8-22 (Association Request frame body).

*Instructions to Editor: Add a row to Table 8-22 as follows*

**Table 8-22—Association Request frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| … | … | … |
| ANA | EAP Message Transport | One or more EAP elements are optionally present |

[…]

**8.3.3.6 Association Response frame format**

*Instructions to Editor: Add a row to Table 8-23 as follows*

The frame body of a management frame of subtype Association Response contains the information shown in

Table 8-23 (Association Response frame body).

**Table 8-23—Association Response frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| … | … | … |
| ANA | EAP Message Transport | One or more EAP elements are optionally present |

[…]

**8.3.3.10 Probe Response frame format**

*Instructions to Editor: Add a row to Table 8-27 as follows*

The frame body of a management frame of subtype Probe Response contains the information shown in Table 8-27 (Probe Response frame body). See additional details and procedures in 9.18.3 (Determination of hopping patterns for FH PHYs) and 10.1.4 (Acquiring synchronization, scanning), respectively.

**Table 8-27—Probe Response frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| … | … | … |
| ANA | ANonce | The ANonce element is present when Fast Initial Link Setup field of Extended Capabilities element is set to 1. |

**8.3.3.11 Authentication frame format**

The frame body of a management frame of subtype Authentication contains the information shown in Table 8-28. FT authentication is used when FT support is advertised by the AP and dot11FastBSSTransitionActivated is true in the STA. SAE authentication is used when dot11MeshActiveAuthenticationProtocol is sae (1).

*[Change Table 8-28 as:]*

**Table 8-28—Authentication frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 5 | RSN | The RSNE is present in the FT and FILS Authentication frames as defined in Table 8-29. |
| … |  |  |
| ANA | EAP Message | EAP elements are present in the FILS Authentication frames as defined in Table 8-29. Multiple EAP elements can be present to encapsulate a single upper layer message.These upper layer messages includes EAPoL messages defined in 802.1x and EAPoL\_Key frames defined in 11.6.2. The detail of the EAP elements usage sees *TBD*. |
| Last | Vendor Specific | One or more vendor-specific elements are optionally present.These elements follow all other elements. |

*[Change Table 8-29 as:]*

**Table 8-29—Presence of fields and elements in Authentication frames**

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication algorithm** | **Authentication transaction sequence no.** | **Status code** | **Presence of fields 4-16** |
| FILS | 1 | Reserved | One group of EAP elements are present and an EAPoL(EAP\_Response/ID) is encapsulated in them. |
| FILS | 2 | Status | Two groups of EAP elements are present. An EAPoL(EAP\_Request), the first EAP\_Request of EAP method is encapsulated in first group of EAP elements. The First EAPoL(EAPoL-Key) of 4-way handshake is encapsulated in second group of EAP elements. |
| FILS | 2+x(x=1,3,5) | Status | One group of EAP elements are present. An EAPoL(EAP\_Response), additional step for some EAP method, is encapsulated in the EAP elements.  |
| FILS | 2+x(x=2,4,6) | Status | One group of EAP elements are present. An EAPoL(EAP\_Request), additional step for some EAP method, is encapsulated in the EAP elements. |

[…]

**8.4.1.1 Authentication Algorithm Number field**

*Instructions to Editor: Add underlined text as shown below*

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 Figure 8-35. 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

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

Authentication algorithm number = 4: Fast Initial Link Setup (FILS)

Authentication algorithm number = 65 535: Vendor specific use

NOTE—The use of this value implies that a Vendor Specific element is included with more information.

All other values of authentication algorithm number are reserved.

**8.4.2.27 RSN element**

**8.4.2.27.3 AKM suites**

*[Change Table 8-101 as:]*

**Table 8-101—AKM suite selectors**

|  |  |  |
| --- | --- | --- |
| OUI | Suite Type | **Meaning** |
| **Authentication type** | **Key management type** | **Key derivation type** |
| 00-0F-AC | ANA | 802.1x over FILS | RSNA key management as defined in 11.6. | Defined in 11.6.1.2 |
| 00-0F-AC | ANA+1 –255 | Reserved | Reserved | Reserved |

**8.4.2.29 Extended Capabilities element**

*[Change Table 8-101 as:]*

**Table 8-103—Capabilities field**

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| ANA | Fast Initial Link Setup | The STA sets the Fast Initial Link Setup field to 1 when dot11MgmtOptionFILSActivated is true and sets it to 0 otherwise. See 10.25. |
| ANA | Unencrypted HLS request supported | This indicates whether the Access Point supports reception of an un-encrypted HLS request from a STA. |
|  |  |  |

[…]

*Instructions to Editor: Add the following new section*

**8.4.2.x EAP element**

The EAP element includes one or part of an EAP message. Multiple EAP elements may be occurred in a management frame to carry a whole EAP message. This element is shown in Figure 8-11ai01.

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | EAP Message Type | EAP Message body |

**Figure 8-11ai01 EAP element format**

The Element ID is set to the value given in Table 8-54 (Element IDs) for this element.

The Length field is set to the value of bytes of the field EAP Message.

The EAP Message Type is shown in Table 8-11ai01.

|  |  |
| --- | --- |
| EAP Message Type | EAP Message |
| 1 | FILS Authentication Message |
| 2 | FILS Key Exchange Message |
| 3 to 255 | Reserved |

EAP Message Body is a whole EAP message or part of an EAP message.

[…]

**10.3.2 State transition diagram for non-mesh STAs**

Figure 10-6 shows the state transition diagram for non-mesh STA states. Note that only events causing state changes are shown. The state of the sending STA given by Figure 10-6 is with respect to the intended receiving STA.

*[Change Figure 10-6 as:]*

**Figure 10-6—Relationship between state and services**

*[Change subclause 10.3.4 as:]*

**10.3.4 Authentication and deauthentication**

This subclause describes the procedures used for IEEE 802.11 authentication and deauthentication. The states used in this description are defined in 10.3.1.

Successful authentication without FILS sets the STA's state to State 2, if it was in State 1. Successful FILS authentication sets the STA’s state from State1 to State4 directly. Unsuccessful authentication leaves the STA's state unchanged. The STA shall not transmit Class 2 frames unless in State 2 or State 3 or State 4. The STA shall not transmit Class 3 frames unless in State 3 or State 4.

Deauthentication notification sets the STA's state to State 1. The STA shall become authenticated again prior to sending Class 2 frames. Deauthentication notification when in State 3 or 4 implies disassociation as well. A STA may deauthenticate a peer STA at any time, for any reason.

If STA A in an infrastructure BSS receives a Class 2 or Class 3 frame from STA B that is not authenticated with STA A (i.e., the state for STA B is State 1), STA A shall discard the frame. If the frame has an individual address in the Address 1 field, the MLME of STA A shall send a Deauthentication frame to STA B.

Authentication is optional in an IBSS. In an infrastructure BSS, authentication is required. APs do not

initiate authentication.

[…]

*Instructions to Editor: Insert a new section as follows*

**10.3.x Association and Reassociation with FILS**

FILS consists of two cases.

* When FILS context is not setup, an EAP authentication is performed using either IEEE 802.1X-2004 or optimized EAP Authentication as specified in 10.3.x.1.
* When FILS context is setup, a concurrent EAP-RP authentication with IP address assignment is performed as specified in section 10.3.x.2.

**10.3.x.1 Optimized EAP Authentication**



Figure 10ai0 **—Call flow for FILS using Optimized EAP**

Optimized Full EAP is performed when EAP-RP context (EMSK, rRK, rIK) is not setup or has expired.

Different IP address assignment mechanism could be used, depending on the network deployment.

Figure 10-ai0 describes the steps required for FILS with Optimized EAP

Step-1: EAPoL-Start and EAP-Request/ID are skipped. An EAP-Response/ID is carried in the first Authentication frame. The EAP-Response/ID is encapsulated in multiple EAP elements.

Step-2,3: The AP extracts the FILS Authentication Message element and forwards it to Authentication Server (AS) and gets response from AS. The protocol between AP and AS is out of this standard.

Step-4: The AP sends the second Authentication frame in which an EAP-Request message is carried in one or multiple EAP elements. The EAP-Request message starts an EAP method to make mutual authentication. The first EAPoL-Key message of 4-way handshake is also carried in another one or multiple EAP elements.

Step-5 is optional. For some EAP method, more steps are needed before the non-AP STA sends the last EAP-Response message to AP. All the additional EAP-Request and EAP-Response messages are carried in additional Authentication frames.

Setp-6: Before the non-AP STA sends the last EAP-Response message to the AP, the non-AP must can calculate the MSK, so the PMK it can get also. Since the non-AP STA has got ANonce at step 4, it can calculate PTK with ANonce and itself nonce SNonce. Before step-6, the non-AP STA and the AP change the state from State 1 to State 2.

Step-7: The non-AP sends the Association Request frame carrying the last EAP-Response message. The EAP-Response message is encapsulated in one or multiple EAP elements. The second EAPoL-Key message of 4-way handshake is also carried in the Association Request frame and encapsulated in one or multiple EAP elements.

The non-AP STA must includes a MIC element described in 8.4.2.121 to protect the whole frame.

Step-8: AP caches MSDU MIC before PTK is available.

Step9,10,11: The AP exchanges with AS for the last steps of EAP method. After the successful EAP authentication, the AS must get MSK, and the AS must send the PMK to the AP with the EAP success information.

Step 12: AP verifies MSDU MIC once PTK is calculated based on PMK received from AS and ANonce and SNonce.

Step-13: The AP sends Association Response frame to the non-AP STA. An EAP-Success or EAP-Failure message must be carried in the frame by encapsulating the message in one or multiple EAP elements. The third EAPoL-Key message of 4-way handshake must be carried in the frame and encapsulated in one or multiple EAP elements. The AP must includes a MIC element in the frame to protect the frame.

Step-14: The non-AP STA verifies the MIC of the Association Response. If OK, it installs the PTK, GTK, IGTK.

Step-15: Once the AP receives the ACK of the Association Response frame and the EAP procedure is successful, it installs the PTK of the non-AP STA.

**10.3.x.2 EAP-RP based authentication**

This subclause describes the FILS procedures using EAP-RP based authentication. The states used in this description are defined in 10.3.1 (General). Figure 10-ai1 assumes that a full EAP authentication is performed and the FILS context (which consists of rRK, rIK, EMSK) is setup at the STA as described in section 10.3.x.1



**Figure 10-ai1—Call flow for FILS using EAP-RP**

Figure 10-ai describes the steps required for FILS

* Step-1: STA obtains the ANonce from the AP by passive or active scan.
* An AP with dot11MgmtOptionFILSActivated set to true sends ANonce either through beacon or Probe Response as described below:
	+ the AP shall send ANonce in the Probe Response.
	+ the AP may send ANonce in the beacon.
* Step-2: The STA shall generate SEQ & compute rMSK as specified in [IETF RFC 5295] and [IETF RFC 5296].
* Step-3: The STA shall generate SNonce. In addition the STA shall derive PTK using ANonce, SNonce & rMSK.
* Step-4: The STA sends Association Request Frame. The STA shall include EAP elements for each of the following as defined below
	+ ‘EAP-Re-auth-Initiate’ shall be included in EAP elements with the EAP Message Type set to 1 (FILS Authentication Message). The encoding of EAP-Re-auth-Initiate shall follow the requirements specified in [IETF RFC 5296].
	+ SNonce and ANonce shall be included in EAP elements with the EAP Message Type set to 2 (FILS Key Exchange Message)
* Step-5: The AP extracts the FILS Authentication Message element and forwards it to Authentication Server (AS)
* Step-6: AS verifies Authentication Tag and derives rMSK as specified in in [IETF RFC 5295] and [IETF RFC 5296].
* Step-7: AS sends EAP-Finish/Re-Auth including rMSK to the AP
* Step-8: The AP shall derive PTK using ANonce, SNonce & rMSK
* Step-8a: The AP shall decrypt the Upper Layer message for IP address assignment Request if it was encrypted by the STA.
* Step-10: The AP shall generate GTK if needed as defined in section 11.6 of this specification
* Step-12: The AP sends Association Response Frame. The AP shall include EAP elements in the Association Response Frame for each of the following as defined below
	+ EAP-Finish/Re-Auth obtained from AS shall be included in EAP elements with the EAP Message Type set to 1 (FILS Authentication Message). The encoding of EAP-Finish/Re-Auth shall follow the requirements specified in [IETF RFC 5296].
	+ EAPOL-Key message shall be included in EAP elements with the EAP Message Type set to 2 (FILS Key Exchange Message)
* Step-13: Upon successful sending of Association Response Frame, the AP shall enter state-4 with the STA. The AP shall also install the keys as specified in section 11 of this specification.
* Step-14: Upon successful reception of Association Response Frame with successful authentication, EAPOL-Key, the STA shall enter state-4 with the AP. If the authentication fails, the STA shall consider the FILS context invalid. The STA may perform EAP authentication to re-setup the FILS context.