IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PQC Protocol Definitions | | | | |
| Date: 2025-07-07 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This document proposes text to define PQC protocols for the PQC TG.

*Instruct the editor to modify table 9-62 as indicated:*

**Table 9-62—Beacon frame body**

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| 94 | EBCS TIM | The EBCS TIM is present if dot11EBCSSupportActivated is true, dot11EBCSTIMInBeaconActivated is true, and one or more BUs for an EBCS traffic stream for which dot11EBCSTrafficStreamBuffered is true are buffered, otherwise not present. |
| <ANA1> | PQC Key Selector | The PQC Key Selector is present within Beacon frames when certain PQC algorithms are advertised in the RSNE. |
| Last – 1 | Vendor Specific | One or more Vendor Specific elements are optionally present. |
| Last | MME | The MME is present if dot11BeaconProtectionEnabled is true at the AP. |

*Instruct the editor to modify Tables 9-70 and 9-71 in 9.3.3.11 as indicated:*

**Table 9-70—Authentication frame body**

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| 27 | Tunneled PASN | A Tunneled PASN element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| <ANA2> | PQC Key | A PQC Key element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| <ANA2>+1 | PQC Commit | A PQC Commit element is present only in certain Authenticaiton frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| <ANA2>+2 | Ciphertext | A ciphertext element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| <ANA2>+3 | PQC Key Selector | A PQC Key Selector element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| <ANA2>+4 | PQC Signature | A PQC Signature element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| Last-1 | Vendor Specific | One or more Vendor Specific elements are optionally present |
| Last | MIC | A MIC element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |

**Table 9-71—Presence of fields and elements in Authentication frames**

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication algorithm** | **Authentication transaction sequence number** | **Status code** | **Presence of fields and elements indicated as conditional in Table 9-70 (Authentication frame body)** |
| PASN Authentication | 3 | Status | PASN Parameters element is present if Status Code  field is 0.  Wrapped data element is present if wrapped data  format in PASN Parameters element is nonzero and not  reserved; and Status Code field is 0.  MIC element is present.  Fragment element may be present if any of the  elements are fragmented and Status Code field is 0. |
| PQC No Sig Authentication | 1 | Any | The Ciphertext element is present. The PQC Key Selector element is present. |
| PQC No Sig Authentication | 2 | Any | The Ciphertext element is present if the Status Code field is zero. |
| PQC Digital Signature | 1 | Any | The PQC Key element is present. The Session element is present. |
| PQC Digital Signature | 2 | Any | The Ciphertext element is present. The Session element is present. |
| PQC Digital Signature | 3 | Any | The PQC Certificate element is present. The Session element is present. |
| PQC Digital Signature | 4 | Any | The PQC Certificate element is present if the status is zero. The Session element is present. |
| PQC Digital Signature | 5 | Any | The PQC Signature element is present. The Session element is present. |
| PQC Digital Signature | 6 | Any | The PQC Signature element is present if the status is zero. The Session element is present. |
| PQC PAKE | 1 | Any | The Ciphertext element is present. The Password Identifier element is present. The Session element is present. |
| PQC PAKE | 2 | Any | The Session element is present. |
| PQC PAKE | 3 | Any | The PQC Commit element is present. The Session element is present. |
| PQC PAKE | 4 | Any | The Ciphertext element is present. The MIC element is present. The Session element is present. |
| Opportunistic ML-KEM | 1 | Any | The PQC Key element is present. |
| Opportunistic ML-KEM | 2 | Any | The Ciphertext element is present if the Status Code is zero. |
| PQC PMK Caching | 1 | Any | The RSNE is present. |
| PQC PMK Caching | 2 | Any | The RSNE is present if the Status code is zero. |

*Instruct editor to modify section 9.4.1.1 as indicated:*

**9.4.1.1 Authentication Algorithm Number field**

The Authentication Algorithm Number field indicates a single authentication algorithm. (M118)(#4170)The

Authentication Algorithm Number field is shown in Figure 9-137 (Authentication Algorithm Number field

format). The following values are defined for authentication algorithm number:

Authentication algorithm number = 0: Open System

Authentication algorithm number = 2: Fast BSS Transition

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

Authentication algorithm number = 4: FILS Shared Key authentication without PFS

Authentication algorithm number = 5: FILS Shared Key authentication with PFS

Authentication algorithm number = 6: FILS Public Key authentication

Authentication algorithm number = 7: PASN authentication

Authentication algorithm number = <ANA3>: PQC signature authentication

Authentication algorithm number = <ANA4>; PQC non-signature authentication

Authentication algoirithm number = <ANA5>: PQC PAKE authentication

Authentication algorithm number = <ANA6>: PQC unauthenticated

Authentication algorithm number = <ANA7>: PQC PMK Caching

Authentication algorithm number = 65 535: vendor specific use

*Instruct the editor to modify Table 9-130 in section 9.4.2.1 as indicated:*

**Table 9-130—Element IDs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| Tunneled PASN (see 9.4.2.315 (Tunneled PASN element)) | 255 | 143 | Yes | No |
| PQC Key Selector | 255 | <ANA8> | Yes | Yes |
| PQC Key | 255 | <ANA9> | Yes | Yes |
| PQC Commit | 255 | <ANA10> | Yes | Yes |
| Ciphertext | 255 | <ANA11> | Yes | Yes |
| PQC Signature | 255 | <ANA12> | Yes | Yes |
| Reserved | 255 | <ANA12>+1-255 |  |  |

*Instruct the editor to modify Table 9-190 in section 9.4.2.23.3 as indicated:*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **OUI** | **Suite Type** | **Authentication Type** | **Key management type** | **Key derivation type** | **Authentication algorithm numbers (see 9.4.1.1 (Authentication Algorithm Number field))** | **Cipher suite selector restriction** |
| 00-0F-AC | 25 | FT authentication over SAE | FT key management defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm specified in 12.4.2 (Assumptions on SAE) | 3 (SAE) for FT Initial Mobility Domain Association 2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol)  0 (open) for FT Initial Mobility Domain Association over PMKSA caching | none |
| 00-0F-AC | <ANA13> | PQC Auth With No Signature | PQC Mutual Auth defined in 12.7.1.3 (Pairwise Key Heirachy) | Defined in 12.7.1.6.2 (Key Derivation function (KDF)) using HKDF | <ANA4> for PQC mutual authentication  without signatures | None |
| 00-0F-AC | <ANA14> | PQC Digital Signature | PQC Mutual Auth defined in 12.7.1.3 (Pairwise Key Hierarchy) | Defined in 12.7.1.6.2 (Key Derivation (KDF)) using HKDF | <ANA3> for PQC mutual authentication using ML-DSA | Used only with 00-0F-AC:9 (GCMP-256) |
| 00-0F-AC | <ANA15> | PQC PAKE | PQC Mutual Auth defined in 12.7.1.3 (Pairwise Key Hierarchy) | Defined in 12.7.1.6.2 (Key Derivation (KDF)) using HKDF | <ANA5> for PQC mutual authentication using a password | None |
| 00-0F-AC | <ANA16> | Opportunistic ML-KEM | None | Defined in 12.7.1.6.2 (Key Derivation (KDF) using HKDF) | <ANA6> for PQC Unauthenticated | None |
| 00-0F-AC | <ANA17> | Authentication negotiated over IEEE Std 802.1X using a CNSA 2.0-compliant EAP method | RSNA Key management as defined in 12.7 | Defined in 12.7.1.6.2 (Key Derivation (KDF)) using HKDF | 0 (Open) | Used only with 00-0F-AC:9 (GCMP-256) |
| 00-0F-AC | <ANA17>+1-255 | Reserved | Reserved | Reserved | Reserved | Reserved |
| Other OUI or CID | Any | Vendor-specific | Vendor-Specific | Vendor-Specific | Vendor-Specific | Vendor-Specific |

*Instruct editor to modify table 9-277 in section 9.4.2.91 as indicated:*

**9.4.2.91 Advertisement Protocol element**

**Table 9-277—Advertisement protocol ID definitions**

|  |  |
| --- | --- |
| Name | Value |
| Access network query protocol (ANQP) | 0 |
| MIS Information Service | 1 |
| MIS Command and Event Services Capability Discovery | 2 |
| Emergency Alert System (EAS) | 3 |
| Registered location query protocol (RLQP) | 4 |
| PQC Key Query | 5 |
| Reserved | 6-220 |
| Vendor Specific | 221 |
| Reserved | 222-255 |

*Instruct the editor to modify section 9.4.2.178 as indicated:*

**9.4.2.178 Session element**

The Session element is used to convey the (unique) identifier of an in-progress authentication protocol session. The format of the Session element is shown in Figure 9-749 ( Session element format).

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | Session |

Octets 1 1 1 variable

**Figure 9-749— Session element format**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1. For FILS, the Session field is 8 octets and chosen randomly by the non-AP STA. For PQC protocols, the Session field is a variable length.

*Instruct editor to modify section 9.4.2.188 as indicated:*

**9.4.2.188 Nonce element**

The Nonce element is used for exchanging an additional source of randomness in authentication exchanges. The format of the Nonce element is shown in Figure 9-769 (Nonce element format).

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | Nonce |

Octets 1 1 1 16

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1. The Nonce field contains randomly generated data.

*Instruct the editor to create new sections 9.4.2.2.U, 9.4.2.2.V, 9.4.2.W, 9.4.2.X, 9.4.2.Y, and 9.4.2.Z including new figures, as indicated:*

**9.4.2.U PQC Key Selector element**

The PQC Key Selector element contains a hash of a public key used in a PQC algorithm. The algorithm definition determines the hash function used to compute the hash. See figure 9-ABCD (PQC Key Selector element format).

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | Key Selector |

Octets: 1 1 1 variable

**Figure 9-ABCD—Key Selector element format**

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

The Key Selector contains a hash of a PQC Key. The definition of the PQC algorithm determines the hash function used to compute the hash and therefore the length of the Key Selector field.

**9.4.2.V PQC Key element**

The PQC Key element contains a public key used in a PQC algorithm. See Figure 9-LMNO (PQC Key element format). This element contains public keys for key establishment.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | PQC Parameter Set | Length of PQC Key | PQC Key |

Octets: 1 1 1 1 2 variable

**Figure 9-LMNO—PQC Key element format**

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

The PQC Parameter Set is an 8-bit unsigned integer that maps an identifying number to a parameter set defining the algorithm. The following values are defined for PQC Parameter Set:

PQC Parameter Set = 0: Reserved

PQC Parameter Set = 1: ML-KEM-512

PQC Parameter Set = 2: ML-KEM-768

PQC Parameter Set = 3: ML-KEM-1024

PQC Parameter Set 4-254: Reserved

PQC Parameter Set 255: Vendor Specific

The Length of Public Key indicates the length in octets of the public key that follows. Some PQC public keys can be too large to fit in a single element and in many cases too large to fit in a single frame. Therefore, these elements will necessarily require fragmentation and reassembly.

The PQC field is a public key from the indicated PQC Parameter Set whose length depends on the PQC Parameter set.

**9.4.2.W PQC Commit**

The PQC Commit element contains the information a STA sends to an AP when committing to a guess of a password in the PQC PAKE exchange. See Figure 9-PQRS (PQC Commit).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | PQC Parameter Set | Random Commit | Encoded public key |

Octets: 1 1 1 1 96 variable

**Figure 9-PQRS—PQC Commit element format**

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

The PQC Parameter set indicates the parameter set of the encoded public key (see 9.4.2.V). The Random Commit is always 96 octets and the length of the encoded depends on the PQC Parameter Set of the encoded public key (see Table 12.Y in section 12.X.4).

**9.4.2.X Ciphertext element**

The Ciphertext element contains an encapsulated secret encrypted using the public key from a PQC key establishment algorithm. See Figure 9-WXYZ (Ciphertext element).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | Length of Ciphertext | Ciphertext |

Octets: 1 1 1 2 variable

**Figure 9-WXYZ—Ciphertext element format**

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

The Length of Ciphertext indicates the length in octets of the ciphertext that follows. PQC ciphertexts are too large to fit in a single element and in some cases too large to fit in a single frame. Therefore, these elements will necessarily require fragmentation and reassembly (see 10.28.11 (Element fragmentation) and 10.28.12 (Element defragmentation)) and possibly encompass multiple frames.

The Ciphertext field contains a secret encrypted using a public key from a PQC key establishment algorithm. Its length depends on the PQC Parameter Set of the public key used for encapsulation.

**9.4.2.Y PQC Certificate element**

The PQC Certificate element contains an X.509 certificate which eontains a public key from a PQC digital signature algorithm. See Figure 9-PQRS (PQC Certificate format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | Length of Certificate | Certificate |

Octets: 1 1 1 2 variable

**Figure 9-PQRS—Ciphertext element format**

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

The Length of Certificate indicates the length in octets of the certificate that follows.

**9.4.2.Z PQC Signature element**

The PQC Signature element contains a digital signature from a PQC digital signature algorithm.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | PQC Parameter Set | Length of PQC Signature | PQC Signature |

Octets: 1 1 1 1 2 variable

**Figure 9-TUVW—PQC Signature element format**

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

The PQC Parameter Set is an 8-bit unsigned integer that maps an identifying number to a parameter set defining the algorithm. The following values are defined for PQC Parameter Set:

PQC Parameter Set = 0: Reserved

PQC Parameter Set = 1: ML-DSA-44

PQC Parameter Set = 2: ML-DSA-65

PQC Parameter Set = 3: ML-DSA-87

PQC Parameter Set 4-254: Reserved

PQC Parameter Set 255: Vendor Specific

The Length of PQC Signature indicates the length in octets of the signature that follows. PQC signatures are too large to fit in a single element and in many cases too large to fit in a single frame. Therefore, these elements will necessarily require fragmentation and reassembly.

The PQC Signature field is a singature generated by the indicated PQC Parameter Set whose length depends on the PQC Parameter set.

*Instruct the editor to create section 12.7.X*

**12.7.X Key Derivation and Proof-of-Possession for PQC Exchanges**

The 4-way handshake (12.7.6.4 (4-way handshake)) performs derivation of a PTK and proof-of-possession of the PMK between two peers for legacy, not PQC, protocols. PQC exchanges do PTK derivation and proof-of-possession using 802.11 Association request and Association response frames by computing a digest of the transcript of the PQC exchange and binding that to the keys derived from the key derivation function.

This digest is computed by hashing the body of each of the Authentication frames sent, in order, by each side where the body is defined as the Authentication algorithm number (inclusive) to the end of the frame. If an Authentication frame is fragmented (see section ???) the data hashed for a particular message (defined as all frames with a singular authentication algorithm number) shall be the body of each fragment of the message in the order in which they were received. The acknowledgement message sent by a peer to acknowledge receipt of a fragment shall not be included in the digest.

Upon successfully terminating, each PQC key exchange protocol shall generate a PMK, a PMKID, and a digest representing a hash of the transcript hash, T. This data is used to derive a PTK as

PTK = HKDF-expand(HKDF-extract(T, PMK), “IEEE 802.11 PQC PTK Derivation”, PTKLen)

Where:

PMK is the shared secret created as a result of running the PQC algorithm

T is a digest of the transcript from the PQC algorithm that generated the PMK

PTKLen is the length of the PTK from table X.Y

*Instruct the editor to create section 12.X*

**12.X PQC Key Exchanges**

The PQC Key Exchanges are performed between a non-AP STA and an AP to establish a PMKSA using ML-KEM. Five PQC exchanges are defined: one in which authentication is performed with a shared password, another in which authentication is performed with signatures, another employing a signature-less form of authentication using trusted ML-KEM keys, an unauthenticated key establishment exchange, and a PMK Caching indication. In addition, an exchange used to obtain a PQC key from a peer is defined.

There are trust assumptions made about the PQC exchanges which perform authentication. In the signature-less exchange it is assumed that the two peers possess each other’s trusted ML-KEM public encapsulation key. In the password authenticated key exchange (PAKE) it is assumed that the AP has a static ML-KEM encapsulation key which the non-AP STA trusts (or is willing to trust), and that the peers share a password or passphrase. In the signature exchange it is assumed that the two peers have a way of trusting each other’s signature public key (through, for instance, a certificate issued by a trusted third party). The manner in which trust is obtained is out of scope of the standard, with the exception of the AP’s static ML-KEM encapsulation key used in the PAKE which can be obtained using an action frame exchange described in section 12.X.1.

These exchanges use Authentication frames (9.3.3.11 Authentication frame format)) to perform the key exchange, except the PQC Key Query exchange which uses GAS frames.

Every PQC exchange that generates, or identifies, a PMK shall also generate a hash transcript of the messages sent that comprise the exchange.

The hash functions used in PQC exchanges depends on the parameter set used for key establishment as shown in table 12.X.

|  |  |
| --- | --- |
| **Parameter Set** | **Hash Algorithm** |
| ML-KEM-512 | SHA256 |
| ML-KEM-768 | SHA384 |
| ML-KEM-1024 | SHA512 |

**Table 12.X PQC Hash algorithms**

**12.X.1 PQC Key Query Exchange**

A STA may obtain a peer’s ML-KEM key using a GAS protocol exchange. The querying STA issues a GAS Initial Request frame indicating the PQC Key Query protocol in the Advertisement Protocol element. If the queried STA’s PQC Key can fit in a single frame, the queried STA responds with a GAS Initial Response frame with its key as the a PQC Key field of a PQC Key element (section 9.4.2.X). If the PQC Key is too large for a single frame the queried STA responds with GAS Comeback Response frame containing the first portion of the fragmented PQC key and the remainder of the fragmented key is obtained with GAS Comeback Requests and Responses.

Note—This exchange is unsecured and a querying STA has no reason to trust the integrity of a PQC key obtained with this exchange. In certain cases, though, a querying STA can gain trust in the key if, for instance, a queried STA is able to subsequently authenticate with a different credential.

**12.X.2 PQC Key Exchange without Signature**

The two peers in this exchange have obtained each other’s trusted public KEM encapsulation keys a priori in a manner outside the scope of this standard. The encapsulation keys used in this exchange do not need to be from the same parameter set. In the event that the encapsulation keys differ, the AP’s key will be used to determine the appropriate hash function to use. The AP includes a SHA256 hash of its KEM encapsulation key in the Key Selector field of a PQC Key Selector element in all beacons and probe responses. A non-AP STA determines which KEM encapsulation key to use with this exchange by checking which of its known and trusted KEM keys hash to the same value as that indicated in the PQC Key Selector element. A match identifies the AP’s encapsulation key.

The non-AP STA initiates this exchange by calling the KEM.Encaps() routine with the AP’s encapsulation key, *pkap*, generating a key, K1, and a ciphertext, c1 and then derives a secret:

(K1, c1) = KEM.Encaps(pkap)

ss = HKDF-Expand(HKDF-Extract(c1,K1), “IEEE 802.11 PQC NoSig Handshake Key”, 64)

It then computes a hash of its KEM encapsulation key and encrypts the resulting digest with AES-SIV-512 using ss as the key. It then generates an Authentication frame with the Authentication algorithm set to <ANA4> and with transaction sequence number set to 1. It places c1 in the body of a Ciphertext element (see 9.4.2.Y (Ciphertext element)), and the ciphertext output of AES-SIV-512 into the PQC Key Selector field of a PQC Key Selector element. Finally, it transmits the frame to the AP.

**STA --> AP: c1, {H(pkap)}ss**

Upon receipt of the Authentication frame with Authentication algorithm set to <ANA4> and transaction sequence number set to 1, the AP extracts the ciphertext, c1’, from the Ciphertext element and calls the KEM.Decaps() routine with its decapsulation key, skap, to generate a key, K1’, and it a secret, ss:

K1’ = KEM.Decaps(c1’, skap)

ss = HKDF-Expand(HKDF-Extract(c1’, K1’), “IEEE 802.11 PQC NoSig Handshake Key”, 64)

It then passes the data in the PQC Key Selector field of the PQC Key Selector element to AES-SIV-512 with ss as the key. If decryption fails, the exchange fails. Otherwise, the AP determines which KEM encapsulation key in its database of trusted KEM encapsulation keys has a hash digest that matches the plaintext output from AES-SIV-512. If none is found, the exchange fails. Otherwise, the AP then calls the KEM.Encaps() routine with the non-AP STA’s encapsulation key, *pksta*, generating a key, K2, and a ciphertext, c2.

(K2, c2) = KEM.Encaps(pksta)

This is transmitted to the non-AP STA in an Authentication frame with transaction sequence number set to 2 and c2 in the body of a Ciphertext element (9.4.2.Y (Ciphertext element)).

**STA <-- AP: c2**

The AP then generates shared secret PMK and a PMKID using HKDF and H with a hash algorithm from table 12.X for its public key:

PMK = HKDF-expand(HKDF-extract(c1’ | c2, K1’ | K2), “IEEE 802.11 PQC NoSig Secret”, 32)

PMKID = Truncate-128(H(c1’ | c2))

It then generates a transcript digest, T, consisting of a hash of the body of Authentication frame 1 from the Authentication algorithm number (inclusive) to the end of the frame followed by the body of Authentication frame 2 from the Authentication algorithm number (inclusive) to the end of the frame using the hash algorithm from table 12.X with the AP’s public key.

Upon receipt of Authentication frame with transaction sequence number 2, the non-AP STA extracts the ciphertext, c2’, from the Ciphertext element and calls the KEM.Decaps() with its decapsulation key, sksta, and c2’, generating a key K2’:

K2’ = KEM.Decaps(c2’, sksta)

The non-AP STA then generates shared secret PMK and a PMKID using HKDF and H with a hash algorithm from table 12.X for the AP’s public key:

PMK = HKDF-expand(HKDF-extract(c1 | c2’, K1 | K2’), “IEEE 802.11 PQC NoSig Secret”, 32)

PMKID = Truncate-128(H(c1 | c2’))

It then generates a transcript digest, T, in the same fashion as above.

**12.X.3 PQC Key Exchange with Digital Signature**

Authentication using digital signatures is accomplished by doing a KEM exchange do derive a shared secret and each peer signing context of the exchange with PQC digital signature algorithm to authenticate. It is assumed that the peers have a priori trust of each other’s digital signature key or have a way of obtaining such trust, such as use of a trusted third party which has signed certificates containing the peer’s signing key. Both sides maintain a static signature key and the STA generates an ephemeral key pair.

A non-AP STA initiates the PQC Digital Signature exchange by first generating its ephemeral keypair:

(skeph, pkeph) = KEM.KeyGen()

Then, it constructs an Authentication frame with the Authentication algorithm set to <ANA3>, the transaction sequence number set to 1, and a PQC Key element in the body of the frame. The parameter set of the key pair indicated in the PQC Parameter Set of the PQC Key Element, and the public key, pkeph, is the PQC Key field. The frame is transmitted to the AP.

**STA --> AP: pkeph**

Upon receipt of an Authentication frame with a transaction sequence number of 1, the AP checks the PQC Parameter set of the PQC Key element. If the parameter set not supported, the AP constructs an Authentication frame with the Authentication algorithm set to <ANA3>, and the status set to INVALID\_PUBLIC\_KEY. The frame is transmitted to the non-AP STA and the exchange fails. If the parameter set is supported, the AP extracts the public key, pk, from the PQC Key field and generates a key and ciphertext and a session identifier, sid:

(K, c) = KEM.Encaps(pkeph)

sid = rand()

The AP then derives secrets as:

bk = HKDF-Extract(c, K))

ke = HKDF-Expand(bk, “IEEE 802.11 PQC Sig Handshake Key”, 64)

km = HKDF-Expand(bk, “IEEE 802.11 PQC Sig Mac Key”, n)

where n is the length of the digest output by the hash algorithm from table 12-X.

The AP then constructs an Authentication frame with Authentication algorithm set to <ANA3>, the transaction sequence number set to 2, and a Session element and a Ciphertext element in the body of the frame. The ciphertext c is copied into the Ciphertext field of the Ciphertext element and the sid is encrypted using AES-SIV-512 with ke as the key and the entire Ciphertext element as the sole component of AAD. The output of AES-SIV-512 encryption is copied to the Session field of the Session element. The frame is transmitted to the non-AP STA.

**STA <-- AP: c, session({sid}ke)**

Upon receipt of an Authentication frame with a transaction sequence number of 2, the non-AP STA extracts the ciphertext, c, from the Ciphertext field of the Ciphertext element and generates a key using its ephemeral private key:

K = KEM.Decaps(c, sk)

The non-AP STA then derives secrets as:

bk = HKDF-Extract(c, K))

ke = HKDF-Expand(bk, “IEEE 802.11 PQC Sig Handshake Key”, 64)

km = HKDF-Expand(bk, “IEEE 802.11 PQC Sig Mac Key”, n)

where n is the length of the digest output by the hash algorithm from table 12-X. The non-AP STA then decrypts the Session field of the Session element using AES-SIV-512 with ke as the key and the entire Ciphertext element as a single component of AAD. If decryption is unsuccessful, the exchange fails, otherwise the non-AP STA retains sid as the session identifier.

The non-AP STA then constructs an Authentication frame with Authentication algorithm set to <ANA3>, the transaction sequence number set to 3, and a PQC Certificate element in the body of the frame. It then encrypts its certificate using AES-SIV-512 with ke and no AAD and places the resulting output into the Certificate field and sets the length to be the length of the ciphertext received from AES-SIV-512. The non-AP STA sends the frame to the AP.

**STA --> AP: certificate({certsta}ke)**

Upon receipt of an Authentication frame with transaction sequence number of 3, the AP constructs an Authentication frame with Authentication algorithm set to <ANA3> and transaction sequence number set to 4. It then extracts the encrypted certificate from the Certificate field of the PQC Certificate element and passes it to AES-SIV-512 with ke. If decryption fails, the AP sets the status of the Authentication frame to REQUEST\_DECLINED and transmits the frame to the non-AP STA, the exchange fails. If decryption succeeds, the AP validates the non-AP STA’s certificate. If validation fails, the AP sets the status of the Authenticaiton frame to UNSUPPORTED\_AUTH\_ALGORITHM and transmits the frame to the non-AP STA, the exchange fails. If validation is successful, the AP adds a Session element and a PQC Certificate element to the body of the Authentication frame, places the concatenation of the two session ids, sidi followe by sidr, into the Session field of the Session element and then encrypts its own certificate using AES-SIV-512 with ke placing the output in the Certificate field. The AP transmits the frame to the non-AP STA.

**STA <-- AP: certificate({certap}ke)**

Upon receipt of an Authentication frame with transaction sequence number of 4, the non-AP STA extracts the encrypted certificate from the Certificate field of the PQC Certificate element and passes it to AES-SIV-512 with ke. If decryption fails, the exchange fails. If decryption is successful, the STA validates the AP’s certificate. If validation is fails the exchange fails. If validation is successful, the non-AP STA produces a keyed digest using km:

stadig = HMAC(km, pkeph | c | sid | cert-STA)

where HMAC() is instantiated with the hash algorithm from 12.X and the parameter set of the STA’s ephemeral key and then digital signature, sigsta, using its private static signature key, ssigsta, over the digest:

stasig = Signature(ssigsta, stadig, “IEEE 802.11 PQC Signature”)

where Signature() is the call to the digital signature algorithm. The non-AP STA then constructs an Authentication frame with Authentication algorithm set to <ANA3>, transaction sequence number set to 5, and a PQC Signature element in the body of the frame. The non-AP STA copies sigsta into the Signature field of the PQC Signature element and transmits the frame to the AP.

**STA --> AP: signature(sigsta)**

Upon receipt of an Authentication frame wth transaction sequence number 5, the AP constructs an Authentication frame with Authentication algorithm set to <ANA3> and transaction sequence number set to 6. It then extracts the non-AP STA’s signed data, stadata, from the Signature field of the PQC Signature algorithm and verifies the signature by reconstructing the digest with HMAC and the hash algorithm from table 12-X, and then a using the non-AP STA’s public key from its certificate, pksta, to check the signature:

stadig = HMAC(km, pkeph | c | sid | cert-STA)

good-sta = Verify(pksta, stadig, stadata, “IEEE 802.11 PQC Signature”)

where Verify() is the call to the verification algorithm for the particular digital signature algorithm. If good-sta is false, the AP sets the status of the Authentication frame to FILS\_AUTHENTICATION\_FAILURE. If good-sta is true, the AP produces a digest, apdig, with HMAC and the hash algorithm from table 12-X, and a digital signature, sigap, as follows:

apdig = HMAC(km, c | pksta | sid | cert-AP)

sigap = Signature(ssigap, apdig, “IEEE 802.11 PQC Signature”)

where Signature() is the call to the digital signature algorithm with its static signature key ssigap. The AP puts a PQC Signature element in the body of the Authentication frame and copies sigap into the Signature field. The frame is transmitted to the non-AP STA. The exchange succeeds for the AP.

**STA <-- AP: signature(sigap)**

Upon receipt of an Authentication frame with transaction sequence number 6, the non-AP STA extracts the signature, sigap, from the Signature field of the PQC Signature element and verifies the signature by reconstructing the digest with HMAC and the hash algorithm from table 12-X, and using the AP’s public key from its certificate, pkap, to check the signature:

apdig = HMAC(km, c | pk | sidi | sidr | cert-AP)

good-ap = Verify(pkap, apdig, apdata, “IEEE 802.11 PQC Signature”)

where Verify() is the call to the verification algorithm for the particular digital signature algorithm. If good-ap is false, the exchange fails. Otherwise, the exchange succeeds for the STA.

If the exchange succeeds, the AP and non-AP STA generate a transcript digest by hashing of the body of each of Authentication frames 1 through 6, the body being defined as from the Authentication algorithm number (inclusive) to the end of the frame, using the hash algorithm from table 12.X. They then produce a PMK and PMKID as follows:

PMK = HKDF-Expand(sk, “IEEE 802.11 PQC Sig Auth Key”, 32)

PMKID = Truncate-128(H(pk | c))

**12.X.4 PQC Exchange with Password Authentication**

OQUAKE is used to perform password authentication with PQC (PQC PAKE). OQUAKE is a variant of the Encrypted Key Exchange and uses Kemeleon encodings to transform an ML-KEM encapsulation key into a random string prior to encipherment.

**12.X.4.1 Kemeleon**

The ML-KEM encapsulation key is a vector of polynomials, each with 256 coefficients, and a 32 octet random string, *rho*. Each coefficient is a 12 bit integer less than 3329. Before running the Kemeleon encoding, it is necessary to deserialize the vector of polynomials into an array of numbers. With n = 256, q = 3329, k from the ML-KEM parameter set, and t from table 12.Y, Kemeleon encode is:

KemeleonEncode(pk)

w | rho = pk

a = deserialize(w)

r = 0

b = log\_2(q^(k\*n))

for i from 1 to k\*n:

r += q^(i-1)\*a[i]

m = rand[0,...,floor((2^(b+t)-r)/(q^(k\*n)))]

r = r + m\*q^(k\*n)

z = r | rho

return z

|  |  |  |
| --- | --- | --- |
| **Parameter Set** | **Value of t** | **Size of encoded key** |
| ML-KEM-512 | 128 | 797 |
| ML-KEM-768 | 192 | 1180 |
| ML-KEM-1024 | 256 | 1562 |

**Table 12.Y—Kemeleon Security Parameter**

Encoded keys must be decoded and the decoded output must be serialized back into the form of a vector of polynomials and appended with rho in order to reconstruct the key. Using the same constants, Kemeleon decode is:

KemeleonDecode(z)

r | rho = z

r = r % q^(k\*n)

for i from 1 to k\*n:

a[i] = r % q

r = r / q

w = serialize(a)

pk = w | rho

return pk

**12.X.4.2 Privacy Exchange and PQPAKE**

Each AP that advertises the PQPAKE AKM shall also possess a static ML-KEM encapsulation key which STAs use to encrypt their identities to the AP. The AP that advertises the PQPAKE AKM shall include a SHA256 hash of its static ML-KEM encapsulation key in the Key Selector field of a PQC Key Selector element in all beacons and probe responses. A non-AP STA determines whether it knows the AP’s static ML-KEM encapsulation key by checking which of its known keys hash to the same value as indicated in the PQC Key Selector element.

STAs receive static encapsulation keys in a trusted manner outside of the scope of this specification. In addition, if a STA does not possess an AP’s static encapsulation key, evidenced by not recognizing a SHA256 hash of it in a beacon or probe response, the STA may use the exchange from 12.X.2 to request the AP’s key and tentatively trust it on first use, establishing full trust if the AP is able to complete the PQPAKE algorithm, the OPAQUE exchange.

A privacy-providing exchange precedes OQUAKE, the PQCPAKE exchange. In the privacy-providing exchange, the identifier associated with the password is sent encrypted in a request and an encrypted session identifier is sent in the response. The parameter set used to protect the identity exchange can differ from the parameter set used to perform OQUAKE and the messages comprising the privacy-providing exchange must be part of the resulting hashed transcript. Since the first two messages are sent before agreeing on the ML-KEM parameter set for OQUAKE, the hash algorithm used for transcript generation for the entire PQPAKE, including the privacy exchange, shall be SHA512 regardless of the parameter set used in the OQUAKE exchange.

A non-AP STA initiates the PQC PAKE by sending its encrypted identity to the AP. For all PQC Keys defined in section 9.4.2.X, the STA shall use AES-SIV-512 to encrypt its identity. The non-AP STA does this by first invoking ML-KEM.encaps() with the AP’s static encapsulation key to generate a secret k1 and a ciphertext c1. The STA then generates a key, ki:

ki = HKDF-Expand(HKDF-Extract(c1, k1), “802.11 PQC PAKE Identity Protection”, 64) (12-X-1)

For the purposes of preventing traffic analysis, the non-AP STA then pre-pends its identity with a single octet, whose value indicates the number of random octets (up to 255) that follow the single octet and precede the actual identity. If a STA chooses to add no additional padding then a single octet with value zero is pre-pended to its identity. The STA then constructs an Authentication frame with the Authentication algorithm set to <ANA5> and the transaction sequence number set to 1 containing a Ciphertext element with c1 in the Ciphertext field, and a Password Identifier element. The padded identity is passed to AES-SIV-512 with ki as the key and the vector of AAD consisting of one component, the Ciphertext element. The output of AES-SIV-512 is copied into the identifier field of the Password Identifier element. This frame is transmitted to the AP.

**STA --> AP: c1, pi({identity}ki)**

Upon receipt of an Authentication frame with sequence number set to 1, the AP extracts c1 from the Ciphertext element and passes it to ML-KEM.decaps() to produce secret K1. It then generates ki using equation 12-X-1 above and decrypts the identity in the Password Identifier element. The first octet is inspected and discarded along with the number of following octets indicated by the value of the first octet to reconstruct the STA identity. The password credential associated with this identity is looked up in dot11RSNAConfigPasswordValueTable. If there is no entry for that identity the AP may choose to abandon this exchange or it may, optionally, continue with a random password in order to prevent an attacker from querying the existance of identities in its configuration. If the AP does not abandon the exchange at this point it generates a random session identifier, sid, and encrypts sid using AES-SIV-512 and ki and no AAD. It constructs an Authentication frame with the Authentication algorithm set to <ANA5> and the transaction sequence number set to 2 with a Session element containing the encrypted sid in the Session field. This frame is transmitted to the non-AP STA.

**STA <-- AP: session({sid}ki)**

The AP generates a fullsid by appending the decrypted password identity to the sid:

fsid = sid | identity

Upon receipt of an Authentication frame with transaction sequence number 2, decrypts the encrypted sid with AES-SIV-512, and generates the full sid as above. It then generates a key pair, and encodes the public key to obtain a randomized string, z.

(sk, pk) = ML-Kem.KeyGen()

z = KemeleonEncode(pk)

OQUAKE uses a password, pwd, and several constants:

* A domain separation tag: DST = SHA256(“IEEE 802.11 PQC PAKE”)
* Length of a random number: RLEN = 96
* Length of an authenticating tag: NKC = 64
* Length of the output key: NKEY = 32

The STA then generates a random number, r of RLEN octets. The STA then computes T and s using HKDF with the hash algorithm described in table 12.X as follows:

t\_ikm = HKDF-Extract(pwd, DST | “OQUAKE” | fsid | r)

t\_pad = HKDF-Expand(t\_ikm, “t\_pad”, len(z))

T = z xor t\_pad

s\_ikm = HKDF-Extract(pwd, DST | “OQUAKE” | fsid | T)

s\_pad = HKDF-Expand(s\_ikm, “s\_pad”, RLEN)

s = r xor s\_pad

The STA then constructs an Authentication frame with the Authentication algorithm set to <ANA5>, the transaction sequence number set to 3, and a PQC Commit element in the body of the frame. It then copies s into the Random Commit field of the Commit element, sets the PQC Parameter set to the ML-KEM parameter set of the keypair created above, and copies T into the Encoded Public Key field.

**STA --> AP: s, T**

Upon receipt of an Authentication frame with transaction sequence number 3, the AP extracts inspects the PQC Parameter set in the PQC Commit element. If the value indicates a parameter set that is not acceptable, the exchange fails. Otherwise, s and T from the PQC Commit element and processes them as follows using the same OQUAKE constants as above:

s\_ikm = HKDF-Extract(pwd, DST | “OQUAKE” | fsid | T)

s\_pad = HKDF-Expand(s\_ikm, “s\_pad”, RLEN)

r = s xor s\_pad

t\_ikm = HKDF-Extract(pwd, DST | “OQUAKE” | fsid | r)

t\_pad = HKDF-Expand(t\_ikm, “t\_pad”, len(T))

z = T xor t\_pad

The randomized string z is then passed to KemeleonDecode to reconstruct the key pk. The AP generates a key and ciphertext as follows:

(K, c) = ML-KEM.Encaps(pk)

The AP generates a PMK, a tag, and a PMKID as follows:

(DNH: should c be added to the prk\_pmk calculations with K?)

prk\_pmk = HKDF-Extract(pwd, DST | "OQUAKE" | fsid | K)

PMK = HKDF-Expand(prk\_pmk, DST | "sk", NKEY)

tag = HKDF-Expand(prk\_pmk, DST | “confirm”, NKC)

PMKID = Truncate-128(H(s | T | tag | fsid)

The AP then generates an Authentication frame with the Authentication algorithm set to <ANA5> and the sequence number set to 4 and Ciphertext element followed by a MIC element in the body of the frame. It copies the tag to the MIC field of the MIC element, and the Ciphertext in the Ciphertext field of the Ciphertext Element. This frame is transmitted to the STA.

**STA <-- AP: c, mic**

The AP then generates a transcript digest by hashing of the body of each of Authentication frames 1 through 4, the body being defined as from the Authentication algorithm number (inclusive) to the end of the frame, using SHA512.

Upon receipt of an Authentication frame with sequence number of 4, the STA extracts the tag and ciphertext, c, from the frame and processes them as follows:

K = ML-KEM.Decaps(c, sk)

prk\_pmk = HKDF-Extract(pwd, DST | "OQUAKE" | fsid | K)

verify = HKDF-Expand(prk\_pmk, DST | “confirm”, NKC)

If verify differs from tag, the STA generates a random PMK:

x = rand()

PMK = HKDF-Expand(x, c, NKEY)

Otherwise it produces a PMK and PMKID as follows:

PMK = HKDF-Expand(prk\_pmk, DST | "sk", NKEY)

PMKID = Truncate-128(H(s | T | tag | fsid)

It then generates a transcript digest by hashing of the body of each of Authentication frames 1 through 4, the body being defined as from the Authentication algorithm number (inclusive) to the end of the frame, using SHA512.

**12.X.5 Opportunistic KEM**

The Opportunistic KEM exchange is performed between a STA and AP in order to create an unauthenticated PMKSA. This exchange establishes a shared secret suitable to generate keys for encryption but that secret is unauthenticated. This exchange is designed for cases where encryption is desired but access control is either not necessary or is handled outside of this standard.

The Opportunistic KEM exchange is a simple exchange of an KEM encapsulation key and a ciphertext. The STA initiates the exchange by generating a keypair:

(sk, pk) = KEM.KeyGen()

The STA then constructs an Authentication frame with the Authentication algorithm set to <ANA6> and with transaction sequence number set to 1, with a PQC Key Element with the parameter set of the key pair indicated in the PQC Parameter Set and pk in the PQC Key field. The STA transmits this frame to the AP.

Upon receipt of an Authentication frame with transaction sequence 1, the AP inspects the PQC Key Element. If the PQC Parameter Set is not acceptable the exchange fails. Otherwise, the AP extracts the encapsulation key from the PQC Key field and generates a key and a ciphertext:

(K, c) = Kem.Encaps(pk)

The AP constructs an Authentication frame with the Authentication algorithm set to <ANA6> and with transaction sequence number set to 2, with a Ciphertext element and c in the Ciphertext field. The AP transmits this frame to the STA. It then computes a transcript digest, T, consisting of a hash of the body of Authentication frame 1 from the Authentication algorithm number (inclusive) to the end of the frame followed by the body of Authentication frame 2 from the Authentication algorithm number (inclusive) to the end of the frame using the hash algorithm from table 12.X.

Upon receipt of an Authentication frame with transaction sequence 2, the STA extracts the ciphertext from the Ciphertext element and generates a key:

K = KEM.Decaps(sk, c)

It then computes a transcript digest, T, in the same fashion as the AP.

Both the STA and AP export their transcript digest T, and generate a PMK and a PMKID as:

PMK = HKDF-Expand(HKDF-Extract(c, K), “IEEE 802.11 Opportunistic KEM”, 32)

PMKID = Truncate-128(H(pk | c))

Where H() is the hash algorithm from table 12.X.

**12.X.6 PQC PMK Caching**

If a STA believes it shares a PMKSA with an AP it can query the AP to find out. This is accomplished by chosing a random 16 octet number, SNonce, and then constructing an Authentication frame with Authentication algorithm set to <ANA7> and transaction sequence number set to 1 and with an RSNE in the body of the frame containing the desired PMKID, or list of PMKIDs, and SNonce in the Nonce field of a Nonce element. This frame is transmitted to the AP.

Upon receipt of an Authentication frame with transaction sequence number of 1, the AP checks the PMKID(s) in the RSNE to see if it has any PMKSAs in its database of PMKSAs whose PMKIDs match those listed in the RSNE. The AP responds with an Authentication frame with Authentication algorithm set to <ANA7> and the transaction sequence number set to 2. If there was not match, the status set to STATUS\_INVALID\_PMKID. The frame is transmitted to the STA and the exchange fails. If the AP has a PMKID match, it generates a random 16 octet number, ANonce, and places the selected PMKID into an RSNE in the body of the frame, and ANonce in the Nonce field of the a Nonce element. This frame is transmitted to the STA. The AP then computes a transcript digest, T, consisting of a hash of the body of Authentication frame 1 from the Authentication algorithm number (inclusive) to the end of the frame followed by the body of Authentication frame 2 from the Authentication algorithm number (inclusive) to the end of the frame using the hash algorithm from table 12.X.

Upon receipt of an Authentiation frame with transaction sequence number of 2 and a zero status, the STA checks if the PMKID in the RSNE is one it sent in the first frame. If not, it abandons the exchange. If so, it computes a transcript digest, T, consisting of a hash of the body of Authentication frame 1 from the Authentication algorithm number (inclusive) to the end of the frame followed by the body of Authentication frame 2 from the Authentication algorithm number (inclusive) to the end of the frame using the hash algorithm from table 12.X.

Both the AP and STA export the PMK from the PMKSA identified by the PMKID and the transcript hash digest.

**References:**

FIPS 203 <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf>

FIPS 204 <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>