IEEE P802.11
Wireless LANs

|  |
| --- |
|  Post-Quantum Opportunistic Wireless Encryption specification |
| Date: 2025-07-24 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Alex LUNGU | Samsung Cambridge Solution Centre | OCS, CB4 0AE, U.K. | +44 1223 434600 | da.lungu@samsung.com |
| Mark RISON | Samsung Cambridge Solution Centre | OCS, CB4 0AE, U.K. | +44 1223 434600 | at samsung (a global commercial entity) I'm the letter emme then dot rison |

Abstract

This document proposes an extension to the currently existing opportunistic wireless encryption specification to adopt a post-quantum cryptographic algorithm.

### Editor: Modify Subclause 2. Normative references, as follows:

FIPS 197, Advanced Encryption Standard (AES).

FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard

### Editor: Modify Subclause 3.1 Definitions, as follows:

integration service: The service that enables delivery of medium access control (MAC) service data units

(MSDUs) between the distribution system (DS) and a local area network (LAN) (via a portal).

key-encapsulation mechanism (KEM): A set of three cryptographic algorithms (KeyGen, Encaps, and Decaps)

that can be used by two parties to establish a shared secret key over a public channel.

### Editor: Modify Subclause 3.4 Acronyms and abbreviations, as follows:

MLME MAC sublayer management entity

ML-KEM Module-Lattice-Based Key-Encapsulation Mechanism

### Editor: Modify Subclause 9.3.3.11 Authentication frame format, Table 9-70, as follows:

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 27  | Tunneled PASN | A Tunneled PASN element is present only in certain Authentication frames as defined in Table 9-71. |
| <ANAo> | KEM Encapsulation Key | A KEM Encapsulation Key element is present only in certain Authentication frames as defined in Table 9-71. |
| <ANAo+1> | KEM Ciphertext | A KEM Ciphertext element is present only in certain Authentication frames as defined in Table 9-71. |
| 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. |

### Editor: Modify Subclause 9.3.3.11 Authentication frame format, Table 9-71, as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication algorithm** | **Authentication transaction sequence number** | **Status Code** | **Presence of fields and elements indicated as conditional in Table 9-70** |
| 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. |
| ML-KEM Authentication | 1 | Status | KEM Encapsulation Key element is present. |
| ML-KEM Authentication | 2 | Status | KEM Ciphertext element is present if the Status Code field is 0; otherwise not present. |

### Editor: Modify Subclause 9.4.1.1 Authentication Algorithm Number field, as follows:

Authentication algorithm number = 7: PASN authentication

Authentication algorithm number = <ANAaan>: ML-KEM authentication

Authentication algorithm number = 65 535: vendor specific use

### Editor: Modify Subclause 9.4.2.1 General, Table 9-130, as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| Tunneled PASN (see 9.4.2.315) | 255 | 143 | Yes | No |
| KEM Encapsulation Key (see 9.4.2.xxx) | 255 | <ANAeid> | Yes | Yes |
| KEM Ciphertext (see 9.4.2.yyy) | 255 | <ANAeid+1> | Yes | Yes |
| Reserved | 255 | < ANAeid+2>-255 |  |  |

### Editor: Modify Subclause 9.4.2.23.3 AKM suites, table 9-190, as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **OUI** | **Suite type** | **Meaning** | **Authentication algorithm numbers (see 9.4.1.1)** | **Cipher suite selector restriction** |
| **Authentication type** | **Key management type** | **Key derivation type** |
| 00-0F-AC | 25 | FT authentication over SAE | FT key management defined in 12.7.1.6 | Defined in 12.7.1.6.2 using the hash algorithm specified in 12.4.2 | 3 (SAE) for FT Initial Mobility Domain Association2 (FT) for FT protocol reassociation as defined in 13.5 0 (open) for FT Initial Mobility Domain Association over PMKSA caching | None |
| 00-0F-AC | <ANAakm> | ML-KEM authentication using ML-KEM-512 parameter set | RSNA key management as defined in 12.7 | Defined in 12.14.XXX | <ANAaan> | Used only with cipher suite selector values 00-0F-AC:9 (GCMP-256), 00-0F-AC:10 (CCMP-256), 00-0F-AC:13 (BIP-CMAC-256), and 00-0F-AC:12 (BIP-GMAC-256) |
| 00-0F-AC | <ANAakm+1> | ML-KEM authentication using ML-KEM-768 parameter set | RSNA key management as defined in 12.7 | Defined in 12.14.XXX | <ANAaan> | Used only with cipher suite selector values 00-0F-AC:9 (GCMP-256), 00-0F-AC:10 (CCMP-256), 00-0F-AC:13 (BIP-CMAC-256), and 00-0F-AC:12 (BIP-GMAC-256) |
| 00-0F-AC | <ANAakm+2> | ML-KEM authentication using ML-KEM-1024 parameter set | RSNA key management as defined in 12.7 | Defined in 12.14.XXX | <ANAaan> | Used only with cipher suite selector values 00-0F-AC:9 (GCMP-256), 00-0F-AC:10 (CCMP-256), 00-0F-AC:13 (BIP-CMAC-256), and 00-0F-AC:12 (BIP-GMAC-256) |
| 00-0F-AC | <ANAakm+3>-255 | Reserved | Reserved | Reserved | Reserved | Reserved |
| Other OUI or CID | Any | Vendor-specific | Vendor-specific | Vendor-specific | Vendor-specific | Vendor-specific |

### Editor: Add Subclause 9.4.1.xx, KEM Parameter Set field

The KEM Parameter Set field indicates a KEM parameter set. A KEM parameter set is used to select a trade-off between security and efficiency. The following values are defined for the KEM Parameter Set field:

KEM Parameter Set = 1: ML-KEM-512

KEM Parameter Set = 2: ML-KEM-768

KEM Parameter Set = 3: ML-KEM-1024

KEM Parameter Set = 255: Vendor Specific

All other values of the KEM Parameter Set field are reserved. The KEM Parameter Set field is shown in Figure 9-XXX.

|  |
| --- |
| KEM Parameter Set |
| 1 |

Octets:

Figure 9-XXX -- KEM Parameter Set field format

### Editor: Add Subclause 9.4.2.xxx, KEM Encapsulation Key element, as follows:

The KEM Encapsulation Key element contains the encapsulation (public) key used in a key encapsulation mechanism. The format of the KEM Encapsulation Key element is shown in Figure 9-YYY.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | KEM Parameter Set | KEM Encapsulation Key |
| 1 | 1 | 1 | 1 | Variable |

Octets:

Figure 9-YYY -- KEM Encapsulation Key element format

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

The KEM Parameter Set field is defined in Figure 9-XXX, and indicates the parameter set used by the KEM and the size of the KEM encapsulation key, as shown in Table 9-XXX.

Table 9-XXX KEM encapsulation key size

|  |  |
| --- | --- |
| **KEM parameter set** | **KEM encapsulation key size (octets)** |
| ML-KEM-512 | 800 |
| ML-KEM-768 | 1184 |
| ML-KEM-1024 | 1568 |

The KEM Encapsulation Key field contains the KEM encapsulation key.

### Editor: Add Subclause 9.4.2.yyy, KEM Ciphertext element, as follows:

The KEM Ciphertext element contains the ciphertext used in a key encapsulation mechanism. The format of the KEM Ciphertext element is shown in Figure 9-ZZZ.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | KEM Parameter Set | KEM Ciphertext |
| 1 | 1 | 1 | 2 | Variable |

Octets:

Figure 9-ZZZ -- KEM Ciphertext element format

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

The KEM Parameter Set field is defined in Figure 9-XXX, and indicates the parameter set used by the KEM and the size of the KEM ciphertext, as shown in Table 9-YYY.

Table 9-YYY KEM ciphertext size

|  |  |
| --- | --- |
| **KEM parameter set** | **KEM ciphertext size (octets)** |
| ML-KEM-512 | 768 |
| ML-KEM-768 | 1088 |
| ML-KEM-1024 | 1568 |

The KEM Ciphertext field contains the KEM ciphertext.

### Editor: Modify Subclause 12.14.1 General, as follows:

The Opportunistic Wireless Encryption handshake is executed between a non-AP STA and an AP to establish a

PMKSA using either a simple Diffie-Hellman key exchange or an ML-KEM exchange. The handshake does not provide true authentication of the non-AP STA or AP but does enable encryption. This handshake is designed for cases in which access control is either not necessary or can be handled outside of this standard.

NOTE—An AP can support opportunistic wireless encryption both using a Diffie-Hellman exchange and using an ML-KEM exchange.

### Editor: Modify Subclause 12.14.2 Opportunistic Wireless Encryption, as follows:

12.14.2 Classical cryptography Opportunistic Wireless Encryption ~~exchange~~ using a Diffie-Hellman exchange.

The classical cryptography Opportunistic Wireless Encryption (OWE) exchange using a Diffie-Hellman exchange occurs during association of a non-AP STA and an AP that indicate ~~the OWE~~ AKM suite selector 00-0F-AC:18 (9.4.2.23.3) by placing a Diffie-Hellman Parameter element in the (Re)Association Request and Response frames, respectively.

### Editor: Add Subclause 12.14.XXX, Post-quantum cryptography Opportunistic Wireless Encryption using an ML-KEM exchange, as follows:

An AP signals support for post-quantum cryptography opportunistic wireless encryption using an ML-KEM exchange by advertising an ML-KEM AKM suite selector (9.4.2.23.3).

The ML-KEM exchange occurs during the authentication of a non-AP STA and an AP, prior to (re)association. ML-KEM is standardized under NIST’s FIPS 203.

The non-AP STA first chooses the highest parameter set it supports from the parameter sets advertised by the AP using ML-KEM AKM suite selectors. Using that parameter set, the non-AP STA runs the key generation algorithm and obtains an encapsulation key (ek) and a decapsulation key (dk):

(ek, dk) = ML-KEM.KeyGen()

The decapsulation key shall remain private to the non-AP STA, while the parameter set and encapsulation key shall be sent to the AP in a KEM Encapsulation Key element. The size of the decapsulation and encapsulation keys depends on the parameter set chosen by the non-AP STA.

NOTE—Given the size of the KEM encapsulation key the KEM Encapsulation Key element has to be fragmented.

The non-AP STA shall then send an Authentication frame with authentication transaction sequence number set to 1, authentication algorithm number set to <ANAaan> and a KEM Encapsulation Key element containing the chosen parameter set and ek.

Upon receiving an Authentication frame with authentication algorithm number set to <ANAaan>, the AP shall determine a processing status as follows:

1. If the authentication transaction sequence number is not equal to 1, the processing status shall be set to TRANSACTION\_SEQUENCE\_ERROR.
2. Otherwise, if the size of the encapsulation key does not match parameter set expectations, the processing status shall be set to STATUS\_INVALID\_ELEMENT.
3. Otherwise, if the encapsulation key does not pass the modulus check (see FIPS 203), the processing status shall be set to INVALID\_PARAMETERS.
4. Otherwise, the processing status shall be set to SUCCESS.

If the processing status is SUCCESS, the AP shall run the encapsulation algorithm using the ek it received from the non-AP STA to generate its copy of the shared secret (K) and a ciphertext (c):

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

The AP shall then send an Authentication frame with authentication transaction sequence number set to 2, authentication algorithm number set to <ANAaan> and the status code set to the processing status. If the status code is SUCCESS, the AP shall include a KEM Ciphertext element containing the parameter set chosen by the non-AP STA and c.

NOTE—Given the size of the KEM ciphertext the KEM Ciphertext element has to be fragmented.

Upon receiving an Authentication frame with authentication algorithm number set to <ANAaan>, the non-AP STA shall:

1. Validate that the authentication transaction sequence number is equal to 2. Otherwise the non-AP STA shall silently discard the frame and stop processing.
2. Validate that the size of the ciphertext matches parameter set expectations. Otherwise the non-AP STA shall silently discard the frame and stop processing.

If all validation is successful the non-AP STA shall run the decapsulation algorithm using dk and c to generate its copy of the shared secret (K’):

(K’) = ML-KEM.Decaps(dk, c)

All parameter sets defined for the KEM Parameter Set field derive a shared secret key size of 32 octets, which shall be used as the PMK.

NOTE—There is a marginal posibility that K ≠ K’ (1 in 2138 or lower). In that case the PMK held by the non-AP STA and the PMK held by the AP will differ and establishing the RSNA will fail.

**References:**

[NIST’s FIPS 203](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf)