Quantum-Resistant Cipher Suites for EDHOC

draft-selander-lake-pq-suites-01

Göran Selander, John Preuß Mattsson
Ericsson AB

IETF 124, LAKE WG, Montreal, Nov 06, 2024

Making EDHOC Quantum-Resistant

- Quantum-resistance means replacing ECC with PQC.
- EDHOC uses ECC for ephemeral key exchange, static DH authentication, and signature authentication.
- NIST has finalized standardization of three new quantum-resistant algorithms. ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205).
- All standardized PQC algorithms are signatures or KEMs.
- PQC signatures, such as ML-DSA are drop-in replacement for signature algorithms such as ECDSA.
- PQC KEMs, such as ML-KEM are drop-in replacement for ephemeral key exchange algorithms such as ECDHE.
- PQC KEMs cannot be used for authentication in methods 1—3 (Static DH), which require a DH/NIKE interface. Supporting PQC KEMs for authentication requires a new EDHOC method.

Value	Initiator Authentication Key	Responder Authentication Key	Requires DH/NIKE
0	Signature Key	Signature Key	No
1	Signature Key	Static DH Key	Yes
2	Static DH Key	Signature Key	Yes
3	Static DH Key	Static DH Key	Yes
4	PSK	PSK	No

Using KEMs for EDHOC Key Exchange

Section 3 specifies how to use KEMs for EDHOC Key Exchange:

— The ephemeral KEM encapsulation key ek is transported in the G_X field in message_1.

— The KEM ciphertext c is transported in the G_Y field in message_2.

— G_XY is the shared secret key K.

```
Initiator                                                     Responder
|                  METHOD, SUITES_I, G_X, C_I, EAD_1                  |
+-------------------------------------------------------------------->|
|                              message_1                              |
|                                                                     |
|       G_Y, Enc( C_R, ID_CRED_R, Signature_or_MAC_2, EAD_2 )         |
|<--------------------------------------------------------------------+
|                              message_2                              |
```

— message_2 = G_Y_CIPHERTEXT_2 thus becomes concatenation of the KEM ciphertext and CIPHERTEXT_2. The length of the former is known from the selected cipher suite in SUITES_I.

IANA Updates

EDHOC Method Type Registry:

Value	Initiator Authentication Key	Responder Authentication Key	Requires DH/NIKE
0	Signature Key	Signature Key	No
1	Signature Key	Static DH Key	Yes
2	Static DH Key	Signature Key	Yes
3	Static DH Key	Static DH Key	Yes

EDHOC Cipher Suites Registry:

Value	Description	Supports DH/NIKE
0	AES-CCM-16-64-128, SHA-256, 8, X25519, EdDSA, AES-CCM-16-64-128, SHA-256	Yes
1	AES-CCM-16-128-128, SHA-256, 16, X25519, EdDSA, AES-CCM-16-64-128, SHA-256	Yes
2	AES-CCM-16-64-128, SHA-256, 8, P-256, ES256, AES-CCM-16-64-128, SHA-256	Yes
3	AES-CCM-16-128-128, SHA-256, 16, P-256, ES256, AES-CCM-16-64-128, SHA-256	Yes
4	ChaCha20/Poly1305, SHA-256, 16, X25519, EdDSA, ChaCha20/Poly1305, SHA-256	Yes
5	ChaCha20/Poly1305, SHA-256, 16, P-256, ES256, ChaCha20/Poly1305, SHA-256	Yes
6	A128GCM, SHA-256, 16, X25519, ES256, A128GCM, SHA-256	Yes
24	A256GCM, SHA-384, 16, P-384, ES384, A256GCM, SHA-384	Yes
25	ChaCha20/Poly1305, SHAKE256, 16, X448, EdDSA, ChaCha20/Poly1305, SHAKE256	Yes
TBD1	AES-CCM-16-128-128, SHAKE256, 16, **MLKEM512, ML-DSA-44**, AES-CCM-16-64-128, SHA-256	No
TBD2	A256GCM, SHAKE256, 16, **MLKEM512, ML-DSA-44**, A256GCM, SHA-256	No