Post-Quantum (PQ) EDHOC Design Team (DT)

LAKE Interim Meeting
26-May-2026

Outline

1. DT: Introduction and Objectives (Renzo, 2 min)
2. Objective 1 : Scenarios (Lidia, 15 min)
3. Objective 2 : PQ cipher suites recommendation (Renzo, 2 min)
4. Objective 3 : KEM-based authentication methods (Renzo, 1 min)
5. Objective 4 : Statement for CFRG on LAKE requirements (Renzo, 2 min)

DT Members and Work

John Mattsson
Lidia Pocero Fraile
Christos Koulamas
Shujaatali Badami
Blumenthal, Uri
Clement Papon
Rafael Marin Lopez
Vaishnavi Sundararajan
Renzo Navas
Mališa Vučinić
Johann Großschädl
Muhammad Usama Sardar
Göran Selander

Five Weekly 1h Meetings

- Wednesdays 16h00-17h00 UTC
  - 22,29 April; 6,13,20 May
- Minutes and a Shared Folder
- Lots of discussion based on inputs provided by Lidia Pocero Fraile (Thank you Lidia!)

DT Objectives

1. The definition of a set of deployment scenarios where PQ-EDHOC is realistically deployable

2. A recommendation on standardizing PQC cipher suites for EDHOC methods 0 (SIG-SIG) and 4 (PSK)

3. A recommendation on standardizing new KEM-based authentication methods, satisfying the deployment scenarios defined in (1)

4. A statement for CFRG on LAKE requirements, potentially including the deployment scenarios from (1), for the standardization of “lightweight” PQC algorithms

Objective 1 (Lidia, 15 min)

The definition of a set of deployment scenarios where PQ-EDHOC is realistically deployable

Approach: Estimate the performance and resource impact of the proposed post-quantum (PQ) methods using constrained-environment classifications from draft-ietf-iotops-7228bis-07

1. C-Class → memory constraints (RAM/flash)
2. S-Class → link-layer MTU constraints
3. B-Class → effective link bitrates

Feasibility and Performance Evaluation:

- Memory: feasibility of PQ crypto fitting in memory of constrained platforms
- Computational cost (processing time)
- Communication cost (handshake TX/RX time)

Objective 1: Methodology

PQC EDHOC Methods Evaluated

- **Signature** → EDHOC method 0 with PQC KEM key exchange and **PQC signatures authentication** (RFC 9528 + draft-spm-lake-pqsuites)
- **PSK** → draft-ietf-lake-edhoc-psk + draft-spm-lake-pqsuites (PQC KEM key exchange and **PSK authentication)**
- **KEM** → method 5 from draft-pocero-lake-authkem-edhoc PQC KEM key exchange and PQC **KEM-based authentication**
- **NIKE** → EDHOC method 3 with **PQ NIKE** key exchange and **authentication**

Common Assumptions

- Both parties authenticate using the same method
- Credentials used for mutual authentication are provided by reference

PQC Algorithms

- **NIST-standardized algorithms** and algorithms selected for standardization → excluding HQC and SLH-DSA due to their large message and key sizes
- **Second-round NIST PQC signature** candidates → only SIG algorithms providing lower EDHOC handshake footprint than ML-DSA-44 f
- **High-potential compact PQC schemes** → including DAWN-β-512 KEM alternative and dCTIDH-2048-205 NIKE scheme

Data Source:

- **Processing time and memory usage** data are primarily obtained from pqm4 benchmarks on Cortex-M4 platforms.
  - Except for: SQ-sign, DAWN-β-512 and dCTIDH-2048-205
    - Cortex-M4 benchmarks for these algorithms are not yet available; benchmarks are taken for higher-performance platforms
- The **artifact sizes** (keys, signatures, and ciphertexts) used to estimate EDHOC message sizes are taken from the corresponding NIST PQC submission specifications and from DAWN-β-512 and dCTIDH-2048-205 specifications.

Objective 1: Memory footprint (C - class)

	Mutual Authentication	Key Exchange	PQC Memory footprint [KiB]			PQC Memory footprint [%inClass]		
Authe Type	Algorithm-Imp.	Algorithm-Imp.	pk+sk	FLASH	RAM	Min Class	FLASH-C	RAM-C
KEM	ML-KEM-512 clean*	ML-KEM-512 clean*	2,38	5,0	9,3	C1	7,4%	93,4%
Signature	ML-DSA-44-ref*	ML-KEM-512 clean*	3,78	13,0	50,8	C3	1,7%	50,8%
Signature	FNDS-512-ref*	ML-KEM-512 clean*	2,13	105,7	41,1	C2	43,1%	82,3%
PSK	PSK	ML-KEM-512 clean*	0,00	5,0	9,3	C1	5,0%	93,4%
Signature	SNOVA-24-5-16-4-esk*	ML-KEM-512 clean*	36,98	55,9	115,7	C4	4,6%	11,6%
Signature	SNOVA-24-5-16-4-ssk*	ML-KEM-512 clean*	1,04	55,9	165,5	C4	2,8%	16,5%
Signature	MAYO1-ref*	ML-KEM-512 clean*	1,41	34,3	209,7	C4	1,8%	21,0%
Signature	HAWK512-ref*	ML-KEM-512 clean*	2,50	104,6	9,3	C4	5,4%	0,9%
Signature	ov-Ip*	ML-KEM-512 clean*	504,23	26,8	12,4	C3	53,1%	12,4%
Signature	ov-Ip-pkc*	ML-KEM-512 clean*	274,88	27,1	277,2	C4	15,1%	27,7%
Signature	ov-Ip-pkc-skc*	ML-KEM-512 clean*	73,93	27,1	277,2	C4	5,1%	27,7%
KEM	ML-KEM-512 m4fstack*	ML-KEM-512 m4fstack*	2,38	13,0	2,3	C1	15,4%	22,9%
Signature	ML-DSA-44-m4fstack*	ML-KEM-512 m4fstack*	3,78	37,3	5,0	C2	16,4%	9,9%
PSK	PSK	ML-KEM-512 m4fstack*	0,00	13,0	2,3	C1	13,0%	22,9%
Signature	ov-Ip-pkcm4fstack*	ML-KEM-512 m4fstack*	274,88	99,5	6,4	C3	37,4%	6,4%
Signature	ov-Ip-pkc-skcm4fstack*	ML-KEM-512 m4fstack*	73,93	99,5	237,4	C4	8,7%	23,7%

	Metric PQC Memory Footprint
KEM	1KEMkeygen+1KEMenc+2KEMdec
FLASH	Text+Data
RAM	data+bss+STACKmax
SIG STACKmax	max(KEMkeygen,KEMenc,KEMdec, sign,verify)
PSK STACKmax	max(KEMkeygen,KEMenc,KEMdec)
KEM STACK max	max(KEMkeygen,KEMenc,KEMdec)
Min Class	Minimum Class that can fix it
FLASH/RAM-C	Percentage of memory in the fixit class*

* Assuming the authentication key is stored in non-volatile memory (FLASH).

	RAM [KiB]	ROM[KiB]
C1	10	100
C2	50	250
C3	100	1000
C4	1000	2000

- Minimum supported class: **C1** → **PSK** and **KEM methods** with ML-KEM-512
- Minimum supported class: **C2** → **Signature-based methods** with ML-KEM-512 and ML-DSA-44
- Minimum supported class: **C3/C4** → **Signature-based methods** with ML-KEM-512 and compact NIST PQC signature candidates

Objective 1: Link-layer MTU constraints (S - class)

	Mutual Authentication	Key Exchange	Message Size [B]						MIN S	Total No. of Fragments in Handshake				
Authe Type	Algorithm-Imp.	Algorithm-Imp.	m1	m2	m3	m4	m5	TOTAL	without frag	S1	S2	S3	S4	S10
KEM	ML-KEM-512 clean*	ML-KEM-512 clean*	806	776	786	779	17	3164	S4	35	17	9	5	5
Signature	ML-DSA-44-ref*	ML-KEM-512 clean*	806	3.199	2.438			6443	S13	67	30	13	6	6
Signature	FNDS-512-ref*	ML-KEM-512 clean*	806	1.445	684			2935	S12	32	15	7	4	4
PSK	PSK	ML-KEM-512 clean*	806	772	4			1582	S3	18	9	3	3	3
Signature	SNOVA-24-5-16-4-esk*	ML-KEM-512 clean*	806	1.026	265			2097	S4	23	11	5	3	3
Signature	SNOVA-24-5-16-4-ssk*	ML-KEM-512 clean*	806	1.026	265			2097	S4	23	11	5	3	3
Signature	MAYO1-ref*	ML-KEM-512 clean*	806	1.100	339			2245	S4	25	11	6	3	3
Signature	HAWK512-ref*	ML-KEM-512 clean*	806	1.334	573			2713	S11	29	13	7	4	4
Signature	ov-Ip*	ML-KEM-512 clean*	806	906	144			1856	S4	21	10	5	3	3
Signature	ov-Ip-pkc*	ML-KEM-512 clean*	806	906	144			1856	S4	21	10	5	3	3
Signature	ov-Ip-pkc*	ML-KEM-512 clean*	806	906	144			1856	S4	21	10	5	3	3
Signature	SQ-Sign **	ML-KEM-512 clean*	806	926	164			1896	S4	21	10	5	3	3
KEM	DAWN-β-512 **	DAWN-β-512 **	520	458	465	579	17	2039	S4	16	13	6	5	5
PSK	PSK	DAWN-β-512 **	520	454	4			978	S3	12	7	3	3	3
NIKE	dCTIDH-2048-205**	dCTIDH-2048-205**	262	273	21			556	S3	7	5	3	3	3

	Field Sizes
EAD	0
SUIT	1
Method	1
C	1
ID_CRED	4
MAC	9
AEAD	8

	6lowpan fragmentation	
Class	L2 MTU size	max. payload
S0	12	not practical
S1	127	99
S2	255	227
S3	575	547
S4	1279	1251
S10	1280	1252

CoAP POST/ACK Overhead	12

$$N_{frames} = \sum_{\{i=1\}}^{\{N_{messages}\}} \lceil \left(\frac{m_i + CoAP\ ov}{Payload\ in\ S} \right) \rceil$$

$$if\ m_i > 1282B\ \ then\ CoAP\ ov = \lceil m_i/1024B \rceil * 12B$$

- **MIN S:** Minimum S-class for which no 6LoWPAN fragmentation is required.
- For a “MIN S” class, number of fragments equals number of messages
- For a lower S-class than the “MIN S”, number of fragments increases

But how does this impact time-on-air?

Objective 1: Handshake Time: Processing Time@20 MHz + Time-on-Air over S-Type and B-Type Networks

			Proc.Time for PQC Op. at 20 MHz	Total Handshake Time (estimated) [s]									
				S1-B2			S2-B2			S1-B1		S4-B2	
	Mutual Authentication	Key Exchange		Z wave plus	IEEE 802.15.4	BLE			BLE			NB-IoT	LT-CATM1
Authe Type	Algorithm-Imp.	Algorithm-Imp.	[Sec]	10^4	2.5x10^5	10^6	10^4	10^5	10^6	10^1	10^2	10^5	10^6
KEM	ML-KEM-512 clean*	ML-KEM-512 clean*	0,307	3,81	0,45	0,34	3,81	0,66	0,34	3503,51	350,63	0,58	0,33
Signature	ML-DSA-44-ref*	ML-KEM-512 clean*	1,147	8,15	1,43	1,22	8,15	1,85	1,21	7001,15	701,15	1,69	1,20
Signature	FNDS-512-ref*	ML-KEM-512 clean*	5,174	8,41	5,30	5,21	8,41	5,50	5,20	3236,37	328,29	5,42	5,20
PSK	PSK	ML-KEM-512 clean*	0,109	1,88	0,18	0,13	1,88	0,29	0,12	1769,7	177,07	0,25	0,12
Signature	SNOVA-24-5-16-4-esk*	ML-KEM-512 clean*	22,919	25,23	23,01	22,94	25,23	23,15	22,94	2336,52	254,28	23,10	22,94
Signature	SNOVA-24-5-16-4-ssk*	ML-KEM-512 clean*	26,403	28,72	26,50	26,43	28,72	26,63	26,42	2340,00	257,76	26,58	26,42
Signature	MAYO1-ref*	ML-KEM-512 clean*	5,040	7,52	5,14	5,06	7,52	5,29	5,06	2489,84	253,52	5,23	5,06
Signature	HAWK512-ref*	ML-KEM-512 clean*	0,475	3,45	0,59	0,50	3,45	0,77	0,50	2974,88	297,92	0,71	0,50
Signature	ov-Ip*	ML-KEM-512 clean*	0,939	3,01	1,02	0,96	3,01	1,15	0,96	2068,94	207,74	1,10	0,95
Signature	ov-Ip-pkc*	ML-KEM-512 clean*	2,000	4,07	2,08	2,02	4,07	2,21	2,02	2070,00	208,80	2,16	2,02
Signature	ov-Ip-pkc*	ML-KEM-512 clean*	25,597	27,66	25,68	25,62	27,66	25,80	25,61	2093,60	232,40	25,76	25,61
Signature	SQ-Sign **	ML-KEM-512 clean*	31,758	33,86	31,84	31,78	33,86	31,97	31,78	2131,76	241,76	31,92	31,77
KEM	DAWN-β-512 **	DAWN-β-512 **	0,019	2,12	0,10	0,04	2,12	0,23	0,04	2101,62	210,18	0,20	0,04
PSK	PSK	DAWN-β-512 **	0,008	1,14	0,05	0,02	1,14	0,12	0,02	1128,01	112,81	0,10	0,02
NIKE	dCTIDH-2048-205**	dCTIDH-2048-205**	286,062	286,72	286,09	286,07	286,72	286,13	286,07	944,46	351,90	286,12	286,07

The Fastest
Second-Fastest

Blue: t < 0.5 s

Class	PHY bit rate (bit/s)
B0	< 10
B1	10-1000
B2	1000-1000000
B3	> 1000000

- **PSK → Overall fastest**
- **Runner-up** depends on the **bitrate:**
  - 10^2 – 10^4 bit/s → **Signature** Auth (ov-Ip)
  - 10^4 – 10^5 bit/s → **Signature** Auth(HAWK)
  - >10^5 bit/s → **KEM-based** Auth

- **KEM-based** methods → Lower processing time, larger message sizes
- **Signature-based** methods with **compact** NIST PQC **schemes** → Higher processing time, smaller message sizes
- **NIKE → lowest message sizes**, largest processing time

Objective 1: Main Observations

- **PSK and KEM-based authentication** with ML-KEM-512 provide the lowest memory overhead, remaining feasible even for **Class C1** devices.
- **PSK authentication** achieves the lowest processing time, followed by **KEM-based authentication** (both when ML-KEM-512 is used).
- **Signature-based authentication** using compact NIST PQC candidates r**educes network overhead**, but requires significantly higher memory resources, typically from **Class C3/C4** devices**.**
- **The total handshake time,** including communication and processing costs, shows that:
  - **KEM-based authentication** with ML-KEM-512 is faster for link bitrates above 10^5 bit/s (e.g., B2-S1/S2 classes).
  - **Signature-based methods** using compact schemes such as OV and HAWK become faster at lower bitrates below 10^5 bit/s (e.g., B1-S1 and lower-end B2-S1/S2 scenarios)**.**
- **NIKE-based authentication** with dCTIDH-2048-205 achieves the lowest network overhead, but at the cost of very high processing time.
  - Interesting for powerful devices with constrained links (low S and B classes)
- **Under extremely constrained links** near the **S1/B0-B1** regime (~10 bit/s), communication overhead dominates the total handshake time for all schemes, making even the very slow dCTIDH-2048-205 NIKE-based approach a competitive option.

Objective 1: Proposed Scenarios

- The three authentication approaches **PSK, KEM-based,** and **signature-based** authentication should be considered, as they address different constrained-environment requirements.
- **PSK authentication** with ML-KEM-512 can operate on the most constrained Class C1 devices while also achieving the lowest handshake time**.** However, it is limited to scenarios where a PSK can be securely provisioned beforehand.
- For non-PSK environments:
  - **KEM-based** authentication with ML-KEM-512 can operate on the same **C1** constrained devices and achieves lower total handshake times than signature-based methods for higher-bitrate links (e.g., upper end of the **B2** class).
  - **Signature-based** authentication using compact PQC schemes significantly reduces network overhead and can achieve lower total handshake times in highly constrained low-bitrate networks (**B1** and lower end of **B2**). However, requires classes **C3/C4**.
- Lower B1 physical-layer bitrates (or effective bitrates in technologies such as LoRaWAN) significantly increase time on air, potentially becoming prohibitive and motivating the need for more compact PQC schemes.
- Based on the current state of open-source implementations

Feasible Auth type	S1/S2 B2 (10^3-10^4 bit/s)	From S1/S2/ B2/B3 (from 10^5 bit/s)	From S3/S4 B2/B3 (from 10^5 bit/s)
C1/C2	**PSK and KEM**	**PSK and KEM**	**PSK, KEM and SIG (ML-DSA)**
C3/C4	**PSK, KEM and SIG (T_KEM > T_Signature)** **@ f<250 MHz**	**PSK, KEM and SIG (T_Signature > T_KEM)** **@ f<250 MHz**	

Objective 2 (Renzo, 2 min)

A recommendation on standardizing PQC cipher suites for EDHOC methods 0 (SIG-SIG) and 4 (PSK)

- We conclude that https://datatracker.ietf.org/doc/draft-spm-lake-pqsuites/ provides the foundation, we suggest adopting it as a WG Item
- Include Method 4 (PSK, IANA TBD defined in draft-ietf-lake-edhoc-psk)
- Draft-spm-lake-pqsuites specifies:
  - Clarifies that EDHOC with Signature and PSK authentication works with KEM key exchange and specified the content of G_X and G_Y
  - Updates the Registry to identify methods that require DH/NIKE
  - Updates the Registry to identify cipher suites that that support DH/NIKE
  - Registers cipher suites based on currently registered and planned COSE algorithms. This includes a cipher suites using CNSA 2.0 algorithms as requested by EDHOC users on the mailing list

Objective 3 (Renzo, 1 min)

A recommendation on standardizing new KEM-based authentication methods, satisfying the deployment scenarios defined in Objective 1

The DT States:

- Unanimous consensus to recommend standardising a KEM-KEM solution
- We can recommend to adopt KEM-KEM from draft-pocero-authkem-edhoc
  - Standalone: https://datatracker.ietf.org/doc/draft-pocero-lake-authkem-edhoc/
- We need further discussion for mixed methods

Objective 4 (1 min)

A statement for CFRG on LAKE requirements, potentially including the deployment scenarios from Obj 1, for the standardization of “lightweight” PQC algorithms

- **Under extremely constrained links** near the **S1/B0-B1** regime (~10 bit/s), time on air dominates the total handshake time for all schemes. Compact PQC schemes become essential
  - PSK-based, Signature-based and KEM-based authentication methods rely on a KEM. Standardizing more compact KEMs is important.
  - NIKE-based authentication approaches with low overhead become a competitive option, even if very slow in processing time
  - Compact PQC signature schemes significantly reduce network overhead and can achieve lower total handshake times. Standardizing more compact PQC signatures is important

Follow-Up of DT

- DT agrees to continue discussions bi-weekly until Vienna
- Open points
  - Standardize mixed authentication methods?
  - Objective 4

Discussion