OpenSSL CONFERENCE

Open Quantum Safe: Post-Quantum software research in the era of the first standards

History, current work, what's next

Rodrigo Martín Sánchez-Ledesma · Chair, OQS Technical Steering Committee · Senior Cryptography Researcher, Indra

13.10.2026

About me

OpenSSL CONFERENCE

- **Chair of the OQS Technical Steering Committee**
- **Maintainer of oqs-provider:** the OpenSSL 3 & 4 provider for post-quantum algorithms
- **Senior Cryptography Researcher at Indra:** PhD candidate in lattice-based cryptography

A show of hands

OpenSSL CONFERENCE

- **1.** Who's heard of OQS before today?

A show of hands

OpenSSL CONFERENCE

- **1.** Who's heard of OQS before today?
- **2.** Who's used it at some point?

A show of hands

OpenSSL CONFERENCE

- **1.** Who's heard of OQS before today?
- **2.** Who's used it at some point?
- **3.** Who continues to use it nowadays?

What OQS is

OpenSSL CONFERENCE

- **liboqs:** C library of quantum-safe KEMs & signatures. Common API, test harness, benchmarking.
- **Part of PQCA:** Supported by the Post-Quantum Cryptography Alliance, Linux Foundation
- **Academic first:** Founded by Douglas Stebila & Michele Mosca, University of Waterloo
- **Integrations:** oqs-provider (OpenSSL 3 & 4), demos, wrappers: C++, Go, Java, Python, Rust

OQS is one of four PQCA projects

PQ Code Package

High-assurance, production-ready implementations, starting with ML-KEM — mlkem-native, mldsa-native

Longfellow

Zero-knowledge protocols for legacy identity standards: ISO MDOC, JWT, W3 Verifiable Credentials

CBOMkit

Cryptographic Bill of Materials tooling, donated by IBM Research — finds quantum-vulnerable crypto in the wild

Same alliance, different jobs: OQS tests algorithms, PQ Code Package hardens them, Longfellow and CBOMkit tackle what's next to them.

The ground shifted

OpenSSL CONFERENCE

- **The first standards are final:** ML-KEM, ML-DSA and SLH-DSA (FIPS 203, 204, 205) — with more standardization efforts under way
- **OpenSSL ships it:** Version ≥ 3.5 implements all three natively, in its default provider

- ***If the winners are standardized and shipping in OpenSSL — what is the role of OQS now?***

Four commitments

OpenSSL CONFERENCE

- 1. Focus on experimental algorithms and features
- 2. Keep supporting PQC research, in all of its forms
- 3. Keep the project trustworthy, and keep improving its organization
- 4. Deepen collaboration with OpenSSL and the wider open source community

01

Re-focusing on the experimental

What OQS prioritizes, now that the core is standardized

13.10.2026

We can keep pace with new schemes

OpenSSL CONFERENCE

- **On the standardization rounds' own clock:** New candidates integrated on that timescale
- **Upstream teams publish support:** CROSS, MAYO, mlkem-native, mldsa-native, MQOM, and more
- **Promotion is evidence-based:** PR-reviewed, requires time-in-tier — not a popularity contest

Sourcing – and pruning

OpenSSL CONFERENCE

- **Every algorithm is labeled:** Actively maintained · Best effort · No active maintenance
- **Inclusion follows the community:** algorithms are incorporated based on community interest and support
- **We remove what standards supersede:** e.g. SPHINCS+ removed in release 0.16.0 — SLH-DSA stays

- *Stated policy: OQS does not aim to pick winners. It's meant to help with research and prototyping.*

NIST on-ramp: round 3

- **ALREADY MERGED**
- UOV, MQOM, MAYO, SNOVA

- **BEING INTEGRATED NOW**
- SDitH, QR-UOV, FAEST, SQIsign
- Working with each submission team on the right inclusion path.

All of them will be in the next liboqs release (0.17.0), before the end of the year.

“

What would you – or your organization – want OQS to keep supporting, no matter what?

- Someone tell us:

02

Keep supporting research

Why a scheme designer still reaches for liboqs

13.10.2026

Research comes first, by governance.

OpenSSL CONFERENCE

- **Governance principle:** favor long-term research goals over short-term commercial interests
- **A broad community behind it:** AWS, Cisco, evolutionQ, IBM Research, Indra, Microsoft Research, SandboxAQ, softwareQ among others — 1,757 across OQS since August 2024

The research apparatus

Common API

Swap schemes without touching callers

KAT generation

Matches the format standardization submissions use

Benchmarking

Speed and memory harnesses, built in

Assurance tracking

Constant-time status and formal verification, per algorithm

Inclusion in protocols

Algorithms can be exercised inside real protocols: oqs-provider, demos

Standardized algorithms can also carry research

New implementations

Other platforms

Reduced code size

New capabilities

OQS wants the version that offers something new or experimental you can't find elsewhere.

03

Keeping the project trustworthy

Security hardening, vulnerability response, and the strain on maintainers

13.10.2026

A support-tier system

OpenSSL CONFERENCE

- Every algorithm sits in a support tier that states OQS's own support commitment for each algorithm.

- **TIER 1 — CORE:** ML-KEM. That's it.
- **TIER 2 — SUPPORTED:** FrodoKEM, HQC, ML-DSA, LMS, XMSS
- **TIER 3 — COMMUNITY:** BIKE, Classic McEliece, Kyber, NTRU, NTRU-Prime, CROSS, Falcon, MAYO, MQOM, SLH-DSA, SNOVA, UOV

- ***Tier 1 is one family. And the list moves, based on capacity and support.***

Trail of Bits is contributing directly

Threat model

A documented threat model (PR #2477)

Public-input fuzzing CI

New coverage for attacker-controlled input (PR #2478)

Mutation testing CI

Verifies the test suite catches injected bugs (PR #2479)

Vulnerabilities go back to scheme authors

Advisories without waiting on CVEs

Published as GitHub Security Advisories, not delayed by a CVE number

Direct line to submission teams

Rolling out now: scheme-level findings route straight to the team that designed it

Triage first

Sort before you fix — duplicates and known issues are a real share of the queue

The same trend, showing up in our queue

- **WHAT WE'RE SEEING**
- More AI-assisted pull requests, issues, and comments landing in liboqs and oqs-provider
- A non-negligible share is now low-quality — "AI slop" — the same pattern already hitting curl, the Linux kernel, and Node.js
- The real cost: a toll on response capacity that's already stretched thin

- **WHAT WE'RE DOING**
- CONTRIBUTING.md requires disclosing generative-AI use, and describing how it was used
- Trail of Bits-authored security guidance aimed at cutting invalid LLM reports (PR #2477)
- New fuzzing and mutation-testing CI, to catch issues before a human has to
- Disclosure in practice: reviewers ask directly, contributors answer by hand (PR #2520)

“

What’s worked for your project against AI-generated noise – and what should OQS try next?

- Someone tell us:

04

Collaborating with OpenSSL and open source

The provider model is the bridge — built to be built on

13.10.2026

A provider, not a fork

PQ + hybrid crypto

In stock OpenSSL ≥ 3, via the standard provider interface

TLS 1.3 key establishment

Including hybrid KEMs and DSAs

Both KEMs and DSAs

Consumed via EVP

Key persistence

X.509, encode/decode, PKCS#12

> Once OpenSSL's own provider implements an algorithm, oqs-provider steps aside for it — automatically.

- The behavior documented in oqs-provider's own README, effective OpenSSL ≥ 3.5.

The ask: formalize the split

OpenSSL CONFERENCE

- **OpenSSL owns the standardized core:** ML-KEM, ML-DSA, SLH-DSA — production-grade
- **OQS owns the experimental frontier:** On-ramp candidates, and hybrids OpenSSL doesn’t ship
- **Together: a shared test pipeline:** Interop and code-points for pre-standard schemes
- **Co-maintain the provider bridge:** The stable seam between the two

What can we do for you?

OpenSSL CONFERENCE

- **A place to test before you commit:** experimental algorithms and hybrids get proven out before selection
- **Coverage for users not on 3.5 yet:** oqs-provider keeps PQ access alive for everyone still on OpenSSL 3.0–3.4
- **Independent comparative data:** benchmarks across candidates and hybrids, under the same conditions
- **Tooling other projects can reuse:** wrappers for C++, Go, Java, Python and Rust
- **Findings that reach the scheme authors:** advisories published directly, without waiting for a CVE number. Another validation environment for submission's teams.

What can you do for OQS?

- **Feedback and review**
- Side-channel and constant-time hardening expertise
- Production-scale feedback on the provider API and use
- More eyes on the testing and quality work already under review

- **Hands-on approach**
- Help with implementation: optimized code, new platforms, new wrappers
- Bug fixes, and hands on open issues and pull requests
- Testing in your own stack, and reports of what breaks
- Reviews, including security and constant-time reviews
- Your use case, so it can set our priorities

Better together

OpenSSL CONFERENCE

- **The winners are standardized.** OpenSSL ships them. Good — that was always the goal.
- **OQS re-focused:** on what still needs a home: the long tail, and the research on-ramp.
- **The provider is the bridge.** Let's build on it.

- github.com/open-quantum-safe · openquantumsafe.org · pqca.org

Over to you

OpenSSL CONFERENCE

Used it before? What was it for?

Which algorithms, which integration, and did it do the job?

Over to you

OpenSSL CONFERENCE

Used it before? What was it for?

Which algorithms, which integration, and did it do the job?

Using it today? What for?

And what is still missing for you?

Over to you

OpenSSL CONFERENCE

Used it before? What was it for?

Which algorithms, which integration, and did it do the job?

Using it today? What for?

And what is still missing for you?

Stopped using it? Why?

What made you move on is the most useful thing you can tell us.

Before we close

OpenSSL CONFERENCE

What should OQS have that it doesn't today?

Algorithms, features, platforms, integrations.

Who wants to use OQS, and for what?

Your use case is what sets our priorities.

Scan the code to tell us what's working and what should change — it helps us prioritize what OQS works on next.

Audience poll: OQS priorities

Two minutes — results shared back with the OQS community

Thank you.

Questions, pushback, and volunteers all welcome.

Rodrigo Martín Sánchez-Ledesma
rodrma01@ucm.es or rmsanchezledesma@indra.es