OpenSSL CONFERENCE

FIPS 140-3 Meets PQC: The Compliance Gap Nobody Planned for

Chris Brych | OpenSSL Conference 2026

15.10.2026

FIPS 140-3 Meets PQC: The Compliance Gap Nobody Planned For

1 Overview of the Problem
2 Understanding the Compliance Gap
3 The Organizational Dilemma
4 Why Hybrid PQC Deployments Matter
5 Practical Framework For Navigating the Compliance Gap
6 Looking Forward

Problem



Architect

We need to prepare for post quantum threats

Why aren’t we deploying PQC today?



Procurement

Because procurement requirements may require the use of FIPS 140 validated modules

Problem



Securit
y

We need security and the threat won't wait for FIPS 140 validation

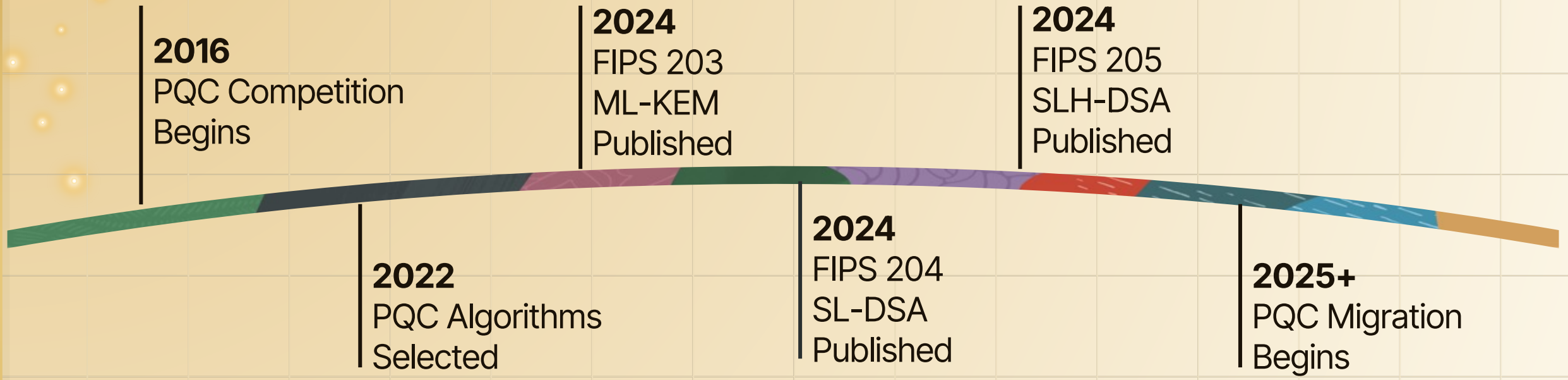


Compliance

Neither will the auditor as FIPS 140 is a requirement for procurement

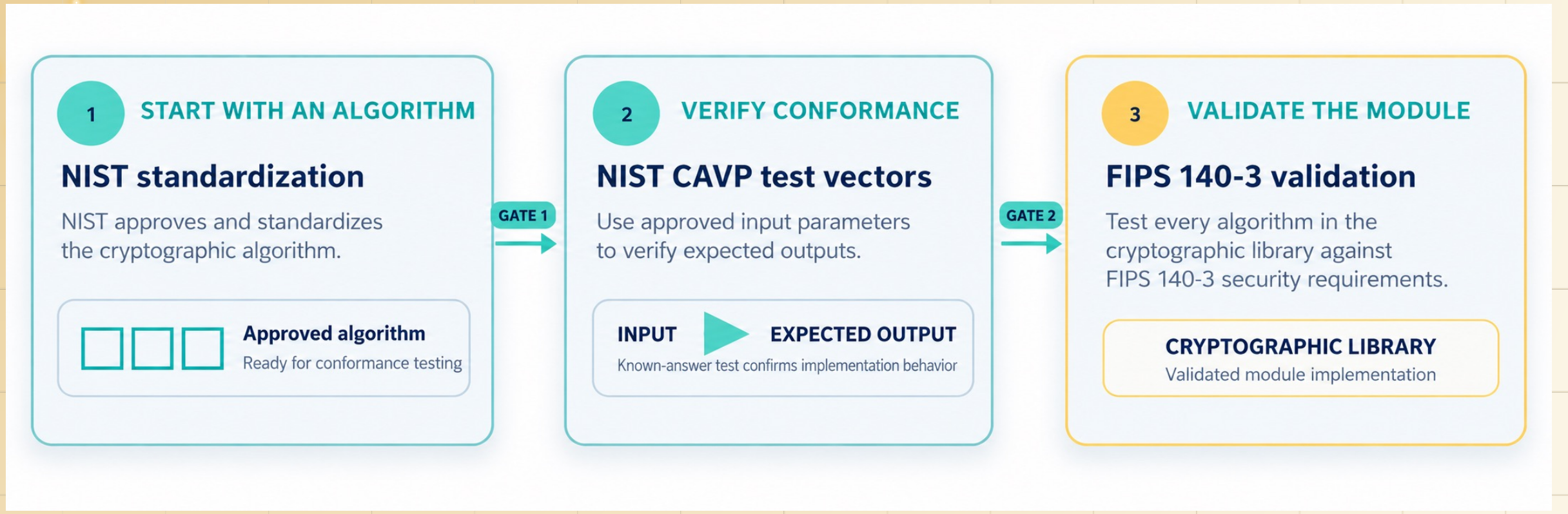
This is what we call the compliance gap

PQC Path to Standardization



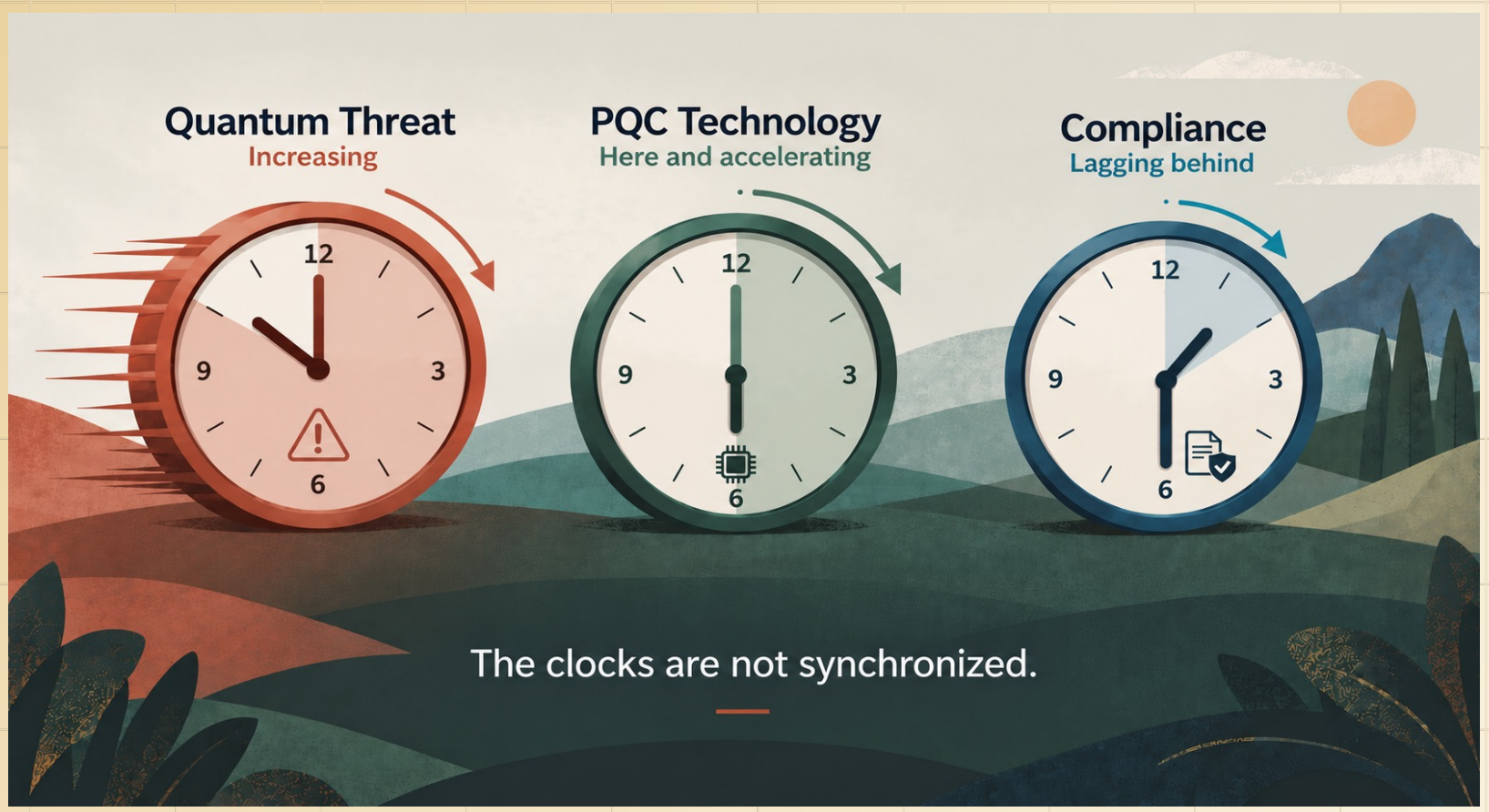
Source: NIST Post-Quantum Cryptography Project

Standardized ≠ Validated



Understanding the Compliance Gap

Understanding the Compliance Gap



Why is the Quantum Threat Increasing?

- Cryptographically relevant quantum computers are coming sooner than initially thought
- Long-lived data is already exposed to “harvest now, decrypt later” attacks
- Public key cryptography is deeply embedded
- Migration can require significant planning and implementation time
- Risk is to asymmetric cryptography only



How PQC Algorithms in OpenSSL Has Impacted Being PQC Ready

- Can help reduce integration effort
- Can facilitate faster ecosystem testing
- Can support practical migration approaches
- Vendor and platform enablement
- Can help improve crypto agility



How has Compliance Lagged Behind

- OpenSSL availability does **not** automatically make a deployment PQ-ready
  - Organizations therefore need to distinguish where they are at as part of the transition:

Capability	Meaning
PQC Ready	Can implement or test PQC or hybrid PQC algorithms
Production Ready	Meets performance, interoperability, and operational requirements
FIPS Ready	PQC functionality is supported within the validated scope of the OpenSSL FIPS Provider and its approved operating configuration

OpenSSL has helped facilitate PQC adoption by making PQC technology accessible in mainstream deployments. Vendors and organizations should evaluate PQC adoption in light of applicable security requirements, validation status, procurement obligations, and operational considerations

Security vs FIPS 140 Compliance

- Vendor products require agility
- Validation timelines and evolving security threats progress at different rates
- Locked in configurations with FIPS 140 validation may lead to false sense of security
- Product vendors must continue to update their FIPS 140 validations



The Organizational Dilemma

The Organizational Dilemma

OpenSSL CONFERENCE

Choosing an OpenSSL PQC strategy to meet all of your business needs

Option	Security	Compliance	Rationale
Stay Classical	Low	High	Least disruptive and easiest near-term audit story, but leaves growing exposure to “harvest now, decrypt later” threats
Go Full PQC	Higher	Higher	Strongest long-term cryptographic posture but could take time to fully implement across all applications and systems
Hybrid PQC	High	High	Combines classical and post-quantum cryptographic protection. FIPS 140-3 Standard now allows for hybrid PQ KEX

Real Deployment Scenarios

Federal Agency



- Requires FIPS 140 compliance
- Long-term confidentiality of data

Critical Infrastructure



- Requires operational stability
- Requires regulatory compliance

Financial Institution



- Requires risk reduction
- Auditability
- Security

What type of PQC strategy would you deploy today given these options?

a) Classical Approach

b) Full PQC Approach

c) Hybrid PQC Approach

The Audit Perspective

"Why didn't you use ML-KEM?"



Do you Know Where Your Cryptography is Used?

Locate



Have you Assessed the PQ Quantum Risk?

Assess



Is There a Migration Plan?

Plan



Are Exceptions Documented?

Record

Inventory → Risk Assessment → Migration Roadmap → Exception Governance

Documented Evidence Matters



Cryptographic Inventory



Migration Roadmap



Risk Assessment



Architecture Decisions



Exception Approvals

As long as you have a documented plan you will be better able to manage risk with your auditors

Why Hybrid PQC Deployments Matter

Why Hybrid PQC Deployments Matter

Why hybrid / staged migration matters

Reduce Transition Risk
Improve quantum resilience without unnecessary operational or security risk

Protect Sensitive Data
Mitigate “harvest now, decrypt later” exposure

Move Gradually
Support a phased migration path across systems and teams

Lower Interoperability Risk
Keep connected services working during cryptographic change



Defense in Depth
Layer protections instead of relying on a single control

Expose Dependencies Early
Identify cryptographic dependencies and technical debt before they block migration

Preserve Continuity
Align security progress with business operations and service commitments

Does OpenSSL Support Hybrid PQC Strategies?

YES with OpenSSL 3.5.9 in default mode and FIPS mode “pending FIPS 140 validation”

- X25519 with ML-KEM 768
- X448 with ML-KEM 1024
- SecP256r1 with ML-KEM 768
- SecP384r1 with ML-KEM 1024

Note: X25519 and X448 are currently not FIPS Approved algorithms however they are allowed under the requirements of NIST SP 800-227 when used in combination with a FIPS approved ML-KEM

Practical Framework for Navigating the Gap

Practical Framework for Navigating the Gap



01

Cryptographic Inventory

Map keys, algorithms, certs, libraries, and crypto dependencies



02

Identify Long-lived Sensitive Data

Find data that must remain confidential beyond current cryptographic strength of classical algorithms



03

Prioritize Migration Targets

Rank systems or applications by exposure, data value, dependency depth, and business criticality



04

Pilot Hybrid Solutions

Test hybrid patterns before broad migration



05

Track Validation Milestones

Use evidence-based checkpoints to prove readiness and reduce residual risk

Looking Forward

Looking Forward

Expect to see









1

More Validated Implementations

2

Additional Procurement Guidance

3

Evolving Regulatory Requirements

4

Increased Customer Interest

Final Takeaways



1 • PQC migration and FIPS 140 validation are separate milestones that organizations should evaluate together based on applicable security and compliance requirements

2

3 • Differences between PQC availability and FIPS 140 validation may create transitional challenges

• Organizations need a defensible migration strategy, not a perfect one

In summary, the question facing OpenSSL users today is how to deploy PQC through a risk-based approach while security requirements, procurement policies, and compliance frameworks evolve at different speeds. Success won't belong to the organizations that move first - it will belong to the organizations that can demonstrate why they moved when they did

Questions?

chris.brych@oracle.com