CRYPTOSPHERE

Post-Quantum Migration Guide

Preparing your critical infrastructure for the quantum era

Version 2026.1 — March 2026

cryptops.fr

Table of Contents

1. Why migrate now?

The "Harvest Now, Decrypt Later" threat

State and private adversaries are already collecting encrypted data in transit, with the intention of decrypting it later when sufficiently powerful quantum computers become available. Organizations handling data with long confidentiality requirements — defense, healthcare, finance, intellectual property — are the most exposed.

ANSSI timeline: mandatory hybridization by 2030

ANSSI recommends the immediate adoption of a hybrid approach (classical + post-quantum) as a transitional measure, and advises complete migration of classified systems before 2030. CSPN and CC security certifications will integrate PQC requirements into their evaluation criteria.

NIS2 and DORA mandate cryptographic resilience

The NIS2 directive (effective since October 2024) requires essential entities to assess risks related to emerging technologies, explicitly including the quantum threat. The DORA regulation, specific to the financial sector, mandates resilience testing that must integrate cryptographic compromise scenarios.

2030-2035 horizon: cryptographically relevant quantum computers

Estimates converge on 2030-2035 for the emergence of a quantum computer capable of breaking RSA-2048 and ECC via Shor's algorithm. The RSA, ECC and Diffie-Hellman algorithms that currently protect virtually all digital communications will then be obsolete.

> **Mosca's inequality:** If the required confidentiality duration of your data (x) plus the time needed to migrate (y) exceeds the time before a quantum computer arrives (z), then you must act now.

2. Post-quantum algorithms

In August 2024, NIST finalized three post-quantum cryptography standards, recommended by ANSSI for French information systems:

Standard	Usage	Mathematical basis	Note
ML-KEM-1024 (FIPS 203)	Key encapsulation (replaces DH/ECDH)	Lattice-based (Module-LWE)	Levels 512/768/1024. Competitive performance.
ML-DSA-87 (FIPS 204)	Digital signatures (replaces RSA/ECDSA)	Lattice-based (Module-LWE)	Larger signature sizes, excellent speed.
SLH-DSA (FIPS 205)	Backup signatures	Hash-based (Merkle trees)	Independent of lattices. Additional assurance.
AES-256-GCM	Symmetric encryption	—	Unchanged, already resistant to quantum attacks.

Hybrid approach: classical + post-quantum

The hybrid approach combines a classical algorithm (ECDH, ECDSA) with a post-quantum algorithm (ML-KEM, ML-DSA) during the transition. If either algorithm proves vulnerable, security is maintained by the other. This strategy is unanimously recommended by ANSSI, BSI and NSA.

In practice, hybrid mode concatenates two independent operations: for key exchange, both an ECDH and an ML-KEM are performed simultaneously, and the session key is derived from both shared secrets. The bandwidth overhead is moderate (approximately 1 KB per TLS handshake).

3. Assess your PQC maturity

Use this self-assessment grid to determine your organization's position and identify priority actions:

Level	Description	Recommended actions	Target
0	**Not considered** No quantum risk awareness. No sensitization.	Brief executive leadership. Launch crypto inventory. Train security teams.	Immediate
1	**Aware** Risk identified. Cryptographic inventory in progress.	Complete inventory. Map encrypted flows. Assess HNDL exposure.	3-6 months
2	**Planned** Migration strategy defined. POC planned.	Qualify hybrid solutions. Execute POC. Budget the migration.	6-12 months
3	**In progress** Hybrid deployment on critical flows.	Extend coverage. Automate testing. Prepare certification.	12-24 months
4	**Achieved** Complete migration. ANSSI certification obtained.	Ongoing maintenance. Algorithm monitoring. Prepare classical deprecation.	24-36 months

> **Where are you?** Most European organizations are between levels 0 and 1. The ANSSI target is to reach level 3 before 2030 for critical infrastructure operators and NIS2 essential entities.

4. The 5 migration steps

1. Cryptographic inventory

Identify all encrypted flows, protocols, algorithms and certificates across the organization. Catalog each asset with its algorithm, key size, residual lifetime and business criticality. Also cover partners and subcontractors — digital supply chains inherit cryptographic vulnerabilities from each link.

2. Quantum risk analysis

Classify data by required confidentiality duration vs quantum horizon. Apply Mosca's inequality to prioritize. Data requiring confidentiality beyond 2030 is at immediate risk if transmitted today over channels protected only by classical cryptography. Present results to management as a risk matrix.

3. Proof of concept

Deploy a hybrid PQC tunnel on a non-critical flow. Measure impact on latency, throughput and memory consumption. Test interoperability between different implementations (liboqs, BoringSSL, wolfSSL, FPGA). Verify that intermediate equipment (firewalls, proxies, IDS) accepts the larger packets.

4. Progressive deployment

Critical flows first (datacenters, production sites, partner links), then extension. Hybrid mode during transition to maintain connectivity with sites not yet migrated. Migrate PKI hierarchy top-down: trust root, intermediate authorities, then end-entity certificates.

5. Certification and compliance

CSPN / EAL4+ for critical infrastructure environments. Document the PQC migration strategy in your ISSP. Maintain a quarterly-updated cryptographic asset register. Ensure traceability of all migration decisions and actions for NIS2 and DORA compliance audits.

5. The Cryptosphere approach

Cryptosphere designs and manufactures sovereign post-quantum network encryptors, entirely developed in France, for European critical infrastructure.

FPGA line-rate encryptors

Our encryptors implement post-quantum algorithms directly on FPGA, delivering deterministic performance from 1 Gbps to multi-Tbps. Hardware implementation ensures resistance to side-channel attacks and constant latency regardless of load. FPGA reconfigurability allows algorithm updates without hardware replacement.

Transparent deployment

Encryptors integrate transparently into existing infrastructure via IPsec. No application modifications required. Hybrid mode (classical + PQC) is enabled by default during the transition period.

Three operating modes

- **Full sovereignty:** keys generated and stored on-site, no external dependency.
- **Autonomous:** delegated management via the GARANCE platform (PKI + orchestration + monitoring).
- **Managed:** turnkey service, operated by Cryptosphere from France.

GARANCE: PKI + orchestration + monitoring

The GARANCE platform centralizes key management, encryptor orchestration and real-time monitoring. Unified dashboard, automated alerts, schedulable key rotation, complete logging for compliance.

Certification and sovereignty

Targeting ANSSI CSPN certification, EAL4+ trajectory. 100% Rust codebase, EUPL-1.2 license. Design, development and manufacturing entirely in France.

6. Deployment spectrum

The Cryptosphere range covers all post-quantum encryption needs, from remote sites to operator backbones:

Segment	Model	Throughput	Use case
Edge	PQC-WAN Agent	1 — 100 Gbps	Remote sites, branches, partner links
Datacenter	PQC-800 / 1600 / 2400	800 Gbps — 2.4 Tbps	Core network, DC interconnections
Backbone	PQC-3200 / 6400	3.2 Tbps — multi-Tbps	Operator backbone, hyperscaler
Standalone	PQC-800S / 1600S	800 Gbps — 1.6 Tbps	Isolated sites, air-gapped environments
Cloud	PQC SecNumCloud	As needed	Managed service, sovereign cloud

All models support hybrid mode (classical + post-quantum), line-rate IPsec encryption and centralized management via GARANCE. Built-in crypto-agility allows algorithm updates through FPGA reconfiguration, without hardware intervention.

7. Regulatory compliance

The European regulatory framework imposes increasing requirements for cryptographic resilience. The table below summarizes key obligations and Cryptosphere coverage:

Regulation	Requirement	Cryptosphere coverage
LPM / OIV	Securing vital information systems. Encryption of sensitive flows.	CSPN/EAL4+ certifiable encryptors. Full key sovereignty.
NIS2	Emerging technology risk assessment. Essential entity resilience.	PQC hybrid encryption. Automated crypto register.
DORA	Digital operational resilience for the financial sector. Crypto resilience testing.	Automated testing. Schedulable key rotation. Complete logging.
II 901	Protection of IS handling classified information.	Line-rate encryption. Sovereign key management.
SecNumCloud	Qualification of sovereign cloud services.	PQC SecNumCloud model. French hosting.
ANSSI PQC 2030	Complete PQC migration before 2030 for classified systems.	End-to-end support. Native crypto-agility.

8. Recommended migration timeline

2025-2026 **Phase 1 — Preparation**

Cryptographic inventory. Executive briefing. Team training. Quantum risk assessment. Solution selection. Budget.

2026-2027 **Phase 2 — POC and qualification**

Proof of concept on non-critical flow. Interoperability testing. Hardware and software solution qualification. Target architecture validation.

2027-2028 **Phase 3 — Hybrid deployment**

Hybrid mode deployment on critical flows. PKI migration. Progressive extension. CSPN certification.

2028-2030 **Phase 4 — Complete migration**

Extension to all perimeters. Progressive deprecation of classical-only algorithms. ANSSI PQC 2030 compliance. Operational maintenance.

> **Recommendation:** Start now with the cryptographic inventory (Phase 1). It is a low-risk, high-impact action that conditions the entire migration process.

9. Next steps

Ready to assess your PQC maturity and plan your migration? Here is how to proceed:

Request a PQC maturity audit

Our team performs a complimentary diagnostic of your cryptographic infrastructure. In half a day, we identify your at-risk flows, evaluate your maturity level and propose a migration roadmap tailored to your context.

Schedule a proof of concept

Deploy a PQC encryptor on a test flow to measure performance and validate integration with your existing infrastructure. The POC can be completed in two weeks.

Contact us

- Secure form: **cryptops.fr/en/contact**
- Email: **contact@cryptops.fr**

> Our contact form is end-to-end encrypted (RSA-4096 + AES-256-GCM). Your message is encrypted in your browser before transmission. No intermediary has access to the content.

10. About Cryptosphere

Cryptosphere is a French manufacturer of post-quantum network encryptors for European critical infrastructure. Founded with the conviction that cryptographic sovereignty is a strategic imperative, the company designs, develops and manufactures all its solutions in France.

Our FPGA encryptors implement NIST-standardized post-quantum algorithms (ML-KEM, ML-DSA) with line-rate performance, from 1 Gbps to multi-Tbps. Native crypto-agility allows algorithm updates through reconfiguration, without hardware intervention.

Headquarters	19 rue du Colisée, 75008 Paris
R&D Laboratory	Rouen, France
Website	cryptops.fr
Contact	contact@cryptops.fr

Sovereign post-quantum encryption for European critical infrastructure