Quantum-resistance: why action is needed now in Europe and how to proceed without disruption

A practical guide for CISOs, IT teams and business leaders on risk, hybrid approaches and an EU-ready roadmap

Executive summary

Imagine a perfectly sealed safe that is secure today, but opens on its own in a few years because the technology behind its lock has changed. This is the core idea behind **Harvest-Now, Decrypt-Later** (HNDL): attackers intercept and store encrypted data – such as emails, backups, application traffic, or B2B exchanges – with the expectation of decrypting it later, when advances in computing, including quantum technologies, make currently unfeasible attacks practical.

This is not scaremongering, but a call to action

The most pragmatic way to address emerging quantum threats is a hybrid approach: introducing, where appropriate, certificates and protocols that combine classical cryptography with post-quantum components (PQC). This approach reduces long-term data exposure while preserving operational continuity and existing systems.

In Europe, the evolving cybersecurity framework – including the NIS2 and eIDAS2 Regulations, the Cyber Resilience Act, and technical standards developed by ETSI and ENISA – promotes a structured approach to risk management that also recognises the need to address potential vulnerabilities in current cryptographic methods.

This roadmap defines an **18-month transition path**. In its initial phase, it focuses on measurable pilot projects conducted within controlled and test environments. These pilots are designed to identify where quantum-related risks are most relevant in practice. Based on the evidence gathered, the approach can then be progressively extended and standardised in a secure, controlled and repeatable manner.

As a European **QTSP (Qualified Trust Service Provider)**, Actalis adopts a **lab-first approach** – combining tools, methods and support – to help organisations and public sector infrastructure transition towards quantum-resistant security.

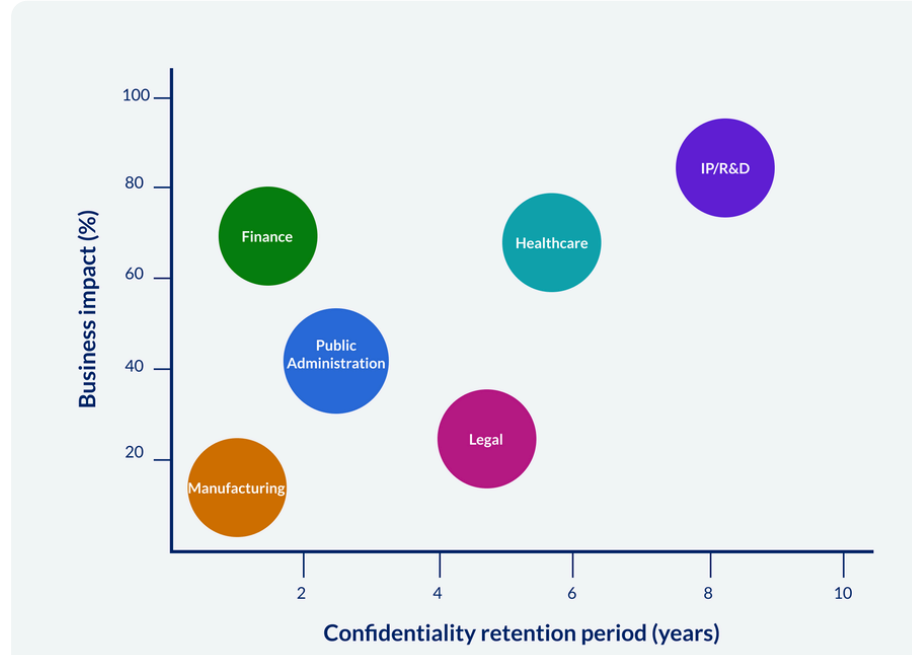
➜ ***This is not a revolution that happens overnight. Organisations that start today reduce exposure to HNDL and prepare to adapt without disruption.***

1. Understanding the risk: HNDL in plain English

In everyday business, encryption is largely invisible: the padlock icon in the browser, a certificate on a server, or a policy governing data and document storage. It is therefore easy to assume that if it works today, it will continue to work tomorrow.

The challenge lies in the time horizon. Many categories of data must remain confidential for years, or even decades – including medical records, financial documents, legal files, industrial intellectual property, M&A strategies, tax data and product plans. If an attacker intercepts and stores encrypted network traffic or data archives today, they may be able to decrypt them in the future, once sufficiently powerful and reliable quantum computers become available. This moment represents a point of no return. The impact of a Harvest Now, Decrypt Later (HNDL) attack is therefore not immediate, but delayed: the data breach materialises in the future, when mitigation or remediation is no longer possible.

Understanding HNDL requires viewing risk as a function of probability and impact over time. Probability increases as technology evolves; impact depends on the value, sensitivity and required confidentiality duration of the encrypted data. This is why not all systems carry the same priority: public information poses little risk, while an R&D project, a health record or a strategic business dataset does.



60 seconds on HNDL

- This is not a “tomorrow everything fails” scenario, but a deferred risk affecting data that must remain secret or confidential over the medium to long term.
- The priority is to protect today what must remain confidential in the future.

2. What is Post-Quantum Cryptography?

Post-Quantum Cryptography (PQC) is a branch of cryptography focused on developing algorithms designed to withstand attacks from quantum computers, whose computational capabilities are expected to exceed those of classical systems. PQC is not a “magic” replacement, nor does it require an immediate overhaul of existing infrastructure. Rather, it introduces a new set of cryptographic tools that can be adopted progressively to strengthen the resilience of services and protocols.

A realistic transition strategy does not discard existing cryptographic systems. Instead, it relies on hybrid solutions, in which classical and post-quantum components coexist within the same certificate or protocol. In practice, this approach offers two key advantages: (1) Compatibility with current servers, applications and cryptographic libraries; (2) Long-term resilience, as the post-quantum component provides additional protection for confidential data over the medium to long term.

For **hybrid solutions** to remain effective over time, implementations must support the rapid replacement of keys and algorithms as standards evolve, without requiring widespread changes to applications or infrastructure.

For this reason, hybrid cryptography and crypto-agility should be viewed as complementary, independent strategies.

➡ ***Protecting systems today means being able to adapt tomorrow. The true bulwark is cryptographic agility, not the pursuit of a perfect algorithm.***

What’s a hybrid certificate?

A hybrid certificate combines classical cryptography with quantum-resistant components. End-user experience remains unchanged, while the underlying architecture gains continuity today and resilience for the future.

The European perspective: risk, trust and supply chains

Europe is accelerating its efforts in post-quantum cryptography through a regulatory framework designed to guide businesses and public administrations in the transition to quantum-resistant technologies.
The new eIDAS2 Regulation requires Trust Service Providers to adopt state-of-the-art cryptographic solutions, creating the conditions for the progressive integration of quantum-resistant algorithms within trusted digital services.

At the same time, the NIS2 Directive mandates structured digital risk management across critical sectors. This includes the assessment of cryptographic dependencies and the definition of transition plans towards post-quantum cryptography (PQC).

ENISA guidelines and ETSI technical standards already provide operational recommendations and technical profiles for the adoption of quantum-resistant schemes and hybrid approaches, supporting a gradual, interoperable and standards-based transition.

Taken together, these regulatory and technical initiatives outline a clear path forward: mapping cryptographic assets, progressively introducing quantum-resistant algorithms, and ensuring continuity, security and compliance across digital supply chains, even in the presence of emerging threats.
For organisations and public administrations, investing early in the transition to post-quantum cryptography is therefore not only a matter of future security, but also a means to strengthen compliance and ensure the long-term resilience of digital services.

➜ ***Three EU-focused verbs: Plan. Document. Demonstrate. Cyber resilience is a matter of governance, not cryptography alone.***

Important note

This section is provided for informational purposes only and does not constitute legal advice.
Organisations should consult qualified legal or regulatory experts to assess and implement requirements applicable to their specific context and EU jurisdiction.

4. Why a hybrid solution is the most cautious and practical approach

The digital industry has learned that large, disruptive technology shifts carry significant risk. Hybrid solutions enable the gradual introduction of post-quantum cryptography (PQC) where appropriate, while preserving compatibility, control and operational stability. In practice, this approach enables:

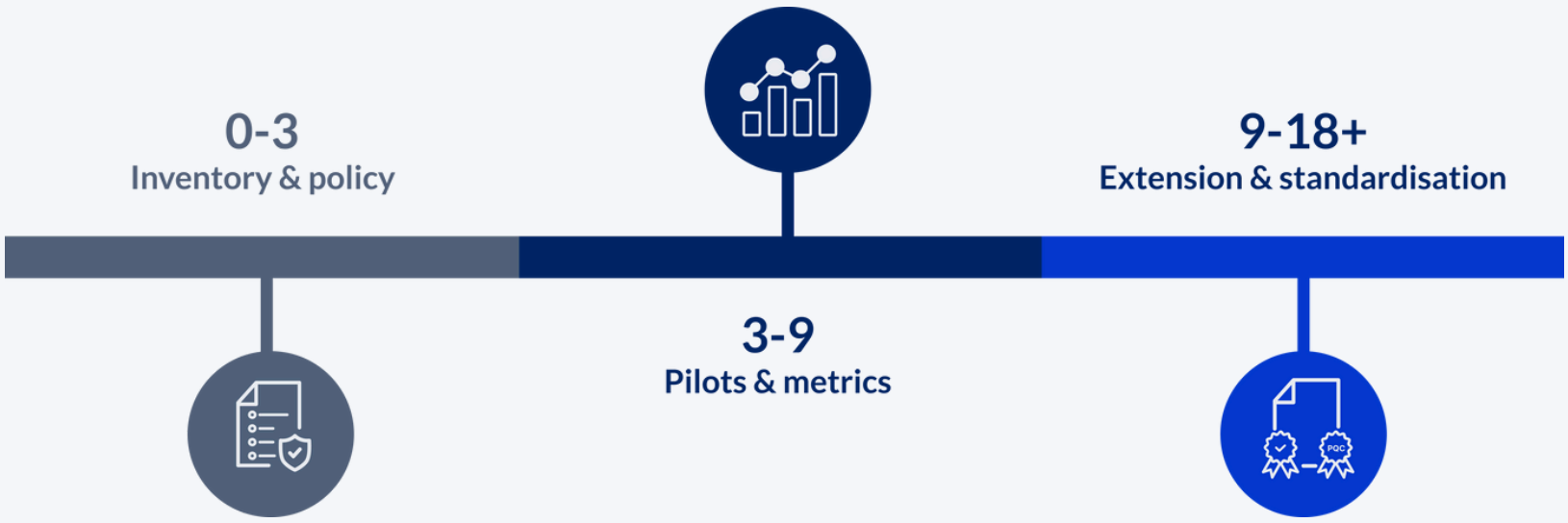
- Continuity for end users
- Reduced exposure to HNDL risk for long-lived and sensitive data
- Controlled adoption through limited pilot projects
- Defined and tested rollback mechanisms
- Organisational alignment, supporting clearly defined crypto-agility roles, responsibilities and policies

➜ ***Avoid technical lock-in. Preserving the ability to change tomorrow is the most effective way to stay ahead.***

Three questions to ask before getting started

1. Do I know where encryption matters most over time?
2. Do I have clear metrics to measure impact and compatibility?
3. Is my rollback plan clearly defined, rapid and tested?

5. An 18-month ‘EU-ready’ roadmap



The roadmap is structured into three phases, with the objective of launching hybrid pilot projects within controlled production environments.

Phase 1

0–3 months: understanding and decision-making

The first phase focuses on clarifying scope and defining priorities.

A tangible **cryptographic inventory** is established, covering certificates in use, TLS libraries, email gateways, APIs and B2B integrations, OT devices and components, and long-term data archives. This is not a theoretical exercise: its purpose is to map concrete dependencies between data, communication channels and underlying technologies.

Data with long confidentiality requirements is then classified and prioritised by identifying relevant processes, suppliers and points of exposure. By cross-referencing confidentiality duration with business criticality and exposure levels, a limited set of high-priority areas typically emerges.

Finally, **the foundations of crypto-agility are defined.** This includes encryption architecture principles, key and algorithm rotation strategies, X.509 extensions, change and rollback flows, as well as roles and responsibilities.

The phase concludes with a cryptographic **inventory report**, a risk and priority matrix, and an initial draft policy to guide subsequent phases.

➜ ***The 80/20 rule applies. 20% of data and channels account for 80% of long-term risk. Start there.***

Phase 2

3–9 months: measurable pilots in controlled production environments

During this phase, pilot deployments are made live but remain deliberately restricted. Typical pilot use cases include:

- A non-customer-facing domain for mTLS or API communication using hybrid certificates
- A highly sensitive department (for example, legal) using hybrid S/MIME
- Hybrid code signing within the build or CI/CD pipeline, where applicable
- Digitally signed legally valid documents
- Secure connections, such as virtual private networks
- Encryption of data at rest
- Authentication processes

For each pilot, simple and comparable metrics are defined – including handshake latency, error rates, compatibility and operational impact. Feature flags and canary releases are used to ensure that changes can be progressed or rolled back safely.

The primary value of this phase lies in the evidence collected: concrete measurements and operational feedback that support informed decision-making and guide the transition to broader deployment.

➜ ***Small. Real. Measurable. Effective pilots produce evidence, not opinions.***

Phase 3

9–18+ months: extend, standardise and formalise

With evidence in hand, deployment is progressively extended, starting with domains that have low user exposure and then moving towards more critical services and business processes.

At this stage, policies and operational artefacts are standardised, including playbooks, CMDB entries, procurement criteria and incident response models related to cryptographic components.

The supply chain dimension is addressed by updating contracts and SLAs to include minimum crypto-agility requirements, defined transition timelines and appropriate reporting obligations.

Finally, training and communication activities embed the new practices into day-to-day operations, transforming the transition from a project into a sustained operational routine.

Directional KPIs

- Percentage of assets with a defined encryption profile
- Percentage of quantum-resistant channels (based on extended pilot deployments)
- Average rollback time without disruption
- Percentage of suppliers with updated crypto-agility clauses

➜ ***From test to programme. The transition succeeds when it becomes part of the service lifecycle, not a one-off project.***

6. What really changes for the organisation

The transition to post-quantum cryptography is not only a technological shift, but a cultural and operational one.

Change management becomes the backbone of the programme: governance bodies (such as CABs), maintenance windows, testing plans and reversibility mechanisms are now the focus. At the same time, investment shifts from purchasing standalone products to building processes and skills – including assessment, piloting, training, certificate lifecycle automation and cryptographic key management.

People play a critical role. Crypto-agility is inherently cross-functional, requiring close collaboration between Security, Architecture, DevOps, Legal and Procurement teams.

Suppliers should also be evaluated not only on current capabilities, but on their roadmap: can they support hybrid and post-quantum cryptography? Do they provide tools for testing, linting, certificate chain verification and interoperability? Are their support models aligned with your SLAs?
In essence, the real value lies in demonstrating that the organisation can evolve in a controlled, documented and measurable way.

7. The role of Actalis as a European QTSP

Actalis operates in a dual strategic role. On the one hand, it acts as a European **Certification Authority,** providing **TLS/SSL, S/MIME** and **Code Signing** certificates and **participating actively in the SSL CAB Forum**. On the other, it operates as a **Qualified Trust Service Provider (QTSP)** under the **eIDAS 2 Regulation**, ensuring governance, compliance and long-term trust in the delivery of regulated digital services.

In this position, Actalis approaches the transition to **post-quantum cryptography** through an integrated and standards-aligned strategy, consistent with European regulatory requirements and international technical frameworks in cybersecurity.

This strategy follows a **lab-first approach**: first test, then extend.

The **PQC Lab** (beta) provides a controlled environment for issuing and verifying hybrid certificates, performing X.509 chain linting, and measuring latency and interoperability across common use cases such as TLS/mTLS, S/MIME and code signing.

Our **30-day**, evidence-driven **method** follows these steps:

1. Structured discovery to define scope, objectives and priorities
2. Rapid assessment of cryptographic inventory and long-lived data
3. Pilot design, including metrics and rollback mechanisms
4. Access to the PQC Lab to generate, test and validate hybrid certificates
5. Evidence-based reporting to decide whether to scale, adjust or pause

Actalis PQC Lab (beta)

- Issuing and verification of hybrid certificates
- X.509 chain linting and basic conformity checks
- Inter-operability and latency testing on real-world use cases

(Specifications and usage restrictions available upon request; EU-focused)

➜ ***Minimal effort, maximum impact. A well-executed pilot is worth more than a hundred slides.***

8. Frequently asked questions (non-technical)

Do we need to change everything right away?

No. The priority is to protect data that must remain confidential over the medium to long term. A hybrid approach allows organisations to begin addressing quantum-related risks while preserving operational continuity.

Are standards expected to change?

Yes – and this is already anticipated. Cryptographic standards evolve in response to newly identified risks. This is precisely why crypto-agility is critical: to protect processes and platforms that may change over time.

Is there a significant impact on end users?

When pilot projects are deployed internally using feature flags and rollback mechanisms, the impact on end users is minimal. Wider deployment typically follows only after successful testing and validation.

Why can't we wait until everything is fully defined?

Delaying action increases exposure to Harvest Now, Decrypt Later (HNDL) risks for data that has already been collected. Starting now allows organisations to manage risk and costs in a controlled way.

9. Notes and EU references (non-legal)

This document does not constitute legal advice.
From an EU perspective, the following considerations are particularly relevant:

- Integration of HNDL risk into organisational risk management and supply-chain governance, as required by the NIS2 framework
- Protection of the chain of trust within the eIDAS2 perimeter, with a clear distinction between public trust services and private or enterprise trust domains during the transition
- Adoption of best practices and technical guidance published by ETSI and ENISA to define policies, inventories and post-quantum migration plans

For sector-specific or country-specific application within the EU, organisations should involve Compliance functions and trusted legal or regulatory advisors.