# Quantum-Safe: Warum man in Europa jetzt handeln sollte und wie man dies tun kann, ohne den Betrieb zu blockieren

Ein praktischer Leitfaden für CISO, IT- und Business-Führungskräfte zu Risiken, hybriden Ansätzen und „EU-ready“-Roadmaps.

# Executive Summary

Stellen Sie sich einen heute perfekt verschlossenen Safe vor, der sich in einigen Jahren von selbst öffnet, weil sich die Technologie der Schlüssel geändert hat. Das ist das Wesen der Bedrohung **„Harvest-Now, Decrypt-Later"** (HNDL): Cyberangreifer fangen heute verschlüsselte Daten ab und speichern sie – E-Mails, Backups, Anwendungsdatenverkehr, B2B-Austausch –, um sie morgen zu entschlüsseln, wenn Fortschritte bei Prozessoren, einschließlich Quantenprozessoren, Angriffe ermöglichen, die heute noch undurchführbar sind.

Keine Panikmache, sondern Planung ist gefragt

Die pragmatischste Antwort ist der hybride Ansatz: die Einführung von Zertifikaten, Schlüsseln, Algorithmen und Protokollen, die klassische kryptografische Komponenten mit Post-Quantum-Komponenten (PQC) kombinieren. Der hybride Ansatz [MM1.1] ermöglicht es, bereits jetzt Daten für Systeme zu schützen, die PQC implementieren, ohne Auswirkungen auf bestehende Systeme und Prozesse zu haben.

Im europäischen Kontext drängt das überarbeitete Rahmenwerk für Cybersicherheit, darunter die europäischen Verordnungen NIS2, eIDAS2, der Cyber Resilience Act und die technischen Standards ETSI und ENISA, auf ein strukturiertes Risikomanagement, das sich auch auf mögliche Schwachstellen der aktuellen kryptografischen Methoden konzentriert.
Diese Roadmap sieht einen **18-monatigen Zeitplan** vor, in dessen Anfangsphase wir messbare Pilotprojekte in Demo- und kontrollierten Umgebungen durchführen werden. Diese ersten Experimente werden uns helfen zu verstehen, wo das Risiko des Quantencomputings wirklich signifikant ist, sodass wir dank der erzielten Ergebnisse den Ansatz auf sichere und strukturierte Weise erweitern und standardisieren können.

Actalis bietet als europäischer QTSP (**Qualified Trust Service Provider**) und Certification Authority im Ökosystem der SSL-Zertifikate einen **Lab-First-Ansatz** – Tools, Methoden und Support –, um Unternehmen und öffentliche Verwaltungen beim Übergang zu quantensicheren Technologien zu begleiten.

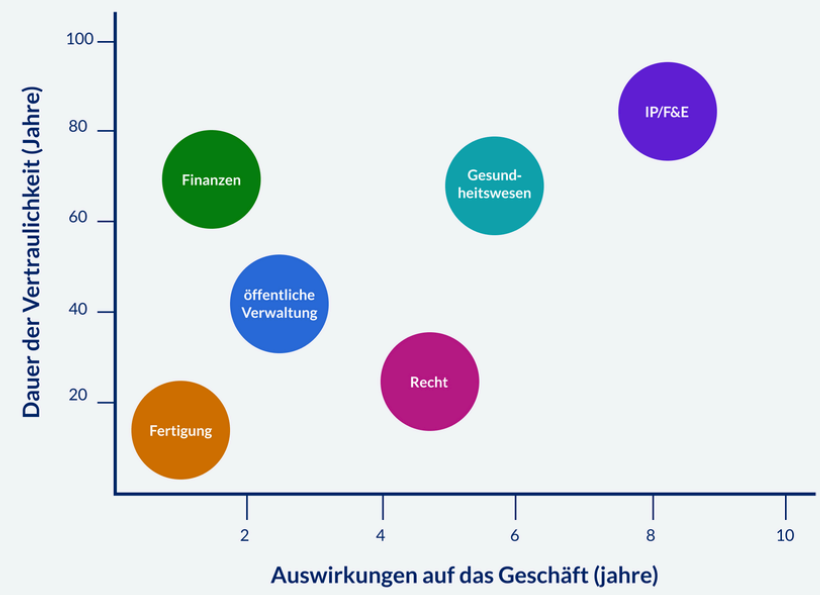
➜ ***Dies ist keine nächtliche Revolution, sondern ein Programm. Wer heute damit beginnt, reduziert das HNDL-Risiko für seine Daten und bereitet sich auf eine reibungslose Weiterentwicklung vor.***

# 1. Das Risiko verstehen: HNDL einfach erklärt

Im Unternehmensalltag ist die Verschlüsselung unsichtbar: das Schloss-Symbol im Browser, ein Zertifikat auf dem Server, eine Richtlinie zur Speicherung von Daten und Dokumenten. Man könnte leicht denken: „Wenn es heute funktioniert, wird es auch morgen funktionieren."

Das Problem ist der Zeithorizont: Viele Informationen müssen über Jahre oder sogar Jahrzehnte hinweg geheim oder geschützt bleiben (Krankenakten, Finanzdokumente, Rechtsakten, industrielles geistiges Eigentum, M&A-Strategien, Steuerdaten, Produktpläne). Wenn ein Angreifer heute den Datenverkehr oder die mit den aktuellen Methoden verschlüsselten Computerarchive sammelt und speichert, kann er versuchen, diese zu entschlüsseln, sobald zuverlässige und leistungsfähige Quantencomputer zum Einsatz kommen, die den Punkt ohne Wiederkehr bestimmen. Die Auswirkungen treten nicht unmittelbar, sondern verzögert ein: Eine potenzielle Sicherheitslücke, die sich in der Zukunft öffnet und Schäden verursacht, wenn eine Reaktion bereits nicht mehr möglich ist.

HNDL zu verstehen bedeutet, das Risiko als Produkt aus Wahrscheinlichkeit und Auswirkung im Laufe der Zeit zu betrachten. Die Wahrscheinlichkeit steigt mit dem technologischen Fortschritt; die Auswirkung hängt vom Wert, der Dauer und der Vertraulichkeit der verschlüsselten Daten ab. Aus diesem Grund haben nicht alle IT-Systeme die gleiche Priorität: Öffentliche Informationen sind kein Problem, ein F&E-Projekt oder eine Gesundheitsakte hingegen durchaus.




## 60 Sekunden zu HNDL

- Es ist nicht so, dass „morgen alles zusammenbricht". Es handelt sich um ein aufgeschobenes Risiko, das Daten betrifft, die mittel- bis langfristig geheim oder vertraulich bleiben müssen.
- Die Priorität besteht darin, heute das zu schützen, was über Jahre hinweg vertraulich bleiben muss.

# 2. Was ist Post-Quanten-Kryptografie

Die **Post-Quanten-Kryptografie** (PQC) ist ein Zweig der Kryptografie, der kryptografische Algorithmen entwickelt, die gegen Angriffe von Quantencomputern gewappnet sind, deren Rechenleistung weit über der von klassischen Computern liegt. Dabei handelt es sich weder um eine „magische" Technologie, noch ersetzt sie alles auf einen Schlag: Vielmehr ist sie das neue Instrumentarium, mit dem nach und nach widerstandsfähigere Dienste und Protokolle aufgebaut werden können.

Der realistische Weg besteht nicht darin, das Bestehende wegzuwerfen, sondern **hybride Lösungen** zu verwenden, bei denen eine klassische Komponente und eine Post-Quanten-Komponente im selben Zertifikat oder Protokoll nebeneinander existieren. In der Praxis ergeben sich daraus zwei Vorteile: (1) Kompatibilität mit aktuellen Servern und Bibliotheken; (2) Langfristige Widerstandsfähigkeit, da das PQC-Element mittel- bis langfristig zusätzlichen Schutz für vertrauliche Daten bietet.

Damit das Hybridsystem funktioniert, müssen Lösungen implementiert werden, die es in Zukunft ermöglichen, Schlüssel und Algorithmen sehr schnell zu ersetzen, ohne dass dies Auswirkungen auf alle Anwendungen hat.

Der hybride Ansatz und die Krypto-Agilität sind also zwei Lösungen, die parallel und unabhängig voneinander angewendet werden können.

➜ ***Sich heute gut zu verteidigen bedeutet, morgen veränderungsfähig zu sein. Die wahre Sicherheit liegt in der kryptografischen Agilität, nicht im perfekten Algorithmus.***

### Was ein Hybridzertifikat ist

Ein Hybridzertifikat kombiniert eine klassische kryptografische Komponente mit einer Komponente, die gegen Angriffe durch Quantencomputer resistent ist. Für den Endnutzer ändert sich nichts, für die IT-Architektur bedeutet dies jedoch Kontinuität im Betrieb heute und Widerstandsfähigkeit morgen.

# 3. Die europäische Perspektive: Risiko, Vertrauen und Wertschöpfungsketten

Europa treibt die Post-Quanten-Verschlüsselung voran und definiert einen Rechtsrahmen, der Unternehmen und die europäische öffentliche Verwaltung beim Übergang zu „quantensicheren“ Technologien leiten wird.

Die neue eIDAS2-Verordnung verpflichtet Vertrauensdienstleister wie Actalis dazu, die derzeit besten verfügbaren Verschlüsselungslösungen einzusetzen und damit den Weg für die Integration quantencomputerresistenter Algorithmen zu ebnen.

Parallel dazu schreibt die NIS-2-Richtlinie allen kritischen Sektoren ein strukturiertes digitales Risikomanagement vor, einschließlich der Überprüfung kryptografischer Abhängigkeiten und der Planung der PQC-Migration.

Die ENISA-Leitlinien und ETSI-Technikstandards bieten bereits heute operative Empfehlungen und technische Profile für die Einführung von Post-Quanten-Schemen und Hybridlösungen und erleichtern so einen schrittweisen und interoperablen Übergang.

Die Gesamtheit dieser Vorschriften und technischen Standards schafft einen klaren Weg: alle kryptografischen Vermögenswerte zu erfassen, schrittweise quantensichere Algorithmen einzuführen und Kontinuität, Sicherheit und Konformität der erbrachten Dienstleistungen auch im Falle neuer Bedrohungen zu gewährleisten.

Für Unternehmen und Verwaltungen bedeutet eine Investition in den Übergang zur Post-Quanten-Kryptografie jetzt eine Stärkung der Compliance und die Gewährleistung der langfristigen Widerstandsfähigkeit ihrer digitalen Dienste.

➜ ***Drei EU-Verben: Planen. Dokumentieren. Nachweisen. Cyber-Resilienz ist ein Governance-Prozess, nicht nur eine Frage der Verschlüsselung.***

### Wichtiger Hinweis

Dieser Abschnitt dient nur zu Informationszwecken und ersetzt keine Rechtsberatung. Für die korrekte Anwendung der spezifischen Anforderungen für Ihre Organisation und Ihr EU-Land wenden Sie sich bitte an erfahrene Berater.

# 4. Warum Hybrid die praktische und vernünftige Lösung ist

Die digitale Industrie hat auf eigene Kosten gelernt, dass technologische Big Bangs riskant sind. Der hybride Ansatz ermöglicht es, PQC in kleinen Schritten dort einzusetzen, wo es nötig ist, und dabei Kompatibilität und Steuerbarkeit zu gewährleisten:

- Kontinuität für die Nutzer,
- Reduzierung des HNDL-Risikos für langlebige Daten,
- Kontrolle durch begrenzte Pilotprojekte
- definierte und getestete Rollback-Pläne
- und eine organisatorische Ausrichtung, die Richtlinien und Rollen der Krypto-Agilität umsetzt.

➜ ***Vermeiden Sie technische Lock-in-Effekte. Heute die Möglichkeit planen, morgen zu ändern, ist der beste Weg, um nicht zurückzubleiben.***

### Drei Fragen vor dem Start

1. Weiß ich, wo Verschlüsselung im Laufe der Zeit wirklich wichtig ist?
2. Verfüge ich über einfache Messgrößen, um Auswirkungen und Kompatibilität zu messen?
3. Ist mein Rollback-Plan klar, bewährt und schnell?

# 5. Eine „EU-ready“-Roadmap in 18 Monaten


Unsere Roadmap umfasst drei Phasen mit dem Ziel, hybride Pilotprojekte in einer kontrollierten Produktionsphase zu realisieren.

Phase 1

## 0–3 monate: Verstehen und Entscheiden

Die erste Phase zielt darauf ab, den Umfang zu erfassen und zu entscheiden, wo anzusetzen ist.

Es wird eine konkrete **kryptografische Bestandsaufnahme** durchgeführt: verwendete Zertifikate, TLS-Bibliotheken, E-Mail-Gateways, APIs und B2B-Integrationen, OT-Geräte und -Komponenten, Langzeitarchive. Dies ist keine theoretische Übung, sondern dient dazu, Daten, Kanäle und Zusammenhänge miteinander zu verknüpfen.

**Langlebige Daten werden klassifiziert**, wobei Prozesse, Anbieter und Expositionspunkte identifiziert werden. Durch die Gegenüberstellung von Vertraulichkeitsdauer, Prozesskritikalität und Exposition kristallisieren sich einige wenige Bereiche mit hoher Priorität heraus.

Anschließend werden die **Grundsätze der Krypto-Agilität definiert**: Architektur der Verschlüsselungslösungen, Rotationen, X.509-Erweiterungen, Änderungsströme, Rollen und Verantwortlichkeiten.

Die Phase endet mit einem **Bestandsbericht**, einer Risiko-/Prioritätsmatrix und einem Policy-Entwurf.

➜ ***80/20-Regel. 20 % der Daten und Kanäle verursachen 80 % des langfristigen Risikos. Beginnen Sie dort.***

Phase 2

## 3–9 monate: Messbare Pilotprojekte in kontrollierter Umsetzung

Das Pilotprojekt ist real, aber begrenzt:

- eine nicht kundenorientierte Domäne für mTLS/API mit hybriden Zertifikaten;
- eine hochsensible Abteilung (z. B. Rechtsabteilung) mit hybridem S/MIME;
- und, falls zutreffend, eine hybride Code-Signierung in der Build-Pipeline
- die Unterzeichnung rechtsgültiger Dokumente (digitale Signatur)
- sichere Verbindungen (z. B. virtuelle private Netzwerke)
- Verschlüsselung ruhender Daten
- Authentifizierungsprozesse.

Für jedes Pilotprojekt werden einfache Metriken definiert (Handshake-Latenz, Fehler, Kompatibilität, betriebliche Auswirkungen) und Feature-Flags und Canary-Releases verwendet, um sicher voranzukommen oder zurückzugehen.

Der wahre Wert liegt in den für die Entscheidung nutzbaren Erkenntnissen.

➜ ***Klein, real, messbar. Ein gutes Pilotprojekt liefert Erkenntnisse, keine Meinungen.***

Phase 3

## 9–18+ monate: Ausweiten, Standardisieren, Kontraktualisieren

Mit den vorliegenden Erkenntnissen wird schrittweise erweitert: zunächst Domains mit geringer Benutzerexposition, dann kritischere Dienste.

Richtlinien, Playbooks, CMDBs, Beschaffungskriterien und Vorlagen für Vorfälle im Zusammenhang mit der Verschlüsselungskomponente werden standardisiert.

Die Supply Chain wird optimiert, indem Verträge und SLAs mit Mindestanforderungen an Krypto-Agilität, Anpassungsfristen und Berichterstattung aktualisiert werden.

Abschließend sorgen Schulungen und Kommunikation dafür, dass der Übergang zur operativen Routine wird.

### KPI für die Geschäftsleitung

- % der Vermögenswerte mit bekanntem Krypto-Profil
- % der „quantum-ready“-Kanäle (vom Pilotprojekt bis zur flächendeckenden Einführung)
- Durchschnittliche Rollback-Zeit ohne Betriebsstörungen
- % der Anbieter mit aktualisierten Krypto-Agile-Klauseln

➜ ***Vom Test zum Programm. Der Übergang gelingt, wenn er in den Lebenszyklus der Dienste integriert und nicht nur als einmaliges Projekt betrachtet wird.***

# 6. Was sich für die Organisation wirklich ändert

Der Wandel ist nicht nur technologischer Natur, sondern auch kultureller und operativer Art.

Das Änderungsmanagement (CAB, Fenster, Testpläne, Reversibilität) wird zum tragenden Element. Das Budget verlagert sich vom Kauf von Produkten hin zur Umsetzung von Prozessen und Kompetenzen: Bewertung, Pilotprojekte, Schulungen, Automatisierung des Zertifikatszyklus und der kryptografischen Schlüssel.

Die Menschen stehen im Mittelpunkt: Krypto-Agilität erfordert Teamarbeit zwischen den Bereichen Sicherheit, Architektur, DevOps, Recht und Beschaffung.

Anbieter müssen auch anhand ihrer Roadmap bewertet werden: Sind sie in der Lage, Hybrid- und PQC-Lösungen zu begleiten? Verfügen sie über Tools für Tests, Linting, Kettenüberprüfung und Interoperabilität? Bieten sie Supportmodelle, die mit Ihren SLAs übereinstimmen?

Zusammenfassend lässt sich sagen: Der Wert liegt darin, zu zeigen, dass sich die Organisation auf kontrollierte, dokumentierte und messbare Weise weiterentwickeln kann.

# 7. So hilft Actalis (europäisches QTSP)

Actalis fungiert in einer doppelten strategischen Rolle: einerseits als **europäische Certification Authority** für **TLS/SSL-, S/MIME**- und **Code Signing-**Zertifikate und **aktives Mitglied des CAB Forum SSL**, andererseits als **Qualified Trust Service** Provider (QTSP) gemäß der e**IDAS 2-Verordnung**, wodurch eine strategische Governance bei der Erbringung konformer und sicherer Vertrauensdienste gewährleistet wird.

In dieser Position begegnet Actalis dem Übergang zur **Post-Quanten- Kryptografie** mit einem integrierten Ansatz, der den wichtigsten europäischen und internationalen Vorschriften und technischen Standards im Bereich der Cybersicherheit entspricht.

Es handelt sich um einen **Lab-First-Ansatz**: erst testen, dann ausweiten.

Das **PQC Lab** (Beta) bietet eine kontrollierte Umgebung zum Ausstellen und Überprüfen von Hybridzertifikaten, zum Linting von X.509-Ketten und zum Messen der Latenz und Interoperabilität bei gängigen Anwendungsfällen (TLS/mTLS, S/MIME, Code-Signing).

Unsere **Methode in 30 Tagen**:

1. Eine strukturierte Bestandsaufnahme, um Umfang und Prioritäten zu definieren;
2. Ein Quick Scan des Kryptografie-Inventars und der langlebigen Daten;
3. Ein Pilotplan mit Metriken und Rollback;
4. Zugang zum PQC Lab, um hybride Zertifikate zu generieren und zu validieren;
5. Ein Bericht, um in aller Ruhe zu entscheiden, ob man skalieren oder den Kurs korrigieren möchte.

### Actalis PQC Lab (Beta)

- Ausstellung und Überprüfung von Hybridzertifikaten
- Linting von Ketten und grundlegende Konformitätsprüfungen
- Interoperabilitäts- und Latenztests anhand realer Anwendungsfälle

(Spezifikationen und Nutzungsbeschränkungen auf Anfrage erhältlich; Schwerpunkt EU)

➜ ***Erster Schritt, minimaler Aufwand. Ein gut konzipiertes Pilotprojekt ist mehr wert als hundert Slides.***

# 8. Häufig gestellte Fragen (nicht technischer Art)

### Müssen wir sofort alles ändern?

Nein. Die Priorität liegt darin, die Vertraulichkeit und den Schutz der Daten mittel- bis langfristig zu gewährleisten. Der hybride Ansatz ermöglicht es, Maßnahmen zu ergreifen, ohne den Betrieb zu unterbrechen.

### Werden sich die Standards weiter ändern?

Mit Sicherheit, und das ist auch schon vorgesehen: Sie werden sich jedes Mal ändern, wenn ein potenzielles Risiko besteht. Aus diesem Grund ist Krypto-Agilität erforderlich: Die Entwicklung von Prozessen und Plattformen, die sich im Laufe der Zeit kontinuierlich weiterentwickeln können.

### Sind die Auswirkungen auf die Endnutzer erheblich?

Bei internen Pilotprojekten mit Feature-Flags und einem definierten und getesteten Rollback-Plan sind die Auswirkungen minimal. Eine Ausweitung erfolgt nur, wenn die Erkenntnisse fundiert sind.

### Können wir warten, bis alles definiert ist?

Warten erhöht das HNDL-Risiko für bereits gesammelte Daten. Ein früher Start ermöglicht kontrollierte Kosten und Risiken.

# 9. Hinweise und Referenzen auf EU-Ebene (nicht rechtlich)

Dieses Dokument ersetzt keine Rechtsberatung.

Aus Sicht der EU ist Folgendes zu berücksichtigen:

- die Integration des HNDL-Risikos in das Risikomanagement und die Supply-Chain gemäß dem NIS2-Rahmen;
- der Schutz der Vertrauenskette im Rahmen von eIDAS2, wobei während des Übergangs zwischen Bereichen des öffentlichen Vertrauens und des privaten/unternehmerischen Vertrauens unterschieden wird;
- die Verwendung der von ETSI und ENISA veröffentlichten bewährten Verfahren zur Festlegung von Grundsätzen, Bestandsaufnahmen und Migrationsplänen.

Für die Anwendung in Ihrer Branche/Ihrem EU-Land empfehlen wir Ihnen, Ihre Compliance-Abteilung und Ihre vertrauenswürdigen Berater hinzuzuziehen.