Quantum-Safe: perché muoversi adesso in Europa e come farlo senza bloccare l’operatività

Una guida pratica per CISO, IT e Business Leader su rischi, approcci ibridi e roadmap “EU-ready”.

Executive summary

Immagina una cassaforte perfettamente chiusa oggi che, tra qualche anno, si apra da sola perché è cambiata la tecnologia delle chiavi. È questa l'essenza della **minaccia Harvest-Now, Decrypt-Later (HNDL)**: aggressori informatici che intercettano e conservano oggi dati cifrati — email, backup, traffico applicativo, scambi B2B — per decifrarli un domani quando i progressi degli eleboratori , inclusi quelli quantistici, renderanno accessibili attacchi oggi impraticabili.

Non serve allarmismo: serve programmazione.

La risposta più pragmatica è l'approccio ibrido: introdurre certificati, chiavi, algoritmi e protocolli che combinano componenti crittografiche classiche con componenti post-quantum (PQC). L'approccio ibrido consente di proteggere i dati fin da subito, per quei sistemi che implementano la PQC, , senza impatti sui sistemi e sui processi esistenti.

Nel contesto europeo, il rinnovato framework di sicurezza informatica, tra cui i Regolamenti Europei NIS2, eIDAS2, il Cyber Resilience Act, e gli standard tecnici ETSI ed ENISA, spinge verso una gestione del rischio strutturata e focalizzata anche sulle possibili vulnerabilità delle attuali metodologie crittografiche.

Questa roadmap delinea un percorso di **18 mesi** in cui, nella fase iniziale, prevediamo di realizzare dei pilot misurabili all'interno di ambienti demo e controllati. Questi primi esperimenti ci aiuteranno a capire dove il rischio del quantum computing è davvero significativo e, grazie ai risultati ottenuti, potremo poi estendere e standardizzare l'approccio in modo sicuro e strutturato.

Actalis, come QTSP (**Qualified Trust Service Provider**) europeo e Certification Authority nell'ecosistema dei certificati SSL, mette a disposizione un **approccio lab-first** — strumenti, metodi e supporto — per accompagnare imprese e Pubbliche Amministrazioni nella transizione a tecnologie quantum-safe.

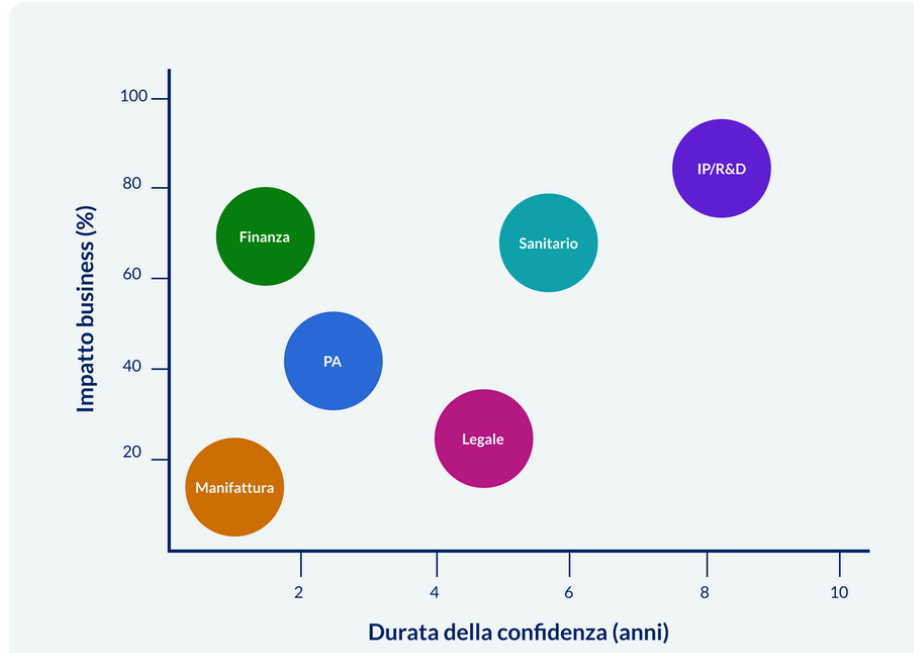
➜ ***Non è una rivoluzione notturna ma un programma. Chi inizia oggi riduce l'esposizione al rischio HNDL sui dati e si prepara a evolvere senza traumi.***

1. Capire il rischio: HNDL spiegato bene

Nel quotidiano aziendale la cifratura è invisibile: l'icona del lucchetto nel browser, un certificato sul server, una policy sull'archiviazione di dati e documenti. È facile pensare che "se oggi funziona, funzionerà anche domani".

Il problema è l'orizzonte temporale: molte informazioni devono restare segrete o protette per anni o anche decine di anni (cartelle cliniche, documenti finanziari, dossier legali, IP industriale, strategie di M&A, dati fiscali, piani di prodotto). Se un attaccante raccoglie e conserva oggi il traffico dati o gli archivi informatici cifrati con le attuali metodologie, potrà tentarne la decrittazione quando si cominceranno ad utilizzare calcolatori quantistici affidabili e abbastanza potenti che determineranno il punto di non ritorno. L'effetto non è immediato, ma differito: una breccia potenziale che si apre nel futuro, con danni che si materializzano quando la reazione è ormai impossibile.

Comprendere HNDL significa leggere il rischio come prodotto tra probabilità e impatto nel tempo. La probabilità cresce man mano che la tecnologia progredisce; l'impatto dipende dal valore, dalla durata e dalla confidenzialità del dato cifrato. Per questo non tutti i sistemi informatici hanno la stessa priorità: un'informazione pubblica non è un problema; un progetto di R&D o un fascicolo sanitario lo sono.



60 secondi su HNDL

- Non è "domani cade tutto". È un rischio differito che colpisce i dati che devono rimanere segreti o confidenziali nel medio-lungo periodo.
- La priorità è proteggere oggi ciò che deve restare riservato per anni.

2. Che cos’è la Post-Quantum Cryptography

La **Post-Quantum Cryptography** (PQC) è una branca della crittografia che sviluppa algoritmi crittografici progettati per resistere agli attacchi dei computer quantistici, che avranno una potenza di calcolo molto superiore a quella dei computer classici . Non è una tecnologia “magica” né sostituisce tutto in un colpo solo: è il nuovo set di attrezzi con cui costruire, gradualmente, servizi e protocolli più resilienti.

La via realistica non è buttare via l’esistente, ma adottare **soluzioni ibride**, in cui una componente classica e una componente post-quantum co-esistono nello stesso certificato o nello stesso protocollo. In pratica, si ottengono due vantaggi: (1) Compatibilità con server e librerie attuali; (2) Resilienza nel tempo, perché l’elemento PQC offre una protezione aggiuntiva su dati riservati nel medio-lungo periodo.

Per far funzionare l’ibrido serve implementare soluzioni che consentiranno, in futuro, di sostituire chiavi e algoritmi in tempi rapidissimi, senza impatti su tutti gli applicativi.

L'approccio ibrido e la cryprto-agility, quindi, sono due soluzioni da poter applicare in parallelo in modo indipendente.

➜ ***Difendersi bene oggi significa saper cambiare domani. La vera assicurazione è l’agilità crittografica, non l’algoritmo perfetto.***

Cos’è un certificato ibrido

Un certificato ibrido combina una componente crittografica classica e una componente crittografica resistente agli attacchi di computer quantistici. Per l’utente finale nulla cambia; per l’architettura significa continuità operativa oggi e resilienza domani.

3. La prospettiva europea: rischio, fiducia e filiera

L'Europa sta accelerando sulla crittografia post-quantum, definendo un framework regolamentare che guiderà imprese e la Pubblica Amministrazione europea nella transizione verso tecnologie "quantum-safe".

Il nuovo Regolamento eIDAS2 richiede ai Prestatori di Servizi Fiduciari, come Actalis, di adottare le migliori soluzioni crittografiche ad oggi disponibili, aprendo la strada all'integrazione di algoritmi resistenti ai computer quantistici.

In parallelo, la Direttiva NIS 2 impone a tutti i settori critici una gestione strutturata del rischio digitale, includendo la revisione delle dipendenze crittografiche e la pianificazione della migrazione PQC.
Le linee guida ENISA e gli standard tecnici ETSI offrono già oggi raccomandazioni operative e profili tecnici per l'adozione di schemi post-quantum e soluzioni ibride, facilitando una transizione graduale e interoperabile.

L'insieme di questi regolamenti e standard tecnici crea un percorso chiaro: mappare tutti gli asset crittografici, introdurre algoritmi quantum-safe in modo progressivo e garantire continuità, sicurezza e conformità ai servizi erogati anche nello scenario di nuove minacce emergenti.

Per aziende e amministrazioni, investire ora nella transizione alla crittografia post quantum significa rafforzare la compliance e garantire la resilienza di lungo periodo dei propri servizi digitali.

➜ ***Tre verbi UE: Pianificare. Documentare. Dimostrare. La cyber-resilienza è un percorso di governance, non solo di cifratura.***

Nota importante

Questa sezione è informativa e non sostituisce una consulenza legale. Per la corretta applicazione dei requisiti specifici alla vostra organizzazione e al vostro Paese UE rivolgetevi a consulenti esperti.

4. Perché l’ibrido è la via pratica e prudente

L’industria digitale ha imparato a proprie spese che i big-bang tecnologici sono rischiosi. L’ibrido permette di inserire PQC a piccole dosi dove serve, mantenendo compatibilità e governabilità:

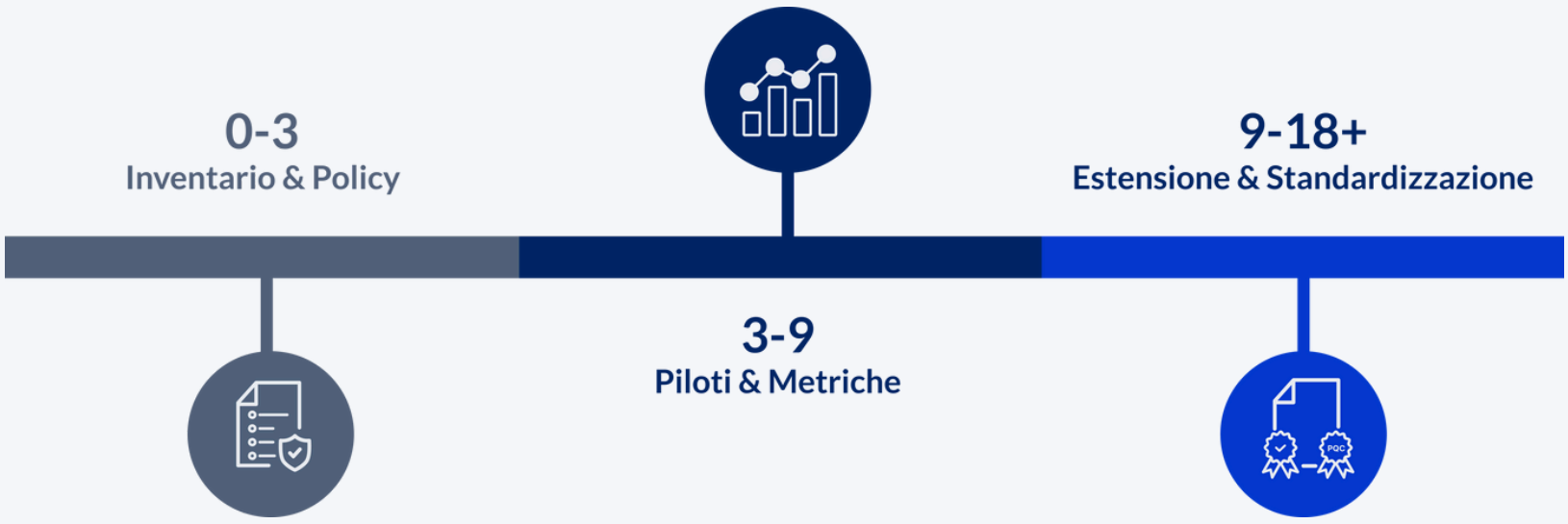
- continuità per gli utenti,
- riduzione del rischio HNDL sui dati longevi,
- controllo tramite progetti pilota circoscritti
- piani di rollback definiti e testati
- e un allineamento organizzativo che mette a terra policy e ruoli di crypto-agility.

➜ ***Evitare il lock-in tecnico. Progettare oggi la possibilità di cambiare domani è il modo migliore per non restare indietro***

Tre domande prima di partire

1. So dove la cifratura conta davvero nel tempo?
2. Ho metriche semplici per misurare impatto e compatibilità?
3. Il mio piano di rollback è chiaro, provato e rapido?

5. Una roadmap “EU-ready” in 18 mesi



La nostra roadmap si articola in tre fasi. L’obiettivo è arrivare a progetti pilota ibridi in produzione controllata.

Fase 1

0–3 mesi: capire e decidere

La prima fase punta a illuminare il perimetro e scegliere dove partire.

Si avvia un **inventario crittografico** concreto: certificati in uso, librerie TLS, gateway e-mail, API e integrazioni B2B, dispositivi e componenti OT, archivi a lungo termine. Non è un esercizio teorico: serve a collegare dati, canali e dipendenze.

Si **classificano i dati a lunga vita**, identificando processi, fornitori e punti di esposizione. Incrociando durata della confidenzialità, criticità di processo ed esposizione emergono poche aree ad alta priorità.

Infine, si **definiscono i principi di crypto-agility**: architettura delle soluzioni di crittografia, rotazioni, estensioni X.509, flussi di change, ruoli e responsabilità.

La fase si chiude con **report di inventario**, matrice rischio/priorità e bozza di policy.

➜ ***Regola 80/20. Il 20% di dati e canali genera l’80% del rischio lungo termine. Inizia da lì***

Fase 2

3–9 mesi: piloti misurabili in produzione controllata

Il pilota è reale ma circoscritto:

- un dominio non customer-facing per mTLS/API con certificati ibridi;
- un reparto ad alta sensibilità (es. legale) con S/MIME ibrido;
- e, se applicabile, un code-signing ibrido sulla pipeline di build
- la sottoscrizione di documenti a valore legale (firma digitale)
- le connessioni sicure (esempio reti private virtuali)
- la cifratura dei dati a riposo
- i processi di autenticazione.

Per ogni pilota si definiscono metriche semplici (latenza di handshake, errori, compatibilità, impatto operativo) e si adottano feature-flag e canary release per avanzare o tornare indietro in sicurezza.

Il valore vero sta nel documentare evidenze utilizzabili per la decisione.

➜ ***Piccolo, reale, misurabile. Un buon pilota produce evidenze, non opinioni.***

Fase 3

9–18+ mesi: estendere, standardizzare, contrattualizzare

Con le evidenze in mano, si estende in modo graduale: prima domini a bassa esposizione utente, poi servizi più critici.

Si standardizzano policy, playbook, CMDB, criteri di procurement e modelli di incident legati alla componente crittografica.

Si affronta la supply chain aggiornando contratti e SLA con requisiti minimi di crypto-agility, tempistiche di adeguamento e reportistica.

Infine, formazione e comunicazione trasformano la transizione in routine operativa.

KPI per la direzione

- % di asset con profilo crittografico noto
- % di canali “quantum-ready” (dal pilota all’esteso)
- Tempo medio di rollback senza disservizi
- % di fornitori con clausole crypto-agili aggiornate

➜ ***Dalla prova al programma. La transizione riesce quando entra nel ciclo di vita dei servizi, non come progetto una tantum.***

6. Che cosa cambia davvero per l'organizzazione

Il cambiamento non è solo tecnologico: è culturale e operativo.

La gestione del cambiamento (CAB, finestre, piani di test, reversibilità) diventa l'asse portante. Il budget si sposta dal comprare prodotti a mettere a terra processi e competenze: assessment, pilot, formazione, automazioni del ciclo certificati e delle chiavi crittografiche.

Le persone sono centrali: la crypto-agility richiede lavoro di squadra tra Security, Architetture, DevOps, Legal e Procurement.

I fornitori vanno valutati anche sulla loro roadmap: sanno accompagnare su ibrido e PQC? Hanno strumenti per test, linting, verifica di catena e inter-operabilità? Offrono modelli di supporto coerenti con i vostri SLA?

In sintesi: il valore sta nel dimostrare che l'organizzazione sa evolvere in modo controllato, documentato e misurabile.

7. Come aiuta Actalis,QTSP europeo

Actalis opera con un doppio ruolo strategico: da un lato come **Certification Authority europea** per certificati **TLS/SSL, S/MIME e Code Signing e membro attivo del CAB Forum SSL**, dall'altro come **Qualified Trust Service Provider (QTSP)** ai sensi del **Regolamento eIDAS 2**, garantendo una governance strategica nell'erogazione di servizi fiduciari conformi e sicuri.

In questa posizione, Actalis affronta la transizione verso la **crittografia post-quantum** adottando un approccio integrato e conforme ai principali regolamenti e standard tecnici europei ed internazionali in ambito di cybersicurezza.

Si tratta di un **approccio lab-first:** prima si prova, poi si estende.

Il **PQC Lab** (beta) offre un ambiente controllato per emettere e verificare certificati ibridi, eseguire linting delle catene X.509, misurare latenza e inter-operabilità su casi d'uso comuni (TLS/mTLS, S/MIME, code-signing).

Il nostro **metodo in 30 giorni**:

- una discovery strutturata per delineare perimetro e priorità;
- un quick scan dell'inventario crittografico e dei dati a lunga vita;
- un pilot plan con metriche e rollback;
- l'accesso al PQC Lab per generare e validare certificati ibridi;
- un report per decidere con serenità se scalare o correggere la rotta.

Actalis PQC Lab (beta)

- Emissione e verifica di certificati ibridi
- Linting di catene e controlli di conformità di base
- Test di inter-operabilità e latenza su casi d'uso reali

(Specifiche e limiti d'uso disponibili su richiesta; focus UE.)

➜ ***Primo passo, minimo sforzo. Un pilot ben progettato vale più di cento slide.***

8. Domande frequenti (non tecniche)

Dobbiamo cambiare tutto subito?

No. La priorità è preservare la riservatezza e la confidenzialità dei dati nel medio-lungo periodo. L'approccio ibrido permette di intervenire senza fermare l'operatività.

Gli standard cambieranno ancora?

Sicuramente, ed è già previsto: cambieranno ogni volta che vi sarà un potenziale rischio. Per questo motive serve crypto-agility: progettare processi e piattaforme che possano evolvere continuamente nel tempo.

L'impatto sugli utenti finali è rilevante?

Se i progetti pilota sono interni, con feature-flag e piano di rollback definito e testato, l'impatto è minimo. L'estensione avviene solo quando le evidenze sono solide.

Possiamo aspettare che tutto sia definito?

Aspettare accumula esposizione HNDL sui dati già raccolti. Iniziare presto consente costi e rischi controllati.

9. Note e riferimenti UE (non legali)

Questo documento non sostituisce una consulenza legale.
In ottica UE, è necessario considerare:

- l'integrazione del rischio HNDL nella gestione del rischio e nella supply-chain prevista dal quadro NIS2;
- la tutela della catena di fiducia nel perimetro eIDAS2, distinguendo tra ambiti di public trust e private/enterprise trust durante la transizione;
- l'uso delle buone pratiche pubblicate da ETSI ed ENISA per impostare policy, inventari e piani di migrazione.

Per l'applicazione al vostro settore/Paese UE, vi invitiamo a coinvolgete Compliance e i vostri consulenti di fiducia.