QuSecure + Sabadell

Case Study

Four Months. One Pilot. Zero Disruption. The Quantum Migration Blueprint Financial Services Needed

2026

QuSecure + Sabadell

Banco Sabadell piloted new quantum standard encryption and crypto agility leveraging QuProtect R3™ in a lab environment replicating their customer-facing web infrastructure – proving feasibility and zero disruption in four months.

The US Security and Exchange Commission cited it as 'a benchmark for industry-wide adoption strategies.'

The Strategic Context

While most financial institutions are still debating when to address quantum threats, Banco Sabadell took action. The Spanish global bank recognized that waiting for regulatory mandates would leave them reactive, resource-constrained, and vulnerable. Instead, they chose to pilot post-quantum cryptography (PQC) migration now – controlling the timeline, learning on their terms, and positioning themselves as industry leaders.

The decision proved prescient. The Securities and Exchange Commission's Post-Quantum Financial Infrastructure Framework (PQFIF) specifically cited Banco Sabadell's pilot as the stand alone "Real-World Implementation Precedent" of practical PQC implementation. The engagement proved the ability to solve real business challenges and the SEC deemed it "a benchmark for industry-wide adoption strategies."

In collaboration with Accenture, the pilot focused on a single but critical application: the bank's customer-facing web portal, proving that organizations don't need to boil the ocean before they start. By replicating production infrastructure in a controlled lab environment, Banco Sabadell could validate feasibility without production risk.

Why This Matters Now

The quantum threat is no longer theoretical, and regulators are taking notice. FS-ISAC, SEC, PCI DSS v4.0, NIST, and SWIFT CSP are all signaling expectations. More importantly, the greatest business risk is not a future quantum computer, it is the slow spread of cryptographic sprawl that has taken over networks where vulnerabilities hide.

> "Cryptography plays a crucial role in banking, securing processes such as payments, digital interactions with customers and communications with market infrastructure. It is also essential for protecting sensitive information. As we transition into a post-quantum computing era, the challenges include identifying the use of cryptographic methods vulnerable to quantum attacks and transitioning to quantum-safe cryptography with agility and efficiency."
>
> Joan Puig, Group CISO of Banco Sabadell

Financial Services Leaders Face Three Converging Pressures

- **Security Exposure**
  Hidden cryptographic vulnerabilities across complex infrastructure that AI-driven attacks are already exploiting
- **Regulatory Momentum**
  Industry frameworks signaling imminent compliance requirements
- **Operational Constraints**
  Critical systems that cannot tolerate disruption during migration

Banco Sabadell addressed all three of these pressures simultaneously with QuProtect R3.

QuSecure + Sabadell

What They Did

In collaboration with QuSecure and Accenture, Banco Sabadell conducted a four-month PQC pilot using QuProtect R3—the only production-ready platform that enables the kind of cryptographic agility Forrester Research recommends.

The pilot focused on customer-facing infrastructure: a lab replica of the bank's main web portal where customers access accounts. The team updated encryption protocols to NIST quantum-safe algorithms and tested all FIPS 203 candidates, including the Kyber algorithm Key-Encapsulation Mechanism (the standards had not been released at the time of the pilot).

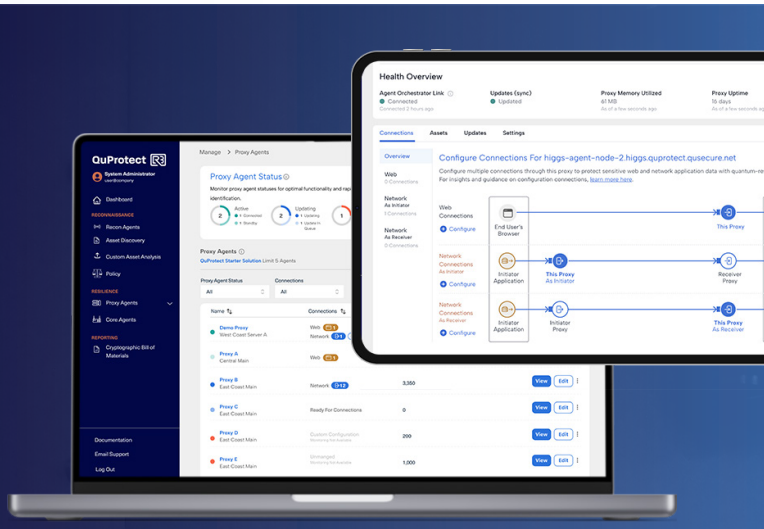
Methodical Approach

Applying Protection
Using the QuProtect Resilience module for Web App Security, a proxy agent was placed as close as logically possible to the web application being protected.

Updating Encryption
Administrators used a graphical interface to change cryptographic algorithms to quantum-safe versions without command-line complexity, no specialized expertise required.

Testing Comprehensively
The team tested all NIST round 4 candidate algorithms available at the time, including FIPS 203 Kyber, to understand performance characteristics and optimize for their environment.

Measuring Impact
QuSecure, Accenture, and Banco Sabadell built a testing methodology to measure performance impacts on operational continuity, with full control over algorithms and the ability to run performance tests using different TLS variations.



Measurable Impact

The engagement was featured in the SEC's Post-Quantum Financial Infrastructure Framework guidance document as well as the World Economic Forum's 2025 report on Quantum Technologies in Financial Services.

"This pilot project demonstrates that migration to post-quantum cryptography is both technically feasible and operationally practical for major financial institutions, providing a benchmark for industry-wide adoption strategies."

SEC PQFIF Report

Demonstrated Speed of Deployment
Four months to complete a PQC pilot under real-world conditions within existing infrastructure frameworks

Crypto Agility Realized
In a matter of clicks, the Banco Sabadell team executed updates to PQC, applying different TLS versions for ideal posture within their complex environment.

Support For Industry Standards
Updated to NIST quantum-safe algorithms with no system overhaul

Performance Validation
Testing proved minimal performance impact throughout the pilot period

QuSecure + Sabadell


U.S. Securities and Exchange Commission

MENU

More in this Section

CTF WRITTEN SUBMISSION

Post-Quantum Financial Infrastructure: A Roadmap for the Quantum-Safe Transition of Global Financial

- The framework aligns with U.S. federal directives including NSM-10, the Executive Order of January 2025, and CNSA 2.0, mandating a full migration to post-quantum cryptography (PQC) by 2035 for federal systems, with implications for financial institutions handling sensitive or investor-related data.

Securities and Exchange Commission (SEC) highlights Banco Sabadell's pilot with QuSecure and Accenture as a blueprint for addressing the PQC migration.

The SEC's Post-Quantum Financial Infrastructure Framework (PQFIF) guidance document

Banco Sabadell: Undertook four-month project to explore PQC adoption, focusing on crypto agility

Implementation Results:

- Successful integration of quantum-resistant algorithms
- Maintained operational continuity throughout pilot period
- Established clear roadmap for full-scale quantum-safe transition

Industry Impact:

This pilot project demonstrates that migration to post-quantum cryptography is both technically feasible and operationally practical for major financial institutions, providing a benchmark for industry-wide adoption strategies.

SEC Highlight

When the SEC featured Banco Sabadell's pilot in their Post-Quantum Financial Infrastructure Framework, they were answering the question keeping financial services leaders paralyzed: Can we actually do this without breaking everything?

Most institutions have been stuck between competing fears—quantum-enabled attacks versus massive infrastructure disruption during migration. They're waiting for someone else to prove it's possible without catastrophic operational risk.

Why This Became a Benchmark

The SEC spotlighted three breakthrough findings:

Feasibility within existing infrastructure
Organizations don't need to "rip and replace" their entire technology stack. Quantum-safe encryption works within current infrastructure frameworks—fundamentally changing the cost and complexity equation.

Network-layer solutions as the unlock
By updating encryption at the network layer rather than rewriting applications, Banco Sabadell showed a path that doesn't require massive developer resources or years of modernization.

Practical crypto-agility in action
The ability to switch algorithms quickly and optimize security-performance balance in real-time worked in the messy reality of complex banking environments, pushing beyong testing laboratory conditions.

The SEC concluded this pilot "demonstrates that migration to post-quantum cryptography is both technically feasible and operationally practical for major financial institutions, providing a benchmark for industry-wide adoption strategies."

That language matters. The SEC wasn't just validating what one bank accomplished—they were telling the industry: this is how you should think about solving this problem.

QuSecure + Sabadell

What This Means For Financial Institutions

Banco Sabadell's pilot provides a replicable blueprint that dispels three common assumptions:

MYTH ONE **Migration takes years and requires massive infrastructure overhauls**	Banco Sabadell validated feasibility in four months in a lab environment replicating production infrastructure—proving you can test without production risk.
MYTH TWO **We need complete inventory and a perfect plan before starting**	The pilot approach let Banco Sabadell learn while testing, developing their roadmap based on real evidence rather than theoretical projections.
MYTH THREE **Performance impacts will degrade customer experience**	Testing proved minimal impact, with administrators able to fine-tune the security-performance balance in real-time using different TLS variations.

The Market Leadership Opportunity

PQC Adoption Advantages Today:

- **Strategic Positioning**
  Demonstrated quantum readiness becomes a differentiator with customers, partners, and regulators. When peers scramble to start, be ready with protection and agility.
- **Real Remediation of Risk**
  Early identification and remediation of cryptographic vulnerabilities before they are exploited. QuProtect R3™ is the only production ready, unified platform that enables the immediate remediation of crypto risks on your network as soon as they are discovered.
- **Regulatory Advantage**
  Proactive compliance posture versus reactive scrambling when mandates arrive. The SEC and WEF's recognition of Banco Sabadell shows regulators value early movers.
- **Operational Learning**
  Time to build internal capabilities and refine processes without crisis pressure. Banco Sabadell's team now understands what full-scale migration requires.
- **Cost Control**
  Pilot-based approach allows measured investment and resource allocation. Test hypotheses before committing to enterprise-wide rollouts.

Proof of Performance

The pilot went beyond performance testing the latest algorithms for securing data in transit, validating a new approach to cryptographic control and a replicable methodology for financial institutions.

Administrators had full control over the algorithms employed to secure communications, with the capability to run performance tests using different TLS variations. This enabled them to optimize the balance between security and performance impact on application communications.

The R3 admin console provided additional monitoring capabilities, giving Banco Sabadell's technical team valuable insights into connection performance and security posture that they could corroborate with their own tests.

Testing proved minimal performance impact on application communications throughout the pilot period, validating that quantum-safe encryption doesn't require sacrificing user experience.

QuSecure + Sabadell

Industry Take Aways

Banco Sabadell's pilot with QuProtect R3™ solved the real cryptographic challenges every bank faces. The SEC recognized this methodology as best practice for the financial sector, and the proof points from their pilot translate directly into action for your organization.

What Banco Sabadell Proved

- PQC implementation is feasible within existing infrastructure frameworks
- Network-layer encryption solutions enable quantum-safe standards without complete system overhaul
- Crypto agility approaches demonstrate practical viability for complex banking environments

What This Means For BFSI

These findings remove the barriers that keep organizations paralyzed. You can now:

Act swiftly to pilot

Transform uncertainty into an actionable, risk-based plan that prioritizes your most critical systems for early testing. Lab environments enable validation without production risk, just as Banco Sabadell did.

Ensure compliance and auditability

Start building evidence of progress before mandates hit. Regulators will demand verifiable action, and early pilots demonstrate strategic foresight.

Move forward with confidence

Banco Sabadell validated PQC feasibility in complex banking infrastructure in months rather than years, while respecting resource constraints and performance requirements.

Next Steps

The time for admiring the PQC problem has passed – standardization and regulatory pressure has already been implemented and will only intensify.

To explore how QuSecure can help your organization test quantum-safe encryption without disruption, visit our Banking and Finance page or connect with us to schedule a demo.

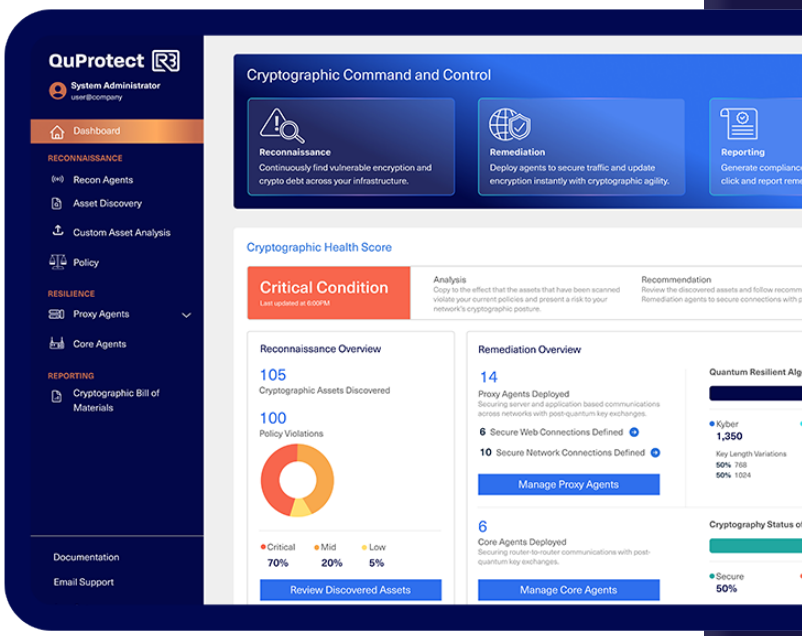
Credits

[The Architect's Guide to Quantum Security, Forrester Research, 2025]

[The SEC's Post-Quantum Financial Infrastructure Framework (PQFIF) guidance document]

[Banco Sabadell Collaborates with Accenture and QuSecure to Advance Quantum Safe Infrastructure]

[WEF Quantum Technologies Key Strategies and Opportunities for Financial Service leaders 2025]



QuSecure
+1 (650) 356-8001
info@qusecure.com
www.qusecure.com