



BANKING AND FINANCE

Protecting your organization's future. Today.

QuSecure



Helping a large financial institution secure their sensitive customer data

A large financial services organization is in the process of building a secure document management and transactional platform to provide a single, enterprise-wide, quantum-resilient file and data transfer platform serving information from internal systems to both employee and external customers and partners.

QuSecure is engaged to deliver post-quantum protections to the organization's new secure portal.

The challenge

The challenge is to deploy a security solution which addresses a number of customer concerns and priorities:

- Deployment of certified, industry-accepted, and validated cryptography, including risk-mitigation by deploying candidate NIST Post-Quantum Cryptographic algorithms in a crypto-agile implementation
- Integration with identity and access management (IAM), key management (KMS), policy, and Security Information and Event Management (SIEM) systems
- Simple integration with existing platforms and processes with minimal disruption, cryptography control, auditability, and monitoring and remediation
- Enables upgrades to future cryptographic algorithms (future-proofing against upcoming attacks on cryptography)

The customer needs seamless deployment without service interruption so that users can continue to access data throughout the upgrade and the overall customer experience is not negatively impacted.

Our Approach

To fully address the customer's needs, QuSecure architected an end-to-end solution complete with:

- Supported, staged integration – working with the customer to implement targeted upgrades through test, approval, and staged rollout
- Standard product deployment (not a customized product) that facilitates simple integrations and compliance, and scalability to meet future demand
- Close attention to existing systems, network, and platform types and capacity requirements ensuring minimal, if any, impact to network performance
- Engagement with the customer's compliance and certification teams, to ensure the protection regulatory programs are supported and strengthened from the start
- Tight administrative and operational integration so the system is easy on the IT security team

Ready for today. And tomorrow.

The result was a rapidly implemented quantum-grade security solution that seamlessly integrated with the organization's existing infrastructure – offering protection from the quantum threat today and in the future.

Key benefits of our solution

- ✓ Efficient Zero-Trust Quantum Resilient Communication
- ✓ Quantum Driven Data at Rest Protection
- ✓ Cryptographic Agility By Design
- ✓ Comprehensive and Direct Integration with Application and Device Support
- ✓ Multi-Cloud and On-Prem Deployable



TEAM MEMBER SPOTLIGHT

Skip Sanzeri
Board Chair – COO, QuSecure

Skip is an accomplished entrepreneur and finance executive completing over half a dozen successful exits including one IPO. Skip also co-authored The Quantum Design Sprint which outlines methodologies to develop quantum computing applications.

“It is likely that a quantum computer will exist within the next decade that will be able to crack today's public key cryptography. [Everyone that relies] on public key cryptography will therefore need to transition to security protocols that quantum computers can't crack.”

Morgan Stanley,
Oct 2020

Quantum-grade security.

For today's financial organizations.



The quantum threat to today's banking and financial organizations is real, but preventable. Find out why you need to act today.

With the ability to simulate highly complex systems and interactions, the game-changing capabilities of quantum computers will provide an easy avenue for criminals and other adversaries to steal your data and exploit your organization.

Store Now, Decrypt Later (SNDL) is a common cyber attack where a bad actor will harvest an encrypted data source with the expectation of being able to decrypt it in the future. Once decrypted, it will be distributed or sold on the dark web, compromising the confidentiality and integrity of an organization's digital assets and information. For today's banking and finance organizations, the security and compliance risks are high. As we accelerate towards a cashless society, banking and financial organizations face an increasing number of cyber attacks due to interconnected attack surfaces, ransomware, emerging technologies such as deepfakes and 5G, and malware attacks that spur multiparty and cross-sector targeting.

In response, QuSecure has developed QuProtect™ – a robust all-in-one software-based quantum security solution that's quick to implement and effortless to manage. Highly compatible with today's technologies, and easily integrated across various devices, QuProtect offers a powerful and seamless solution, so that banks and financial organizations are ready for today. And tomorrow.

QSMS Key Features

100% standards based & compliant

Including NIST & FedRAMP to provide trusted delivery of post-quantum resilience

Minimal to zero client-side installs required

Seamlessly upgrades managed and non-managed endpoints and devices, achieving BYOD encryption compliance

Easily integrated

Designed to be simple to deploy, operate and manage

Low-risk

Software-based solution optimized for the smallest changes with minimal disruption

Solves staged upgrade problems

Policy controlled backwards compatibility allows upgrades to be staged over time

Fully protects data

Delivers an end-to-end, zero trust oriented solution

Resilient to attack

Searches out and resolves attacks through deep instrumentation, ML-based threat and attack analytics, countermeasure deployment and remediation

Maximum Protection

Strengthened encryption with a quantum entropy source

Protects data at rest and in transit

Built-in legacy support

High availability and reliability with self-healing

Active monitoring and remediation of threats

Policy-based controls

Zero trust architecture

Are you ready?
Contact us today

Set up a 15 min intro call 

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

