Quintessence Labs

SOLUTION GUIDE

Banking Solution Guide

The financial industry is anchored by strong information technology — sophisticated networks, incisive data analytics and customer-friendly internet services drive growth in this sector. This reliance on technology naturally calls for trustworthy data security that can handle ever-growing threats and constantly changing business environments and needs.

Business Situation

One of the toughest data security challenges is also the most important: effectively protecting data through encryption. Are encryption keys strong enough? Are they safely stored? Can different protocols be managed, as well as practical policies for effective operations? It's a large and complex challenge that demands sophisticated management capability.

Another obstacle is ensuring seamless end-to-end protection across the whole infrastructure. Large banks are made up of different business units with offices in various locations, often with security systems from multiple vendors in service for years if not decades. Replacing long-standing systems can be hard, but so can integrating them organization-wide. Failures to integrate can lead to siloed data protection that makes the information between systems vulnerable.

> "...The transformation underway in many banks is largely technology-driven [and] they should ensure cyber risk is explicitly considered and managed in every aspect..."
>
> *— Deloitte 2018 Banking Industry Outlook*

Financial organizations must stay compliant with industry and government regulations, especially when those regulations include cybersecurity mandates. Much discussion was made around the EU's General Data Protection Regulation (GDPR), but others remain on the radar for banks, such as China's Cybersecurity Law and New York's 23 NYCRR 500.

Clearly there's increased need inside and outside banks to have robust security plans with compliant networks comprising robust hardware and software. With QuintessenceLabs' cybersecurity products, enterprises can operate at their best without compromise. We make some of the fastest, most cost-competitive security products in the market that tackle all these challenges with best-in-class data protection strengthened by quantum-based technology, and encryption key and policy management to secure information now and in the future.

True Random Number Generation for the Strongest Keys

Using strong cryptographic keys is crucial in protecting data through encryption, but the deterministic, algorithm-based methods of generating randomness traditionally in use can be vulnerable to attacks, with the risk increasing as computing power grows stronger, in particular with the development of quantum computers.

qStream™: The Power of Quantum

QuintessenceLabs is unique in offering banking customers the security of high-speed true random numbers to strengthen their data protection. The qStream™ quantum random number generator (QRNG) solutions use a QRNG to generate perfectly unpredictable random numbers for use in all security applications. It works by measuring an effect called quantum tunneling, whereby electrons tunnel through an electrical barrier in an unpredictable way. The resulting random numbers are then delivered through networks at up to 1 Gbit/sec, a rate well suited to cost-effective centralized deployment in large firms, ensuring the highest-quality encryption keys, and delivering a stronger security posture.

The qStream™ 200 quantum random number generator (QRNG) is a rackmount appliance with a built-in QRNG and administration software; the qStream™ 100 quantum random number generator (QRNG) is delivered as a standalone PCIe card for use in your own appliance.

KMIP-Conformant Key Management

The challenge of storing and managing encryption keys across an enterprise is often exacerbated by vendor systems with proprietary protocols, which could can to costly retrofits or other workarounds.

The OASIS Key Management Interoperability Protocol (KMIP), is a set of industry standards that addresses issues with key management compatibility and upgrades. Today, enterprises look for solutions that test well against the KMIP standards, and QuintessenceLabs is among the cybersecurity firms that ensure conformant products.

TSF®: Enterprise-Level Key Management

The Trusted Security Foundation® (TSF®) appliance is QuintessenceLabs' key management solution, interoperable with our other devices and third-party solutions, enabling a centrally managed, integrated solution. The TSF key and policy manager can be deployed as a virtual machine or dedicated appliance, the latter enhanced with an embedded FIPS 140-2 Level 3 hardware security module (HSM) and True Random Number generator.

The TSF key and policy manager handles keys and key operations at high volumes, supporting thousands of end-client systems per server node and thousands of key requests per minute per node. And because it's important that keys be managed over their full lifecycles — or risk data loss — the TSF key and policy manager fully implements stringent lifecycle management approaches, as specified by the NIST standard SP 800-57 Part 1, to ensure proper control of keys and their data.

The TSF key and policy manager is ideal for managing keys and policies for common enterprise applications such as databases, disk and tape storage encryption, and VM and VSAN integration. Its KMIP capability enables seamless integration with applications from vendors including Dell, Oracle, HP Enterprise, IBM, NetApp, CipherCloud, DataStax, Fujitsu, Quantum, Spectra, VMware, and more.

Simple Integration

While enterprises struggle to evolve their security systems, vendors will often market integrated solutions to increase the appeal of their products. However, the definition of "integrated" can vary. Some products have key and policy management but lack HSM protection, and others may have solutions designed to protect only specific platforms. Integration can sometimes mean a simple bundle of devices from partnered vendors, each with their own contacts and responsibilities for their products should problems arise.

All-In-One Security Solution

The TSF key and policy manager is QuintessenceLabs' truly integrated one-device solution, combining vendor-neutral key and policy management with HSM hardening, all backed by quantum-powered randomness to protect against the most advanced cyber attacks. It includes a client SDK to enable development teams to easily harness the power and features of the platform.

Get in Touch

QuintessenceLabs has formed proven partnerships with banking institutions and other enterprises, where our quantum-based encryption and key management solutions have effectively strengthened the data protection across entire organizations. We deliver the strongest security for your data so you can focus on what you do best.

For more information contact us at **info@quintessencelabs.com** or visit **quintessencelabs.com**.

Quintessence Labs

AUSTRALIA
Unit 11, 18 Brindabella Circuit
Brindabella Business Park
Canberra Airport ACT 2609
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 3752