Quintessence Labs

SOLUTION GUIDE

All-In-One Data Security with qCrypt 350TSF

Encryption and encryption key management are fundamental to strong data security. QuintessenceLabs' qCrypt 350TSF delivers the best encryption key and policy management capabilities allowing you to keep your data safe, today and into the future.

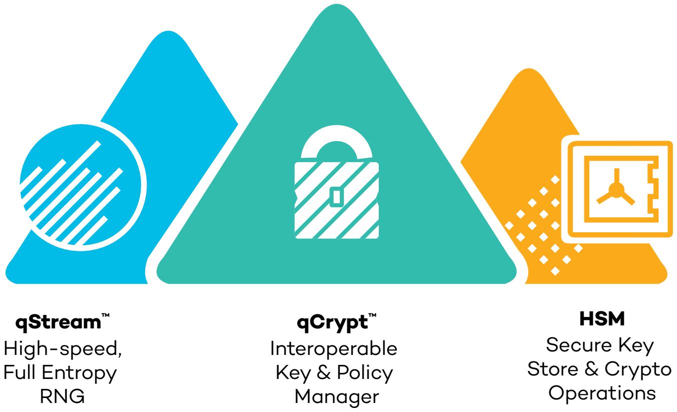
> With the qCrypt line of key and policy management devices, enterprises can seamlessly implement the strongest cybersecurity and focus on growing their business.

Integration That Matters

QuintessenceLabs uniquely offers a truly integrated, highly secure one-device solution in the qCrypt 350TSF appliance. qCrypt 350TSF combines vendor-neutral key and policy management with an embedded HSM, all backed by quantum-powered randomness to protect against the most advanced cyber-attacks. This results in an easily deployable, high performing, data protection capability — the Trusted Security Foundation — allowing you to focus on what your organization does best.

Centralized Security with qCrypt 350TSF

qCrypt 350TSF delivers a very comprehensive key and policy management solution. At its core is the qCrypt key manager, which handles large numbers of cryptographic keys and their policies. It also includes the qStream quantum random number generator, which provides true random numbers for use as encryption keys or other cryptographic parameters, at very high throughputs. The third element is an HSM, a physically secure device that further protects the data moving through the security infrastructure. The rack-mounted qCrypt 350TSF is easily integrated into your IT infrastructure, providing high-availability protection and management of cryptographic keys.



QuintessenceLabs Trusted Security Foundation

Embedded HSM

An HSM (hardware security module) is a physical device providing an isolated, protected environment for securely handling encryption keys or other sensitive cryptographic material, and performing cryptographic operations such as encryption and digital signing. HSMs that are validated to meet the requirements of FIPS 140-2 Level 3 are tamper resistant, and will destroy (or "zeroize") cryptographic material if an attempt is made to breach the device's security boundary.

Powerful Key Management

As enterprise data is processed and encrypted, the keys to decrypt that data need to be managed and stored throughout their lifetime, and policies need to be implemented to ensure secure and streamlined operations and access to the protected information. Critical features of a secure key management system include separation of duties, key lifecycle management, "m-of-n" quorum rules, consistent and available key management services, effective access and user policy enforcement, among others.

qCrypt is a vendor-neutral platform designed to simplify integration with new and legacy systems, and conforms to the OASIS Key Management Interoperability Protocol (KMIP), a standard specifying interoperability between key management clients and servers. qCrypt is regularly tested for interoperability with other vendors' KMIP implementations, in accordance with the rules and regulations of the OASIS KMIP Interoperability Subcommittee. For additional information on key management challenges and how qCrypt addresses them, see the QuintessenceLabs white paper "Key Management Best Practices".

qCrypt 350 TSF: QRNG + Key Manager + HSM integrated into one device

qCrypt 350TSF features

- FIPS 140-2 Level 3 cryptographic module
- Supports symmetric key and asymmetric key generation, key derivation, random objects, and certificates
- Built-in synchronous and asynchronous replication for up to 16 nodes
- Granular and auditable access control
- Event log, audit log, date and time of transaction
- Thousands of end-client systems per node, 200 key requests/sec. per node
- Attended or unattended startup

Quantum Random Number Generation

Generating strong cryptographic keys is crucial when encrypting data, and this relies on the quality of the random numbers used. Deterministic, algorithm-based methods of generating randomness may introduce security vulnerabilities. QuintessenceLabs' qStream quantum random number generator (QRNG) generates the highest quality random numbers at high rates by measuring a truly random quantum phenomenon: quantum tunneling.

qCrypt 350TSF integrates the qStream random number generator, giving qCrypt 350TSF users access to the highest quality umbers for the generation of keys or other cryptographic objects at rates up to 1Gbit/s.

QuintessenceLabs QRNG device

Embedded qStream QRNG features

- Quantum random number generator (QRNG) PCIe card delivering true random numbers
- 1Gbit/s uniformly distributed true random number output
- Conforms with NIST SP 800-90A, B (draft) and C (draft)
- Each user's output is 100% independent; traceability from hardware to entropy, to random number, to key to consumer

Where Integrated Devices Excel

Simple Setup - For enterprises, data centers, and other large businesses, installing new hardware can be complex, time consuming and costly.

qCrypt 350TSF delivers enhanced security that is interoperable with existing infrastructure. There's no need to separately load key management software onto a hardware appliance; no need to install and manage external HSMs; no need to plug in an RNG or other external entropy source; no need to install and manage a separate database as a keystore; no need to separately set up replication, and no need to procure, install, configure, and manage a range of individual components.

In addition, conformance with KMIP means that administrators do not need to be experts in key management standards – much less quantum technology – to set up and take advantage of the features of qCrypt 350TSF.

Networking: The Weak Link - Some key management solutions offer additional protection from an HSM, but as a separate rackmount device rather than an embedded module. Besides the potential integration headaches mentioned above, a security setup that links several devices through networking cables can present its own issues.

Though the devices may be hardened and make secure transfers before the data's final destination, a weak link in the network chain could nullify any security efforts and negatively impact performance. Similarly, any kind of hardware or software failure of one of the devices can impact the whole system.

Support That's Integrated, Too - A bundled solution of different devices may perform as expected, but if things don't go as planned, such as a failure that can't be fixed easily, this bundled solution transforms into a new problem as you juggle support conversations and accrue maintenance overhead.

With a single integrated, interoperable device, your support and maintenance are streamlined and simplified. Support staff is available on a 24/7/365 basis. With qCrypt 350TSF, you have one vendor, one device, and one phone call.

For more information on qCrypt products and other cybersecurity solutions from QuintessenceLabs, visit **quintessencelabs.com** or contact **info@quintessencelabs.com.**

Quintessence
Labs

AUSTRALIA
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+61 2 6260 4922

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

www.quintessencelabs.com

Document ID: 3751