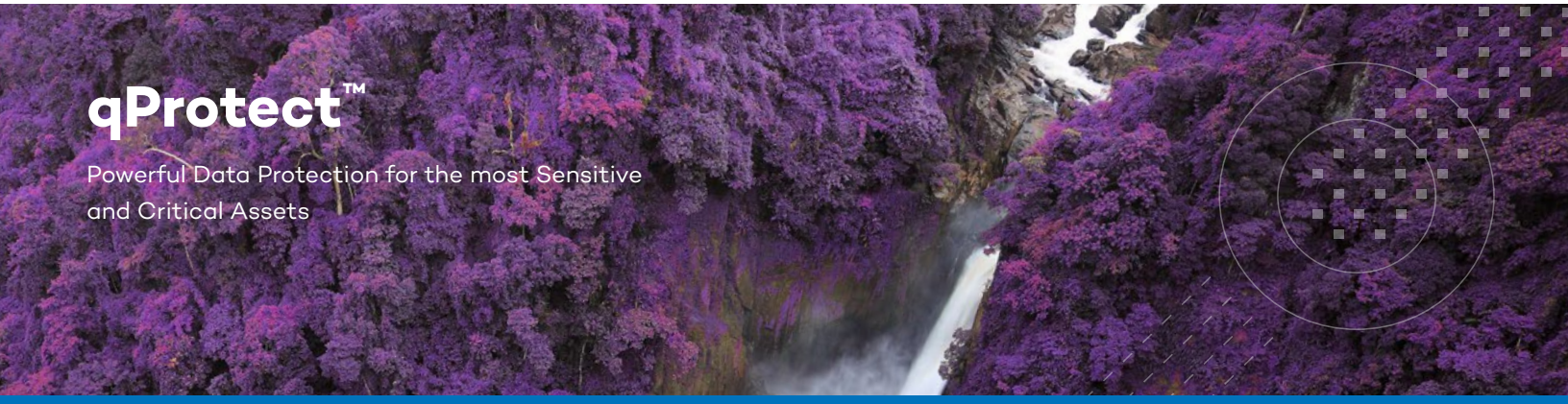
Quintessence Labs



qProtect™

Powerful Data Protection for the most Sensitive and Critical Assets

Virtual zeroization automatically destroys encryption keys while the data is encrypted

One-time pad encryption protects against the strongest attacks

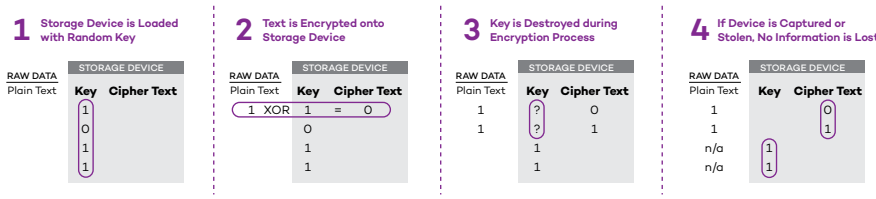
Overview

The most critical information needs the strongest possible protection to keep it safe, particularly when that data is in uncontrolled or dangerous environments. This means ensuring that the encryption is strong enough to withstand the most advanced attacks, and that any vulnerable information is automatically removed, or zeroized, from the device. Financial details, personal files, or other records may need to be protected not just today, but into the future.

qProtect from QuintessenceLabs offers a solution to both these challenges. It integrates a powerful alternative to manual or physical zeroization, that can be unreliable and costly, by providing instead automatic or "virtual" zeroization. In addition, it uses the strongest, mathematically proven, encryption: One-Time Pad encryption (OTP).

Protection Through Virtual Zeroization

qProtect's proprietary technology delivers automatic secure erasure of one-time key material when recording data, a process known as "virtual zeroization". This protects confidential information wherever it is, now and into the future. The data is encrypted using the one-time pad (OTP), the strongest known encryption technique, enabled using QuintessenceLabs high speed true random number generator, qStream. The virtual zeroization process is illustrated below:



The qProtect advantage allows encrypted data to be physically transported or transmitted across networks without risk, where it can be accessed by authorized users who can decrypt and use the data in a secure location. The process also provides tamper-resistance revealing, on decryption, any attempts to modify the data.

qProtect Capabilities

Through virtual zeroization, qProtect ensures the data and its encryption key are never co-located on the same device, removing the steps needed in traditional physical zeroization.

qProtect integrates QuintessenceLabs' quantum random number generator and advanced key management capabilities to deliver ultimate data security to end users.

qProtect Deployment

The high security of qProtect's virtual zeroization has practical applications in the military, law enforcement, and aircraft recorders. Securely transporting data is also paramount in media, financial institutions, and multiple commercial applications. The QuintessenceLabs team can partner with you to define the best qProtect implementation strategy for your organization.

SPECIFICATIONS

qProtect™

Unbeatable security for data in uncontrolled environments

Configuration	**Virtual zeroization storage devices** • Standard form factors: 32GByte SD Card / 8GBytemicroSD Card *Other device types available on request* • Storage densities from 16 to 256GByte *Higher densities available on request*
Automatic Key Destruction (Zeroization)	• The one-time pad key on the device is automatically destroyed during encryption • Removes need for manual data destruction or additional zeroization steps • Data remains accessible to authorized users for decryption in a secure location
Key & Policy Management	Administered via qCrypt products; abridged specifications below. *Please see qCrypt data sheets for more details.*
Replication	• Secure replication of policies and managed cryptographic objects — up to 16 nodes per replication group • Synchronous and asynchronous replication
Operations	• FIPS 140-2 Level 3 cryptographic module • Granular, hierarchical and auditable access control • Thousands of end-client systems per node, 8,000 key requests per minute per node per node • Attended or unattended secure startup
Standards & Interoperability	• KMIP 1.0, 1.1, 1.2, 1.3, and 1.4 • Basic and advanced KMIP profiles • Supports PKCS#11 over KMIP • Fully implements all requirements in NIST SP800-57 Part 1 • Common Criteria EAL 2
Implementation	• Delivered with qClient SDK, a software development kit adhering to the OASIS Key Management Interoperability Protocol (KMIP) and the PKCS#11 API. *Please see qClient data sheets for more details.*

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: 1622