Quintessence Labs

qCrypt™

200V | 250A | 300H | 300R | 350TSF

Flexible Key and Policy Management for Stronger Encryption

- Highly capable key and policy management, a foundation for strong encryption
- Can be used with a wide range of third party solutions
- Available as virtual machines or hardware appliances

Overview

Encryption key management is one of the biggest challenges in data security. Keys must be managed over their full lifecycle and sophisticated policy management is needed to ensure strong data protection without impacting operations. Poor quality encryption keys can significantly weaken data protection. Finally, integrating with legacy devices can complicate or delay implementation and drive up costs.

Improving Key Management

Strong encryption requires effective key and policy management to properly protect your data, keeping it safe even in the event of a breach. Many key managers are not interoperable with other devices or platforms, generate weak keys, or lack the proper policy control, resulting in siloed data protection, negative impacts on operations, and potentially weaker encryption.

qCrypt delivers secure, centralized, and highly interoperable key and policy management across any organization. As either a virtual machine or hardware appliance, qCrypt can manage keys over their full life cycle, implement strong object and user policy management, and offers built-in replication for up to 16 nodes for maximum availability.

QuintessenceLabs uses quantum technology to capture a level of randomness only seen in nature, resulting in perfectly unpredictable random numbers, encryption keys or other security objects, of much higher entropy than those generated by typical deterministic sources. qCrypt can integrate and manage this high-speed, high-entropy source of keys to enable the implementation of strong encryption.

qCrypt Integration

qCrypt products support the OASIS Key Management Interoperability Protocol (KMIP). The qCrypt product range has been tested with many third party devices commonly in use. These include products from IBM, HP, Oracle and NetApp, enabling qCrypt to be seamlessly integrated into legacy infrastructure with minimal disruption and delay. In addition, qCrypt fully meets the NIST SP 800-57 key lifecycle requirements. qCrypt supports thousands of end-client systems, tens of millions of keys, and transaction rates of eight thousand key requests per minute per node.

qCrypt Deployment

QuintessenceLabs offers qCrypt in several configurations, from an efficient Hyper-V or VMware virtual machine (qCrypt 200V) to dedicated key management appliances (qCrypt 250A, 300H, 300R) and a comprehensive appliance with the true random number generation and hardware security module features of our Trusted Security Foundation® (qCrypt 350TSF). qCrypt fits the needs of any organization looking to transform their key management.

SPECIFICATIONS

qCrypt™

200V | 250A | 300H | 300R | 350TSF

	200V	250A	300H	300R	350TSF
Configuration & Dimensions	Virtual Machine	Appliance	Appliance w/HSM	Appliance w/QRNG	Appliance w/HSM+QRNG
	N/A	• 1RU: H: 4.28 cm (1.69"), W: 48.20 cm (18.98"), D: 80.85 cm (31.83") • Weight: 22 kgs • Support for running multiple Virtual Machines (VMs)			
Power Supply	N/A	1RU: Dual, redundant, hot-swappable, 550 W			
Cryptography & Security	• Supports non-embedded FIPS 140-2 Level 3 cryptographic module • Supports one-time pad, symmetric key and asymmetric key ciphers, key derivation, random objects, certifications and some cryptographic operations • Support for Bring Your Own KEY (BYOK) operations with AWS and MS Azure • Granular, hierarchical and auditable access control • Supports both attended and unattended secure start-up • Event log, audit log, date and time of transaction, management and user reports • Thousands of end-client systems per node, 8,000 key requests/minute per node				
	N/A	N/A	FIPS 140-2 Level 3 HSM root of trust	N/A	FIPS 140-2 Level 3 HSM root of trust
Replication	• Secure replication of policies and managed cryptographic objects — up to 16 nodes per replication group • Supports both synchronous and asynchronous replication				
Random Number Generator	N/A	N/A	N/A	• QRNG included • Up to 1Gbit/sec true random stream • Conforms with NIST SP 800-90 A, B, and C (draft) • Satisfies NIST SP 800-22 (NIST STS) and Dieharder tests • Fully independent output for each user, audit trail from hardware through to consumer • RESTful API support for delivering random data	
Standards & Interoperability	• OASIS KMIP: Conformant with standards 1.0/1.1/1.2/1.3/1.4/2.0 • Fully implements all requirements in NIST SP 800-57 Part 1 • Common Criteria EAL 2 certified (does not apply to 200V) • PKCS#11 supported via qClient SDK				
Administration & Management	• Web (HTTPS) or command-line (SSH) management interfaces • Purpose-built QRE secure operating system • Delivered with qClient SDK • Support for 10 Gbit/sec Ethernet				

©2019 QuintessenceLabs. All rights reserved

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: 1621