



# 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. Integrating with legacy devices can complicate or delay implementation and drive up costs. Keys must be managed over their full lifecycle and sophisticated policy management is needed to ensure strong data protection without impacting operations. Finally, poor quality encryption keys can significantly weaken data protection.

## Improving Key Management

Strong encryption requires effective key and policy management to properly protect your data, even in the event of breaches or accidental loss. 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 in-built 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**

|   | <b>200V</b>   | <b>250A</b>   | <b>300H</b>                          | <b>300R</b>   | <b>350TSF</b>                        |
|---|---|---|--------------------------------------|---|--------------------------------------|
| <b>Configuration</b>                    | Virtual Machine   | Appliance   | Appliance w/HSM                      | Appliance w/QRNG  | Appliance w/HSM+QRNG                 |
| <b>Cryptography &amp; Security</b>      | <ul style="list-style-type: none"> <li>• Supports one-time pad, symmetric key and asymmetric key ciphers, key derivation, random objects, and certificates</li> <li>• Granular, hierarchical and auditable access control</li> <li>• Supports both attended and unattended secure start-up</li> <li>• Event log, audit log, date and time of transaction</li> <li>• Thousands of end-client systems per node, 8,000 key requests/minute per node</li> </ul> |   |                                      |   |                                      |
|   | N/A   | N/A   | FIPS 140-2 Level 3 HSM root of trust | N/A   | FIPS 140-2 Level 3 HSM root of trust |
| <b>Replication</b>                      | <ul style="list-style-type: none"> <li>• Secure replication of policies and managed cryptographic objects, up to 16 nodes per replication group</li> <li>• Supports both synchronous and asynchronous replication</li> </ul>  |   |                                      |   |                                      |
| <b>Random Number Generator</b>          | N/A   | N/A   | N/A                                  | <ul style="list-style-type: none"> <li>• QRNG included</li> <li>• Up to 1Gbit/s true random stream</li> <li>• Conforms with NIST SP 800-90 A, B, and C (draft)</li> <li>• Fully independent output for each user; full audit trail from hardware through to consumer</li> </ul> |                                      |
| <b>Standards &amp; Interoperability</b> | <ul style="list-style-type: none"> <li>• OASIS KMIP: Conformant with standards 1.0/1.1/1.2/1.3/1.4</li> <li>• Fully implements all requirements in NIST SP 800-57 Part 1</li> <li>• Common Criteria EAL 2 certified (does not apply to 200V)</li> </ul>   |   |                                      |   |                                      |
| <b>Admin &amp; Management</b>           | <ul style="list-style-type: none"> <li>• Web (HTTPS) or command-line (SSH) management interfaces</li> <li>• Purpose-built qRE secure operating system</li> <li>• Includes <b>qClient</b> SDK</li> </ul>   |   |                                      |   |                                      |
| <b>Dimensions</b>                       | N/A   | <ul style="list-style-type: none"> <li>• 2U: H: 8.73 cm (3.44"), W: 44.40 cm (17.49"), D: 68.40 cm (26.92")</li> <li>• 1U: H: 4.28 cm (1.68"), W: 43.40 cm (17.08"), D: 60.70 cm (23.9")</li> </ul> |                                      |   |                                      |
| <b>Power Supplies</b>                   | N/A   | <ul style="list-style-type: none"> <li>• 2U: Dual, redundant, hot-swappable 750 W</li> <li>• 1U: Dual, redundant, hot-swappable 550 W</li> </ul>  |                                      |   |                                      |