



SPECIFICATIONS

qCrypt™ 350TSF



Complete key management solution forming our
Trusted Security Foundation® (TSF®)

Configuration	<p>Rackmount Appliance with HSM and QRNG</p> <ul style="list-style-type: none"> • Dimensions - 1RU: H: 4.28 cm (1.69”), W: 48.20 cm (18.98”), D: 80.85 cm (31.83”) • Weight - 22 kgs • Power Supply - 1RU: Dual, redundant, hot-swappable, 550 W • Support for both centralized and distributed deployment topologies to suit any availability or performance requirements • Support for running multiple Virtual Machines (VMs)
Replication	<ul style="list-style-type: none"> • Secure replication of policies and managed cryptographic objects — up to 16 nodes per replication group • Supports both synchronous and asynchronous replication
Random Number Generation	<ul style="list-style-type: none"> • Includes quantum random number generator (QRNG) PCIe card supporting true random key generation • Up to 1 Gbit/sec true random stream • Conforms with NIST SP 800-90A, B, and C (draft) • Satisfies NIST SP 800-22 (NIST STS) and Dieharder tests • Fully independent output for each user; full audit trail from hardware to consumer • RESTful API support for delivering random data
Cryptography & Security	<ul style="list-style-type: none"> • 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 • Encrypted keystore with protected root of trust • Granular, hierarchical and auditable access control • 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 • Attended or unattended secure startup
Standards & Interoperability	<ul style="list-style-type: none"> • 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 • Supports PKCS#11 over KMIP
Administration & Management	<ul style="list-style-type: none"> • Web (HTTPS) or command-line (SSH) management interfaces • Purpose-built QRE secure operating system • Delivered with qClient SDK • Support for 10 Gbit/sec Ethernet