



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 <ul style="list-style-type: none"> 2U: H: 8.73 cm (3.44"), W: 44.40 cm (17.49"), D: 68.40 cm (26.92") 1U: H: 4.28 cm (1.68"), W: 43.40 cm (17.08"), D: 60.70 cm (23.9") • Power Supply <ul style="list-style-type: none"> 2U: Dual, redundant, hot-swappable 750 W 1U: Dual, redundant, hot-swappable 550 W • Support for both centralized and distributed deployment topologies to suit any availability or performance requirements
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"> • Included quantum random number generator (QRNG) PCIe card supporting true random key generation • Up to 1 Gbit/s 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
Cryptography & Security	<ul style="list-style-type: none"> • FIPS 140-2 Level 3 cryptographic module • Supports one-time pad, symmetric key and asymmetric key ciphers, key derivation, random objects, and certificates • Encrypted keystore with protected root of trust • Granular, hierarchical and auditable access control • Event log, audit log, date and time of transaction • 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 SP800-57 Part 1 • Certified for Common Criteria EAL 2 • PKCS#11 supported via qClient SDK
Administration & Management	<ul style="list-style-type: none"> • Web (HTTPS) or command-line (SSH) management interfaces • Purpose-built qRE secure operating system • Includes qClient SDK