Qukee®

gmv
INNOVATING SOLUTIONS

State-of-the-art QKD is not just about generating keys. It is about operating them safely, reliably, and at scale

GMV's ***QuKee***® key management solution turns quantum-generated key material into an enterprise-ready security service. It provides secure key ingestion, lifecycle control, authenticated relay across trusted nodes, standards-based delivery to applications, and full operational visibility across the QKD service stack. It is designed for secure, stable, efficient, and robust operation, whether deployed as software or embedded in a hardened appliance.

marketing.TIC@gmv.com

gmv.com

MAIN FEATURES

- Secure key lifecycle management: ingest, buffer, identify, deliver, zeroize, and audit every key.
- Standards-based APIs aligned with ETSI GS QKD 004 / 014.
- Secure key relay across trusted nodes with synchronization and authenticated transport.
- Policy-driven key supply with session control and deterministic behavior under key scarcity.
- Multi-vendor QKD module compatibility.
- Hybrid QKD + PQC key service profiles for defense in depth, including ETSI TS 103 744-aligned hybrid key establishment and QKD-based key-combination options.
- Internal HSM for hardware-rooted trust, hardware-backed key protection / validated crypto-boundary and strong tamper resistance (*).
- QRNG-assisted continuity for transient QKD degradation via hybrid continuity buffer (*).
- Inter-KMS interoperability roadmap aligned with ETSI GS QKD 015 / 020 and QKDN interworking.
- Quantum-safe authentication and fine-grained access control for applications, peer systems, and administrators, enabled through ML-DSA and/or securely managed pre-shared-key authentication.
- Trusted operations and administrative control including separation of duties and granular Role Based Access Control.
- Integration with AI-driven analytics for enhanced system behavior and operator support.
- FCAPS-aligned monitoring, alerting, and security telemetry, enabled through Dell iDRAC (*).
- Flexible deployment as software or hardened appliance, with secure upgrade and HA/failover options

(*) applicable to product hardware appliance only, through selected options

Feature	*QuKee*®	*QuKee*® |+⟩
Form factor	1U rack server, short-length	1U rack server, standard-length
Intrusion detection	Yes	Yes
Hardware rooted trust	TPM 2.0	Embedded HSM, certified FIPS 140-2 Level 3, CC EAL 4+, PQC-ready, CPSTIC ENS high (optional)
Random number generator	OpenSSL	NIST SP800-90B compliant QRNG, PCSTIC ENS high (optional)
Cybersecurity	OS hardening, secure boot	GMV's ***CosmicGuard*** EAL 2, CPSTIC ENS high
Processing unit	Single processor	Dual processor
Network ports	9 x RJ45	6 x RJ45 + 4 x SFP28
Power supply	Single PSU (1+0)	Dual, Fully Redundant (1+1), Hot-Plug
Internal storage	SSD	HW RAID5 SSD, Hot-plug
Remote administration	Dell's iDRAC9, 16G Basic	Dell's iDRAC9, 16G Enterprise

From quantum link to application consumption, ***QuKee***® provides the operational key-management layer required to make QKD usable as a real security service — not just a laboratory capability.