QSphere™

Data Security Suite

Datasheet

- Quantum-Resistant Encryption
- Comprehensive Data Protection
- Centralized Key Management
- Digital Signing and Verification
- Secure Communication

QuantumGate™

Features

Utilizing a proprietary Post-Quantum Cryptography (PQC) stack, QSphere ensures secure data at rest and in transit, robust data integrity, and non-repudiation—effectively future-proofing your enterprise security needs.

Key Directory Server	Centralized key management with sovereign-national cryptography for encryption and digital signing; enhances security and compliance.
Key Management	Generate, revoke, export, share, and attest digital keys with support for sub-keys and multiple IDs; increases security and flexibility.
Text Encryption/Decryption	Securely encrypts and decrypts text messages, protecting sensitive information from unauthorized access.
File and Folder Encryption/Decryption	Provides PQC encryption and decryption for files and folders, ensuring data security both at rest and in transit.
Email Encryption/Decryption	Encrypts, decrypts, signs, and verifies emails, ensuring secure corporate communications and protecting against email threats.
Document Signing/Verification	Supports digital signing and verification of documents, ensuring authenticity, integrity, and facilitating non-repudiation.

Capabilities

Quantum-Resistant Encryption

Utilizes proprietary Post-Quantum Cryptography to protect data against classical and quantum threats, ensuring future-proof security.

Comprehensive Data Protection

Offers encryption and decryption for text, files, folders, emails, and documents, securing data at rest and in transit.

Centralized Key Management

Provides a robust Key Directory Server for centralized management of encryption keys including generation, revocation, export, sharing, and attestation.

Digital Signing and Verification

Enables digital signing and verification of documents and emails, ensuring authenticity, integrity, and non-repudiation.

Secure Communication

Ensures secure corporate communications through email encryption, decryption, signing, and verification.

QSphere Data Security Suite is a comprehensive, quantum-resistant solution designed to safeguard your organization's most sensitive data against both classical and emerging quantum threats.

QuantumGate™

Requirements

Technical

Key Directory Server	Deployment and configuration of the QSphere Data Security Key Directory Server to manage encryption keys. The server offers centralized, sovereign-national cryptography for key management, encryption, and digital signing. It supports key generation, revocation, export, sharing, and attestation, with options for sub-keys and multiple IDs to enhance security.
DataSec Client Applications	Available for major desktop and mobile platforms, including MacOS, iOS, Windows and Android. The applications provide user-friendly interfaces for encryption/decryption, key management, and digital signing/verification.
Deployment Options	Supports flexible deployment models, including on-premises, cloud-based, or hybrid environments. The Key Directory Server can be deployed in data centres or cloud infrastructures, and client applications can be distributed via standard software deployment tools.

System

Operating System	✓ Desktop: macOS 13 or later, Windows 10 or later ✓ Mobile: iOS 17 or later ✓ Linux (CLI): Debian-based distributions (others pending testing); supports Docker and Kubernetes
Storage Space	Minimum of 1000 MB
RAM	8 GB for Windows/MacOS
Additional Requirements	All necessary frameworks or dependencies are bundled into the application

quantumgate.ae contact@quantumgate.ae