Quantum Bridge

Product Data Sheet

Quantum Bridge Symmetric Key Distribution System

Unbreakable key distribution technology for protecting data and infrastructure

What is a Symmetric Key Distribution System?

The Quantum Bridge Symmetric Key Distribution System (SDS) is a flexible, comprehensive, and cost-effective security solution that enables your organization to protect sensitive data and communications across the entire network stack, regardless of the encryption methods or devices used.

Even as your security requirements change, the SDS can scale dynamically without impacting the performance, security, or usability of the entire solution, allowing it to meet your needs without compromising on core functionality or user experience.

Our solution delivers unconditional security for your critical data and communications through quantum-safe, crypto-agile security protocols. The SDS protects against even the most advanced threats, ensuring that your organization can meet its security and compliance requirements with confidence.

What is the Key Management Entity?

The Quantum Bridge Key Management Entity (KME) enhances your data security **anywhere you operate**, on-premises or in the cloud.

As the core of the Quantum Bridge SDS solution, each KME can deliver symmetric keys to multiple network encryptors, firewalls, routers, or any other network appliance for use at any layer. Key delivery occurs near-instantaneously, ensuring even the most demanding applications and high-traffic networks maintain **peak performance** while adhering to the **highest encryption standards**.

Key Features

- Layer-agnostic, multi-layer security
- Compatible with existing networks
  - ETSI GS QKD 014
  - SKIP
- Crypto-agile, supporting multiple protocols
  - PQC
  - PSK
  - QKD
  - DSKE
- No single point of failure
- Perfect secrecy and quantum-safety
- Automated dynamic symmetric key distribution

Applications

- **Layer 1:** Optical encryptors
- **Layer 2:** MACsec encryptors, routers, switches
- **Layer 3:** IPsec encryptors, WireGuard®, VPNs, compatible with RFC 8784

Cryptography

- **Post-Quantum Cryptography (PQC)**
  - CRYSTALS-Kyber (512, 768, and 1024)
  - ML-KEM (512, 768, and 1024)
  - BIKE (Level 5)
  - Classic McEliece (mceliece6960119)
- **DSKE**
  - Information-theoretic security
  - Confidentiality: One-time-pad encryption between KME and Security Hub
  - Authentication: One-time key with universal hash function
  - Trust distribution: Shamir secret sharing
  - AES-256-GCM for anti-DoS message security
- **Quantum Key Distribution (QKD)**
  - Supported for additional link security

Contact Us

+1-249-225-5099

contact@qubridge.io

Use Cases

WAN/LAN interconnect. The Quantum Bridge SDS can be used to **protect traffic** between different WAN/LAN networks, especially when communication goes through untrusted third-party infrastructure or the public internet. A KME can be used to interface with most existing network appliances to distribute cryptographic keys, protecting all valuable information and building a secure communication network.

Data centre interconnect. The Quantum Bridge SDS can be used to provide **secure access** to data centres while ensuring the highest level of security for both encryption and authentication. With its layer-agnostic approach, the SDS can integrate into Layers 1, 2, and 3 to interface with existing network appliances or run as a native application in existing hardware. This provides information-theoretic security, keeping data secure even against adversaries with unlimited quantum or classical computational resources.

What's Your Solution?

The Quantum Bridge SDS software can be tailored to meet users' specific needs or requirements, such as:

- Radio communication
- Satellite communication
- Sensor communication

Please contact Quantum Bridge to discuss use cases of interest or custom development to integrate the Quantum Bridge SDS into your infrastructure.

Contact Us +1-249-225-5099 contact@qubridge.io