Quantum Bridge

DATA SHEET

Key Management Entity

Scalable, future-proof, quantum-safe, symmetric-key distribution system.

Layer agnostic
Future-proof technology
Seamless Integration

Quantum Bridge's Key Management Entity (KME) fully automates the creation and distribution of Pre-Shared Keys (PSK) with its unique patented technology. The KME is secure, scalable, has a low computational footprint, and is quantum-safe by design. The core architecture behind the KME is based on Quantum Bridge's Distributed Symmetric Key Exchange (DSKE) model. It removes the need for centralized key distribution, so there are no bottlenecks or any single points of attack or compromise. Furthermore, the core protocol operates directly over the internet, removing the need for out-of-band key distribution channels. The KME allows any group of clients to dynamically generate symmetric keys in both on-demand and pre-shared modes without the use of asymmetric encryption algorithms. Keys are known at only the authorized endpoints.

Note: Physical form factors vary by model, and may not be as illustrated.

KEY FEATURES AND BENEFITS

- Layer-agnostic
- Seamless integration into existing networks
- Multiple form factors
- Distributed trust architecture
- Perfect secrecy and quantum-safety
- Not certificate-based
- Automated pre-shared key distribution
- Scalable to any number of devices
- Single key-generation mechanism for all PSK-compatible protocols

APPLICATIONS

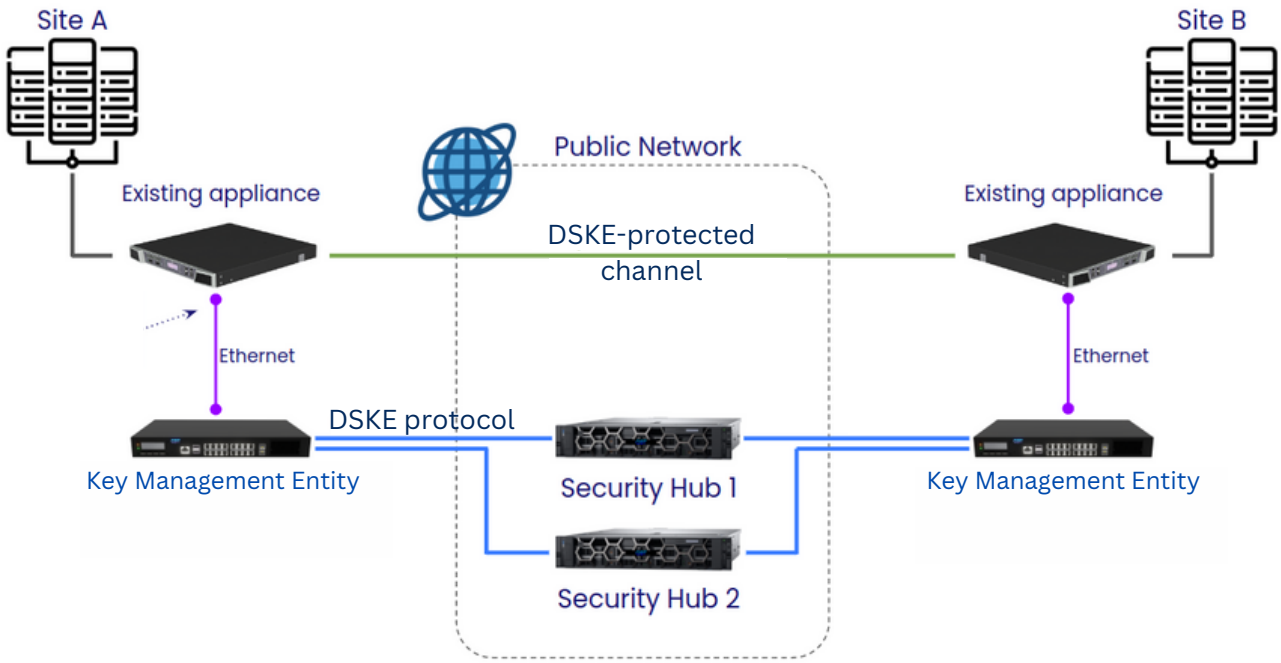
- **Layer 1**: optical encryptors
- **Layer 2**: MACsec encryptors, routers, switches
- **Layer 3**: IPsec encryptors, WireGuard®, VPNs, compatible with RFC 8784
- **Applications**: email, VoIP, video calls, SSL/TLS, DTLS
- Easily integrate into custom security solutions at all layers

✉ contact@qubridge.io ☎ (+1) 437-232-9840

Product Description

The Quantum Bridge's Key Management Entity (KME) provides an easy-to-use, cost-efficient, compact DSKE client services that can be installed in existing infrastructure to provide symmetric key distribution functionality. Quantum Bridge KMEs incorporate the DSKE client and can deliver keys to network appliances in any layers, for example, network encryptors and switches. The KME connects to existing appliances via ethernet cable and supports standard API calls like the ETSI QKD 014. Once installed, the KME requires activation data from one or more Quantum Bridge Security Hubs, which can be delivered via a secure, tamper-proof hard drive, or via Quantum Key Distribution (QKD) in case a QKD link is available to a Security Hub. DSKE keys delivered via the KME can be layered to PKI keys to make current infrastructure quantum-safe, and future-proof, and to eliminate any vulnerability associated to PKI and its certificates.

Network Security



Quantum Bridge's Key Management Entities (KME) connect directly to existing network encryptors and infrastructure. The KMEs key distribution and management is supported by the Security Hubs, which orchestrate and synchronize the generation of secret keys between the KMEs. Once set up, it provides and manages symmetric cryptographic keys on demand, making existing infrastructure quantum-safe and securing it against any weakness or failure in the PKI.