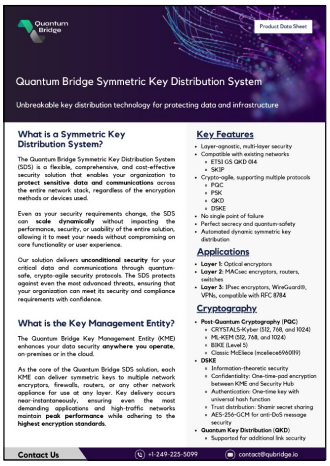

Quantum Bridge Symmetric Key Distribution System

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 reassage security
- Quantum Key Distribution (QKD)
  - Supported for additional link security

Contact Us

+1 249-225-5099

contact@qubridge.io

Quantum Bridge Symmetric Key Distribution System

Thank you for downloading this Quantum Bridge Solutions data sheet. Carahsoft is the master government aggregator for Quantum Bridge solutions available via NASA SEWP V, ITES-SW2, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring Quantum Bridge's solutions, please check out the following resources and information:

For additional resources:
carah.io/QBTResources

For upcoming events:
carah.io/QBTEvents

To set up a meeting:
QuantumBridge@carahsoft.com
844-214-4790

To purchase, check out the contract vehicles available for procurement:
carah.io/QBTContracts

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.

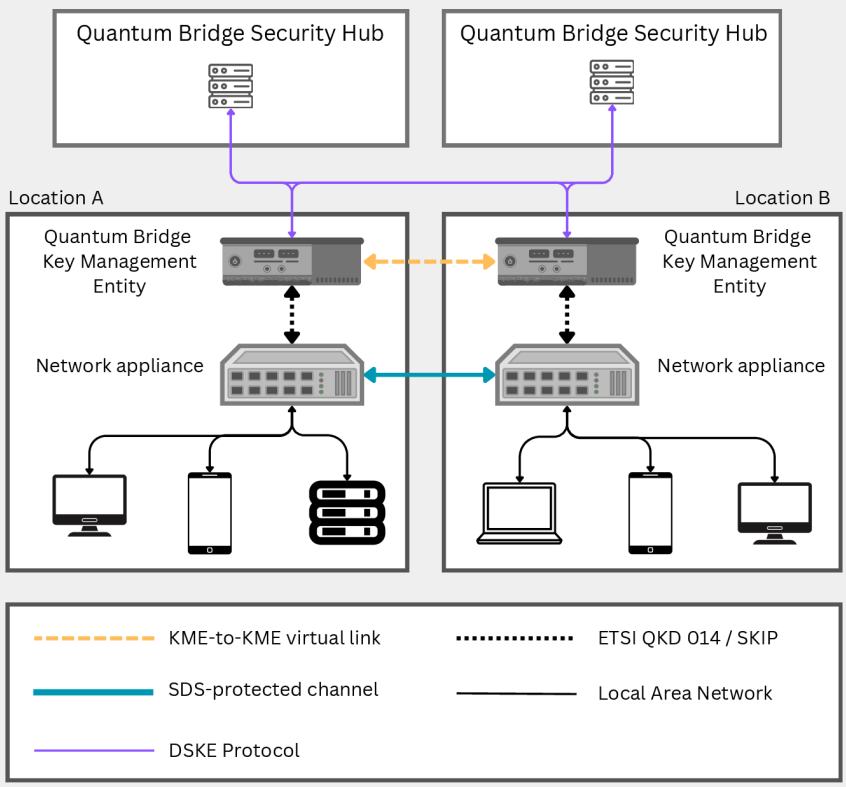
Contact Us +1-249-225-5099 contact@qubridge.io

Implementation

The Quantum Bridge SDS software is developed in Rust, a programming language distinguished for its small footprint, enhanced security, and unparalleled performance. Rust's emphasis on memory- and thread-safety makes it ideal for creating secure applications, effectively minimizing vulnerabilities and ensuring robustness. This ensures that our software uses minimal resources while maximizing execution speed, setting it apart in efficiency.

Deployment

Cryptographic keys supplied by the KME to existing appliances can be combined with other keys in compatible existing protocols to make current infrastructure quantum-safe and future-proof, and to eliminate any vulnerability associated with asymmetric key management protocols or Public Key Infrastructure (PKI) and its certificates.



Example deployment. In the figure, Quantum Bridge KMEs in different locations are connected to network appliances to provide quantum-safe keys. A network appliance, such as a firewall, network encryptor or router, must support ETSI GS QKD 014 or SKIP. The diagram also includes two Security Hubs, needed should the DSKE protocol be activated on top of PQC. PQC and DSKE independently provide end-to-end security of key delivery. Security of traffic between KMEs is additionally protected through a Virtual Private Network (VPN), where the link security can be further enhanced by PSK or QKD. All traffic is delivered over the VPN, where packets are routed from KME to KME with flexible routing rules.

Software Requirements

- **Host**
  - Operating System*: RHEL 9.4; Ubuntu 22.04
- **CPU**
  - Minimum: Intel® Core™ i3 (2 GHz) or equivalent
  - Recommended: Intel® Core™ i5 processor or equivalent
- **Memory**
  - Minimum: 4 GiB RAM
  - Recommended: ≥ 8 GiB RAM
- **Disk**
  - Minimum 5 GB
  - Additional storage for DSKE
- **Network**
  - UDP + TCP + link management (DNS, etc.)
  - IP connectivity for the following links:
    - KME to KME
    - KME to Security Hub (if DSKE is activated)

Performance

- **KME key throughput (256-bit keys)**
  - > 12,000 keys per second in PQC mode
  - > 1,000 keys per second in DSKE mode
- **KME average response time to network appliance**
  - Max load: 50 ms
  - Low load: 20 ms
- **Security Hub key request response time**
  - < 100 ms (excluding network delays)

Routing Capabilities

Configuration of the KME virtual private network allows for the definition of:

- Static routes between specific KME appliances
- Dynamic routing using OSPF (default), IS-IS, RIP or any protocol supported by the FRRouting Project
- Routing cost metrics based on the security paradigm of each tunnel (QKD or PSK)
- SNMP hosts to send traps to as well as the traps to send

* Available on Debian-based Linux distributions on request.

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