Quantum Bridge

Quantum Bridge Symmetric Key Distribution System

Scalable, provably secure, key distribution and management system without asymmetric cryptography

The Problem

Quantum computers, under development by organisations in several countries, threaten the security of asymmetric encryption currently in use. While the timeline for a sufficiently powerful quantum computer remains uncertain, this threat creates the need to migrate current infrastructure to a quantum-safe posture as soon as possible. To be secure, data, digital assets, and infrastructure must be protected against the quantum threat long before this threat becomes actual.

Symmetric Key Management System

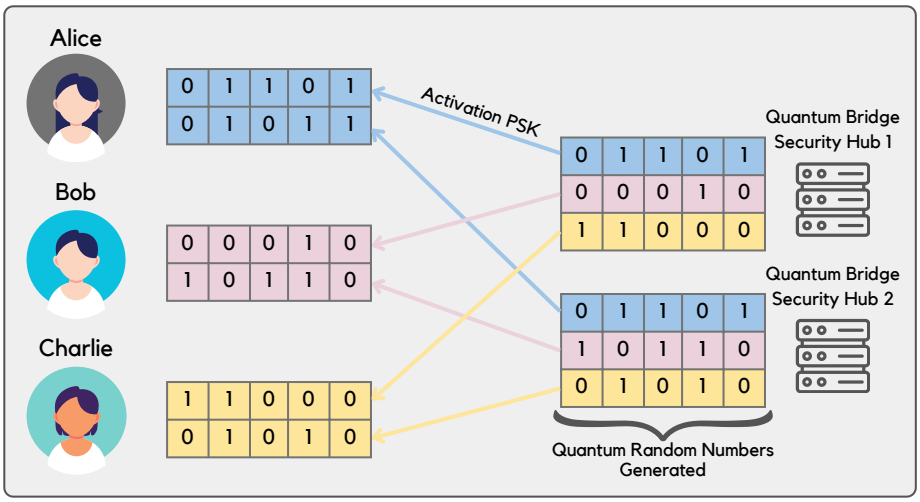
Quantum Bridge's Symmetric-Key Distribution System (SDS) fully automates the **creation and distribution of symmetric keys,** without using any asymmetric cryptography. SDS is scalable, non-disruptive, and is provably quantum-safe, meaning that the underlying protocol has been proved to achieve information-theoretical security.

The core architecture behind SDS is based on **Distributed Symmetric Key Exchange** (**DSKE**). DSKE removes the need for centralized key distribution through secret-sharing and redundancy, so there are no bottlenecks nor any single points of trust or compromise. The core protocol operates directly over the internet, removing the need for out-of-band key distribution channels.

The SDS solution includes two components: the **Key Management Entity** (**KME**), and one or more **Security Hubs** (**SH**). The KME is a plug-and-play device colocated with existing network appliances. The KME does not require any special hardware, and can be installed in off-the-shelf devices or directly in the network appliances. The Security Hub can be run in the cloud. The KMEs require one-time Pre-Shared Random Data (PSRD) for activation. After activation, the KME can exchange secret keys with any other active KME.

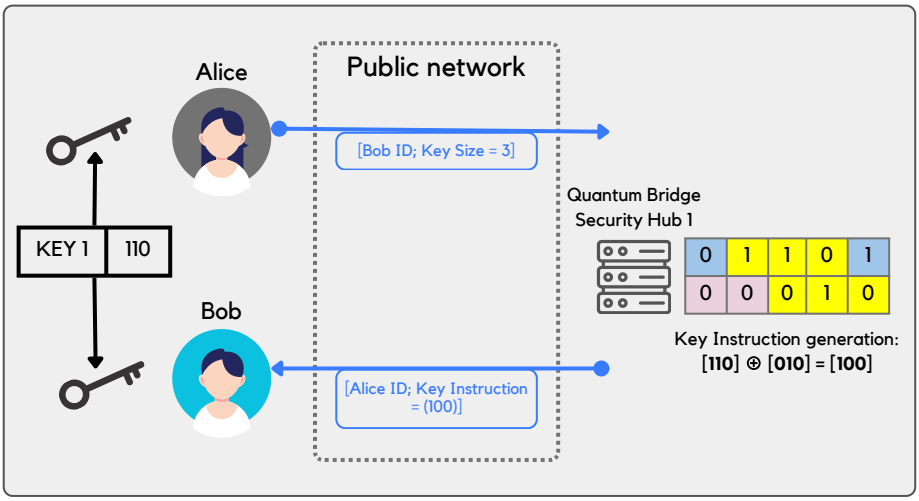
Contact Us +1-437-232-9840 contact@qubridge.io

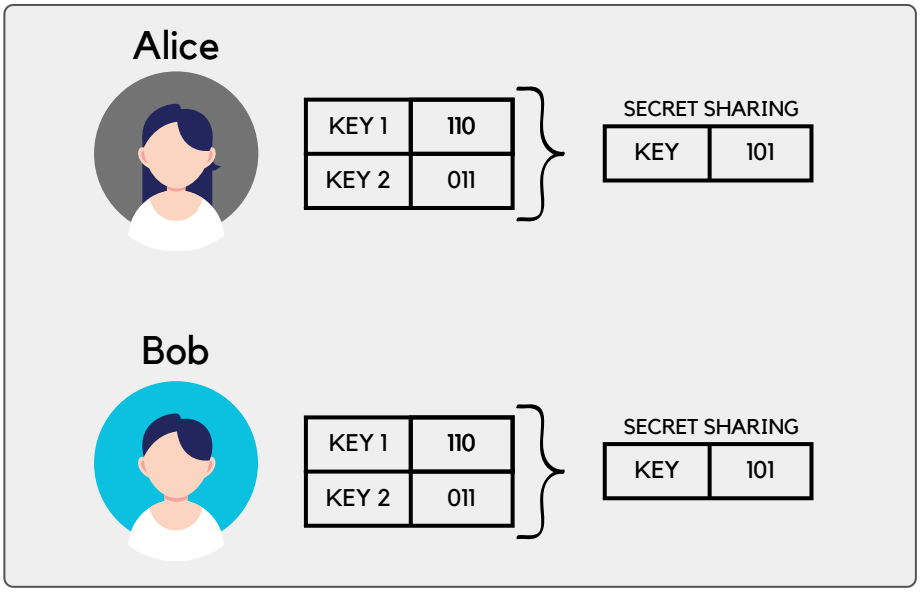
How DSKE works



Set-up.
When a new client joins the system, each Security Hub generates some new secret random data from a Quantum Random Number Generator. The random data is delivered to the client using physical tamper-proof devices or other secure channels.

Key generation.
When Alice requests a key with Bob, each Security Hub broadcasts the exclusive-or of Alice and Bob's secret strings. Bob can use this to generate a key shared with Alice.

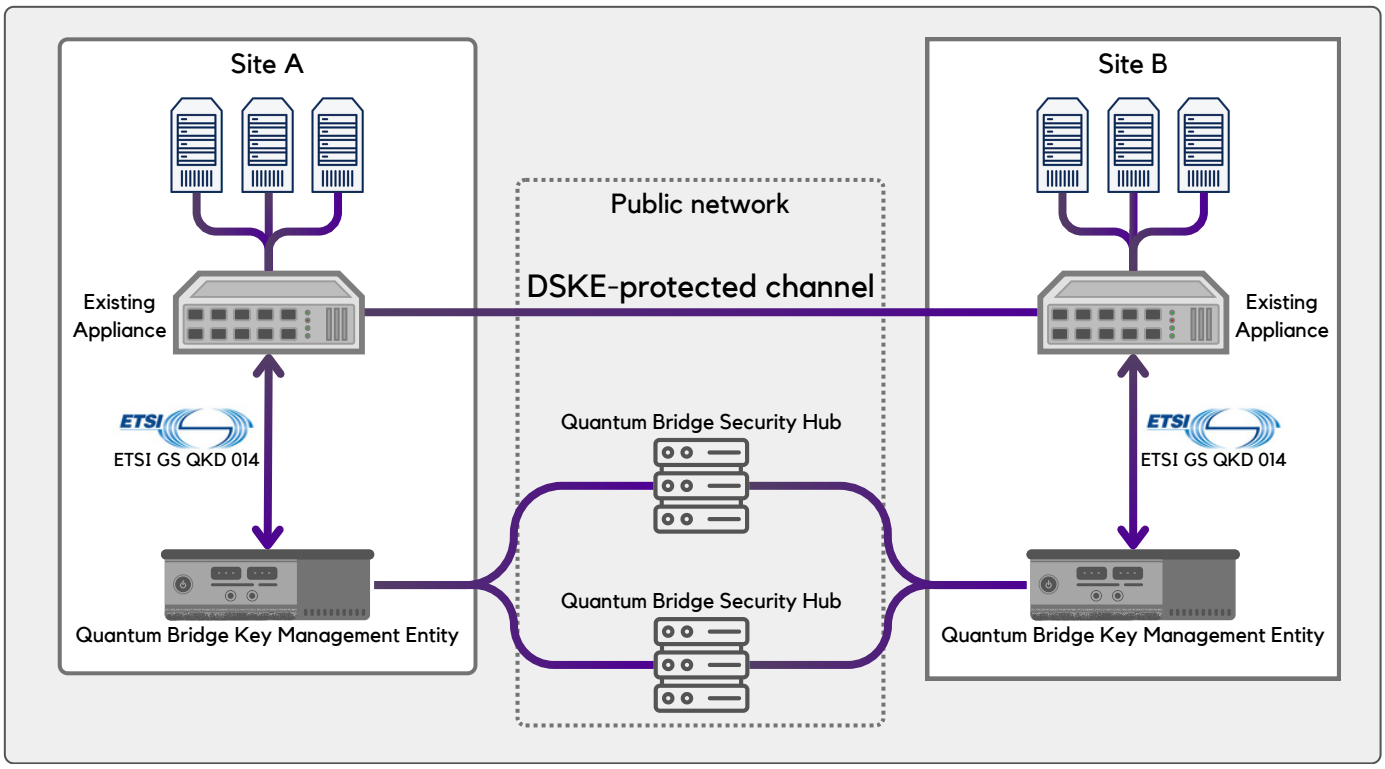




Trust removal.
Alice and Bob generate a key share from each Security Hub, and then combine these shares using a secret sharing protocol. This way, they remove the need to trust any single Security Hub.

Security Hubs never know, nor can reconstruct, the shared key (confidentiality). No complex mathematical operation is used in the protocol (unconditional security).

Infrastructure Security



Solution Summary

Quantum Bridge's **Key Management Entities** (KME) connect directly to existing network appliances (such as firewall, routers, and network encryptors) via ETSI GS QKD 014. The KME can alternatively be integrated directly into existing appliances as a software module, removing the need for any additional hardware in the network. **Security Hubs** orchestrate the generation of secret keys between the KMEs, with redundancy that protects against against failures or compromise. The security of DSKE is formally proven.

Key Features and Benefits

- Perfect secrecy and quantum-safety
- Not certificate-based
- Automated symmetric key distribution
- Layer-agnostic
- Seamless integration into existing networks
- Distributed trust architecture
- Scalable to any number of devices
- Single key-generation mechanism for all PSK-compatible protocols
- Built with Rust's memory- and thread-safe assurances

SDS Value Proposition

⇒ Elevated security of existing IT infrastructure

⇒ Reduced complexity for key management

⇒ Robust, scalable solution that can be integrated with ease

⇒ Quantum resilient: mitigate the quantum threat

Examples of Use Cases

WAN/LAN interconnect.

Quantum Bridge's KME provides cryptographic keys to protect the most valuable information. The Quantum Bridge KME can be interfaced with most existing network appliances to build secure communication networks. The solution can be used to protect traffic between different WAN/LAN networks, especially when communication goes through untrusted third-party infrastructure or the public internet.

Data centre interconnect.

Quantum Bridge KME provides information-theoretical security, meaning that third parties intercepting data won't be able to extract any information from it. Quantum Bridge KME is layer-agnostic and can integrate into Layers 1, 2, and 3, interfacing with existing network appliances, or running as a native application in existing hardware. The KME can be used to provide secure access to data centres and guarantee the highest level of security for both encryption and authentication.

About Quantum Bridge Technologies

Quantum Bridge is committed to deliver to its customers the highest level of cryptographic security to cope with modern, fast-evolving threat environments. Quantum Bridge's unique and novel approach to key distribution eliminates a wide range of threats and drawbacks typical of other solutions like asymmetric cryptography, Pre-Shared Keys (PSK) and Quantum Key Distribution (QKD). Distributed Symmetric Key Exchange (DSKE) fills the technology gap for all these organizations who cannot compromise on security and need to always stay ahead of the fast-moving threat from computational advances.

Contact Us +1-437-232-9840 contact@qubridge.io

Additional Information

Is DSKE scalable?

The DSKE system is designed to scale to any number of DSKE clients, meaning that the cost of adding a client to a network does not increase as the network size increases, despite the increasing network interconnectivity.

Further, a Security Hub has a scalable structure, being composed of one Security Server and multiple Local Distributors, and meaning that as the geographic region and client base served by the Security Hub grow, the costs remain contained. The Security Server can run in the cloud (for example AWS) or in a colocation. The Local Distributors deliver random data to clients, via either physical delivery or Quantum Key Distribution, depending on each client's need.

How many Security Hubs does DSKE need?

The number of Security Hubs depends on the customer's needs. A minimum of three Security Hubs is recommended for fault tolerance and trust-sharing, since if one of the three Security Hubs is faulty, the DSKE system still maintains its functional and security properties. Depending on the use case, this number can be increased. For example, a customer may want to distribute trust so that even collusion between or failure of two Security Hubs does not compromise the system's function or security, in which case, five Security Hubs suffice.

Who operates the Security Hubs?

The operation of any Security Hub can be directly by the customer, by Quantum Bridge, or by a trusted third-party provider, in any combination.

If a Security Hub is operated by the customer, Quantum Bridge can provide and maintain the software. The customer then runs the Security Server and delivers the random data to the clients from the Local Distributors.

If a Security Hub is operated by Quantum Bridge (or any third-party provider partnering with Quantum Bridge and approved by the customer), the customer simply subscribes the DSKE clients to Security Hubs. Quantum Bridge (or the third-party provider) then runs that Security Server and operates the Local Distributors.