Quantum Bridge

DATA SHEET

Security Hub

Symmetric key distribution and management, without single points of trust.

Layer agnostic
Quantum-safe
No asymmetric cryptography

The Quantum Bridge Security Hub delivers decentralized quantum-safe key management for communication over any layer of the network. Each Security Hub can serve several Distributed Symmetric Key Exchange (DSKE) clients, and it includes a Quantum Random Number Generator (QRNG) to generate high-quality, strong cryptographic keys, providing highly scalable key distribution and management services to support critical data communications.

Quantum Bridge Security Hubs allow effective deployment and seamless integration of symmetric key distribution in any infrastructure. Each Security Hub spawns high-quality random numbers to be delivered to clients. The delivery can happen via secure hard drive shipment, Quantum Key Distribution, or electronically in case the Security Hub already pre-shared keys with the client. Once set up, the Security Hub can provide clients with symmetric keys using the DSKE protocol, without using any asymmetric encryption.

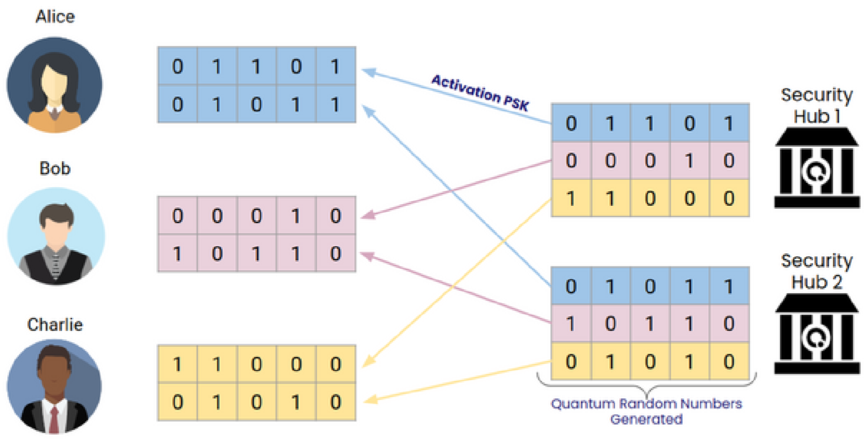
KEY FEATURES AND BENEFITS

- Decentralized, symmetric key management, providing highly scalable key distribution and management services.
- No single point of trust – multiple Security Hubs can seamlessly work together to remove the single point of failure.
- Automatic synchronized key rotation and distribution for any DSKE client.
- Enhanced security, simpler operations, and reduced labor costs through unified key management and encryption policies.

APPLICATIONS

- **Layer 1**: optical encryptors key distribution
- **Layer 2**: macSEC encryptors, routers, switches
- **Layer 3**: IpSec encryptors, WireGuard, VPNs
- **Applications**: emails, VoIP, video calls, SSL/TLS, DTLS
- Integrate easily in custom security solutions at all layers

How it works



Alice

0	1	1	0	1
0	1	0	1	1

Bob

0	0	0	1	0
1	0	1	1	0

Charlie

1	1	0	0	0
0	1	0	1	0

Security Hub 1

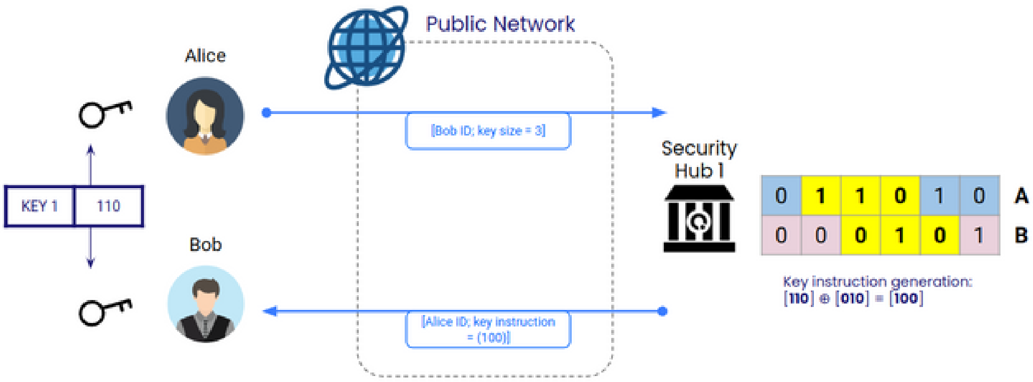
0	1	1	0	1
0	0	0	1	0
1	1	0	0	0

Security Hub 2

0	1	0	1	1
1	0	1	1	0
0	1	0	1	0

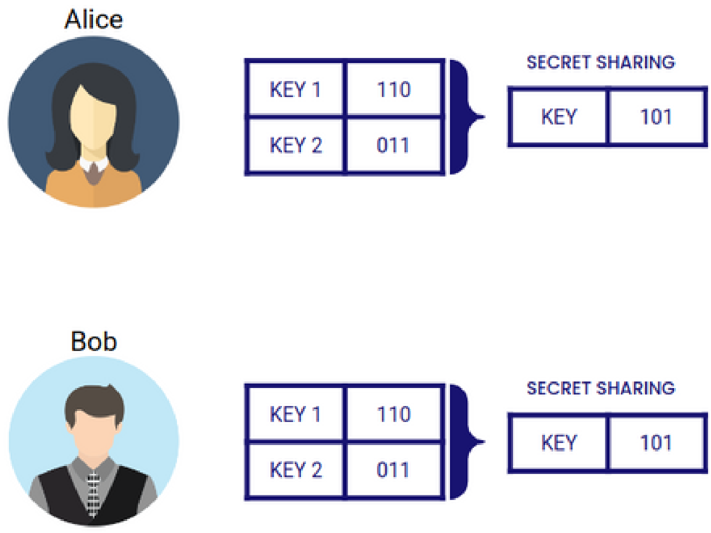
Set-up. When a new DSKE client (Alice, Bob or Charlie here) joins the system, each Security Hub generates some new secret random data from a Quantum Random Number Generator. The random data is delivered to the KME using physical tamper-proof devices or other secure channels.

Key generation. When Alice requests a key with Bob, Security Hub 1 broadcasts the exclusive-or of Alice and Bob's secret strings. Bob can use this to generate a key shared with Alice.



0	1	1	0	1	0	A
0	0	0	1	0	1	B

Key instruction generation: [110] ⊕ [010] = [100]



Alice

KEY 1	110
KEY 2	011

SECRET SHARING

KEY	101

Bob

KEY 1	110
KEY 2	011

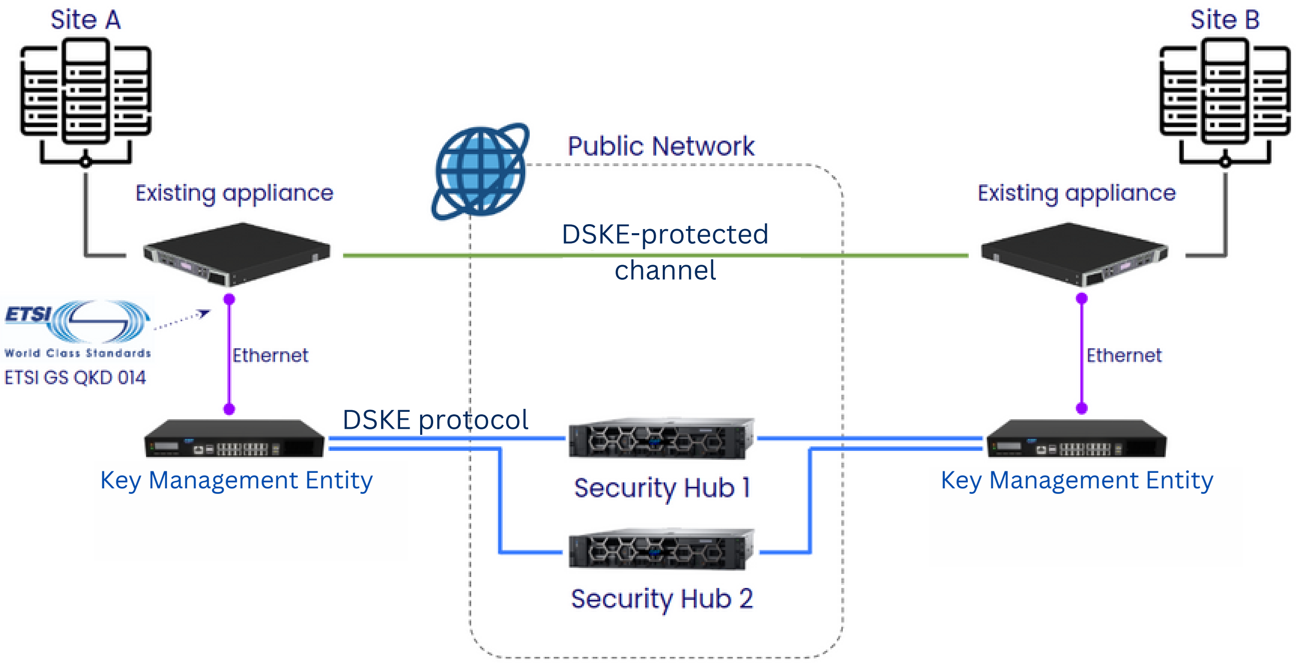
SECRET SHARING

KEY	101

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

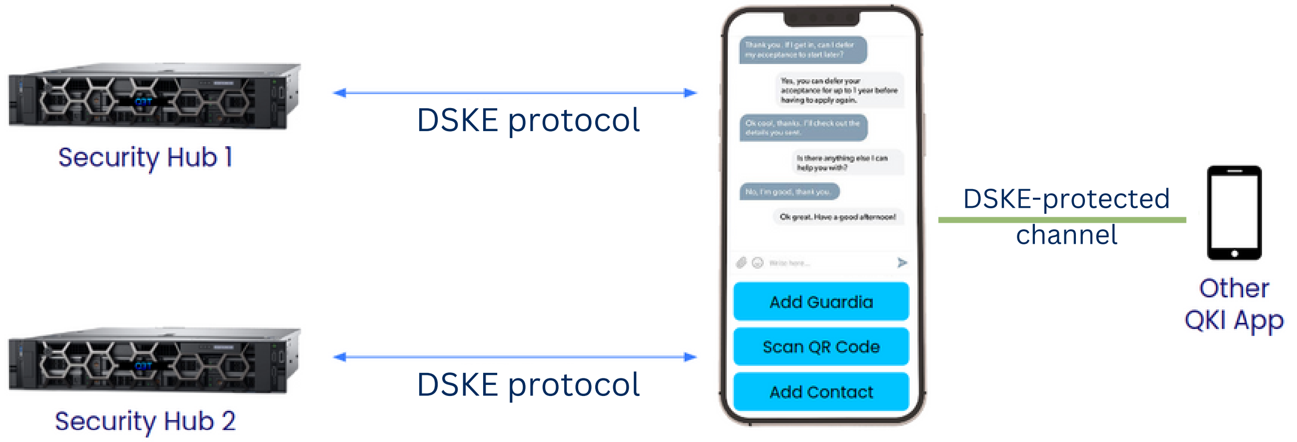
Patented technology: “Encryption key exchange system and method” (US11177950B2)

Application - 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.

Application - Endpoint Security


Thank you. If I get in, can I defer my acceptance to start later?

Yes, you can defer your acceptance for up to 1 year before having to apply again.

Ok cool, thanks. I'll check out the details you sent.

Is there anything else I can help you with?

No, I'm good, thank you.

Ok great. Have a good afternoon!

DSKE clients can be easily integrated into endpoint devices such as mobile phones and personal computers. The DSKE clients provide unconditionally secure authentication and encryption, and remove the need to trust any single service provider. DSKE clients can be easily integrated into existing protocols such as TLS/DTLS, WireGuard, IPsec, or any other customized communication protocol with pre-shared key compatibility.