Open Source
Distributed Symmetric Key Establishment

Funded by RIPE NCC

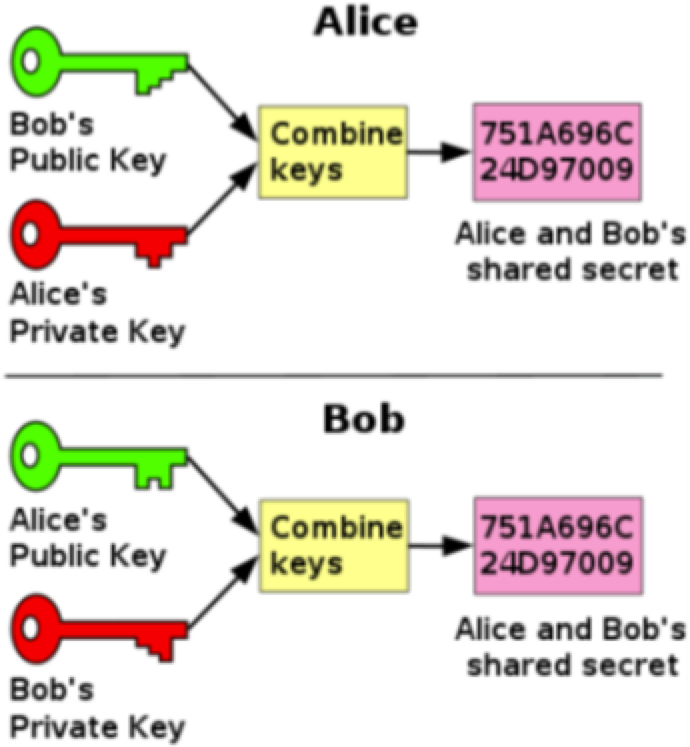
PROBLEM DEFINITION ASYMMETRIC CRYPTOGRAPHY

Problem statement:

- Asymmetric cryptography has a *definitive mathematical link* between public and private key.
- This mathematical connection is usually based on discrete logarithms (used by e.g. Diffie-Hellman).
- Classic computers would take millions/trillions of years to attempt to break Diffie Hellman.
- **Shor's Algorithm** can however be used by quantum computers to break Diffie-Hellman/RSA based cryptographic schemes in polynomial (i.e. short!) timeframes.
- While powerful enough quantum computers are not available now, the concern/opportunity is in attackers stealing and storing encrypted data to decrypt with the quantum computers of tomorrow.

Conclusion:

Asymmetric cryptography as it exists today is not, and cannot, therefore be 'quantum secure'.



Agencies Perspective

"By December 31, 2023, agencies maintaining NSS shall implement symmetric-key protections [...] to provide additional protection for quantum-vulnerable key exchanges."

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, May 2022

"Symmetric Pre-Shared Keys (PSKs) should be used instead of or in addition to asymmetric public/private key pairs to provide quantum resistant cryptographic protection of classified information within CSfC solutions."

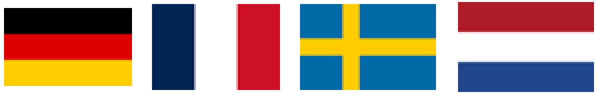
National Security Agency, Commercial Solutions for Classified, May 2022

Agencies Perspective

“Novel PQC standards are being developed to address this threat, and are under a great deal of expert scrutiny to assure their security. Nevertheless, it is theoretically impossible to prove whether any such algorithm is secure. The potential impact of a failure of new cryptographic standards is great, so there is scientific interest in understanding alternatives and complementary solutions, such as quantum-secured communications.”

Overview of Quantum 2030, DND/CAF 2023

“In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.”



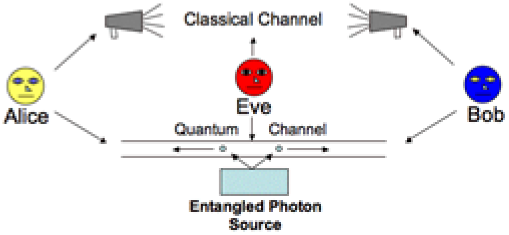
“Position Paper on Quantum Key Distribution” 2024

Quantum-safe key exchange options

Post-Quantum Cryptographic Algorithms

- Standardization of new 'quantum resistant' crypto algorithms in the works
- May be vulnerable against "classical computer" attack
- Selection process finalized

Quantum Key Distribution (QKD)



- Hardware based
- Uses photon properties to generate secure keys
- Limited range (for now)
- Point-to-Point (for now)

Symmetric Key Establishment

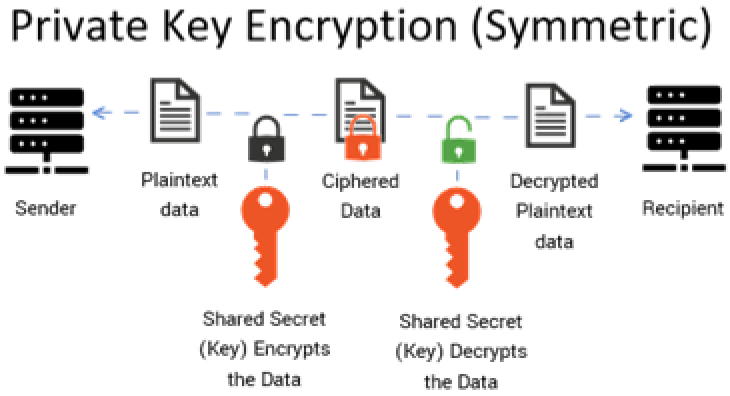
- Add an additional secret to symmetric key material based on long random number
- Otherwise uses normal IKE/IPsec standards
- Key distribution mechanism not standardized (yet)

SOLUTION
SYMMETRIC KEY CRYPTOGRAPHY

- Keys cannot be intercepted.
- No public/private pairs.
- No mathematics in the key creation so cannot be reverse engineered – long random numbers which are unbreakable are the ‘essence’ of secure symmetric key.
- Quantum Random Number Generator (QRNG) can be used to derive keys with high entropy.
- Symmetric keys are therefore ‘quantum safe’.

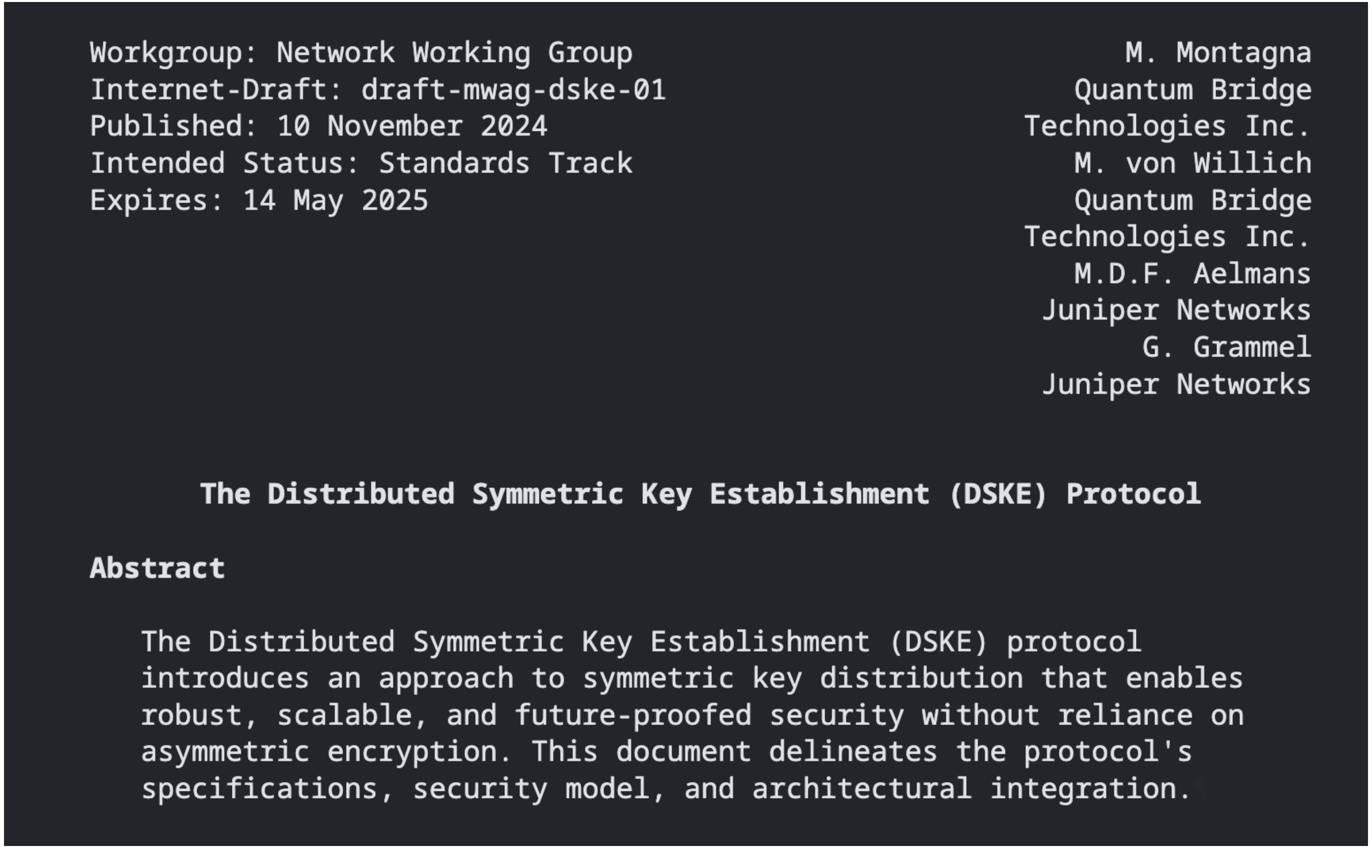
However…..

- Symmetric key exchange is not easily scalable.
- Symmetric keys may be difficult to securely distribute over current communications structure.


Private Key Encryption (Symmetric)
Sender
Plaintext data
Ciphered Data
Decrypted Plaintext data
Recipient
Shared Secret (Key) Encrypts the Data
Shared Secret (Key) Decrypts the Data

DSKE Protocol

DSKE standardisation effort in IETF



Workgroup: Network Working Group
Internet-Draft: draft-mwag-dske-01
Published: 10 November 2024
Intended Status: Standards Track
Expires: 14 May 2025

M. Montagna
Quantum Bridge Technologies Inc.
M. von Willich
Quantum Bridge Technologies Inc.
M.D.F. Aelmans
Juniper Networks
G. Grammel
Juniper Networks

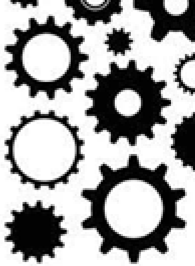
The Distributed Symmetric Key Establishment (DSKE) Protocol

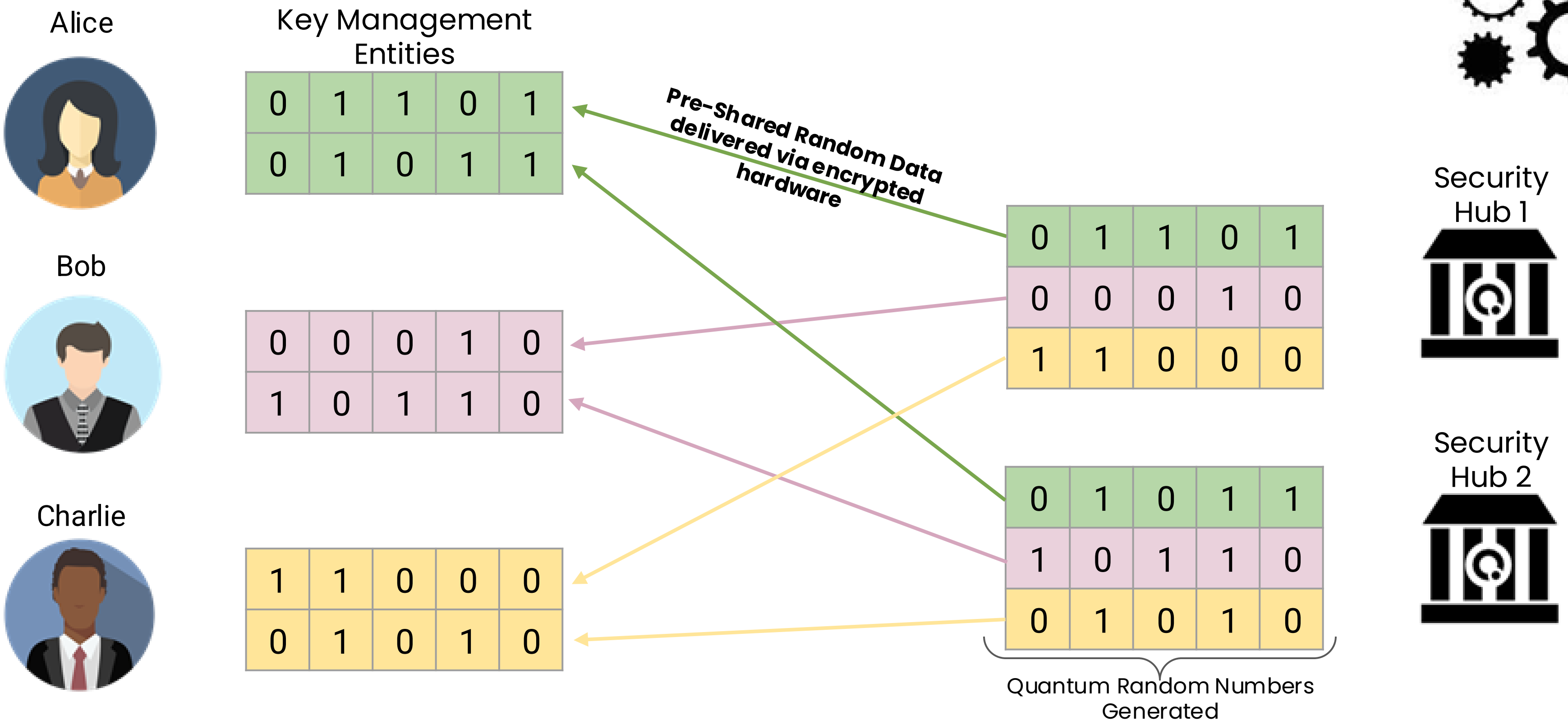
Abstract

The Distributed Symmetric Key Establishment (DSKE) protocol introduces an approach to symmetric key distribution that enables robust, scalable, and future-proofed security without reliance on asymmetric encryption. This document delineates the protocol's specifications, security model, and architectural integration.

https://datatracker.ietf.org/doc/draft-mwag-dske/

Set-up Phase





Alice

Bob

Charlie

Key Management Entities

0	1	1	0	1
0	1	0	1	1

0	0	0	1	0
1	0	1	1	0

1	1	0	0	0
0	1	0	1	0

Pre-Shared Random Data delivered via encrypted hardware

Security Hub 1

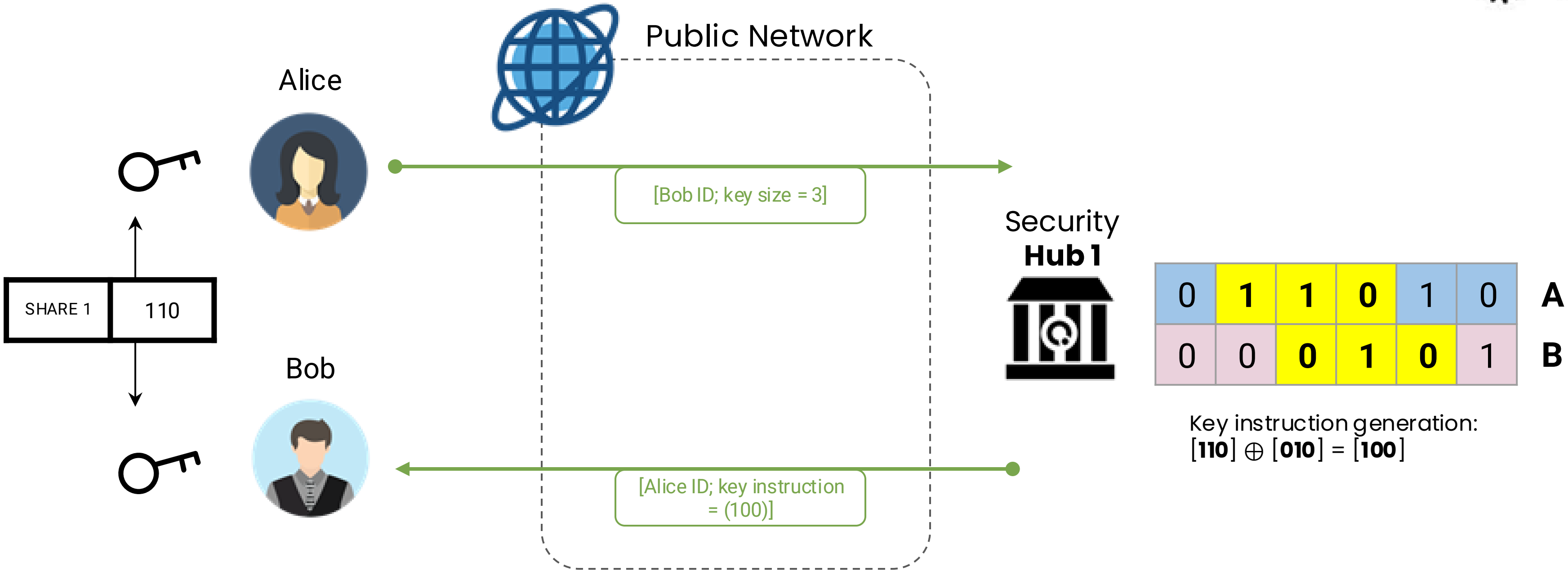
0	1	1	0	1
0	0	0	1	0
1	1	0	0	0

Security Hub 2

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

Quantum Random Numbers Generated

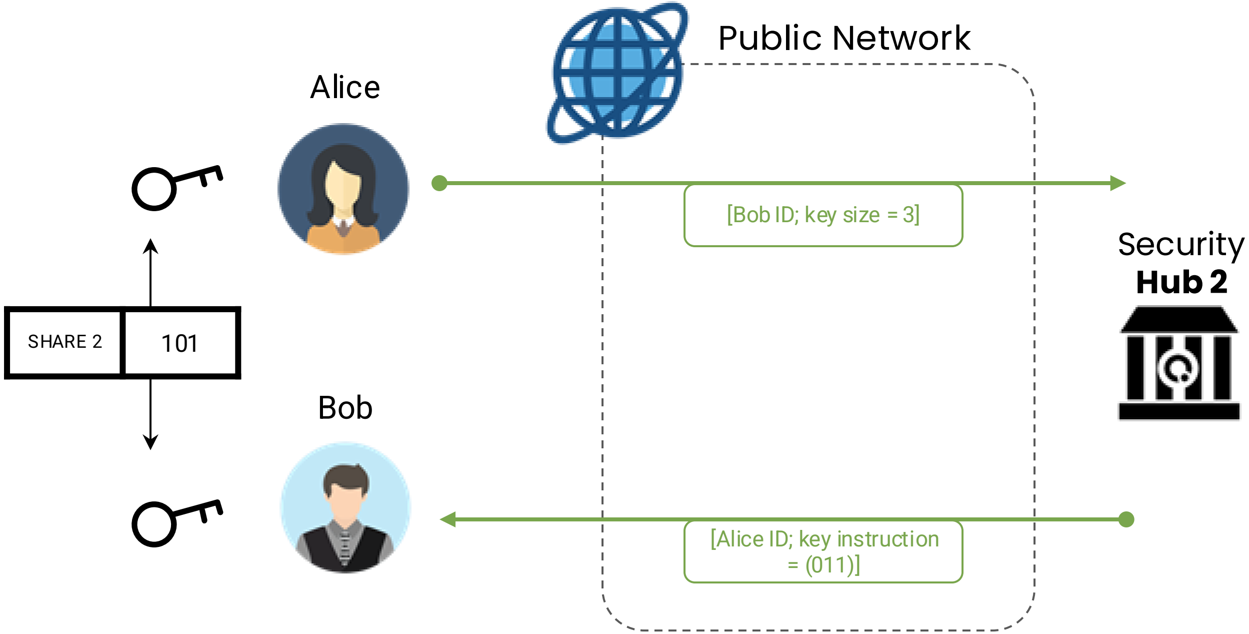
Key Share Creation – Hub #1



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

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

Key Share Creation – Hub #2



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

Key instruction generation:
[**101**] ⊕ [**110**] = [**011**]

Trust Distribution

Alice

SHARE 1	110
SHARE 2	101

SECRET SHARING

KEY	011

Bob

SHARE 1	110
SHARE 2	101

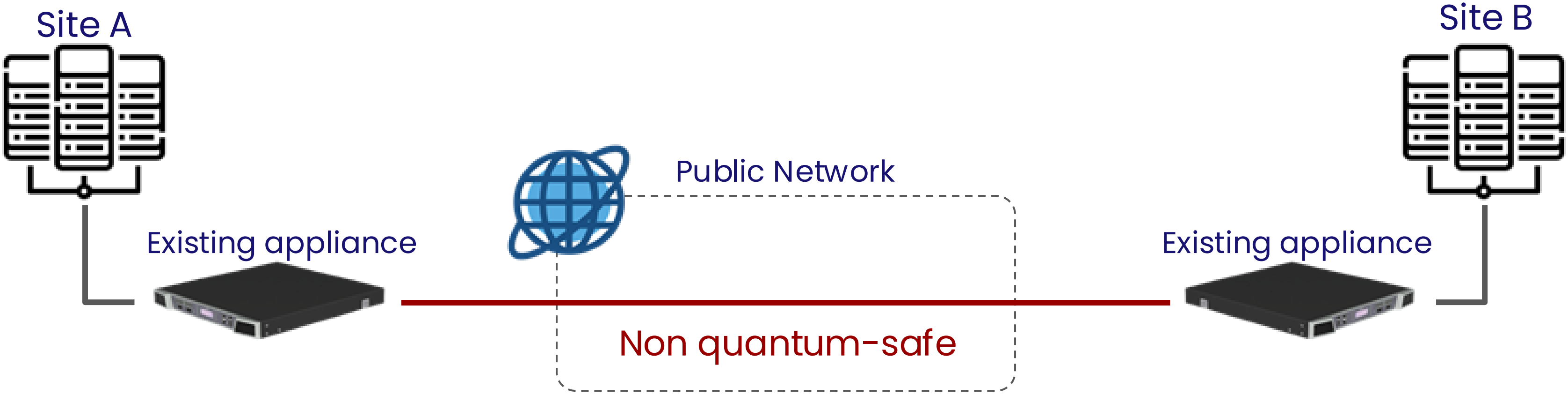
SECRET SHARING

KEY	011

Final secret keys

- ✓ Quantum-secure
- ✓ No single Security Hub knows the key
- ✓ Delivered over the Internet
- ✓ On-demand and pre-share modes

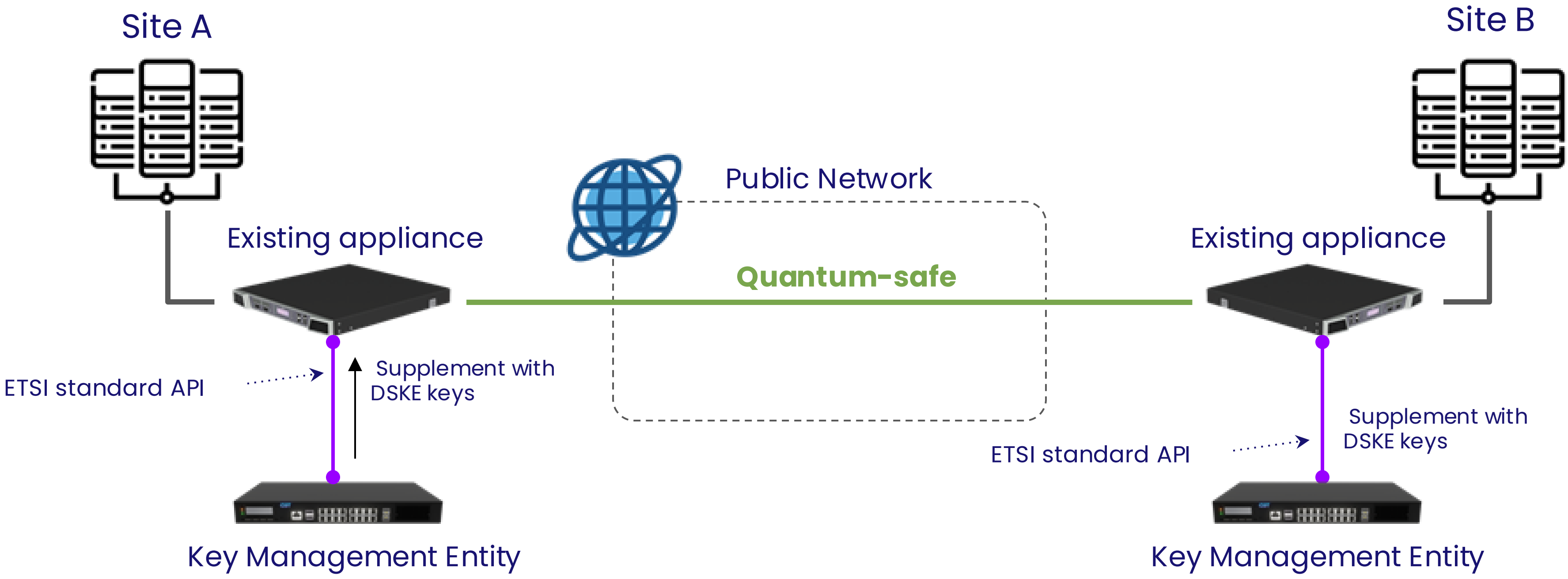
Network Security



Current infrastructure:

- PKI based networks
- Subject to **harvest now decrypt later**
- Difficult to upgrade using QKD and/or PQC

Network Security



Project timeline

- Contract developer
- Scope the work based on the IETF draft
- Build open source KME application

Questions?

melchior@aelmans.eu