Quintessence Labs

# qConnect
# Quantum Safe Key Distributor

April 2025

# Current situation

- Data-in-transit is protected using **cryptography**
  - Confidentiality, integrity, authentication and non-repudiation
  - TLS, IPSec, SSH
  - VPN for secure server-server and client-server communications channels
  - HTTPS for secure online services: banking, online sales, bill payment, document transfer, email, social media, cloud storage, …
  - SSH for secure remote login, and control and monitoring of IT infrastructure
- Public key cryptography (RSA, ECC, DH) enables **key exchange** for confidentiality and integrity, and **digital signatures** for authentication and non-repudiation
- High degree of **interoperability** and ease of use
- Almost all electronic systems interacting with each other or with humans over networks rely on the security provided by **public key cryptography**

# The problem

- **Quantum computing poses a threat** to the security of our cryptographic systems
  - RSA, ECC, and DH public key cryptography are vulnerable to quantum attack
  - Harvest Now, Decrypt Later
- Standards for potentially new, quantum-safe public key algorithms have been released
  - Wide-spread and interoperable **deployment will take time**
  - **Legacy systems could be vulnerable** while updates and new infrastructure are rolled out
  - Standards for supporting PQC in TLS, IPSec/IKE, SSH, CMS are **still under development**
  - **PQC is not yet proven over time** in the field
- **QKD** offers a safe, quantum-resistant alternative, or addition, to PQC for key distribution
  - **Point-to-point** only
  - **Key rate, distance and latency may be issues** for some deployments
  - **Not recommended**, or **not approved**, in some scenarios

# The solution

- **Flexibility** in deployment
  - Support both PQC and QKD, separately or together
  - “Defence in depth”
- Maximise **interoperability**
  - Delegate connectivity to deploy “quantum-safe” more quickly
- **Support legacy** with a quantum-safe key distribution layer
- Overcome technology limitations
  - **Extend the reach** of QKD systems
  - Provide a logical key distribution network overlay for **fault tolerance**

**The qConnect Quantum Safe Key Distributor delivers a future-ready solution for distributing symmetric key material across hybrid cryptographic infrastructures**

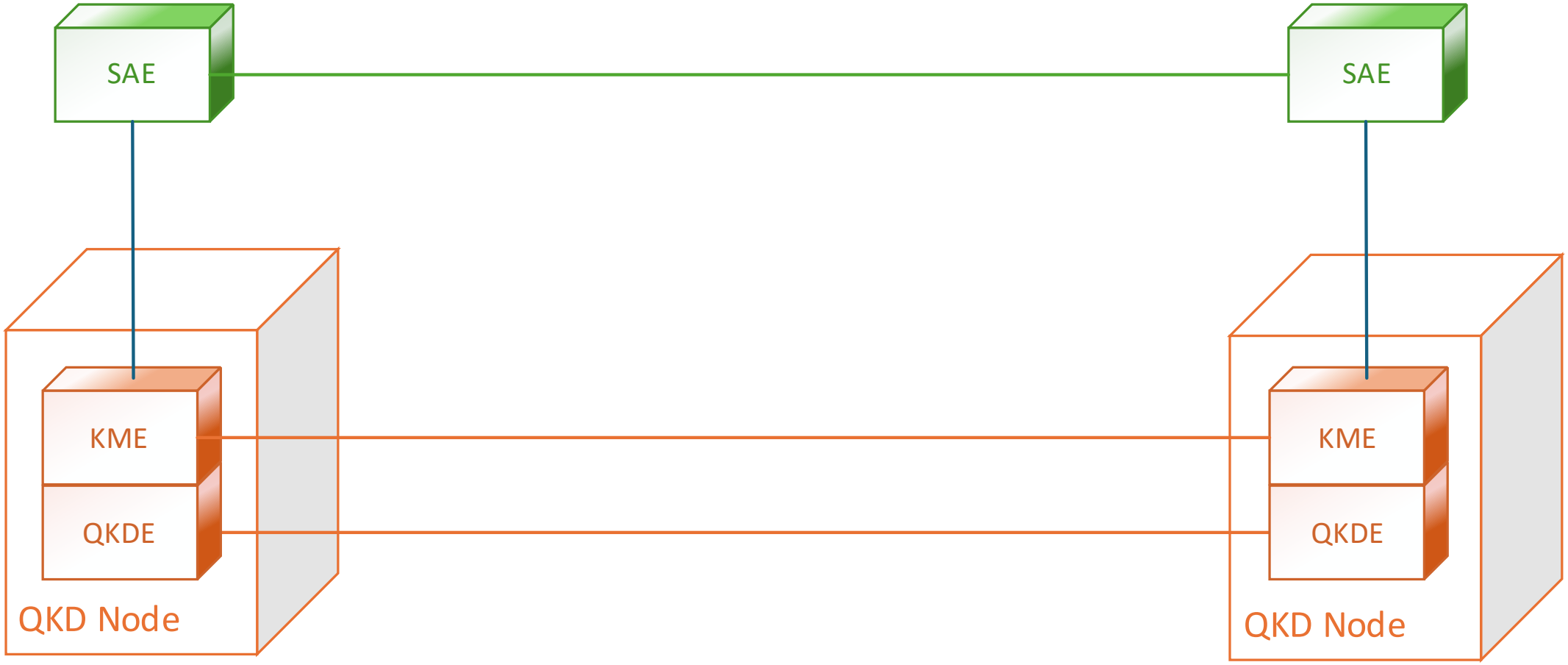
# qConnect feature summary

- Quantum safe distribution of cryptographic keys
  - Protected by PQC and/or QKD
- 1RU 19-inch rack mount with internal QRNG or virtual appliance
- Internal QRNG, network-attached QRNG, or ETSI 014 key sources
- ETSI 014, SKIP, and NOKIA key output
- Hybrid QKD/PQC key delivery
- Provider, pass-through, and buffer modes of operation
- Network HSM supported as a root of trust

**The qConnect Quantum Safe Key Distributor delivers a future-ready solution for distributing symmetric key material across hybrid cryptographic infrastructures**

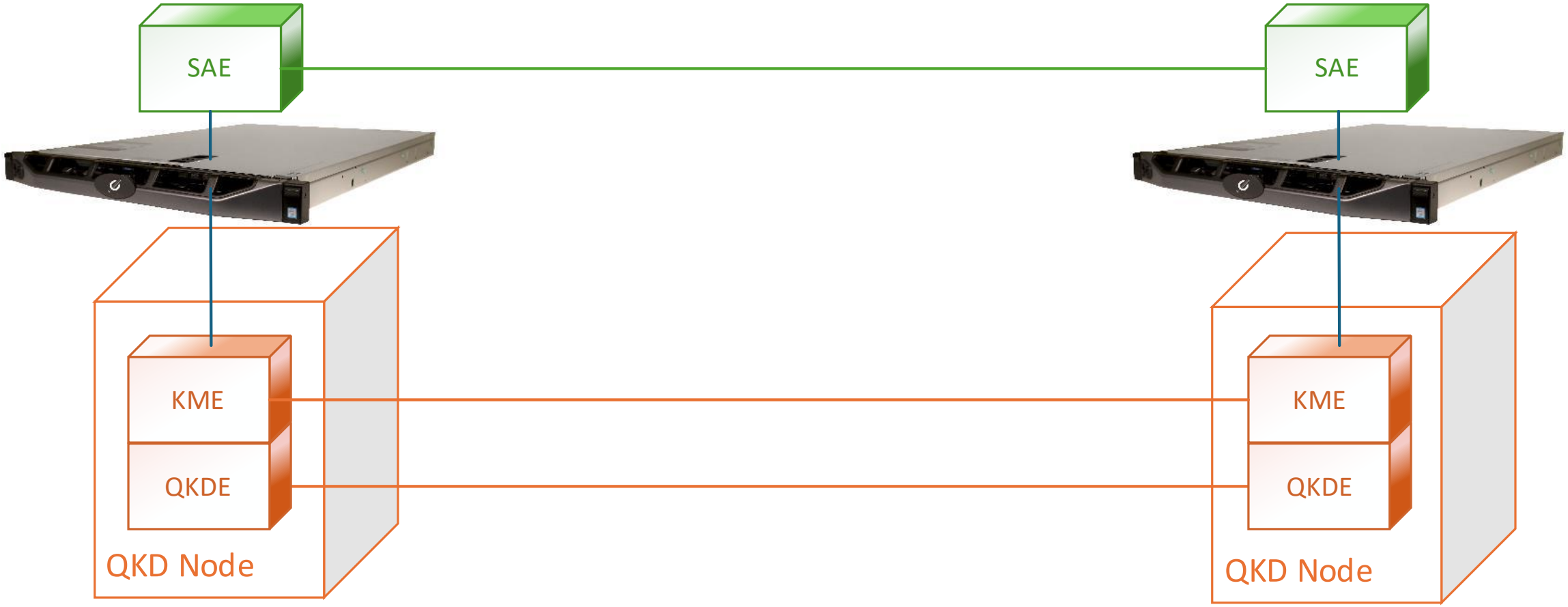
# Use cases and recommendations
## (Slightly technical stuff)

# Simplest QKD
## One pair of nodes



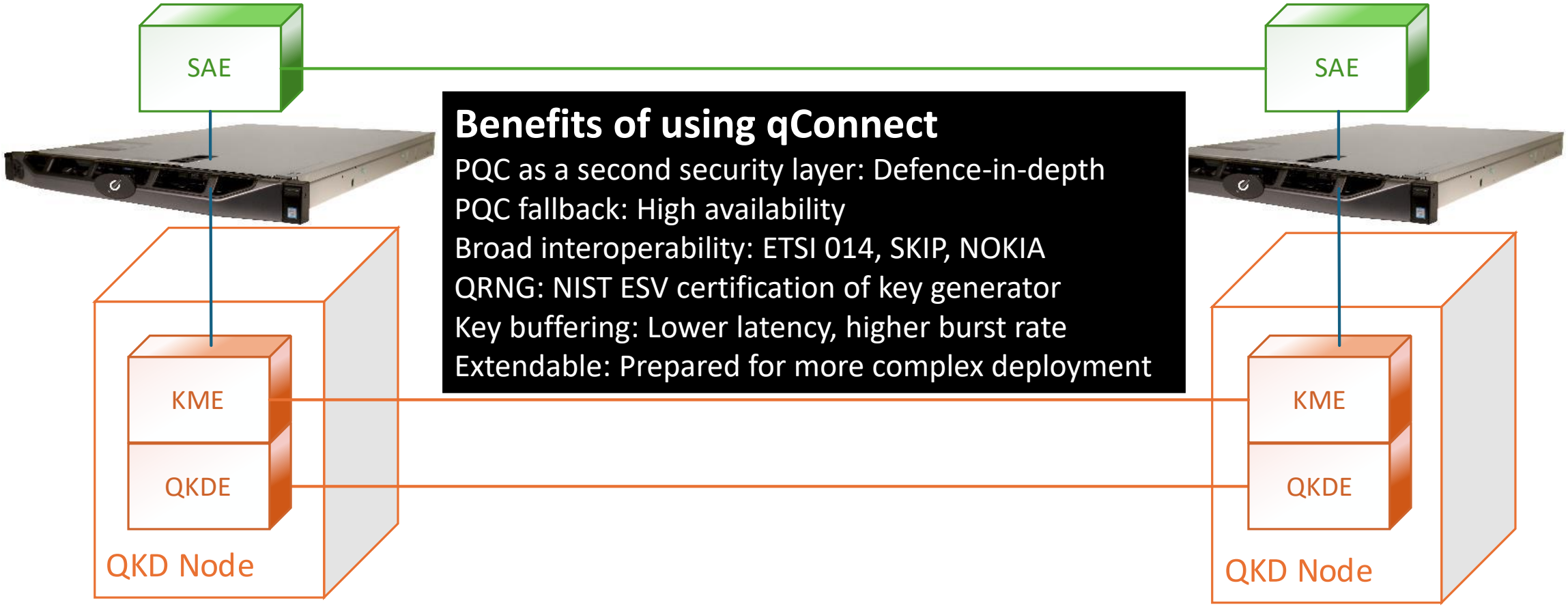
# Better, simplest QKD

## Add qConnect



# Better, simplest QKD

## Add qConnect

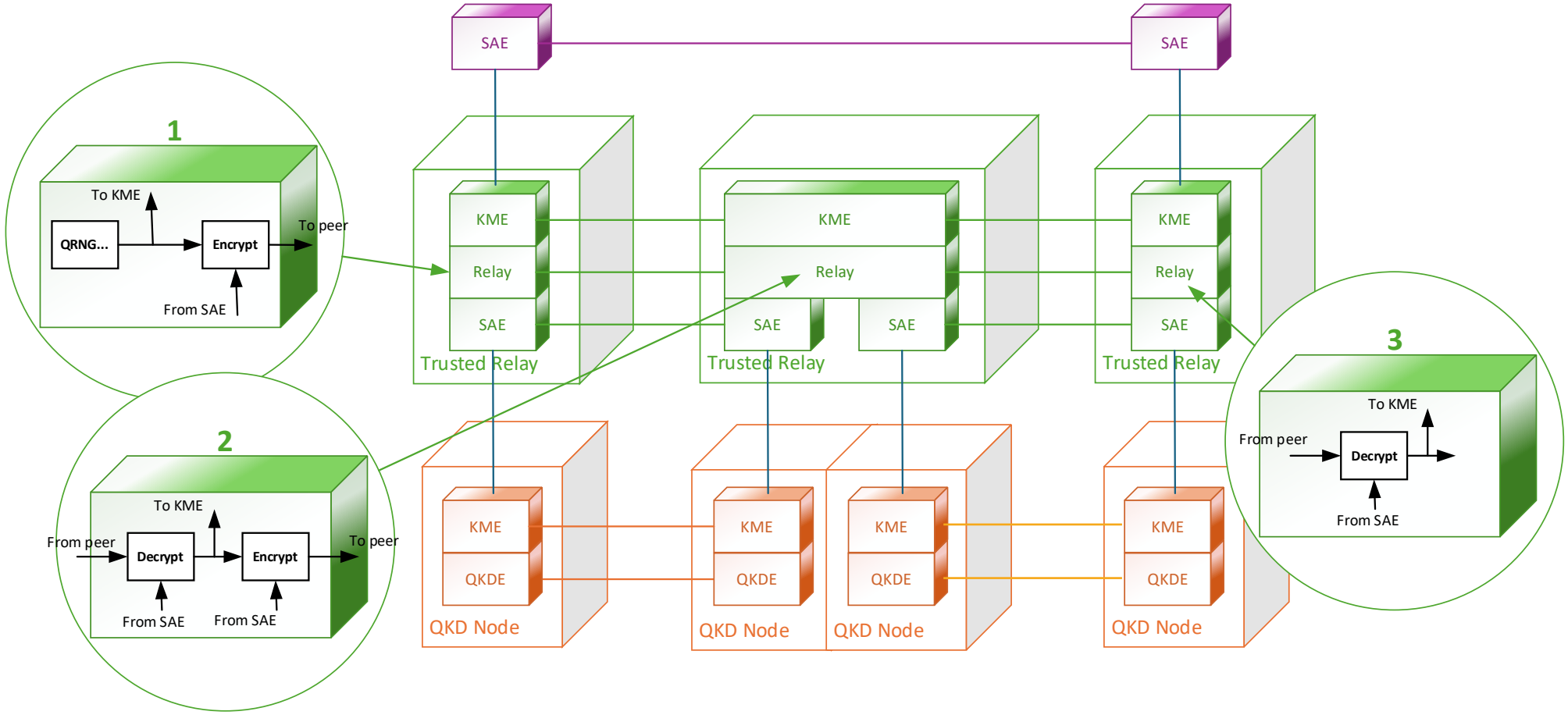



**Benefits of using qConnect**

PQC as a second security layer: Defence-in-depth
PQC fallback: High availability
Broad interoperability: ETSI 014, SKIP, NOKIA
QRNG: NIST ESV certification of key generator
Key buffering: Lower latency, higher burst rate
Extendable: Prepared for more complex deployment

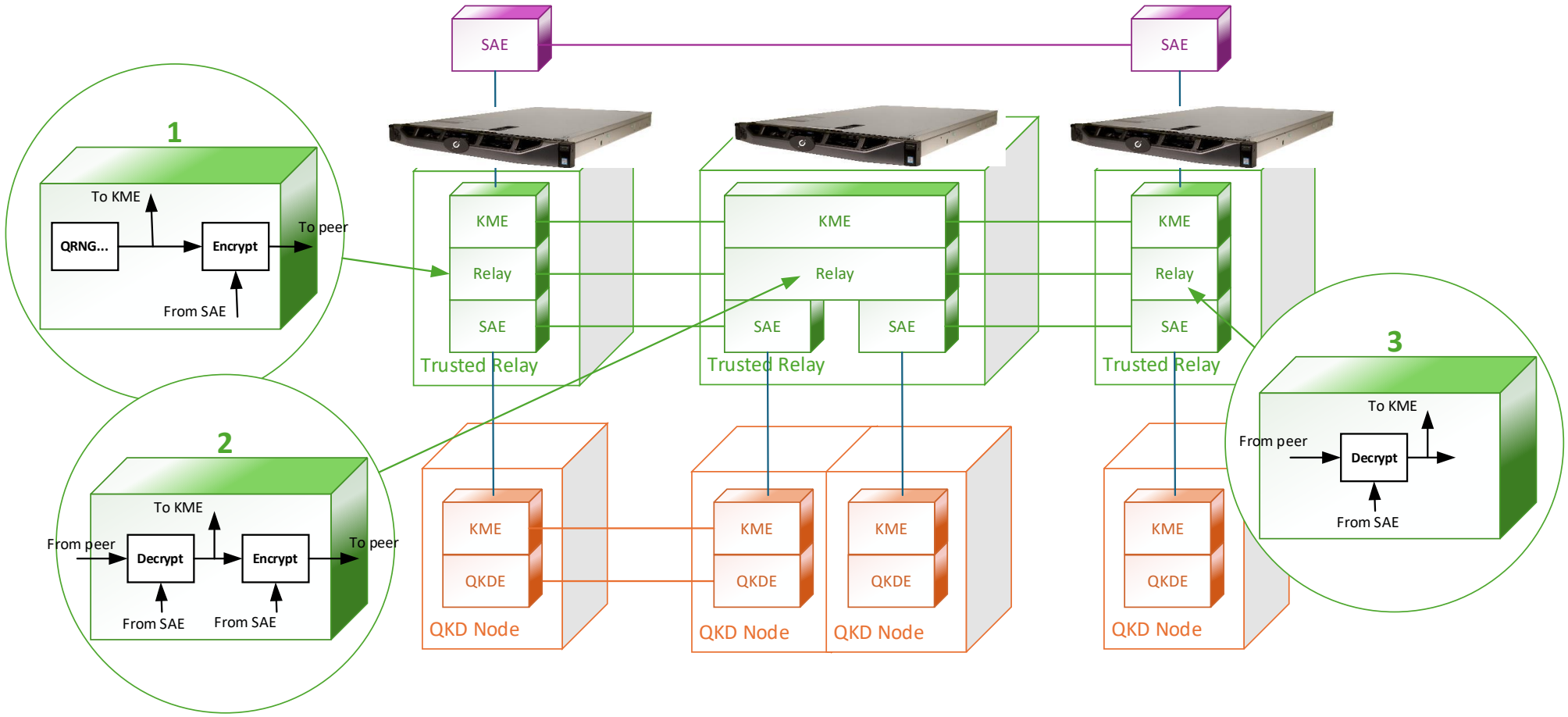
# QKD with trusted relay nodes

## Extend end-to-end reach with QKD



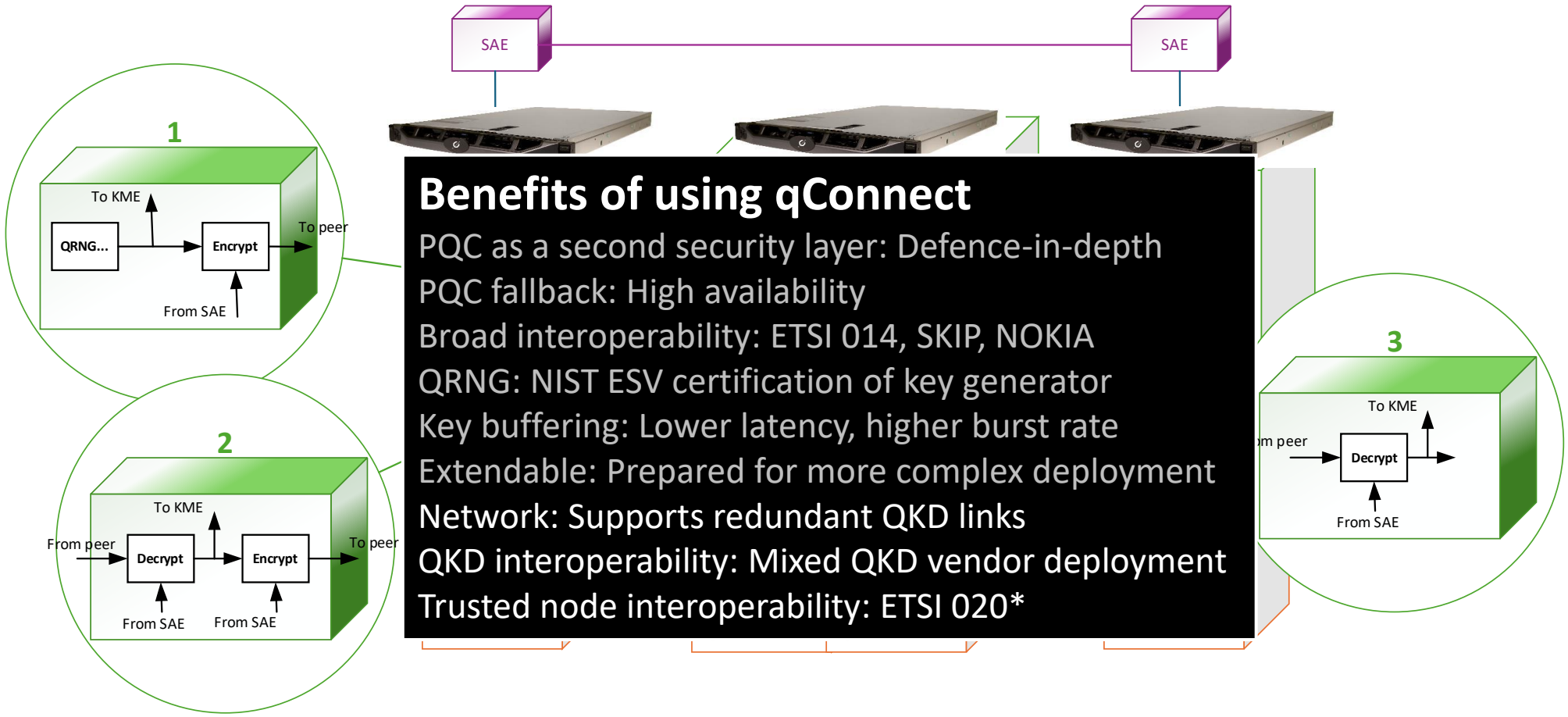
# QKD with trusted relay nodes

## qConnect as a trusted node



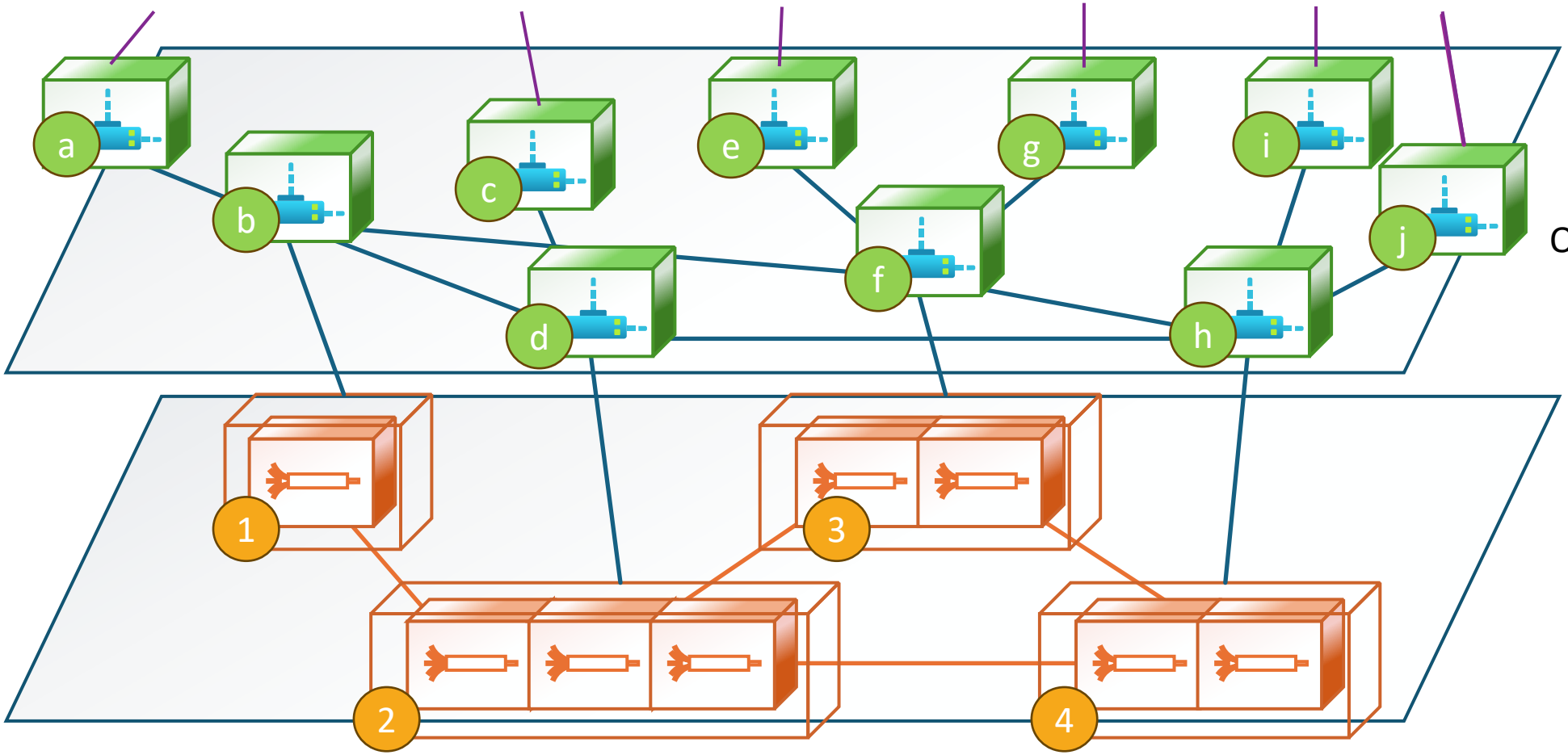
# QKD with trusted relay nodes

## qConnect as a trusted node



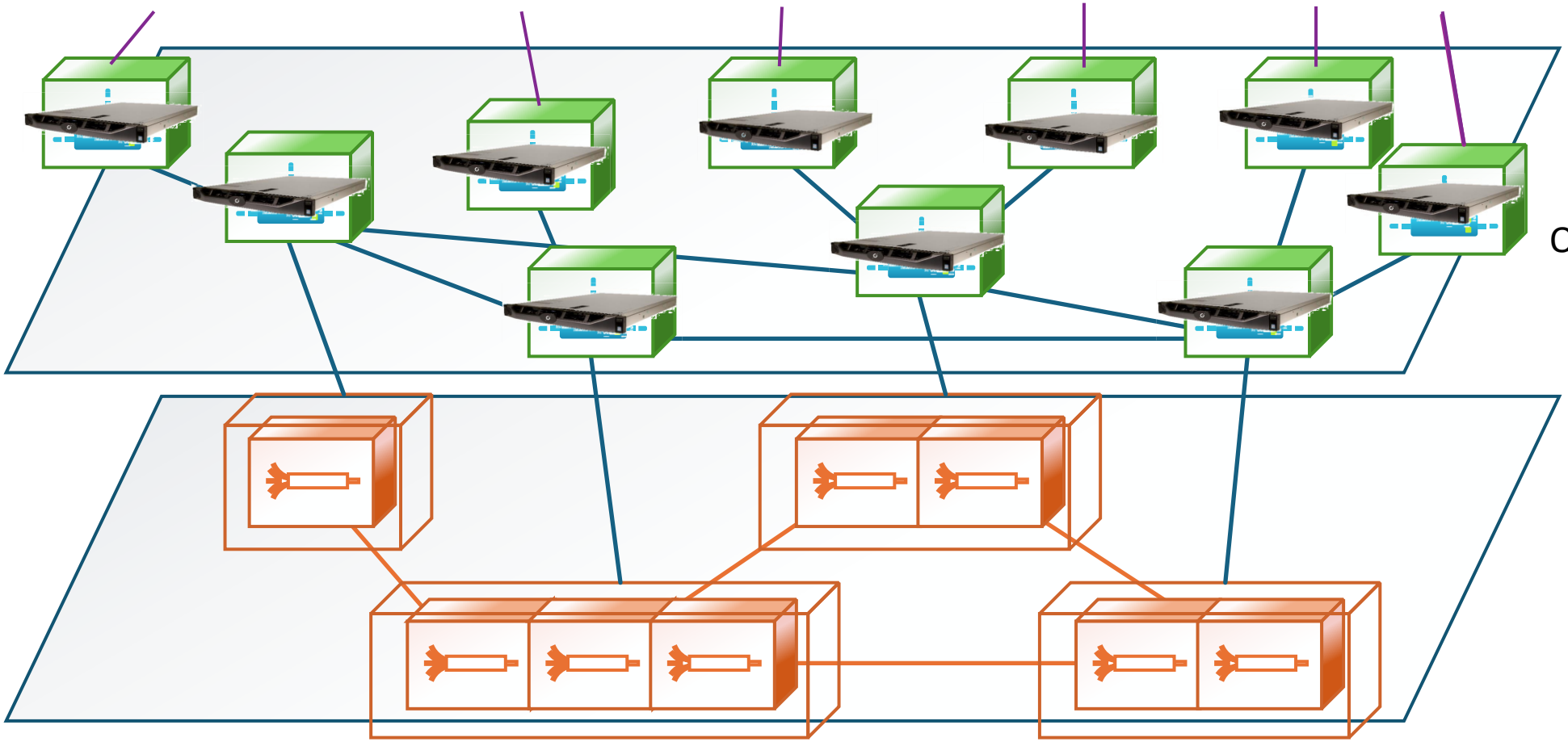
# Hybrid QKD/PQC key distribution

## Extend end-to-end reach beyond QKD



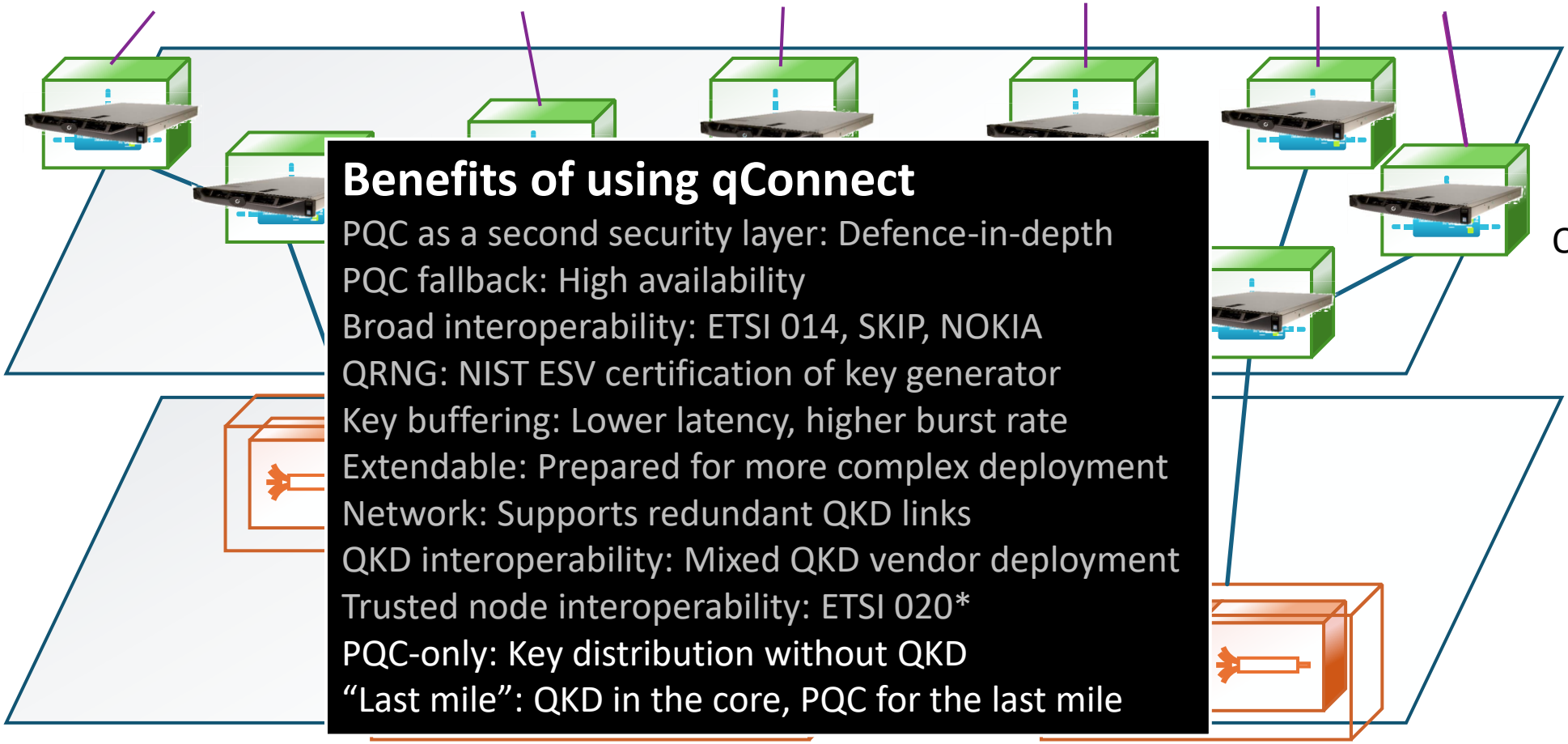
# Hybrid QKD/PQC key distribution

## Extend end-to-end reach beyond QKD



# Hybrid QKD/PQC key distribution

## Extend end-to-end reach beyond QKD



**Benefits of using qConnect**

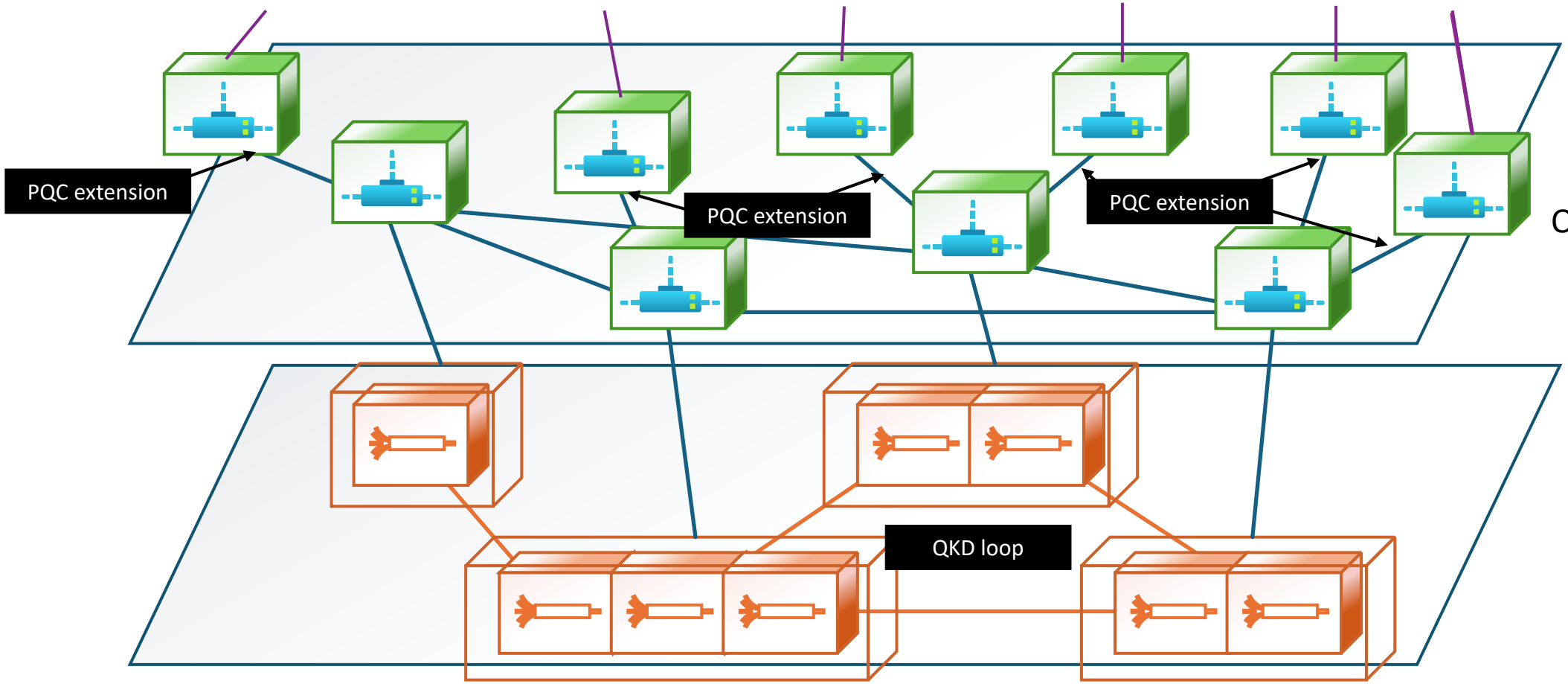
PQC as a second security layer: Defence-in-depth
PQC fallback: High availability
Broad interoperability: ETSI 014, SKIP, NOKIA
QRNG: NIST ESV certification of key generator
Key buffering: Lower latency, higher burst rate
Extendable: Prepared for more complex deployment
Network: Supports redundant QKD links
QKD interoperability: Mixed QKD vendor deployment
Trusted node interoperability: ETSI 020*
PQC-only: Key distribution without QKD
“Last mile”: QKD in the core, PQC for the last mile

Quantum-safe key delivery network

QKD

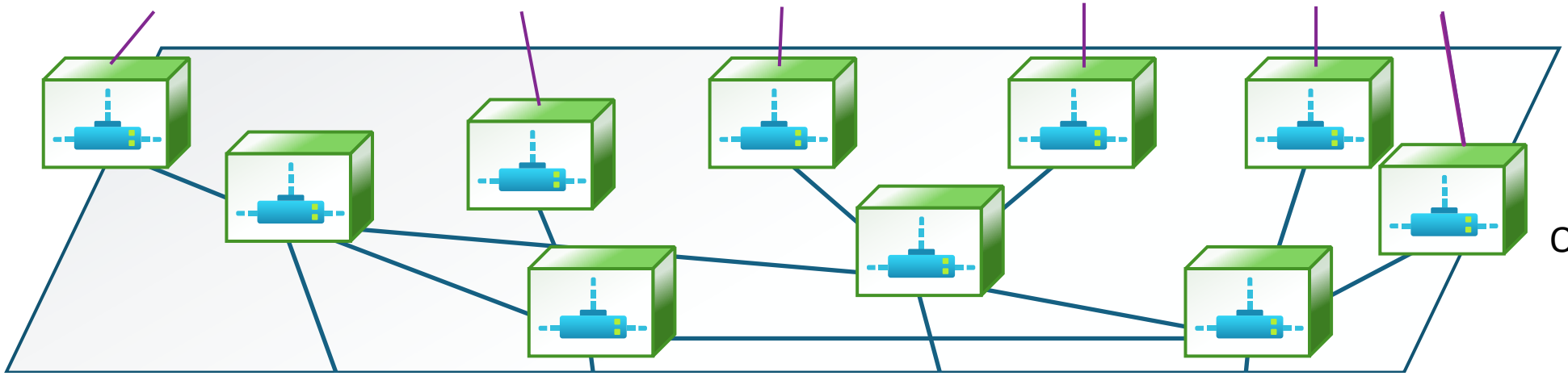
# Hybrid QKD/PQC key distribution

## Extend end-to-end reach beyond QKD



# PQC key distribution

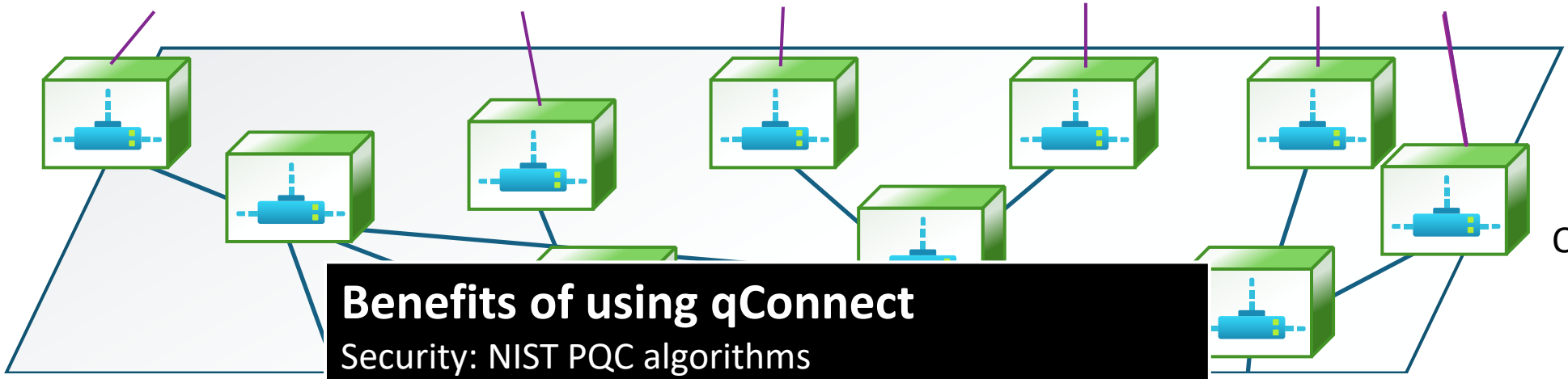
## Use only PQC for quantum safe key delivery



Quantum-safe key delivery network

# PQC key distribution

## Use only PQC for quantum safe key delivery



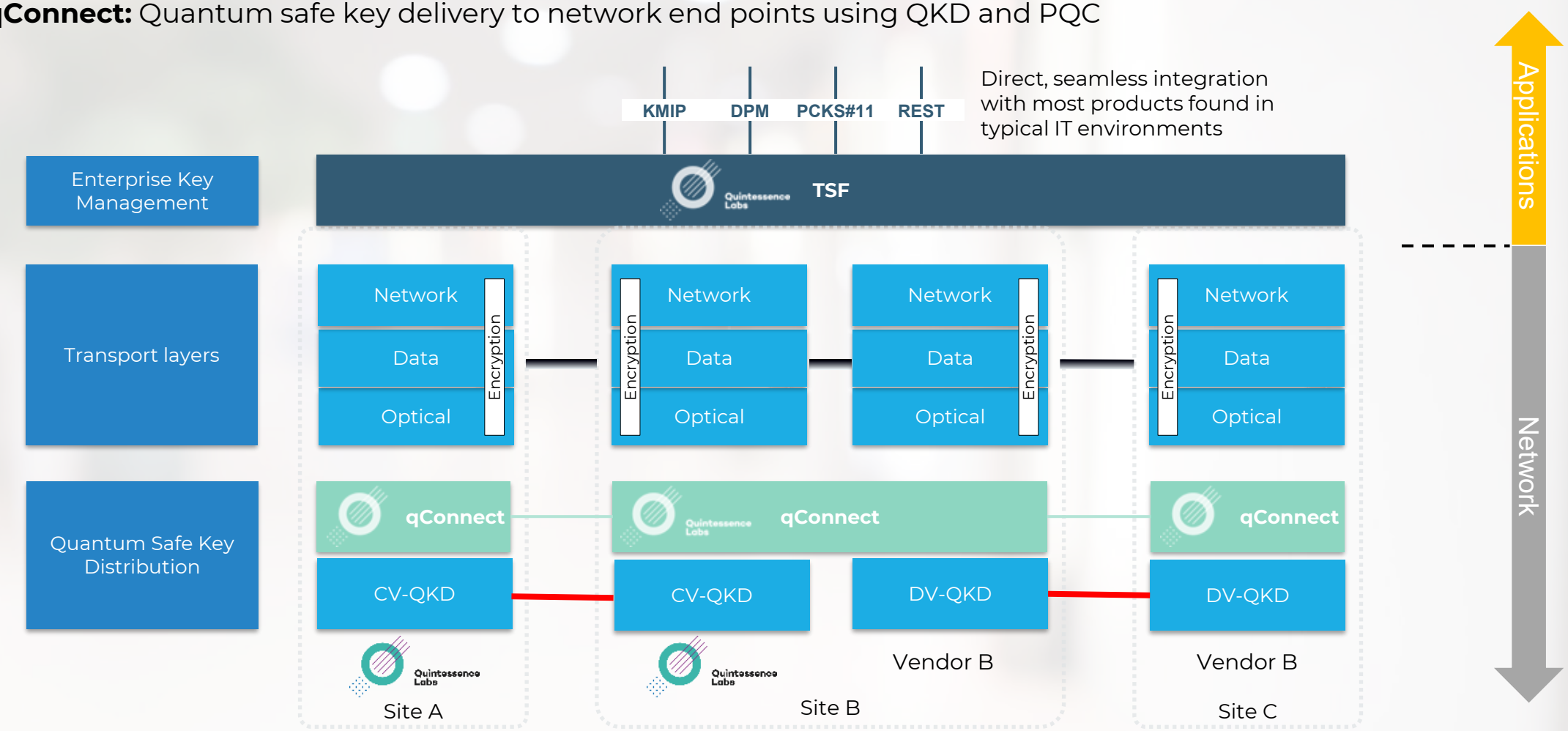
Quantum-safe key delivery network

**Benefits of using qConnect**

Security: NIST PQC algorithms
IP routing: Only requirement is an IP network
Broad interoperability: ETSI 014, SKIP, NOKIA
QRNG: NIST ESV certification of key generator
Key buffering: Lower latency, higher burst rate
Extendable: Prepared for more complex deployment
Network: Supports redundant links
PQC-only: Key distribution without QKD
QKD ready: PQC now, QKD can be added later

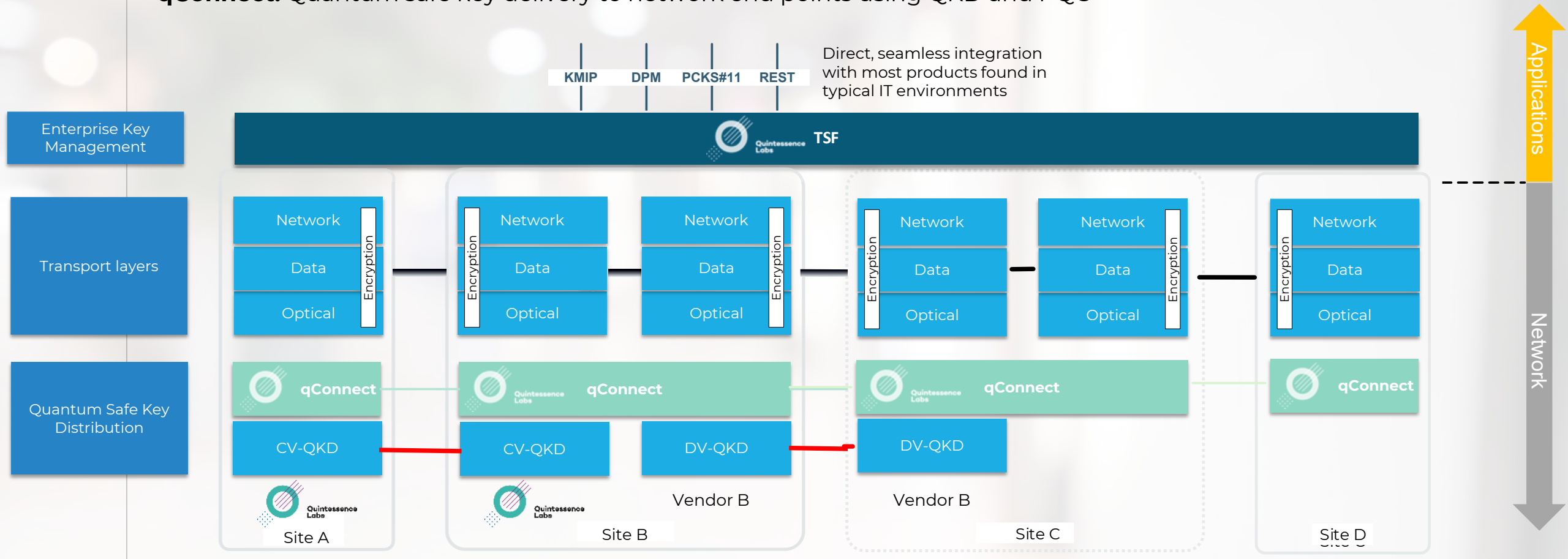
# Use Case: Hybrid QKD/PQC Key Distribution

**Trusted Security Foundation:** Cryptographic key and policy management for Enterprise Applications
**qConnect:** Quantum safe key delivery to network end points using QKD and PQC



# Use Case: Hybrid QKD/PQC Key Distribution - PQC “last mile”

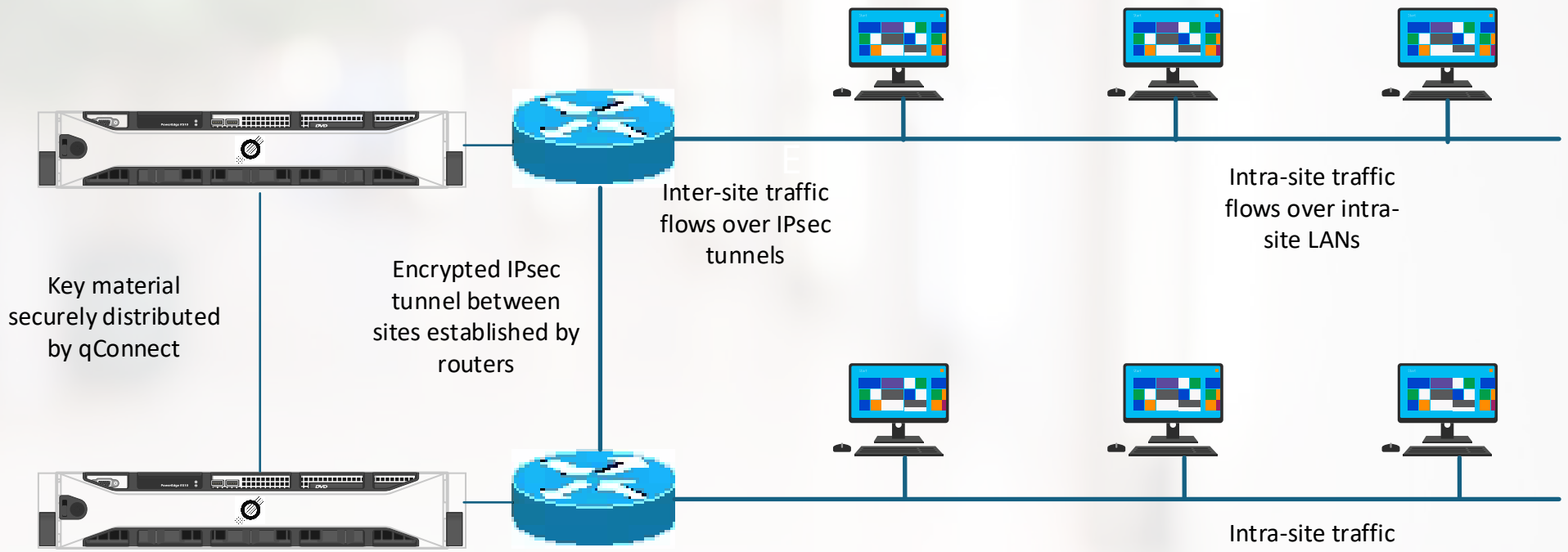
**Trusted Security Foundation:** Cryptographic key and policy management for Enterprise Applications
**qConnect:** Quantum safe key delivery to network end points using QKD and PQC



# Use Case: Quantum-resilient VPN and Link Encryption

**FACT:**
Most VPN and OTN links are vulnerable to HNDL attacks and QKD might not be applicable due to its limitations

**SOLUTION:**
QRA are used to provide QS security for delivery of key material used by the VPN devices or link encryptors



# Use Case: Additional QRNG Key Material for VPN's

**FACT:**
Most VPN equipment uses RSA/ECC asymmetric crypto to exchange AES keys. Vulnerable to quantum attack.
**SOLUTION:**
Deliver a 2nd crypto key material into local and remote encryption devices, generated out of a QRNG, at a price point that is viable and not technically overwhelming. Instantly increases your security posture over the WAN