

# BasejumpQDN™ Overview

## Quantum-Safe Networking for Trusted Service Providers

As the quantum era approaches, protecting data requires more than conventional cryptography. BasejumpQDN™ from evolutionQ enables trusted service providers, telecoms, utilities, cloud operators, government and enterprise networks to deploy quantum-safe key distribution at scale.

The Basejump platform unifies Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC) into a single interoperable control plane providing end-to-end key establishment across optical, satellite, and wireless networks. BasejumpQDN is architected to be crypto agile with the ability to change (algorithms and key sizes) over time depending on the desired security posture. It can deliver pure QKD keys, pure PQC keys or a hybrid for greater defence-in-depth security.

### What BasejumpQDN™ Does

BasejumpQDN™ orchestrates keys across multi-vendor, multi-domain networks through a standards-based Quantum Delivery Network (QDN). It abstracts the complexity of quantum systems, enabling secure interconnection between enterprise sites, cloud regions, and national backbones.

### Core Functions

**Vendor-Neutral QKD Operations** – Validated with over 10 QKD vendors via ETSI GS QKD 014 (IDQ, Toshiba, LuxQuanta, KETS, QTI, Quantum Optics Jena, HEQA, Quintessence Labs, Celare, S-Fifteen Instruments, and ThinkQuantum).

**Satellite QKD Integration** – Developed in collaboration with ESA and Honeywell to merge optical and free-space QKD networks.

**PQC-Based Fallback** – Can be configured to automatically switch to PQC or hybrid key establishment (EvolutionQ's Multimodal Key Establishment) when the QKD key supply is interrupted.

**Adaptive Key Routing & Management** – Dynamically distributes quantum-derived keys based on QKD capacity, demand, and buffer health, ensuring low latency and fault tolerance.

**Visibility & Telemetry** – Full SNMPv3 support, logging, and customizable dashboards for monitoring key usage, generation rates, buffer status, and latency.

**Network Vendor Integration** – Validated with Nokia, Cisco, Juniper, Fortinet, Palo Alto Networks, Ciena, and ADVA — providing quantum-safe keys for OTNSec, MACsec, and IPsec/IKEv2 using ETSI GS QKD 014, Cisco SKIP, and Nokia SNMPv3 interfaces.

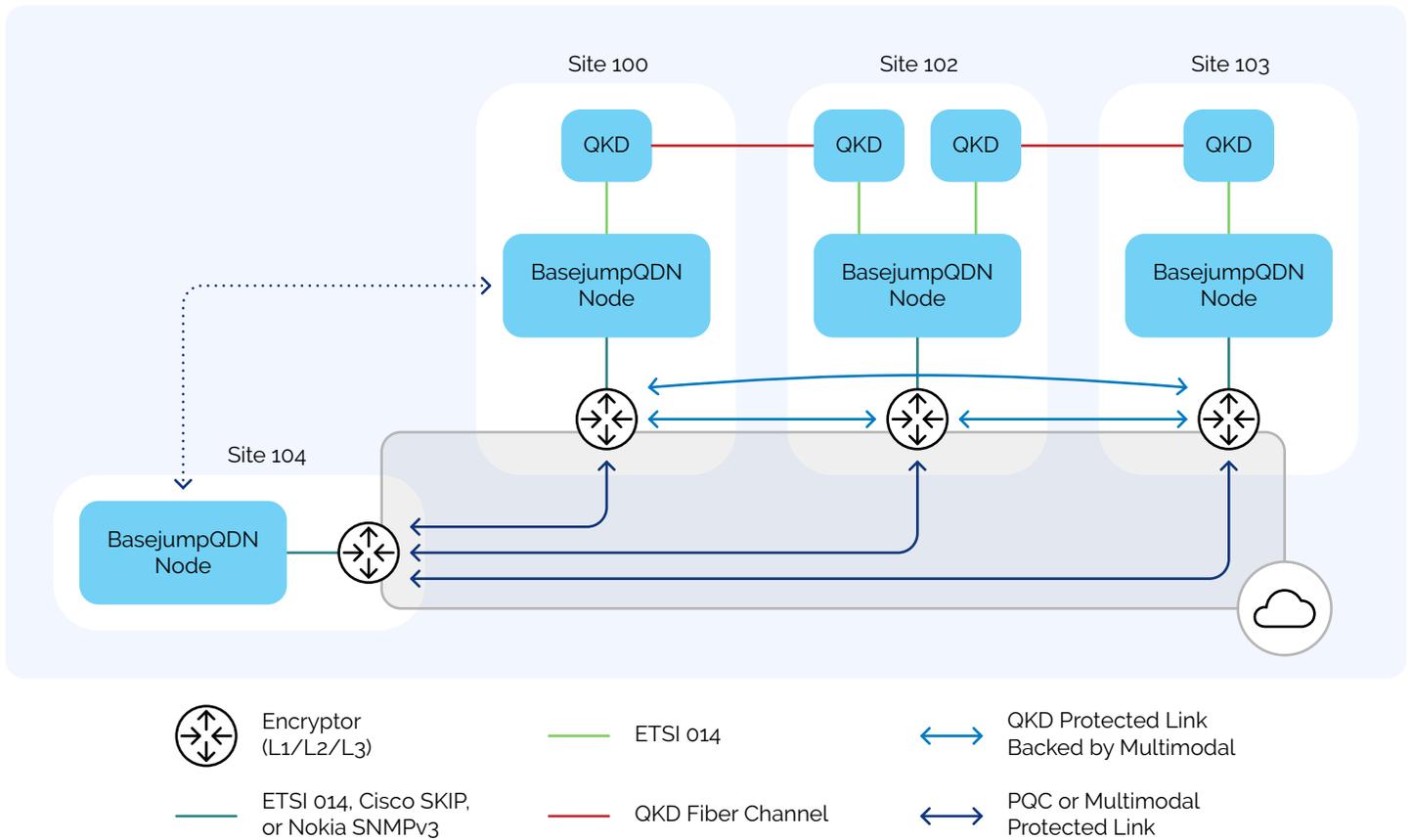
### Key Benefits

**Enable quantum-safe services** – Deliver managed key distribution to enterprise and government customers.

**Deploy QKD, PQC and Hybrid Keys through a single interface** – Developed in collaboration with ESA and Honeywell to merge optical and free-space QKD networks.

**Maintain vendor and cloud neutrality** – Built on open standards to eliminate lock-in.

**Comply with global frameworks** – Aligned with ETSI QKD, ITU-T Y.3800, NIST PQC, and EuroQCI initiatives.capacity, demand, and buffer health, ensuring low latency and fault tolerance.



## Architecture & Deployment Readiness

### Trusted-Network Architecture

BasejumpQDN™ is engineered for environments where reliability, sovereignty, and interoperability are critical. Its modular design supports phased deployments — from metro pilots to nationwide networks following ITU-T Y.3802 architecture principles.

In a multi-vendor QKD network, BasejumpQDN™ nodes maintain Time-to-Live (TTL)-controlled key buffers and proactively relay keys to match real-time demand.

This design ensures Information-Theoretic Security (ITS) and low-latency delivery, even when QKD links experience outages. All links and control messages are authenticated using ML-DSA.

### Optimized Key Routing

A built-in adaptive routing algorithm continually balances QKD capacity against operator-defined key demand to:

- Minimize delivery latency across the network
- Maintain service during hardware downtime (QKD key buffers)
- Optimize bandwidth and key buffer utilization

### Resilient Operation

BasejumpQDN™ supports any desired network topology for maximum availability.

If a QKD device or link fails, the system automatically reroutes keys over alternate QKD path if available.

## QDN Nodes and Key Agents (KAs)

Each BasejumpQDN Node hosts evolutionQ's crypto-agaile key agent. These agents establish and deliver session keys in multiple modes:

- QKD-derived keys
- PQC-derived keys (ML-KEM and ML-DSA)
- Multimodal hybrid keys (PQC, Classical and symmetric key)
- Hybrid QKD + Multimodal keys

Key delivery is supported via the following standard interfaces: ETSI GS QKD 014, Cisco SKIP, and Nokia SNMPv3. BasejumpQDN has been tested with Nokia, Juniper, Cisco, Fortinet and Palo Alto Networks.

BasejumpQDN Deployment Options include:

- Basejump Secure Edge Node 500: A tamper-resistant, hardened Linux platform.
- Customer server or Virtual Machine (VM): Deployable on any cloud or virtualization platform.

## Centralized Management Console

The BasejumpQDN™ Management Console provides a unified dashboard for monitoring and control. Operators can visualize and manage real-time network performance, key health, and QKD operations, including:

- Key usage by external applications
- Keys available to encryptors or services
- QKD key generation rates and buffer levels
- QKD Key Relay throughput and latency
- Link status and network-level visualization



## BasejumpQDN™

The foundation for quantum-safe key delivery across trusted networks.



sales@evolutionq.com  
+1 (647) 499-0747  
www.evolutionq.com