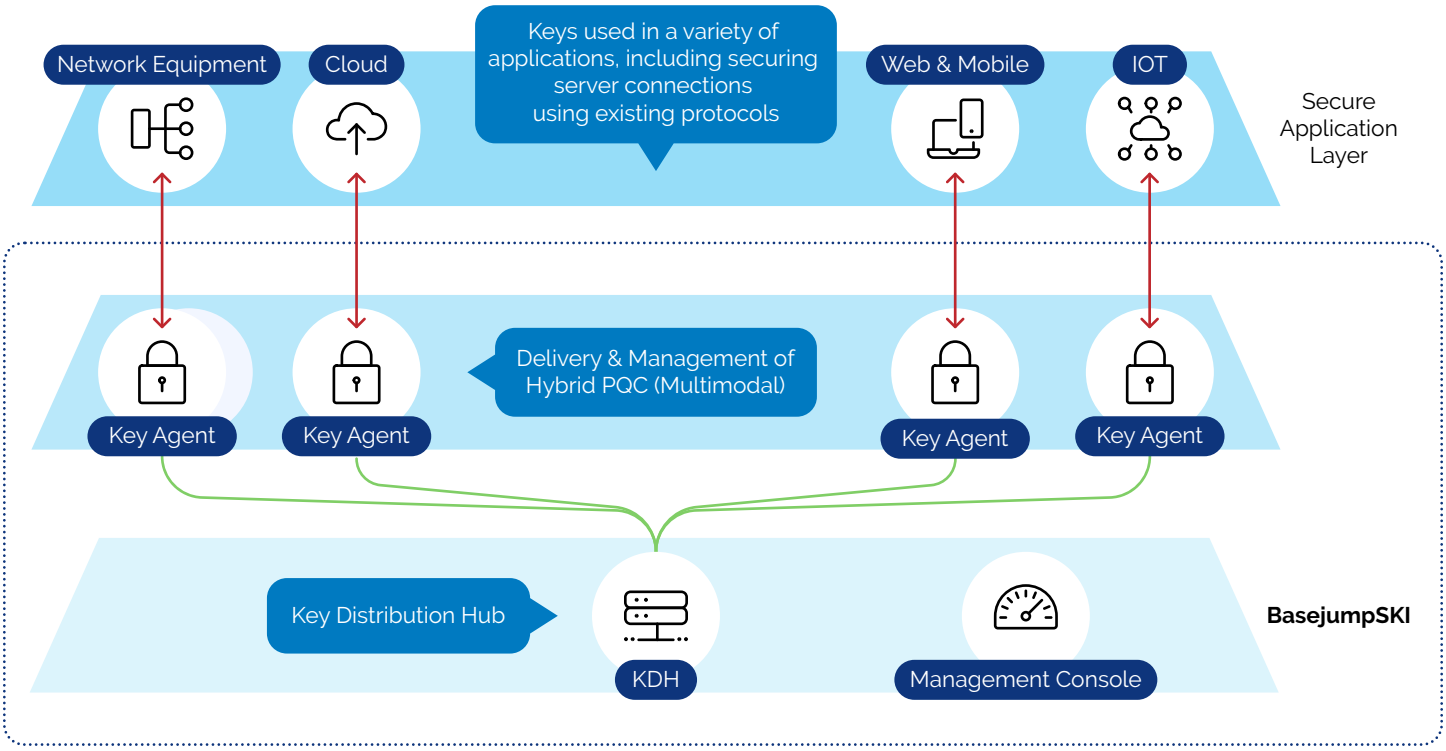
evolution

BasejumpSKI™

Compliant quantum-safe migration that works with your infrastructure

BasejumpSKI upgrades your infrastructure with quantum-safe technologies to protect your data. Compared to single use of post-quantum cryptography, it also combines symmetric keys and other state-of-the-art cryptographic techniques to deliver long-term security and defense-in-depth. BasejumpSKI adds cryptographic agility by seamlessly integrating with existing security protocols (TLS, IPsec, MACsec, OTNSec, etc.) and applications and with your current equipment and processes.



Why act now

- Meets the PQC compliance mandate today for critical infrastructure
- Eliminates the Harvest-Now, Decrypt-Later threat
- Integrates seamlessly into existing infrastructure without requiring costly replacement of network equipment, making it both practical and cost-effective
- Key Agent is available in different for factors including an external hardened secure module, a virtual machine, a docker container for network equipment, an openssl provider and SDK for application integration.
- The KDH can be deployed as a service or local instance backed by a FIPS 140-3 third party HSM

What is BasejumpSKI

BasejumpSKI (Symmetric Key Infrastructure) is built on evolutionQ's Multimodal key establishment protocol. It combines classical cryptography (Elliptic Curve Diffie-Hellman, ECDH) with NIST-approved post-quantum algorithms (ML-KEM), and incorporates a pre-shared key (PSK) to unify the strengths of both asymmetric and symmetric cryptographic methods. The resulting composite key is cryptographically resilient (Long-term Secure, Defence-in-depth and agile). Session keys are distributed using standard, vendor-supported interfaces, ensuring interoperability with existing network equipment and adherence to established cryptographic standards.

Why BasejumpSKI

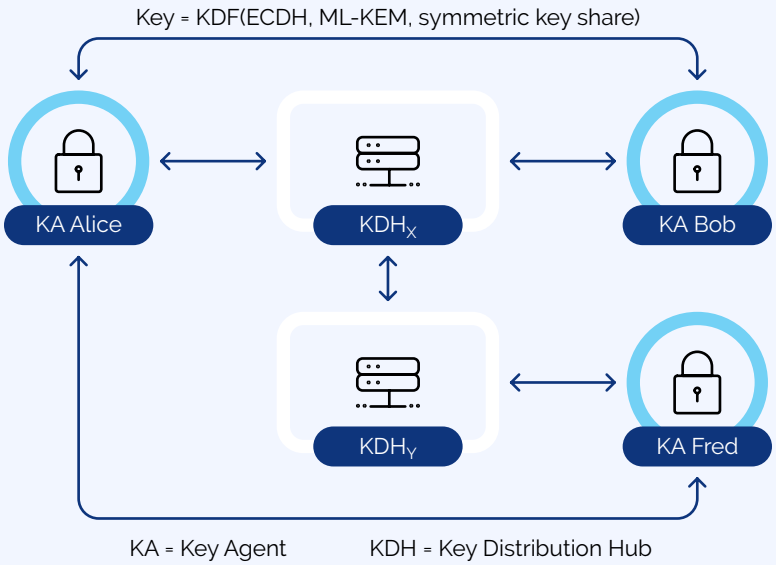
- **No rip-and-replace network equipment:** Use existing protocols (TLS 1.3, IKEv2, MACsec, OTNSec, etc.) and your current vendors (e.g., Nokia, Cisco, Juniper, Fortinet etc).
- **Long-Term Security (LTS):** Final keys depend on well-studied and quantum-resistant symmetric keys.
- **Defense-in-Depth:** Combines multiple cryptographic techniques.
- **Crypto Agility:** The ability to support multiple cryptographic suites.
- **Operational fit:** Deploy on-premise or as a service.
- **Cost-effective & scalable:** Works across data centers, branches, and IoT/OT without forklift upgrades.
- **Infrastructure offline mode:** Can maintain operations if BasejumpSKI's infrastructure (KDH) is unavailable.
- **Random Number Generation compliant with NIST SP 800-90 A/B/C**
- **Upgradeable to support Quantum Networks:** Quantum Key Distribution (QKD).

What's in the system

- Key Distribution Hubs (KDHs) are highly available services responsible for endpoint registration and for delivering one of the multimodal cryptographic key components. A KDH can be deployed either as a cloud service or as a local instance, and may optionally be backed by a third-party Hardware Security Module (HSM) for enhanced key protection.
- **Key Agent (endpoint):** A lightweight software component that runs on servers, appliances, clients, or embedded devices to locally generate end-to-end encryption keys. The Key Agent is available in multiple forms: as an external hardened secure module, a Docker container for network equipment, and as an OpenSSL provider or SDK for seamless application integration.

How BasejumpSKI works (at a glance)

1. **Enroll:** Endpoints register securely with one or more KDHs.
2. **Initiate Key Establishment (Pre-key Data):** When Alice wishes to connect to Bob, she connects to her local KDH to get Pre-key-Data for Bob.
3. **Establish the end-to-end key using the Multimodal key establishment protocol:** Alice and Bob derive the final key in one round trip with a key confirmation.
4. The end-to-end **key is delivered** to the security protocol (i.e. TLS, IKEv2, MACsec, OTNSec) over a standard protocol interface such as ETSI GS QKD014 or Cisco SKIP. Keys can also be delivered through the Key Agent SDK or OpenSSL.



Security properties

- Strong computational security—even if asymmetric keys are later broken.
- Forward Secrecy (FS) and Post-Compromise Security (PCS)
- Ratcheting (symmetric key freshness)
- Secret splitting (infrastructure and endpoints).
- Breaching any number of KDHs does not result in endpoint identity theft.
- Zero trust architecture

Download the whitepaper

evolution

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