Future-Proofing Cybersecurity with Juniper Networks and evolutionQ's MultimodalKES™

INTRODUCTION

Quantum computing is transforming the cybersecurity landscape, posing an unprecedented threat to traditional cryptographic systems. NIST's new post-quantum cryptography (PQC) standards serve as a clear call to action for organizations to begin transitioning their infrastructure. However, even as organizations migrate to PQC, those that rely solely on public key cryptography remain vulnerable to both future computational and quantum-enabled attacks.

To address these vulnerabilities, evolutionQ introduces MultimodalKES, a defense-in-depth approach to key establishment that combines symmetric, classical asymmetric, and post-quantum cryptography to ensure long-term security and resiliency from evolving threats. Through the ETSI GS QKD 014 protocol, Juniper Networks integrates quantum-safe keys from MultimodalKES into its infrastructure platforms, providing enhanced security and future-ready protection for its customers.

THE CHALLENGE

Organizations face two key challenges in preparing for the quantum era:

1. **Limitations of Public Key Cryptography:**
   - Public key cryptography is scalable and offers security properties such as forward secrecy. However, even with PQC, the potential for unforeseen attack methods or evolving quantum capabilities means that relying on a single layer of protection is insufficient for long-term security.
2. **Limitations of Symmetric Key Solutions:**
   - Symmetric key cryptography is quantum-safe and offers long-term security. However, frequently distributing symmetric keys at scale adds operational complexity and potentially, new threat vectors.

THE SOLUTION:

Juniper Networks and MultimodalKES™

The Quantum-safe VPN with Crypto Agility solution delivered by Juniper Networks, evolutionQ, and our ecosystem of partners leverages virtual and/or physical key management entities to secure mobile networks and their end-users. This approach enhances existing Internet Key Exchange (IKE) protocols with an additional secret (key), provided by a quantum-secure key distribution solution, enabling it to provide a new level in crypto agility for VPNs and ease the transition into the post-Quantum era.

Because the physical or virtual key management entities, are separate from the existing network infrastructure, if a key-distribution method becomes vulnerable or outdated by evolving standards or government regulations, key-management entities can be updated via software or swapped out without affecting VPN service availability, while keeping the current level of PKC security. In other words: IPsec with a quantum-secure Airbag.

The solution leverages the ETSI GS QKD 014 protocol, which provides an innovative key management approach, bridging classical and quantum-resistant cryptography. It enables Juniper routers, switches, and firewalls to securely acquire keys from ecosystem partners like evolutionQ's MultimodalKES, ensuring compatibility and enhancing security across network infrastructures.

MultimodalKES combines symmetric, classical asymmetric, and post-quantum cryptography to generate long-term secure, quantum-safe keys. These keys are used to secure data communications through Juniper's IPsec and MACsec integrations, providing end-to-end encryption for both Layer 2 and Layer 3 networks. By leveraging ETSI GS QKD 014, MultimodalKES effortlessly integrates with Juniper Networks RFC8784 enabled infrastructure solutions. The resulting Quantum-safe VPN with Crypto Agility solution provides unmatched operational security.

SUPPORTED JUNIPER NETWORKS PRODUCTS

- Juniper routing, switching, and security platforms that support IPsec and MACsec

SUPPORTED PROTOCOLS

- ETSI GS QKD 014: Used to request external quantum-safe encryption keys for IPsec/IKEv2 (RFC 8784) and MACSec (IEEE 802.1AE)

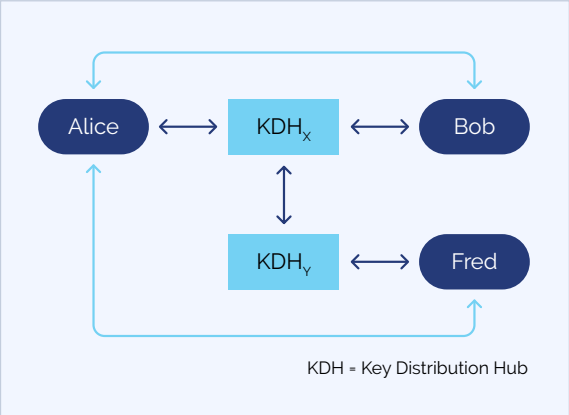
MULTIMODAL CRYPTOGRAPHY

Multimodal cryptography represents an advanced approach to securing communications by intelligently blending multiple cryptographic techniques. This method delivers strong security guarantees, including Long-Term Security (LTS), Forward Secrecy, and Post-Compromise Security (white paper and security proof available at evolutionQ.com).

The architecture centers on Key Distribution Hubs (KDHs), which manage symmetric secrets. Endpoints (such as Alice, Bob, and Fred) leverage classical asymmetric and post-quantum cryptography in conjunction with these symmetric secrets to generate robust end-to-end encryption keys.

The system incorporates cutting-edge cryptographic innovations, including:

- Ratcheting symmetric keys to ensure forward secrecy
- Use of ephemeral asymmetric keys
- Hybrid authenticated key agreement protocols
- Secret-splitting techniques distributed between KDHs and endpoints



This approach creates a flexible, resilient cryptographic infrastructure designed to withstand emerging computational threats.

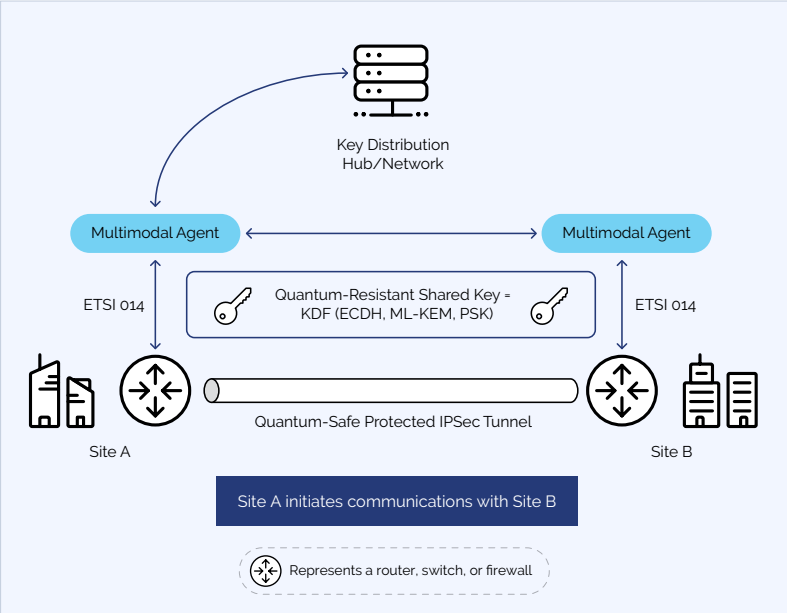
OPERATIONAL SECURITY ADVANTAGES

- **Availability:** Only Initiators interact with the (KDH) and can cache received data. Offline mode ensures service continuity during disruptions.
- **Redundancy:** Endpoints can register with multiple KDHs, enabling flexible configurations and resilience against individual KDH failures.
- **Federation:** Interconnected MultimodalKES networks allow secure, cross-domain key management and interoperability.
- **Scalability:** Designed for linear expansion by adding KDHs to the network.
- **Enrollment:** Supports proxy-based and strong remote onboarding, accommodating diverse organizational requirements with ease.

KEY BENEFITS

Organizations deploying MultimodalKES with Juniper solutions gain:

- **Enhanced Security:** Compliance with NSA's CSFC guidelines and superior resilience to quantum and classical threats.
- **Operational Efficiency:** Streamlined key management reduces administrative overhead.
- **Future-Ready Infrastructure:** A scalable, quantum-resistant architecture designed to adapt as threats evolve.



WHY ACT NOW?

The quantum threat is no longer a distant possibility—it is a pressing reality. NIST's PQC standards emphasize the urgency of transitioning to quantum-safe solutions, as cryptographic migrations are inherently complex and can take a decade or more to fully implement. Meanwhile, organizations remain vulnerable to "Store Now, Decrypt Later" and other attacks.

By leveraging the Juniper-evolutionQ partnership, organizations can proactively secure their data and communications against both current and future threats, avoiding costly vulnerabilities and ensuring long-term resilience.

TAKE THE NEXT STEP

Prepare your organization for the quantum era. Contact evolutionQ to learn how the Juniper-MultimodalKES solution can strengthen your cybersecurity infrastructure.

evolution

www.evolutionq.com
multimodalKES@evolutionQ.com