



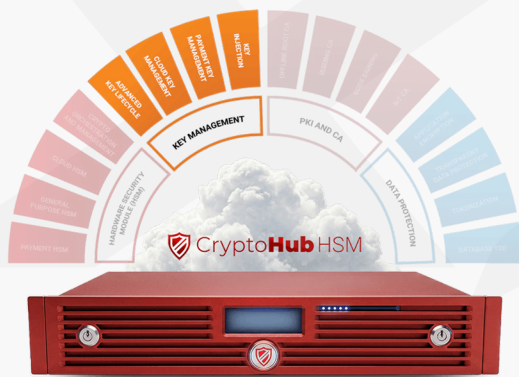
Native Quantum Key Distribution Integration

Eliminating Middleware for Quantum-Safe Key Management

QKD Integration Without Middleware

As organizations adopt Quantum Key Distribution (QKD), a key challenge remains: how to integrate quantum-generated keys into existing applications and infrastructure without adding complexity. Many current approaches rely on external middleware layers to bridge QKD systems and HSM environments. Futurex takes a fundamentally different approach.

CryptoHub natively supports the ETSI GS QKD 014 Key Management Entity (KME) interface, enabling direct integration with QKD infrastructure, without requiring an external key broker or middleware layer.



CryptoHub QKD Capabilities

-  Native ETSI 014 KME interface
-  Direct QKD key ingestion
-  Unified application API
-  HSM-backed key protection
-  Integrated caching and synchronization
-  Hybrid QKD + PQC + classical support

The Legacy Approach

Middleware-based Architecture

- Abstracts QKD protocols via a separate layer
- Translates ETSI 014 interfaces externally
- Brokers key distribution between QKD and apps
- Middleware becomes central integration point

The Futurex Approach

CryptoHub Direct KME Model

- ETSI 014 interface is native - no translation needed
- CryptoHub acts directly as the KME
- Single platform from QKD source to application
- No middleware dependency or third-party broker

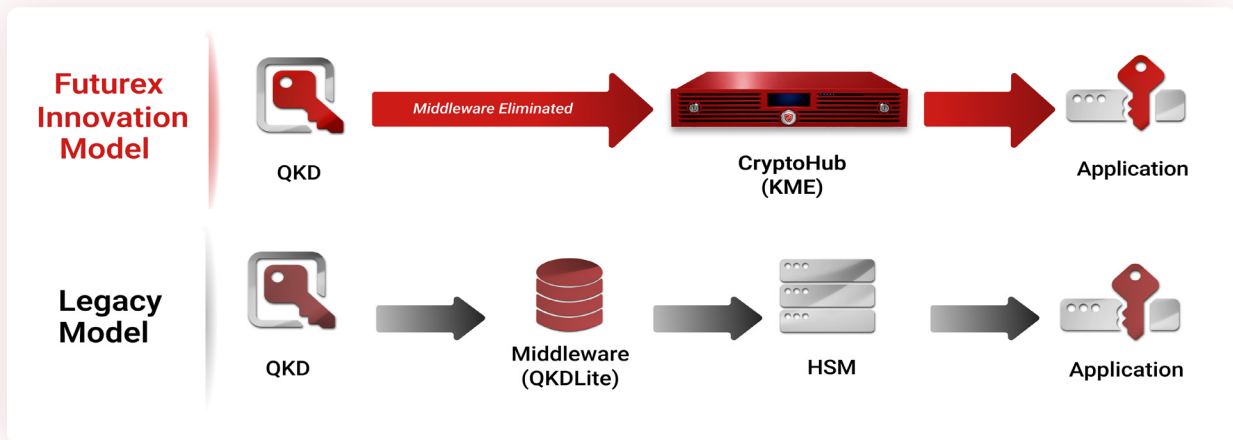
The Compounding Risk and Cost

- Additional infrastructure components to maintain
- Latency and synchronization overhead
- Expanded attack surface across middleware layer
- Dependency on third-party vendor roadmaps

Fewer Components, Lower Risk

- Simplified architecture and faster integration
- Reduced operational complexity and overhead
- Smaller attack surface - HSM-centric security boundary
- Full control under a unified Futurex platform

Architecture Comparison



CryptoHub QKD Benefits

Because CryptoHub provides native ETSI 014 support, it eliminates the need for a separate middleware layer and the complexity that comes with it. Traditional middleware-based approaches rely on a multi-layer architecture where key management, integration services, and orchestration functions are split across multiple components. This increases deployment effort, creates additional points of failure, and requires ongoing maintenance of multiple systems. In contrast, CryptoHub acts directly as the Key Management Entity (KME), creating a simplified, HSM-centric architecture with a unified key lifecycle and a clearly defined security boundary.

With CryptoHub, organizations reduce integration effort, accelerate deployment timelines, and simplify ongoing operations. This approach allows security and infrastructure teams to spend less time integrating and managing components and more time delivering secure services, accelerating adoption while reducing both operational overhead and long-term costs.

QKD Use Cases

Quantum-safe VPN

CryptoHub directly supplies quantum-derived keys to IPsec environments (RFC 8784 PPK).

Financial services / payments

High-value transaction security with centralized, HSM-backed key control.

Data center interconnect

Secure key distribution across high-assurance links between facilities.

Critical infrastructure

Energy, telecom, and government deployments requiring quantum-safe control.

Learn more at www.futurex.com/cryptohub.

About Us

For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents, Futurex delivers unmatched support for its clients' mission-critical data encryption and key management requirements.



864 Old Boerne Road,
Bulverde, Texas 78163

