

FUTUREX

Key Management for Payment and General-Purpose Applications



Why Futurex For Key Management



Futurex is the leading choice for key management solutions, thanks to its cutting-edge unified architecture, industry-leading compliance, and proven reliability across critical sectors. With decades of trusted expertise and a commitment to innovation, including the only HSM supporting PQC that has been PCI HSM validated, Futurex enables seamless interoperability and rapid deployment.

The global network of VirtuCrypt data centers ensures low-latency and flexible access, delivering unmatched expert support and scalable managed services that empower enterprises to protect data with confidence, agility, and complete peace of mind.



What Is Enterprise Key Management



In today's digital economy, data security is only as strong as the cryptographic keys that protect it. Effective key management ensures those keys are securely created, distributed, rotated, and retired, safeguarding payment transactions and enterprise data across every environment.

- **For payments**, strong key management is the backbone of PCI compliance and customer trust, protecting cardholder data at every stage of its lifecycle.
- **For enterprises**, centralized key management systems simplify operations across on-premises, cloud, and hybrid infrastructures.

These solutions deliver high-assurance protection at scale by automating lifecycle tasks, enforcing consistent security policies, and integrating with hardened HSMs.

The stakes are clear: without robust key management, organizations face data breaches, regulatory fines, and loss of customer confidence. With a modern, unified solution, they gain centralized control, seamless automation, and compliant, scalable protection, ensuring sensitive data stays secure while the business moves faster.



UNIVERSAL HSM PLATFORMS



Futurex's HSMs provide a powerful, scalable foundation for enterprise key management. PQC-ready and PCI/FIPS validated, they automate and centralize the key lifecycle with unified policies, auditability, and multitenant control across on-premises, cloud, and hybrid environments.

Designed for performance, crypto-agility, and long-term resilience, they enable organizations to protect and modernize cryptographic operations with efficiency and compliance.

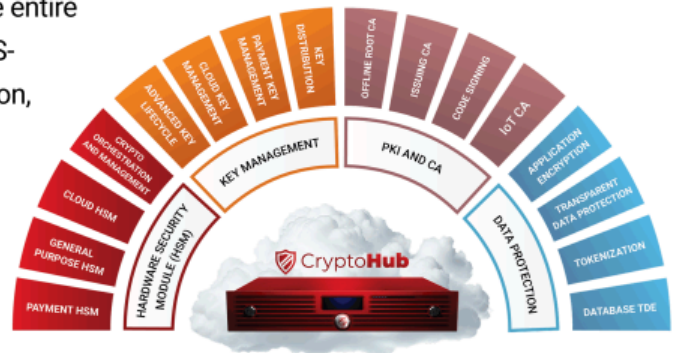
Excrypt HSMs: Payment And General-Purpose

Excrypt HSMs redefine enterprise key management, securing transactions, credentials, and identities with speed and confidence. Built for payment and general-purpose workloads, they eliminate complexity with broad API support and up to 75 fully isolated virtual HSMs per device for true agility and control. Capable of 100,000 transactions per second and post-quantum ready, Excrypt HSMs offer unmatched performance, scalability, and simplicity for automating key management and orchestrating policies across hybrid and cloud environments.

CryptoHub: The Unified Enterprise Security Platform

CryptoHub is the all-in-one security platform that automates the entire key lifecycle with a single, centralized interface. Leveraging FIPS-certified HSMs it supports symmetric and asymmetric encryption, PKI, and BYOK across multi-cloud and physical deployments.

Its intuitive dashboard and advanced automation, including remote key distribution and automated rotation, streamline operations, boost security, and ensure compliance under PCI DSS and EMV standards, eliminating complexity.



VirtuCrypt: The Cloud HSM Platform

VirtuCrypt offers cloud-native, HSM-powered key management with robust multi-cloud integration, supporting major algorithms and protocols. It enables secure remote key loading for distributed environments such as ATMs and POS devices while delivering customizable cryptographic controls, high availability, and disaster recovery that are PCI and FIPS-validated for easy regulatory compliance.



Implementing cloud-based remote key loading through VirtuCrypt has enabled us to radically streamline the deployment and maintenance of our payment devices across a whole range of geographic markets and customer use cases.



— Darren Shaw,
Chief Product Officer,
Miura Systems



Advanced Key Lifecycle Spotlight



Comprehensive, automated platforms focus on managing the entire lifecycle of cryptographic keys to support payments and enterprise environments. Organizations can streamline cryptographic operations, enhance data protection, and efficiently meet evolving regulatory and business requirements.

Core features include:

- **Full lifecycle automation:** Automates key generation, secure distribution, rotation, revocation, and destruction, minimizing manual intervention and reducing the risk of human error or outdated keys
- **Centralized management:** A unified, intuitive interface for managing all encryption keys (symmetric and asymmetric) across on-premises, cloud, and hybrid infrastructures
- **Versatile use cases:** It supports certificate management, PKI creation, digital signature workflows, and secure key management for cloud-based data and applications
- **Granular access controls:** Enforces role-based access controls (RBAC), dual control, and segregation of duties, ensuring only authorized personnel can access or manage keys
- **High availability and disaster recovery:** Up to 99.999% key availability for data recovery and business continuity in case of failures or disasters
- **Interoperability and scalability:** Built on Futurex's standard architectural model, ensuring seamless integration, interoperability, and scalability across diverse systems and platforms
- **Enhanced security:** Utilizes PQC-ready, PCI and FIPS-certified HSMs for secure key generation and storage, protecting sensitive data throughout its lifecycle.



Futurex reduced our crypto infrastructure by over 30% while enabling us to support 90M transactions per day. The transformation has been exceptional.

— Director of
Cryptography,
Leading Payment
Processor

Cloud Key Management Spotlight



Comprehensive, automated platforms focus on managing the entire lifecycle of cryptographic keys to support payments and enterprise environments. Organizations can streamline cryptographic operations, enhance data protection, and meet evolving regulatory and business requirements efficiently.

Core features include:

- **Seamless cloud integration:** Supports AWS, Azure, Google Cloud, and other major providers, facilitating BYOK and EKM strategies for complete key ownership
- **Automated key lifecycle management:** Generates keys locally using HSM entropy, securely pushes them to cloud environments, and manages generation, storage, rotation, and revocation with FIPS-certified HSM protection
- **Centralized management dashboard:** Provides a user-friendly interface with detailed audit trails, robust access controls, and streamlined cryptographic operations
- **Flexible deployment:** Integrates with cloud-native services and third-party tools for scalable key and certificate management across multiple regions and applications
- **Operational resilience:** Supports remote key loading, disaster recovery, and high availability to ensure compliance and business continuity for sensitive cloud workloads.



Payment Key Management Spotlight



Delivering end-to-end security and automation for the entire lifecycle of cryptographic keys used in payment ecosystems to help banks, processors, and payment providers reduce fraud risk, ensure regulatory compliance, and maintain operational resilience throughout the payment ecosystem.

Solutions ensure secure key generation, distribution, injection, rotation, and revocation, all fully compliant with PCI DSS, PCI PIN, and EMV standards, safeguarding sensitive financial data and maintaining transaction integrity.

Core features include:

- **Secure key generation and injection:** Keys are generated and injected using FIPS-certified HSMs, protecting payment terminals, ATMs, and POS devices from tampering and unauthorized access
- **Automated lifecycle management:** Centralized solutions automate key rotation, remote key loading, and revocation, reducing manual effort and operational risk while ensuring uninterrupted payment services
- **Centralized monitoring and audit trails:** All key activities are tracked through a single portal, providing detailed audit logs for compliance and incident response
- **Interoperability and scalability:** Supports symmetric and asymmetric encryption, PKI, and Certificate Authority functions, enabling integration with multi-vendor environments and scaling to large, distributed payment networks.



Our customers trust us to provide rapid, reliable, and secure retail services, and our key injection systems are a crucial component of this.

— Anthony Siracuse,
CEO, Trintas

Key Distribution Spotlight



Delivering secure, automated, and scalable dissemination of cryptographic keys to a wide range of applications and devices, including payment terminals, ATMs, POS systems, IoT devices, and enterprise infrastructure. Organizations can streamline cryptographic operations, enhance security, and maintain compliance across diverse and distributed environments.

Core features include:

- **Automated key distribution:** Keys are securely delivered to remote devices and applications over encrypted networks, eliminating manual handling and reducing the risk of human error or unauthorized access
- **Remote key loading:** This technology enables secure, compliant remote key injection for distributed devices, supports both on-premises and cloud environments, and reduces logistical burdens for global deployments
- **Lifecycle management:** Automates the entire key lifecycle, from generation and distribution to rotation and destruction, minimizing manual intervention and ensuring timely deactivation of unused keys
- **Audit and compliance:** Maintains complete audit trails of key activity, supports regulatory requirements, and provides visibility into key distribution history for compliance and incident response
- **Customizable and scalable:** Solutions are tailored to unique business needs, supporting large-scale deployments and integration with existing enterprise systems.





...we have a segregated cryptographic key architecture. Thanks to VirtuCrypt's solutions, we generate, transport, and use these keys... to offer a comprehensive issuance product with... wallet migration.

– Franco Pinto,
Staff Software Engineer,
The Issuance Team

IoT Key Injection Spotlight



As IoT devices rapidly grow across industries, securing them from manufacture to deployment is essential. Futurex provides a secure, automated, and scalable method to provision cryptographic keys, ensuring strong data protection and device authentication from day one. This allows manufacturers and enterprises to confidently embed encryption keys that prevent unauthorized access and tampering throughout the device lifecycle.

Core features include:

- **Automated mass key injection:** Efficiently provisions large volumes of IoT devices using scalable templates and batch processes, speeding up manufacturing and deployment
- **FIPS-certified security:** Uses tamper-resistant HSMs to generate and protect keys during injection, ensuring compliance and strong security
- **Flexible deployment modes:** Supports on-premises and remote key injection, integrating seamlessly with cloud and hybrid infrastructures for global scale
- **Comprehensive audit and compliance:** Maintains detailed audit trails, supporting standards like PCI PIN v3 and enterprise governance.

Summary



Futurex provides industry-leading, secure, unified, and compliant key management for payments and enterprise data. Its proven reliability, rapid deployment, flexible integration, and expert support empower organizations to confidently protect, scale, and automate key management across any environment.



[FUTUREX.COM](https://futurex.com)

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.

864 Old Boerne Road,
Bulverde, Texas 78163

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

