



Unified Cryptography, Delivered as Cloud Services

VirtuCrypt delivers Futurix cryptography as managed cloud services, including payment HSM, general-purpose HSM, key-management, and CryptoHub Cloud capabilities. Futurix operates the infrastructure while customers retain responsibility for applications, identities, access decisions, key and policy choices, connectivity, routing, and failover design. Now you can expand as operational and regional requirements change.



Choose the Service That Fits Your Workload

CLOUD PAYMENT HSM - Used to support transactions for acquiring, issuing, PIN, EMV, DUKPT, verification values, key translation, and remote key operations through managed payment HSM services.

CLOUD HSM - Use managed HSM capabilities for general-purpose cryptographic workloads that need hardware-backed key protection through configurable encryption, signing, and certificate workflows.

CRYPTOHUB CLOUD - Use a cryptographic management and orchestration platform for HSM clusters, key management, payment RKL, PKI, data protection, monitoring, discovery, and unified governance.

Unified Cryptographic Cloud Capabilities

Mutual TLS Application Identity

Both endpoints authenticate. Client certificates identify calling applications, environments, regions, or roles for policy and audit attribution.

Key Custody and Control

Use KeyLink for controlled payment-key administration. CryptoHub Cloud supports centralized lifecycle policy, BYOK, external-key patterns, and multicloud key governance.

Regional Availability Architecture

Regional HSM resources, load-balanced clusters, health checks, independent network paths, and dual-region patterns support resilient service designs.

CryptoTunnel and Service Isolation

CryptoTunnel validates certificate chains, applies connection restrictions, and routes authenticated requests only to assigned services.

Private Access for Cloud-Native Apps

Connect AWS, Azure, Google Cloud, hybrid, and on-premises workloads through region-aware VAPs and supported private or encrypted paths.

Proven Integrations

Use Excrypt, REST, PKCS #11, Java JCA/JCE, Microsoft CNG, KMIP, and supported application integrations, depending on service.

Phased Cloud Adoption

Move selected workloads based on your application, environment, or recovery requirements. Keep existing infrastructure where needed, adopting VirtuCrypt without replacing your complete cryptographic environment at once. As requirements evolve, expand VirtuCrypt across supported cloud, hybrid, and integrated cloud architectures.



Choose the Deployment Path That Fits Your Environment

VirtuCrypt supports multiple deployment paths. Start with the architecture matching your current applications and operating model.



FULL CLOUD

Deliver selected Futurex cryptographic capabilities through VirtuCrypt managed cloud services.



HYBRID

Combine VirtuCrypt with existing infrastructure for migration, expansion, development, or disaster recovery.

Match Each Workload to the Appropriate Service

WORKLOAD REQUIREMENT	VIRTUCRYPT SERVICE
Transaction acquiring and issuing	Cloud Payment HSM
Payment-key workflows	Cloud Payment HSM or CryptoHub Cloud
Payment-application migration and disaster recovery	Cloud Payment HSM
General-purpose cryptographic workloads	Cloud HSM
Enterprise key management	CryptoHub Cloud
PKI, CA, data protection, policy, and lifecycle management	CryptoHub Cloud

Managed Infrastructure. Defined Customer Control.

Managed service delivery changes who operates the infrastructure. It does not remove architectural responsibility.

- **Applications and identities:** Customers retain responsibility for applications, identities, and access decisions.
- **Keys and policies:** Customers retain responsibility for key and policy choices unless contract terms state otherwise
- **Connectivity and resilience:** Customers retain responsibility for connectivity, routing, resilience, and failover design.

Availability depends on the selected service, redundancy model, connectivity, and application architecture. SLA commitments support the architecture but do not replace resilience planning.

Learn more at www.futurex.com/solutions/cloud-hsm

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 PQC-ready hardware security modules, key management, PKI and CA, data protection, 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

