DATA SHEET

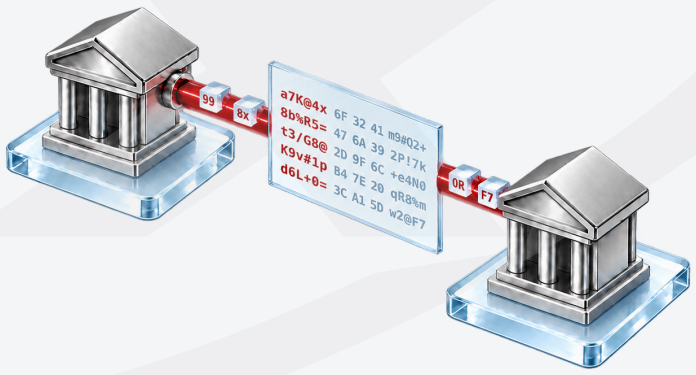


UPI Cryptographic Infrastructure

Capacity and control for always-on payments

Keep cryptography ready for the next peak

Unified Payments Interface (UPI) supports instant account-to-account payments. For PSP banks, remitter and beneficiary banks, and processors, the cryptographic workload depends on their role in the payment path. Futurex combines HSM-backed processing, workload isolation, and centralized management to support growth without losing operational control.



Unified Control for Code Signing Operations

Processing headroom
Excrypt HSMs support up to 100,000 payment operations per second in applicable configurations.

Separate operating domains
Firmware-isolated virtual HSMs separate keys, administrators, and configurations.

One management layer
CryptoHub coordinates policy and key lifecycle workflows across supported services.

Futurex capabilities for UPI environments

Hardware-backed processing
Protect keys and perform the payment and general-purpose cryptographic operations used by your bank-side applications.

Firmware-level isolation
Separate clients, applications, and test environments with up to 75 virtual HSMs per appliance.

Centralized key lifecycle
Coordinate generation, distribution, rotation, recovery, and retirement through CryptoHub policies and workflows.

High availability and recovery
Build clustered HSM services with planned failover and key recovery for your availability objectives.

Application integration
Connect through payment interfaces, PKCS #11, JCA/JCE, and REST APIs as required by the workload.

Operational visibility
Use HubIQ dashboards, notifications, and reporting to monitor supported HSM health and workload activity.

Performance is configuration- and workload-dependent; payment operations per second is not UPI transactions per second. Virtual HSM capacity depends on the selected configuration.

Scale the protected payment path

Futurex brings payment and general-purpose cryptography into one native HSM architecture. Add capacity, isolate a service, or modernize an existing estate while using CryptoHub to coordinate operations across supported environments.

01 Make capacity decisions with evidence

Size and test against your command mix, concurrency, retries, and latency targets, including demand after a node or site loss.

02 Keep client boundaries clear

Assign separate keys and administrative domains as processor portfolios grow, with throughput allocation for supported virtual HSMs.

03 Reduce lifecycle handoffs

Bring key policy, approvals, and lifecycle records into a common operating model so changes are easier to coordinate and review.

04 Prepare for cryptographic change

Evaluate ML-KEM and ML-DSA on supported platforms in an isolated test environment before changing production dependencies.

Choose the deployment that fits your controls



On premises

Excrypt appliances or PCIe deployments for direct custody and local application connectivity.



Managed cloud

VirtuCrypt for approved production, development, recovery, or migration workloads.



Hybrid

Combine local and managed services for staged migration or a defined recovery design.

For India deployments, establish the location of data, keys, logs, backups, administration, and recovery for the proposed service.

Excrypt HSM
Protected Processing

CryptoHub
Management and lifecycle

Hub IQ
Operational visibility

Prove the fit with your UPI workload

Bring your participant role, application interfaces, peak demand, and recovery targets. Work with a Futurex solutions architect to define an evaluation covering command compatibility, P95/P99 latency, surviving capacity, key recovery, and India deployment requirements.

Plan your UPI infrastructure evaluation: www.futurex.com

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.

FUTUREX

864 Old Boerne Road,
Bulverde, Texas 78163