DATA SHEET



RuPay Cryptographic Infrastructure

HSM-backed control for card and PIN operations

Unify the cryptography behind card payments

RuPay is NPCI's domestic card payment network, supporting issuing and acceptance across ATM, POS, and e-commerce channels. Issuers, acquirers, and processors own different card, PIN, and key responsibilities. Futurex brings the cryptographic functions behind those roles into one HSM architecture with centralized lifecycle control.



Control across card and acceptance operations

Card and PIN processing
Excrypt HSMs support PIN translation and verification, CVV generation and validation, and EMV cryptographic functions.

Defined key domains
Use dedicated HSMs or firmware-isolated virtual HSMs to separate issuer, acquirer, and processor environments.

Coordinated key change
CryptoHub applies policy and approval workflows to supported key lifecycle operations.

Futurex capabilities for UPI environments

PIN and card verification
Perform PIN translation and verification, PIN generation, and CVV generation and validation in the HSM.

EMV cryptographic operations
Support EMV validation and key generation or derivation for the card workflows in scope.

Message integrity
Generate and verify message authentication codes for supported payment application interfaces.

Controlled key exchange
Support TR-31/X9.143 key blocks and TR-34 workflows for protected key distribution and exchange.

Terminal key provisioning
Use CryptoHub for workstation injection and supported TMS-connected activation and rekeying across acceptance fleets.

Domain separation
Separate keys, administrators, and configurations with up to 75 firmware-isolated virtual HSMs per appliance.

Functions and performance depend on the model, firmware, and application interface. Confirm scheme interoperability and applicable PCI HSM and FIPS validation scope for the selected configuration.

Coordinate the card and key lifecycle

Futurex connects card processing, terminal key operations, and lifecycle governance across supported environments. Excrypt HSMs perform protected cryptographic operations; CryptoHub coordinates key policy and change; HubIQ adds monitoring and operational reporting.

01 Expand payment capacity

Support growing authorization workloads with up to 100,000 payment operations per second in applicable Excrypt configurations.

02 Simplify acceptance rollout

Coordinate local loading, remote TMS activation, replacement terminals, and fleet rekeying through supported CryptoHub workflows.

03 Maintain control during recovery

Define key custody, approvals, backups, and restore procedures that preserve issuer and acquirer boundaries through maintenance and failover.

04 Make key activity traceable

Document lifecycle events and operator actions for audit review, with terminal identity and provisioning history where terminal workflows are deployed.

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 RuPay applications

Bring your issuing or acquiring role, payment command set, card and terminal key domains, and peak authorization demand. Work with a Futurex solutions architect to test PIN, CVV, and EMV compatibility, key exchange, failure-mode capacity, and the validation scope your deployment requires.

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