DATA SHEET



AePS Cryptographic Infrastructure

Centeral key control for assisted banking

Strengthen the infrastructure behind assisted access

Aadhaar Enabled Payment System (AePS) is a bank-led service for interoperable financial and non-financial transactions through business correspondents and micro-ATMs using Aadhaar authentication. Futurex supports the bank and processor cryptographic layer with hardware-backed key protection, lifecycle control, and separation across participating organizations.



Central control across a distributed channel

Hardware-backed key custody
Excrypt HSMs protect the keys used by supported bank and processor cryptographic services.

Separation between organizations
Firmware-isolated virtual HSMs establish distinct key and administrator domains for supported multi-client environments.

Documented lifecycle activity
CryptoHub coordinates policy, approval workflows, and key lifecycle records.

Futurex capabilities for AePS environments

Protected cryptographic services
Support encryption, message authentication, and signing where these functions belong in your bank or processor path.

Key and certificate management
Use CryptoHub key management and PKI capabilities for the application keys and certificate workflows in scope.

Multi-client isolation
Separate participating organizations with up to 75 firmware-isolated virtual HSMs per appliance in supported configurations.

Controlled administration
Apply role-based permissions and defined approval paths for sensitive key operations and recovery activity.

Recovery workflows
Coordinate key backup, restore, and lifecycle recovery with the bank or processor service recovery plan.

Operational evidence
Use lifecycle audit records and HubIQ monitoring to help teams investigate key events and supported infrastructure activity.

The scope covers supported institutional cryptographic services. Device-level biometric capture and UIDAI authentication controls remain within their respective systems and responsibilities.

Keep key operations accountable as access expands

Distributed assisted banking adds devices, connectivity, and institutional dependencies. Futurex gives banks and processors a common operating model for the keys and cryptographic services they control, while device trust and Aadhaar authentication retain their own owners.

01 **Support additional institutions**
Use isolated HSM environments to add client workloads while keeping keys, administrators, and configuration boundaries defined.

02 **Reduce manual key coordination**
Apply lifecycle policy and approval workflows across supported applications, key services, and certificate environments.

03 **Preserve control during disruption**
Rehearse key recovery and central HSM failover alongside device, network, sponsor, and processor recovery procedures.

04 **Improve incident reconstruction**
Maintain attributable key and administration records alongside application and channel evidence for operational review.

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 across your AePS boundaries

Bring your issuer, acquirer, sponsor, or processor role and the services you operate. Work with a Futurex solutions architect to map key ownership, verify application interfaces, test institution separation and recovery, and document India hosting and administration 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