



WHITEPAPER

Securing the **NPCI** Ecosystem

An executive guide for India's payment, card, ATM, clearing, and Aadhaar-enabled services.



Table of Contents

Executive Summary	3
One Ecosystem Does Not Mean One Architecture	4
1. <i>UPI</i>	5
2. <i>RuPay</i>	6
3. <i>AePS</i>	7
4. <i>BHIM</i>	8
5. <i>BHIM Aadhaar</i>	9
6. <i>IMPS</i>	9
7. <i>NACH</i>	12
8. <i>NFS</i>	13
9. <i>CTS</i>	14
10. <i>NETC/FASTag</i>	15
What Technology Leaders Should Ask Their Teams	17
Conclusion	18
References	19

Executive Summary

India's payments story is often best told through its sheer scale. Unified Payments Interface (UPI) alone processed more than 24.5 billion transactions in August 2026ⁱ, while RuPay, Immediate Payment Service (IMPS), National Financial Switch (NFS), National Automated Clearing House (NACH), National Electronic Toll Collection (NETC/FASTag), Cheque Truncation System (CTS), Aadhaar Enabled Payment System (AePS), Bharat Interface for Money (BHIM), and BHIM Aadhaar support different parts of a payment and clearing ecosystem that reaches almost every segment of India's economy.

For enterprise ITDMs, payments leaders, and cryptography architects, the broader strategic issue is that these programs do not pose a single uniform cryptographic problem. A bank may participate in six or seven National Payments Corporation of India (NPCI) programs simultaneously. Yet, each may involve a different transaction path, participant role, key hierarchy, availability model, recovery requirement, audit boundary, and operating team.

UPI may place intense pressure on both continuous availability and burst capacity. RuPay introduces issuer, acquirer, PIN, and card security considerations, NFS brings ATM switching and terminal key operations into focus, and CTS shifts the discussion toward digital signatures, certificate trust, and cheque image integrity.

This distinction changes the architecture conversation. The useful question is not, *"What hardware security module (HSM) do we need for NPCI?"*; it is, *"For this NPCI program, and for our role within it, what cryptographic architecture gives us the required performance, availability, control, evidence, and operating fit?"*

This whitepaper provides technology leaders with a concise overview of the ten NPCI programs and the architectural issues that warrant attention in each. The deeper implementation questions, including capacity modeling, control boundaries, key lifecycle governance, localization, resilience testing, and evidence requirements, are covered in the companion **'Understanding Cryptographic Architecture Across the NPCI Ecosystem'** whitepaper. Download it [here](#).

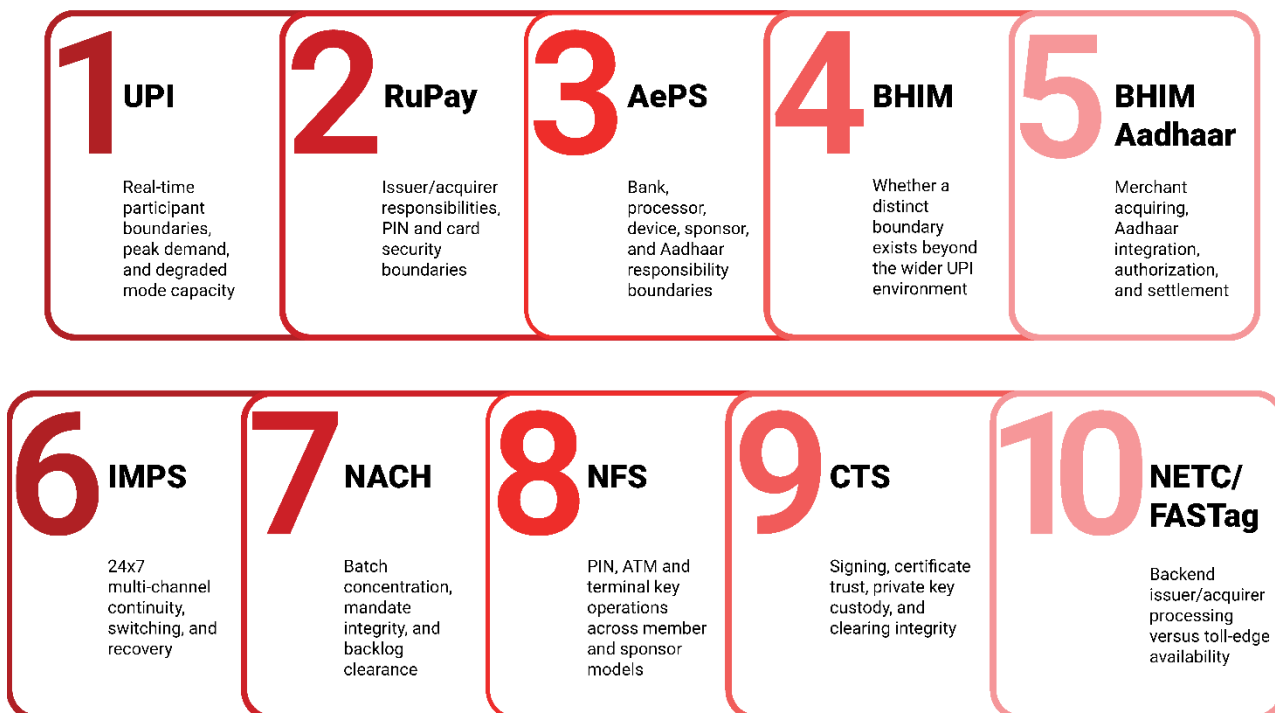
One Ecosystem Does Not Mean One Architecture

NPCI provides the common infrastructure and interoperability behind a broad portfolio of Indian payment and settlement services, yet the shared umbrella does not make the underlying architectures uniform.

Participant responsibilities can shift from one program to another, business volume does not translate directly into HSM operations, and the consequences of a failure can look very different across a real-time payment rail, an ATM network, a batch clearing environment, or a signing-intensive cheque workflow.

This creates a practical governance challenge. The organization may want common standards, consistent key policy, better visibility, and less operational fragmentation, while individual programs may still require separate capacity, failure domains, administrator groups, or audit boundaries. The architectural decision should preserve both objectives: consistency, which improves control, and separation, where the workload or risk model requires it.

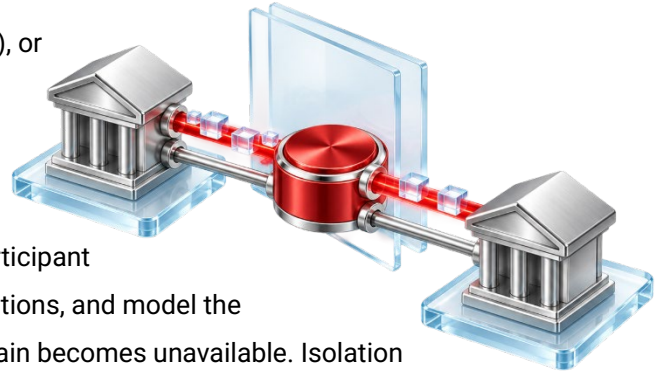
The following ten profiles keep the focus at that decision-making level. Each one explains what changes to make, what leadership teams should pay attention to, and where Futurex can support the resulting architecture.



1. UPI

UPI's scale makes it the most visible of NPCI's workloads, yet ecosystem transaction volume is a poor substitute for an individual organization's cryptographic demand.

A PSP bank, issuer bank, third-party application provider (TPAP), or prepaid payment instrument (PPI) processor can occupy a different position in the transaction path, which changes both the protected functions and the infrastructure owner.



Organizations should ask their teams to establish the exact participant boundary, translate peak transaction demand into secure operations, and model the remaining capacity after a node, link, site, or maintenance domain becomes unavailable. Isolation also deserves explicit attention where separate applications, client environments, or institutional tenants use different keys, administrators, policies, or audit domains.

The critical concern is resilience under real operating conditions. A design that looks comfortable under average load can become constrained during spikes, retries, failover, or maintenance, particularly when the surviving environment must absorb additional demand simultaneously.

WHERE FUTUREX HELPS

Futurex's FIPS 140-3 Level 3-compliant Excrypt HSMs provide a hardware-backed foundation for UPI payment cryptography, with payment and general-purpose cryptography built into a single native HSM architecture.

For qualified high-scale workloads, Excrypt HSM supports up to 100,000 payment operations per second, providing architecture teams with a documented performance ceiling to test against their own command mix, concurrency, latency, and degraded-mode requirements. Where a UPI environment needs stronger workload or administrative separation, firmware-isolated virtual HSMs provide supported cryptographic isolation without requiring every domain to become a separate physical estate.

Futurex's [CryptoHub](#) unifies management, policy, automation, and lifecycle control across supported cryptographic services, while HubIQ provides operational visibility into supported health, capacity, throughput, events, and logs.

VirtuCrypt offers a managed cloud or hybrid model that fits the organization's responsibilities, data location, connectivity, and recovery requirements, giving teams another deployment path without requiring core UPI workloads to move away from on-premises infrastructure.

LEADERSHIP QUESTION: If a node or site fails during peak UPI demand, how much cryptographic processing capacity remains for the protected operations our participant boundaries require?

2. RuPay

RuPay brings a more traditional card-security operating model to the NPCI portfolio. The architecture changes materially depending on whether the organization issues cards, acquires transactions, processes payments, operates ATMs, or supports acceptance infrastructure.^{ii iii}

PIN processing, card verification, terminal and issuer key domains, EMV-related operations, and controlled key exchange can all be relevant. However, the exact mix depends on the participant's role rather than the program name alone.



For technology leaders, the critical issue is governance across card and PIN boundaries. The architecture should make issuer and acquirer responsibilities visible, keep key ceremonies and privileged administration under control, and preserve sufficient capacity and recovery capability during maintenance or failure.

PCI and RBI requirements also need to be mapped to the in-scope entity and activity, rather than treated as a blanket product compliance statement.

WHERE FUTUREX HELPS

Futurex's FIPS 140-3 Level 3-compliant Excrypt HSMs become integral to RuPay environments that require hardware-backed payment cryptography, PIN-related processing, general-purpose cryptography, or controlled workload isolation in supported configurations.

For organizations that must standardize management across card-related cryptographic services, Futurex's CryptoHub provides unified management and orchestration across supported HSM, key management, PKI, and CA, and data protection workflows. HubIQ adds supported operational visibility for capacity, health, events, and reporting.

[VirtuCrypt](#) provides managed cloud payment HSM capabilities in which the chosen regional service, customer responsibility model, connectivity, and payment security scope align with the organization's requirements. This can be useful for selected production, recovery, migration, or testing scenarios rather than as a default replacement pattern.

LEADERSHIP QUESTION: For the RuPay roles we perform, where do our PIN, card, and key-management responsibilities begin and end, and who controls the keys and privileged access?

3. AePS

AePS is a bank-led model that supports Aadhaar-enabled financial and non-financial transactions through business correspondent and micro-ATM environments.^{iv}

Its distributed nature can make the customer journey appear device-centric. At the same time, cryptographic ownership may reside with issuer banks, acquirer banks, sponsor organizations, processors, and other technology providers rather than the business correspondent agent.

Payment teams should insist on a clear boundary map across device, network, processor, bank, NPCI, and Aadhaar authentication domains. That map needs to show who owns participant authentication, authorization, key and certificate operations, recovery, administration, and incident records. It should also avoid unsupported assumptions about biometric cryptography, since those controls need to be traced to current UIDAI material and the organization's actual implementation.

WHERE FUTUREX HELPS

Futurex's [Excrypt HSMs](#) provide hardware-backed payment or general-purpose cryptography for the bank-side or processor-side AePS functions that the organization has confirmed are within its protected boundary. Where a processor supports multiple organizations, firmware-isolated virtual HSMs support approved cryptographic separation between workloads or administrative domains without implying that every function in the AePS transaction path belongs in the same HSM.



CryptoHub unifies management, policy, key lifecycle, PKI and CA, and supports automation across the cryptographic services the bank or processor actually owns. HubIQ adds supported visibility into HSM health, capacity, events, and reporting, which is valuable in a distributed service with sponsor and processor dependencies.

VirtuCrypt supports managed or hybrid deployment patterns in which regional service availability, data and key locations, access, recovery, and customer responsibilities align with the institution's requirements. That gives banks and processors a way to evaluate infrastructure modernization while keeping the Aadhaar and NPCI responsibility boundaries explicit.

LEADERSHIP QUESTION: Who owns authentication, key and certificate operations, and recovery across the bank, processor, device, NPCI, and Aadhaar domains in our AePS transaction path?

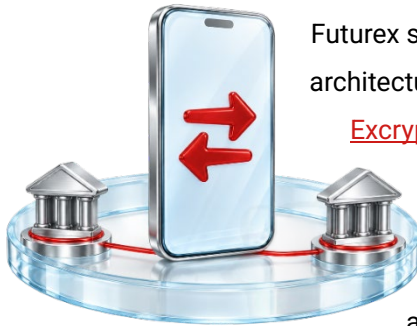
4. BHIM

BHIM is NPCI's UPI-based payment application, which sets it apart from a broad, standalone payment rail. For many banks and supporting platforms, BHIM transactions reuse existing UPI services, keys, connectivity, and recovery processes. The pertinent question is whether BHIM introduces any cryptographic boundary that is genuinely distinct from the organization's wider UPI environment.^v

A separate application identity, certificate boundary, capacity allocation, service provider, release cycle, or audit requirement may justify additional isolation. Where none of those distinctions exist, creating a separate HSM estate simply to mirror the program label can add infrastructure and operational work without changing the underlying risk.

Cryptography teams should ask the UPI owner and security architecture team to document that distinction before approving another platform.

WHERE FUTUREX HELPS



Futurex supports the BHIM-related infrastructure through the same program-specific architecture used for the bank or processor's underlying UPI responsibilities. Futurex's [Excrypt HSMs](#) provide hardware-backed payment and general-purpose cryptography where the protected bank-side or processor-side workload requires it. At the same time, firmware-isolated virtual HSMs support a distinct BHIM administrative or application boundary when such separation is justified and supported.

[CryptoHub](#) centralizes management, policy, automation, and lifecycle control across the supported cryptographic services that BHIM shares with the broader UPI estate, reducing the need to create another management silo. HubIQ adds supported monitoring and operational intelligence across those workloads.

If the organization determines that BHIM does not create a separate cryptographic boundary, the Futurex architecture can remain aligned to the wider UPI environment rather than forcing product duplication. That outcome is consistent with the broader principle of matching infrastructure to the actual control boundary, which can be more valuable than creating another dedicated stack simply because BHIM appears as a separate program in the portfolio.

LEADERSHIP QUESTION: What distinct identity, certificate, capacity, or audit requirement, if any, justifies separating BHIM from our existing UPI cryptographic environment?

5. BHIM Aadhaar

BHIM Aadhaar supports Aadhaar-authenticated merchant payments, which creates a merchant-acquiring context that should remain distinct from BHIM and from the broader AePS model.^{vi}

Acquirer banks, issuer banks, processors, authentication services, merchant-facing technology, and settlement systems can all participate in the flow. At the same time, the merchant and customer remain users rather than direct HSM buyers.

The primary focus must be on ownership across merchant onboarding, application or device trust, Aadhaar authentication integration, transaction authorization, message integrity, settlement, and dispute evidence.

Shared components with AePS can be entirely reasonable, yet the overlap needs to be demonstrated through the actual transaction and control model. A common Aadhaar context does not by itself prove that the same capacity, key, administration, or failure boundary should be used.

WHERE FUTUREX HELPS



Futurex's [Excrypt HSMs](#) support hardware-backed cryptographic processing and key protection for the acquiring, issuing, processor, or authentication-adjacent functions that fall within the organization's confirmed boundary. Firmware-isolated virtual HSMs are helpful when a supported separation between merchant-acquiring, issuer, processor, or other administrative domains is required within an approved deployment.

[CryptoHub](#) provides unified management and orchestration for supported key management, PKI, and CA, as well as policy, automation, and lifecycle workflows that sit behind the merchant payment service. HubIQ provides supported operational intelligence across the relevant Futurex workloads, giving operations teams better visibility into capacity, health, events, and alerts.

[VirtuCrypt](#) supports managed or hybrid patterns where the organization has validated regional availability, data and key location, connectivity, support access, and recovery responsibilities.

LEADERSHIP QUESTION: Where do BHIM Aadhaar's merchant-acquiring, authentication, and settlement responsibilities overlap with AePS, and what evidence justifies shared or separate cryptographic controls?

6. IMPS

IMPS supports 24x7 interbank funds transfer across channels, including mobile, internet, ATM, branch, and other digital interfaces. ^{vii}

That channel diversity can create an operating profile different from UPI's, even when parts of the bank's infrastructure are shared. A technology review should trace the protected transaction path through the participating bank, processor, and interbank switch, identifying which functions genuinely depend on the cryptographic environment and which belong to TLS, application, network, or channel controls.

The business issue is continuity across a broad channel estate. Capacity, key state, administrative controls, logs, reconciliation, and backlog recovery must remain dependable after a switch, node, site, or connectivity failure. This is the point at which "high availability" needs to become a tested operating condition rather than a topology label.



WHERE FUTUREX HELPS

Futurex's [Excrypt HSMs](#) provide hardware-backed payment and general-purpose cryptography for supported IMPS workloads, allowing the organization to size protected processing around the actual secure operation mix rather than the aggregate transaction count. Dedicated capacity or firmware-isolated virtual HSMs can be used where the design calls for a clearer workload, administrative, or failure boundary.

[CryptoHub](#) helps when the organization wants consistent management, policy, lifecycle control, and supported automation across the cryptographic services used by IMPS and adjacent payment environments. HubIQ provides dashboards, alerts, health, throughput, event, and log visibility that gives operations teams a clearer view of the cryptographic layer during demand spikes or service degradation.

[VirtuCrypt](#) supports managed cloud or hybrid deployment patterns for approved production, recovery, development, or migration use cases, in which the organization has defined the region, connectivity, key custody, support, and failover model. That flexibility can be useful when IMPS modernization must progress without forcing every channel or adjacent payment workload into the same deployment decision.

LEADERSHIP QUESTION: After an IMPS switch, node, or connectivity failure, can our cryptographic services sustain the protected workload across affected channels during recovery?

7. NACH

NACH is a useful reminder that real-time transaction processing speeds do not always dominate the requirements of payment cryptography. Recurring and bulk payment flows create concentrated processing windows in which mandate handling, signing or authentication, file and message integrity, retries, reconciliation, and backlog clearance can matter more than continuous retail authorization speed.^{viii}



For technology teams, this changes the conversation around sizing. The relevant question is whether the environment can complete the protected workload inside the required business window, including recovery after disruption. Teams should also make ownership visible across the bank, processor, and corporate boundaries, especially for keys, certificates, recovery artifacts, and evidence.

A system that performs comfortably at average daily volume can still miss the business objective if a failed batch cannot be recovered before the next processing window.

WHERE FUTUREX HELPS

Futurex supports NACH architectures through a combination of hardware-backed cryptography and lifecycle governance. [Excrypt HSMs](#) provide payment and general-purpose cryptographic processing for supported signing, verification, message authentication, encryption, and key protection requirements once the organization has confirmed the exact functions in its implementation.

Futurex's [CryptoHub](#) is particularly useful where NACH workflows create a broader need for enterprise key management, PKI and CA, policy, supported automation, or lifecycle control across signing and certificate-based processes. HubIQ provides operational visibility into supported capacity, health, events, and logs, which become useful when teams need to understand whether a processing window is at risk during recovery.

[VirtuCrypt](#) supports approved managed cloud or hybrid patterns for production, recovery, testing, or migration when the workload, data location, support model, and recovery responsibilities have been

validated. For NACH, the resulting value is operational fit around batch and lifecycle requirements rather than a generic cloud vs. hardware argument.

LEADERSHIP QUESTION: If a NACH batch fails, can our applicable signing, authentication, and key services support recovery and backlog clearance within the required processing window?

8. NFS

NFS connects ATM transactions across member organizations, which puts PIN security, terminal or host keys, switching availability, sponsor relationships, and distributed key operations at the center of the architecture discussion. ^{ix}

The organization operating the customer-facing ATM may not own every protected component in the transaction path, so direct members, sponsor banks, sub-members, processors, ATM controllers, and issuer hosts need to be mapped before an HSM boundary is approved.

The important question is whether the organization can maintain trusted ATM operations amid key rotation, terminal changes, processor disruptions, sponsor dependencies, and central HSM failures. The design must also separate distributed device operations from the central payment HSM workload so that recovery planning covers the full service rather than a single appliance pair.



WHERE FUTUREX HELPS

Futurex's [Excrypt HSMs](#) provide the payment cryptographic foundation for supported PIN, switching, key, and message-related workloads in NFS environments. Where multiple member, application, or administrative domains share infrastructure, firmware-isolated virtual HSMs support cryptographic separation in approved configurations, provided the capacity and failure model have been tested.

[CryptoHub](#) centralizes supported key policy and lifecycle control, while HubIQ provides operational visibility across supported HSM and related workloads.

[VirtuCrypt](#) supports selected managed or hybrid use cases, including recovery or distributed operations, where the architecture and policy permit them. This allows the organization to evaluate ATM and key

distribution modernization as separate decisions instead of assuming that every NFS control must move together.

LEADERSHIP QUESTION: If a central NFS HSM or sponsor connection fails, who restores PIN-processing services, and how are distributed ATM key operations coordinated across responsible parties?

9. CTS

CTS changes the cryptographic conversation because cheque clearing is centered on image integrity, digital signatures, certificate trust, private key custody, and dependable evidence rather than card or PIN processing.^x



Since the presenting bank, clearing layer, and drawee bank can each sit at a different point in that trust chain, architecture teams must establish who signs, who verifies, who owns the relevant certificates and private keys, and how those credentials are recovered or replaced.

For organizations, the business risk is trust in the clearing process itself. A disputed cheque, an expired certificate, a failed signing component, or an unavailable recovery key can affect clearing even when the rest of the payment infrastructure is healthy.

Throughput must be measured around clearing windows, image volumes, verification demand, and backlog recovery rather than borrowed from a real-time payment profile.

WHERE FUTUREX HELPS

Futurex's [Excrypt HSMs](#) provide hardware-backed general-purpose cryptography and secure key protection for applicable CTS signing and verification architectures. The value here is less about processing speeds and more about protecting private keys and trust operations inside a controlled cryptographic boundary.

[CryptoHub](#) brings PKI and CA, enterprise key management, policy, lifecycle control, and supported HSM operations into a unified management and orchestration model, which is relevant where CTS depends on certificate issuance, signing, validation, renewal, or trust store governance. HubIQ adds supported operational visibility for the HSM, PKI, and related services.

[VirtuCrypt](#) provides managed cloud HSM capabilities where the organization's CTS architecture, data location requirements, support model, and recovery design allow a managed deployment.

The final implementation should still be tested against the bank's current CTS rules, certificates, interfaces, and trust model, especially where the organization is changing certificate authorities, signing workflows, or recovery procedures that sit outside the HSM itself.

LEADERSHIP QUESTION: If a CTS signing certificate expires or a signing component fails during clearing, how will we restore trusted signing and verification while preserving the necessary evidence?

10. NETC/FASTag

NETC/FASTag is highly visible at the road toll lane, while the more important cryptographic architecture sits behind that customer experience. Issuer banks, acquirer banks, processors, and program technology teams protect the institutional messaging, keys, settlement processes, and backend services that allow a distributed acceptance environment to work at a national scale.^{xi}

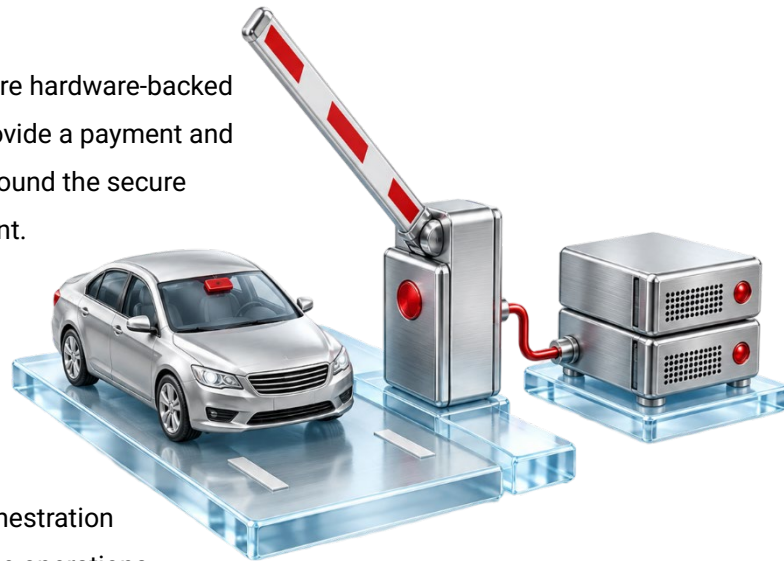
Organizations must separate edge performance from central cryptographic performance. Toll lane response time can be affected by device, network, processor, and application behavior that never reaches the HSM.

The architecture review should identify which backend message authentication, certificate, key management, reconciliation, and settlement functions need protected cryptographic services, who owns the relevant keys, and how the organization handles disruption when edge connectivity and central processing fall out of sync.

WHERE FUTUREX HELPS

For issuer, acquirer, or processor workloads that require hardware-backed cryptographic processing, Futurex's [Excrypt HSMs](#) provide a payment and general-purpose HSM foundation that can be sized around the secure operations actually reaching the protected environment.

Firmware-isolated virtual HSMs help when the organization needs supported separation between workloads, administrative domains, or client environments.



[CryptoHub](#) provides a common management and orchestration layer to standardize NETC-related key policies, lifecycle operations, supported automation, and broader cryptographic governance needs. HubIQ supports operational teams with dashboards, alerts, reporting, and visibility across supported workloads, which is useful when service availability depends on understanding both capacity and infrastructure health.

[VirtuCrypt](#) becomes helpful for approved managed cloud, recovery, development, or hybrid use cases once residency, support access, connectivity, failover, and customer responsibilities have been documented. This gives NETC participants room to modernize specific backend functions while keeping the operating model tied to the responsibility of the issuer, acquirer, or processor.

LEADERSHIP QUESTION: When a NETC/FASTag transaction is delayed or interrupted, can we distinguish toll-lane and network issues from backend cryptographic or settlement dependencies, and identify who is responsible for recovery?

What Technology Leaders Should Ask Their Teams

Before approving an HSM refresh, consolidation, or managed-service deployment, ask your teams three questions across the NPCI programs you support:

1. Where does our responsibility begin and end?

- Can we identify the protected operations, key owners, and trust boundaries for each program?

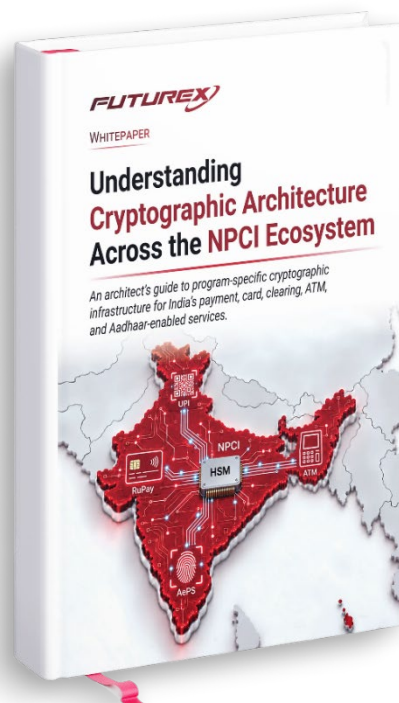
2. Will our architecture hold up when a component fails?

- Have we tested peak workload, reduced capacity, and recovery requirements?

3. Can we defend our design decisions?

- Are our key policies, administrative controls, deployment choices, and supporting evidence aligned with each program's responsibilities?

These answers depend on your architecture and operating model. The companion *technical whitepaper*, ***Understanding Cryptographic Architecture Across the NPCI Ecosystem***, explains how to evaluate control boundaries, capacity, deployment options, key governance, and recovery across all ten programs.



**DOWNLOAD THE
WHITEPAPER**

Download

Conclusion

NPCI is a single ecosystem, not a single cryptographic workload. That distinction is easy to lose when an enterprise looks at the portfolio from a boardroom, budget, or vendor management perspective. Yet, it is central to making the right technology decision. UPI, RuPay, IMPS, NFS, NACH, NETC/FASTag, CTS, AePS, BHIM, and BHIM Aadhaar place different demands on participant roles, key ownership, resilience, auditability, and operations.

The strongest technology approach is to preserve a common governance philosophy while allowing each program to justify the architecture it needs. Some workloads may benefit from dedicated infrastructure; others from firmware-isolated virtual HSMs, managed cloud services, or hybrid patterns; and some may need no material change to HSM at all.

ABOUT FUTUREX

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.

References

- ⁱ NPCI, UPI Product Statistics, reporting period August 2026, <https://www.npci.org.in/product/ecosystem-statistics/upi>
- ⁱⁱ NPCI, RuPay product overview and program resources, <https://www.npci.org.in/what-we-do/rupay/product-overview>
- ⁱⁱⁱ Reserve Bank of India, Master Direction on Digital Payment Security Controls, February 18, 2021, <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0>
- ^{iv} NPCI, Aadhaar Enabled Payment System product overview and participant context, <https://www.npci.org.in/what-we-do/aeps/product-overview>
- ^v NPCI, BHIM product overview, <https://www.npci.org.in/what-we-do/bhim/product-overview>
- ^{vi} NPCI, BHIM Aadhaar product overview, <https://www.npci.org.in/what-we-do/bhim-aadhaar/product-overview>
- ^{vii} NPCI, IMPS product overview and product statistics, <https://www.npci.org.in/what-we-do/imps/product-overview>
- ^{viii} NPCI, NACH product overview and program resources, <https://www.npci.org.in/what-we-do/nach/product-overview>
- ^{ix} NPCI, National Financial Switch product overview and program resources, <https://www.npci.org.in/what-we-do/nfs/product-overview>
- ^x NPCI, Cheque Truncation System product overview and program resources, <https://www.npci.org.in/what-we-do/cts/product-overview>
- ^{xi} NPCI, National Electronic Toll Collection product overview and program resources, <https://www.npci.org.in/what-we-do/netc-fastag/product-overview>