From Cryptographic Modernisation to Cryptographic Trust Infrastructure

Why Post-Quantum Cryptography Alone Is Not Enough

Verify · Protect · Prove

Get in Touch — karthik.iyer@fortytwolabs.com · www.fortytwolabs.com

Every interaction. Every entity.

FORTYTWO LABS · π-CONTROL PLATFORM · 2026

Trust, Enforced.

EXECUTIVE SUMMARY

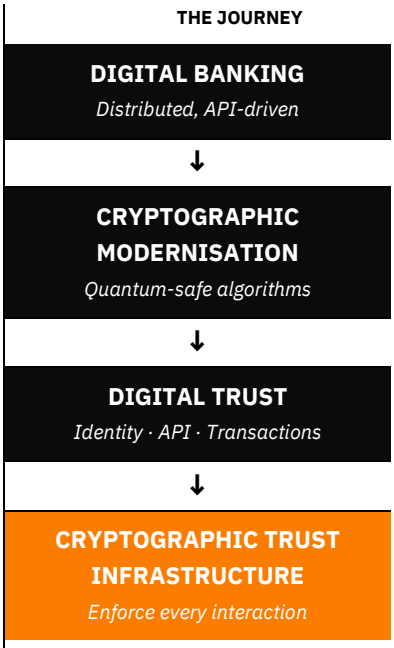
Financial institutions face two related but distinct modernisation imperatives that are easy to conflate and costly to confuse.

The first is cryptographic modernisation: replacing public-key algorithms that quantum computing will eventually compromise. NIST has finalised its initial post-quantum standards, regulatory signals are clear, and the 'harvest now, decrypt later' threat means the exposure window is already open.

The second is less discussed but more consequential in its immediacy. The architecture of financial services has changed fundamentally. Machine identities and AI agents now conduct most digital financial interactions and the trust mechanisms those interactions depend upon were designed for a simpler world.

Passwords, API keys, bearer tokens and certificates have become the transferable mechanisms through which digital systems establish trust. Stronger cryptography protects these mechanisms. It does not eliminate the structural weakness of a trust model in which possession of a credential is treated as proof of identity.

Post-quantum cryptography modernises the mathematics of security. Cryptographic Trust Infrastructure modernises the architecture of trust itself.



DIGITAL TRUST AT AN INFLECTION POINT

The Architecture of Trust Has Not Kept Pace

The Evolution of Security Architecture

Perimeter	Identity	Zero Trust	PQC	Cryptographic Trust Infrastructure
Network boundary	*Credentials & certs*	*Verify explicitly*	*Quantum-safe math*	*Enforce every interaction*

A decade ago, most banking interactions occurred between identifiable parties inside largely controlled environments. The perimeter was real, the participants were known, and trust decisions were made at manageable frequency. The security architectures built for that world were adequate to their context.

The context has changed. Open banking expanded the number of authorised third parties. Real-time payment networks now process hundreds of millions of transactions daily. APIs have become the connective tissue of the financial ecosystem and increasingly, the entities initiating and completing those transactions are not human users. They are software agents, microservices and automated systems operating at machine speed.

Machine identities now outnumber human identities in most large financial institutions. Each presents a credential to gain access - a certificate, a token, an API key. And each of those credentials is, in principle, transferable. Whoever holds the credential can act as the identity.

> **EXECUTIVE INSIGHT**
> *Security architectures have not failed. They have simply outlived the assumptions on which they were designed. As financial interactions become distributed, trust must become continuous. The challenge is no longer improving individual security controls. It is recognising that the architecture of trust itself has changed.*

BORROWED TRUST

Every major breach of the last decade is one story

Every major cybersecurity breach of the last decade has one thing in common: attackers rarely broke cryptography. They borrowed trust.

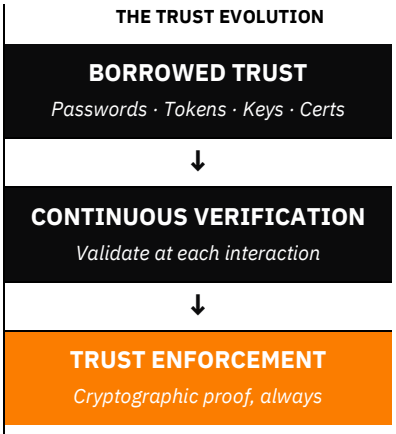
Digital systems do not establish trust directly. They rely on transferable representations of trust - passwords, certificates, API keys, bearer tokens and cryptographic secrets - that allow systems to recognise and authorise one another. These mechanisms remain indispensable, but they were never designed to prove that the entity presenting a credential is the entity to which it was originally issued.

Their limitation is structural rather than technical. A password proves knowledge, not identity. A certificate proves issuance, not legitimacy. A bearer token authorises whoever possesses it by design. The cryptography may be mathematically sound, but possession of a credential has never been equivalent to proof that the presenter is the legitimate identity.

Modern attacks exploit this gap with precision. Adversaries rarely attempt to break encryption. They steal API keys, compromise session tokens and abuse machine identities whose certificates have not expired. In each case, the cryptographic mechanism functioned exactly as designed. The trust relationship had already been broken.

> ***The industry has spent decades strengthening cryptography. The next decade will be about strengthening trust.***

Until possession of a credential is inseparable from proof of the identity it represents, trust remains borrowed and borrowed trust can be stolen.



CRYPTOGRAPHIC TRUST INFRASTRUCTURE

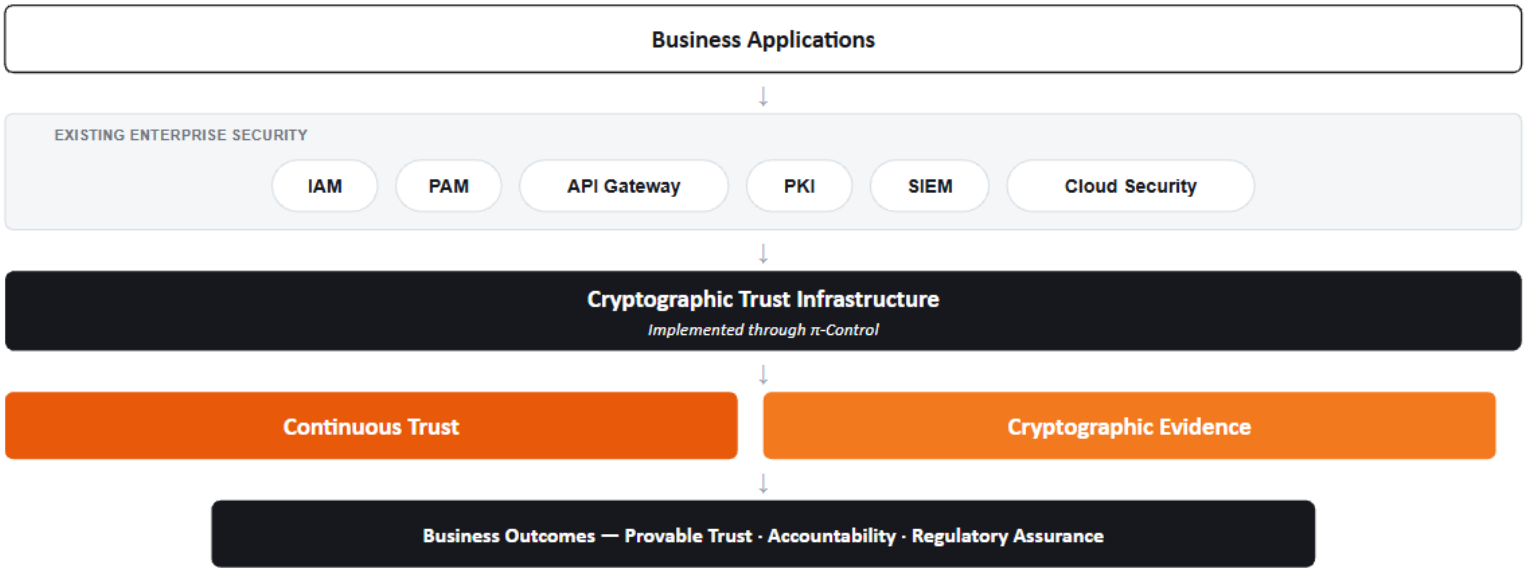
The Architectural Layer That Completes the Picture

Financial institutions are increasingly recognising that trust cannot be managed independently across identities, APIs, applications and transactions. Instead, these interactions require a common enforcement layer that spans the existing security estate.

This emerging architectural layer is not another security product. It is an approach to consistently establishing, protecting and demonstrating trust across every digital interaction.

This layer does not replace IAM platforms, API gateways, PKI or Zero Trust. The gap those technologies share is that none continuously enforces trust at each individual interaction. They control access and manage certificates, but they do not cryptographically bind an identity to this action, on this device, for this transaction, at this instant.

Where Cryptographic Trust Infrastructure Fits



The Three Principles of Continuous Trust Enforcement

Verify	Protect	Prove
· Every identity	· Communications	· Cryptographic evidence
· Every application	· Transactions	· Audit & non-repudiation
· Every API	· Runtime integrity	· Regulatory demonstration
· Every machine agent	· Data in transit & at rest	· Dispute resolution

Verification extends beyond human users to machine identities, software agents and APIs, re-establishing identity dynamically at each interaction, rather than assuming it from a credential issued hours earlier. Protection travels with the transaction, not merely the transport layer. Proof is cryptographic, not merely logged: evidence that cannot be retrospectively altered and can be produced when regulators or auditors require it.

AN EMERGING REGULATORY EXPECTATION

RBI Authentication Directions (2025), DORA, PCI DSS 4.0 and India's DPDP Act all reflect the same regulatory evolution: institutions are expected to demonstrate trust cryptographically not merely assert it through policy. The gap between current capabilities and this expectation is widening.

PRACTICAL ROADMAP

Four Steps Toward Enforced Trust

Most financial institutions already possess many of the technologies required. The opportunity is not to replace them, but to connect them through a common trust architecture.

01 PROTECT	02 MODERNISE	03 ENFORCE	04 PROVE
Protect critical identities, APIs, applications and transactions using quantum-safe cryptography while reducing immediate cryptographic risk.	Introduce crypto agility and migrate to quantum-resistant algorithms without disrupting existing applications or business services.	Continuously verify identities, applications, machine agents and APIs so trust is established at every interaction, not assumed from credential possession.	Generate cryptographic evidence that supports audit, regulatory compliance, accountability and non-repudiation.

> *Post-quantum cryptography modernises the mathematics of security. Cryptographic Trust Infrastructure modernises the architecture of trust itself. Together, they represent the next evolution of trust in digital financial services.*

About Fortytwo Labs

Fortytwo Labs is a deep-tech cybersecurity company building **π-Control**, a Cryptographic Trust Infrastructure platform for enterprises where digital trust is business critical. Built on patented cryptographic protocols, π-Control enables organisations to continuously verify identities, protect digital interactions and generate cryptographic evidence across identities, applications, APIs, communications, transactions and data. Rather than replacing existing security investments, it acts as an enforcement layer that strengthens trust while supporting crypto agility and post-quantum readiness.

Trust, Enforced. Verify. Protect. Prove. Every interaction. Every entity.

π-Control Platform · www.fortytwolabs.com

GET IN TOUCH

Ready to enforce trust across every digital interaction?

Let's start the conversation.

Karthik Iyer
SVP Revenue & Growth
karthik.iyer@fortytwolabs.com