Is Post-Quantum Cryptography the Next Y2K Moment for Global Digital Infrastructure?

Are enterprises ready for a Y2K-scale disruption as post-quantum cryptography reshapes digital security?

BENGALURU, KARNATAKA, INDIA, March 18, 2026 /EINPresswire.com/ -- eMudhra today raised a critical question for global enterprises, governments, and infrastructure operators: could the transition to post-quantum cryptography (PQC) represent a “Y2K moment” for digital security?

As advances in quantum computing threaten to break widely used encryption standards, organizations worldwide face the challenge of replacing cryptographic systems that underpin financial transactions, identity systems, digital signatures, and secure communications.

Governments and regulators in the United States and Europe have already begun pushing organizations toward quantum-resistant cryptography to protect long-term data and critical infrastructure. Security experts warn that sensitive information encrypted today could be harvested and decrypted in the future once quantum capabilities mature.

eMudhra said the transition to post-quantum security could require large-scale changes across enterprise infrastructure, identity systems, and digital public infrastructure (DPI), comparable in complexity to the global technology remediation efforts seen during the Y2K transition.

“The world’s digital infrastructure is built on cryptography. If existing encryption becomes vulnerable, the impact could be systemic,” said Biju Varghese, EVP, eMudhra. “Organizations must begin preparing now for post-quantum security transitions to maintain trust in digital systems.”

The company said the shift may affect certificate lifecycles, authentication systems, secure communications, and long-term data protection strategies.

Enterprises must evaluate cryptographic inventories, update trust architectures, and implement migration strategies to ensure operational continuity.

eMudhra noted that post-quantum readiness is becoming a strategic priority for boards and security leaders as organizations expand cloud adoption, digital services, and autonomous systems. The transition also has implications for digital identity, financial systems, and global trust infrastructure.

As quantum research accelerates, eMudhra said proactive planning and trust infrastructure modernization will be essential to ensure resilience and confidence in the digital economy.

About eMudhra

eMudhra is a global provider of digital identity, authentication, and trust services, enabling secure digital transformation for enterprises and governments. With a strong foundation in PKI, digital signatures, certificate lifecycle management, and identity and access management (IAM), eMudhra powers secure transactions and digital public infrastructure at population scale.

Serving customers across more than 35+ countries, eMudhra partners with leading technology providers and governments worldwide to deliver compliant, scalable, and high-assurance digital trust solutions.

As global cyber threats continue to evolve, eMudhra said establishing verifiable trust across users, devices, and digital services will be essential to protecting digital economies and public infrastructure.

Sudesh Kumar
eMudhra Limited
email us here
Visit us on social media:
LinkedIn