PCI Security Standards Council®

SISA

Navigating the Quantum Shift

A Framework for Transitioning to Post-Quantum Cryptography

State of Digital Payments, Today

Growth

US$ 24.31 trn

Projected market for global digital payments by 2030.

Encryption, tokenization & cryptograms protect data security, confidentiality, authenticity, and integrity

YET BREACHES CONTINUE!

vs.

Escalating Threats

US$ 3.5 trn

Cost of a potential cyberattack to the global economy.

US$ 12 Billion

Losses in the financial sector over the past 20 years

Now, imagine the scale of threats when **Quantum Computing** enters the equation, making current encryption obsolete!

The Countdown to Quantum Supremacy

01

2025

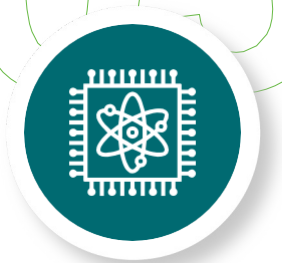
The United Nations has proclaimed 2025 the International Year of Quantum Science and Technology

02

$50 billion

Projected size of the global quantum computing market by the end of this decade.

03



9-10 years

Quantum supremacy will render RSA, DSA, and ECDSA algorithms obsolete, allowing quantum computers to break these defenses.

We are on the brink of a very near, very real Quantum future!

The Compliance Challenge in the Quantum Age

Traditional Encryption

Modern computers would take 300 trillion years to crack an RSA 2048-bit key.

Card payment systems use symmetric & asymmetric cryptographic mechanisms Per EMV® specs, with TDES for online & RSA for offline protocols

Current encryption techniques, such as Rivest–Shamir– Adleman (RSA) and Elliptic Curve Cryptography (ECC) are used in EMV® card payment systems.

VS.

300 Tr. Years vs. 10 Seconds

Compliance at Risk

Shor's Algorithm Threat

Quantum Threats

A quantum computer could do it in 10 seconds.

Algorithms like TDES and AES are not directly threatened by quantum computing but would require longer keys due to quantum speedups like Grover's algorithm.

Shor's algorithm will enable quantum computers to break these cryptographic methods in minutes, putting key exchanges, digital signatures, and compliance at risk..

As the **quantum era** approaches, current cryptographic defenses will fail!

Why Worry Now? It's Some Time Away… Or Is It?

The Quantum Threat is Closer Than You Think

Quantum Computing on the Horizon

- A fully error-corrected quantum computers will emerge by 2029
- By 2033, 25% of experts believe there's a 50% chance that quantum computing will compromise cybersecurity.

Data is Already at Risk

- The "harvest now, decrypt later" strategy puts today's data at risk for tomorrow's quantum breakthroughs.
- Sensitive information that needs to remain secure for decades is already exposed to long-term vulnerability!.

Time is Running Out for Critical Industries

- Sectors such as financial services, automotive and government systems, face heightened quantum risks.
- Critical infrastructure with long lifespans is already falling behind in terms of quantum readiness.

The Challenge of Cryptographic Migration

- Previous cryptographic migrations took 20 years.
- 62% of companies lack visibility into their keys and certificates, making quantum risk management even more challenging.

Quantum threat is not a distant future — it's only a decade away from exposing widespread cryptographic vulnerabilities!

New Algorithms for a New Era

Building Resilience Against Quantum Threats

01

Post-Quantum Cryptography (PQC) are cryptographic systems that can withstand quantum attacks and designed to **future-proof** data security.

02

The **National Institute of Standards and Technology (NIST)** has led the global push to standardize PQC algorithms, publishing its first set of post-quantum cryptography standards.

The NIST competition is selecting quantum-resistant algorithms like Kyber (key encapsulation) and Crystals-Dilithium, Falcon, and Sphincs+ (digital signatures).

03

Global Push Towards Quantum-Resilient Cybersecurity

Global initiatives are driving a global shift as nations assess the risks and requirements for secure quantum technologies.

.

A Signal for Action: Post-Quantum Cryptography (PQC) standards are here, marking the beginning of a new era in data security!

Post-Quantum Impact on Payment Security: Key Scenarios

The implications of post-quantum cryptography must be examined across various payment scenarios and their lifecycle.

The following scenarios cover card usage in ATMs, PoS transactions, card manufacturing, and web transactions via payment gateways like VISA and MasterCard.

- Chip card authentication
- Chip card data encryption
- PIN translation
- VPN / MPLS – TLS encryption
- PIN/Password validation
- RFID reading
- HTTPS/ TLS
- CVV2 validation
- RSA file encryption
- SFTP encryption
- Digital Signatures

Quantum-Driven Change: The Next Chapter in Payment Evolution

03

Future Resilience

The development of crypto-agile payment systems will be crucial for long-term resilience. These systems would allow the payment industry to rapidly switch to quantum-resistant algorithms when needed, minimizing disruption.

02

Long-term Impact

- As quantum computing advances, a complete overhaul of cryptographic systems will be needed.
- Adopting PQC algorithms will reshape payment card designs, terminals, and communication protocols, with implementation challenges requiring new chip designs and extensive industry collaboration.

01

Near-term Impact

A gradual migration from RSA to ECC for card authentication and from TDES to AES for transaction security is expected. The industry will focus on strengthening existing cryptographic systems against advanced classical attacks.

Ensuring Compliance in the Post Quantum Era

01

Develop a Quantum-Safe Compliance Strategy

- Start today by adopting a crypto-agile strategy.
- Evaluate how transitioning to PQC affects performance and regulatory requirements.
- Develop a compliance-driven timeline and communicate it to your customers and suppliers.

02

Build Strategic Relationships

- Building strong relationships with regulators, suppliers, and industry peers will ensure your organization stays compliant with evolving post-quantum standards.

03

Prepare Your Infrastructure

- Design your hardware and software to be retrofit-ready for cryptography updates. Having modular architectures will allow for easy adaptation to regulatory changes as post-quantum standards evolve.

04

Migration Recommendations for Digital Payments

- The payment industry is advised to migrate from RSA to ECC to counter current threats posed by classical cryptanalysis.
- Hybrid cryptography, combining pre-quantum (RSA or ECC) & post-quantum algorithms, could be an interim solution.

Develop Cryptographic Agility

01

Assessing your cryptographic inventory, identify compliance risks, and start the migration to Quantum-Safe Cryptography.

02

Assessing cryptographic health and identifying compliance gaps for quantum preparedness.

03

Where vulnerable cryptography like RSA or ECC is deployed in your products and business processes.

04

Developing guidelines to ensure compliance with data protection regulations during and after the transition.

05

Map out where your long-life sensitive data (e.g., data that must remain secure for 10+ years) resides and its flow across the organization.

PCI Security Standards Council®

THANK YOU!