Post-Quantum

Cryptography Conference

Crypto-Agile PKI: A Strategic Blueprint for Post-Quantum Trust

Ganesh Mallaya
Distinguished Architect at AppViewX Inc

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

appviewx

Crypto-Agile PKI: Strategic Blueprint for Post-Quantum Trust

Navigating the quantum cryptography transition with strategic foresight and hybrid innovation

Ganesh Mallaya

Speaker Introduction

Ganesh Mallaya

- **Distinguished Architect & Technical Evangelist, AppViewX**
- Leading global initiatives in Crypto-Agile PKI, Post-Quantum Cryptography (PQC) readiness, and automated certificate lifecycle management
- Contributor and industry participant in CA/B Forum policy discussions and IETF’s ACME Device Attestation draft, advancing secure, hardware-bound certificate automation for IoT and enterprise ecosystems

LinkedIn

ganeshmallaya

Your Journey Through the Quantum Shift

We'll cover the critical elements of transitioning your PKI infrastructure to a post-quantum world—from understanding the threat landscape to implementing automated, crypto-agile solutions.

The Quantum Threat

Real, near, and strategic

Multi-Year Transition

From discovery to deployment

Hybrid PKI

Bridging classical and quantum worlds

Automation & Crypto-Agility

Scaling with ACME

Strategic Blueprint

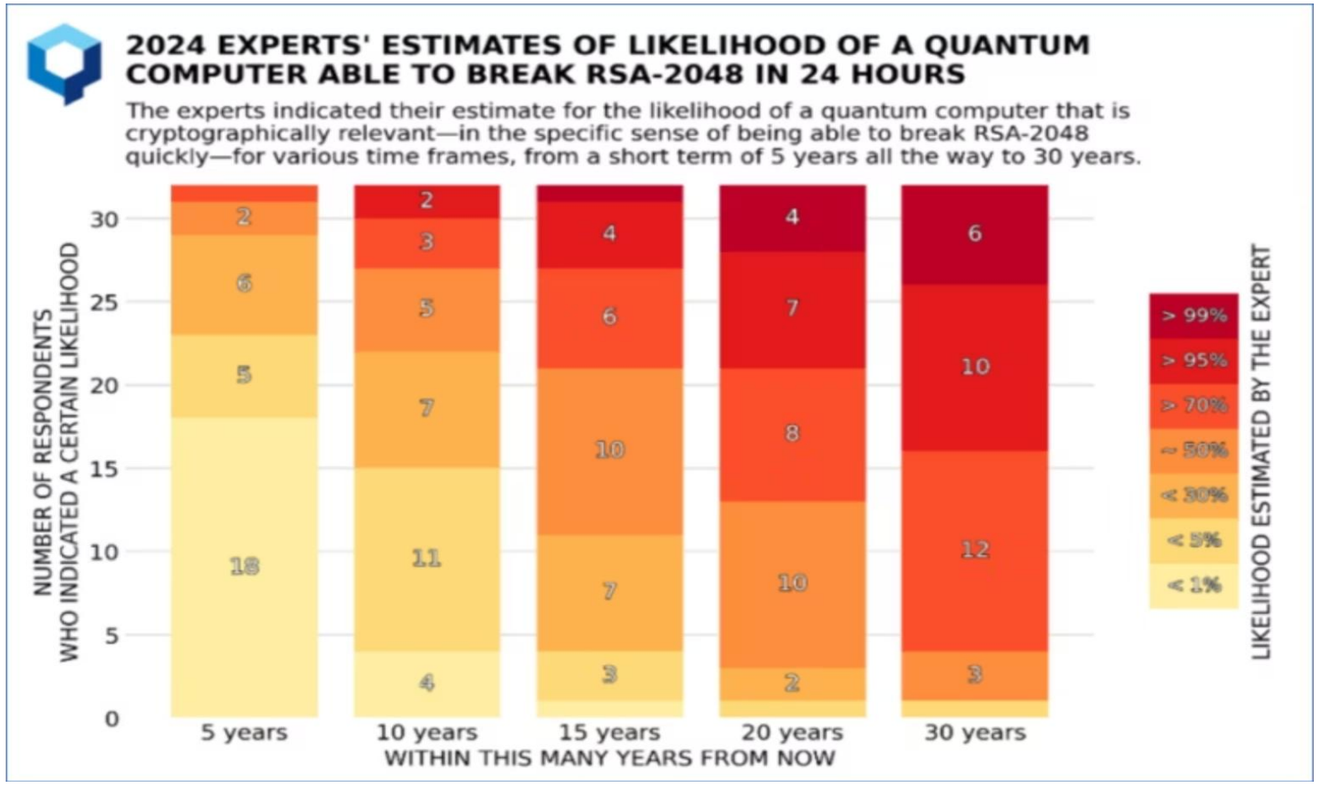
Governance, triggers, and readiness

Spoiler alert: The quantum apocalypse won't happen overnight, but "harvest now, decrypt later" attacks are already in progress.

The Quantum Threat: Real, Near, and Strategic

The danger of quantum computers isn't what they can do today—it's what they'll be capable of tomorrow, with data collected today. Adversaries are already hoarding sensitive, long-life data: medical records, legal documents, military communications, and intellectual property.

Harvest Now, Decrypt Later: Encrypted data intercepted today will be vulnerable once cryptographically relevant quantum computers (CRQCs) emerge. Waiting until quantum computers are fully implemented is not a solution—it's a strategic failure.



Healthcare Data

Patient records with decades-long sensitivity

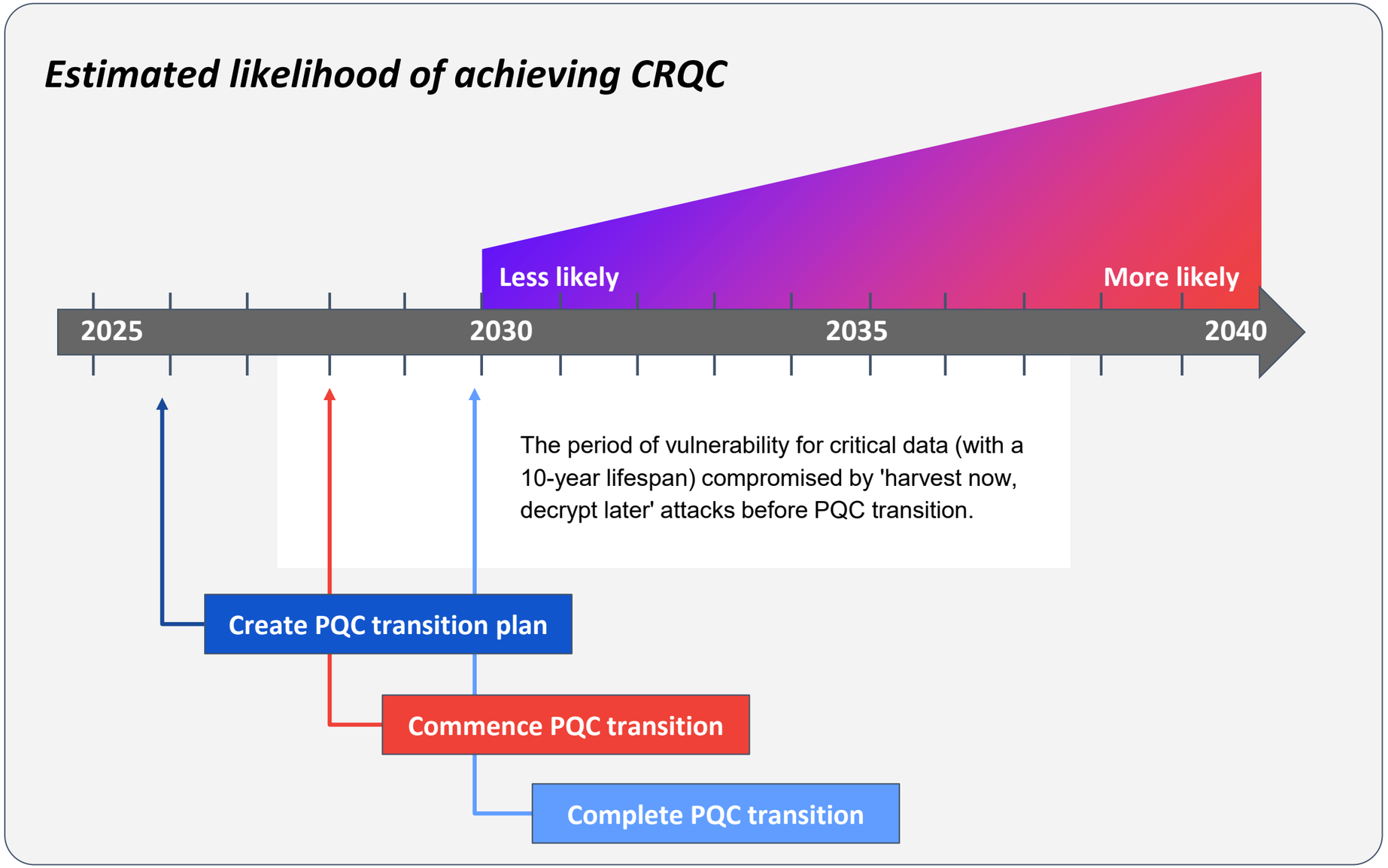
Government Intel

Classified communications and strategic plans

Financial Systems

Transaction histories and proprietary algorithms

Harvest Now, Decrypt Later: The Multi-Year Migration Reality



The Multi-Layer Cryptography Problem

Why There's No "One-Click" Fix

Every asset, system, and application contains multiple layers of cryptography. In a single 5G call, hundreds of cryptographic mechanisms activate from device authentication through network connection, call setup, roaming interfaces, and backend billing systems.

RSA and ECC, the encryption standards of the 20th century, are aging rapidly. While post-quantum cryptography offers solutions, the transition demands massive infrastructure overhauls, updated standards, and global compliance alignment.

No Drop-In Replacements

PQC algorithms like CRYSTALS-Kyber and Dilithium require changes to data structures, message sizes, and performance characteristics

Hardware Dependencies

Many systems need software modifications or complete hardware upgrades to support quantum-resistant algorithms

Piece-by-Piece Migration

Organizations must systematically identify and address every instance of RSA, ECC, and DSA across their infrastructure

Strategic Blueprint: The Four-Phase Transition

Asset & Cryptographic Inventory: Map all cryptographic implementations and assess data confidentiality lifetimes—PII, contracts, source code, SSL certificates, telemetry data, and long-lived secrets

Define PKI Strategy: PKI serves as the trust hub where quantum-safety becomes visible to customers and auditors. Let PKI strategy lead the cryptographic transition with clear governance and risk-based prioritization

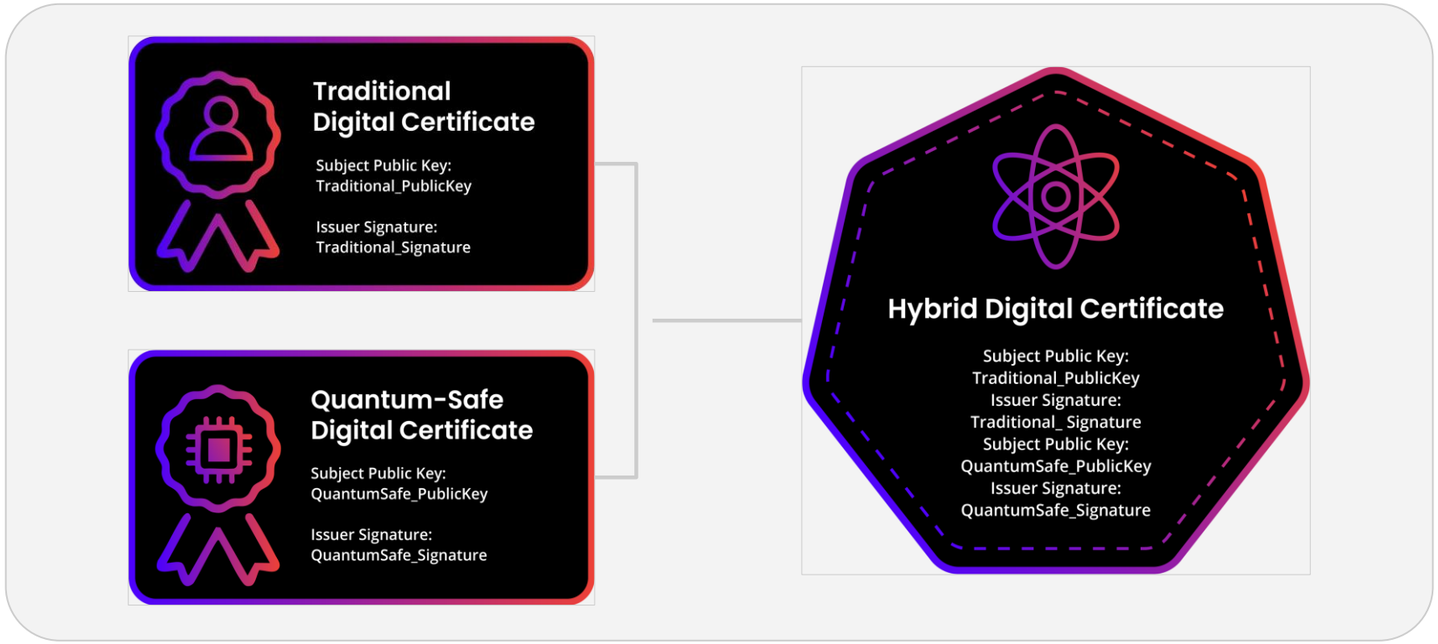
Risk-Based Prioritization: Focus on high-value, long-life data and systems with limited crypto-agility. Address harvest-now-decrypt-later vulnerabilities in critical infrastructure first

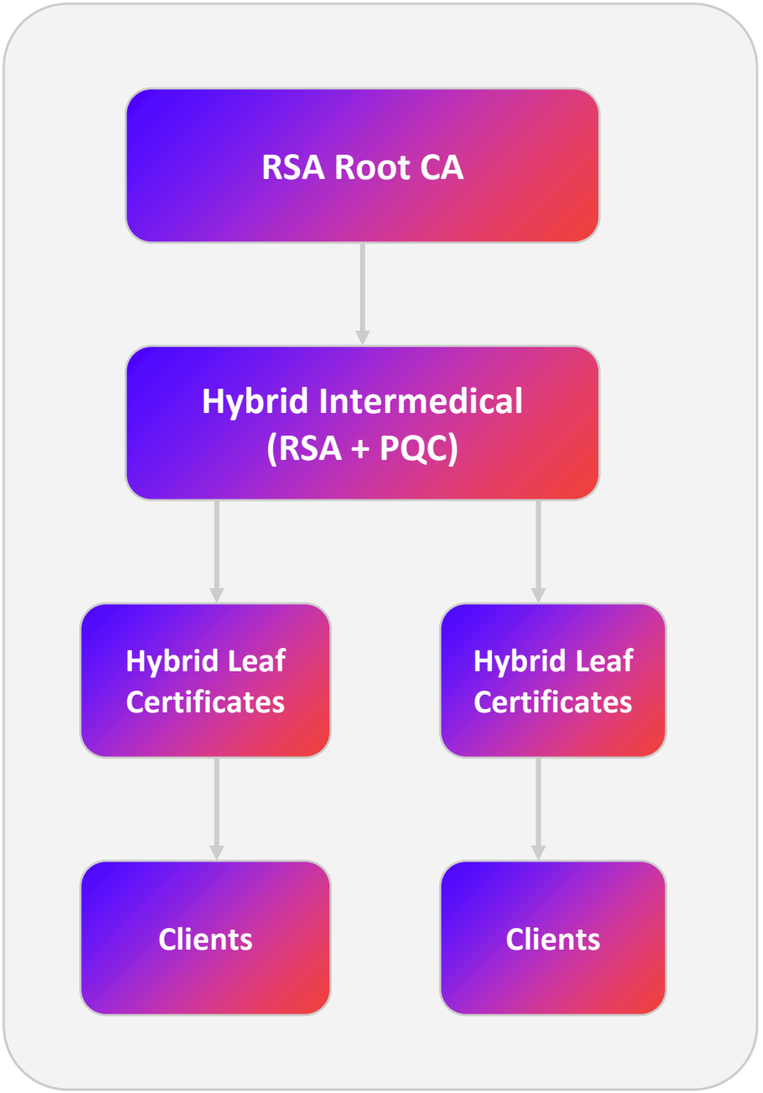
Phased Deployment: Execute hybrid cryptography rollout with automated certificate management, continuous monitoring, and trigger-based transitions to full PQC as standards finalize

Hybrid PKI in Action - The Pragmatic Migration Path

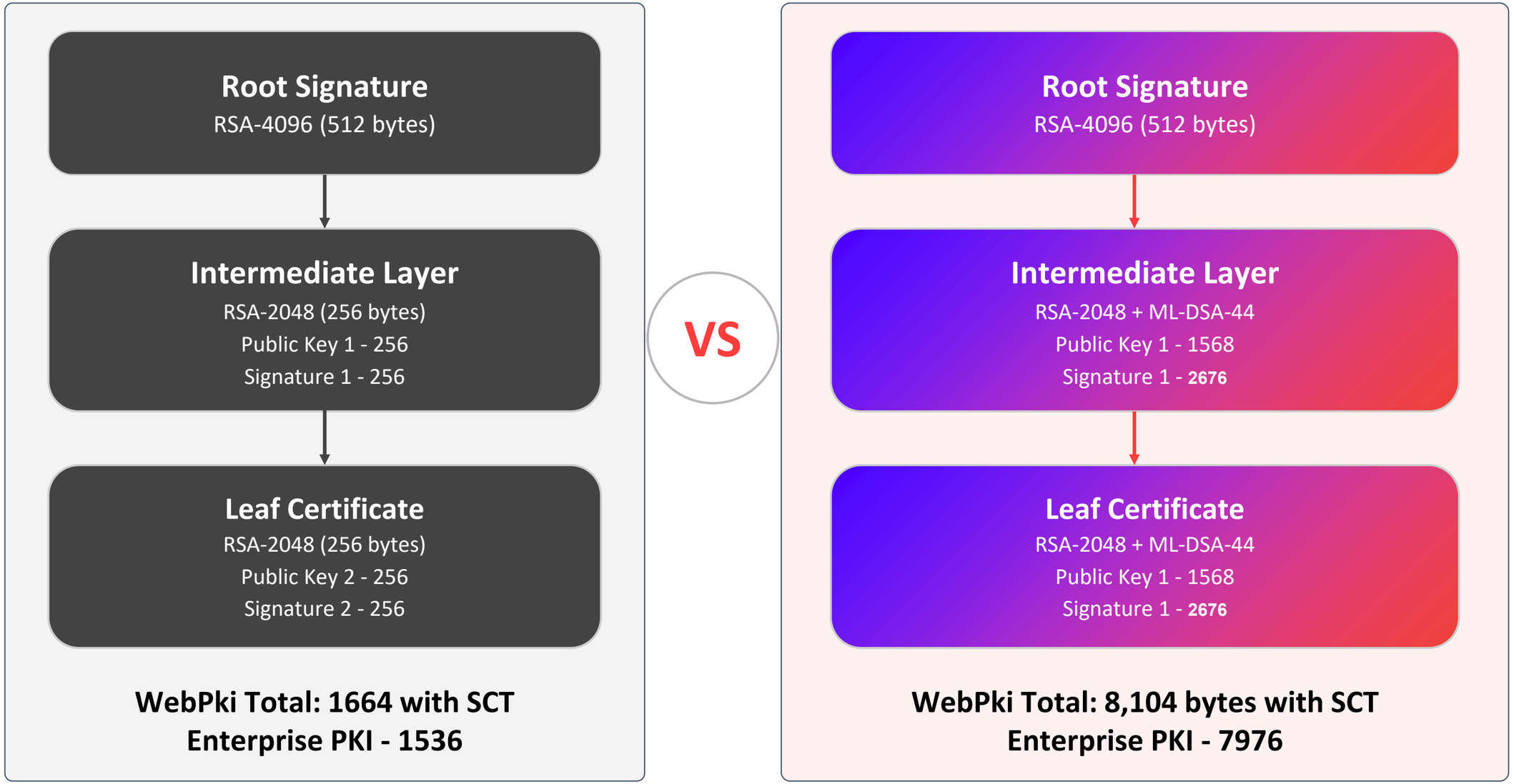
Hybrid PKI combines classical algorithms (RSA, ECDSA) with post-quantum algorithms (ML-DSA-44, ML-KEM) in a single certificate or signature structure. This approach maintains backward compatibility with existing systems while adding quantum-resistant protection.

Active IETF Draft -





Visual Comparison: Classical vs Hybrid PKI



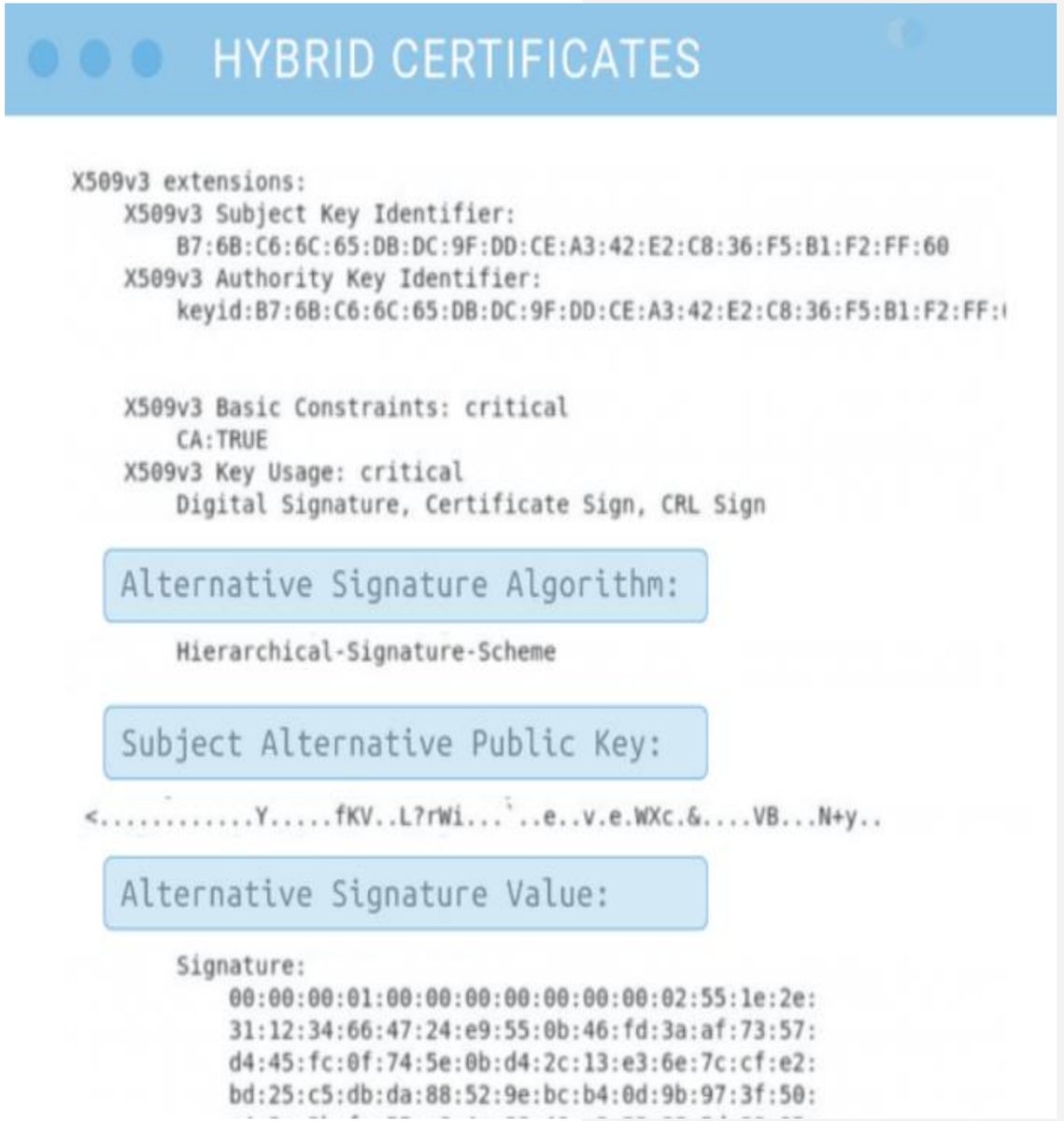
Why Hybrid PKI is the Optimal Balance

Certificate Chain	Total Size	Δ vs. RSA	Practicality Assessment
Classical RSA	1,664 bytes	Baseline	Efficient—current standard
Big RSA-4096	2,688 bytes	+1,024	Still manageable for most use cases
ML-DSA Leaf Only	4,484 bytes	+2,820	Acceptable with modern infrastructure
Smaller ML-DSA Leaf	4,020 bytes	+2,356	Better performance trade-off
Hybrid (RSA → ML-DSA)	**8,104 bytes**	**+6,440**	**Optimal balance of security & compatibility**
Full PQC Chain	14,724 bytes	+13,060	Quantum-secure but bandwidth-intensive

Hybrid chains ~5× larger than RSA but offers massive ~45% size reduction compared to full PQC implementations while maintaining quantum resistance where it matters most.

How it looks?

Hybrid PKI combines classical algorithms (RSA, ECDSA) with post-quantum algorithms (ML-DSA, ML-KEM) in a single certificate or signature structure. This approach maintains backward compatibility with existing systems while adding quantum-resistant protection.



Fortune 100 Leading the Charge

The world's largest organizations are already deploying hybrid cryptography as part of their PQC transition strategies. These early adopters are establishing blueprints others can follow.

Meta

Testing Hybrid TLS across its infrastructure, implementing hybrid key exchange to protect billions of daily connections. Their PQR (Post-Quantum Readiness) initiative provides a transparent roadmap.

Google

Integrated hybrid ECDH-Kyber key exchange in Chrome and across cloud services. Leading standards development and providing open-source implementations.

Global Telecom Providers

Major carriers are piloting hybrid PKI for network infrastructure and SIM card authentication—protecting subscriber identity in a quantum future.

Fortune 100 Leading the Charge

38%

Public Websites

Now support hybrid key exchange protocols

60%

Fortune 100 Companies

Have active PQC transition programs in 2025

5-10

Year Timeline

Average enterprise migration duration

Key Insight: Organizations need success stories and blueprints. The transition plans of early adopters—like Meta's PQR framework and Google's BoringSSL roadmap—provide critical templates for planning your own migration. Hybrid cryptography is the common thread across all successful strategies.

Why Hybrid PKI is Essential for Enterprises

Defense in Depth

Dual signatures (RSA/ECC + ML-DSA) require both to validate. Protection against unknown PQC flaws and future quantum attacks simultaneously.

Immediate Protection

Guards against "harvest now, decrypt later" attacks with quantum-resistant components active today, even as classical layers remain secure.

Crypto-Agility

Enables rapid algorithm switching without operational disruption. Test and validate PQC in production with secure classical fallback.

Phased Migration

Backward compatibility with legacy systems while providing quantum protection for updated infrastructure—critical for multi-year transitions.

RSA + PQC Dual Handshake: Enterprises can deploy interoperable transitions using hybrid CAs that issue certificates containing both classical and post-quantum public keys, enabling gradual ecosystem modernization.

Hybrid PKI: Policy and Governance Alignment

Implementing hybrid PKI isn't just a cryptographic upgrade—it requires evolving governance frameworks, compliance postures, and operational policies across your entire organization.

1 Certificate Policy Updates

Revise CPs and CPSs to define hybrid certificate lifecycle, validation rules, and algorithm combinations. Specify fallback behavior and sunset timelines.

2 Compliance Mapping

Align with NIST SP 800-208, CNSA 2.0, and emerging PQC mandates. Ensure audit trails for cryptographic transitions meet regulatory requirements.

3 Vendor & Partner Readiness

Assess third-party dependencies. Require hybrid support in procurement contracts. Coordinate migration timelines across the supply chain.

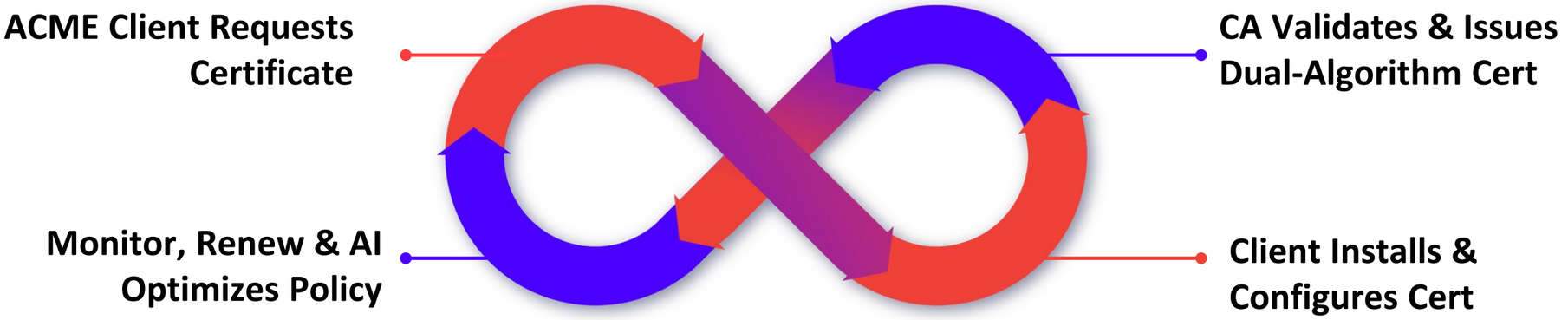
4 Incident Response Evolution

Update playbooks for PQC-related incidents—algorithm breaks, compatibility failures, performance degradation. Define clear rollback procedures.

Governance Tip: Establish a cross-functional PQC steering committee with representation from security, compliance, engineering, and business units. Crypto-agility is an enterprise transformation, not just an IT project.

Automation and Crypto-Agility: Scaling with ACME

Manual certificate management doesn't scale to hybrid PKI. ACME (Automated Certificate Management Environment) provides the automation backbone for rapid, consistent hybrid issuance across thousands of endpoints.



The ACME Advantage

Speed: Zero-touch provisioning reduces issuance time from days to minutes

Consistency: Standardized workflows eliminate configuration drift

Scalability: Handle millions of certificates without linear staffing growth

Agility: Swap algorithms via policy update—no manual intervention

ACME + AI: The Intelligent Migration Engine

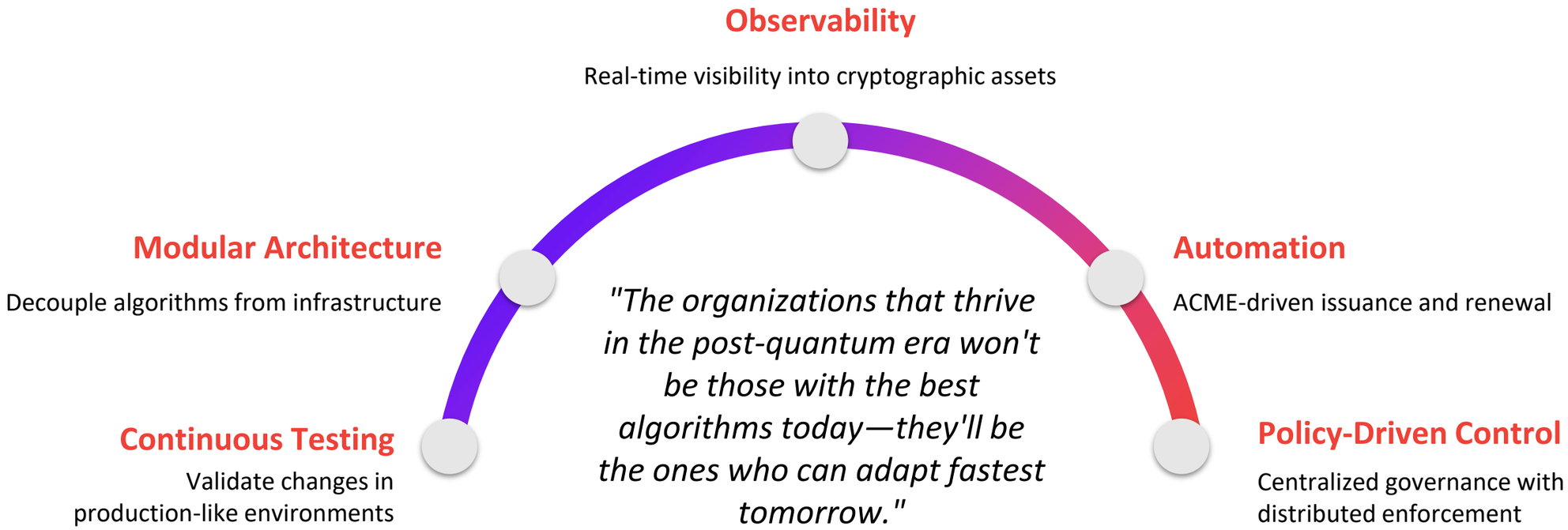
Combine ACME automation with AI-driven analytics to create measurable crypto-agility. Machine learning identifies optimal migration sequences, predicts compatibility issues, and dynamically adjusts rollout pace.

AI + ACME = Measurable Crypto-Agility

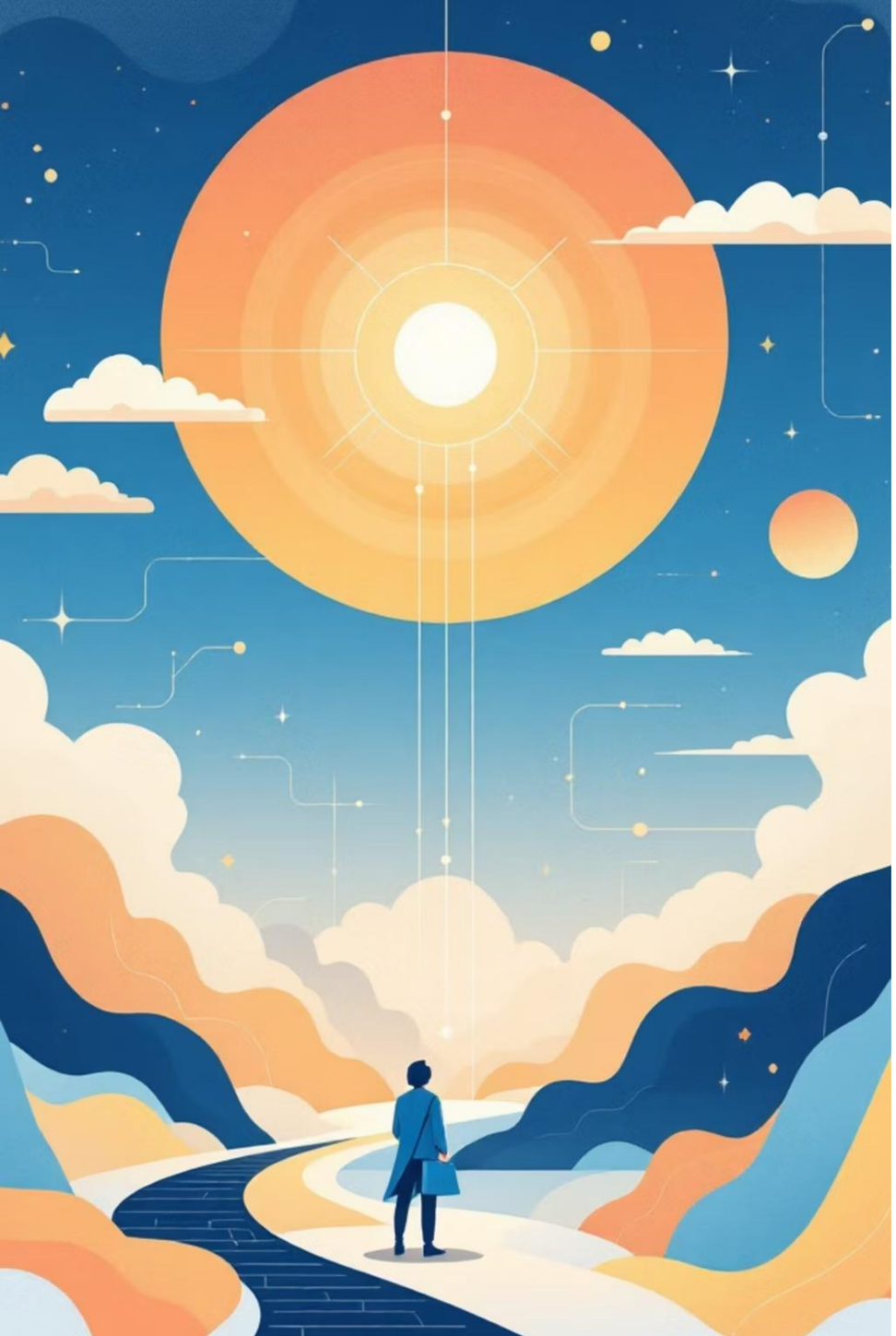
Organizations leveraging ACME for hybrid PKI report 80% reduction in operational overhead and 95% faster response to cryptographic vulnerabilities compared to manual processes.

Building Crypto-Agile PKI: The Foundation for PQC Success

Crypto-agility—the ability to rapidly swap cryptographic algorithms and protocols—is the ultimate goal. A crypto-agile PKI doesn't just ease the PQC transition; it future-proofs your organization against the next cryptographic evolution.



Your Next Steps: Assess your cryptographic inventory, prioritize high-value assets, pilot hybrid certificates, and invest in automation. The quantum threat is real, but with strategic planning and crypto-agile infrastructure, your organization will be ready.



Crypto-Agility: The Foundation of Quantum Readiness

Crypto-agility is the capability to rapidly switch cryptographic algorithms and primitives with minimal disruption. NIST emphasizes this as essential for post-quantum transition, enabling organizations to respond to emerging threats and evolving standards.

Gradual Introduction

Deploy quantum-resistant algorithms alongside classical ones without risky infrastructure overhauls

Layered Security

System remains secure even if one algorithm is compromised—protection against both current and future threats

Real-World Testing

Validate emerging NIST standards in production while maintaining baseline security with proven algorithms

Who Needs Hybrid Now? Organizations with long-lived secrets (governments, law firms, pharmaceuticals) or inflexible infrastructure (aerospace, automotive, telecommunications, HSM-dependent systems) face the highest risk and should prioritize immediate hybrid deployment.

Your Roadmap to Post-Quantum Readiness

01. Audit & Inventory with AI

Scan and catalog all cryptographic assets—certificates, keys, libraries, protocols. Prioritize based on data sensitivity and lifespan using AI-enhanced analytics

02. Pilot Hybrid Certificates

Deploy in non-production environments. Leverage AI to simulate performance, detect compatibility issues, and optimize rollout strategies

3. Define Transition Triggers

Establish clear catalysts for moving from hybrid to full PQC: regulatory mandates, customer requirements, NIST standard finalization, or risk threshold breaches

4. Update Governance & Documentation

Revise security policies, HSM configurations, incident response plans, and compliance frameworks. Deploy AI-based governance tools for consistency

"Standardization is essential, but adoption requires agility. The combination of strategic planning, hybrid implementation, and AI-enhanced orchestration transforms theoretical PQC migration into a measurable, actionable reality."

The time to act is now. Quantum computers may be years away, but your adversaries are already collecting your data. Build crypto-agility, deploy hybrid PKI, and secure your organization's long-term trust infrastructure today.

Q&A

Thank You for listening

- Build Crypto-Agility Now
- Inventory → Hybrid → Automate → Govern
- Start small. Automate fast. Evolve continuously

Linked in

ganeshmallaya

Thank You

appviewx