ARQIT

Beyond PKI:
Rethinking Trust in the Quantum Era

Roberta Faux

October 2025

“What you're supposed to do when you don't like a thing is change it. If you can't change it, change the way you think about it. Don't complain.”

— ***Maya Angelou***
Wouldn't Take Nothing for My Journey Now

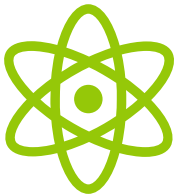
A Path to a Secure Future

ENCRYPTION

Cornerstone of Security

PQ PKI

A Critical Advancement



QUANTUM THREATS

PKI alone cannot address everything

The Way Forward: We must embrace new technologies to build a robust security playbook

PKI Certificate Turmoil

A closer look by DigiCert 2021

50,000	Certs being managed, some 100,000+
1,200	Unmanaged certs
43%	Annual growth in 2021
61%	Concerning amount of time managing certs
37%	3+ departments managing certs
66%	Outages from unexpected expiring cert
47%	Discover ‘rogue’ certs frequently

DigiCert

Global leader of TLS, SSL, IoT and PKI solutions

Used by nearly 90% of the Fortune 500 and 98 of the 100 largest global banks choose DigiCert

https://www.digicert.com/content/dam/digicert/pdfs/report/pki-automation-report-en.pdf

The Vast World of Public Certificates

Website/server identity	USG	National eID	Blockchain	OT/SCADA (utilities)
~300M domains	PIV + CAC = 8M Devices = 9M	200M-400M	~600M	~1 Billion
ePassports	**FIDO Passkey**	**Automotive**	**Financial**	**IOT**
~1.1 Billion	1 Billion	Billions	15+ Billions	Tens of Billions

Challenges of Traditional Public Key Lifecycles

ARQIT

- Inherent complexities / lack of flexibilities
- Improper implementation, i.e., CurveBall, ROCA, etc.
- Human error: forgotten certificates, incorrect installation
- Single Point of Failure: central authority
- Performance bottlenecks in high volume environments
- Scalability: volume, cost, infrastructure, labor, licensing
- Difficulty in ongoing security management and policy
- Key rotation / updates
- Revocation Lists: often slow, expensive to distribute, and nearly broken
- Long chains and rogue certs

Challenges of PQ Public Key

ARQIT

- Performance Hits: Latency/power drain. May be untenable in tactical edge
- Logistical Nightmares: Revocation complexity + interoperability + backwards compatibility
- Legacy Burden that will resist full migration
- Down time for “live systems”
- Lack of flexibility
- Cost
- Massive Scale: many billions

PKI is not a silver bullet.

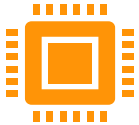
Trust is Expensive

Unraveling the Financial Puzzle of PKI Upgrades

- **PQC Migration**
  - Re-issuance of all certificates
  - Cost: ~$100–$200 billion globally by 2035
    - Breakdown: $50/certificate × 3 billion
  - Infrastructure upgrades: $20–$50 billion for CA systems, HSMs, and automation
  - Labor: $10–$20 billion for manual processes (60% lack automation)

- **PQC OPEX**
  - 10-15% increase due to complexity and volume
  - 2–3x more computationally intensive

The Colossal Certificate Ecosystem



Billions of Active Certificates

Secure connections for websites, apps, IoT, etc.

Rapid Annual Growth

300M+ per year

Projections of **trillions** by 2030 if unchecked

Diverse Ecosystem

Millions of domains

Gov's, enterprise networks, 5G, EVs

200+ CA makes fragmented dependencies

Upgrade Challenge

Concurrent global upgrade is logistically impossible

Downtime risk

1% failure == 15M sites offline or loss $100B+/year

Future Maintenance

Growth of AI automation

Risk of downtime, breaches, compliance failures, or even collapse in infrastructure

"71% of leaders fear their certificate authority could become untrusted."

~CyberArk

March2025

Mapping Quantum Threats: An Engineering Inventory of Cryptographic Dependencies

Carlos Benitez*

[Submitted on 2 Jul 2025 (v1), last revised 14 Jul 2025 (this version, v2)]

Pruning the Tree: Rethinking RPKI Architecture From The Ground Up

Why Public Key Infrastructure Isn't the Silver Bullet for Digital Security

by **EScholar: Electronic Academic Papers for Scholars** · September 9th, 2025

CLOUDFLARE The Cloudflare Blog

AI Developers Radar Product News Security Policy & Legal Zero Trust Speed & Reliability

Avoiding downtime: modern alternatives to outdated certificate pinning practices

2024-07-29

Decentralized Credential Status Management: A Paradigm Shift in Digital Trust

Patrick Herbke

Service-centric Networking

[Submitted on 10 Jan 2024 (v1), last revised 11 Jan 2024 (this version, v2)]

Failures of public key infrastructure: 53 year survey

Adrian-Tudor Dumitrescu, Johan Pouwelse

How do we move forward?

Can we do the unthinkable and ditch certs?

Multi-Pronged Quantum Resilience Strategy

1

Simplify

Lessen reliance on PKI, certificate-based systems, and Type-1 encryptors

2

Password-less Authentication

Token-based systems like OAuth 2.0, device-bound keys, i.e., biometrics or hardware

3

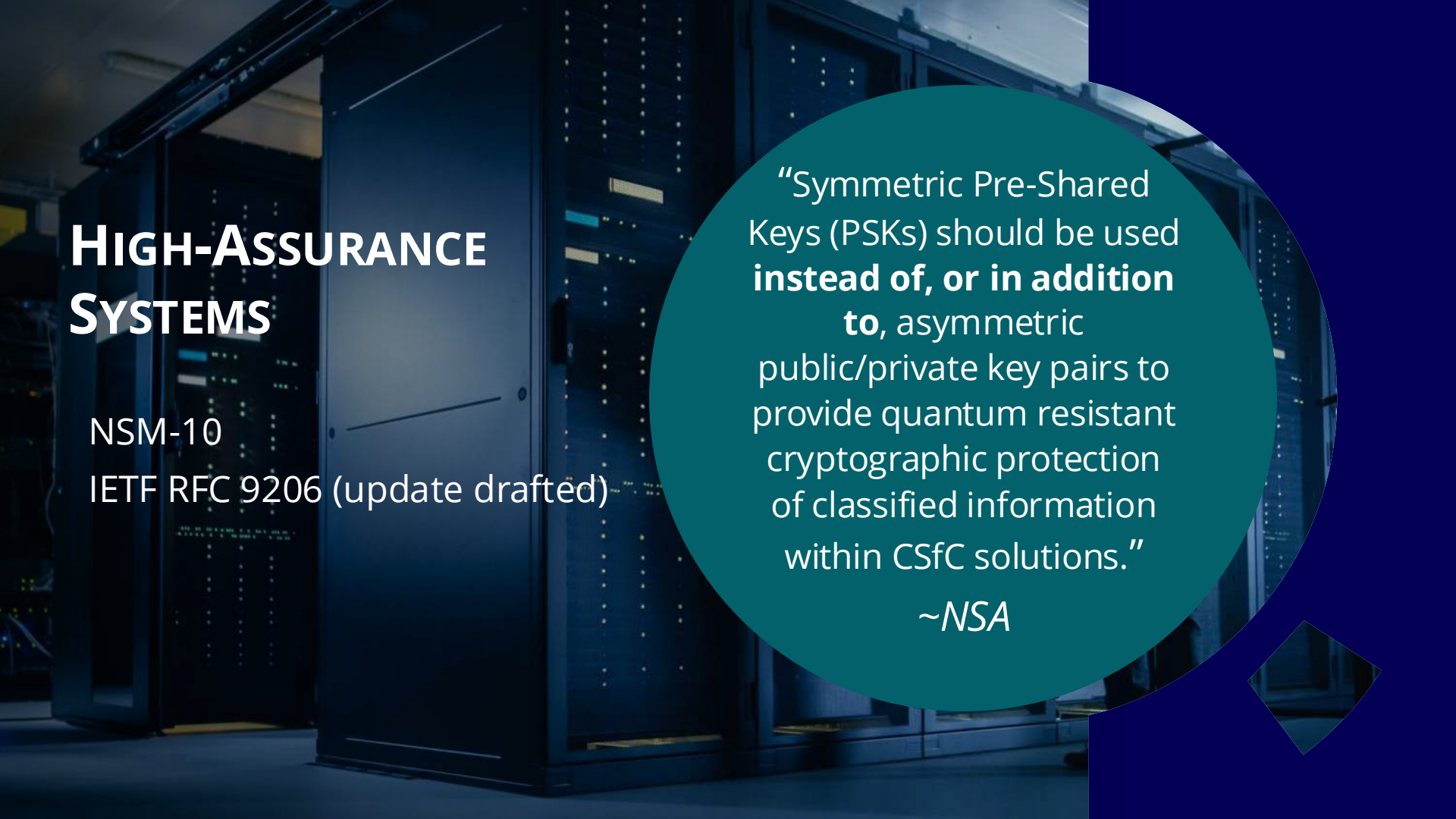
Other Technologies

Secure Multi-Party Computation, Decentralized Identity Systems

4

Symmetric Key Cryptography

Simpler, faster, and quantum-resistant



High-Assurance Systems

NSM-10

IETF RFC 9206 (update drafted)

"Symmetric Pre-Shared Keys (PSKs) should be used **instead of, or in addition to**, asymmetric public/private key pairs to provide quantum resistant cryptographic protection of classified information within CSfC solutions."

~NSA

Symmetric Keys as Quantum-Resistant Backbone

- AES-256: Faster, smaller keys, low overhead
- Larger Quantum Delta
  - Grover's algorithm needs 2^{128} ops—safer margin than Shor’s
- Established resistant to side-channels

Symmetric isn't new—it's battle-tested, quantum-safe, robust, and ready to scale.

Foundational Standards for Symmetric Cryptography

ARQIT

NSA CSfC
RFC 9206

Symmetric Key Management Annex 3.0: Symmetric PSKs may be used instead of X.509 authentication

Standard for CNSA

RFC 8784
RFC 9370

Mixing Preshared Keys in the IKEv2 for Post-Quantum Security

Multiple Key Exchanges

RFC 9257
RFC 9258

Guidance for External Pre-Shared Key (PSK) Usage in TLS

Importing External Pre-Shared Keys (PSKs) for TLS

ISO/IEC 11770-2

Part 2: Mechanisms using symmetric techniques

RFC 8696
IETF draft SKIP

Using PSK in the Cryptographic Message Syntax

Secure Key Integration Protocol

IEEE 802.1AE

PPK based MACsec

encryption keys

Best of Both Worlds: Strategy of KEM + Symmetric

PQ KEM as initial authentication or “bootstrap”

Defense in Depth

Strong auth + efficient ongoing protection

Symmetric agreement and rotation for data flows between endpoints

Benefits of a Symmetric-Centric Approach

ARQIT

- ACCELERATE QS TRANSITION
- REDUCES PKI DEPENDENCY
- ENABLES AGILITY
- SCALABLE
- CONSTRAINED ENVIRONMENTS
- COST-EFFECTIVE

Call for New Conversations and Reflections on Rethinking PKI

In the quantum era, efficiency and simplicity is security.


ARQIT
Let’s collaborate!
<Roberta.Faux@ArqitInc.US>