

digicert®

AUTOMATION DEMO SERIES - SEASON 3

FROM BASICS TO BREAKTHROUGHS:

Practical sessions to help you prepare
for 47-day certificates



Speakers



Dean Coclin
Sr. Director, Industry Strategy
DigiCert



James Jackson
Product & Solutions Strategy
DigiCert



Year-in-Review

CAB Forum Recap

What Happened?

Timelines for Reduction (Ballot SC-81)

October 7, 2024



Apple proposes schedule for radical reduction of certificate lifetime and validation reuse periods

Reasons for Shortening Lifetimes

Web PKI Challenges

- Evolving standards
- Compromised certificates can live long lives
- Stringent revocation requirements

Automation is imperative

- Humans can't keep up with such lifetimes
- Frequent outages are unacceptable
- Available standards for automation (ACME)

Impact on Outages & Costs

www.thestack.technology
Expired Certificate crashed \$6 trillion Bank of England system
Network configuration, CA and SWIFT issues, and certificate expiration blamed for a series of RTGS outage sthe past year.
Sep 30, 2024

cio
ServiceNow certificate error disrupts operations for hundereds of organizations
The expired MID Server Roo G2 SSL certificate caused connectivity failures across multiple services, including Orchestration, Discovery...
Sep 24, 2024

Data Center Knowledge
Windows Azure Cloud Crashed by Expired SSL Certificate
Microsoft suffered a major outage for its Azure storage cloud and other online services after an SSL certificate expired.
May 30, 2024



Expired certificates cause outages

Manual updates are costly

8X more certificates, **40X** more validations will be needed

Massive increase in operational cost, even more outages

Urgent need for PKI Modernization and AUTOMATION

Where Are We Today?

March 15
2026



~ 2X per year frequency renewal

Last Year's Poll Question Results



By-The-Numbers: Preparing For 47 Days

34%

of organizations know where their certificates are*

At current validity periods, an organization with **1,000** public certificates requires approximately **2,000** successful renewal-and-deploy cycles per year.

The Operational Math

At **47-day** certificate validity:
1,000 certificates × ~7.8
renewals/year = **7,800 renewal-
and-deploy cycles annually.**

At a **99%** success rate, that is
still **78 failures per year.** At
98%, it is **156.**

**Manual renewal is mathematically
incompatible with this new reality.**

PKI Complexity Rising Rapidly in Enterprises



100X

Machine to User Identities

**Certificate Management is
Becoming More Complex**

53%

Organizations lack
sufficient PKI staff

256K

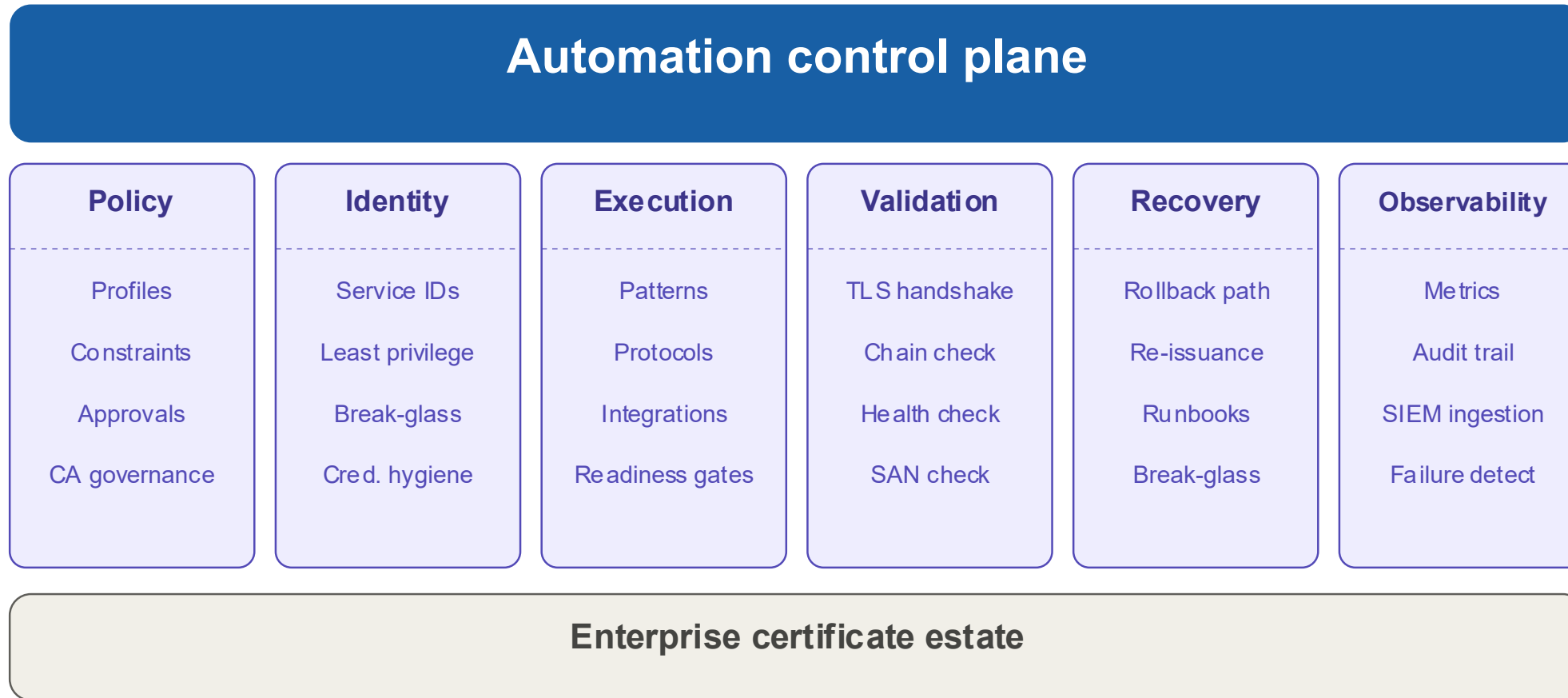
Average certificates
per organization



The Need for Automation

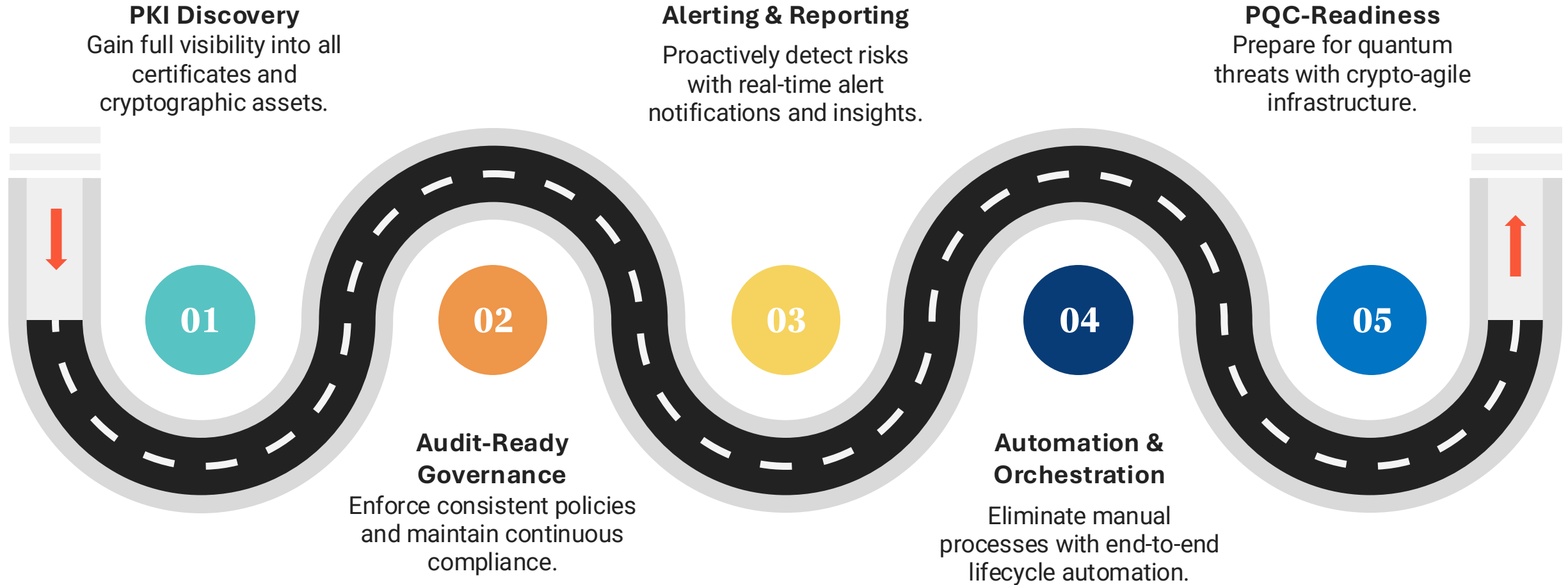
Manual processes are no longer sustainable

Governed Control Plane, Not Convenience Layer



Automation is not only about reducing administrative efforts

Where Do I Start?



Quantum-Safe Cryptography is Here

Begin Transitioning to Post-Quantum Cryptography Now

Quantum computing will render traditional cryptography unsafe by 2029. It's worth starting the post-quantum cryptography transition now.

By [Mark Horvath](#) | September 30, 2024

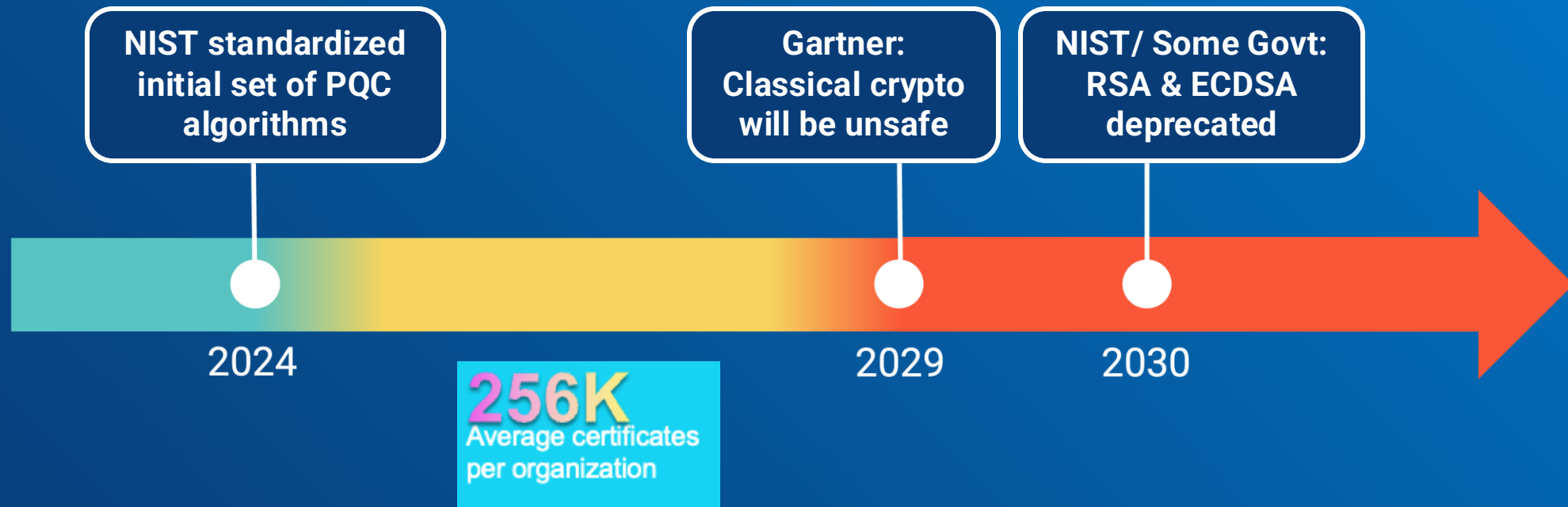
Gartner



Standard	Purpose	Quantum-Safe NIST Algorithm
FIPS 203	Encryption	ML-KEM: Module-Lattice-Based Key-Encapsulation Mechanism (formerly CRYSTALS-Kyber)
FIPS 204	Authentication	ML-DSA: Module-Lattice-Based Digital Signature Algorithm (formerly CRYSTALS-Dilithium)
FIPS 205	Authentication	SLH-DSA: Stateless Hash-Based Digital Signature Algorithm (formerly SPHINCS+)

Quantum computers break current cryptography
Post Quantum Cryptography (PQC) is here
Time to act is NOW, once in a generation upgrade
Aligned with PKI Modernization cycle

Quantum Countdown



- Initial algorithms finalized → PQC Standards activity accelerated
- Target PQC readiness dates being specified by governments & Gartner
- Short window to take action

Considerations

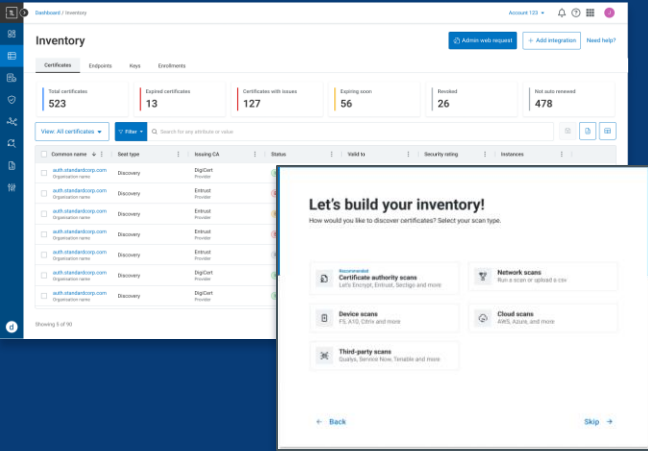
What's next?



PKI Modernization

Baseline

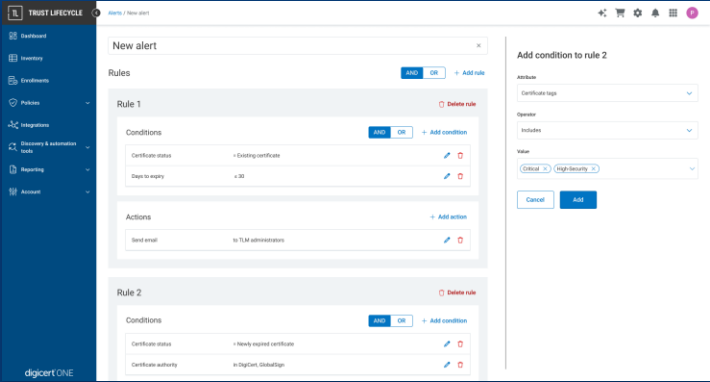
Discovery, visibility and trust baseline



Build a trusted inventory using connectors, scanning and CT monitoring.

Issuance

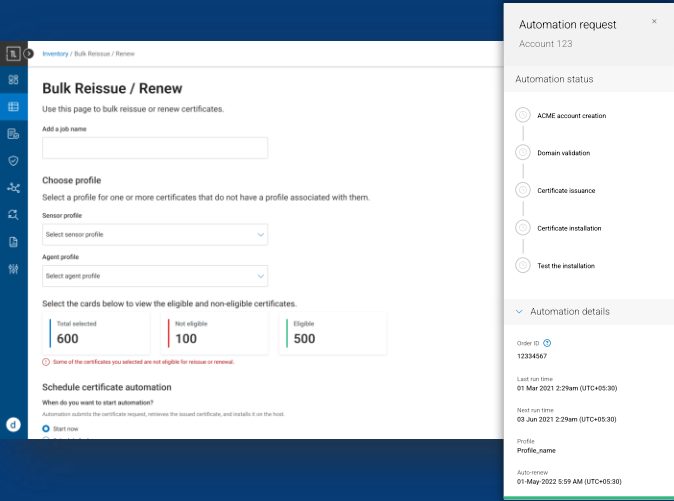
CA design for public and internal CA



Set up CA hierarchies and issuance paths for public and private trust.

Automation

Automation patterns, strategies and readiness



Plan, prioritize and automate certificate lifecycle management across your organization.

Q&A

**THANK
YOU**