KEYFACTOR

Cryptographic governance today

Preparation to Post-Quantum tomorrow

Pierre.Codis@keyfactor.com

What are machine IDs?

- X.509 certificates, Root keys
- SSH keys and certificates
- Encryption keys
- Code signing certificates

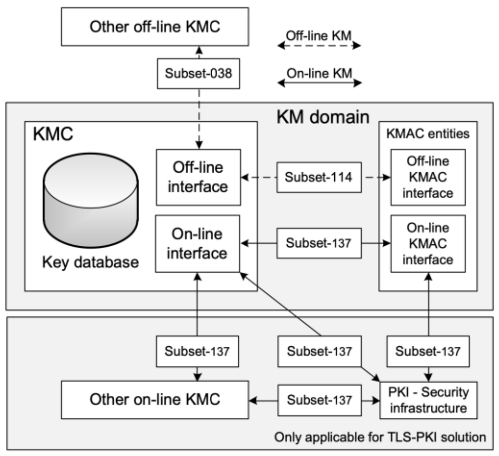
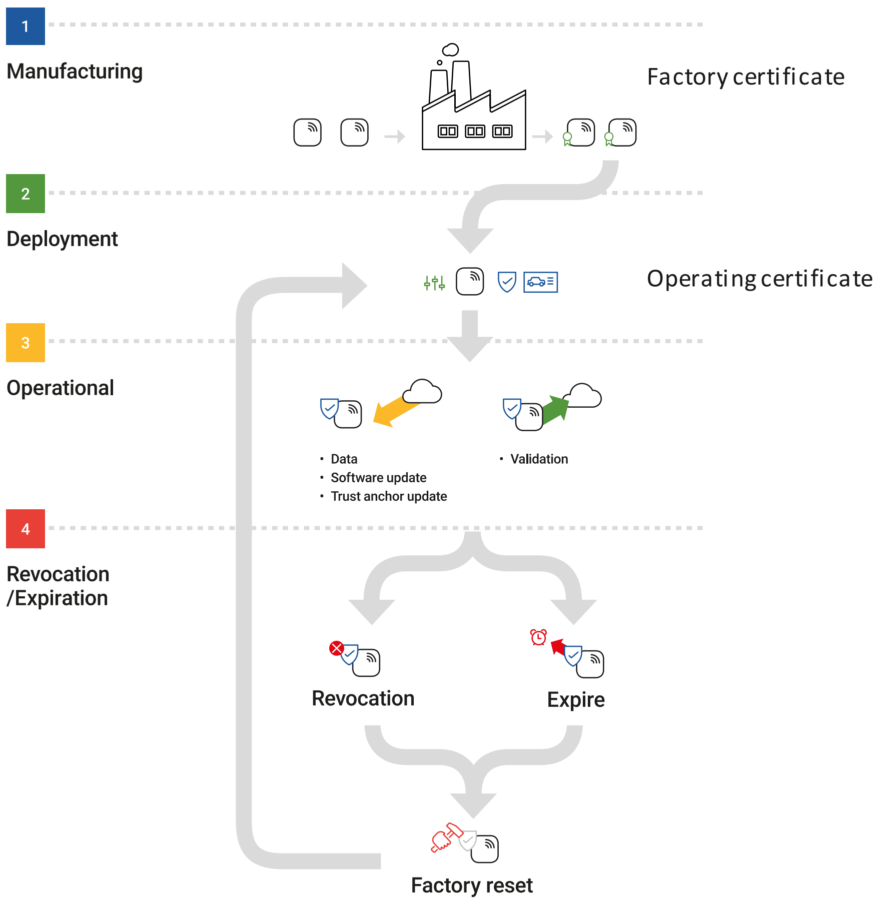


Figure 1 – KMS Reference Architecture



Enrolment protocols: CMP. EST, SCEP, ACME
Real-time certificate validation OCSP

What’s the story?

Quantum is coming

Quantum computers are being developed by tech giants and nation states.

That means new risks

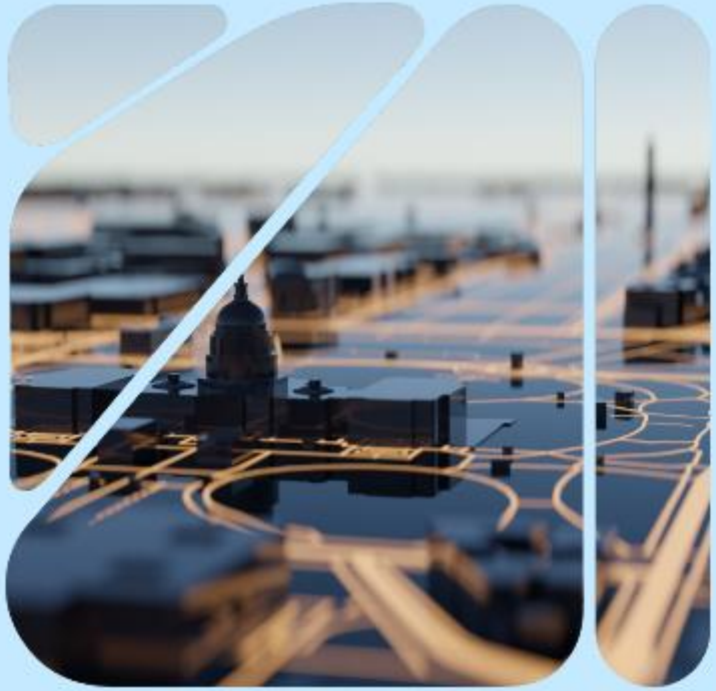
These computers will be capable of cracking the algorithms we rely on today.

We need new algorithms

New quantum-resistant algorithms are already here and will be standardized by 2024.

It’s time to prepare

Making the transition to PQC will take years – the time to plan and prepare is now.



"Although NIST will not publish the new post-quantum cryptographic standard for use by commercial products until 2024, CISA and NIST strongly recommend organizations start preparing for the transition now..."

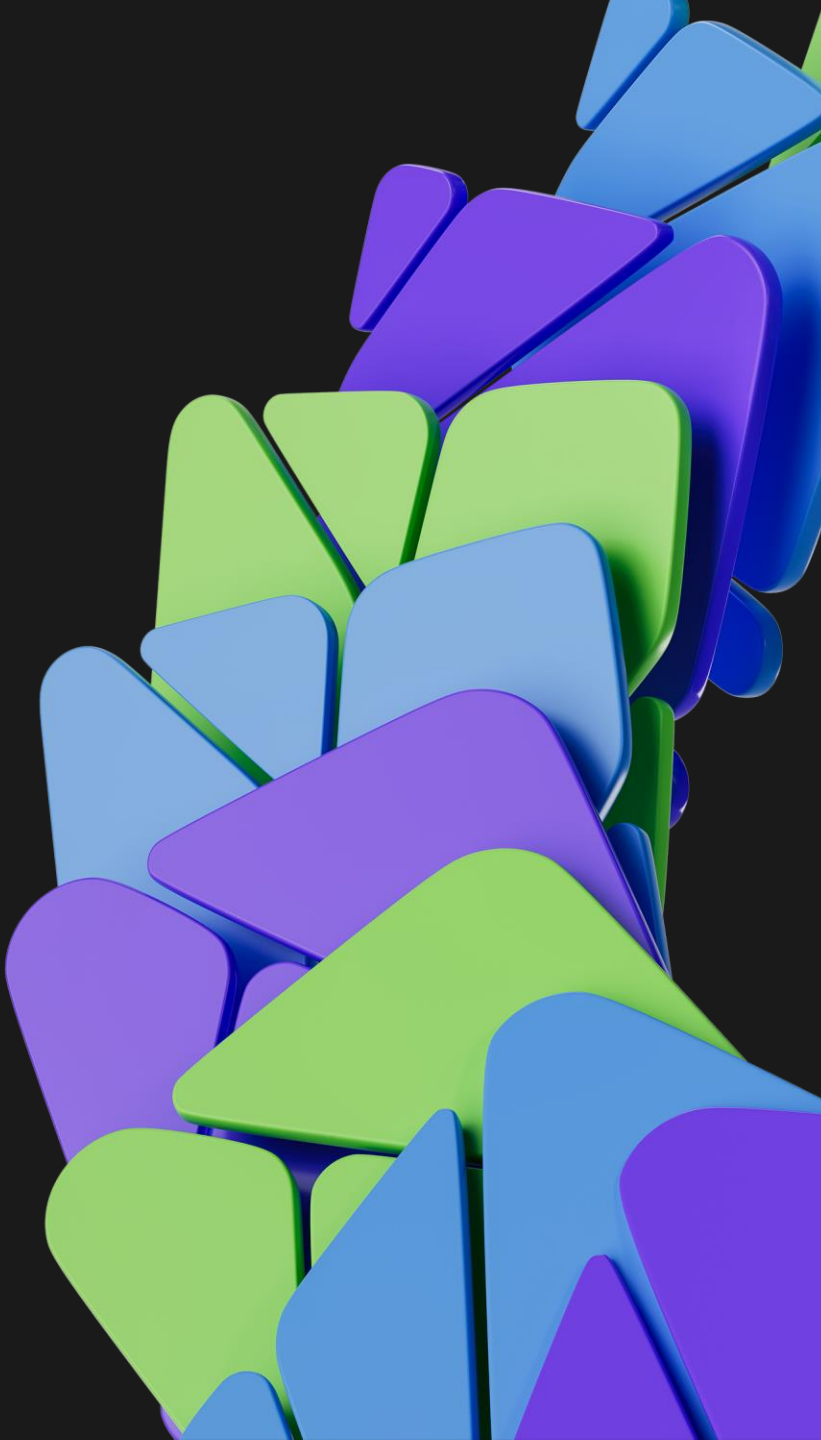
White Paper: Start Planning Ahead for Post-Quantum Security

What organizations should do to prepare

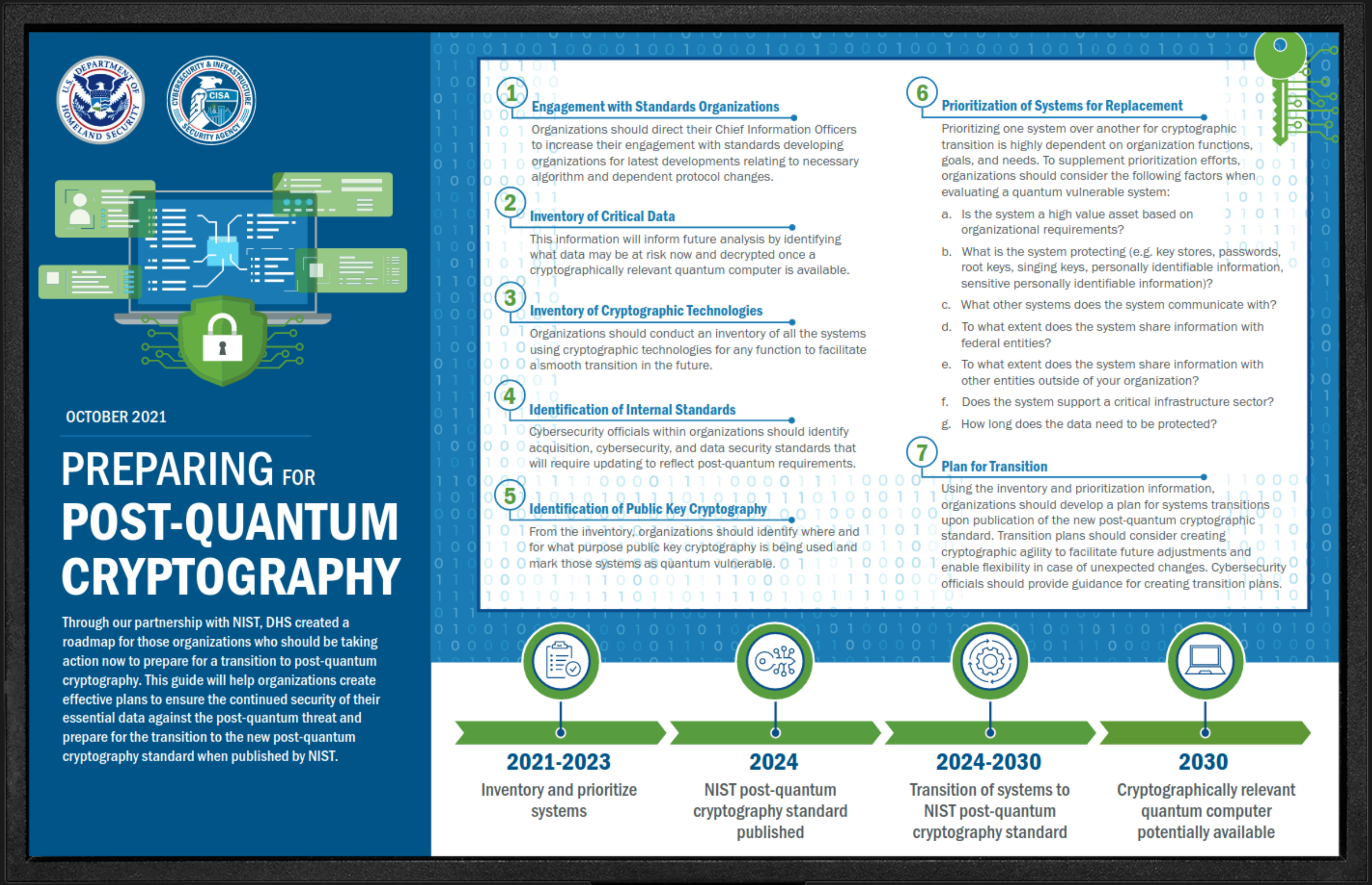
1) Identify where, and how, public-key algorithms are being used on information systems

2) Mitigate enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/update of hardware, software, and services that use quantum-vulnerable algorithms

3) Develop a risk-based playbook for migration involving people, processes, and technology



Goverment Recommendations



OCTOBER 2021

PREPARING FOR POST-QUANTUM CRYPTOGRAPHY

Through our partnership with NIST, DHS created a roadmap for those organizations who should be taking action now to prepare for a transition to post-quantum cryptography. This guide will help organizations create effective plans to ensure the continued security of their essential data against the post-quantum threat and prepare for the transition to the new post-quantum cryptography standard when published by NIST.

1 Engagement with Standards Organizations

Organizations should direct their Chief Information Officers to increase their engagement with standards developing organizations for latest developments relating to necessary algorithm and dependent protocol changes.

2 Inventory of Critical Data

This information will inform future analysis by identifying what data may be at risk now and decrypted once a cryptographically relevant quantum computer is available.

3 Inventory of Cryptographic Technologies

Organizations should conduct an inventory of all the systems using cryptographic technologies for any function to facilitate a smooth transition in the future.

4 Identification of Internal Standards

Cybersecurity officials within organizations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.

5 Identification of Public Key Cryptography

From the inventory, organizations should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

6 Prioritization of Systems for Replacement

Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:

a. Is the system a high value asset based on organizational requirements?

b. What is the system protecting (e.g. key stores, passwords, root keys, singing keys, personally identifiable information, sensitive personally identifiable information)?

c. What other systems does the system communicate with?

d. To what extent does the system share information with federal entities?

e. To what extent does the system share information with other entities outside of your organization?

f. Does the system support a critical infrastructure sector?

g. How long does the data need to be protected?

7 Plan for Transition

Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard. Transition plans should consider creating cryptographic agility to facilitate future adjustments and enable flexibility in case of unexpected changes. Cybersecurity officials should provide guidance for creating transition plans.

2021-2023
Inventory and prioritize systems

2024
NIST post-quantum cryptography standard published

2024-2030
Transition of systems to NIST post-quantum cryptography standard

2030
Cryptographically relevant quantum computer potentially available

PQC Current State of Play

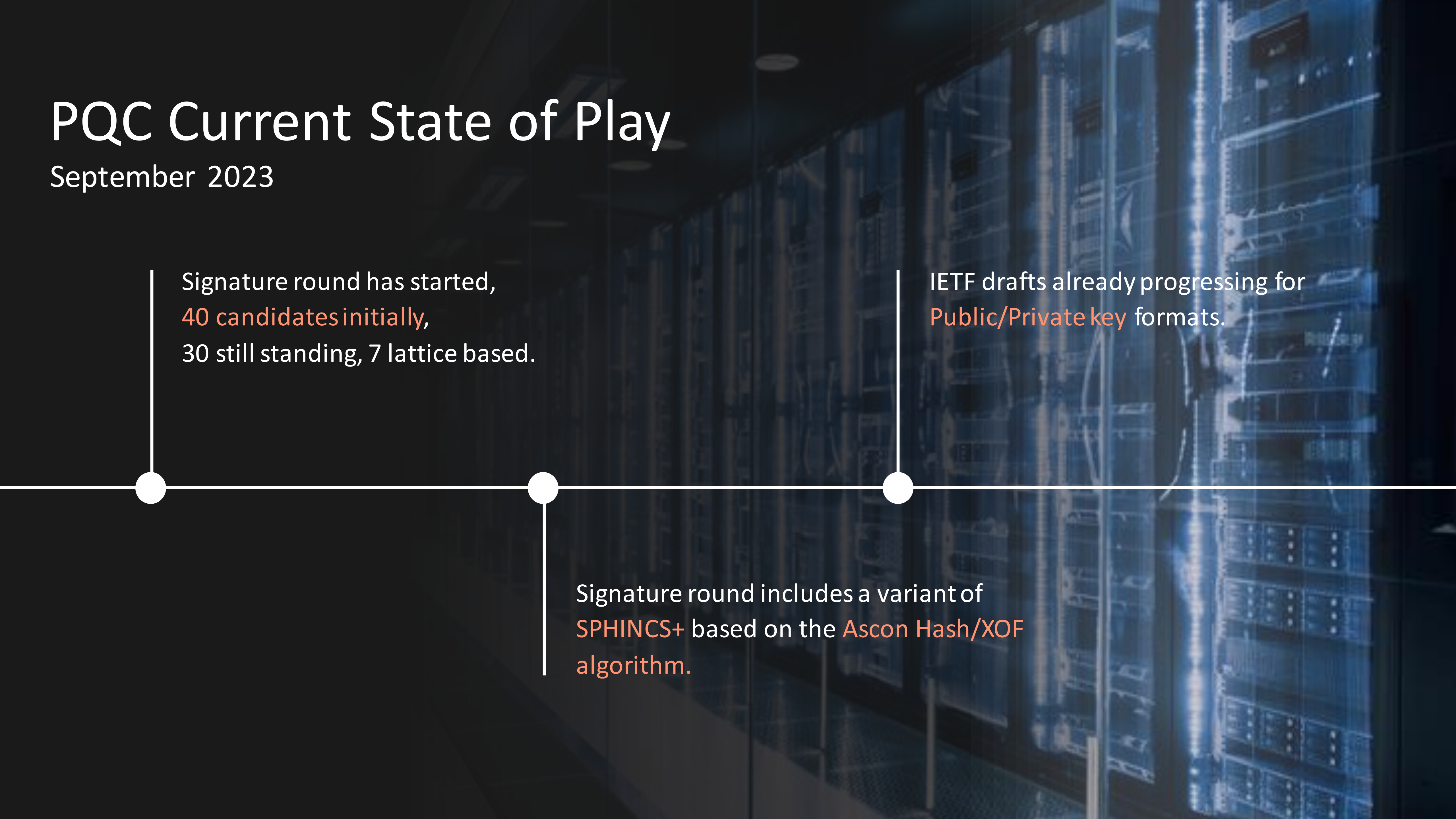
September 2023

FIPS 203 ML-KEM (formerly Kyber), FIPS 204 ML-DSA (formerly Dilithium), and FIPS 205 SLH-DSA (formerly SPHINCS+) now out in draft format.

Round 4 drawing to a close – round between BIKE and HQC. Classic McEliece to be standardized outside NIST, NIST still deciding whether to join in.

PQC Current State of Play

September 2023



Signature round has started,
40 candidates initially,
30 still standing, 7 lattice based.

Signature round includes a variant of SPHINCS+ based on the Ascon Hash/XOF algorithm.

IETF drafts already progressing for Public/Private key formats.

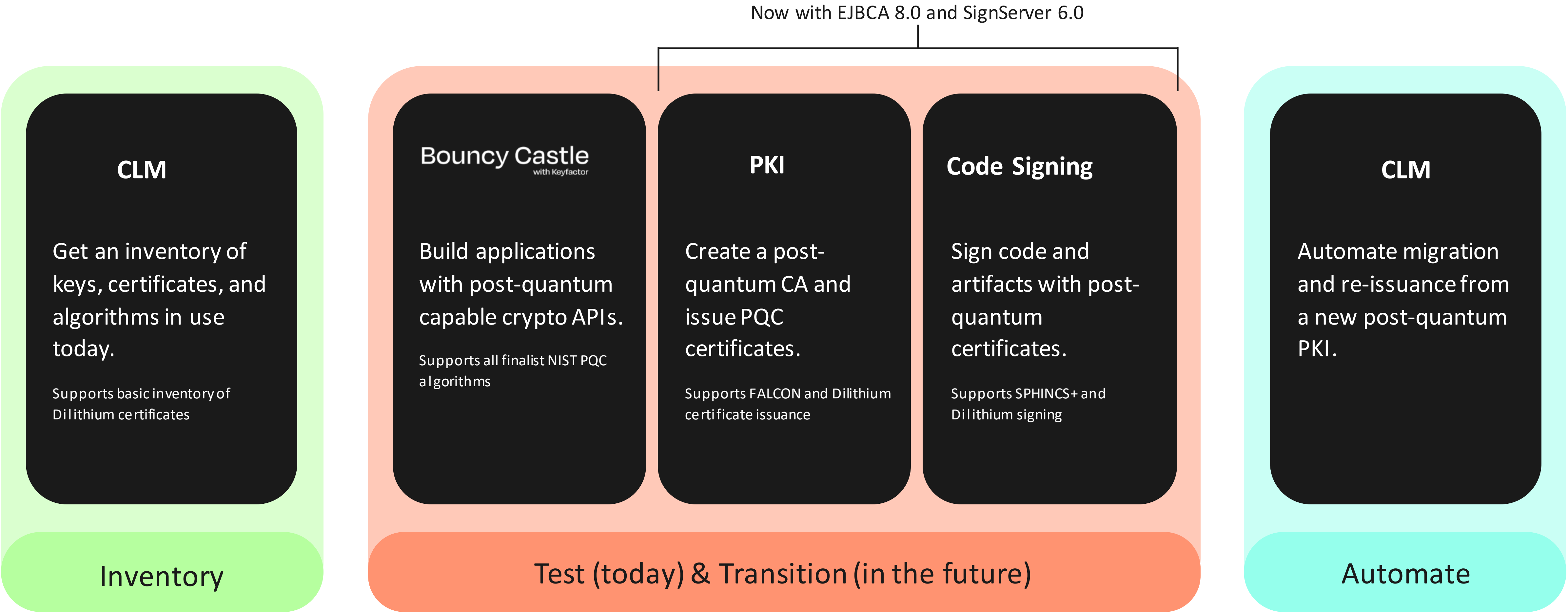
PQC Current State of Play

September 2023

IETF drafts also written for additional elements for certificates, cryptographic message syntax, certification request, management, and migration to quantum ready.

X.509 now includes the “alt” extensions.

Quantum-ready solutions



Now with EJBCA 8.0 and SignServer 6.0

CLM

Get an inventory of keys, certificates, and algorithms in use today.

Supports basic inventory of Dilithium certificates

Inventory

Bouncy Castle with Keyfactor

Build applications with post-quantum capable crypto APIs.

Supports all finalist NIST PQC algorithms

PKI

Create a post-quantum CA and issue PQC certificates.

Supports FALCON and Dilithium certificate issuance

Code Signing

Sign code and artifacts with post-quantum certificates.

Supports SPHINCS+ and Dilithium signing

Test (today) & Transition (in the future)

CLM

Automate migration and re-issuance from a new post-quantum PKI.

Automate

Efharisto poli!

KEYFACTOR