KEYFACTOR

# Cryptographic governance today

# Preparation to Post-Quantum tomorrow

Pierre.Codis@keyfactor.com

# What are machine IDs?

X.509 certificates, Root keys

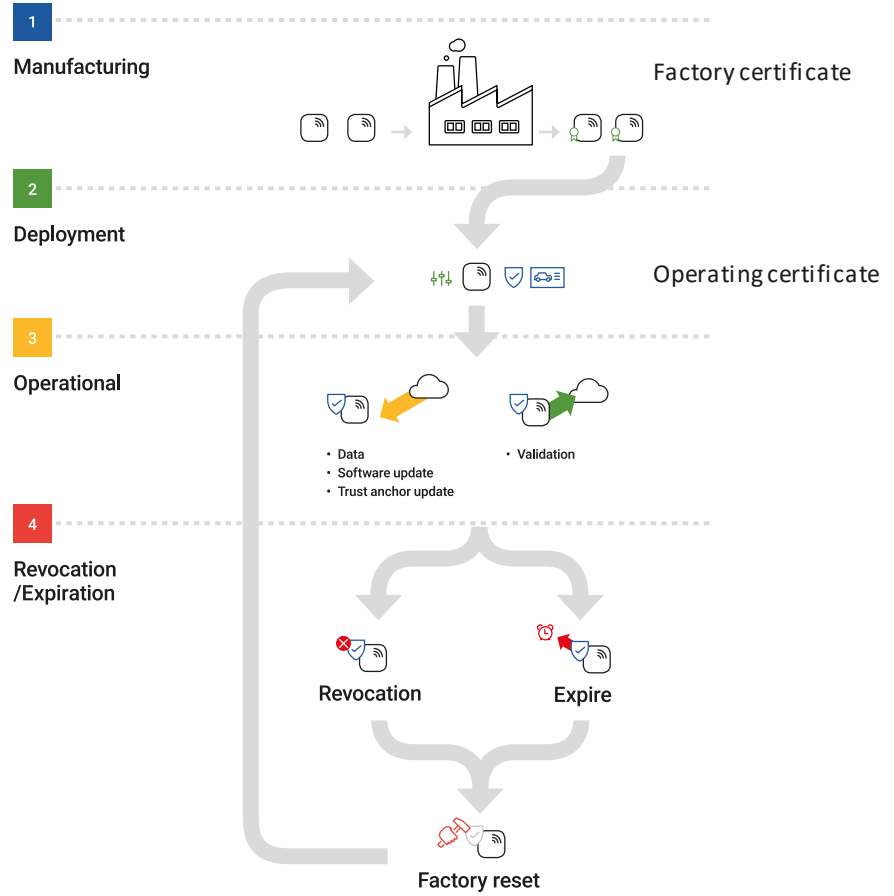
SSH keys and certificates

Encryption keys

Code signing certificates

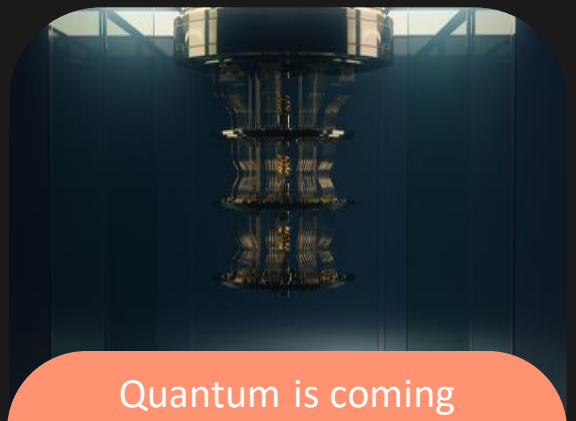



Figure 1 – KMS Reference Architecture




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

# What’s the story?



## Quantum is coming

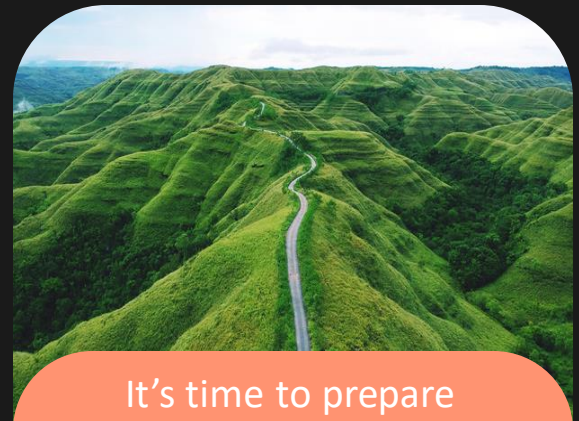
Quantum computers are being developed by tech giants and nation states.

## That means new risks

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

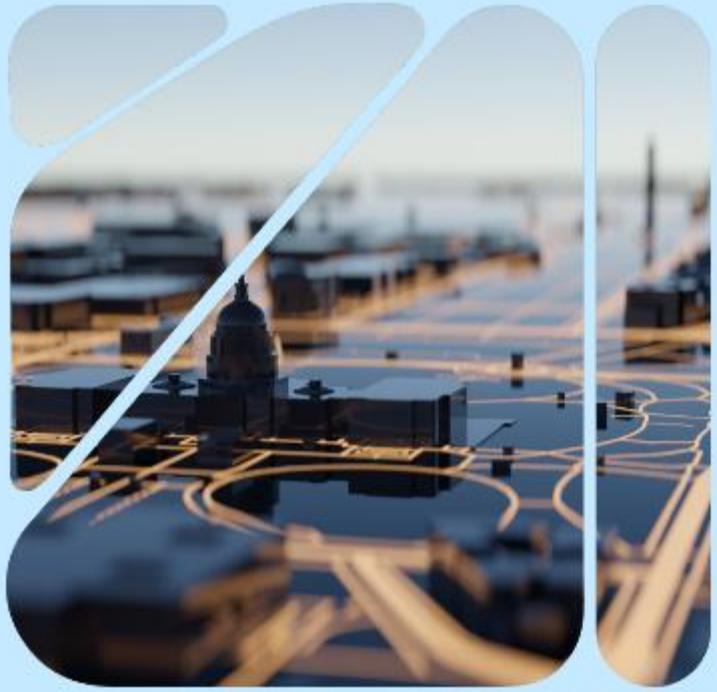
## We need new algorithms

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..."

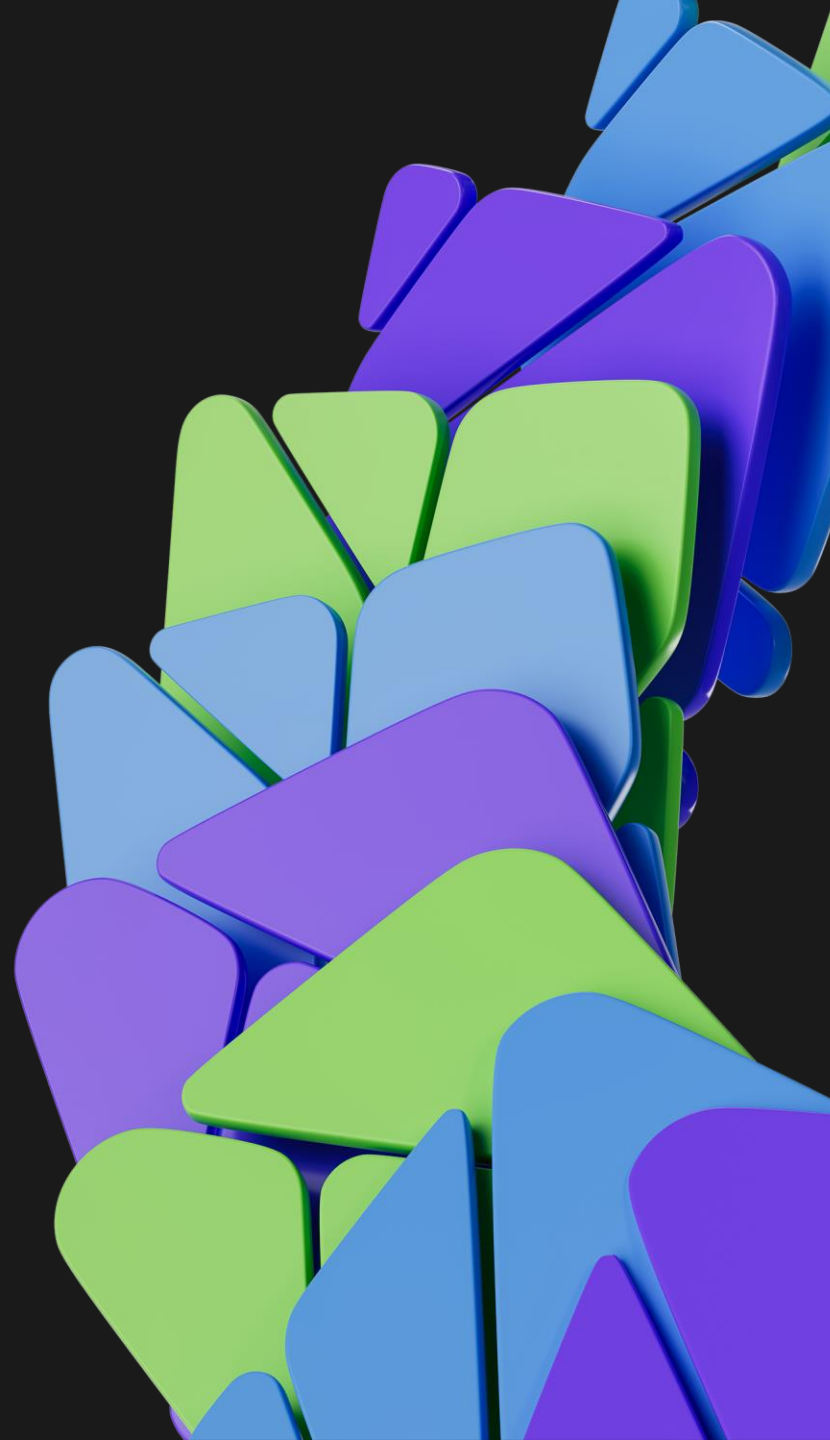
White Paper: Start Planning Ahead for Post-Quantum Security

# What organizations should do to prepare

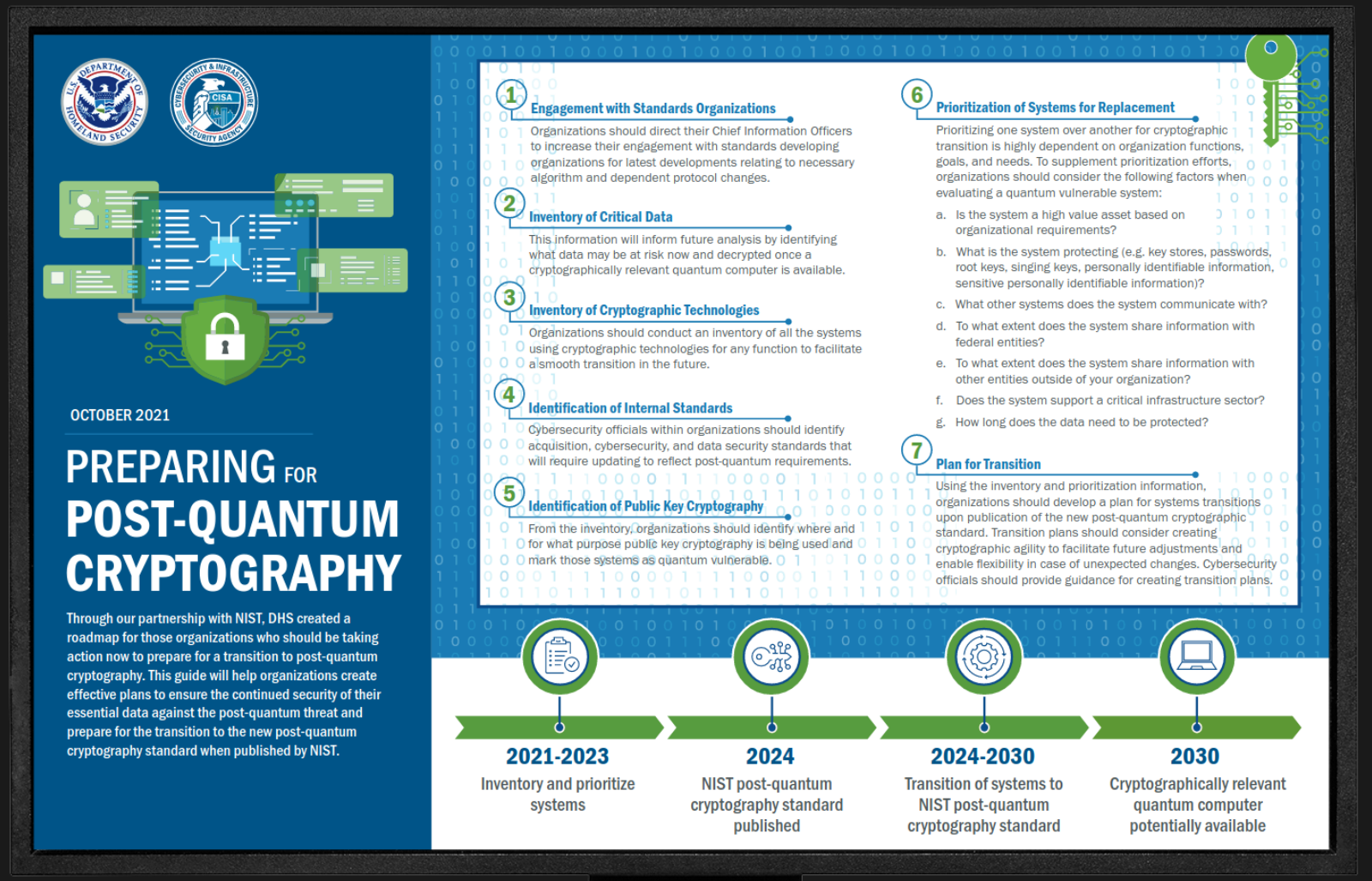
1) Identify where, and how, public-key algorithms are being used on information systems

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



# 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.

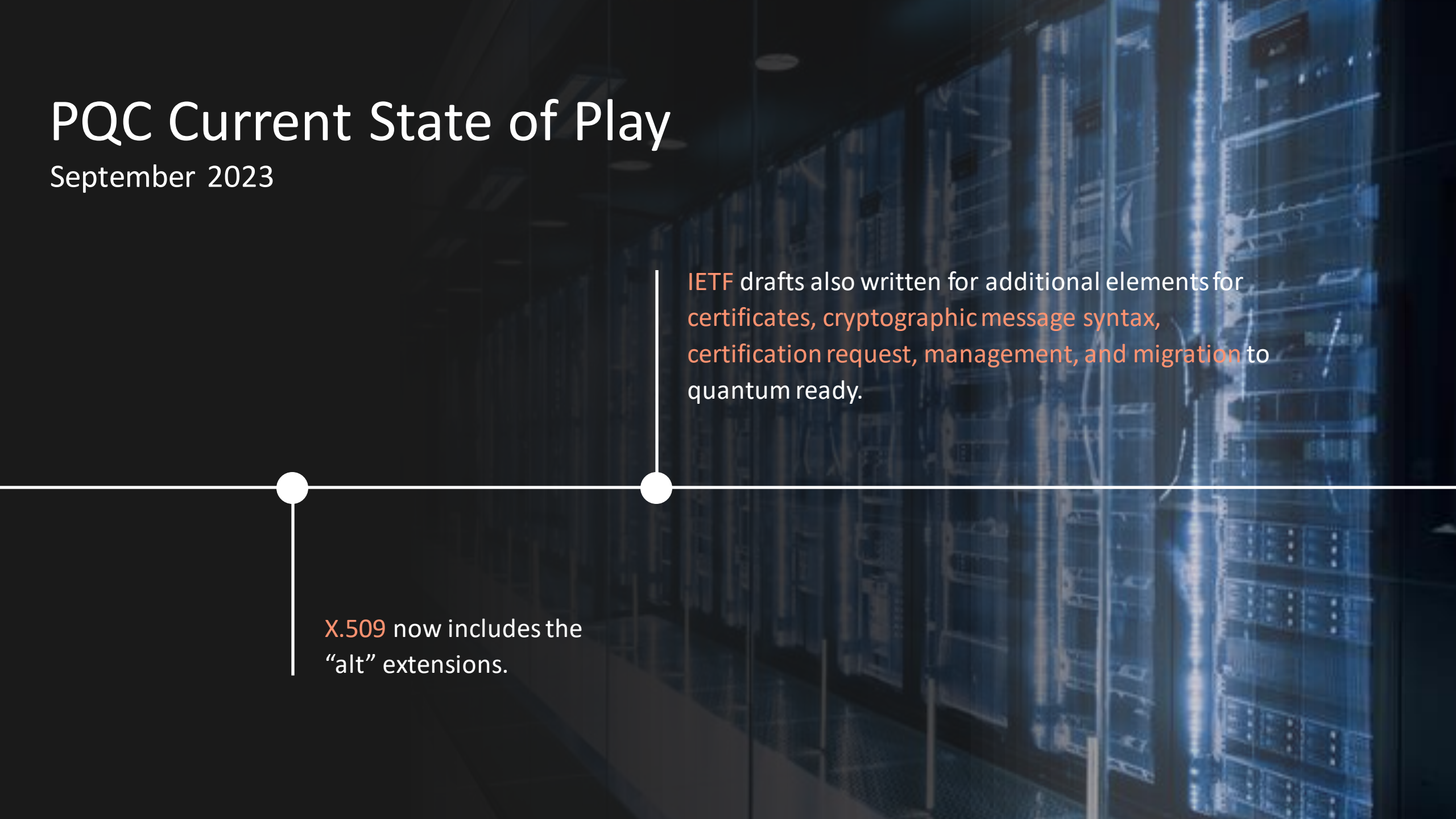
IETF drafts already progressing for Public/Private key formats.

# PQC Current State of Play

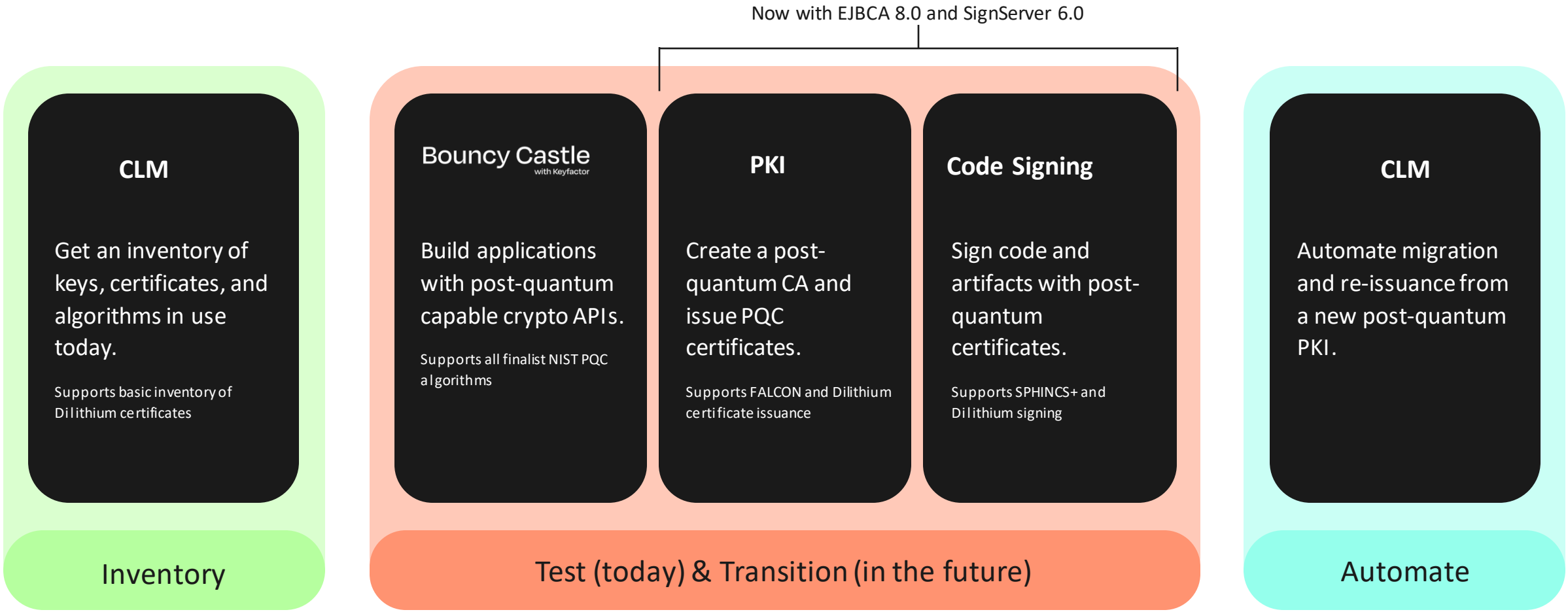
September 2023

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



# Efharisto poli!

KEYFACTOR