THE EU CYBER ACTS CONFERENCE

Tuesday, March 24 - 26.2026
Steigenberger Wiltcher's, Brussels, Belgium

PKI Center™
Aurora™ NETWORKS
A Vistance Networks Business

Secure Boot and Key Management for Embedded Devices in the Post-Quantum Transition

Authors: Oscar Jiang, James Ni, Xin Qiu, Lisa Yin

Presenter: Dr. Xin Qiu

Xin Qiu, Ph.D.

Head of Security Solutions and PKI Center, Aurora Networks

Dr. Xin Qiu brings over 25 years of expertise in Public Key Infrastructure (PKI), device and software security, with a portfolio of 90+ patents.

She leads cross-functional teams delivering trusted, scalable security services to device manufacturers and network operators worldwide.

Agenda

- Introduction - background
- Key Challenges to Post-Quantum Cryptography (PQC) Adoption
- 3-Stage Transition Framework for Gradual PQC Adoption
- Secure Boot & Device Credential Provisioning & Key Mgmt.
- Conclusions

Post Quantum Cryptography (PQC) in Simple Terms

RSA / ECC under quantum threat

- Quantum computers could break today's public-key algorithms

PQC, quantum safe

- New cryptographic algorithms resistant to quantum attacks
- Based on lattice, code-based, or hash-based math instead of integer factoring (RSA) & elliptic curve discrete logarithm (ECC)

NIST standardization progress

- NIST has completed standardization of the first post-quantum algorithms, signaling the industry's move from research to implementation readiness

Why PQC Transition Is Critical Now?

Past transition were slow

- MD5→SHA, DES→AES took years.

PQC is broader in scope

- replacing all public-key algorithms across systems and protocols.

Requires balance

- agility without disrupting core services

Delaying action increases risks

- adversaries may already be harvesting encrypted data for future quantum decryption

Key Considerations – Device Lifecycle & Cost

Long Device Lifespans

- Many hardware systems—consumer and non-consumer alike—are designed to last 10–15+ years.

High Replacement Costs

- Replacing deployed devices is complex and expensive.

In-Field Update

- Limited infrastructure and device capability for secure in-field updates, including secure software and PQC credential provisioning.

Hardware Constraints

Limited Availability of PQC-Ready Hardware

- PQC-capable security chips are not yet available
- Many existing devices cannot be easily upgraded for PQC

PQC Chip and Hardware Design Takes Time

- Developing dedicated PQC accelerators is complex, costly, and affects performance
- Integration requires significant redesign and validation

Leveraging Symmetric Encryption for PQC Transition

Symmetric encryption such as AES remains secure

- Even against quantum attacks, AES-256 retains 128-bit security

How Symmetric Encryption Helps:

- Protects PQC keys: Secures keys at rest and in transit
- Leverages Existing Hardware – Many devices already support AES hardware acceleration
- Bridges the Transition - Provides an efficient alternative before PQC-ready chips become available

We can use existing hardware security features as a foundation to bootstrap PQC migration

Where Security is Enforced

Two dominant approaches in industry to security -

Reactive: Detection-based security reacts to attacks

Network security and malware detection focus on identifying and responding to threats after systems are already running.

Regulatory and ecosystem requires building trust upfront – "Security by Design"

Focus of Today's Presentation

Proactive: Device and Software Security

Device Credentials:

Keys and certificates enable secure access to infrastructure, services, and resources.

Software Trust:

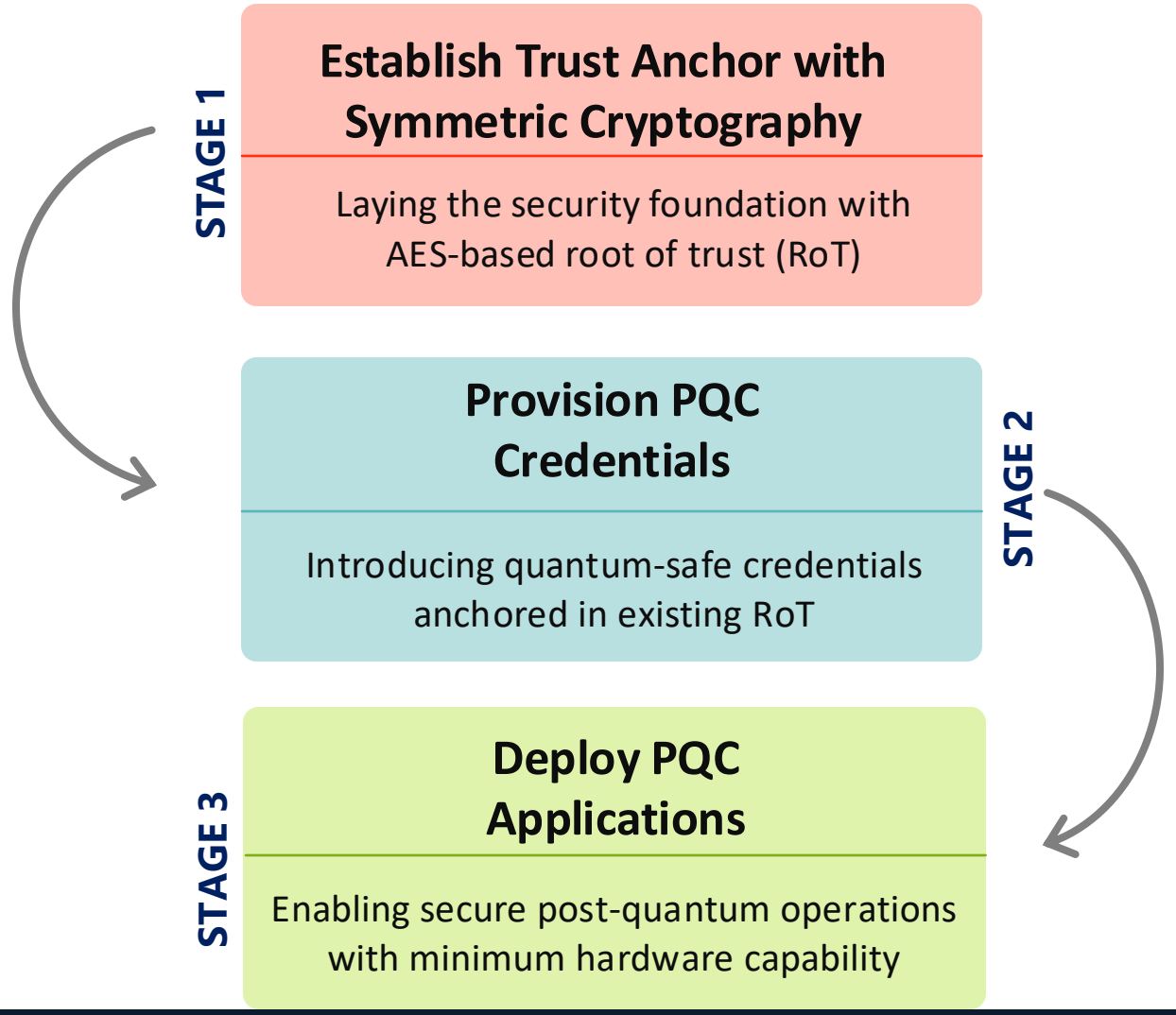
Authenticity, composition visibility, and vulnerability awareness before deployment.

3-Stage Transition Plan

- Leverage device's built-in hardware AES engine to perform authenticated secure boot.
- Store a unique pre-shared AES key in the chip's protected memory.
- Manage keys and access control from the infrastructure side to enforce policy and trust.

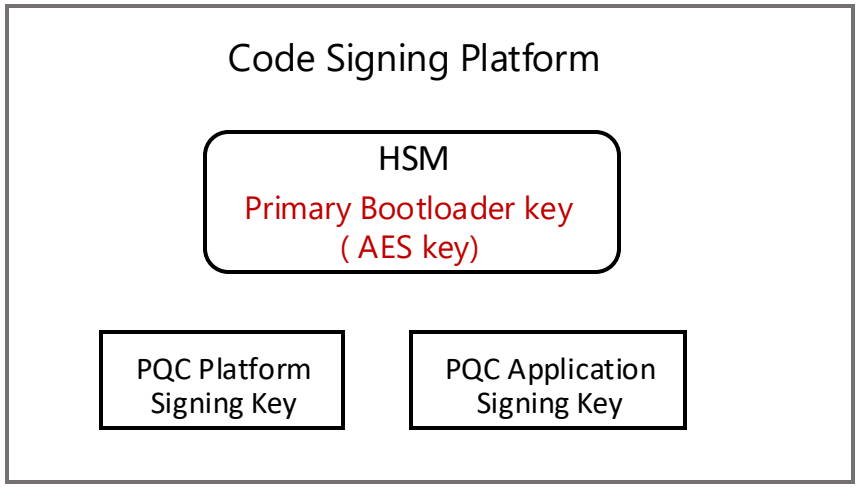
- Securely download the provisioning software to the device, using the secure boot in Stage 1.
- Generate PQC credentials on the device to avoid key exposure.
- Protect PQC private keys using the AES key (already securely stored on chip).

- Securely distribute and install PQC-enabled applications, again leveraging the trusted boot chain from Stage 1.
- Use the PQC credentials provisioned in Stage 2 to enable secure communication and data protection.

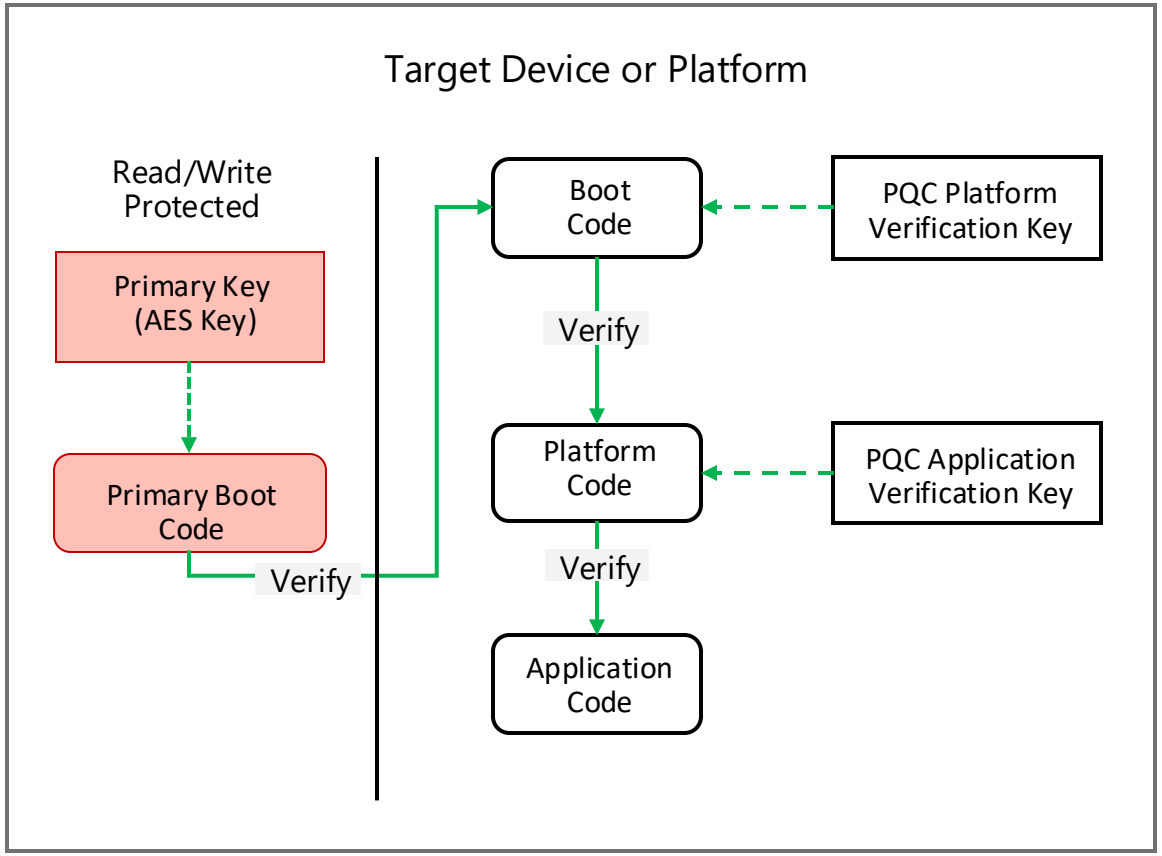


AES RoT for PQC-Based Software Protection

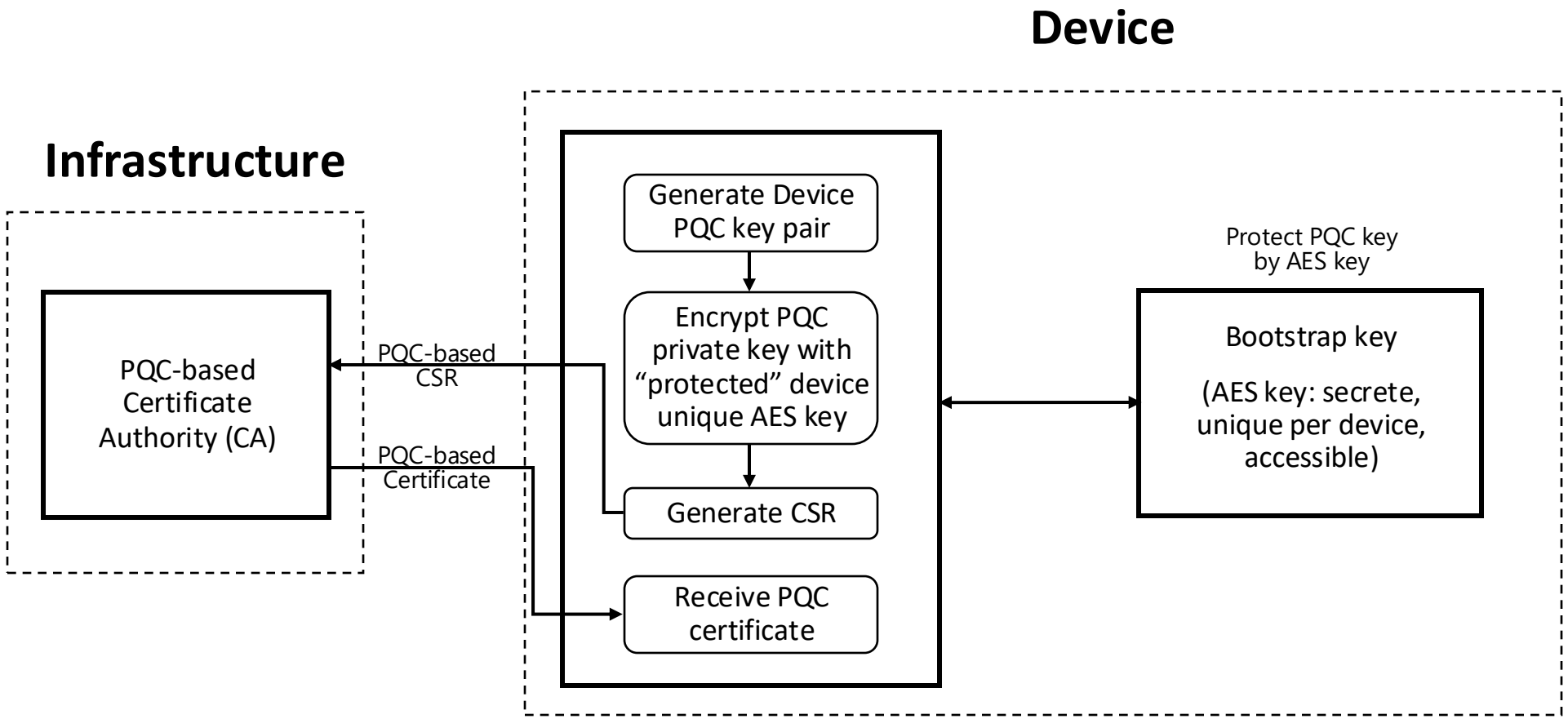
Infrastructure: Signing



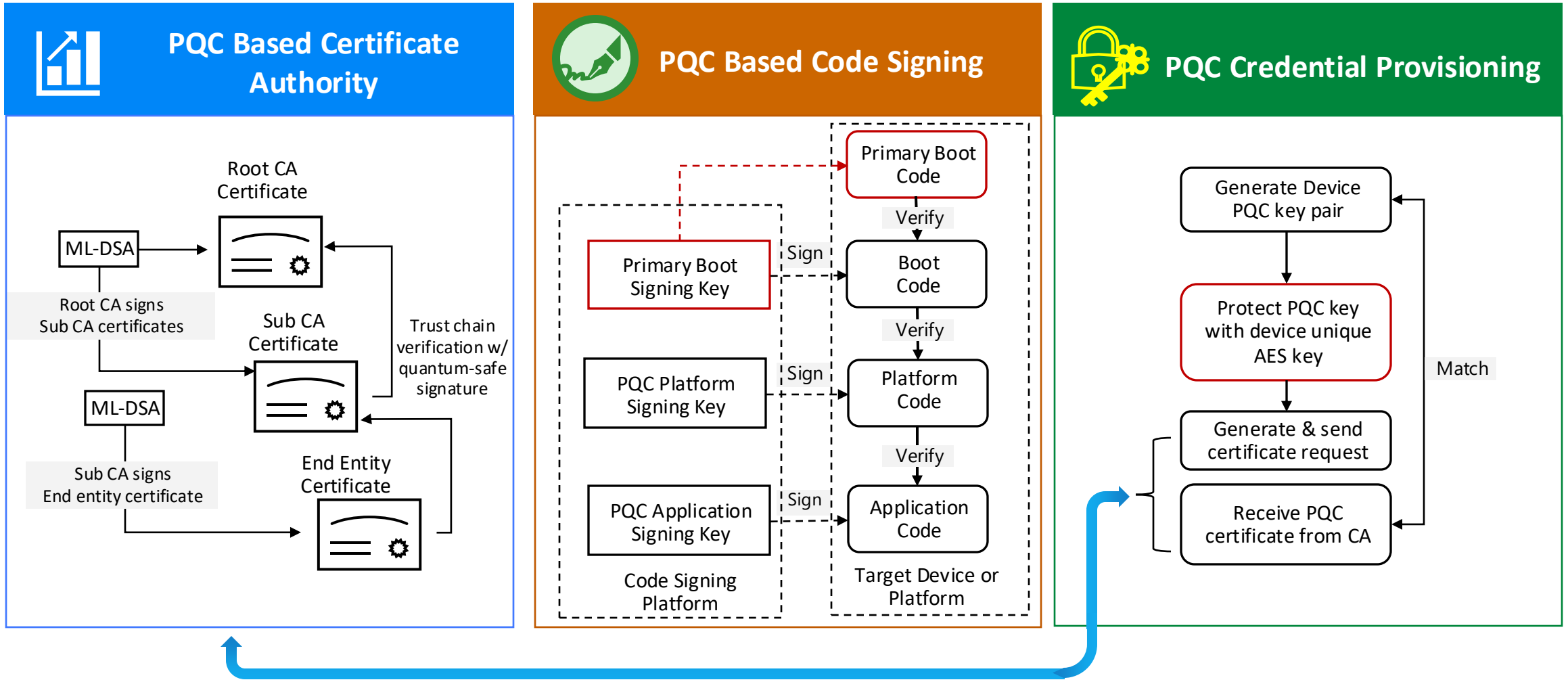
Device: Verifying



AES Protected PQC Credentials Provisioning



Quantum-Safe Advancement Focus



Practical Path to Post-Quantum Readiness

Key decisions

- When and where to introduce PQC
- How to manage mixed device capabilities at scale
- How to evolve cryptography without service disruption

How to engage

- Assess device populations and lifecycle constraints
- Align PQC strategy with operational and business realities
- Pilot safely, then scale across vendors

Key Takeaways

A full hardware swap is unrealistic - an incremental transition through software implementation could be considered.

Balancing security & practicality is needed to ensure both security and feasibility

This framework is about making post-quantum migration actually deployable on real devices to minimize the immediate risk

THANK YOU!

Q&A

xin.qiu@auroranetworks.com

PKI-center.com