COMMSCOPE®

embeddedworld Exhibition&Conference North America

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

November 5, 2025

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

Presenter: Xin Qiu

CommScope PKI Center™ www.pki-center.com

Objectives of This Talk

Understand the impact of Post-Quantum Cryptography (PQC)

Identify what changes with PQC - Secure Boot and Firmware Signing

Explore strategies for a smooth transition

COMMSCOPE®

Why Secure Boot and Key Management Matter

Rising firmware threats

- Code injection and bootloader tampering common in connected devices

Secure boot as foundation of trust

- Each layer verifies the next before execution
- Prevents unauthorized or modified firmware

Key management as the enabler with quantum algorithms

- Defines where signing and verification keys live and how they're protected
- Extends trust from factory to field updates

COMMSCOPE®

 |

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
- Use lattice-, code-, or hash- based math instead of integer factoring (RSA) and 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

COMMSCOPE®

Why PQC Transition Is Critical Now?

Past transitions 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

Quantum timeline uncertain, but impact inevitable

- “Harvest now, decrypt later” risk affects data and firmware signed today

COMMSCOPE®

Secure Boot Today

Layered verification chain

- Hardware bootloader → platform firmware → application firmware

Current crypto foundation

- RSA / ECDSA signatures

Keys and trust anchors:

- Signing keys in HSM
- Verification keys / hash in device secure memory or secure element

Unique Challenges for IoT and Embedded Systems

Limited Availability of PQC-Ready Hardware

- PQC-capable security chips are not widely available for commercial deployment.
- Many existing devices lack flexibility for future PQC upgrades.

PQC Chip and Hardware Design Takes Time

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

COMMSCOPE®

Key Takeaway

01 Full hardware replacement isn't feasible

02 PQC transition will be phased and incremental

*Need a way to **bring PQC trust into devices that don't yet have PQC hardware***

COMMSCOPE®

Leveraging Symmetric Cryptography for PQC Transition

Symmetric encryption like AES remains secure, even in the post-quantum era

How Symmetric Cryptography Helps:

- ***Protects PQC keys*** – Safeguards PQC keys both at rest and in transit
- ***Leverages Existing Hardware*** – Takes advantage of built-in AES support on many devices, enabling security without new hardware
- **Bridges the Gap** – Offers a practical and secure alternative while waiting for widespread adoption of PQC-ready hardware

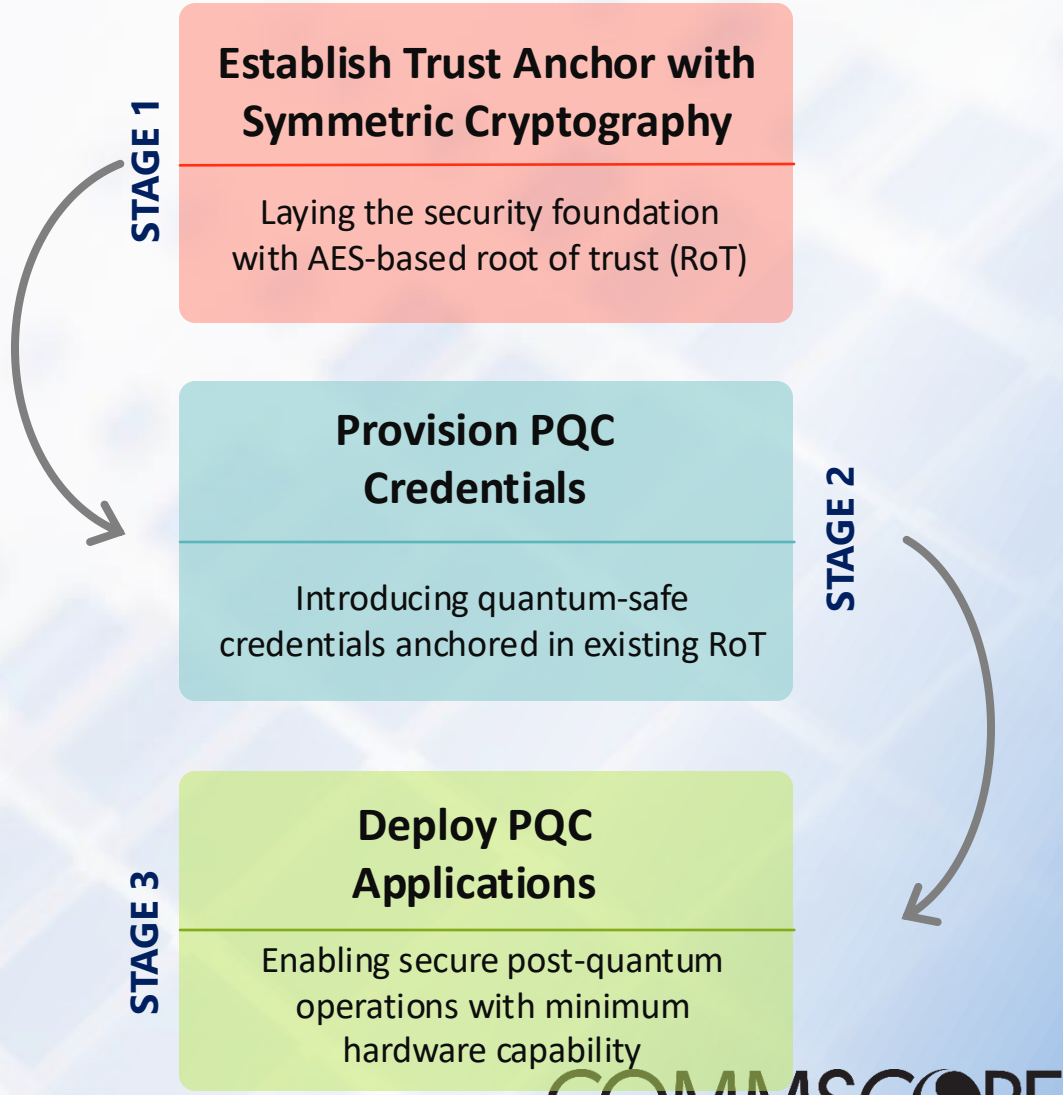
COMMSCOPE®

3-Stage Transition Framework

- Leverage device's built-in hardware AES engine to perform authenticated secure boot.
- 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.
- Using the software to generate PQC credentials on the device; avoiding key exposure.

- Securely distribute and install PQC-enabled applications, leveraging the trusted boot chain.
- Use the PQC credentials on device to enable secure communication and data protection.

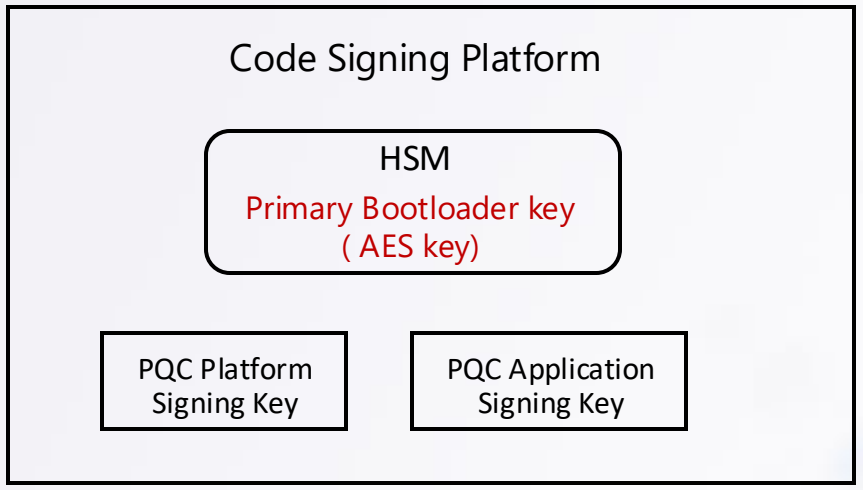


COMMSCOPE®

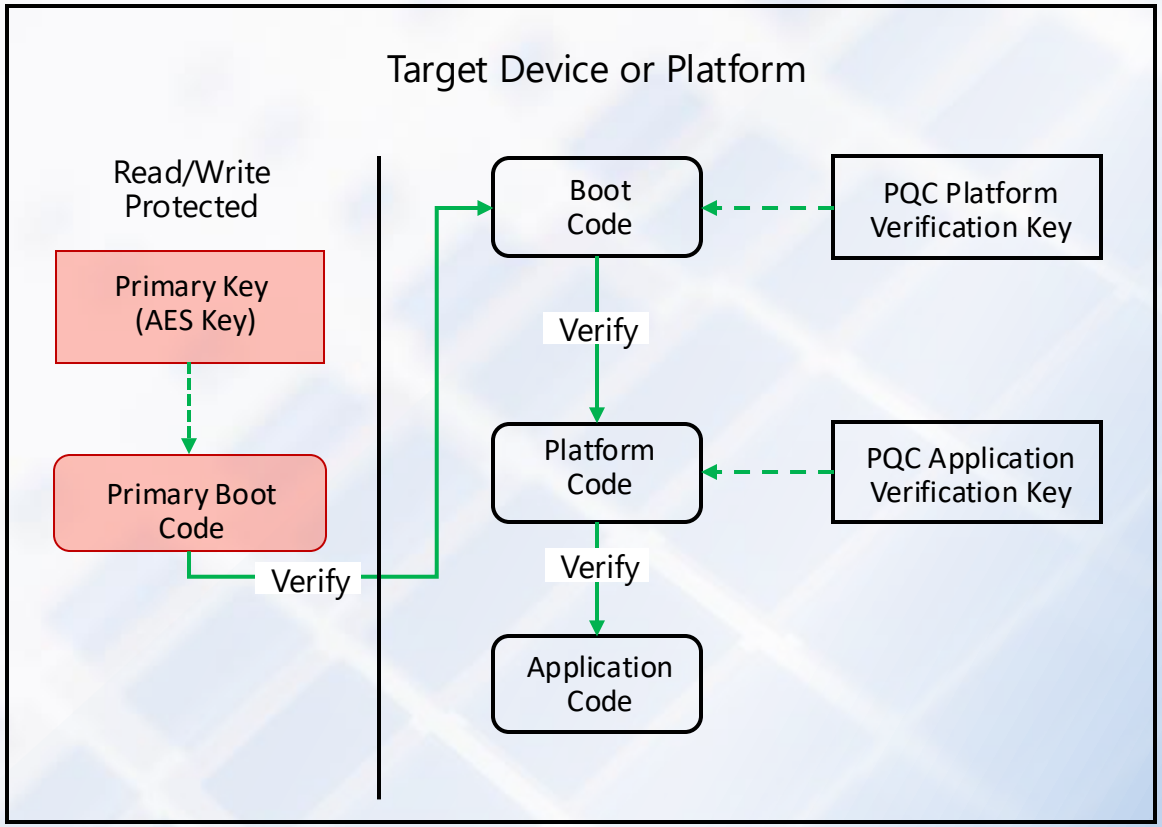
 |

Example: AES-Based RoT for PQC-Based Code Protection

Infrastructure: Signing

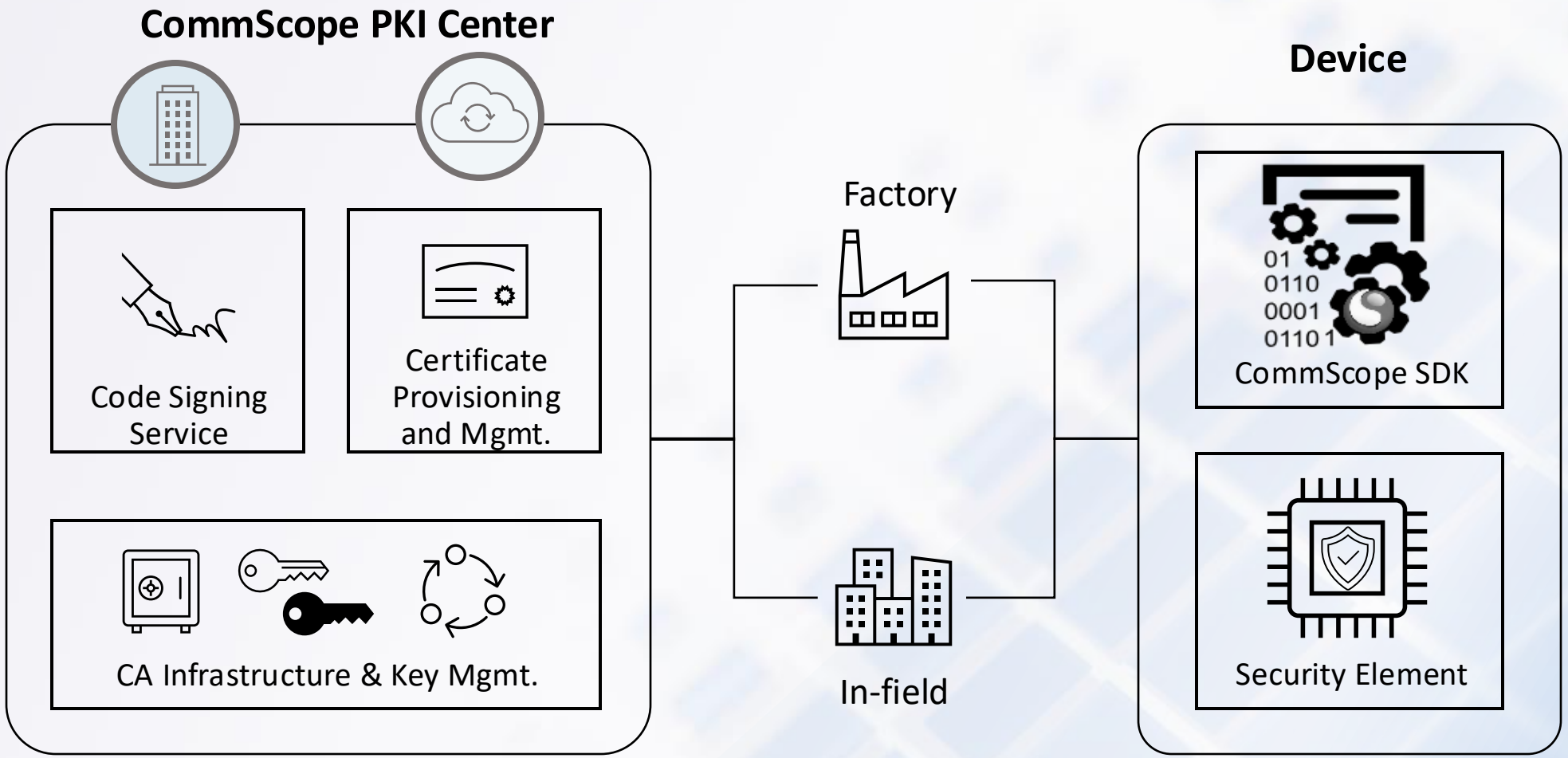


Device: Verifying



 |

Making the Transition Work: PKI Services



How to avoid rewrite: Separate keys/algorithms (PKI) from tools and firmware. Treat PQC as just a new profile.

Current Focus: PQC-based Infra & Application Updates

CommScope PKI

PKI in production for 25+ years. Extensive real-world experience in handling security upgrades

Certificate Authority PQC advancement

PQC Based Code Signing

Close collaborations w/ chip & HSM vendors implementing PQC-based code signing, focusing on secure boot

PQC Code Signing already available; HSM evaluation & testing

PQC Credential Provisioning

Both Factory and in-field provisioning of device credentials for OEMs/ODMs and service providers

PQC device credential provisioning available

COMMSCOPE®

 |

Conclusions

01 **PQC will land first in infrastructure,**

Not in the tiniest devices. Full hardware replacement is not feasible in the short term

02 **Secure Boot is still your trust anchor**

Can be used to deliver PQC securely

03 **Leveraging Symmetric Encryption**

Enables secure bootstrapping using existing hardware capability

Q&A

xin.qiu@commscope.com

PKI-center.com