COMMSCOPE®

ICMC25

Practical Framework for Transitioning to PQC

Balancing Security and Hardware Constraints

April 10, 2025

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

Presenter: Xin Qiu

CommScope PKI Center™ www.pki-center.com

Agenda

Introduction

Key Considerations to PQC Adoption

3-Stage Transition Framework for Gradual PQC Adoption

Details on Secure Boot & Device Credential Provisioning

Conclusions

 |

Why PQC Transition Is Critical Now?

Past cryptographic migrations took years

Unprecedented scope

Balancing adaptability and stability

 |

ICMC25

Key considerations

Device Lifecycle & Cost

Long Device Lifespans

IoT and embedded systems often 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.

COMMSCOPE®

ICMC25

Hardware Constraints

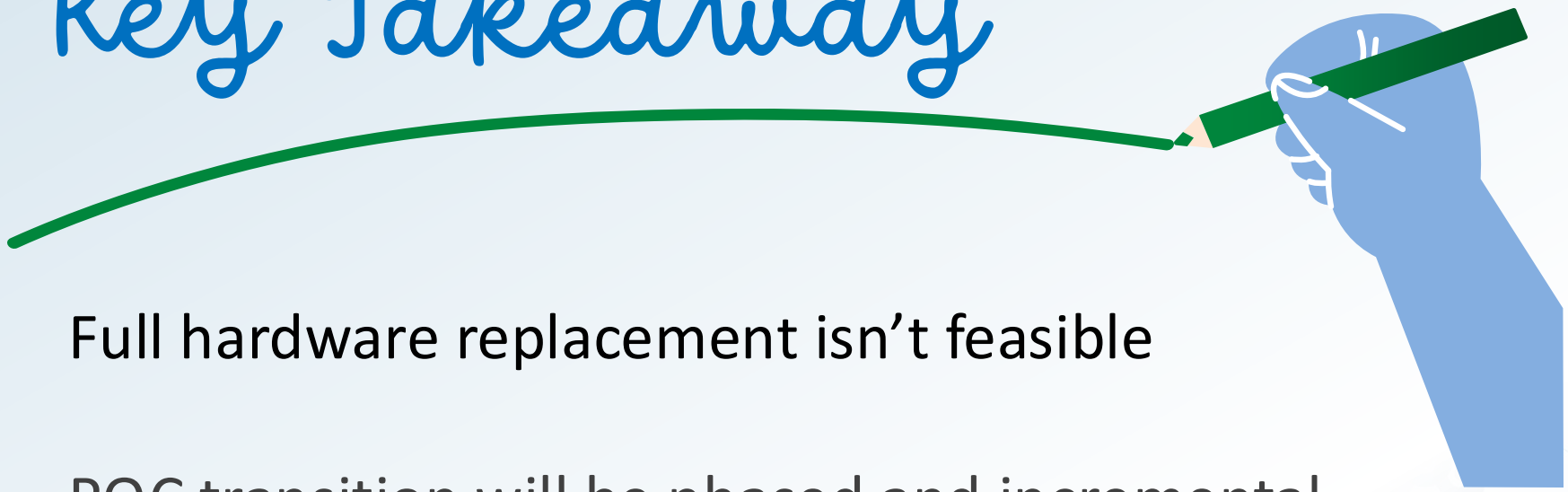
Limited Availability of PQC-Ready Hardware

- 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

Key Takeaway



Full hardware replacement isn’t feasible

PQC transition will be phased and incremental

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®

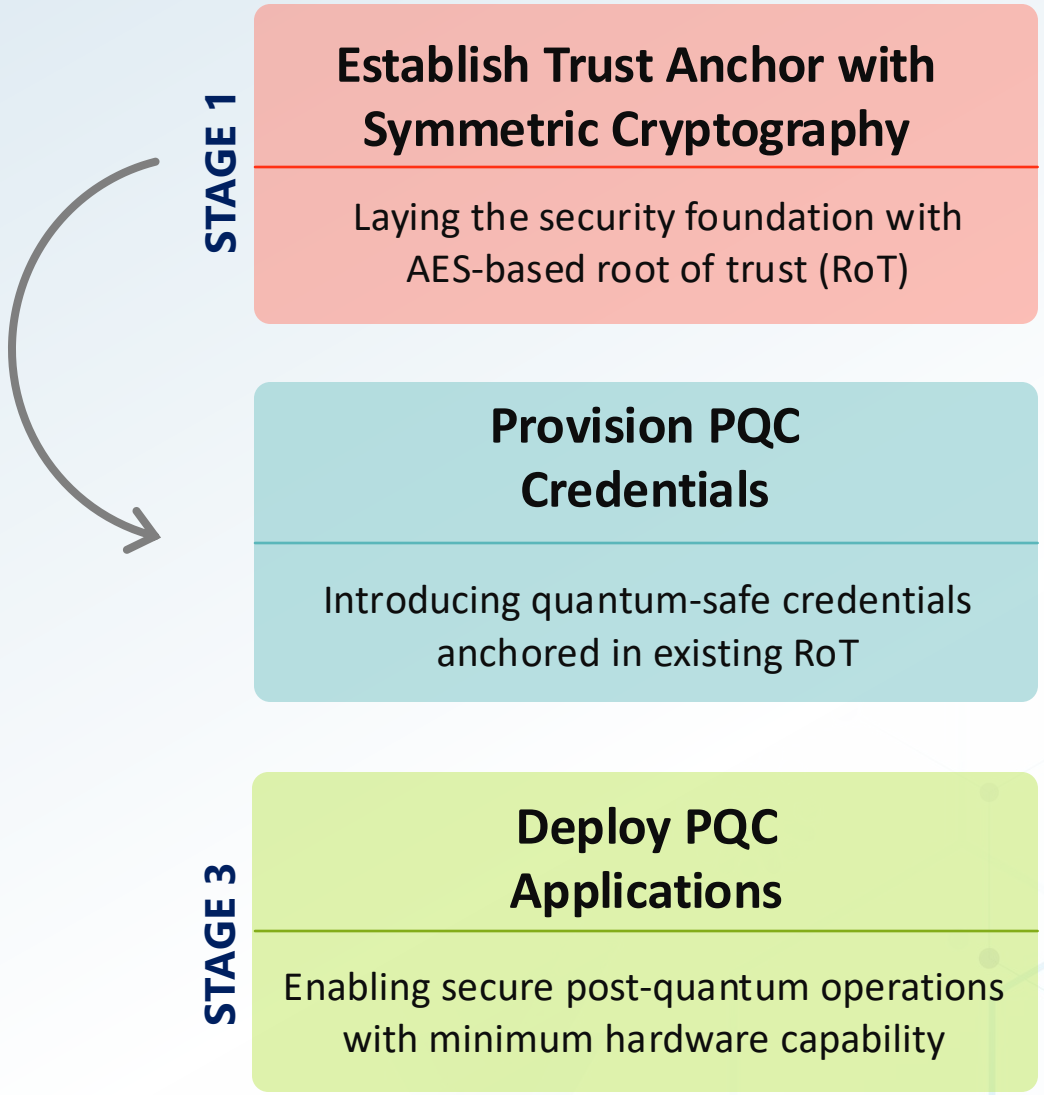
ICMC25

3-Stage Transition Framework

- Leverage device's built-in hardware AES engine to perform authenticated secure boot.
- Store a 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.

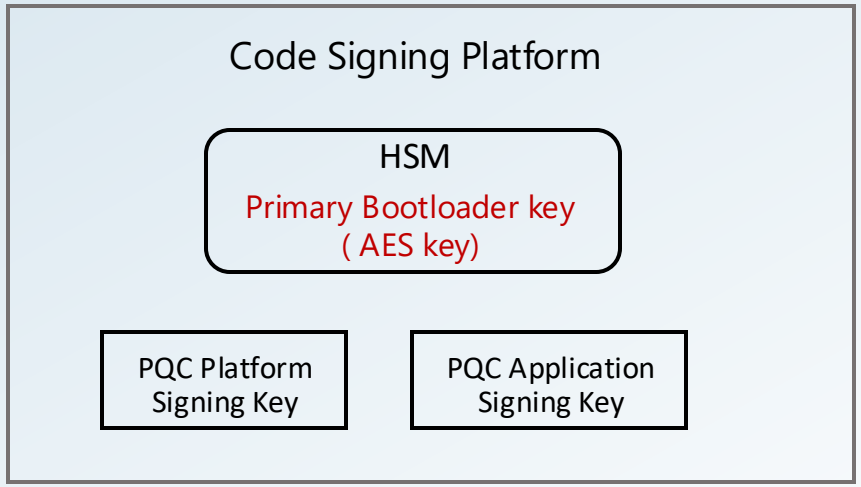


COMMSCOPE®

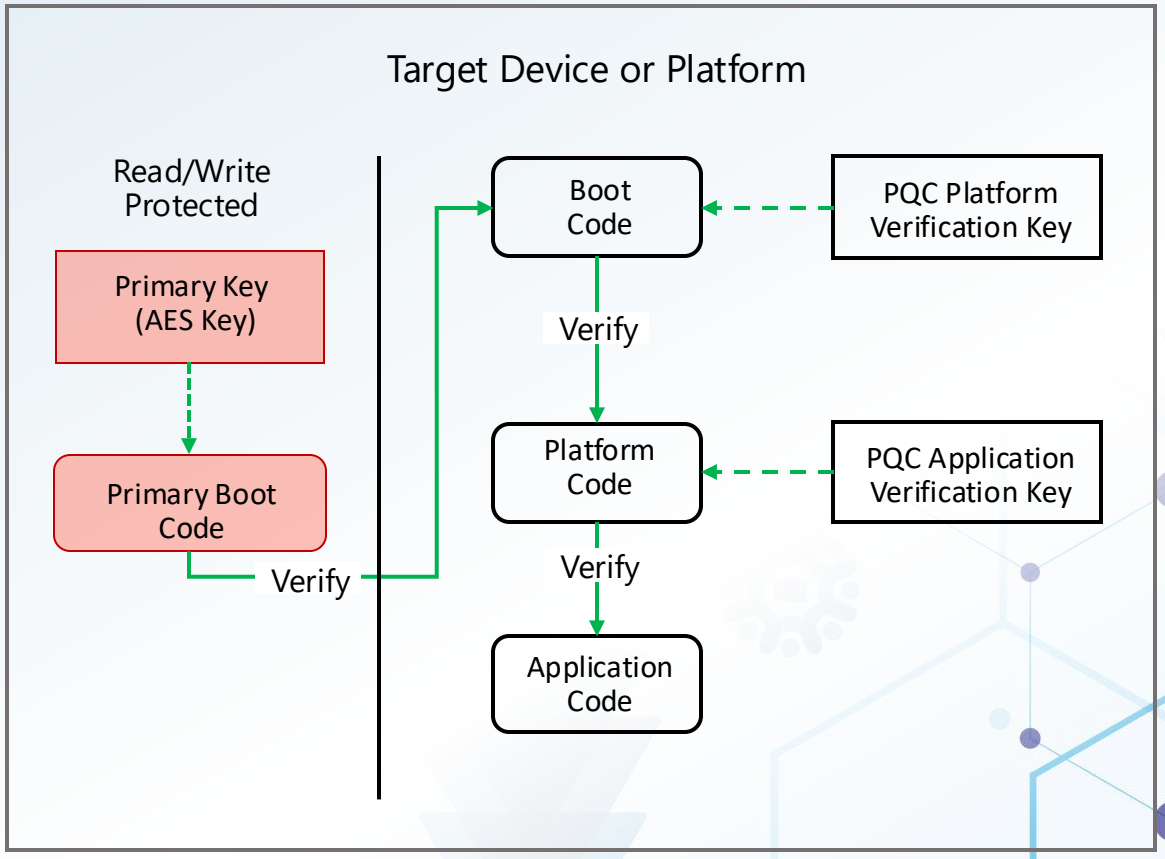
ICMC25

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

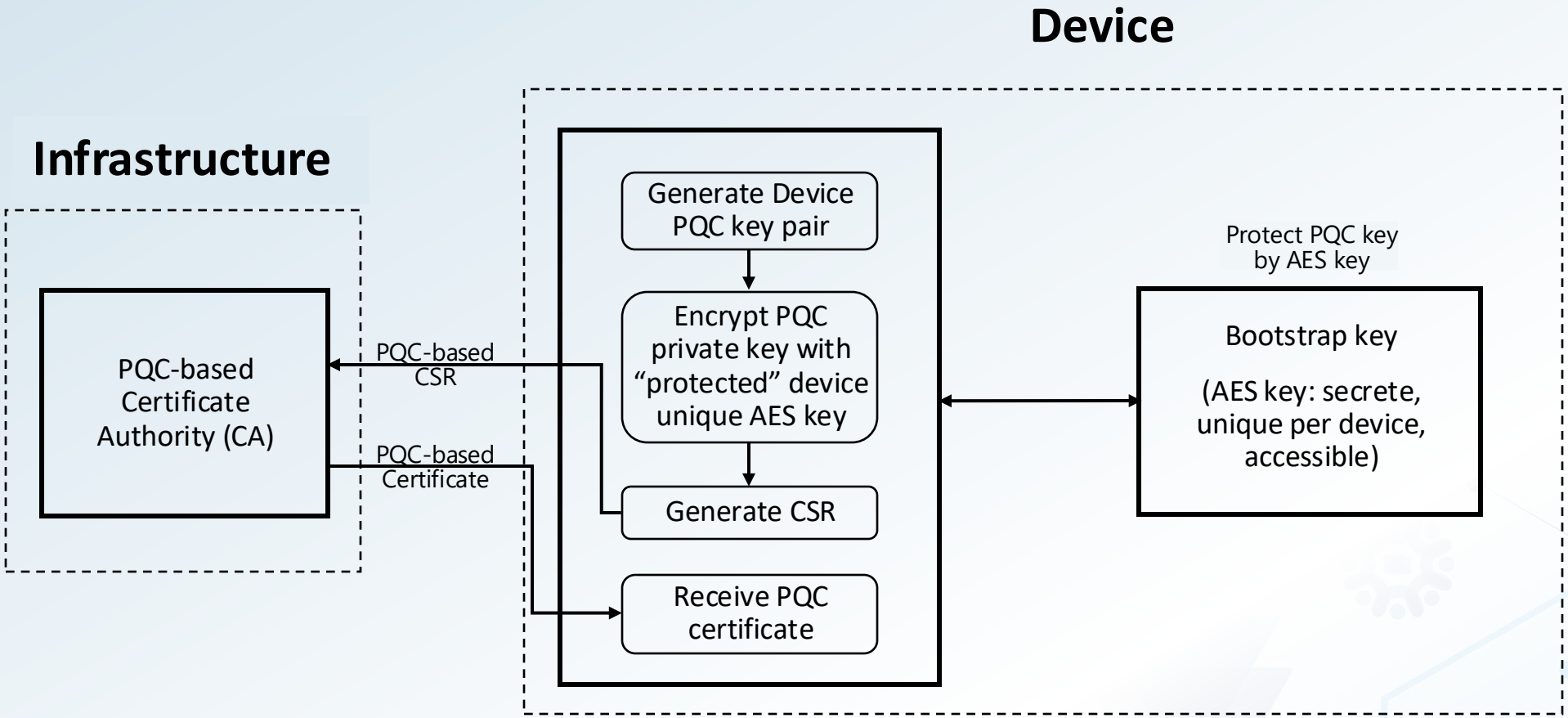
Infrastructure: Signing



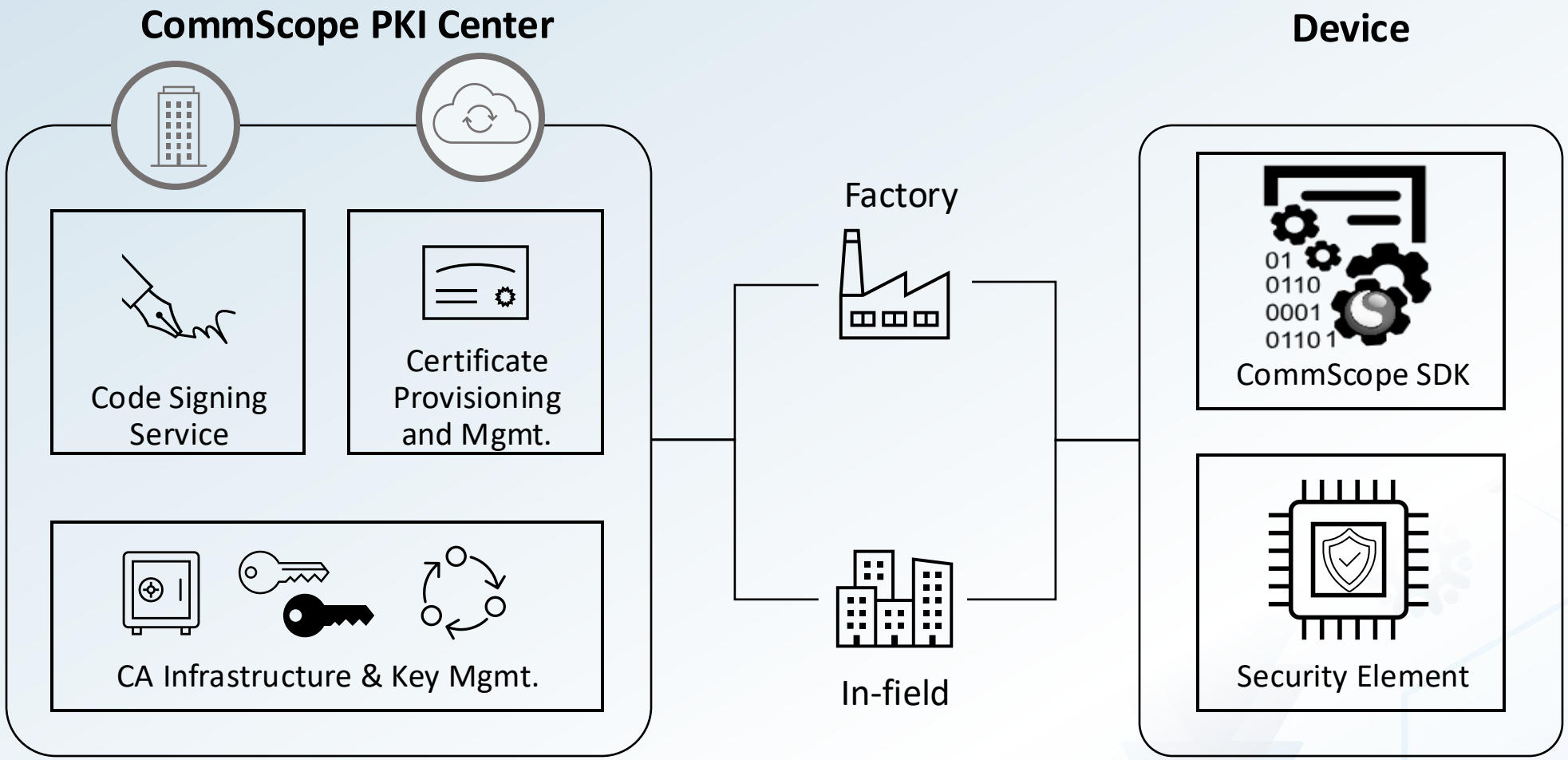
Device: Verifying



AES Protected PQC-Based Credentials Provisioning



Making the Transition Work: CommScope's PKI Services



Current Focus: PQC-based Infra & Application Updates

CommScope PKI

Scalable, Secure Robust 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 coming soon

COMMSCOPE®

ICMC25

Conclusions

Transitioning to PQC is essential to defend against future quantum threats

01 **Hardware Replacement Challenges**
Full hardware replacement is not feasible in the short term

02 **Practical Migration Strategy**
A three-stage migration framework provides a realistic transition path

03 **Leveraging Symmetric Encryption**
Enables secure bootstrapping using existing hardware capability

04 **Balancing Security & Practicality**
A strategic approach is needed to ensure both security and feasibility

COMMSCOPE®

ICMC25

THANK YOU

Contact: xin.qiu@commscope.com

Website: PKI-center.com