Securing Device Credential Provisioning

Matter and the Wider IoT Ecosystem

Presenter: Xin Qiu | Aurora Networks™

Authors: Oscar Jiang, Jason Pasion, Xin Qiu, Lisa Yin

PKI Center™ www.pki-center.com

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

- Device credential and trust in Matter and IoT
- Manufacturing risks in credential provisioning
- Architectural shift: device-generated keys
- Scalable provisioning workflows for production
- Case study: Matter DAC provisioning on STM32WBA6
- Key lessons

Securing Device Credential Provisioning: Why It Is Important

Unique device credentials establish digital trust

- Unique IDs, keys, and certificates serve as each device's trusted identity
- Enable authentication, authorization, and secure communications

Driven by global security standards

- CSA Matter, NIST, ENISA, and emerging IoT trust-label programs

Secure elements alone are not sufficient

- Hardware protection cannot compensate for a weak provisioning workflow

Device Credentials in CSA Matter Ecosystem

Key terms

DAC: Device Attestation Credential
NOC: Node Operational Credential

Device Makers are responsible for provisioning DACs during manufacturing

Factory (provisioning Facility)

Store

Distribute devices to end users

Device Maker

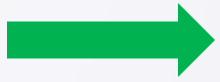
Provision device with DAC

Tablet or Smart Phone

In-home

Consumers install devices

Devices are commissioned using DAC and then operated using NOC



(Secured) On-going IoT Operations

Consumers commission devices into home networks

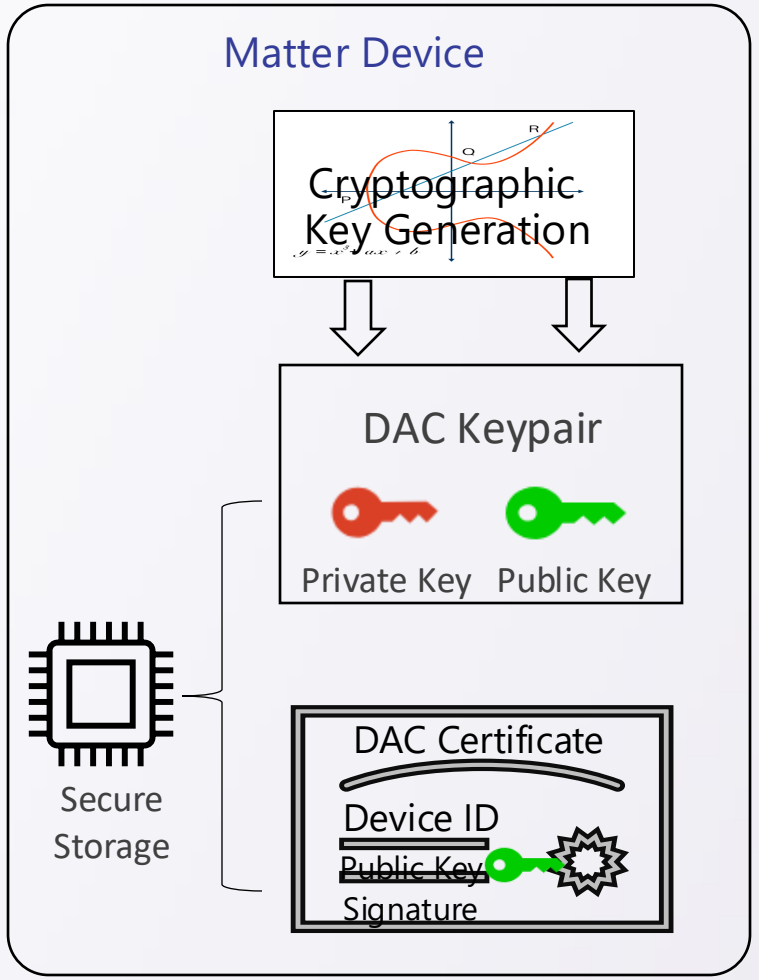
Matter Raised Security Bar on Device Credentials

Matter requires *unique* credential (DAC) for each device

DAC consists of a public & private key pair, together with associated certificate

Each DAC private key should be kept in the device *secure storage*

Anti-cloning & anti-duplication are essential



Manufacturing-Time Credential Defines Lifetime Security

Device trust starts at manufacturing

- Each device receives a unique and verifiable "**birth certificate**"
- Shared credentials create systemic risk

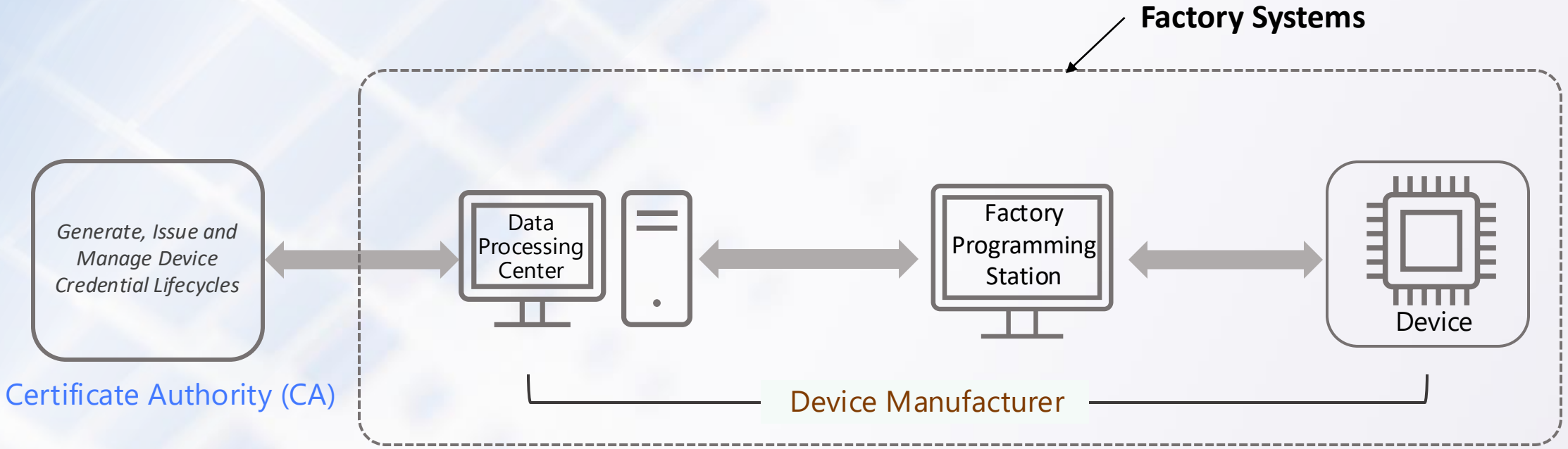
Manufacturing is the most common point of failure

- One device credential can be inadvertently loaded or cloned across multiple devices
- A single factory breach can lead to larger-scale compromise
- Credential compromise is silent and rarely cause functional failure

Post-deployment fixes is extremely costly

- Loss of the trust anchor breaks the ability for authenticated updates
- Secure recovery requires expensive infrastructure and tightly controlled update mechanisms

A Typical Manufacturing Environment

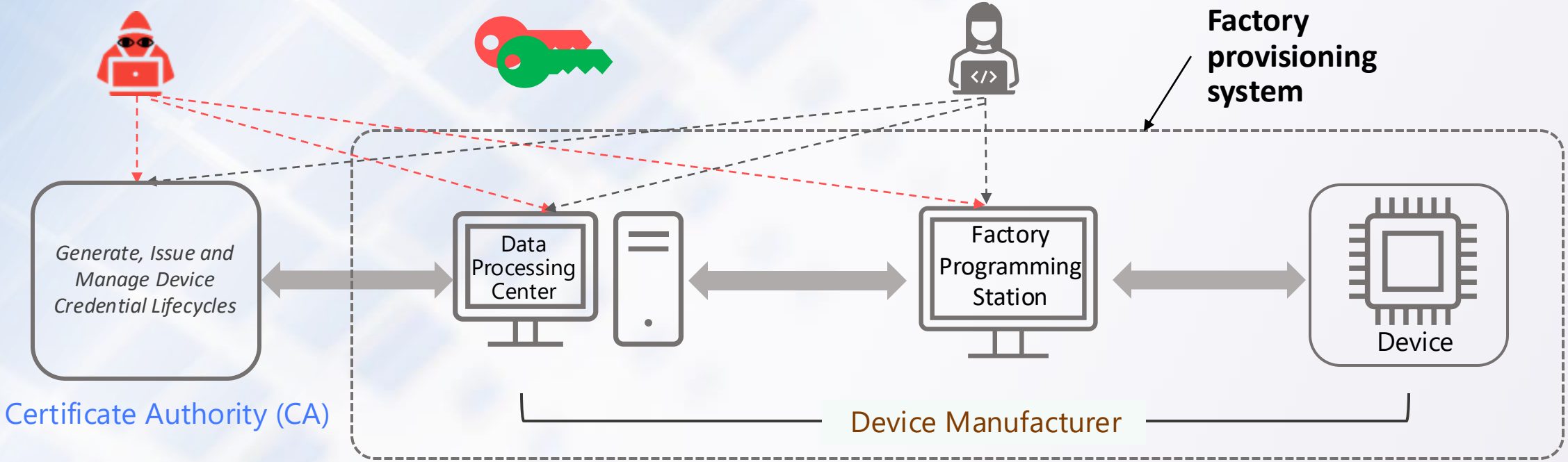


Credential provisioning involves two trust boundaries:

- Certificate Authority (CA)
- Device manufacturer

Factory provisioning systems involves multiple sub systems

Security Risks in Manufacturing Environment



If key pairs are generated outside of the devices:

- The attack surface significantly expands
- The risk of unintentional operational mistakes increases

➔ Manufacturing environments expose credentials → creates systemic risk such as **key duplication or cloning**

Architectural Shift: Generate Keys Inside the Device

Instead of injecting credentials, devices should generate their own credentials internally

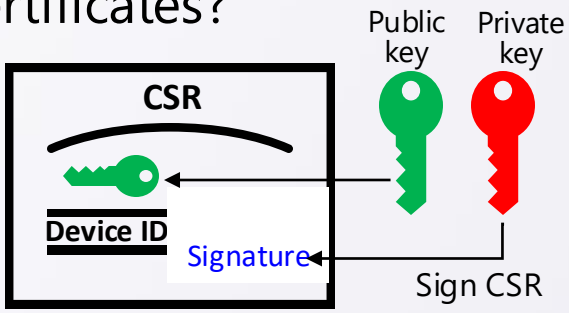
- Private keys never leave the device boundary
- Manufacturing systems handle only public data and certificate issuance
- Eliminates bulk credential exposure risk during production

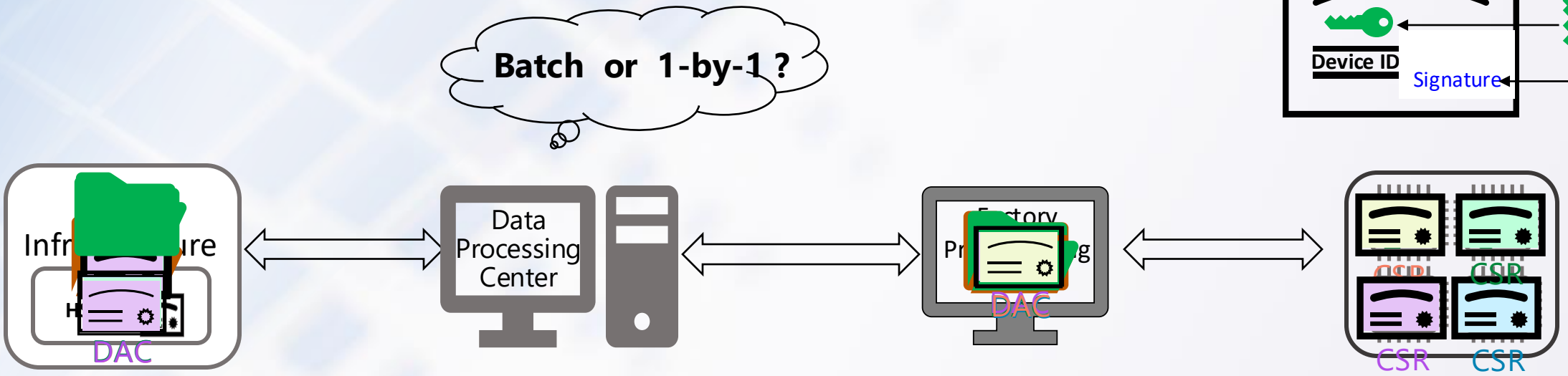
This fundamentally changes credential provisioning from key injection to secure certificate binding

Production Complexity – An Illustrative Question

Once key pairs are generated inside devices, how to obtain the matching certificates?

key pair -> [Certificate Signing Request: CSR] -> certificate





Batching CSRs is a multi-step operation,
impacting production efficiency and increasing error rate

1-by-1 CSRs is much more production friendly

Production Considerations at Scale

Scalability & Operations

- Multi-OEM / multi-site / multi-SKU
- No site-specific exceptions
- Fully automated credential handling

Reliability

- Hidden failures engineered out
- No ad-hoc tools or scripts
- Deterministic, repeatable flows

Traceability

- End-to-end credential traceability
- Audit trail for response & compliance

Signing Infrastructure & Connectivity

- On-prem signing for factory autonomy
- Periodic connectivity revocation & lifecycle management
- Factory-level yield and anomaly visibility

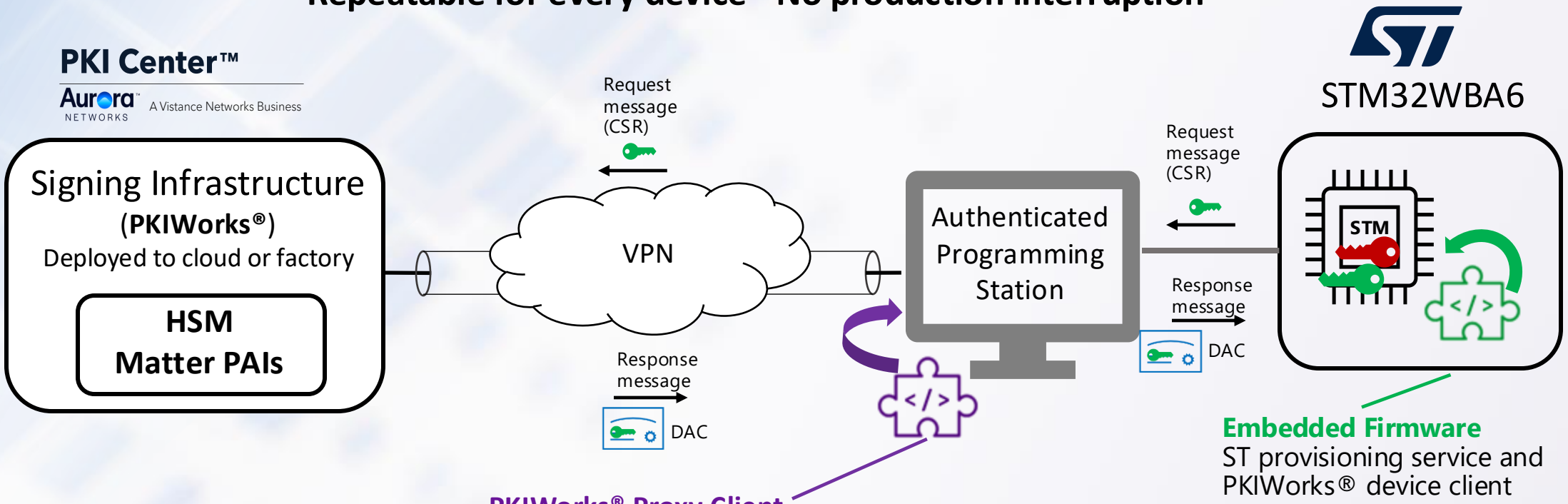
Security

- Bound to hardware-based root of trust
- Authenticated programming stations
- Secure rework / retry / scrap
- Network-level security and monitoring

Case Study Context: Matter DAC Provisioning on STM32WBA6

Zero-touch Streamlined Production Process

Repeatable for every device - No production interruption



- STM32WBA6 enables secure, on-device key generation.
- Representative of modern IoT MCUs.
- Demonstrates provisioning workflow on a real device.

Beyond Matter: Applicability Across the IoT Ecosystem

Reusable architecture and provisioning model

- Common architecture across device makers, products and sites
- Provisioning reused across Matter and other ecosystems
- Simple to adopt, enabling faster production launch

Matter acts as a catalyst, not an exception

- Consistency across ecosystems
- Higher expectations for security and production efficiency

Key Takeaways

- Credential provisioning is fundamentally a manufacturing security problem.
- Centralized key generation does not scale safely in high-volume environments.
- Device-generated keys significantly reduce both attack surface and human error.
- Matter is one concrete example, but the same approach applies to all device credential provisioning.
- Getting provisioning right early prevents irreversible trust failures later.

THANK YOU!

Q&A

xin.qiu@auroranetworks.com

PKI-center.com