COMMSCOPE®

embeddedworld Exhibition&Conference North America

Hardening Credential Provisioning in the Supply Chain

A Multi-Layer PKI Architecture for Embedded Device

November 5, 2025

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

Presenter: Xin Qiu

CommScope PKI Center™: *www.pki-center.com*

Agenda

Why secure credential provisioning matters

Manufacturing challenges in keeping device identities unique

An end-to-end, multi-layer PKI approach

COMMSCOPE®

Securing Device Credential Provisioning: Why It Matters

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

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

Secure elements alone aren't enough

- Hardware protection can't compensate for a weak provisioning pipeline

The Core Problem: Keeping 'Unique Identity' Unique

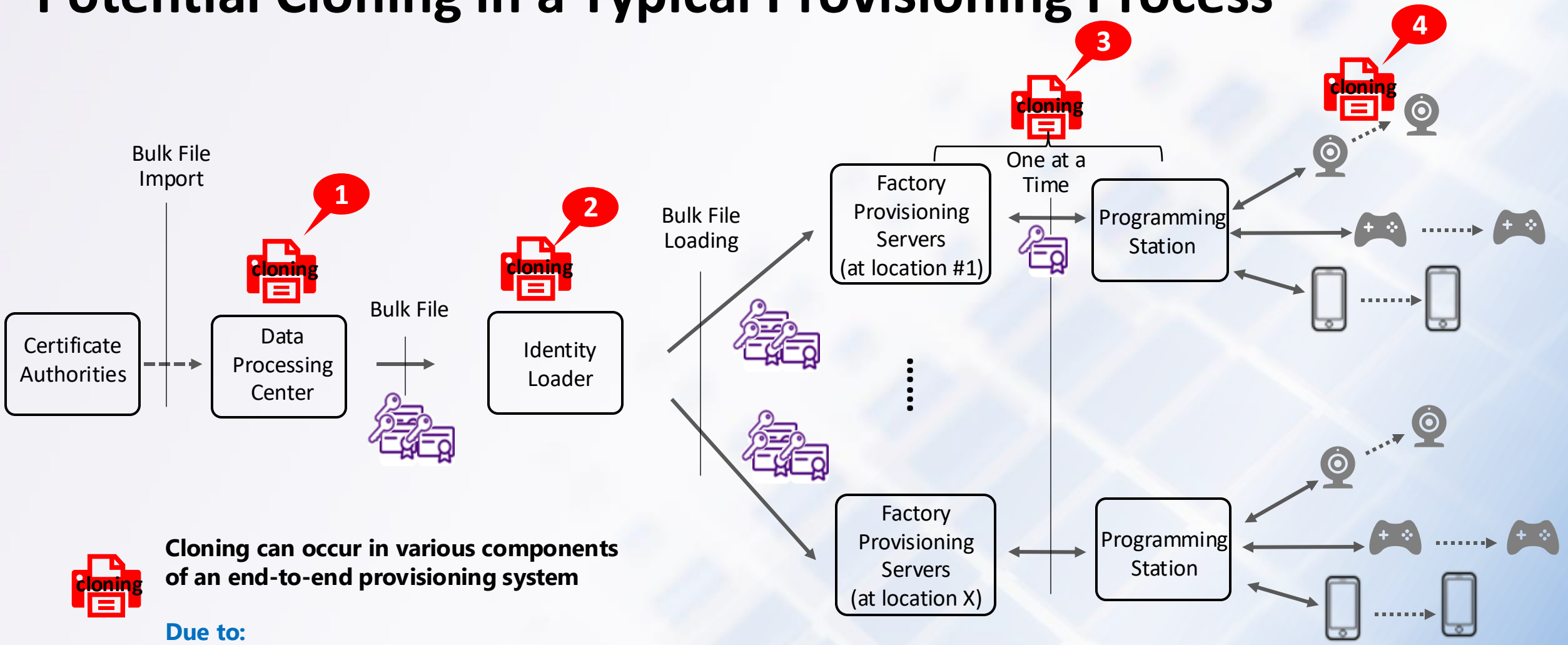
Challenge:

- Identity management is fundamentally different from managing electronic components
- A single identity can be inadvertently loaded onto multiple devices
- Cyber criminals target factories — credential theft = mass cloning

Where it breaks down – supply chain has a long path

- Central data center: generates identity data
- Identity loader- distributes data to factory sites
- Factory systems - provisioning server → programming station → device

Potential Cloning in a Typical Provisioning Process



cloning

Cloning can occur in various components of an end-to-end provisioning system

Due to:

- **Operational errors; or**
- **Security breaches**

COMMSCOPE®

An End-to-End Multi-Layer PKI Architecture

Defense-in-depth:

- need an end-to-end approach to combat volume cloning throughout the system as the workflow is being executed
- security layers that protect and validate each other

System components:

1. Root of trust - certificate authority and data processing center
2. File transfer and factory boundaries
3. Provisioning server and programming station
4. Device side

COMMSCOPE®

1: (Certificate Authority) and Data Processing Center

HSM is the trust anchor

- Makes sensitive keys extractable
- Restricts access & prevents bulk export of private keys

Anti-duplication controls

- Hash records to detect file or database record reuse
- Automatic 'next-available ID' assignment to avoid human error

Two-layer encryption

- Inner layer: per-device AES key or class key for device group
- Outer layer: provisioning-server-specific key before export

2: Securing Transfer and Factory Boundaries

Encrypted identity files only usable by intended factory server

Identity Loader checks before loading

- File hash already used? → reject
- Device IDs already in database? → reject

Provisioning Server creates matching identity objects in HSM

- Database records unusable without matching HSM object

Effect: an offline or stolen file cannot re-provision devices

3: Factory Interface Hardening

Authenticate every Programming Station

- TLS link + cryptographic token bound to station fingerprint
- Server whitelist, enforced by HSM, for authorization

Per-session protection

- Diffie–Hellman key exchange for each provisioning session
- Prevents interception or replay of device keys

Audit logs for traceability

- All requests traceable to factory location, station ID and device

4: Device-Side Protections

Inner AES key binding

- Copied keys won’t decrypt on another device

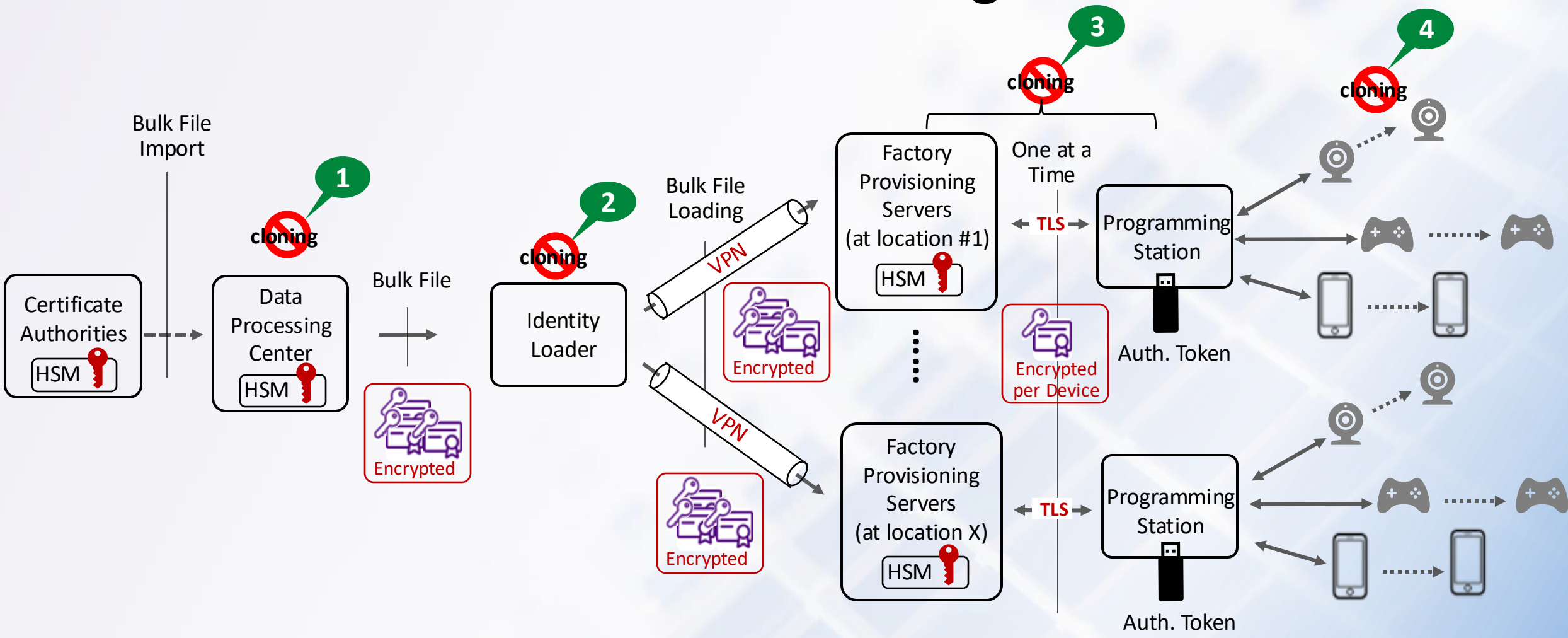
Keys stored securely inside device

- Secure element, TEE, SOC/MCU with built-in security, etc.

Secure boot verifies the code for decryption and injection

- Prevents tampering with provisioning logic

End-to-end Protection in Provisioning Process



 |

Key Takeaways

Credentials are the core of device trust

Provisioning is the weakest link if left unhardened

Multi-layer PKI architecture

- HSM root + layered encryption + crypto tokens + secure boot
- Survives partial breaches and human errors

Future-ready and compliant with global standards

COMMSCOPE®

Q & A

Xin Qiu | CommScope PKI Center

www.pki-center.com | xin.qiu@commscope.com