# Secure Device Provisioning

How to fulfill PCI PIN – guidelines for a practical solution

PCI Security Standards Council®

# Torben Ellgaard

Product Manager for Cryptera A/S

CRYPTERA®

# Speaker Background

## 25 years of secure payment experience

- Product manager with Cryptera handling EPPs and POS devices for 25 years
- Part of Cryptera security management and key handling team
- Cryptera is a Danish company located near Copenhagen
- The company - now known as Cryptera - has manufactured EPPs since 1984!
- Current products are secure devices (EPPs, SCRs and NFC readers) and key management solutions for other device manufacturers
- Cryptera maintains a secure provisioning facility fulfilling PCI PIN requirements

# Agenda

This presentation will cover

- Scope of PCI PIN Security requirements
- Setting up a provisioning facility
- Establishing secure areas
- Device provisioning in practice
- User roles – administrative, operational and supervisory
- Key operations: generation, import/export, key binding, certificates
- Audits and certification

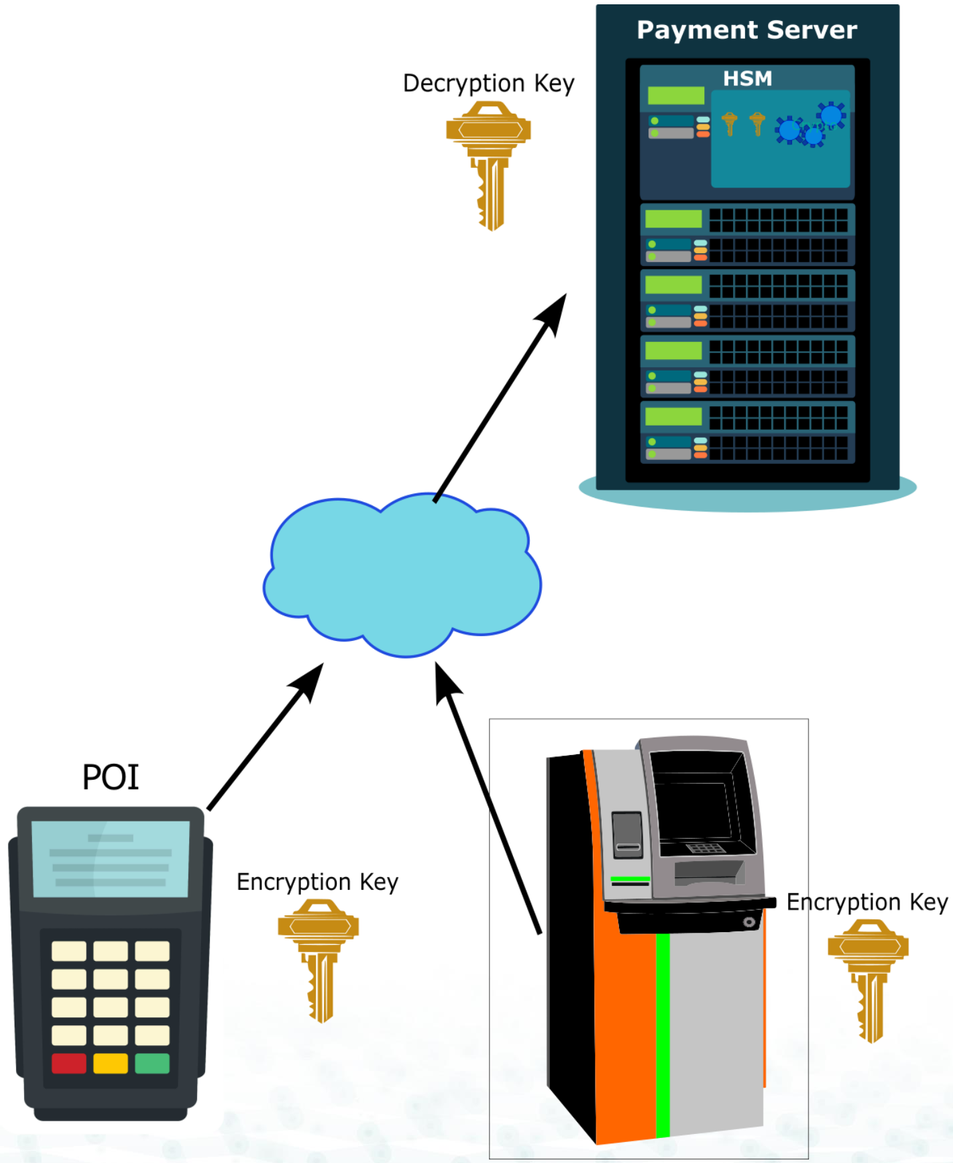
# Starting with the basics

## Handling PIN transactions

- Some payment transactions will require entry of cardholder PIN
- POI devices are designed to protect the PIN
- It is common knowledge that PINs are protected through encryption

**But what has been done to establish the keys?**

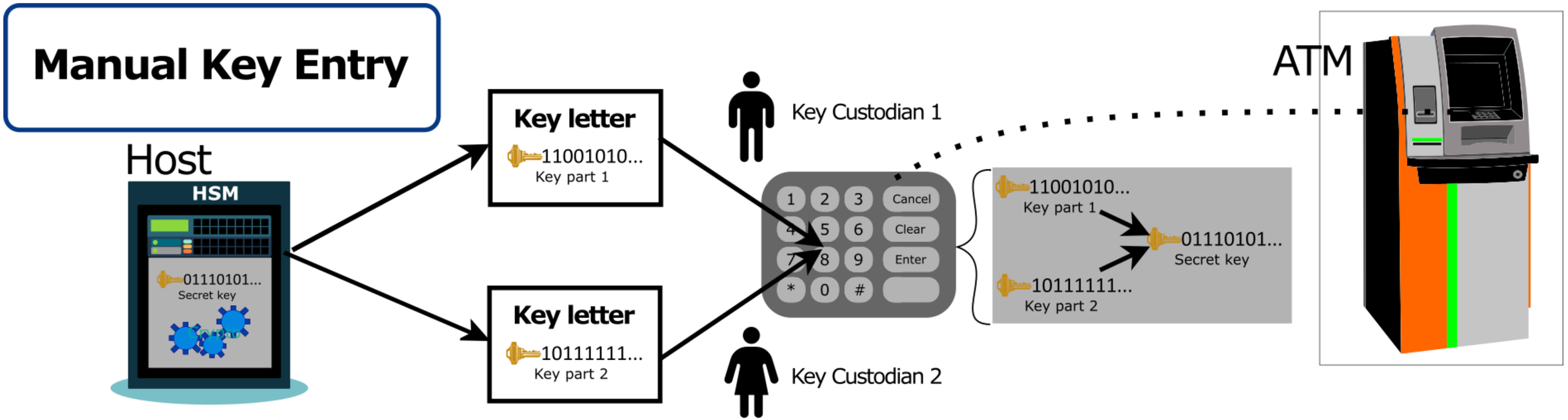
# Let’s dig deeper!




PCI Security Standards Council

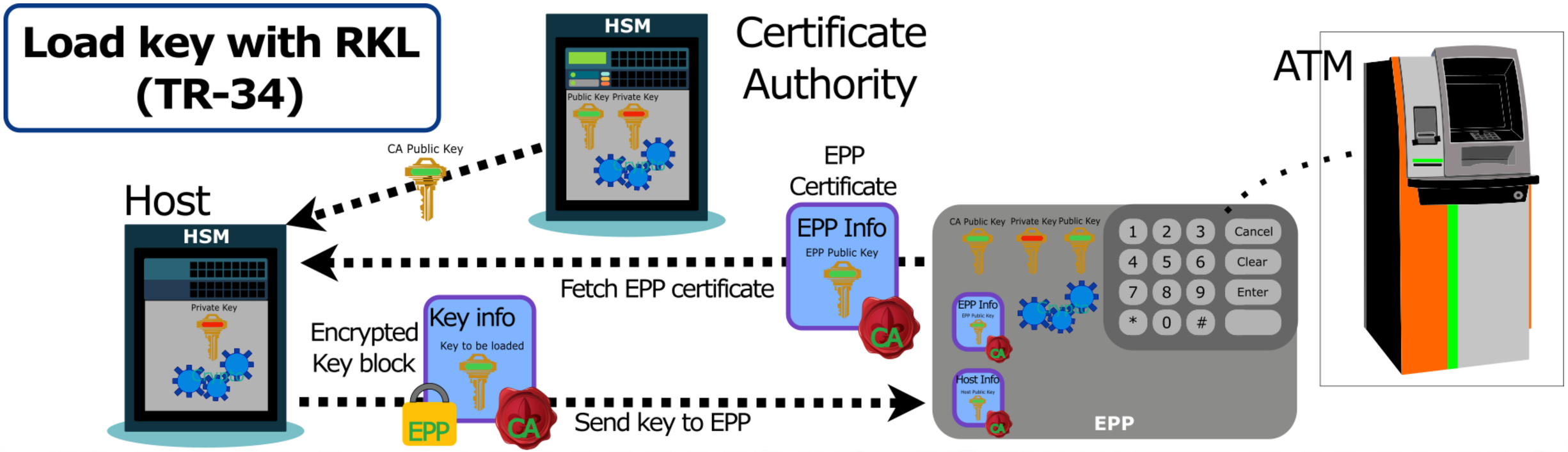
# Key Injection - Manual Key Entry

Linking the POI to an acquirer



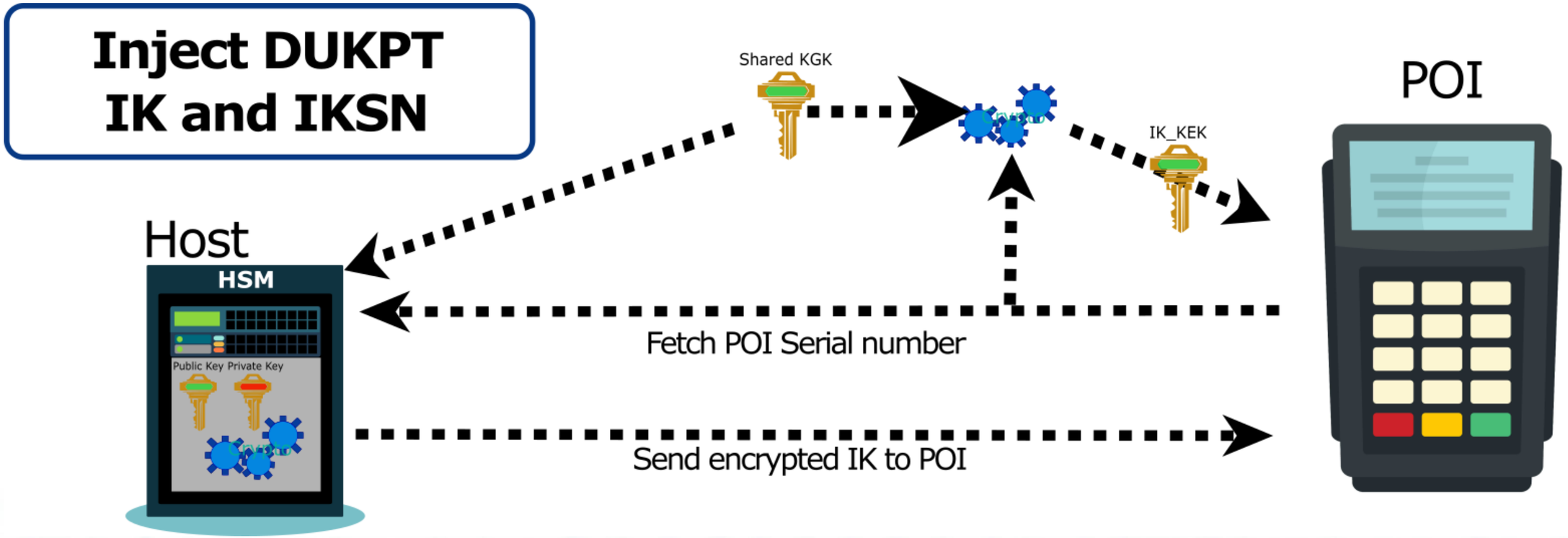
# Key Injection – Remote Key Load

Linking the POI to an acquirer



# Key Injection – DUKPT Key Injection

Linking the POI to an acquirer

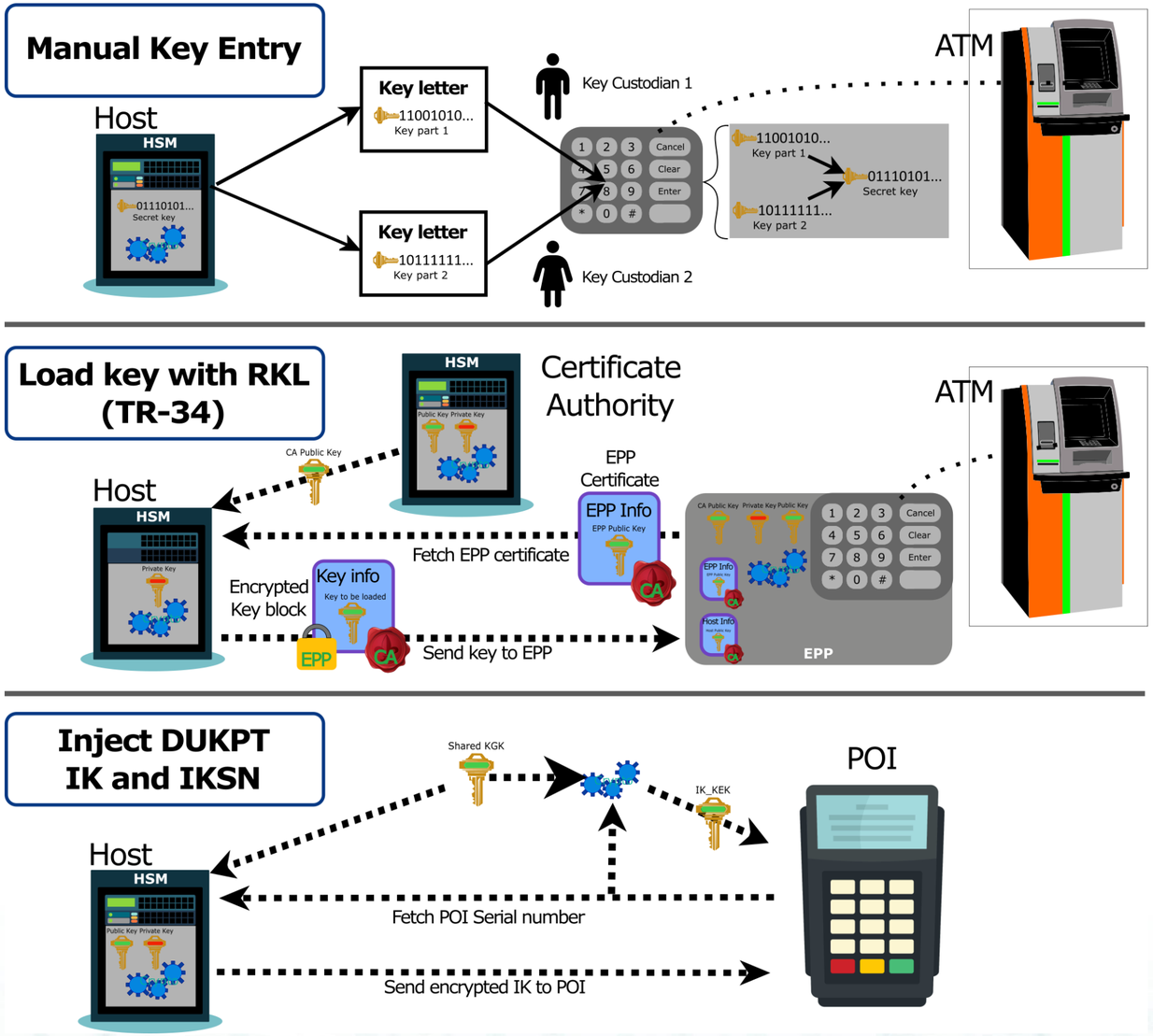


# Key Injection - Summary

## Linking the POI to an acquirer

**Inject keys to link the POI to a specific payment system**

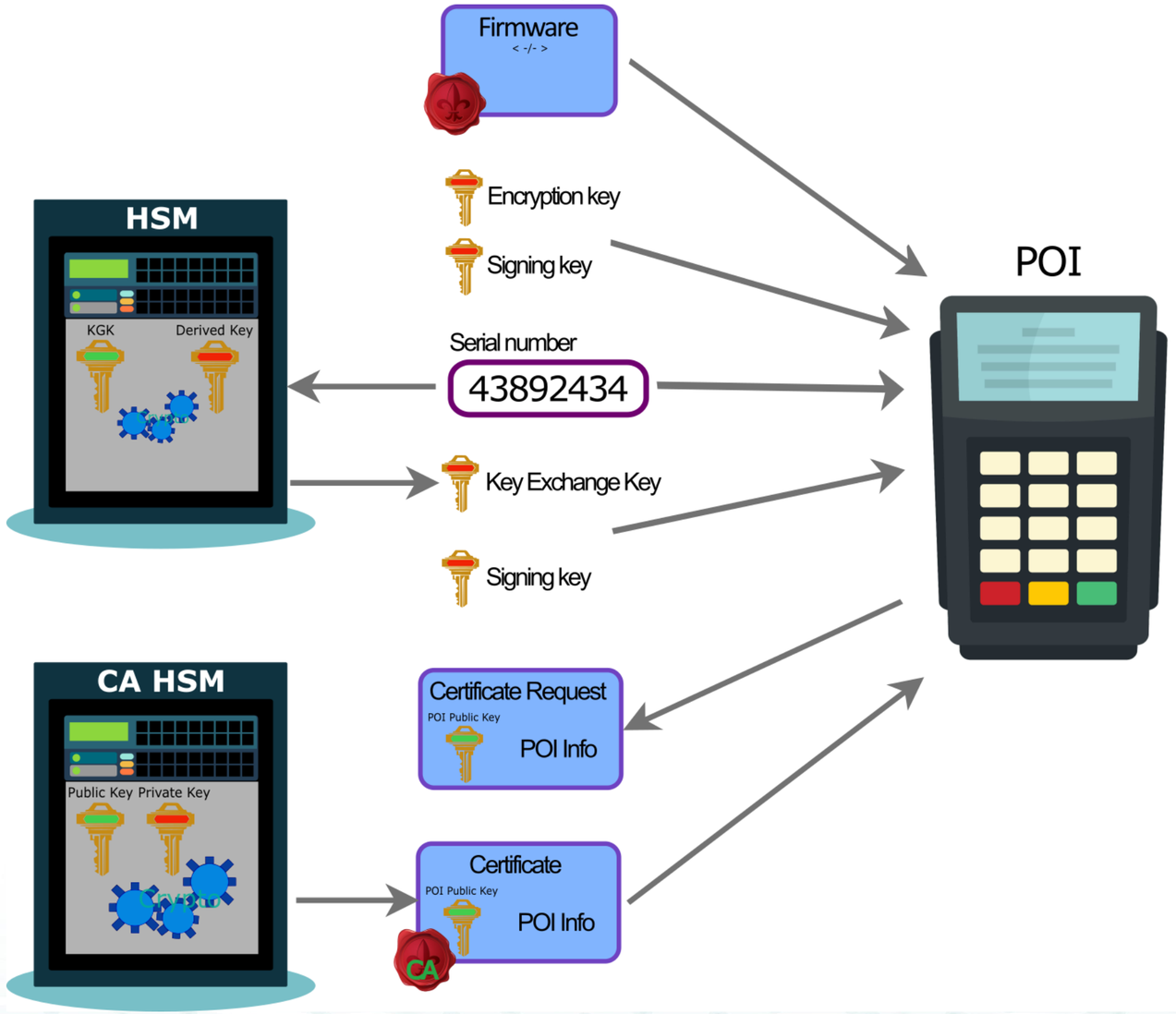
- For ATMs this is typically a Master Key/Session Key concept
- The Master Key is loaded through Manual Key Entry or Remote Key Loading (TR-34)
- The Session Key is loaded in operation through TR-31 key blocks
- For retail POIs it is common to inject a DUKPT Initial Key and related IKSN



# Device provisioning – Serial number and first keys

Giving the ”new born” POI an identity

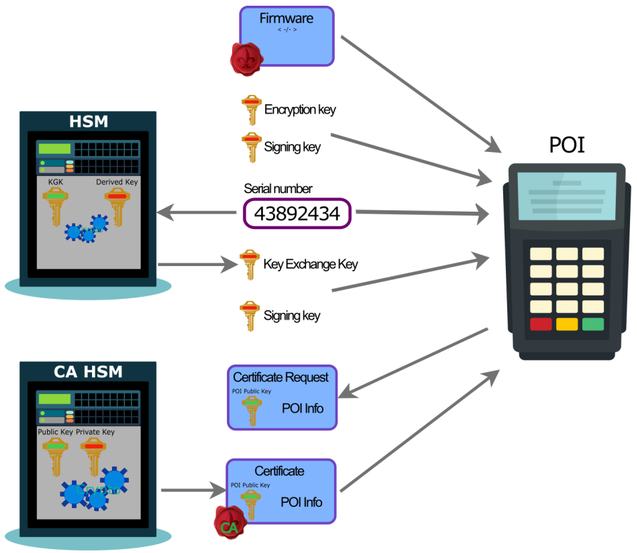
- A ”new born” POI device is sensitive!
- It needs a cryptographic setup to protect its integrity
- The boot stack is secured from the root in the MCU
- Software applications and keys are loaded
- Additional keys for the future Key Injection may be loaded



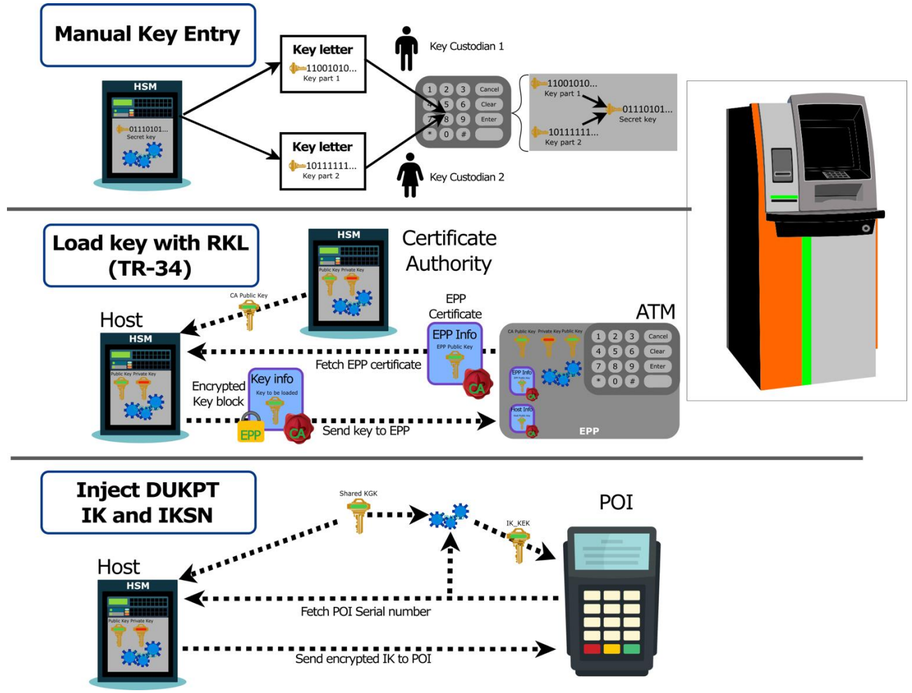
# Scope of PCI PIN

Global protection of PIN and PIN keys

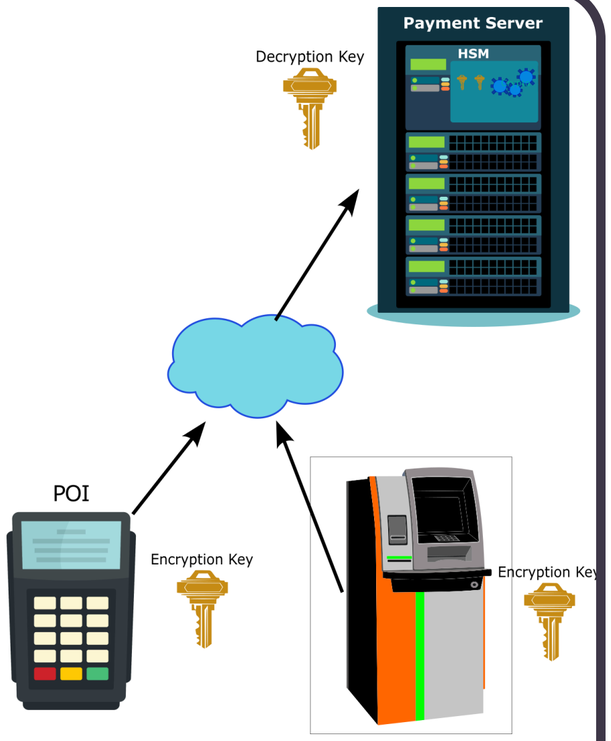
PCI PIN Security




Provisioning




Key Injection




Operation

# Creating a Provisioning Facility

## Applying PCI PIN in practice

The implementation will depend on:

- Existing processes
- Volume of POIs
- Key owners
- Payment processor rules
- Etc....

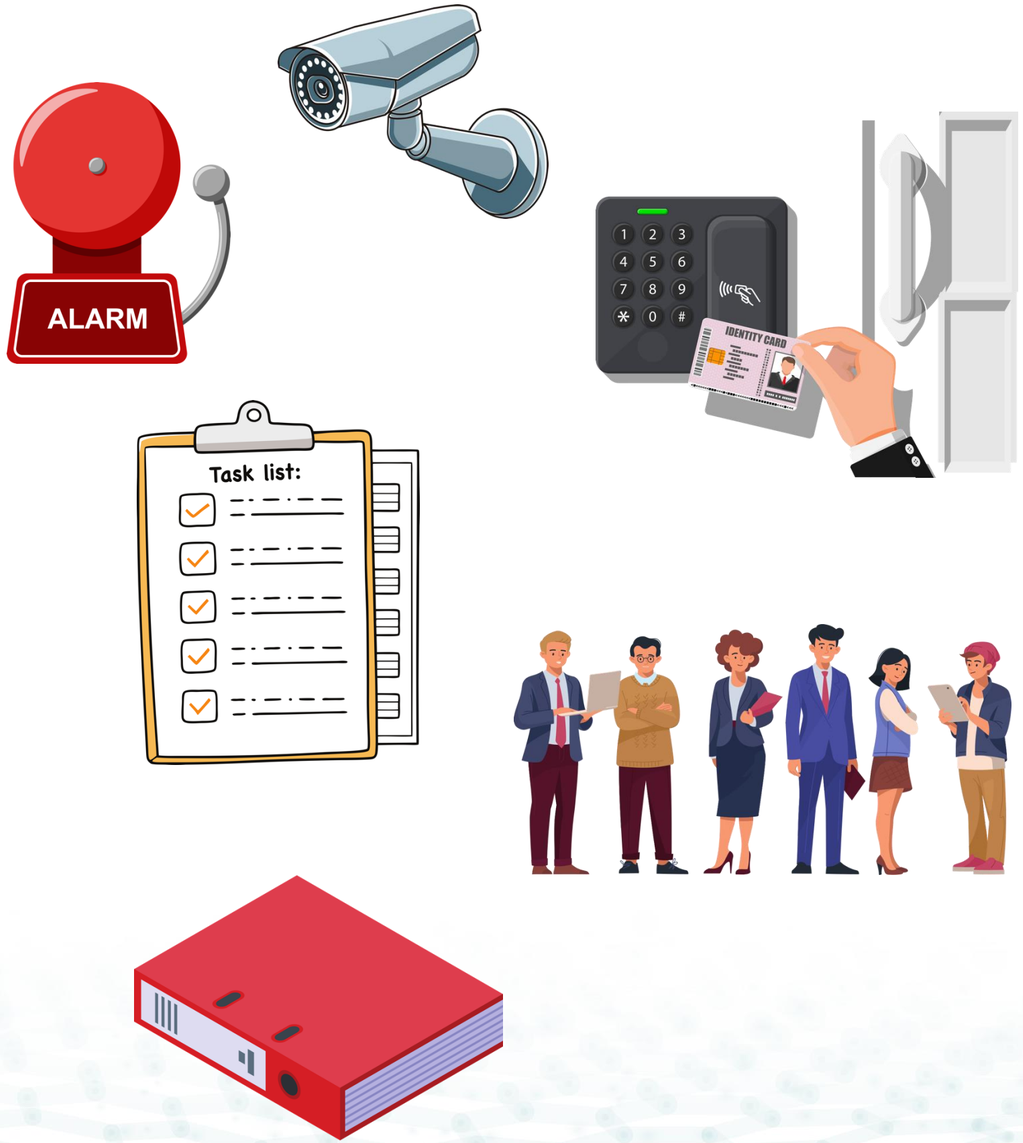
**The following slides describe <u>one</u> implementation!**

PCI Security Standards Council

# Creating a Provisioning Facility

## Define space, tasks and roles

- Areas have to be secured with restricted access, alarms, surveilance cameras etc.
- Tasks related to the setup and execution of the provisioning must be defined
- Tasks are linked to roles that can be assigned to the personnel
- All this is collected in an elaborate set of instructions that must be reviewed and certified

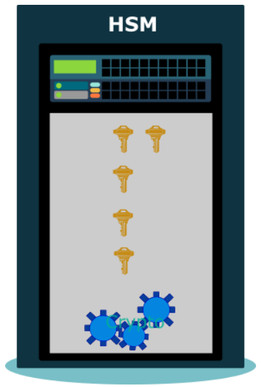


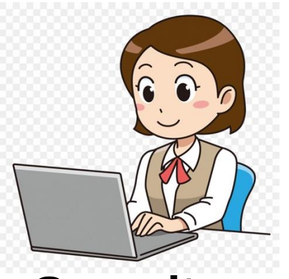
# Limiting exposure

Design to allow need-to-know access

- **Administrative functions** are enabled for a minimum number of administrators
- **Operational functions** may have more operators to handle volume of provisioning
- **Supervisory functions** to check compliance

These functions are split on two restricted areas – allowing differentiation of physical security level and access control

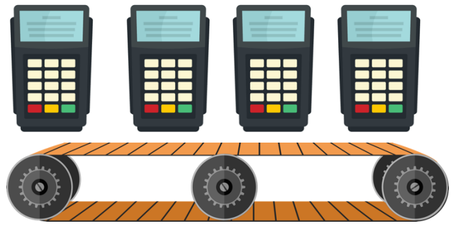


Security Officer 1

Security Officer 2

Operator

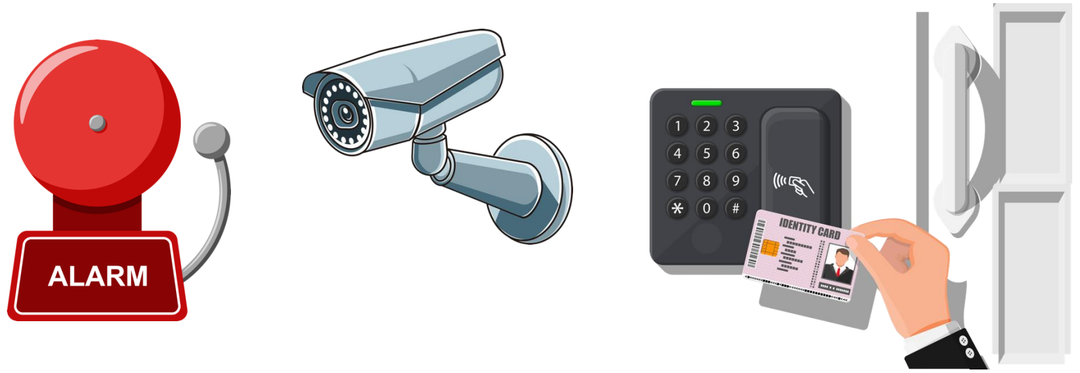


Supervisor

# High Security Area (HSA)

Keep keys and configurations secure

- High Security Area has high physical protection – bars on windows, tamper wires in walls, quick response alarm service, etc.
- Access control has check-in and check-out, it demands present of Security Officers from multiple groups to allow access
- The area holds the provisioning server, HSMs and all the configurations for the provisioning.
- Utilities to support manual key import and export operations are available





PCI Security Standards Council®

# Administration

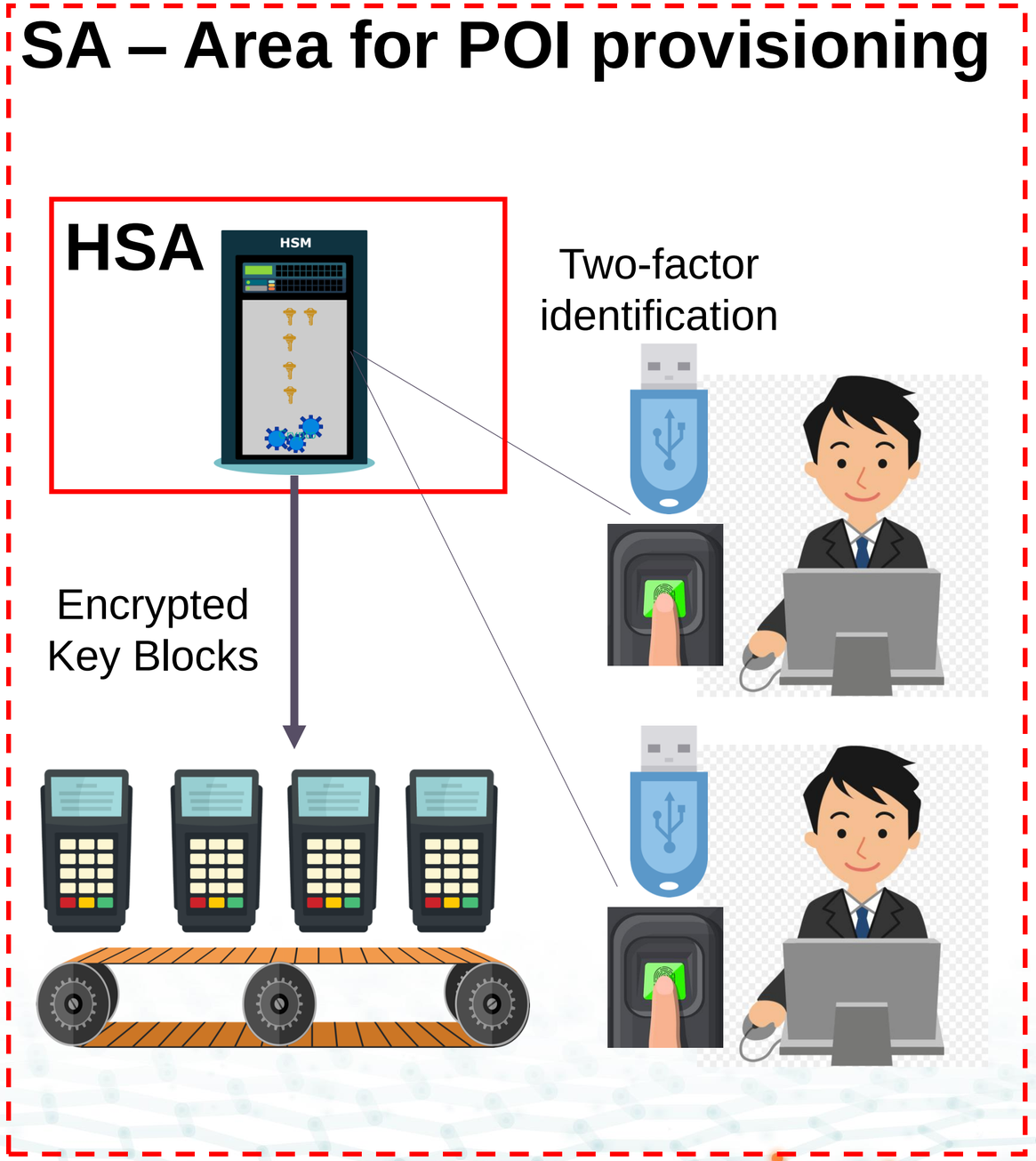
## Setting up the system

- Administrators have access to HSA and can perform tasks on the HSM
- Setup of specific POI configurations
- True random key generation
- Signing of certificates – typically host certificates for RKL operations
- Signing and encrypting firmware for POI devices
- Key Import/Key Export from/to split key letters or as encrypted keyblock

# Secure Area (SA)

Keep track of devices and processes

- The Secure Area is an access restricted area for provisioning
- Operators that move POIs to the Secure Area verify the integrity of the devices
- Operators that connect the POI to the provisioning workstation are identified through security token and fingerprint
- HSM in HSA enforce the presence of minumum two operators in the area to allow provisioning

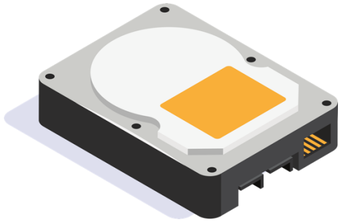



PCI Security Standards Council

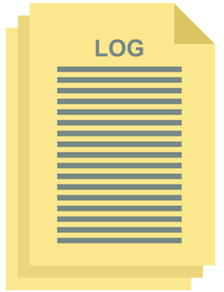
# Supervising

Review access logs, alarm logs and surveilance videos

- Personnel in supervising roles can NOT have administrative or operational roles
- Supervisors are required to review and report abnormal situations to management
- Supervisors review access logs, alarm logs and surveillance videos at defined intervals and immediately in case of exceptional events

**Video log**




**Access log**

**Alarm log**

**Supervisor**


PCI Security Standards Council®

# Audit and Certification

Biennial audit and renewal of certification

- The certification of the secure facility needs to be renewed with two-year intervals
- The auditor will inspect secure facilities
- The auditor will review audit logs, report from supervisors, instructions and interview personnel involved to ensure operations are compliant
- Remarks must be addressed and corrected!
- An AoC is received if all is OK!


PCI Security Standards Council®

# Takeaways

What I hope you have noticed

- PCI PIN covers the whole payment system
- POIs in operation have been through multiple steps that has to be done securely
- The provisioning setup must ensure the integrity of the POIs provisioned
- Administrative setup must be able to support secure key import and export
- **Establishing and maintaning a secure facility for POI provisioning is not trivial!**


Security Standards Council®