Key Management System (KMS)

Enterprise Key Management Without the Complexity of Traditional HSM Systems

⚠️ The Challenge

Modern payment environments depend on secure cryptographic key management—but:

- Key injection and rotation processes are **manual and complex**
- Compliance with **PCI PIN / TR-31 / TR-34** is difficult
- ATM and host systems require **synchronized key states**
- Security operations lack **centralized visibility and control**

Traditional solutions:

- Require **expensive HSM infrastructure**
- Are **difficult to integrate**
- Lack flexibility for modern architecture

👉 Why This Matters

Inefficient key management increases:

- Operational risk
- Compliance exposure
- Cost of maintaining secure environments

A modern KMS must **simplify operations while strengthening security**

🏦 The Statera KMS Solution

Statera KMS provides a **centralized, secure key management platform** designed for ATM networks and payment processors.

It enables:

- Secure generation, storage, and distribution of cryptographic keys
- TR-31 / TR-34 compliant key exchange
- Seamless integration with ATM and host systems

👉 Core Capabilities

Core Capabilities include:

- Key Lifecycle
- Key Exchange
- Integration
- Visibility

🔄 TR-31 / TR-34 Key Exchange

- Remote key loading for ATMs
- Secure key block transport
- Industry-compliant key distribution

🏧 ATM & Host Integration

Designed to operate across **all major ATM environments and payment systems**

- Supports **multi-vendor ATM environments** (e.g., NCR, Diebold Nixdorf, Triton, Hyosung)
- Compatible with **existing ATM protocols and key loading workflows**
- Integrates seamlessly with **ISO8583 host systems**

☁️ Cloud or HSM Integration

- AWS Payment Cryptography support
- HSM-backed key operations
- Hybrid deployment options

📊 Visibility & Control

- Centralized key management dashboard
- Audit logs and compliance tracking
- Key State Monitoring (Active / Pending / Retired)

Designed for multi-vendor ATM environments and modern payment infrastructures

Key Management System (KMS)

Enterprise Key Management Without the Complexity of Traditional HSM Systems

🔐 Zero Key Exposure Architecture

Designed with a security-first model that ensures sensitive cryptographic material is never exposed in operational systems.

- Only **secure key references** are used
- All key material remains within **HSM / cloud KMS boundaries**
- Reduces breach risk and simplifies compliance

Keys are never stored or exposed within the processing environment

⚙️ How It Works

- Keys Generated or Imported
- Keys Securely Wrapped (TR-31 / TR-34)
- Keys Delivered to ATM / Host
- Keys Activated & Synchronized
- Lifecycle Managed Automatically

🎯 Why Statera KMS

- Centralized, secure key management
- Standards-compliant (PCI PIN, TR-31 / TR-34)
- Seamless ATM & host integration
- Automated key lifecycle and operations

👉 Next Steps

Evaluate your current key management process and identify opportunities to:

- Reduce operational complexity
- Improve compliance
- Strengthen security posture

Statera Systems (by Statera Consulting LLC)
anthony.meiring@stateraconsulting.net
+1 (954) 536-1899
www.statera-consulting.net