Utimaco KeyBRIDGE POI

Priyank Kumar
Product Management

May 2020

Creating Trust in the Digital Society

utimaco®

Executive Summary

KeyBRIDGE POI

- Meet **PCI DSS Key Injection** and **Remote Key Injection** requirement
- No need for complex POS terminal manual, with **built-in simplified workflow** and key management for supported POS terminal
- Scale yet meet the complex PCI requirements with **RESTful API**

Digital commerce is growing rapidly, requiring uniqueness and efficient key management

Local Key Injection

Remote Key Injecton

The Market & Why?

Let's Understand the Market First!

Payment terminals must be injected with **special keys** to **encrypt the PIN** and create an **Enciphered PIN Block**

Key Injection / Key injection facility (KIF)

Each device has a truly unique electronic identity that can be trusted, managed and addressed.

Key Rotation

Comply with Payment Card Industry Data Security Standard (PCI DSS) requirements.

Remote Key Loading

A secure, efficient, and cost-effective way to load and manage remote POS encryption keys

Challenges Faced by KIF

utimaco®

Compliance Mandates

Enforcement by ASC X9.24 – Part 1, must use only hardware-based encryption devices to protect payment keys.

Scalability

Existing KIF are usually limited to a single POI or EPP vendor. Mostly lacks graphical user interface tools.

Business Risk

Compliant cryptogram storage facility.

Business Effectivity

As key usage expands, the complexity of managing and tracking keys increases. Increases the risk of key exposure.

New Regulations

Timeline Challenges Faced

Key	Expiration Date	Status
1024-bit	**31 December 2009**	This key must have been removed from all devices by 1 July 2013.
1152-bit	**31 December 2017**	This key must have been removed from all devices by 1 July 2018.
1408-bit CA Public Key	**31 December 2024**	Required to be in **all VSDC devices supporting Offline Data Authentication or Offline Enciphered PIN**. The maximum expiration date for Issuer Public Key certificates will be 31 December 2024.
1536-bit CA Public Key	Considered to have an anticipated lifetime to **at least 31 December 2029**	Designed for use **only in transit fare gates supporting Offline Data Authentication. This key is NOT to be loaded into VSDC POS devices.** The maximum expiration date for Issuer Public Key certificates will be 31 December 2029.
1984-bit VSDC CA Public Key	Considered to have an anticipated lifetime to **at least 31 December 2029**	Required to be in **all VSDC devices supporting Offline Data Authentication or Offline Enciphered PIN**. The maximum expiration date for Issuer Public Key certificates will be 31 December 2029.

Business Effectivity

- Tracking and ensuring key expiration set by EMVCo and the Networks

New Compliance Mandates

- Must meet Key Bundle requirement
- Must have an AES migration plan

Utimaco KeyBRIDGE POI Solution

Value Proposition

Compliant

Fully Futureproof Key Injection and Remote Key Injection Solution

Efficient

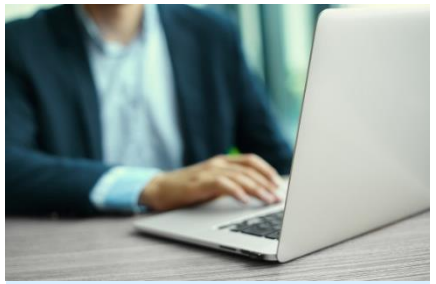
Increases efficiency and **reduces errors** by automating costly manual process such as loading of keys

Compatible

Built-in vendor specific and **Network standard key types**

Effective

Automates with **built-in workflows** including printing of labels for the POS



User-friendly

Easy-to-use graphical interface reduces training and administrative cost

ALL POI Devices in the USA **must be certified** on the KeyBRIDGE platform!

KeyBRIDGE Advanced Security Features

Physical Security

- Built-in **PCI-HSM v3** certified HSM
- Built-in **smart card reader**
- **Secure Cryptographic Device** for Component entry

Logical Security

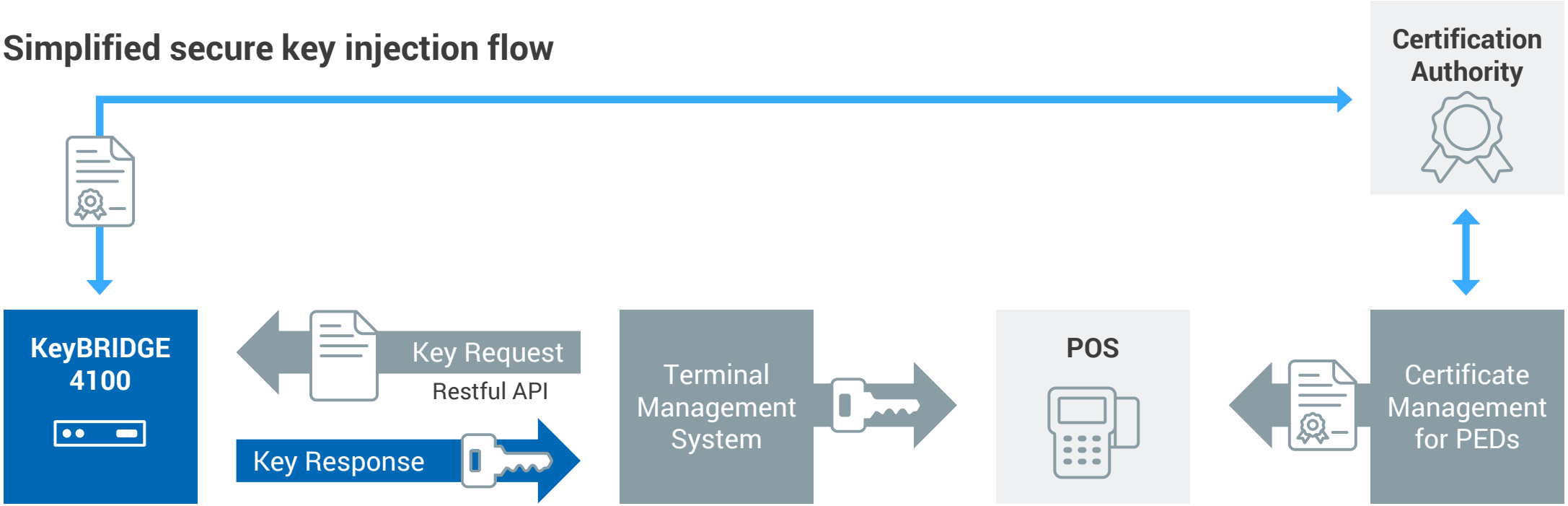
- **RBAC** enforced with dual control and split knowledge
- **Extensive audit logs** containing the complex workflows with mapping to all required data elements
- **Remote Centralized Key Management** built on JSON schema RESTFul API

Remote Key Loading

KeyBRIDGE POI – RKL Solution

- RESTful API for easy integration into your terminal management system
- Support of both symmetric and asymmetric key for PED management
- Including certificate management for remote PEDs

Simplified secure key injection flow



KeyBRIDGE 4100 POI

A state-of-the-art key injection appliance

PCI-PIN approved solution

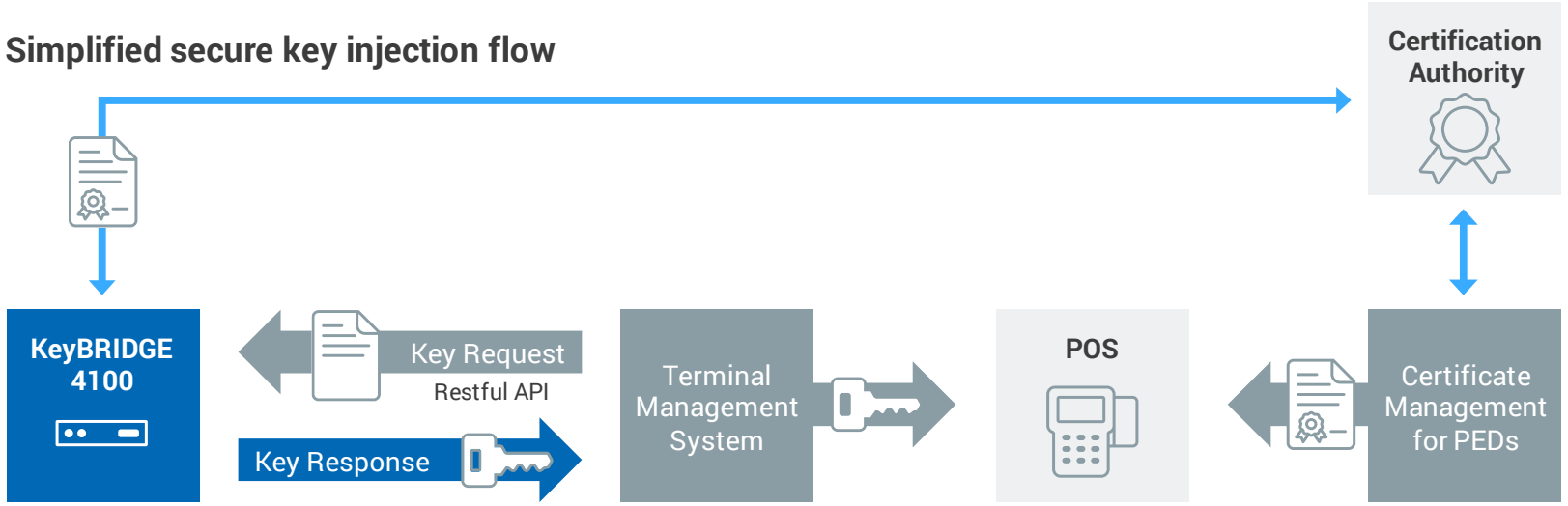
Built-in Health & Reporting

Scalable & High Availability

Built-in Key Lifecycle Management

Summary

- KeyBRIDGE POI allows a business (such as a KIF) to **effectively scale** by **supporting 300+ POS terminals**, continue to add new terminals, regardless of their location
- Remote Key Injection **eliminates shipment cost, downtime and disruptions** caused due to physical shipment of the POS terminal to a KIF
- KeyBRIDGE POI's **built-in simplified workflow and key management process** eliminates administrative costs and overhead associated to avoid errors



Thank you

for your attention!

UTIMACO GmbH

Germanusstraße 4
52080 Aachen
Germany

Phone +49 241 1696-0
Web https://hsm.utimaco.com
E-Mail hsm@utimaco.com