

A photograph of a smiling female barista with short dark hair, wearing a black apron over a dark patterned shirt, interacting with a customer in a coffee shop. The background shows shelves with various bottles and coffee-making equipment. On the right side of the image, there are several overlapping blue and light blue geometric shapes, including squares and diamonds.

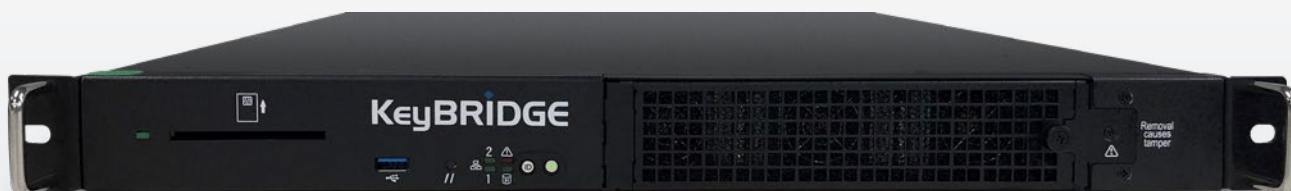
Performing Key Injection and Key Loading Remotely

Performing Key Injection and Key Loading remotely to **Improve Security, Cut Costs and Streamline Operations**

This white paper addresses how remote key loading can improve security, cut costs and streamline operations for ATM and POS/POI Device Manufacturers and Key Injection Facilities (KIFs). In the USA all POI devices must be certified on the UTIMACO KeyBRIDGE platform. In this white paper we will highlight KeyBRIDGE's enhanced capabilities and feature set, as well as outline the remote key distribution and key loading operations and framework.

Table of Contents

- 3 Executive Summary
- 4 Increasing Challenges and Complexities in the Payments Industry
- 4 A More Secure, Efficient, and Cost-Effective Way to Load and Manage Encryption Keys
- 5 Streamlined, Compliant Key Management
- 6 Enabling Remote Key Distribution
- 6 Performing Key Loading
- 7 Conclusion



UTIMACO KeyBRIDGE POI

Executive Summary

The financial industry is a constantly evolving and highly regulated labyrinth where everything is growing exponentially: regulations, transactions and devices.

With no signs of slowing down, it's predicted that **4 million ATMs will be installed worldwide by 2021¹** and the POS terminals market is expected to **grow by USD 3.90 billion during the next four years²**.



Millions of terminals mean hundreds of millions of cryptographic keys that must be secured, tracked and managed.

Payment terminals must be injected with special keys to encrypt the PIN and create an Enciphered PIN Block. Then, each time a transaction takes place, another unique key is created. These keys continue to multiply as they cross sales channels, resellers, and merchants, so it's imperative that each device has a truly unique electronic identity that can be trusted, managed and addressed.

With the growing number of ATMs worldwide, the management and security of cryptographic keys needs special attention.

¹ RBR. Global ATM installed base to reach 4M by 2021. ATM Marketplace, Nov. 8, 2016.

² Global POS Terminals Market 2020-2024 | Growing Need for Self-Service POS Terminals to Boost Market Growth. London. Business Wire, Feb. 25, 2020.

Increasing Challenges and Complexities in the Payments Industry

Injecting special cryptographic keys must take place in a key injection facility (KIF), which is a highly secure environment subject to PCI PIN, TR-39 standards and audit. Traditionally, keys have been directly injected into terminals on premise. However, this is becoming increasingly difficult to manage for a multitude of reasons. New PCI regulations state that keys must be rotated and refreshed every six months to ensure optimal security. Couple this increased rotation schedule with a continually growing number of devices and key injection can become unwieldy and slow. Even more alarming, as key usage expands, and key management becomes more complex, so too does the risk to key exposure. Vendors need to be able to track and abide by key expiration procedures set by regulatory agencies, such as EMVCo and the Networks, as well as accommodate new compliance mandates, like migrating to AES for key blocks.

| 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. |

Adding another layer of complexity, each acquirer, processor and independent sales organization will require a different set of specifications for loading and managing these keys. There is no cookie-cutter approach, so many times facilities are forced to limit their business to a single POI or EPP vendor because they lack the graphical user interface tools.

Lastly, maintaining the proper key maintenance on these devices is costly! Organizations must build up-front costs into the production of their devices for PCI compliant key injection, as well as on-going shipping costs throughout the year.

A More Secure, Efficient, and Cost-Effective Way to Load and Manage Encryption Keys

Remote key loading offers the industry a solution that not only saves money but provides a much more secure process. Now keys can be updated over the network remotely in a compliant, certified way – no downtime, no disruptions! By automating costly manual processes, vendors eliminate error-prone procedures that can lead to security breaches. Moreover, even if an organization suspects criminal activity, they can simply load new keys in a matter of minutes!

It's important that device manufacturers and KIFs work together to establish proper communication protocols. A Certificate Authority (CA) is used to establish trust between these two parties and facilitates secure key exchange. Using a 140-2 Level 3, PCI HSM will secure your CA against the extraction and misuse of your private keys, as well as enforce defined procedures.

Streamlined, Compliant Key Management with UTIMACO KeyBRIDGE POI

The **UTIMACO KeyBRIDGE POI platform** is a fully future-proof key injection and remote key loading solution offered in a PCI v3 certified hardware security module, smart card reader and secure cryptographic device for component entry. It supports compliant key injection for devices that must be managed in a secure facility where physical access controls are relied upon for the establishment of a new key. Keys are delivered from KeyBRIDGE over a connected interface such as USB, Serial, or Ethernet to a target device. In some instances, a clear key may traverse this interface because of the additional policies and procedures that govern the operation of the secure room where this activity is performed.

KeyBRIDGE has helped numerous organizations increase their capabilities and offer a full range of accurate and fast key injection services to their customers. Complete with built-in, vendor-specific and network standard keys types, companies can instantaneously simplify workflows and increase scalability, allowing support for over 300 POS terminals. This creates greater opportunity to grow the business by catering to new customers and devices!

These devices with unique protocols are custom developed to ensure that every key delivered can be associated to a manufacturer, unique model, device serial number, and additionally configurable meta-data elements. Built on JSON schema RESTful API, this platform provides remote centralized key management, streamlining key injection operational efficiency while automatically capturing all relevant audit log details. All information can be exported and validated with ease, further reducing overhead associated with audit cycles. All activities can be reliably traced to at least two unique personnel, while system managers have greater granular flexibility to assign unique role-based access controls.

The KeyBRIDGE appliance allows for the concurrent connection of sixteen unique devices. Injection profiles are configurable allowing a user to inject upwards of thirty keys to a single device in as few as four mouse-clicks. Additional features that can be licensed include:

Key Features & Benefits

- A **fully compliant and secure** PCI v3 certified, FIPS 140-2 Level 3 Hardware Security Module (HSM)
- **Increases efficiency and reduces errors** by automating costly manual process such as loading keys
- **Universal, compatible solution** with built-in vendor specific and **Network standard key types**
- **Intuitive, automated workflows** including printing of labels for the POS
- **Easy-to-use graphical interface** reduces training and administrative costs

Remote Audit Management

(ARCKTM API) Enables the remote access by management to perform audit and statistic reporting.

SCD Component Entry

Allows users to securely enter TDES or AES components through a separate, removable Secure Cryptographic Device (SCD) and send them encrypted to the KeyBRIDGE appliance for storage.

Custom Key Usage

Allows users to define additional Key Usages and determine the permissible characteristics of those Custom Key Usages.

Custom PED Key Export

Allows users to define a specific format for the export file(s) containing POS keys, as well as allows users to change the names associated with POS models.

Network Support

Allows users to save data such as audit logs, key inventory and system backups from the KeyBRIDGE appliance to a network drive.

Custom Key Attributes

Allows users to create up to 12 custom attributes at the key level.

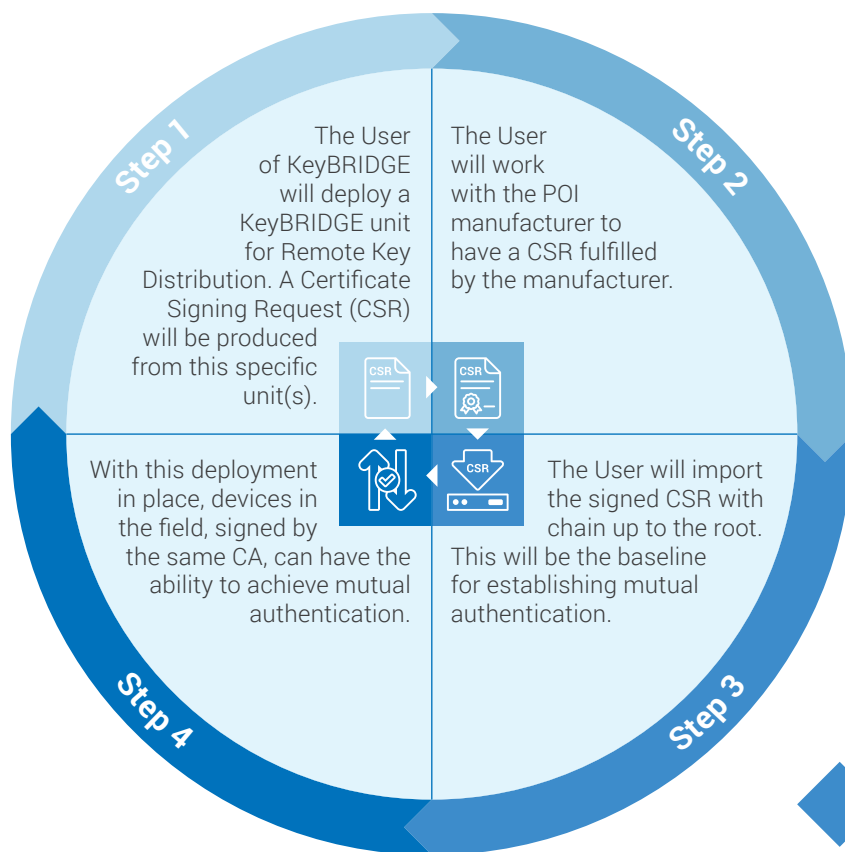
Real-Time DID Back-Up

Performs real time backups of your DID counters ensuring that no future keys end up as duplicates for previous deployments.

Enabling Remote Key Distribution with UTIMACO KeyBRIDGE POI

A POI manufacturer can easily offer remote key injection services for distribution channels such as ISOs and ESOs by using the following process.

Since the devices are signed with the same CA using a similar process, our respective equipment is also capable of performing mutual authentication for other devices, such as mobile.



Performing Key Loading with UTIMACO KeyBRIDGE POI

1. With a cryptographically signed key pair now loaded on the POI device(s), KeyBRIDGE Users will be capable of performing compliant remote key loading for both PIN, Data, MAC, and other keys. In most instances, a distributor will own and operate some form of an "Estate Management System," for the purposes of facilitating mass communication to devices in the field. This channel can be leveraged to perform remote key loading, but KeyBRIDGE can also communicate directly with devices in the field, if that will add value to the service model.

2. With the key pair now in place, the public key certificate may be distributed for key collection. X9.TR-34 provides for two separate verification techniques depending on feasibility:

- **One-Pass Method**

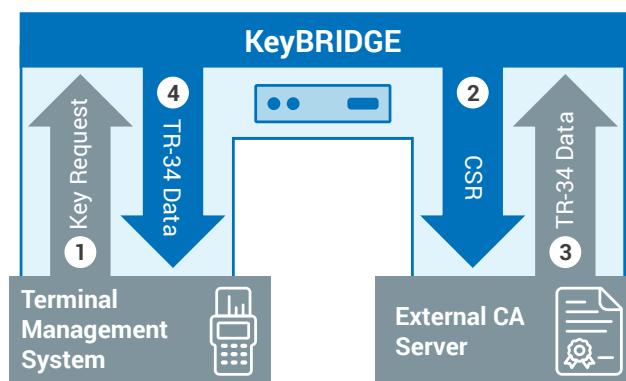
Does not necessarily require the POI device to authenticate an end point that it will obtain a key from.

- **Two-Pass Method**

Preferable, because this method allows for mutual authentication prior to importing a key.


3. Then the POI device will submit its public key certificate to a KeyBRIDGE user. KeyBRIDGE will perform authentication of the signed key. KeyBRIDGE can wrap a designated key with the public key, extracted from the signed certificate.

4. KeyBRIDGE will then return a symmetric key, wrapped by the signed public key of the POI device, back to the requesting entity. The requesting entity may be the "Estate Management System," or the POI device itself.



UTIMACO – Your Trusted Partner

Customers expect speed, efficiency and accuracy, especially in the financial arena. With the continued proliferation of devices and regulatory requirements, POS/ATM Manufacturers and KIFs will need to continue to evolve their business offerings.



By leveraging remote capabilities, organizations can easily accommodate the growing number of key injection and key loading requests, while also providing a more secure payments landscape.

From key injection, tokenization, payment processing and payment issuance to enterprise data protection and key management, UTIMACO provides a full portfolio of products and partners that cater to the entire payment ecosystem. We encourage you to contact our team today.



Get in Touch



EMEA

UTIMACO IS GmbH

📍 Germanusstraße 4
52080 Aachen,
Germany

☎ +49 241 1696 200

✉ hsm@utimaco.com

Americas

UTIMACO Inc.

📍 900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

☎ +1 844 UTIMACO

✉ hsm@utimaco.com

APAC

UTIMACO IS Pte Limited

📍 50 Raffles Place,
Level 19, Singapore Land Tower,
Singapore 048623

☎ +65 6631 2758

✉ hsm@utimaco.com

For more information
about UTIMACO HSM products,
please visit:

hsm.utimaco.com

© UTIMACO IS GmbH 06/20

UTIMACO® is a trademark of UTIMACO GmbH. All other named Trademarks are Trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

utimaco®