Financial Remote Key Loading Overview

TABLE OF CONTENTS

THE FINANCIAL REMOTE KEY LOADING LANDSCAPE

We all depend on encryption keys in one way or another. While few people outside the payments industry are aware of this, anytime you present your payment card at a Point of Sale (POS) terminal or use an ATM, an encryption key quickly goes to work to encrypt the PIN or the primary account number (PAN) associated with your card. This encryption obscures the data and protects against information theft as the transaction is sent back to the card issuer for validation. For this process to work, an encryption key must be securely loaded into that endpoint device, whether it be an ATM, a POS terminal, or a commercial off-the-shelf device used for payment acceptance.

How does that encryption key find its way onto those devices? This has traditionally been done manually through a process known as direct key injection. For POS terminals and PIN entry devices, this involves bringing the devices to a key injection facility where key administrators manually inject each device. This can be time consuming and expensive. It requires the upfront cost of maintaining a validated Payment Card Industry (PCI) Level 3 key injection facility (KIF), and the operational costs of shipping devices to the KIF anytime they need to be rekeyed. For larger devices, like ATMs and gas station payment terminals, key administrators will often have to travel to each device in the field to load the necessary encryption keys. For organizations with widespread ATM or POS networks, this can be a significant operational expense with a high susceptibility to human error.

While the direct injection model has been sufficient for many organizations, others will find a remote key loading (RKL) solution more cost effective and efficient. With RKL, a remote key server establishes a secure, PKI-authenticated connection with each device and remotely distribute encryption keys without having to physically access the device. The ability to remotely rekey the device in the field without extended downtime is a powerful time and money saver for many organizations.

RKL allows organizations to manage keys for an entire infrastructure by sending cryptographically-secure key exchanges from a centralized location. Better yet, devices can be rekeyed instantaneously with an absolute minimum of down time. Gone are the costs associated with maintaining an injection facility and manual injection.

THE MANUFACTURER'S ROLE

Successful RKL operations require collaboration and standardized communication protocols between the device manufacturer and the RKL provider. The backbone of RKL is trust at both ends of the key exchange, one end being the RKL provider and the other being the field-level device. This trust is established by a certificate authority, which provides both the endpoint terminal and the RKL platform with a digital certificate. This certificate serves as a private key in the public key infrastructure (PKI) used to facilitate secure key exchanges. This process is covered in more detail later in this whitepaper. The manufacturer's role is to ensure that their devices have this certificate before deployment.

Furthermore, the endpoint devices and the RKL provider must use the same communication and encryption protocols, which furthers the manufacturer's role in the process. While the most common and accepted encryption standard for RKL is TR-34, there are many others in use depending on manufacturers, geographic location, and other factors. It is important for RKL providers to be accommodating in their platform design to allow integration with multiple manufacturers.

ENDPOINT DEVICE APPLICATIONS

AUTOMATED TELLER MACHINES (ATM)

ATMs are used by millions of people withdrawing cash every year. In 2016, the United States Federal Reserve noted that of the 91% of Americans with a credit, debit or other bank account, 75% use ATMs for cash withdrawals[1]. With so many people depending on ATMs functioning properly, security is a major concern. ATMs rely on network protection and PIN encryption techniques to keep the customer customer's PINs safe.

The encryption keys used to encrypt and validate PINs must be rotated on a regular basis to meet compliance mandates and maintain security. Before remote key loading became a viable option, key holders were required to visit each ATM in person to rotate keys across the network. This process was cumbersome and has grown increasingly infeasible as the number of ATMs continues to grow. The rate of ATM growth is still swelling, with 4 million installations worldwide predicted by 2020[2].

[1] United States. Federal Reserve Board. Consumer and Community Affairs. Consumers and Mobile Financial Services Report. By Sam Dodini, Alejandra Lopez-Fernandini, Ellen Merry, and Logan Thomas. Washington, DC: Federal Reserve Board, 2016.
[2] Cummings, Richard. Global ATM Market Forecasts to 2020. Report. London: Retail Banking Research, 2016.

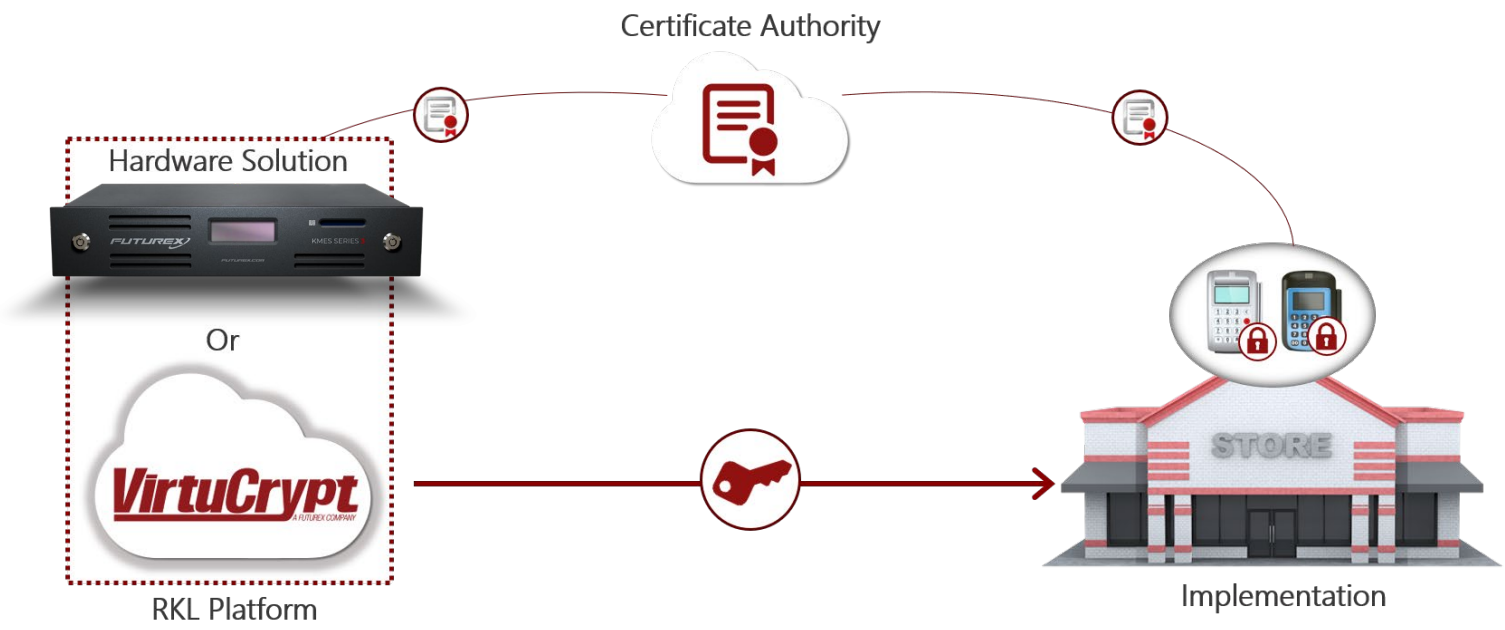
Furthermore, Payment Card Industry Data Security Standard (PCI DSS) regulations require that all PINs be encrypted upon capture at the terminal. RKL provides a secure, efficient, and cost-effective method for loading and managing ATM encryption keys across entire ATM networks.

POS TERMINALS

POS terminals have double the encryption work. Like ATMs, they encrypt PINs for debit card transactions, but many merchants also require primary account numbers, commonly known as PANs, which are the account number associated with credit card payments, to also be encrypted. While PCI DSS regulations do to not currently require PAN encryption, its rapidly becoming the norm in the payments landscape. Recent years have seen high-profile data breaches that were traced back to a lack of PAN encryption. PAN encryption works similar to PIN encryption, but the technology surrounding PAN encryption is typically referred to as Point-to-Point Encryption (P2PE). Like PIN encryption, P2PE encrypts the PAN at the moment of capture in the POS device.

The encryption mechanisms behind PIN and PAN encryption differ slightly on the payment processing end, but they are the same for the purposes of RKL. Both processes require reliable access to encryption keys. Most POS terminals will have at least 2 key slots, with separate keys for both PIN and PAN encryption.

RKL Process Overview



CRYPTOGRAPHIC TECHNIQUES

In order for the endpoint device to receive symmetric encryption keys for PAN or PIN encryption, it must first establish a secure connection with the remote key platform. PKI is a form of asymmetric cryptography where the sender and receiver use public and private keys to both decrypt messages and verify each other's identity. PKI allows the endpoint device and the RKL platform to verify each other's identities and securely exchange keys.

CERTIFICATE-BASED RKL (USING RSA KEY EXCHANGE)

Certificate-based RSA PKI is the most common and accepted method of RKL communication. Unlike symmetric cryptography where a single encryption key can be used to encrypt and decrypt a message, asymmetric cryptography requires two keys to communicate. A public key is used to encrypt and send the message by the sender, and a private key is used to decrypt the message by the recipient. This adds another layer of security in that not only is the message encrypted, but the recipient's identity is verified and authenticated by possessing the appropriate private key.

PKI is the cryptographic backbone of RKL. For ATMs and POS terminals to receive and decrypt the keys sent to them by the RKL service, they must first be possession of a private key, which is known as a certificate. This certificate is injected into the POS terminal or ATM, usually at the time of manufacture by a certificate authority. Once the endpoint device receives its unique certificate, it can be deployed in the field where it can establish a secure connection. This facilitates the exchange of keys with the RKL platform.

The Accredited Standards Committee (ASC) X9, the component of the American National Standards Institute (ANSI) responsible for developing consensus standards for the financial services industry, has established Technical Report 34 (TR-34), which outlines the methods for remote distribution of symmetric keys using asymmetric encryption. TR-34 establishes the certificate-based RKL protocol as the preferred method of delivering encryption keys to POS and ATMs.

SIGNATURE-BASED RKL

Another cryptographic technique used to establish a secure connected for RKL is signature-based. This method is primarily in use among older ATM networks. While similar to certificate-based RKL in some ways, it uses a digital signature that encrypts the key before being sent to the ATM. Signature-based protocols are more simplistic and require less data being sent, which may make them more suitable for older ATM networks based on dial-up connections.

SYMMETRIC KEY RKL

Some manufacturers inject keys into their own devices before deployment. In this symmetric key RKL model, the certificate establishment is skipped by integrating the initial symmetric key injection into the manufacturing process. While its not as prevalent as certificate-based RKL, it is still in use by many organizations.

FUTUREX AND VIRTUCRYPT'S SOLUTIONS FOR RKL

Futurex and VirtuCrypt are the industry's only single-vendor providers of complete cryptographic infrastructures for payment security. Many of Futurex's most important services, like PIN encryption and validation, P2PE, and tokenization, rely on secure and compliant key management.

In response to the growing demand for RKL with the financial services industry, Futurex and VirtuCrypt have developed the most robust RKL solutions in the industry. Whether choosing cloud functionality through VirtuCrypt, on-premises hardware through Futurex, or a combination of both, each solution has the functionality needed to build a comprehensive, single-vendor solution for all cryptographic processes related to financial services and payment processing.

ON-PREMISES HARDWARE SOLUTION: FUTUREX HARDENED ENTERPRISE SECURITY PLATFORM

Futurex's Hardened Enterprise Encryption Platform is an advanced product line of HSMs, key management servers, and payment data security solutions. Within the Hardened Enterprise Security Platform, the primary RKL platform is the Key Management Enterprise Server (KMES) Series 3. The KMES is a complete key management solution for generating, distributing, and injecting POS and ATM encryption keys. The KMES was designed from the outset with RKL as its primary purpose. It is a sophisticated single-device solution for organizations seeking to transition from direct key distribution to RKL. The KMES is equipped with an internal Secure Cryptographic Device (SCD) for key storage. It is fully compliant with Federal Information Processing Standards (FIPS) 140-2 Level 3, PCI HSM, and all other major industry standards for security.

The flexibility of the KMES Series 3 allows individual customers to choose how automated, or how much user interaction is required, which is typically predefined by the customer's security policy. The KMES Series 3 can be fully automated after initial setup and loading of the major keys. For the KMES Series 3 to be fully automated, it requires integration by incorporating the KMES Series 3's application programming interface (API) into the host system. This will be described in greater detail

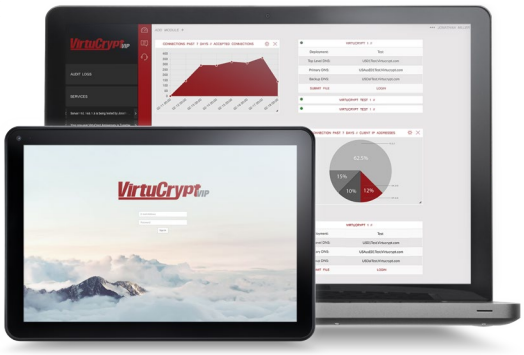
later in this document. The integration application can be written in any language that allows for basic TCP/IP support (Java, C, C++, etc.). The KMES Series 3 uses the Futurex proprietary interface with a fully-functioning GUI.

Futurex On-Premises RKL Overview

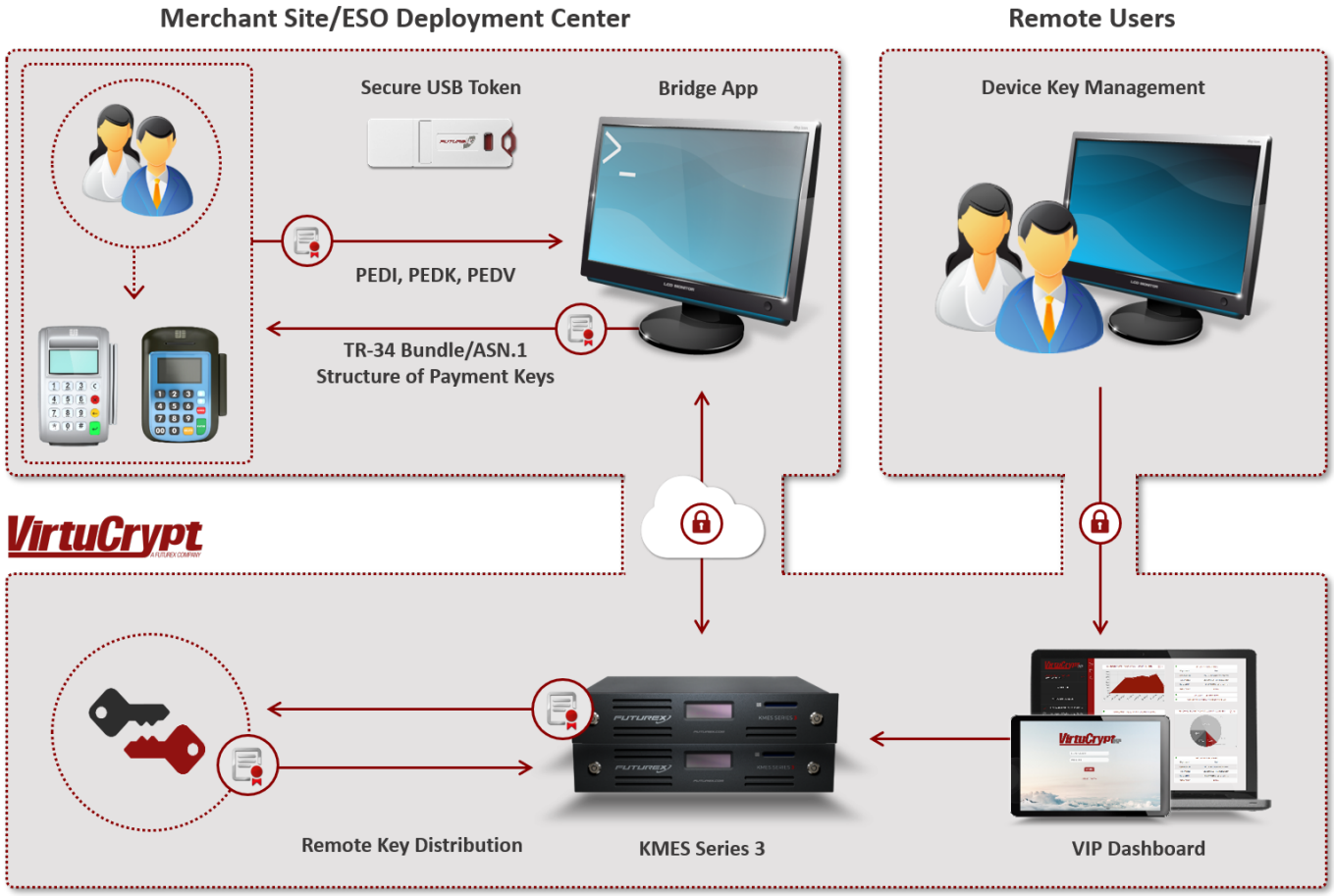
CLOUD SOLUTION: VIRTUCRYPT CLOUD PAYMENT PLATFORM

For clients who prefer "as-a-service" cryptographic functionality, Futurex key loading solutions are available through the VirtuCrypt Hardened Enterprise Security Cloud. VirtuCrypt is best-suited for organizations who prefer hosted cryptographic services as opposed to maintaining their own on-premises hardware. With the VirtuCrypt Elements RKL Service, VirtuCrypt will act as a key distribution host by securely automating the manual key replacement process by managing and loading keys from one central location over a secure IP network. VirtuCrypt is powered by Futurex hardware, which means that VirtuCrypt clients will receive the same security and compliance benefits that would come from owning Futurex hardware, in particular FIPS 140-2 Level 3 and PCI HSM compliance.

Security concerns about the cloud usually revolve around the idea that sensitive data being transferred or stored within the cloud may be viewed by unauthorized people. However, VirtuCrypt's innovative approach to the cloud alleviates these concerns, with all sensitive data being encrypted, decrypted, and authenticated in FIPS 140-2 Level 3 compliant Secure Cryptographic Devices located within SSAE 16 (SOC 1, 2, and 3), PCI, TIA-942 Tier 4, and HIPAA-compliant data centers.



The VirtuCrypt Intelligence Portal (VIP) Dashboard gives customers this centralized management platform for all their VirtuCrypt hosted services. With the VIP Dashboard, users can securely communicate directly with the Futurex device performing the service at the VirtuCrypt data centers. This allows users to import keys and manage key receiving devices. Additionally, users can view and export audit logs detailing past key injections and various other individual user actions.



VirtuCrypt Cloud RKL Overview

CONFIGURING ATM AND POS DEVICES

POS TERMINAL

The KMES Series 3 GUI contains an intuitive way to add remote devices. After the POS devices have been signed by a certificate authority and deployed to the field, the KMES operator can easily connect the devices. KMES configuration is available through the unit itself using the point-and-click GUI, through the Guardian Series 3 for managing clusters of multiple KMES Series devices, or remotely through the Excrypt Touch tablet device.

Device Groups

Organization responsible for managing large numbers of devices will benefit from Futurex's device-grouping options. This functionality allows multiple POS terminals or ATMs to be organized into groups. This facilitates easy management of large estates of devices that have separate requirements from a key management perspective.

Device groups can be configured in a variety of ways. For organizations that have multiple units or subsidiaries involved in key management, these groups can be clustered according to their appropriate owners. Administrators can configure a variety of other settings specific to the device group. These include manufacturers, device types, RKL protocols, and more.

Device Estate Management

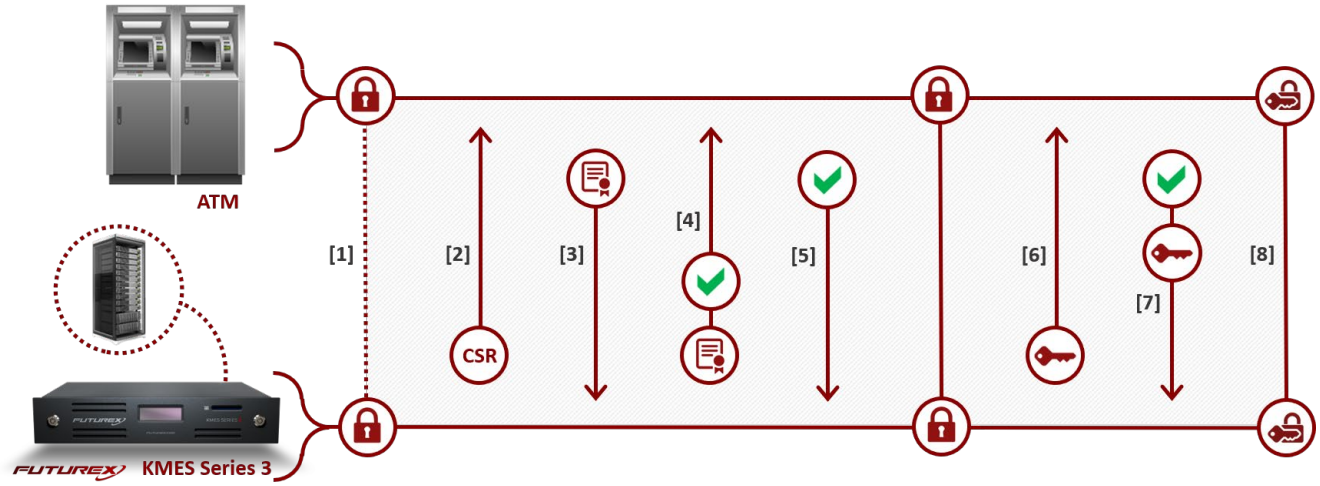
The KMES greatly simplifies management for large estates of endpoint devices. Batch import functionality has been built into Futurex's RKL platform allowing for importing large numbers of devices at once. After the devices have been added and grouped, its simple to maintain awareness of large estates of devices. The KMES' GUI easily displays the key status of each device and makes it simple to perform device-specific administrative tasks like preventing a device from receiving keys.

ATM SUPPORT

All communication between the KMES Series 3, host application, and ATM is conducted over a mutually authenticated TCP/IP connection, with the KMES and ATMs interacting via software loaded onto each ATM. This software on the ATM acts as a bridge between the KMES and the ATM's encrypting PIN pad (EPP).

Depending on the manufacturer, different steps may need to be taken during the setup and remote key loading processes depending on whether the ATM environment is signature-based or certificate-based, with most steps for each method the same or similar. After initial setup, the KMES Series 3 is ready to begin loading keys.

The setup and key loading process happens in a series of simple steps, as outlined below:



Initial Setup

1. During ATM deployment, an application is loaded onto the ATM, which enables communication with the KMES via a secured TCP/IP network.
2. The KMES Series 3 securely generates and exports a certificate signing request, which is sent to the manufacturer for signing under their certificate tree. Once the manufacturer has signed the request, the signed certificate and CA is loaded in the KMES. Organizations can either request a key loaded through the ATM administrative interface, or they can use a host application to configure the KMES Series 3 to push out key injections on a regularly defined basis.

Mutual Authentication

3. Upon receiving a key injection request, the ATM will send its certificates to the KMES.
4. The KMES Series 3 validates the ATM's certificates, then responds with a verification and the KMES Series 3's certificates.
5. The ATM validates the KMES' certificates, then responds with a verification, establishing a mutually authenticated connection.

ATM Key Loading

6. The KMES Series 3 generates and encrypts the ATM symmetric key under the ATM's public key. Next, the KMES forms a key message, signs it with its own private key, and lastly sends the message to the ATM.
7. The ATM decrypts the key with its private key and stores it, then sends back a success code, which the KMES Series 3 saves in logs for reference by the host application.
8. The ATM is now available to process traffic.

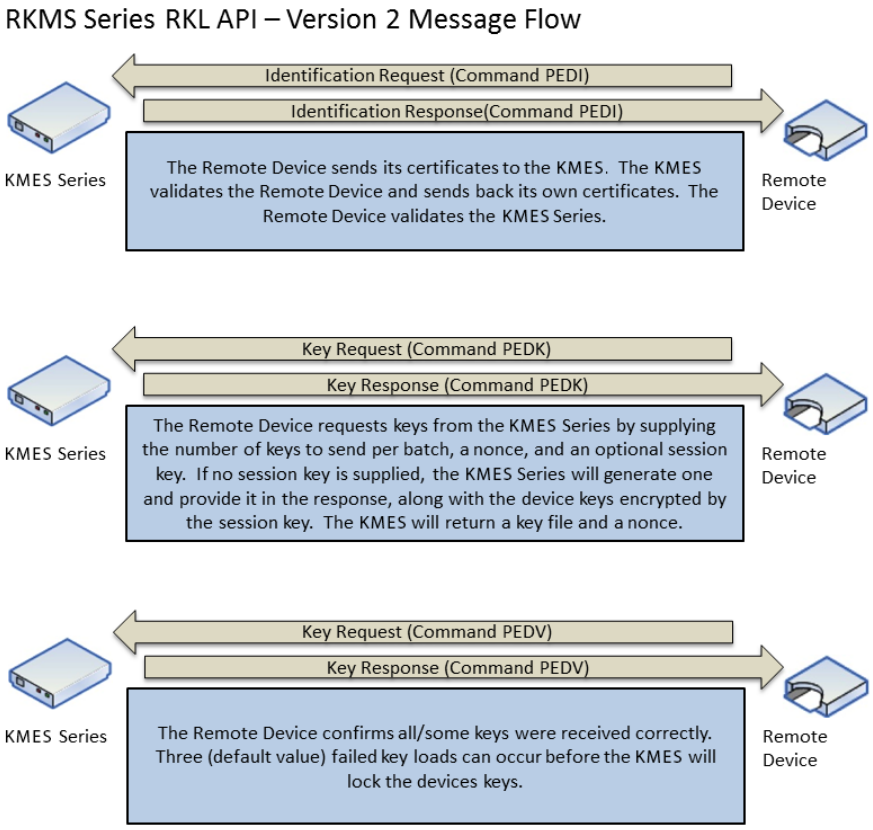
COMMUNICATING WITH THE KMES SERIES API

Whether using an on-premises KMES Series 3 or the VirtuCrypt Element RKL services, clients use Futurex's own application programming interface (API) to communicate with the KMES to manage their RKL services. This is a full-featured API and command set for integration with host application software.

Communication with the KMES Series API must be made via TCP/IP using an ethernet connection that has been wrapped in a TLS tunnel. In most cases, applications communicate directly with the API by sending commands and receiving responses. The Futurex KMES Series API format uses a four-character alphabetic command. There are 3 primary commands used in the Futurex API for remote key loading:

- Command PEDI: Identification Request
- Command PEDK: Key Exchange Request
- Command PEDV: Key Verification Request

TYPICAL RKL MESSGE FLOW



Typical RKL Message Flow

CERTIFICATE AUTHORITY FOR MANUFACTURERS

As discussed earlier, RKL relies on a PKI-secured connection between the endpoint device and the RKL providers. In order for this to happen, device or terminal manufacturer's must utilize a PCI-approved certificate authority to inject private keys into the devices, which act as a certificate to secure the PKI connection. Maintaining an on-premises certificate authority solution for a large deployment of devices can be challenging and expensive. It requires:

- A compliant certificate management solution
- A secure facility validated to PCI Level 3
- A dedicated staff
- Development of internal of policies and procedures for auditing

VirtuCrypt's Certificate Authority service makes this process easy. Rather than endure the hassle of distributed systems to manage, monitor, and maintain certificates within the scope of compliance requirements, VirtuCrypt's Certificate Authority service provides organizations with a central hub from which to perform certificate generation, issuance, storage, revocation, rotation, deletion, and more. This provides invaluable savings in time and costs, simplifies training, and reduces the risks of human error. Perhaps most importantly, with the backing of FIPS 140-2 Level 3-validated secure cryptographic devices, the service is secure.

VirtuCrypt's strength is in their flexible integration procedures and experienced engineering team. VirtuCrypt supports certificate protocols and functionality that can be integrated into terminals from most major manufacturers. Furthermore, VirtuCrypt's engineers can undertake custom initiatives to add functionality for any manufacturers not currently supported.

SUPPORT FOR ALL CRYPTOGRAPHIC TECHNIQUES

The KMES uses asymmetric PKI encryption to distribute keys to remote devices. Before sending keys, the KMES must first generate the Master File Key used to encrypt all the keys it stores or sends. The Master File Key uses either DES or 3DES encryption algorithms to secure the keys for transfer. While 3DES is the commonly accepted encryption algorithm throughout the financial services industry, many organizations take it further with an encryption scheme known as Derived Unique Key Per Transaction (DUKPT), which allows each transaction to be encrypted under a new key.

THE DUKPT PROCESS

There are two main components in creating a DUKPT transaction environment: a Base Derivation Key (BDK) and a unique Key Serial Number (KSN). The KMES contains a counter that increments whenever a new device is added into the network. This counter is encrypted using the BDK, which results in the DUKPT initial key that is injected into the device. This initial key is used later to create a pool of transaction keys, each with a modifier for different key usages. The counter is also used to form the KSN, which is stored on the POS device or ATM's internal HSM. All transactions using DUKPT will include the KSN.

Key Serial Numbers play an integral role in the DUKPT process by enabling the KMES to identify which initial key was used to encrypt the data. As specified by ANS X9.24-1, DUKPT uses a 10-byte KSN, most often represented as a sequence of 20 hexadecimal characters in which each byte of the KSN is represented by a pair of hexadecimal characters.

KEY LIFECYCLE WORKFLOW

All encryption keys in the KMES Series 3 are secured under a device Master File Key, which is protected using the Secure Cryptographic Device's physical and logical security measures and application-level controls, as required by the governing standards. Using the KMES' user-friendly GUI, keys can be sorted into groups assigned to a device or serial number for loading, simplifying the injection process across a network.

AUTOMATIC KEY ROTATION SCHEDULING

The KMES features key grouping options that are similar to the device grouping features discussed early. With this, keys can be organized into groups that assist in key management and implementation for large device estates. Administrators can choose the implementation algorithm for when those keys are distributed. This enables administrators to set up automated key rotation by instructing the KMES to retrieve keys in order of their expiration date, a custom order, or they can keep the process completely manual, if desired.

HOST KEY DISTRIBUTION

In some network infrastructures, it may be necessary for the KMES Series 3 to send keys to the host in addition to the remote devices. This is because the host requires the key to subsequently send session keys to the device. This is known as Host Key Distribution. The KMES has several ways to accomplish this. This can be automated with a compatible host client. This feature uses an available API that is customizable to each host application's needs. Administrators also have the options to distribute the keys through email, set up a retrieval process through network attached storage, or automatically export them.

END-TO-END PAYMENT SECURITY

While this whitepaper is focused on remote key loading, it is important to understand that key management is just one of many elements of a secure payment processing infrastructure. RKL enables PIN processing and validation, Point-to-Point Encryption for PAN protection, and several other encryption-based security solutions. While each one is important on an individual basis, a holistic approach to transaction security would requires utilization of all these measures for a complete umbrella of payment security.

There are multiple security providers on the market that provide individual elements of this functionality. However, Futurex and VirtuCrypt represent the industry's only single-source provider of an entire suite of payment processing cryptographic functionality.

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163