

8541 E. Anderson Drive
Suite 102
Scottsdale, AZ 85255
+1480 699 3119
www.key-innovations.com

Is Key Management a Pain in Your Association?

Adding Security and Reducing Cost with Secure Key Loading

By Scott Spiker, Sr. Security Architect

Contents

Introduction.....	2
Exposed Keys are Vulnerable to Attack	2
Previous Options.....	2
The Key Management Challenge.....	3
Solution.....	3
Benefit 1 – Reduced Key Loading Costs	3
Benefit 2 – Simplified Key Management.....	3
Benefit 3 – Secure Device Authentication	3
Implementation	3
Summary.....	4

Introduction

Since the introduction of the Personal Identification Number (PIN) to authenticate debit card holders and the use of encryption to protect the secrecy of the PIN, security of the encryption keys has been a major concern in order to protect the integrity of the banking system. Today the use of the PIN in the payment industry has become ubiquitous worldwide making key management more important than ever.

Attacks on the electronic payment system is at an all time high; data breaches that compromise credit card information and the PIN have allowed money to be withdrawn from card holder accounts using counterfeit cards in ATMs. Given the global reach of card holder accounts ATM withdrawals can take place anywhere in the world.

Organized crime is heavily involved in attacks on the payment system and is compromising security controls from all angles. In the past the attacks on the system were external, for example skimming card data at the point of sale; shoulder surfing PINs as they are entered; stealing and cracking security mechanisms, as well as sniffing communications traffic over public and wireless networks. In response to this fraud, more secure devices and protocols have been developed and deployed. However, since card holder data is so valuable, these attacks are evolving using technology to break into systems which provide access to bulk credit card and PIN data. These are sophisticated, high-tech attacks using multiple attack vectors, including Internet attacks on servers, installation of sniffer malware and insider attacks on security hardware and systems.

Exposed Keys are Vulnerable to Attack

Have you ever wonder why a PIN Entry Device (PED) must be injected with debit keys inside of a secure room? The reason is

that the injection of the debit key into most PEDs is done in clear text mode, meaning the key that is injected into the device is transfer unencrypted. Most PEDs are injected electronically using communications protocols that could be monitored using electronic equipment exposing the key that was loaded into the device. The standards that are used to regulate PIN encryption keys in the financial industry state that when keys are in clear text form, they must be protected from exposure. When clear text keys are injected in a secure room, the security of the key is ensured by following proper procedures and relying on trusted individuals working together so that the environment remains secure. The processes and procedures are meant to prevent a single person having access into the secure environment so that equipment cannot be tampered with, stolen, or misused. The theory of operation is that by using two trusted people they both would have to work in collusion in order to circumvent the security of the environment.

Now consider, if organized crime is able to get insider access to install malware on an internal merchant or processor network, what prevents them from getting two insiders into the secure key loading environment for the same purpose?

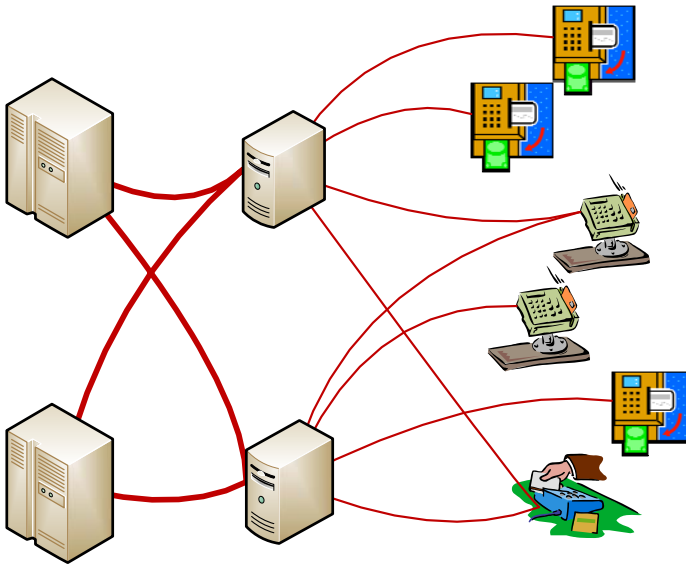
Previous Options

Various methods of key injection have been developed by different PED vendors based on the capabilities of the PED and current technology. Low cost, high volume PEDs have typically implemented basic security features that just meet the current industry requirements; however, due to the lack of processing power of the device, they tend to rely on the secure loading of sensitive data in a secure room that assures the secrecy of the sensitive data loaded. The obvious issue with this solution is that the key loaded into the device can be obtained by monitoring the communications line between the key loader and the PED.

In order to better secure PEDs and support a method of secure key loading, some vendors inject secret encryption keys, unique per device, during the manufacturing process. These keys are typically referred to as terminal master keys (TMKs) and secure the device from the time it is created. Initial debit keys are then encrypted under the TMK so that they are not exposed during key loading. This method allows the device to be secured from the point of manufacture and allow other keys to be loaded outside of a secure room; in fact, keys can be loaded remotely at the time of deployment. However, the terminal master keys must be securely transferred from the manufacturer to the PED purchaser. If the PED purchaser is not the key loading facility, the keys must then be securely transferred to the key loading facility. Many times, during the life of the PED, the control of the PED is moved from one key loading facility to another which requires the terminal master key to be transferred from one key loading facility to another. All of this movement of encryption keys creates a complicated key management process and an environment that could become vulnerable to attack.

The Key Management Challenge

The underlying issue is in the use of symmetric keys for the encryption of PINs. Banking standards require that PINs be encrypted using Triple DES with at least a double length key. Triple DES is a symmetric encryption algorithm that requires the key to be shared between the transmitting and receiving devices. Keys must be created in one device and securely loaded into the other device. Each communicating pair is required to use a unique key or set of keys for processing debit transactions. In the illustration below, every red connection between devices requires a unique and secret key for PIN encryption.



Imagine today with the many different PEDs that are deployed, each having a unique key or set of keys for the secure processing of debit transactions. The number of keys that must be managed is immense. Having these keys in various formats and in a number of different locations provides the potential for a major key compromise. A weak system or secure room procedure could be exploited to obtain a large number of encryption keys.

Solution

To reduce the risk of compromise of PIN encryption keys, the method of distributing these keys needs to be more automated and human handling of the keys needs to be reduced. This means loading the initial symmetric keys directly into a highly secure hardware security module (HSM) from the processor's host or from a secure key loading facility in an encrypted format such that it simplifies the key management burden.

Asymmetric cryptography can be used exactly in this way. In asymmetric cryptography there are two keys, one for each end of the communications channel to be secured. This form of

encryption allows the secure exchange of data, including cryptographic keys, between two devices that have not previously 'met'. Each device has a pair of asymmetric keys, one is called a private key and is retained by the device and other key is called a public key and is transmitted to the other end of the communications channel. The PED can request a debit key from the host's HSM along with its public key, the HSM encrypts the PIN symmetric key with the device's public key and sends it back to the PED. Because of the way that asymmetric encryption works only the PED with the corresponding private key is able to decrypt the received key.

There are a number of affordable security microprocessors today that have the capability to support asymmetric cryptography that is specifically designed for use in PIN entry devices and are cost effective to implement. These security processors also help achieve the PCI PED approvals required by the major card brands.

Benefit 1 – Reduced Key Loading Costs

The number one benefit of the remote key loading is the total reduction of the cost to support PED debit keys. No longer does a device have to be shipped to, or handled by, a secure key loading facility. The device can be configured and securely loaded with both debit keys and payment applications remotely, even at the merchant location. The PED can defend itself from unauthorized key loading attempts by requiring authentication of the key loading device before accepting the encryption key(s).

Management of secure rooms for key injection and the overall cost of key management is reduced because of the elimination of handling clear text keys and simplified key handling procedures.

Benefit 2 – Simplified Key Management

By using specialized security processors, cryptographic keys can be maintained in highly secure hardware devices, never being exposed to the outside world, reducing the threat of compromise from unauthorized monitoring of the communications channel. Devices do not need to be injected within a secure room and can be loaded remotely with keys at the time of deployment.

Benefit 3 – Secure Device Authentication

The asymmetric keys can be used for other secure functions besides key loading. Devices managed by a secure estate management system may not be modified or altered from an unauthorized source. Also, servers and hosts can authenticate devices that process transactions, giving the assurance that the devices are legitimate and have not been modified.

Implementation

Key Innovations has developed a digital certificate based public key infrastructure (PKI), known as a third party trust model

PKI. The use of certificates, signed by a trusted certificate authority, establishes the security of the public keys used in the PKI. Only devices within the Key Innovations trust domain will operate within the PKI and secure connections can be established without a prior meeting of device or other manual intervention. This standards based PKI is used for a number of security related functions to support the PED including software and content authentication, but the primary function is to support the secure distribution of symmetric keys used for debit and other payment related encryption functions.

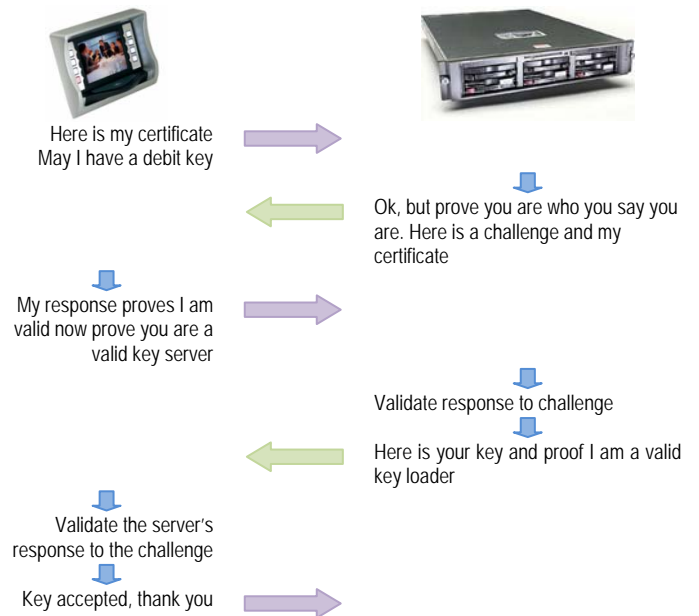
Referred to in the payment industry as ‘remote key loading’ or ‘remote key distribution’, the correct description, from the standards, is ‘symmetric key distribution using asymmetric cryptography’. Key Innovations refers to this method as **Secure Key Injection**. Keys may be loaded to the device in a secure room or at the point of deployment at its remote location. The payload and protocol are the same no matter where keys are loaded into the device. By using the Key Innovations certificate based PKI, the public keys used to protect the symmetric keys are secured and can be tested for trustworthiness. Certificates are distributed on demand so there is no manual loading or intervention required, fully automating the debit key loading process.

The payment device is secured when it is initially manufactured and includes tamper responsive security so that any attempt to modify the device is detected immediately and all secrets in the device are erased, resulting in an inoperative device. When a device requires debit keys, the key loader can test the integrity of the device before a key is loaded into it; thus only loading keys into devices that have not been tampered with.

In the Key Innovations implementation, no cryptographic keys are ever exposed outside of a security processor or HSM; therefore these keys are far less vulnerable to compromise. When the Key Innovations payment device is manufactured the device’s secure microprocessor generates two RSA key pairs, one pair for signing and the other for encryption. The public keys are secured in digital certificates that are signed by the Key Innovations certificate authority (CA), which adds the device to the Key Innovations security world. At this point the Key Innovations payment device is secure and is able to defend itself from tamper attempts. Any tamper attempt is detected and will cause the immediate and automatic erasure of the private keys making the device inoperable, as required under PCI PED 2.0 and PCI UPT 1.0 security requirements. The device is now prepared to perform all security related functions with trusted systems including symmetric key loading.

When there is a key to be exchanged the Key Innovations payment device connects to the secure key distribution host and an exchange of certificates is made between the two devices. For authentication purposes, both devices must confirm that the other is a valid and secure device, in other words, the payment device must ensure that the key loader is legitimate and the key loader must ensure that the PED is secure and is valid to receive

a key. When both sides are satisfied that the other is authentic, the secure key loader encrypts the debit key using the device’s public key. Only the device with the corresponding private key is able to decrypt the key.



Summary

Automation is the key to reducing costs and keeping secrets in hardware devices strengthen security. The Key Innovations KST 9000 does both by design. The use of a public key infrastructure reduces the burden of symmetric key management by automating the distribution of debit keys between secure devices without the possibility of exposing the key to insiders working together to obtain the debit keys as they are injected. The PED generated keys used to transport debit keys are never exposed outside of the secure processor; therefore the risk of a mass compromise of PINs from a collection of encrypted PIN blocks is mitigated.

The Key Innovations PKI implementation supports a number of security functions and features that make it the most secure and easily managed payment product on the market today. The Key Innovations PKI is used for the following security functions:

- Security Firmware authentication, allows for remote updates of firmware
- Application software and user content authentication ensure proper use of the I/O devices
- Secure key loading
- Mutual authentication between payment device and payment server

(Questions, comments or additional information, www.key-innovations.com or e-mail info@key-innovations.com)