Implementing payment card data encryption with HP POS

MSR encryption and key injection

Table of contents

Executive summary ................................................................. 2
Point-to-point encryption ......................................................... 2
  Hardware vs. Software P2PE ................................................... 2
  DUKPT key management ....................................................... 2
  Implementing P2PE with HP POS ........................................... 2
P2PE back end ....................................................................... 3
MSR encryption .................................................................... 3
  Key injection process ........................................................... 4
  Key injection facilities ......................................................... 4
Abbreviations ....................................................................... 5
Executive summary

Multiple card data breaches in the retail industry demonstrate the importance of payment application security. Existing magnetic stripe data (MSD) card payment technology, that was created several decades ago, is highly vulnerable by design. In order to protect cardholder data, many merchants follow Payment Card Industry Data Security Standards (PCI DSS). However, security controls prescribed by PCI DSS are not effective in many situations. Extra measures, such as encrypting the sensitive card data “end to end,” are required in order to provide an adequate level of security and protect the payment transactions from fraud. The HP MX10 (with Retail Jacket) and HP RP7 POS solutions enable hardware encryption of sensitive cardholder data at the entry point which allows merchants to implement a point-to-point encryption (P2PE) solution.

Point-to-point encryption

The idea of point-to-point encryption in general is simple: the sensitive cardholder data is encrypted at one end of the communication and decrypted at the other end. However, when P2PE technology is applied to a retail environment, there are several important conditions that should be taken into account:

- The data must be encrypted as close as possible to the entry point. In case of hardware P2PE, magnetic tracks are encrypted inside the secure module of the magnetic stripe reader (MSR) device.
- Since the encryption end is located in a hazardous environment of a retail store, the decryption end must be placed in a highly secured (both logically and physically) environment such as a payment gateway data center.
- Cryptographic keys must be managed using special secure procedures and equipment that would protect them from the dangerous environment of a retail store.

Hardware vs. Software P2PE

P2PE solutions can be divided into two main groups: Hardware P2PE and Software P2PE. The difference is Hardware P2PE uses hardware for cryptographic operations while the Software P2PE performs encryption (and sometimes decryption) in software. Hardware P2PE is much more secure due to the fact that cryptographic hardware is more protected (both logically and physically) from intrusions than software.

DUKPT key management

Derived Unique Key per Transaction (DUKPT) has been widely used in the industry for many years for debit PIN encryption. It is regulated by security standards (X9.24-1) and supported by multiple hardware and software vendors, payment gateways and processors. DUKPT can be used for MSR encryption exactly the same way it is used for debit PIN encryption. Compared to other key management schemes (such as Fixed or Master/Session Key), there are advantages of DUKPT:

- The sensitive data is encrypted using different keys in each transaction. Even if one transaction is compromised, it does not affect the security of other transactions because it is impossible to recreate the terminal key from the unique session key.
- The terminal encryption key, which is injected into the MSR device, is derived from the Base Derivation Key (BDK) and is unique per device. Even if a single device is compromised, it does not compromise the security of other devices or the entire system because it is impossible to recreate the BDK from the terminal key.

DUKPT key management uses a Base Derivation Key (BDK) to encrypt the key serial number (KSN) that produces an initial encryption key which is injected into the MSR prior to deployment. After each transaction, the encryption key is modified per the DUKPT algorithm so that each transaction uses a unique key. Thus, the data will be encrypted with a different encryption key for each transaction.

Implementing P2PE with HP POS

Figure 1 shows an implementation diagram of a typical P2PE solution architecture with the HP ElitePad Mobile POS Solution. The payment transaction is started by the point-of-sale application located on the HP ElitePad. As soon as the credit card is swiped through the MSR device located on the HP Retail Jacket, the sensitive cardholder information is encrypted using the unique session key which is derived from the pre-injected terminal key. A new unique session key is generated for each transaction. The encrypted data can be safely processed by the point-of-sale application (stored in memory or on the hard drive) and sent over the public networks without the risk of being compromised. The only place where the sensitive cardholder data can be decrypted is the highly secure data center of a payment gateway or processor. Once the information is decrypted, it is processed by the gateway software and routed to appropriate processor or acquirer using proprietary protocols and secure data connections.
The decryption back end, which is usually located in the highly secure data center of a payment processing gateway, is another important part of the P2PE solution (see “Payment gateway data center” in Figure 1). The main function of the P2PE back end is decrypting the sensitive data that was encrypted by the MSR and routing transactions to the appropriate processor or acquirer using their proprietary communication, message, and security protocols. The decryption can be done either in software or hardware. Similar to encryption, hardware decryption is much more secure because it performs decryption and key management operations inside the Hardware Security Module (HSM) which is physically and logically isolated from the rest of the system. HSM devices such as HP Atalla are usually certified with FIPS 140-2 standard and never expose the cryptographic keys (BDK in case of DUKPT).

**MSR encryption**

The HP Mobile POS Solution (jacket) is equipped with an MSR which has encryption capabilities. When a card is swiped through the MSR, the track data can be TDEA (Triple Data Encryption Algorithm, aka Triple DES) or AES (Advanced Encryption Standard) encrypted using Fixed or DUKPT key management (Table 1).

**Table 1. MSR encryption features**

<table>
<thead>
<tr>
<th>Supported method</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encryption algorithm</strong></td>
<td></td>
</tr>
<tr>
<td>TDES with CBC</td>
<td>Industry standard for debit PIN encryption</td>
</tr>
<tr>
<td></td>
<td>Commonly used in P2PE solutions</td>
</tr>
<tr>
<td>AES with CBC</td>
<td>Used in selected proprietary P2PE implementations</td>
</tr>
<tr>
<td><strong>Key management</strong></td>
<td></td>
</tr>
<tr>
<td>DUKPT</td>
<td>Industry standard for debit PIN encryption</td>
</tr>
<tr>
<td></td>
<td>Commonly used in P2PE solutions</td>
</tr>
<tr>
<td>Fixed key</td>
<td>Rarely used in P2PE implementations</td>
</tr>
</tbody>
</table>
Key injection process

In order to enable the MSR encryption functionality, the MSR device must be injected with the terminal encryption key (also known as IPEK in debit PIN encryption implementations). The key injection must be done by a special Key Injection Facility (KIF). The KIF should be certified (TR-39) for performing the secure key injection operations.

Note

For HP MX10 users: it is not necessary to ship the HP ElitePad to the KIF since only the HP Retail Jacket is required for the key injection process.

The KIF and the BDK are determined by the merchant’s P2PE solution provider which is usually merchant’s payment gateway or processor. When retailers decide to implement the HP Mobile POS solution, they should either provide information about their existing P2PE solution provider, or find a new one that supports (or wants to support) the encryption. HP will work with the P2PE solution provider, the KIF, and the POS/payment application vendor on technical details and provide all necessary documentation and equipment (such as additional power and key injection adapter cables) required for key injection.

Figure 2. Key Injection process

Key injection facilities

HP has established relationships and tested the key injection process with the following key injection facilities:

Posdata
www.posdata.com

JRS POS Depot
www.jrposdepot.com

ID Tech
www.idtechproducts.com
Abbreviations

AES - Advanced Encryption Standard

DUKPT - Derived Unique Key per Transaction

FIPS - Federal Information Processing Standards

HSM - Hardware Security Module

IPEK - Initial PIN Encryption Key

KIF - Key Injection Facility

KSN - Key Serial Number

MSD - Magnetic Stripe Data

MSR - Magnetic Stripe Reader

NIST - National Institute of Standards and Technology

PCI DSS - Payment Card industry Data Security Standard

PED - PIN Entry Device

PIN - Personal Identification Number

TDEA - Triple Data Encryption Algorithm