PrimeFactors™

APPLIED DATA PROTECTION

WHITEPAPER

Why Financial Institutions Should Keep EMV Data Preparation In-House

February 2020

Introduction

As the payment network brands continue to push integrated circuit (IC) smart card technology as the preferred payment method for its fraud-busting features, card issuers have had to adjust their card data preparation and issuance practices accordingly.

After more than four decades of service in the financial card industry, magnetic stripe technology may not be going away anytime soon, but it no longer dominates the card issuance scene. For institutions that have honed their magnetic stripe issuance processes into a precise art, the shift to issuing increased numbers of IC smart cards required smart planning and complex decisions about how much of the card issuance process to outsource. In weighing these decisions, it is important to understand that smart card issuance is a shift from mag stripe issuance paradigms.

Bolstering the security of payment cards has been an ongoing process since they were first issued in the 1960s. EMV standards represent an improvement in security over historical magnetic stripe (or mag-stripe) payment cards. EMV stands for Europay, MasterCard and Visa, the original developers of the EMV security standard for IC smart cards, which defines the requirements for payment cards, point of sale terminals and ATMs. EMVCo, owned by American Express, JCB, MasterCard and Visa, manages, maintains and enhances the EMV specifications to ensure global interoperability and sound payment security that meets the ever-evolving challenges in data protection.

Moving from mag-stripe card issuance to issuing EMV smart cards improves transaction security, but it also comes with additional data protection and process requirements. The card personalization process for EMV involves sophisticated data preparation and cryptographic key management tasks, and some amount of specialized knowledge in the area of EMV data preparation is helpful in smoothly transitioning from mag-stripe to EMV smart card issuance.

US card issuers and merchants migrating to EMV had the opportunity to learn from their early-adopter counterparts around the world to minimize the risk and cost incurred by such a migration. One of the biggest lessons learned was in the area of risk exposure. Since EMV issuance is more complex than magnetic stripe card issuance, issuers have much more cryptographic keys and cardholder data to protect, which increases their risk and exposure if cardholder data is breached by unauthorized parties. With the ever-expanding global regulations around data protection, the risk can carry stiff financial penalties, if it is not well managed.

Getting Started: EMV Basics

At its most basic level, the EMV standard, as it relates to those issuing payment credentials, is really more about the software than the hardware. The chip embedded within the card actually runs a card operating system (OS), much like a computer runs Windows or OSX, and a payment application run on the card's secure chip to manage and protect the data stored within it. This setup enables a smart card chip to carry out the following core functions of an EMV card:

- Store secret information securely

- Perform cryptographic processing because it is a secure element
- Perform processing

These capabilities facilitate secure consumer payments. But to ensure interoperability around the world, such advanced technology requires an overarching framework to govern how different chip operating systems, applications and cardholder data works with point-of- sale systems. This is where the EMV standard fits into the picture.

The EMV specifications include standards for contact payment cards and certain contactless payment cards. They also address interoperability at two levels, both the electromagnetic and physical characteristics of the cards, as well as the data elements and protocols of the underlying technology. The most obvious benefit of EMV cards is the ability to store payment information in a secure chip, rather than on a significantly less secure magnetic stripe, but using EMV also improves the security of a payment transaction itself by adding functionality in four areas:

- Card authentication – protecting against counterfeit cards
- Cardholder verification – authenticating the cardholder and protecting against the misuse of lost and stolen cards
- Risk parameter settings – regulating when and how the IC card can be used in a transaction
- Transaction authorization – using issuer-defined rules to authorize transactions

Benefits of Keeping EMV Data Preparation Internal

With so much built-in functionality, EMV requires more data preparation prior to personalizing and issuing cards. While outsourcing magnetic stripe data preparation to third parties has become as much a part of the card issuance process as outsourcing the manufacturing itself, some card issuers may want to rethink that approach with EMV. There are three primary reasons for this: greater flexibility in setting batch-related card personalization settings, improved cost savings, and greater control of critically sensitive encryption key data.

Card issuers must ensure that the data preparation process compiles the application and card profiles, keys and certificates, and cardholder data from several sources, and bundles this information into a single personalization file for the production of the cards.

With the EMV card, the card issuer has added responsibility and a different process than magnetic stripe card issuance: the configuration of the EMV risk parameter settings. These settings must be defined before a card is issued to determine the “rules” under which transactions are conducted and authorized. There are well over 100 parameters that determine options, which include whether a transaction can be authorized online or offline, whether the cardholder verification method will be signature or PIN-based, how many PIN tries should trigger a card lock and so on.

A series of decisions about these parameters must be made before a card is issued and those decisions will determine what information is loaded into the card at the time of personalization. EMV is a much

more data-intensive process than mag-stripe, but by keeping data preparation in-house, the issuer maintains a level of control and responsibility over those decisions rather than giving them to a third party. For example, by keeping this control in-house, values can be assigned to particular cardholders to override the batch settings intended for most cardholders.

Flexibility isn't the only benefit of doing EMV data preparation in-house. In the long run, the decision to invest in an in-house data preparation system could also save money. Card issuers used to traditional magnetic stripe issuance have become accustomed to being able to outsource card production from multiple card manufacturers. This multi-sourced vendor field brings with it the competitive pressure necessary to keep card issuance and manufacturing costs low.

However, the complexity of EMV card issuance and manufacturing will limit vendor choices for organizations that choose to outsource the EMV card issuance process from start to finish. This is in part due to the fact that while card operating systems may all have to adhere to EMV's open standards, each OS can be unique to each card manufacturer. Because of the complexity of the issuance, the largest global manufacturers end up doing all the data preparation and card issuance work necessary to issue a card and end up locking issuers purchasing a certain card into their proprietary OS. When this happens, issuers lose the advantage of having multiple vendors competing for their business. Once a full-service card manufacturer wins an issuer's business to perform data preparation, manage data and generate keys, it is very difficult for that issuer to move to a different service provider.

Maintaining EMV data preparation stage of the issuance cycle in-house has the potential to significantly reduce costs for savvy organizations. If issuers utilize a flexible emboss file format, which can be parsed in any form and used for any card issuance system, they tend to have much better control over their supply chain, minimizing the control any given card manufacturer has over their supply choices. Not only does this posture give issuers a better position in negotiating manufacturing costs with particular personalization service bureaus, it also facilitates the flexibility to move suppliers when business needs arise. See the appendix for additional information.

Keeping Control of the Keystone of EMV: Key Management

Perhaps even more important than flexibility and cost savings is the issue of control. Card issuers have a distinct set of requirements when transitioning from traditional magnetic stripe card issuance to those necessary for EMV issuance in the area of key management.

Cryptographic keys are a critical ingredient to any authentication or communication process secured by encryption. These keys govern the encryption and decryption of data as it is used within or shared between entities, such as payment processors needing to access information secured by a card issuer in order to complete a transaction. The parties involved verify their identities by presenting the appropriate cryptographic keys—essentially an algorithmic shared secret meant to 'unlock' the encryption process.

In the magnetic stripe world, cardholder verification in debit and credit transactions is typically carried out through the use of security codes, PINs, and signatures. However, with EMV, the governance of these

shared secrets largely rests on a master set of keys. Card issuers use these master key sets to generate unique keys for each card in their payment system. The keys on individual cards are based off of the master set using an algorithmic diversification scheme that makes it possible to readily scale the creation of millions of these shared-secret elements that are based on that single secret key set.

The individual cards themselves contain numerous keys to facilitate tasks ranging from secure processing of data and generating transaction cryptograms, to secure communications between the issuer and the card necessary to download software updates and application data/parameter changes.

Safeguarding the information contained within the master key files is of mission-critical importance. The master key generates all of those other keys used as a shared secrets between the issuer and the cardholders, and when secrecy is lost, the protections afforded by encryption are essentially rendered useless. When issuing institutions outsource their EMV data preparation to a third party, allowing them to prepare the complete cardholder data and issue payment cards, the issuing institutions must relinquish control of their master key sets to that third party. When this happens, the issuing institution loses control over their master keys and relinquishes their ability to protect their most important information.

The most typical surrender of key security control occurs when an issuer gives the master key set they have generated in-house to a third party, however some issuers allow their third party manufacturer to generate the master keys, maintain them, and protect them on the issuer's behalf. In both of these cases, issuing institutions are turning over control of one of the most important elements of running a transaction-based business to a third party who has employees, policies and organizational structures over which the issuer has no control. News headlines continue to provide disastrous examples risk incurred through outsourcing, and with the growing amount of global data protection and privacy regulations, stakes are now higher than ever.

Using a Key Management System

Organizations that want to maintain greater control of their data preprocessing, avoid the risk of handing valuable master key sets to third parties and guide the EMV issuance process from end-to-end need the appropriate infrastructure required to manage EMV keys, which should effectively address the following four functions:

1. Generating Keys

   Hardware security modules (HSMs) in key management systems have integrated sophisticated random number generators in order to generate a number to act as a cryptographic key. Card Keys and Application Keys are generated and safeguarded by different business entities. Ideally, Card Keys are generated by the card issuer and securely transported to the card manufacturer. Application Keys are ideally generated by each of the application owners, which might include a retailer, an internet certificate authority, and the issuer's EMV debit/credit application owner. Once the keys are generated and stored in an encrypted state, within a key vault for future reference, they need to be securely communicated and transported to the personalization service bureau.

2. Importing and Exporting Keys

   Card Keys provide a level of security to prevent unauthorized manufacturing or issuing of valid cards. The use of Card Keys requires close coordination between the card manufacturer and the issuer. When a batch of cards is ordered from a card vendor, the issuer typically provides a confidential key. The card vendor places the key on the card IC, which prevents further access to the IC, unless that key is submitted first. Depending upon the type of smart card operating system and the type of applications placed on the card, there may be numerous Card Keys for a single card.

   Application Keys are the technology that enables the security and independence of multiple applications on a single smart card. To access an application, the correct authentication request must be submitted to the card IC. Application Keys are used to generate this authentication request. Each application may have one or multiple key values, attributes and key versions, often referred to as key sets or key profiles. A vital part of the smart card issuance process is the management and secure storage of these key profiles. Managing the key profiles consists of identifying the appropriate keys required for each card and each application on the card, and then providing the ability to generate, import, and export keys. This process requires the use of an HSM to prevent keys from being compromised.

3. Distributing/Transporting Keys

   To support the use of card and application keys, a process must be in place to securely transport the keys between the business entities involved.

   This process requires another type of key, referred to as a Key Encrypting Key (KEK). A KEK is a key that is known by two business entities and used to encrypt confidential information shared between these entities. When working with smart cards, a KEK is used to encrypt the card and application keys for secure transport. The initial KEK is shared through a similar manual exchange process as the one described above. Once a KEK is established between entities, it can then be used repeatedly for encrypting keys that are sent electronically.

   Private and public key pair technology provides yet another method of key transport that eliminates the need to pass the KEK manually between entities. Instead, a public key is shared between the two entities that must be combined with the private key of the other party in order to decrypt the transmission.

4. Protecting Keys

   Keys must be accessible in real time, online, and are often stored within operational systems. To store these keys securely, the keys are usually encrypted by separate keys. This raises the issue of robust protection of the Key Encryption Keys (KEK). This cycle can go on for many levels of protection, creating a hierarchy of keys. Regardless of the number of layers of encryption that are applied to protect operational keys, the KEK must be stored somewhere. For more technical information on how this would look in practice, check out this paper's appendix.

Conclusions

While key management and data preparation for EMV require additional advanced planning and are more complicated than they are for magnetic stripes, issuers should strive to perform these tasks themselves rather than outsourcing in order to maintain control of cardholder data and, even more importantly, the associated cryptographic keys. With an ever-expanding number of keys to manage, the consequences of misappropriation by a third party continue to grow, and risk mitigation is essential. The potential cost-savings, better flexibility and control over an issuer's card personalization service bureau make keeping EMV data preparation in-house something that every payment card issuer should consider.

Appendix: Technical Addendum

I. Participants in EMV Smart Card Issuance and their roles

Issuers own the cardholder relationship, and decide which applications go on the card. However, first they must select a **Card Manufacturer** who embeds the IC component(s) into the plastic card and performs initialization and security operations.

Who receives the cards from the card manufacturer depends on how much of the issuing process will be performed by the issuer. Because of the sensitivity of Master Keys and cardholder data and keys, we recommend that Card Issuers perform their own data preparation; however, this and other tasks can be outsourced to a secure personalization bureau.

The **Certification Authority (CA)** generates the Issuer Public Key (PK) Certificates in response to requests from the Card Issuer and maintains a database of these certificates.

Card Production includes several tasks that the Card Issuer may perform internally or outsource to one or more secure bureaus. These tasks include:

- **Data Preparation**: Compiles the application and card profiles, keys and certificates, and cardholder data from several sources, and bundles this information into a single personalization file for the production of the cards.
- **Personalization**: Performs the production processes of embossing, magnetic stripe encoding, image printing and IC chip personalization of the physical cards they receive from the Card Manufacturer, prior to the start of the issuance process to the cardholders. Here the production process of embossing, magnetic stripe encoding, image printing and IC chip personalization is performed. The cards are received from the Card Manufacturer by secure courier and protected by a cryptographic key.

II. Primary Components of EMV Card Personalization

These are the data elements, keys and payment application parameters that need to be defined, generated and merged into the card personalization data file:

- Card keys provide access to the secure memory of the IC chip
- Application keys provide access to the payment application (e.g., Visa VSDC, MasterCard M/Chip)
- Issuer certificates:
  - Used to generate the secure RSA key pair
  - Securely sign information
- EMV Payment Application Parameters
- Standard Magnetic Stripe and Emboss data

III. Key Management Responsibilities

The Card Issuer, Payment Scheme Certification Authority, Card Manufacturer and Personalization Bureau each have distinctive key management roles that must be well-coordinated to execute a successful card issuance program.

The Card Issuer (Bank, Credit Union, Retailer, etc.)

The card Issuer's data preparation operation is responsible for the following tasks related to keys and certificates:

- Generate and integrate Local Master Keys (LMK and ZMK)
- Create and distribute Key Encrypting Keys (KEKs) to other issuance entities
- Send an Issuer PK certificate request to the payment scheme (e.g., Visa/MasterCard). This requires the creation of the Issuer Public Key Pair and the self-signed Issuer PK Certificate, as an essential part of the Card Issuer request to the Payment scheme CA for the Issuer PK Certificate.
- Receive the Issuer PK Certificate from the payment scheme and store it in the Card Issuer's key vault.
- Generate unique ICC PK pairs and the ICC PK Certificate for Dynamic Data Authentication (DDA) applications only.
- Create Initial Card Manager Master Key (KMC) for the Card Manufacturer
- Create Final Card Manager Master Key (CMK) for the Personalization Bureau
- Transmit production files to the Personalization Bureau using a shared KEK
- Maintain Authentication (AC) keys used to sign transactions and warehoused by the Issuer for verification that the correct card approved the transaction. This is used for non-repudiation purposes. Typically the AC is a double- length 3DES key.
- For the purpose of modifying EMV parameter settings post-issuance, Secure Messaging Keys for integrity/MAC (SMI), and confidentially/encryption (SMC) are utilized. Typically, the SMI and SMC are double length, 3DES keys diversified by the primary account number (PAN) and PAN sequence number (PSN).

The Certification Authority (CA)

The CA (e.g., Visa/MasterCard) is responsible for the following key management tasks:

- Generate Issuer PK certificate in response to the Issuer's request
- Receive and backup the EMV Master Derivation Key (MDK)

The Card Manufacturer

The card manufacturer is responsible for the following key management tasks:

- Receive the KEK from the Card Issuer. If the Card Issuer generates the KMC they will need to send it to the Card Manufacturer encrypted with the KEK.
- Derive the three Initial Card Manager Derived Keys from the KMC
- Enable card with the use of the derived keys

- Generate Card Transport Keys to protect the cards during shipment. The Card Issuer's personalization systems must submit the Card Transport Keys to the cards before they can be personalized.

The Personalization Bureau

The personalization bureau is responsible for the following key management tasks:

- Generate and integrate Local Master Keys (LMK and ZMK)
- Receive and use the KEK from Data Preparation for receipt of the CMK and card production files. If data preparation and card issuance are performed in the same secure facility this step can be avoided. However if the Card Issuer wants a P3 file generated, the KEK is used to encrypt the keys from the Data Preparation operation
- Derivate the three Final Card Manager Derived Keys from the CMK.

IV. Configuring the Personalization System for EMV Card Issuance

The system configuration for EMV is provided in Figure 1 below. It depicts an in-house developed solution for EMV card issuance using Prime Factors' Bank Card Security system for data preparation and key management. Following the diagram is an explanation of the requirements for key generation and management by each of the actors at their respective steps in the personalization process.

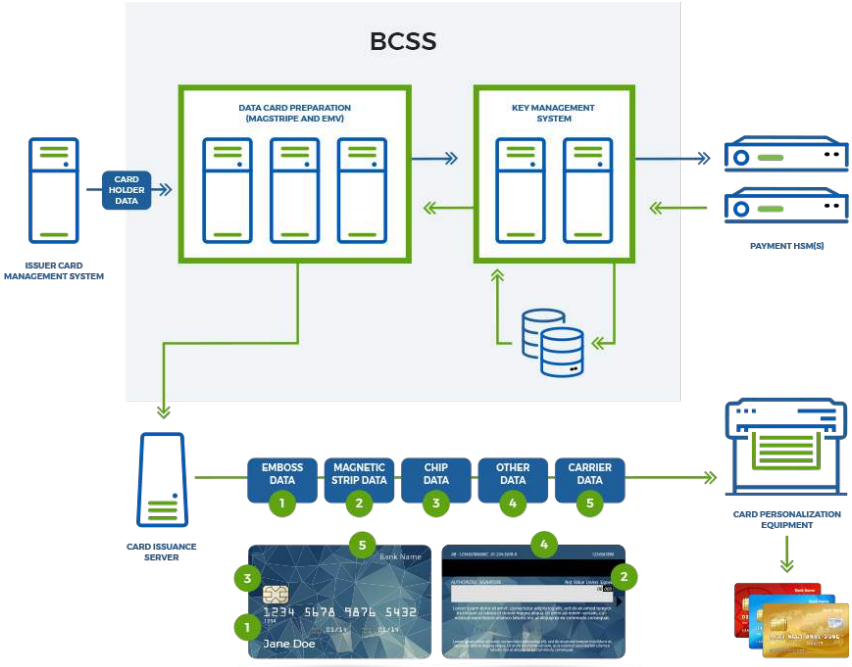

Figure 1: EMV System Configuration Using Prime Factors' Bank Card Security System

The Card Manufacturer

The Card Manufacturer needs a key management application that is supported by an HSM (hardware security module) and Key Vault in order to perform the Card Manager key derivation operations, as identified earlier in this Whitepaper, and to create the required Card Transport keys.

The Card Manufacturer also requires a card personalization device so that card initialization and enablement can be completed prior to shipping cards to the personalization bureau.

The Card Issuer

The Card Issuer maintains the databases that contain the cardholder data and information required for card production. The Data Preparation and Personalization Bureau operations are detailed below.

Data Preparation Operation

The Data Preparation Operation makes use of software application products to determine what information is required for card production and to create and gathered from various sources to build a single card production file.

An application is needed to generate the Card Program to be used from the Card Profile and Application Profile(s) selected by the Card Issuer. Another essential output of this application is the Key Profile, which establishes all of the cryptographic keys and certificates required in the card.

A Key Management application, operating in conjunction with its HSM and Key Vault, is used to create, derive, import/export and store keys and certificates required for personalizing EMV cards. For applications that require card-unique public key pairs (such as dynamic off-line data authentication), a public/private key pair generation software application, with one or more dedicated HSMs, is utilized to generate and warehouse public key pairs for card batches in order to maximize card production performance.

A data preparation software application gathers all the card and application data, cardholder data, keys and certificates required to produce a personalized card, and builds all of this data into a single card production file for each card.

Personalization Bureau

A Card Issuance software application accepts the card production file and using the proper card personalization device support from a large library of personalization devices, performs embossing, image printing, magnetic stripe and chip personalization operations.

Because cryptographic operations are required to support this process, companion key management software applications are utilized with attendant HSM and Key Vault facilities.

The Payment Scheme CA

The payment scheme CA possesses Key Management/HSM/Key Vault facilities in order to generate Issuer PK Certificates.