The Smarts Behind EMV Smart Cards
Part 2 – Offline Transaction Processing

Yash Kapadia
CEO, OmniPayments, Inc.

It seems that every month comes with an announcement of another hack in which the data of millions of payment cards has been stolen. This data is used to clone credit cards and debit cards, which are then sold in the underground Internet. Is there any protection available to us to thwart such attacks?

The answer is yes – smart cards. A smart card, also called a chip card or an integrated-circuit card (ICC), includes an embedded computer chip that employs cryptographic and risk-management features. In conjunction with a smart-card POS or ATM terminal, these features are designed to thwart skimming, card-cloning, card-counterfeiting, and other fraudulent attacks.

A decade or more ago, a consortium of card issuers comprising Europay, MasterCard, and Visa (EMV) began the specification of smart cards or as they are formally known today, EMV cards. EMV card technology has been adopted by most of the countries on all continents in the world except for the United States. The United States is the laggard. Representing almost half of all payment cards and terminals in the world, the U.S. still runs its payment-card services on outdated magnetic-stripe technology.

However, this is about to change. The U.S. payment-card industry has mandated that all merchants be EMV-compatible by October, 2015 (except for gas stations, which have until 2017) or face a "liability shift." If a merchant does not process at least 75% of its transactions through an EMV-enabled terminal (whether via chip-cards or magnetic-stripe cards) and accepts a disputed or fraudulent card payment, the merchant will be liable for the transaction rather than the issuer.

Most card-payment networks include one or more HP NonStop servers. It is therefore important that the NonStop community understand smart-card technology, which is becoming an important component in all financial networks. In this article, we describe how smart cards add significant security to payment-card transactions. Part 1 in the September/October issue of The Connection covered the methods for authorizing EMV transactions online with the issuing bank. In Part 2, we discuss the procedures for securely authorizing EMV transactions offline without direct issuer involvement.

Offline Transactions

The processing of an EMV card transaction is shown in Figure 1. It comprises several steps, with interaction between the card, the terminal, and the issuer. Processing time for an EMV transaction is comparable to that for a magnetic-stripe transaction, where communication delays account for the majority of the time.

EMV transaction processing begins with some preliminary steps that help determine whether the transaction should be handled online with the issuer or offline with no issuer involvement. Once this decision has been made, processing splits into two distinct flows – one for online transactions and one for offline transactions. Part 1 of this article described the common processing flow and the online processing flow. Part 2 describes the offline processing flow.

Most transactions will be processed online, sending the transaction data to the issuer for authorization. However, in some cases, a transaction may be processed offline with no issuer involvement. This can take place if there is no communication link (for instance, terminals used in airplanes to sell food, drinks, and other items), if the communication link between the terminal and the issuer should fail (allowing a retailer to continue to service customer payments at its own risk), or for very small transactions.

The processing of an offline transaction as shown in Figure 1 is a bit more complicated than the processing of an online transaction but follows similar steps.
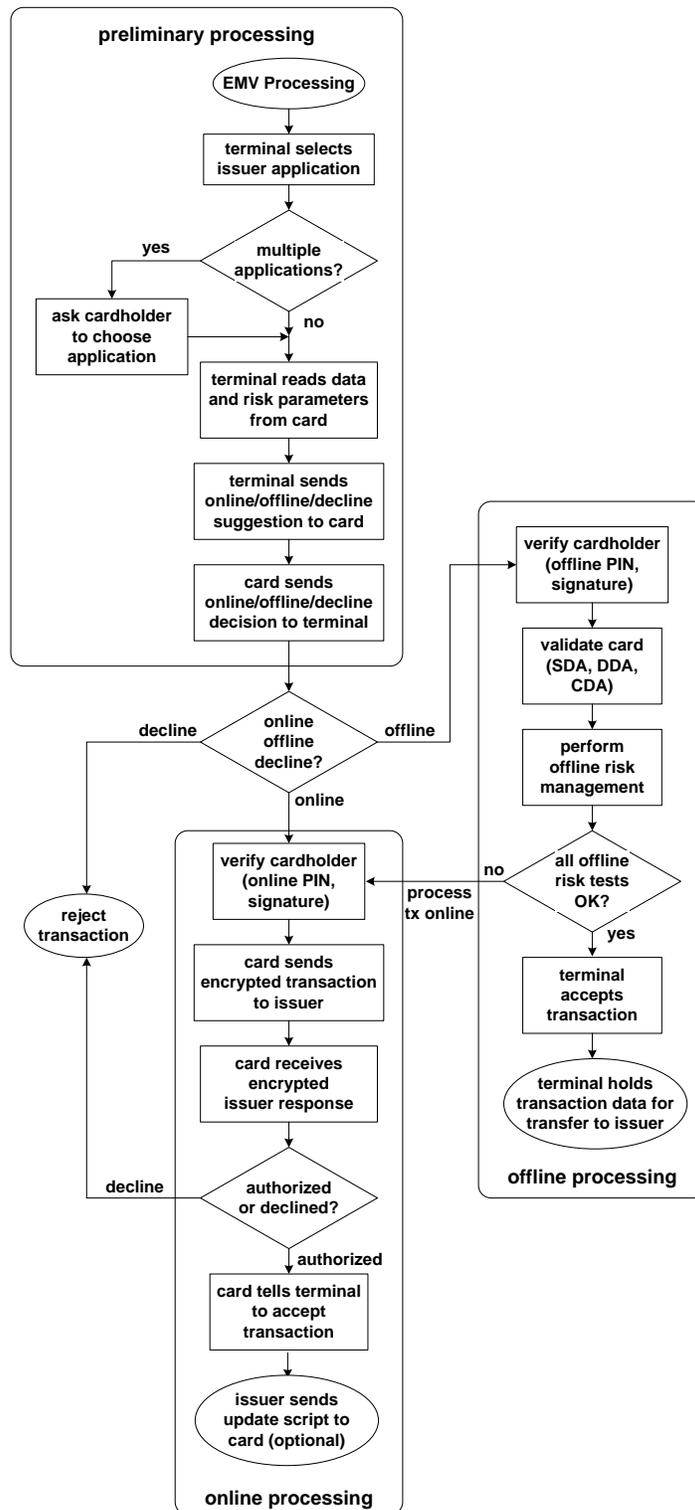

Figure 1: EMV Processing Flow

Issuer Parameters Stored on the Card

The processing of online and offline transactions is controlled by parameters stored on the card by the issuing bank. These parameters are described by a three-byte bit-encoded designator and include:

Byte 1: Card Data Input Capability	Byte 2: Cardholder Verification Method (CVM)	Byte 3: Security Capability
Manual key entry Magnetic stripe IC (integrated circuit) with contacts	Plaintext PIN for ICC verification Enciphered PIN for online verification Signature (paper) Enciphered PIN for offline verification No CVM required	SDA DDA CDA (These capabilities are described later)

Table 1: EMV POS Terminal Capabilities

Cardholder Verification

As with online transactions, if the transaction is to be processed offline, the person presenting the card must be verified as the legitimate cardholder. Offline cardholder verification is also accomplished via the Cardholder Verification Method (CVM) that the issuer has specified in its parameters stored on the card (Table 1). Four methods can be used for offline cardholder verification:

- offline encrypted PIN
- offline plaintext PIN
- signature
- no CVM

The methods selected by the issuer may be arranged in priority order, or they may be selected according to other transaction parameters. For instance, a transaction at an attended POS terminal such as in a store may require both a PIN and a signature. An ATM may require a PIN but no signature. A terminal with no PIN pad may require just a cardholder signature. A small transaction may require no cardholder verification.

If an encrypted PIN is selected, the cardholder enters his PIN into the terminal's PIN pad. The terminal encrypts the PIN with the card's PIN public key and sends it to the card. The card decrypts the PIN with its PIN private key and compares the PIN entered by the cardholder to the PIN value stored in its secret data. If the PIN is wrong, the terminal is informed. According to a PIN counter, the cardholder may be given additional opportunities to enter his PIN. If he reaches a specified limit, the transaction is rejected. The card is blocked and can no longer be used.

If a plaintext PIN is selected, the process is the same as for an encrypted PIN except that the PIN entered into the PIN pad by the cardholder is sent to the card unencrypted.

Card Validation

An extra step required for offline transactions is that the terminal must validate the card to ensure that the card is not counterfeit or is not a clone of another card. For online transactions, card validation is the responsibility of the issuer.

Three techniques for offline card validation provide incrementally improved security – SDA, DDA, and CDA, as described next. The technique to use is specified in the issuer's parameters stored on the card (see Table 1). Typically, DDA or CDA is selected.

Static Data Authentication (SDA)

Static Data Authentication proves that the card is a valid card prepared by the issuer. Included in the static data that the terminal reads from the card is the card's Static Application Data, encrypted with the issuer's private key. This cryptogram includes all of the static data that the issuer has entered into the card at the time the card was produced (PAN, cardholder name, public keys, Application IDs, etc.)

The terminal also reads the issuer's public key from the static data on the card. The terminal decrypts the Static Application Data cryptogram with the issuer's public key and compares the signed static data to the static data that it has read from the card. If the data sets match, the terminal has verified that the card was the card prepared by the issuer. It the data doesn't match, the transaction is rejected.

SDA validates the card's authenticity, but it does not prevent cloning. If an attacker somehow manages to clone an EMV card, the static data including its cryptogram will still pass the SDA test.

Dynamic Data Authentication (DDA)

Dynamic Data Authentication adds cloning protection to the counterfeit protection afforded by SDA. The key to DDA is that the card carries variable data that changes with each transaction. For instance, a transaction counter is incremented with each card insertion into a terminal.

For DDA card validation, the card encrypts its variable data with its private key and sends this dynamic data cryptogram to the terminal. Using the card's public key, the terminal decrypts the variable data contained in the cryptogram and compares it to the variable data that it has read from the card. If the data sets match, the terminal knows that this data has come from the original card and not from a clone because the clone would not have the card's private key (a secret data item that will be erased if an attempt were made to access it).

Furthermore, an attacker cannot simply add its own card public key and private key to the card to fool the terminal. The terminal will discover that the attacker's public key is not a valid key when it checks the key against the key's presumed Certificate Authority, as found in the card's static data.

Thus, between the SDA and the DDA, the terminal can determine that the card is neither counterfeit nor a clone. It is a valid card.

Combined DDA/Application Cryptogram (CDA)

SDA and DDA do not protect against an unlikely but sophisticated attack known as a *wedge attack*. In a wedge attack, a real EMV card is inserted into the terminal so that the SDA and DDA validation tests are passed. The attacker then substitutes the real card with a device that acts like the card but is under control of the attacker. The attacker can force the acceptance of a transaction that the card otherwise would have declined.

To protect against this kind of attack, an application cryptogram (AC), generated by the card's private key, is included with the SDA and DDA cryptograms. The AC's purpose is to inform the terminal of the card's ultimate decision as to whether to process the transaction online, to process the transaction offline, or to decline the transaction (see the section entitled *Card Action Analysis* in Part 1 of this article). The wedge attacker cannot generate a valid AC because it does not know the card's private key.

<u>Offline Terminal Risk Management</u>

For offline transactions, the card and the terminal must cooperate to manage the risk of a transaction, a function performed by the issuer for online transactions. This function is executed under the control of a variety of risk parameters stored on the card. These parameters include a lower floor limit, an upper floor limit, an offline transaction-count limit, and an offline amount limit.

Except for unusual conditions, a transaction can be authorized offline only if its amount is below the lower floor limit. For instance, if the lower floor limit is five dollars, only transactions that are at or below five dollars can be authorized offline. Note that if the lower floor limit is zero, all transactions must be authorized online.

An exception to this rule occurs if the communication between the terminal and the issuer is interrupted. In such an event, transactions can be authorized offline as long as they are below the upper floor limit. The upper floor limit allows retailers to continue to service most of their customers if their POS terminals should go offline. In this case, the merchant is typically responsible for disputed or fraudulent transactions; but it is a risk most retailers are willing to take to maintain customer satisfaction.

The issuer can limit the number or amount of offline transactions that can be authorized before the terminal must go online with a transaction. This is accomplished via the offline transaction-count limit and the offline amount limit. This restriction limits the use of the card to fraudulently make unlimited, small, offline purchases that are below the lower floor limit.

A further protection against the offline use of a fraudulent card is that the card randomly forces online authorization for a transaction that otherwise qualifies for offline authorization.

<u>Offline Transaction Authorization</u>

If all tests prove positive – cardholder verification, card validation, and risk management, the transaction can be authorized offline. The card informs the terminal via a TC cryptogram (see the section entitled *First Card-Action Analysis* in Part 1 of this article) to authorize the transaction. If a signature is required for an authorized transaction, the cardholder is asked to sign a copy of the transaction receipt.

If any test proves negative, the card must be authorized online by the issuer.

The terminal stores the transaction data. According to rules established by the issuer, the terminal will periodically send batches of offline transaction data to the issuer. In the case of a communication failure, this will typically occur as soon as communication between the terminal and the issuer is restored.

Protections

In addition to the SDA/DDA/CDA protections described above for offline transactions, EMV technology provides several other protections.

Swiping

The data from the card cannot be read by an attacker because all data transfers between the card and the terminal are protected by the card's secret private keys.

Cloning

Even if card data could be compromised, it cannot be used to clone a magnetic-stripe card, which will still be in use for some time to come. This is because the cloned card data will not include the CVC1 code that needs to be written in the magnetic stripe. Without the proper CVC1 code, a magnetic-stripe transaction will be rejected.

Another protection against cloning is the transaction counter. Every time a card is inserted into a terminal, its transaction counter is incremented. If a cloned card were also being used, the issuer would note that the transaction counters were out of synchronization and would disable the card account number.

Counterfeiting

One concern is that an attacker could obtain a batch of blank EMV cards and a personalization machine and create what appear to be valid cards for offline transaction purposes. To protect against this, every batch of blank cards has embedded in the cards a unique symmetric key known only to the issuer. Therefore, only the issuer can create usable EMV cards.

Card-Not-Present-Fraud

For Internet transactions, there is no terminal to read the card and to apply the risk management tests. To compensate for this, a private handheld reader may be required by some online merchants. The customer has his own private handheld reader. When he wants to make an Internet purchase, he inserts his EMV card into his reader.

The reader generates a one-time unique passcode, which the customer enters into a field provided on the merchant's checkout page. This passcode verifies to the issuer that the customer is in possession of the EMV card being used.

Using Smart Cards at Dumb Terminals

Until all POS terminals have become EMV terminals and magnetic stripes have been eliminated from smart cards, there will always be cases in which smart cards with magnetic stripes are used at "dumb" POS terminals that read only magnetic stripes. In these cases, all the vulnerabilities of magnetic stripes that we deal with today still exist. A skimming device or skimming malware can send the card data and PIN to an attacker, who can clone the card as a magnetic-stripe-only card that can be used at POS terminals whether they are EMV-capable or not. This is because, for a while to come, all EMV POS terminals must still be able to process magnetic-stripe cards.

The EMV Specifications

The first EMV specifications were developed by a consortium comprising Europay, MasterCard, and Visa – thus the name EMV. The primary members of the consortium now include MasterCard (which acquired Europay), Visa, American Express, Discover, JCB (Japan), and UnionPay (China). Most other payment-card organizations, banks, major merchants, payment processors, and other industry stakeholders support the ongoing specification effort.

The EMV Specifications are contained in four books:
- Book 1: Application Independent ICC to Terminal Interface Requirements
- Book 2: Security and Key Management
- Book 3: Application Specification
- Book 4: Cardholder, Attendant, and Acquirer Interface Requirements

The EMV Specifications can be obtained from the EVMCo web site,
http://www.emvco.com/specifications.aspx.

The OmniPayments Financial Transaction Switch

OmniPayments (www.omnipayments.com) from Opsol Inc. (www.opsol.com) is an HP NonStop-based financial transaction switch that interconnects POS terminals, ATMs, acquiring banks, and issuing banks via any of the various financial transaction networks. OmniPayments supports all features required to process EMV smart-card transactions, from support of EMV POS terminals and ATMs to the protocols

required to communicate with the issuing and acquiring banks. OmniPayments is currently handling EMV transactions with its international banking installations and is ready to handle these transactions with U.S. systems as EMV technology takes hold in the United States.

OmniPayments architecture is based on modern Service Oriented Architecture (SOA). SOA enables new functionality to be easily added to OmniPayments to meet specific needs of its customers. The core of OmniPayments is a set of Business Logic Modules, or BLMs. Each BLM is tasked with providing a specific service for OmniPayments. For instance, OmniATM controls ATMs, OmniPOS controls POS devices, Transaction Screening offers preauthorization services, and OmniAuth provides stand-in authorization services.

A set of adapters connects the external entities to which OmniPayments must connect to the BLMs. Acquirer adapters are supplied for both EMV and non-EMV ATMs, POS devices, IVR systems, the Internet, and bank tellers. Issuer adapters are provided for local host bank communications and for the variety of financial interchange switches with which OmniPayments must interface.

Traffic between acquirer BLMs and issuer BLMs is routed via OmniDirector. OmniDirector is a rules-based routing engine that forwards On-Us transactions to the bank's core systems and Not-On-Us transactions to the appropriate interchange switch. It provides format conversion between different message protocols and is responsible for much of OmniPayment's logging functions. OmniDirector also manages the failover/retry mechanisms in OmniPayments.
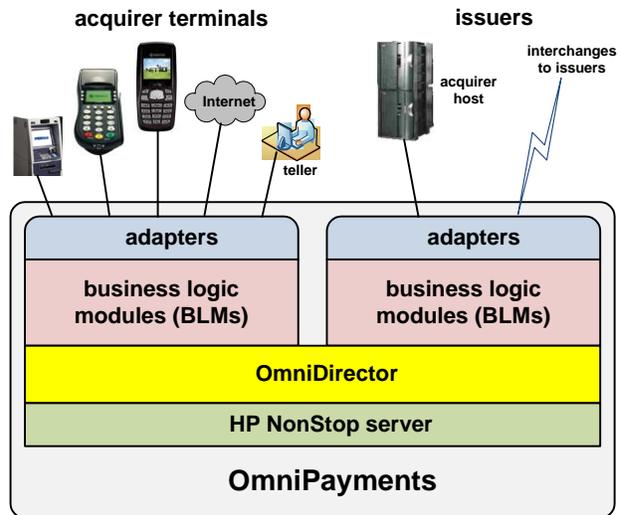
Figure 2: The OmniPayments Financial Transaction Switch

OmniPayments provides complete logging of all transactions. The logs contain the transaction information needed at the end of each day for clearing and settlement. It is this processing function that transfers funds from the card-issuing banks to merchant accounts held by their acquiring banks to reflect the day's sales activities.

OmniPayments is fault-tolerant. Running on an HP NonStop server, all processes are persistent and are automatically restarted should they abort. All database functions such as logging, card parameters, and so on are maintained by a NonStop SQL/MP relational database.

With successful implementations at many customer sites, OmniPayments is just one member of the Opsol family of solutions for the financial industry. Opsol Integrators specializes in NonStop mission-critical applications and is HP NonStop's largest system integrator.

Summary

Magnetic-stripe cards will become a thing of the past as EMV technology is adopted worldwide. This is almost the case now in countries around the world except for the United States. However, within a few years, it is expected that the U.S. will catch up.

Magnetic-stripe cards have been proven over and over again by major hacks to be terribly insecure. Their data is easy to skim, the cards are easy to clone, and cloned cards have an active market in the underground Internet.

EMV technology provides strong protection against card-skimming, card-cloning, card-counterfeiting, and man-in-the-middle attacks. Once EMV technology is universally accepted, our card-payment systems will

become significantly more secure. The OmniPayments financial transaction switch supports EMV POS terminals and ATMs and the EMV protocols for communication between EMV terminals, acquirers, and issuers. OmniPayments brings the entire suite of EMV security protection to an organization's financial switching network.

It is said that hackers are smarter than security professionals. Whenever a security vulnerability is patched, hackers rapidly find a way around it. However, it will take an extremely sophisticated hacker to break through the protective barriers of EMV.