INTRIX TECHNOLOGY

EMV and Chip Cards – Key Information On What This Is, How It Works and What It Means

Document Purpose

This document is intended to provide information about the concepts behind and the processes involved with EMV Chip credit cards and to help the reader understand how this new technology works. Common questions about EMV technology are addressed here. The information in this document is relevant to all parties, including Independent Software Vendors, Merchants, Consumers and others.

Contents

Overview Of EMV

What is EMV? ICC? Chip And Pin? Etc…?

There are many terms being used in relation to the topic, but they all boil down to use of a credit card that has a circuit chip embedded in it. This chip is called an Integrated Circuit Chip, hence the term "ICC". This technology was developed via a joint effort between EuroCard, MasterCard and Visa, hence the term "EMV". Cards with this chip will perform some authentication of the person presenting the card before an actual authorization request occurs. Cardholder authentication may include the use of a PIN, hence the term "Chip And Pin". The PIN is not always applicable; sometimes a signature is used, hence the term "Chip And Signature". They all boil down to the use of cards with an embedded chip, with that card being inserted into a card reader device.

What does an EMV card look like?

The EMV card has a chip as shown here:

What is the difference between EMV and "Contactless" cards?

Some card providers are providing "contactless" cards that can be waved over a card reader device. This technology is branded by the card bands with names like "WavePay", "PayPass" and others. These cards use RFID (Radio Frequency Identification) technology, which involves a small radio field emanating from the card providing the card data to a reader that is very close. The radio field is powered by a battery and antenna on the card, or by an antenna at the merchant location . These cards will have a icon on them that indicates they are radio-frequency enabled, as indicated by the red circle here:

An RFID card must be near an antenna and reading device, while an EMV card must actually be in physical contact with a reader. There is some concern that RFID cards are vulnerable to data theft by reader devices passed near a consumer's wallet, where the RFID card is stored. Sleeves are available for these cards to prevent them from responding to read requests unless they have been removed from the sleeve by the consumer, when paying for a purchase. EMV cards are not vulnerable to this scenario because they do not emit any data without being in physical contact with the reader terminal.

Why is EMV "more secure" than traditional credit cards?

There are several key factors that make an EMV card more secure than a traditional credit card with only a magnetic stripe. Traditional swipe transactions involve a terminal reading track data from a magnetic stripe. Once the data is read by the terminal, it is in memory in the terminal. If the terminal is encrypted (Point to Point encryption, also called P2P), then the data will be encrypted when transmitted by the terminal to the next item in the cycle. Data in memory on the terminal can be stolen. Data transmitted to a POS from an unencrypted terminal becomes data in memory on the computer, and can be stolen. If the track data can be stolen from the memory, then a counterfeit card can be created.

EMV cards work differently. The track data is not part of the transaction, even if the EMV card also has a magnetic stripe on it. The terminal and the chip on the card interact. These interactions, if stolen from memory, don't provide enough information to create a counterfeit chip for a counterfeit card. Data transmitted from the terminal to a POS is a small subset of what needs to be on a chip to make a counterfeit. The POS system (or gateway or processor) will never receive enough from the terminal to recreate the content of the chip on that card.

Even if someone were able to steal enough information to create a counterfeit card, there would be issues using the counterfeit. EMV cards have a chip that gets updated when a transaction is performed. One of the data elements is a transaction counter, which stores how many transactions have been run using that card. This counter increments by one each time a transaction is processed with that card. If someone were to steal all the data and make a counterfeit EMV card, the counter would be set to whatever it was when the data was stolen. As soon as the original card is used again, that number changes. The counterfeit card is almost certain to have the wrong count. This number is submitted with each transaction authorization request, so if the counter number is wrong, the issuing bank will know it is a counterfeit.

Since magnetic stripes on traditional cards are static and never change, creating a duplicate merely requires obtaining the information from the original.

What happens during an EMV transaction?

An EMV transaction involves a number of steps that do not apply to a traditional "swipe" transaction. The first distinction is that the card remains in the terminal device for a longer period, just like it used to be at the ATM (where a person inserts their card, and it stays in the machine until all transactions are completed). While the card is inside the terminal, a dialog occurs between the terminal and the chip on the card to perform some steps to verify the cardholder identity. This is called "offline verification".

If that is successful, then the terminal applies logic specific to the merchant to decide if it should proceed with a transaction authorization. This is called "Terminal Risk Management".

The terminal then proceeds with an outbound connection for an authorization, and this outbound connection may be to a processor front end or an internet payment gateway or to a POS system or other application. The request will contain data elements that are not present in non-EMV transactions. The authorization request is propagated to the Issuer. The issuer responds and may include in the response additional authentication information. The response is propagated back to the originating terminal. If the response includes additional authentication information, then this data (along with the transaction result) is sent to the chip on the card, which is still inside the terminal.

The chip receives the result and makes a final decision to complete the transaction, or to decline it. If the chip elects to not complete the transaction, then a reversal will be initiated to the payment processor.

Who is protected from what during an EMV transaction?

Since there is not any track swipe reader involved, the track data is not read from the card by the terminal. As a result, track data cannot be stolen during an EMV transaction. In theory, the chip data could be stolen, but as yet, no one has managed to counterfeit a chip card. Therefore one main beneficiary of protection during this type of transaction is the consumer, whose card cannot be "counterfeited" if the terminal is compromised. The issuing banks currently are accountable for transactions they approve. Therefore, reducing the likelihood of the transaction being originated using a counterfeit card benefits the issuing bank. One can argue that it is in everyone's interest to make it pointless to hack a Point of Sale (POS) system because the data available cannot be used to make a counterfeit card. However, to date, consumers are not clamoring for availability and use of chip cards.

The table below identifies parties involved in credit card processing, the benefits of EMV adoption to each of those parties, and the current stance of those parties on the topic of EMV adoption.

Party	**Benefit**	**Current Stance / Concerns**
Consumer	Reduced likelihood of having card counterfeited	US consumers are just beginning to demand chip cards
Issuing Bank	Reduced likelihood of approving a counterfeit transaction, resulting in money savings	Reluctant to issue expensive EMV cards in US, since they can't be used most places anyway; Issuing has begun by some banks

Merchant	Reduced likelihood of receiving a counterfeit card; Reduced likelihood of being the target of a Malware Breach attack	Most don’t want to spend the money on the more expensive EMV terminals
POS/ISV Developer	Reduced likelihood of being the target of Malware Breach attack	Each EMV Reader integration is unique and is resource intensive; Certifications are challenging, each processor requires 4 certifications (one for each card)
Gateway	Reduced likelihood of being the target of a malware attack targeting track data if EMV is supported	Certifications are challenging, since each processor requires 4 certifications (one for each card brand); EMV support will be required to remain in the retail game
Processors	Reduced likelihood of being the target of a malware attack targeting track data if EMV is supported, but EMV support implementation was mandated in 2013	They’re ready…
Acquiring Bank	EMV itself does not benefit the acquiring banks much, but due to the Risk Shift, there is an artificially created benefit of reducing financial responsibility for fraudulent transactions	Not looking forward to Risk Shift; Pushing merchants to obtain EMV capable terminals; Will push risk shift to merchants
Terminal Developer	Reduced likelihood of being the source of data for counterfeits	Many merchants still want terminals with swipe only, so these are still being produced

Visa has created an “incentive” for Acquirers to adopt EMV by changing the entity that bears liability for a fraudulent card-present transaction. Starting in late 2015, the entity that holds this risk will shift from Issuers (who carry the risk now) to Acquirers if the transaction involved an EMV card but the transaction did not utilize it. Acquirers will pass this risk on to their merchants. Therefore, performing an EMV transaction ensures fraud liability remains with the Issuer, but this is an artifact of rules changes, not the EMV technology itself.

Keys Points Of Interest

Key Points For Merchants

There are a number of key factors of which merchants should be aware.

Effective October, 2015, the rules of who accepts the risk for fraudulent retail transactions will change to be the same as the rules for ECommerce and Mail Order Phone Order (MOTO) if the transaction was not initiated using EMV. Currently, a retail, swiped transaction that is approved by the card issuer will be funded by that issuer if the card is found to be fraudulent. With the risk shift, that risk moves to the acquiring bank (the merchants bank) unless the merchant used an EMV terminal for the transaction. Acquirers will pass along the risk ownership to the merchant when the risk shift goes into place, so the merchants will be responsible for those fraudulent charges.

EMV is not relevant to merchants who do not perform card-present transactions. The risk-shift is deferred by one year for the Fuel industry, to 2016.

Merchants using Point Of Sale systems or other software need to check with their software providers to determine when their systems will be ready to support EMV, and what equipment those software vendors have implemented.

Consumers And EMV, Why should Consumers care?

Some consumers have expressed indifference about their card data being stolen at a retailer. However, most consumers who have actually experienced card data theft are not indifferent. Once a card is compromised, the cardholder must get a new card. Any bill pay accounts that used the compromised card must be updated to use the new card. Any products ordered on the hold card, but not yet shipped, may experience issues if the card is deactivated. There may be a time lag between when the compromised card is deactivated and when the consumer receives the replacement card, leaving the consumer without a credit card in the interim. While the consumer is not responsible for the fraudulent transactions, there are many factors that make card data theft a major inconvenience for the consumer.

A consumer using an EMV card is not necessarily protected from card data theft in the retail environment. The cards generally also have a magnetic track on the back. Many merchant locations now have EMV capable terminals, but their software (POS, etc) is not capable of using EMV. As a result, those terminals are still being used with magnetic swipe, which means track data is still being used for transaction processing.

It is important for consumers to understand that EMV technology does nothing to protect them from data theft when shopping online or making payments over the phone. EMV only comes into play when the consumer can insert his or her card into a terminal.

It is also important for consumers to be aware of what they do with their credit cards. A restaurant may utilize EMV terminals, but once the consumer hands a credit card over to a waiter, and the waiter walks away with the card to process the payment, the consumer doesn't really know what is being done with that card.

Considerations for ISV/POS Developers

Developers of systems used by Retailers are faced with a number of considerations related to EMV. Point of Sale system developers and other Independent Software System developers must decide on a system approach for EMV, determine the right partners with whom to work on that solution, implement the solution, and then, if relevant, certify with each payment processor for each card brand (Visa, Mastercard, American Express and Discover).

EMV Terminal Integrations

Software which processes credit card transactions must integrate with the terminals their customers plan to use. Some software developers integrate to one brand or even one model of terminal, since such integrations are difficult and time consuming. Terminal manufacturers have not adopted a standard interface specification. As a result, the integration to multiple terminals may mean separate and distinct development efforts.

Certification for EMV Processing

Any entity involved in processing credit card transactions must certify with the processors with whom they plan to work. With EMV, that certification process is multiplied by 4 because certifications must be done separately for

Visa, MasterCard, American Express and Discover. Each card brand uses a slightly different EMV message format, so processors require an integrator to certify the EMV message for each card brand. POS (Point of Sale) System and other ISV (Independent Software Vendor) software which is currently integrated directly to two processors for retail processing will need to complete integrations for EMV with both, and then certify 4 ways with each of the two processors.

This cost can be significantly reduced if a POS/ISV system integrates to a gateway. The gateway then takes the burden of 4 certifications per processor, while the POS vendor can offer their customers a choice in processors – any processors that the gateway offers.

EMV Middleware

Due to the complexities of EMV Terminal integrations and payment processor integrations, the EMV Middleware approach has been developed. This software application is referred to as “middleware” because it sits in between the POS system and the terminal, and would be provided by a gateway or payment processor. The POS system integrates to a middleware application running on the same computer as the POS system. The middleware communicates with the terminal, and also communicates with the gateway to obtain an authorization. This approach further simplifies the EMV implementation process for a POS system by requiring only a single integration to the middleware component.

This middleware application is performing the function of payment processing, and therefore must be PA-DSS certified.

Since the middleware is handling the card transaction processing, and the POS system is not, this approach should serve to remove the POS System from PA-DSS scope.

Additional Details

What is an Offline EMV Transaction?

EMV cards have the ability to make an authorization decision without involving the issuing bank. This means that the chip on the card, while in an EMV terminal, can authorize a purchase without connectivity to the internet, to a gateway, to a processor, etc. This functionality is intended for use when a terminal is in a location that does not have network access. The terminal must be explicitly programmed to do this.

What is P2P Encryption and What Does It Have To Do With EMV?

Point to Point Encryption, abbreviated as P2P, is the use of encryption technology to minimize the risk of a compromised system becoming the source of fraud. An encryption key is injected into a terminal or is deployed in conjunction with an application on a computer. That key is also used by the system that is on the other side of the transaction conversation, often an Internet Payment Gateway. When data is read by the terminal, such as during a card swipe, that data is encrypted before it is transmitted out. P2P encryption can help secure track data because malware that steals the transaction from memory on a computer will have only stolen encrypted data. If the system is secure enough to not store the key required to decrypt data (which it should be, or P2P is pointless), then stolen data can’t be read and can’t be used to create counterfeit cards.

Fundamentally, P2P encryption introduces to the credit card payment the same level of security that is the industry standard for PIN number handling. Recent breaches have resulted in debit card numbers being stolen, and in some cases encrypted PINs being stolen. But these breaches have not resulted in the thieves obtaining the actual PIN numbers. This is because it has long been standard for PIN entry devices to utilize encryption for the PIN once it is entered. The encryption key, required to decrypt the encrypted PIN, is not stored by the system taking payments, so decryption of stolen encrypted PINs is difficult to impossible. P2P encryption applies this same approach to the Primary Account Number (PAN) or the track data.

With EMV, P2P can create an additional layer of protection. By combining the 2 technologies, data stolen should be entirely useless. P2P encryption can also be used without EMV.

However, P2P encryption is not a requirement for EMV.

Transaction Flow Models

The diagrams below document the various transaction processing models, and how data flow for each model.

Diagram 1 – The most common retail transaction flow, in which the consumer swipes his card using a terminal at the merchant's location, and the terminal connects directly to a processor front end. In this model, there is no interaction between the terminal and a local POS system, so an Authorization Code must be copied into any POS system being used.

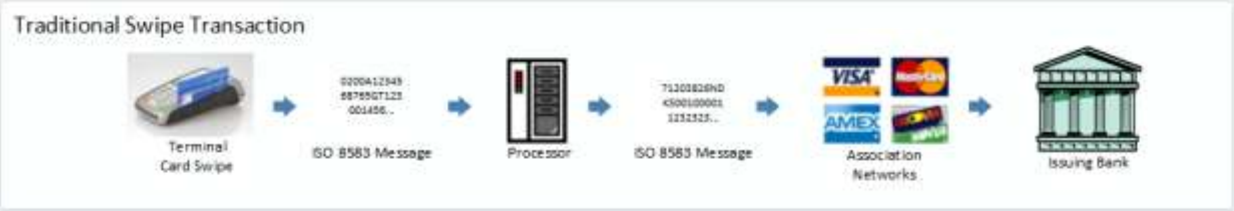


Diagram 2 – The simplest direct method for acceptance of EMV cards in the retail setting. The terminal is EMV capable, and is integrated directly to a processor front end. In this model, there is no interaction between the terminal and a local POS system, so an Authorization Code must be copied into any POS system being used.

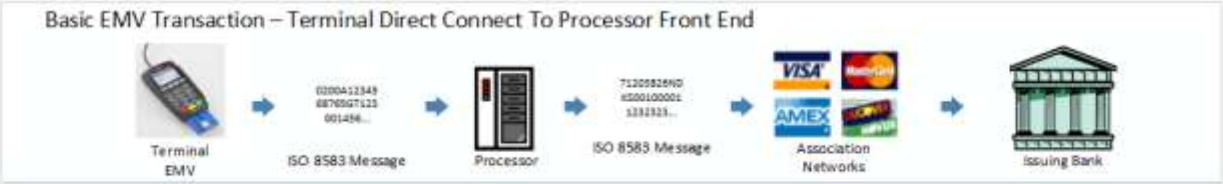


Diagram 3 – This diagram introduces a POS System, which interacts with the terminal, and also interacts with multiple processor front ends. This approach is used by many large retailers, who have a central data center through which all transaction processing flows. This model requires 4 processor integration certifications for each processor with whom the POS software will interact.

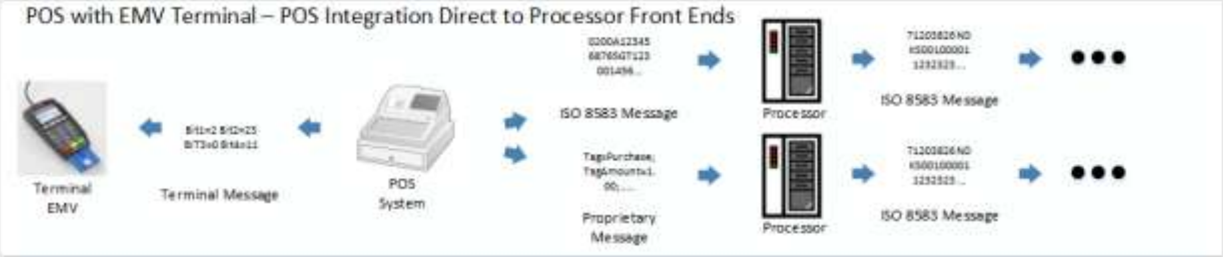


Diagram 4 – The POS System integrates to a single gateway and the gateway is integrated to multiple processor front ends. In this model, the POS vendor can allow his customer to choose from a wide variety of merchant services companies and processor front ends, without having to certify 4 times to each processor. In addition, the integration to the gateway is done using a simple SOAP API (application interface) message format, so the integration itself is much easier. The POS System still must integrate with the terminals. This approach removes the EMV Certification burden from the POS/ISV.

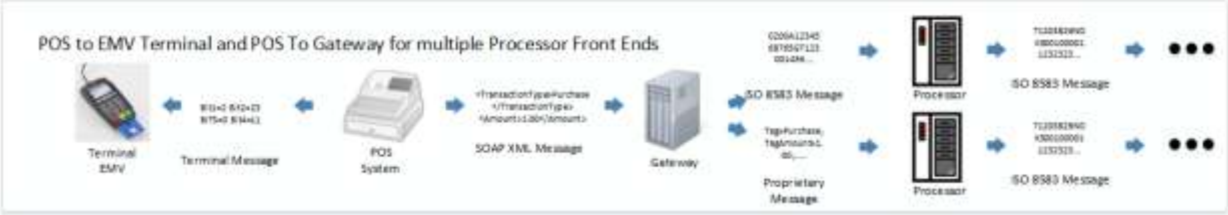
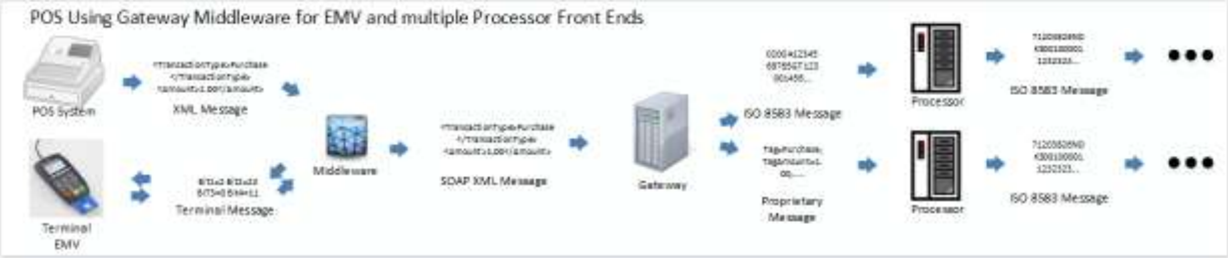


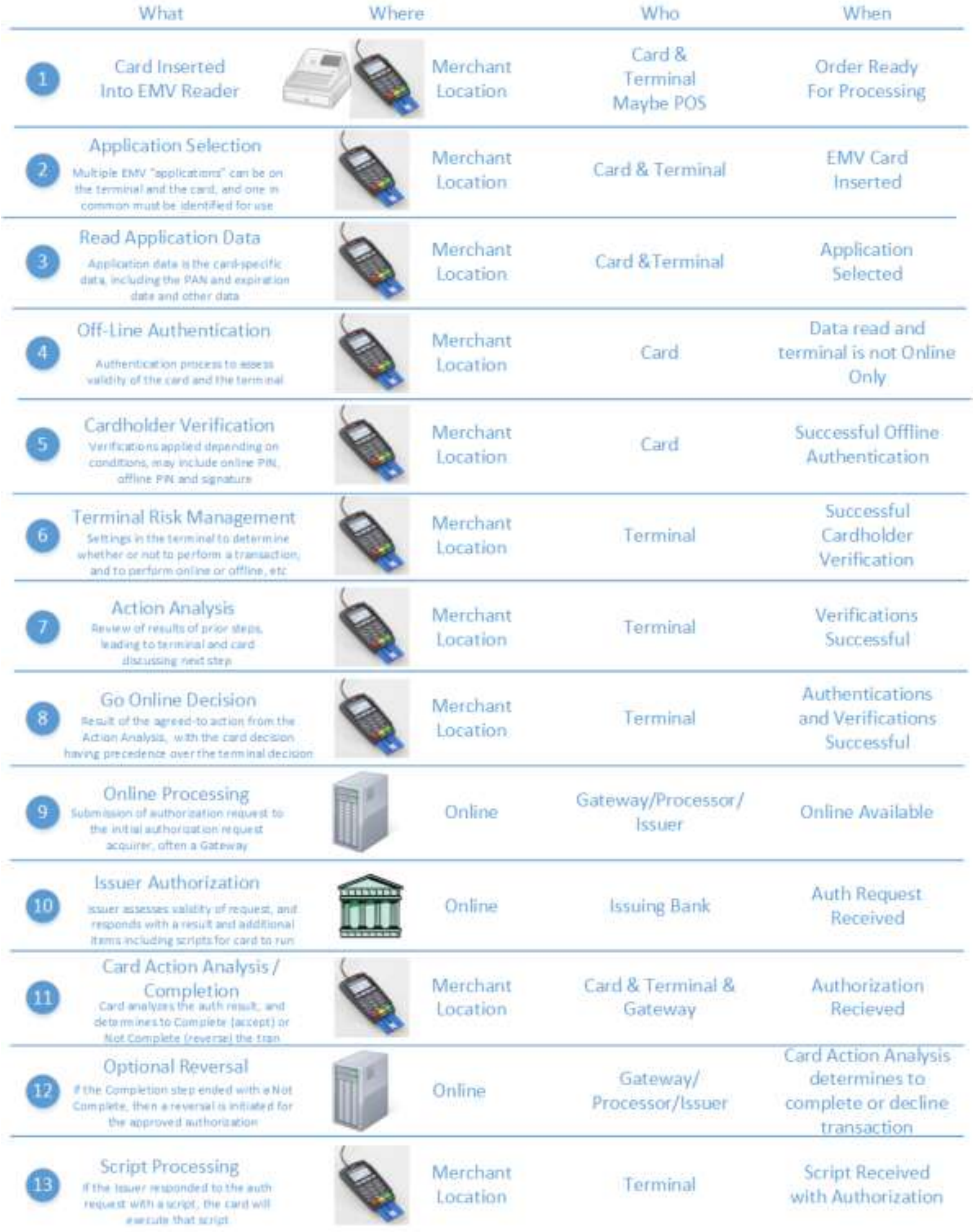
Diagram 5 – The introduction of middleware dramatically reduces the complexity of payment processing and EMV acceptance for the POS System. The middleware takes on responsibility to interact with the terminals in addition to the interaction with the payment gateway. Since the POS System is not accepting, storing, or transmitting card holder data, the POS System should not require PA-DSS compliance.



EMV - Details Of The Transaction Process

EMV transactions experience a lifecycle different than a swiped transaction. With EMV, a significant amount of activity occurs between the terminal and the chip on the card, prior to any authorization request going out.

The diagram below documents the steps that occur during a transaction using an EMV card and terminal. In this diagram, it is assumed that the transaction authorization process is going through an internet payment gateway.



	What	Where	Who	When
1	Card Inserted Into EMV Reader	Merchant Location	Card & Terminal Maybe POS	Order Ready For Processing
2	Application Selection Multiple EMV "applications" can be on the terminal and the card, and one in common must be identified for use	Merchant Location	Card & Terminal	EMV Card Inserted
3	Read Application Data Application data is the card-specific data, including the PAN and expiration date and other data	Merchant Location	Card &Terminal	Application Selected
4	Off-Line Authentication Authentication process to assess validity of the card and the terminal	Merchant Location	Card	Data read and terminal is not Online Only
5	Cardholder Verification Verifications applied depending on conditions, may include online PIN, offline PIN and signature	Merchant Location	Card	Successful Offline Authentication
6	Terminal Risk Management Settings in the terminal to determine whether or not to perform a transaction, and to perform online or offline, etc	Merchant Location	Terminal	Successful Cardholder Verification
7	Action Analysis Review of results of prior steps, leading to terminal and card discussing next step	Merchant Location	Terminal	Verifications Successful
8	Go Online Decision Result of the agreed-to action from the Action Analysis, with the card decision having precedence over the terminal decision	Merchant Location	Terminal	Authentications and Verifications Successful
9	Online Processing Submission of authorization request to the initial authorization request acquirer, often a Gateway	Online	Gateway/Processor/ Issuer	Online Available
10	Issuer Authorization Issuer assesses validity of request, and responds with a result and additional items including scripts for card to run	Online	Issuing Bank	Auth Request Received
11	Card Action Analysis / Completion Card analyzes the auth result, and determines to Complete (accept) or Not Complete (reverse) the tran	Merchant Location	Card & Terminal & Gateway	Authorization Recieved
12	Optional Reversal If the Completion step ended with a Not Complete, then a reversal is initiated for the approved authorization	Online	Gateway/ Processor/Issuer	Card Action Analysis determines to complete or decline transaction
13	Script Processing If the Issuer responded to the auth request with a script, the card will execute that script	Merchant Location	Terminal	Script Received with Authorization

© 2014 Intrix Technology, Inc, All rights reserved

Conclusions

Given the recent POS system data breaches in the US and the prevalence of EMV acceptance in the rest of the world, it is exceedingly unlikely that the Risk Shift target date of October, 2015 will move out.

This mean that, as of October, 2015, merchants will be at greater risk should they continue to accept card-present transactions using track swipe devices. The merchant will be left holding the bag if the card turns out to be counterfeit.

Point of Sale developers and other Independent Software Vendor developers are being asked about EMV now by merchants, but this will develop to a fever pitch over the next 6 months. These developers will need to decide if they will do the terminal integrations themselves, abandon integration to the terminal, or find a middleware solution. If these developers decide to communicate directly with the terminal, then time is running out to complete all the processor certifications that will be necessary.

Alternatively, selecting a company with which to partner for EMV processing should be done with an eye to that partner's knowledge and expertise in the EMV domain.

Visa is a registered trademark of Visa International Services Association.
MasterCard is a registered trademark of MasterCard International, Inc.
American Express is a registered trademark of American Express Company.
Discover is a registered trademark of Discover Financial Services, Inc.

About the Author: Suzanne Coleman is the Chief Technology Officer at Intrix Technology. Ms. Coleman is a technology leader specializing in the Financial Services field. Prior to joining Intrix. Ms. Coleman headed up Engineering and IT organizations at several companies, including First Data Corporation, Hewlett Packard, and others.

Intrix Technology, Inc., is a leading technology enabled registered Independent Sales Organization, delivers innovative payment-processing solutions for developers, enterprises, retailers, processors and sales organizations. We combine the power of technology and scale to deliver merchant services and technology solutions that fulfill all payment acceptance needs.   Intrix combines industry expertise with state-of-the-art technology to bring you results that make payment acceptance seamless to your organization. Intrix Technology offers PA-DSS and PCI-DSS certified solutions, including a Level 1 certified Payment Gateway.

For more information, please contact sales@intrix.com or call us at 855-5INTRIX (855-546-8749) or visit https://intrix.com