Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?

A Smart Card Alliance Payments Council White Paper

Publication/Update Date: January 2013

Publication Number: PC-12001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

The roadmap status described in this white paper is based upon Smart Card Alliance Payments Council analysis as of publication time. Continued analysis or updates from any of the key stakeholders may result in modifications of the roadmap. Any changes will be communicated in future publications on the EMV Connection web site (http://www.emv-connection.com), as needed.

TABLE OF CONTENTS

1 Introduction

Increasing counterfeit card fraud led the financial industry to move to smart chip technology for bank cards and to develop the global EMV specifications[1] for bank cards based on chip card technology. The EMV specifications, first available in 1996 and managed by EMVCo, define the global interoperable standard for smart bank cards and the accompanying point-of-sale (POS) infrastructure.

Financial institutions in the United States, Europe, Latin America, Asia/Pacific and Canada are issuing contact or dual-interface EMV smart cards for credit and debit payment or are migrating to EMV issuance. According to EMVCo,[2] approximately 1.5 billion EMV cards have been issued globally and 21.9 million POS terminals accept EMV cards as of Q4 2011. This represents 44.7% of the total payment cards in circulation and 76.4% of the POS terminals installed globally, excluding the United States.

The United States is one of the last countries to migrate to EMV. American Express, Discover, MasterCard and Visa have announced their plans for moving to an EMV-based payments infrastructure in the U.S.

- In August 2011, Visa announced plans to accelerate chip migration and adoption of mobile payments in the United States,[3] through retailer incentives, processing infrastructure acceptance requirements and counterfeit card liability shift.
- In January 2012, MasterCard announced their U.S. roadmap to enable the next generation of electronic payments, with EMV as the foundational technology.[4]
- Discover announced a roadmap that aligns EMV migration dates with MasterCard and Visa in March 2012.[5]
- In June 2012, American Express announced their U.S. EMV roadmap, which aligns migration dates with the other payment brands and states that issuance of EMV-compliant cards in the U.S. will start in the latter half of 2012.[6]

The objective of this white paper is to educate stakeholders across the payments value chain about the critical aspects of deploying an EMV solution in their business environments. The primary stakeholders are issuers, merchants, processors, and suppliers of hardware, software, and support services. This white paper takes the following approach:

- Provides an overview of the EMV specifications and key implementation options for issuers, acquirers/processors, merchants and ATM operators.
- Summarizes the key milestones and guidance announced by the payment brands for U.S. EMV migration.
- Discusses the relationship between U.S. contactless bank card transactions and EMV and the relationship between the Near Field Communications (NFC) specifications and EMV.

---

1 The original founders of the EMV standards body were Europay, MasterCard, and Visa—hence the acronym "EMV." Information on the specifications is available at http://www.emvco.com.

2 http://www.emvco.com. EMVCo is the organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. With the acquisition of Europay by MasterCard in 2002 and with JCB and American Express joining the organization in 2004 and 2009, respectively, EMVCo is currently operated by American Express, JCB International, MasterCard Worldwide, and Visa, Inc.

3 http://www.smartcardalliance.org/articles/2011/08/09/visa-announces-plans-to-accelerate-chip-migration-and-adoption-of-mobile-payments

4 http://www.mastercard.us/mchip-emv.html

5 http://discovernetworknews.com/stories/discover-implements-emv-mandate-for-u-s-canada-and-mexico/

6 http://about.americanexpress.com/news/pr/2012/emv_roadmap.aspx

- Identifies actions stakeholders need to take to issue EMV cards, and to accept and process EMV transactions.

While critical business drivers are mentioned and can be applied to construct a business case, this paper is not intended to develop the comprehensive business case required to make an investment decision.

The EMV specifications can resolve key issues that challenge financial institutions. The majority of work on EMV was conducted in the late 1990s. Over the years, EMVCo has maintained and revised the specifications to sustain the highest level of security. EMVCo also develops and manages new functionality required by the market.

As the U.S. plans for EMV migration, payments industry stakeholders recognize that there is a need to educate themselves about EMV and to leverage the lessons learned in other parts of the world. Industry stakeholders are exploring the implementation options in the EMV specifications that will be required to meet U.S. market needs in the most cost-effective manner.

2 Overview

Smart card technology embeds a secure integrated circuit chip with a microprocessor into a form factor. The form factor most commonly used is a card; however key fobs, microSD memory cards, adhesive stickers, and most recently, NFC-enabled mobile phones can all accommodate the same basic technologies. The chip is typically powered by a reader and requires the reader to function (for payment, the point-of-sale device).

The interface with the reader can be a contact interface or a contactless interface. Dual-interface cards include both contact and contactless interfaces and, depending on the options available at the acceptance location, can communicate over either interface.

Contact cards communicate with the reader through a contact plate. The plate must come into contact with a terminal, usually through a dip reader into which the card is inserted. ATMs often rely on motorized readers that actually draw the card into the ATM, where it is staged to prevent withdrawal during a transaction. Contactless cards contain an antenna and communicate over a radio frequency (RF) with the reader. Dual-interface cards combine both technologies.

In a contact or dual-interface card, the contact plate is the gold plate on the left side of the card. The embedded antenna is not visible on most contactless cards; however many contactless cards display a graphic symbol to indicate that they have contactless capability.[7]

2.1 EMV and Payment Transaction Security

EMV is an open-standard set of specifications for smart card payments and acceptance devices. EMVCo, owned by American Express, JCB, MasterCard, and Visa, manages, maintains and enhances the EMV specifications, to ensure global interoperability of chip-based payment cards with acceptance devices including point of sale terminals and ATMs.[8] The first version of the specifications was released in 1996. The specifications address interoperability at two levels. Level 1 defines the electromagnetic and physical characteristics of cards and readers, while Level 2 defines the commands, data elements and transaction flows.

EMV's primary purpose is to ensure that standards for smart card-based payments are interoperable globally. In 2007, EMVCo issued the first phase of the EMV contactless specifications, offered a complete version March, 2011, and released version 2.2 in June, 2012.

In addition to storing payment information in a secure chip rather than on a magnetic stripe, using EMV improves the security of a payment transaction by adding functionality in three key areas:[9]

1. Card authentication, protecting against counterfeit cards and skimming (i.e., to produce a copy of an authentic card)
2. Cardholder verification, authenticating the cardholder and protecting against lost and stolen cards
3. Transaction authorization, using issuer-defined rules to authorize transactions

In addition, EMV transactions use cryptograms to digitally sign the actions performed and the conditions at the time of the transaction, providing transaction non-repudiation.

[7] http://www.emvco.com/best_practices.aspx?id=117
[8] http://www.emvco.com/about_emvco.aspx
[9] In addition to payment application security features, an EMV card includes a secure smart card IC, which is tamper-resistant and includes a variety of hardware and software capabilities that immediately detect and react to tampering attempts, countering possible attacks.

2.1.1 Card Authentication Methods

Card authentication protects the payment system against counterfeit cards. Card authentication methods are defined in the EMV specifications and the associated payment brand chip specifications. Card authentication can take place online, offline, or both.

2.1.1.1 Online Card Authentication

Online card authentication requires the transaction to be sent online for the issuer to authenticate and authorize in the same way magnetic stripe transactions are sent online today in the U.S. The important difference is the chip card's use of symmetric key technology to generate an application cryptogram (AC). This cryptogram type, called the Authorization Request Cryptogram (ARQC), is validated by the issuer during the online authorization request.

The ARQC is the dynamic data that makes an EMV transaction unique and provides card-present fraud protection against counterfeiting and skimming. The chip generates this cryptogram by applying a cryptographic algorithm to data provided by the card and the acceptance device, as well as transaction specific data. The process of cryptogram generation uses a symmetric algorithm (such as Triple DES)[10]. Each EMV card uses a derived unique key only known to the issuer host system. The issuer host does not need to store the keys for each card; instead it derives each key from a master key using the primary account number (PAN) as diversification data. The key is stored in a secure area on the chip. Because some of the data used in the cryptogram generation is different for each transaction, the resulting cryptogram is unique for each transaction.

2.1.1.2 Offline Card Authentication

Offline card authentication involves the EMV card and EMV terminal without connection to issuer host. Three methods of offline card authentication are defined by EMVCo, offering increasing levels of protection against counterfeit cards:

- Static data authentication (SDA) (Section 2.1.1.2.1)
- Dynamic data authentication (DDA) (Section 2.1.1.2.2)
- Combined DDA with application cryptogram (AC) generation (CDA) (Section 2.1.1.2.3)

The principle of offline card authentication is to establish a chain of trust without the need for, or prior to the establishment of an online connection. The acceptance device recognizes the card was issued by a trusted member of a payment brand.

2.1.1.2.1 Static Data Authentication

Most cards issued worldwide support SDA. SDA is performed by the terminal using a pregenerated static digital signature stored on the card at the time of issuance. This signature guarantees the integrity and authenticity of critical static data stored on the card. SDA relies on a public key infrastructure (PKI) in which the payment brands act as the certificate authorities (CAs) and provide public key certificates to participating issuers. During the personalization process, the issuer uses the issuer's private key to sign a set of card-specific data and loads the card's certificate, the signed data and the issuer's public key certificate onto the card.

When the POS terminal is configured, the payment brand public keys (for those brands that are accepted) are loaded onto the terminal. At the beginning of the transaction, the terminal uses the payment brand's root key to validate the issuer's public key certificate. The terminal then extracts the issuer's public key from the validated certificate. Using the extracted issuer public key, the terminal authenticates the static card data and the card certificate, validating that the card is authentic and issued by the correct issuer under the authority of the payment brand.

[10] Also referred to as Triple Data Encryption Standard (TDES).

This process is known as static data authentication because the data used for authentication is static—the same data is used at the start of every transaction. If this data can be skimmed, it may be used to recreate a fraudulent offline transaction, below the terminal floor limit.

SDA is the simplest method of chip card authentication and provides the lowest level of protection against skimming and counterfeit fraud for an offline transaction.

2.1.1.2.2 Dynamic Data Authentication

DDA is similar to SDA but goes one step further. When supporting DDA, the card calculates a dynamic signature as opposed to providing a pregenerated static signature (SDA) for each transaction. The DDA signature is unique to the specific card and each transaction. In addition to the issuer asymmetric (RSA) key pair, an asymmetric key pair is generated for each card. The issuer then creates an associated public key certificate by signing the card public key. All data is loaded onto the card during personalization.

To authenticate a card, terminals follow the same process as for SDA, except that unique data is used and signed as part of the DDA signature by the card private key. The terminal then validates the signature using the card public key.

DDA protects against SDA certificate cloning, card skimming and counterfeiting.

2.1.1.2.3 Combined DDA with Application Cryptogram

When supported by both the card and the terminal, CDA combines a request for dynamic signature calculation and application cryptogram in one command. This offers an extra layer of security and faster speed when performing offline transactions. In fact, when a contactless offline transaction is performed, DDA is not an option due to transaction performance (speed). Certain payment brands require CDA for offline contactless transactions.

CDA is faster than DDA and protects against SDA certificate cloning, card skimming and counterfeiting.

2.1.2 Cardholder Verification Methods

Cardholder verification authenticates the cardholder. Use of a personal identification number (PIN) is a common cardholder verification method (CVM) used to authenticate the cardholder and protect against the use of a lost or stolen card. EMV supports four types of CVMs, allows the use of multiple CVMs, and defines the conditions under which they may be used:

- Offline PIN
- Online PIN
- Signature verification
- No CVM

EMV defines a configuration data element called the CVM list. Depending on payment brand rules and/or guidelines and issuer preference, chip cards are personalized with one or more CVMs in order to be accepted in as wide a variety of locations as possible. The issuer's choice of supported CVMs is listed in the CVM list in order of priority. Different terminal types support different CVMs. The terminal and the card use the first matching CVM type in the card's CVM list. Each entry in the CVM list also contains the issuer's choice to attempt (or not to attempt) the following entry if the first attempted CVM failed. For example, attended POS devices, in addition to supporting signature, may support online or offline PINs (or both).

2.1.2.1 Offline PIN

Offline PIN is the only method of cardholder verification supported by EMV that is not available with magnetic stripe cards. The offline PIN is stored securely on the card. When the cardholder enters a PIN during a transaction, the POS terminal sends the PIN to the EMV card for verification. The card

compares the entered PIN to the stored PIN and sends the result of the comparison back to the POS terminal.

It is important to note that while a card may support offline PIN, the card may not support offline transactions. Most EMV implementations globally employ offline card authentication and offline PIN verification yet still require online authorization of the transaction.

Offline PIN is not an option for contactless EMV transactions (unless using a mobile device which can use some form of passcode verification).

The offline PIN is never sent to the issuer host—only the result of the comparison is passed. The issuer may configure the card not to decline transaction if offline PIN fails or if it has not been verified. Instead, the issuer may configure the card to either use the next CVM entry and/or force the transaction online (if offline transaction was requested), and subsequently make a decision at the host system level.

Internationally, most if not all attended acceptance locations support offline PIN, signature and no CVM. Unattended acceptance locations (e.g., unattended gas stations, public transit stations) may be limited to supporting offline PIN and no CVM.

2.1.2.2 Online PIN

The online PIN is not stored on the card; instead the PIN is sent online to the issuer for validation. Online PIN is currently supported for magnetic stripe cards for online PIN debit transactions; online PIN is also used for cardholder verification for cash withdrawals using credit cards.

The cardholder enters the PIN at the POS terminal; the PIN is encrypted by the PIN pad and sent online to the host for validation. The security of the online PIN is standardized globally and is based on Triple Data Encryption Standard (TDES). For an ATM, online PIN is always required and is the only valid CVM when implementing EMV. As a result, any implementation of offline PIN will, as they do today, still require online PIN if ATM access is needed.

If a card supports both online and offline PIN CVMs, the issuer must ensure that the two PINs are synchronized or consumer confusion will result.

In general, online PIN or offline PIN CVMs may help protect against fraud resulting from lost, stolen, and never-received cards.

2.1.2.3 Signature

Signature verification requires a written signature at the POS, as is currently required with magnetic stripe cards. Validation occurs when the signature on the receipt is compared to and matches the signature on the back of the card. As is true today, signature verification also requires that the merchant retain an electronic or physical signed receipt and be in a position to produce this receipt in the event of a cardholder dispute.

2.1.2.4 No CVM

EMV also supports transactions that require "No CVM." Some POS devices may only support “No CVM” if they are not equipped with a PIN pad or a signature panel. POS devices can also be configured to support “No CVM” for transactions below a specific value.

2.1.3 Transaction Authorization

EMV transactions can be authorized online or offline. For an online authorization, transactions proceed as they do today with magnetic stripe cards. The transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either authorizes or declines the transaction.

In an offline EMV transaction, the card and terminal communicate and use payment brand and issuer-defined risk parameters to determine whether the transaction can be authorized. Offline transactions may

be used when terminals do not have online connectivity[11] or when increasing the speed and convenience of a transaction can be further optimized (e.g., in transit and event ticketing, or in peak retail periods to support delayed batch processing).

Cards can be configured to allow both online and offline authorization, depending on the circumstances. It is also important to note that use of the offline PIN CVM is not restricted exclusively to offline authorized transactions. Offline PIN can be used as the CVM, and the transaction can then go online for authorization in the majority of circumstances.

2.1.4 EMV Offline Transaction Risk Management

The EMV specifications define features to allow issuers to manage the risk of when to support offline transactions or if to support offline transactions at all. Payment brands enhance the EMV specifications with additional flexibility and offer issuers a comprehensive set of configuration parameters to allow an EMV card to perform (or not perform) an offline EMV transaction.

Offline risk management parameters on the card are defined by the issuers and usually consist of offline limits expressed in two different ways:

- Number of consecutive offline transactions, or
- Cumulative amount of offline transactions.

When either of these limits is exceeded, the issuer forces the transaction online and/or the card declines the transaction.

There are two main scenarios in which an EMV-capable terminal may request an offline transaction, assuming the issuer supports it on the card:

- **Scenario 1.** The terminal (i.e., merchant) chooses to request an offline transaction for a number of reasons (for example, faster transaction processing and/or slow/costly communication capabilities), but not because the terminal is not capable of connecting to the payment network.
- **Scenario 2.** The terminal has lost network connectivity and is not capable of processing an online transaction.

In summary, EMV transaction risk management is evaluated in two distinct steps allowing both the terminal to provide its preference or capability, as well the card to respond with its agreement (based on issuer's choice) with the terminal's request. The card offline risk management parameters are defined in two groups: lower limits and upper limits.

Issuers have the following choices when defining their EMV offline risk management parameters:

- Online only EMV cards
- Online preferring EMV cards
- Offline capable EMV cards

2.1.4.1 Online only EMV cards

An issuer may decide not to support any offline transaction. In this case the issuer sets both lower and upper offline limits to zero. If the terminal requests offline due to the first scenario above, the card will force the transaction online. In scenario 2, if the terminal is not capable of performing an online transaction, the card will decline an offline transaction.

Online only cards do not need to implement any offline data authentication methods (SDA/DDA/CDA).

[11] Offline authorized transactions may not provide fraud liability protection for merchants depending on payment brand rules.

2.1.4.2 Online preferring EMV cards

In order to support offline transactions, the issuer must implement offline data authentication (SDA/DDA/CDA) based on payment brands' requirements. In addition, as mentioned in section 2.1.2.1, the issuer should consider implementing offline PIN as part of the CVM list, as this is very often the only supported CVM for offline transaction processing.

An online preferring EMV card has its offline transaction lower limits set to zero, and as such, will still request an online transaction in scenario above. However, when the terminal is not capable of connecting online (scenario 2 above), it will approve an offline transaction while the card's offline upper limits are not exceeded.

2.1.4.3 Offline capable EMV card

An offline capable EMV card must support offline card authentication and should support offline PIN; however, in this configuration option both lower and upper offline limits are not set to zero. The card can approve an offline transaction for scenario 1 when the lower limits are not exceeded, and for scenario 2 when the upper limits are not exceeded.

As an example, if an issuer decides to support offline authorization, it may configure its lower limits to three consecutive offline transactions not exceeding $50 in total and its upper limits to five consecutive offline transactions totaling up to $100.

Note: The U.S. is a predominantly zero floor limit environment that requires almost all transactions to be authorized online.

2.2 EMV and Application Selection

Key to the design of EMV is the concept of application selection and the ability for a chip card to support one or more payment applications. To support this capability the EMV specifications defined in Book 1 provides a clear description for how the terminal builds the candidate list of payment applications at the very beginning of the dialog between the card and the terminal. The issuer determines which payment brand applications and associated application IDs (AID) it wishes to load on the card. This list of AIDs is prioritized by the issuer at time of card personalization.

In essence, the candidate list is the compilation of the payment brands supported by the terminal and the payment brands and associated application code available on the card. The list of mutually supported payment applications is established by comparing an AID that is assigned to the payment brand by the ISO/IEC standardization body, as defined in ISO/IEC 7816-5. The payment brand who owns the selected AID defines how this application can be used.

Once the candidate list is assembled, the EMV compliant PIN pad may present the candidate list on the consumer-facing display in the order defined by the issuer. The cardholder may then select the method of payment to use and the transaction will proceed to the next step in the EMV transaction flow. The priority of each application on the card is defined by the issuer. The issuer can also define if the selection is to be done with or without cardholder interaction.

In the case of contactless cards, however, how a slightly different process is executed. The terminal still goes through the process of creating a candidate list. Presenting the candidate list to the cardholder is not a viable option when performing contactless transactions, since the contactless card or device is more often than not already removed from the reader. The terminal selects the highest priority, or first, application identified in the candidate list.

When the payment application is resident on a mobile phone, the wallet application may enable the consumer to change the priority of the payment applications resident in the wallet prior to presenting the mobile phone to the contactless reader.

In the U.S., new legislation, the Durbin Amendment to the Dodd Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), is in effect which may impact the ways in which application selection is implemented. A discussion of these changes is included in Section 3.3.

2.2.1 Issuer Considerations for Multiple Payment Application Support

When supporting multiple applications, an EMV card may need to implement several payment brand application specifications.

There are two possible scenarios:

- **Scenario 1**. Two or more AIDs use the same payment specification. In this case, the issuer can personalize an EMV card with two or more different AIDs pointing to the same application. In smart card terminology, this is known as creating two or more instances of the same application.
- **Scenario 2**. The AIDs must use different payment specifications and associated application. In this case, the EMV card must support two or more different payment applications.

It is important to note that the issuer may need, or choose, to share cardholder relevant data between multiple applications. For example, when implementing offline PIN, the issuer will need to synchronize the PIN by sharing it between applications.

Most EMV chip card platforms (i.e., native, Java, MULTOS) support multiple applications; however, while the mix of payment specifications in scenario 2 is not known at this time, it can create complexity to issuers selecting EMV card products as well as generating EMV data and personalizing cards. (See Figure 2.)

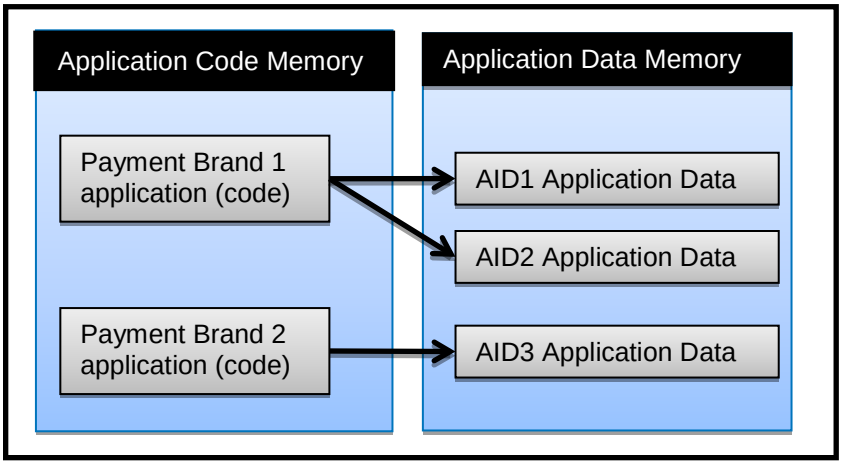


Figure 1: Example of Multi-Application EMV Card Structure

2.3 EMV Changes to the Messaging Infrastructure

The payments industry is moving towards global interoperability with chip technology that provides form factor flexibility with value-added service capabilities and increased security. The EMV payments infrastructure includes a network message field that transports chip data between the card and the issuer. In the U.S., this field is often referred to as Field 55.[12] This field must be added to the authorization request, authorization response and, in some cases, the clearing and settlement data.

Field 55 is defined as a generic, flexible, variable length container that conforms to tag-length-value (TLV) encoding.[13] Every data element carried in the field has a specific tag, followed by the length of the data and then the actual data. Each tag is defined by EMV or specified in the relevant payment brand specifications. The application cryptogram, the terminal unpredictable number, the transaction amount, issuer scripts, and the form factor indicator are typical of the types of data passed in this field.

[12] Outside of the U.S., the data is sometimes carried in a bitmap format known as "third bitmap."
[13] Some acquirer and payment brand implementations do not use TLV coding.

The card sequence number is critical to cryptogram validation. It may be carried in different fields within the authorization and clearing messages. For example, Field 23 carries the card sequence number in some implementations. When two or more cards are associated with a single account number, this field contains the number assigned to a specific card. For example, there are some situations (such as families) where a single primary account number (PAN) is used by different cardholders. For these cards, the card sequence number identifies the individual card sending chip data in the authorization message.

Based on the acquirer and payment brand implementations, other fields (e.g., Fields 22, 48, and 60.2) may need to be accommodated since they describe the terminal characteristics, the way the card was read and the cardholder verification performed.

Issuers, acquirers, and merchants will all need to change their infrastructure to support the new required fields.[14]

Table 1. Field 55 Common Tag Values

Tag	Tag Descriptor	Functionality	Details
57	Track 2 equivalent data	Data required to complete the authorization and clearing records	Contains a representation of the data stored on track 2 of the magnetic stripe
5A	Personal account number	Data required to complete the authorization and clearing records	Contains the same data embossed on the face of the card and stored on the magnetic stripe
5F20	Cardholder name	Data required to complete the authorization and clearing records	Contains the same data embossed on the face of the card and stored on the magnetic stripe
5F24	Application expiry date	Data required to complete the authorization and clearing records	Contain the same data embossed on the face of the card and stored on the magnetic stripe
9F26	Application cryptogram	Card authentication	Contains the cryptogram used to authenticate the transaction.
9F36	Application transaction counter	Card authentication	Contains the value of the chip card transaction counter. The chip card maintains a transaction counter and increments the count each time a transaction is initiated.
9F07	Application usage control	Card authentication	Specifies the issuer's restrictions on the geographic usage and services allowed for the application.*
9F27	Cryptogram information data	Card authentication	Indicates the type of cryptogram and the actions to be performed by the terminal.
9F34	CVM results	Cardholder verification	Identifies how the cardholder was verified at the POS: by cardholder signature, cardholder PIN, or verification not required.

[14] Messaging requirements should be discussed with the payment brands to ensure that all required messaging changes are considered in implementation.

Tag	Tag Descriptor	Functionality	Details
9F0D	Issuer action code—default	Transaction authorization	Specifies issuer conditions that cause a transaction to be rejected if the transaction might have been approved online but the terminal is unable to process it online.*
9F0E	Issuer action code—denial	Transaction authorization	Specifies issuer conditions that cause a transaction to be denied without an attempt to go online.*
9F0F	Issuer action code—online	Transaction authorization	Specifies issuer conditions that cause a transaction to be transmitted online.*
9F10	Issuer application data	Card authentication	Contains issuer application data transmitted from the chip to the issuer.
9F37	Unpredictable number	Card authentication	Contains the POS terminal unpredictable number value. The POS terminal generates the number value that may be used as input to the application cryptogram algorithm.

*http://www.emvlab.org/emvtags/all

Table 2. Field 23, Card Sequence Number

Field	Descriptor	Functionality	Details
23	Card sequence number	Card authentication	Contains a card sequence number from the EMV card chip that identifies to the issuer which card was used at the POS when multiple cards are associated with the same primary account number.

2.4 EMV, Contactless and NFC

Branded contactless credit and debit cards are being issued globally. While all implementations are based on the ISO/IEC 14443 contactless communication protocol, the payment application and security implementation approaches have differed in the U.S. and in countries implementing EMV.

2.4.1 EMV Contactless

Version 2.2 of the EMV specifications for payment terminals that support all payment brand contactless applications was published in June, 2012. Payment brands can implement contactless payment for EMV transactions to function in both offline and online transaction environments and to leverage the EMV cryptogram security function to validate the authenticity of the card and the transaction. This prevents card cloning and replay fraud. Support for the EMV cryptogram requires a network change to carry the additional data required for online authentication.

The EMV contactless transaction flow for each of the payment brands varies according to the extent of EMV risk management functions and type of authentication cryptogram that is implemented in the contactless application. The multiple independent contactless EMV approaches have required POS terminals to be approved by each payment brand. EMVCo recognized the need for standardization and has developed the common contactless terminal roadmap. In March 2011, EMVCo published a

combined set of terminal specifications from the existing four payment brands' specification. EMVCo also manages the testing and approval of the contactless kernels according to these specifications.

2.4.2 U.S. Contactless

In the U.S., the payment brands implemented contactless payment transactions to leverage the existing magnetic stripe payments infrastructure and minimize the impact on merchant and acquirer network messaging. This approach, called contactless MSD (magnetic stripe data), facilitated straightforward contactless payment implementations by issuers, merchants and payment processors and faster consumer adoption and merchant acceptance.

With contactless MSD, the message layout for Track 1 and Track 2 magnetic stripe data remained intact, with one notable difference. The chip on the card allows calculation of a dynamic card verification value based on a card-unique key and a simple application transaction counter. The dynamic card verification value is passed in the message in the same field that was used for the original card verification value. The application transaction counter (ATC) is passed in the area reserved on the track layout for issuer discretionary data. In general, contactless MSD in the U.S. uses online authentication and online authorization.

The dynamic card verification value enhanced the security of the transaction versus the static card verification value/code or card ID (CVV/CVC/CID) used in magnetic stripe transactions. The use of dynamic data in the transaction prevents replay attacks (no transaction can be done twice) and card cloning or skimming (the card key never leaves the protection of the smart card memory).

As the U.S. migrates to EMV, the payments infrastructure will need to continue to support contactless MSD for some period of time to allow acceptance of existing contactless cards and devices, while adding support for contactless EMV.

2.4.3 EMV and NFC Mobile Contactless Payments

An anticipated area of growth in the near future is the use of Near Field Communication (NFC)-enabled mobile phones for mobile contactless payments and other mobile applications, such as coupons and loyalty.[15]

NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart.[16] NFC-enabled mobile phones incorporate smart chips (called secure elements) that allow the phones to securely store the payment application and consumer account information and to use the information as a "virtual payment card." NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by EMV and U.S. contactless credit and debit cards.

NFC-enabled mobile phones will be able to carry one or more payment applications and accounts from different issuers; the NFC specifications don't define or specify the payment application. Payment applications will follow the EMV contactless specifications for the mobile payment application and account credentials are being issued.

EMVCo has been active in defining the architecture, specifications, requirements and type approval processes for supporting EMV mobile contactless payments. The key work of EMVCo has been to provide guidelines for the user interface and a few other tactical elements of the applet in a mobile wallet. The core payment transaction flow is governed by the contactless EMV specifications. This approach

[15] For additional information on mobile marketing applications, see the Smart Card Alliance Payments Council white paper, "Chip-Enabled Mobile Marketing," September 2010, http://www.smartcardalliance.org/pages/publications-chip-enabled-mobile-marketing.

[16] For additional information on NFC, see the NFC Forum web site at http://www.nfc-forum.org. The NFC Forum defines the specifications for communication between NFC tags and readers, but does not define payment application specifications.

has been critical in supporting the launch of NFC mobile contactless payment in Europe, which uses an EMV-based payments infrastructure. EMVCo is working with other industry groups to:[17]

- Develop any required specifications which are specific to mobile contactless payment, and which are common across the payment brands.
- Communicate requirements and provide profiles and guidelines on how architectural elements defined by other organizations are to be used in the context of mobile contactless payments in order to promote interoperability.
- Develop processes to determine the level of conformance of implementations to EMVCo-defined specifications, profiles and requirements.

2.5 EMV Approvals and Certifications

To assure compliance with EMV specifications and payment brand specific functional requirements, terminals, integrated circuit chips (ICC) and EMV cards are tested for compliance. Evaluations are performed by recognized external security laboratories.

2.5.1 EMV Terminal Type Approval

EMVCo established the Terminal Type Approval process to create a mechanism to test compliance with the EMV contact and contactless specifications. Type Approval provides an increased level of confidence that interoperability and consistent behavior between compliant applications have been achieved. EMVCo Type Approval testing is divided into two levels.[18]

- Level 1 Type Approval tests compliance with the electromechanical characteristics, logical interface, and transmission protocol requirements defined in the EMV specifications.
- Level 2 Type Approval tests compliance with the debit/credit application requirements as defined in the EMV specifications.

EMVCo publishes an approved list of terminals on the EMVCo web site.[19]

2.5.2 ICC Chip Security Evaluation

EMVCo evaluates the general security performance characteristics of chips used in EMV cards. EMVCo issues compliance certificates for chips passing the tests and publishes an approved list of chips on the EMVCo web site.[20]

2.5.3 EMV Card Type Approval

EMVCo established the Card Type Approval process to create a mechanism to test cards for compliance with the EMV Common Core Definitions (CCD) and Common Payment Application (CPA) specifications. EMVCo publishes an approved list of cards on the EMVCo web site.[21] Note that EMV approval against CCD and CPA is optional and not required if the card will be approved by a payment brand. CPA is an alternative application an issuer may choose to use instead of a payment brand-specific application.

[17] "Contactless Mobile Payment Architecture Overview," Version 1.0, EMVCo, June 2010, http://www.emvco.com/best_practices.aspx?id=162
[18] http://www.emvco.com/approvals.aspx
[19] http://www.emvco.com/approvals.aspx?id=83
[20] http://www.emvco.com/approvals.aspx?id=81
[21] http://www.emvco.com/approvals.aspx?id=30

2.5.4 Payment Brand Evaluations and Type Approval

Individual payment brands – American Express, Discover, JCB, MasterCard, and Visa – evaluate the implementation of the brand-specific EMV payment application specifications. Following a successful functional and security testing and evaluation, the payment brands issue a type approval letter. A prerequisite for the payment brand evaluation is the EMVCo security evaluation.

Figure 2 illustrates the EMV hardware and software architecture and the evaluations and approvals for EMV cards and applications that are used with each layer.

Figure 2. EMV Hardware and Software Approvals

EMV Architecture	Evaluations and Approvals	Responsibility
Chip Hardware • EEPROM • ROM • Cryptographic engine (DES, PKI) • Memory protection logic • Flash technology	• EMVCo evaluates and certifies the general security performance characteristics of chips used in EMV cards.	• Chip silicon supplier
Operating System and Application Communication Level (Level 1) • Contact EMV Card Level 1 (Protocol/Electrical) • Contactless EMV Level 1 (Analog/Digital)	• EMV contact and contactless Level 1 approval can be done by EMVCo or payment brand-accredited test lab. • Evaluation and testing of communication layer is performed against ISO/IEC 7816-3 (contact) and ISO/IEC14443 (contactless) standards.	• Contact only card: card or chip vendor • Dual-interface card: card vendor
EMV Application Level (Functional and Security) • Common Core Definitions • Common Payment Application	• EMVCo evaluates card implementations of CCD and CPA specifications (not required if payment brand approval is performed). • Cards will likely also require payment brand approval.	• Card or chip vendor
Payment Brand Application Level (Functional and Security) • American Express AEIPS, ExpressPay 2.0 • Discover D-PAS • JCB J Smart • MasterCard M/chip 4, M/Chip PayPass, M/Chip Advance • Visa VIS 1.4 / 1.5, VCPS 2.0.2 / 2.1	• Payment brands perform security and functional evaluation of payment application implementation. Upon successful testing, the payment brands issue an approval letter. • For dual-interface EMV cards, the functional testing includes not only the chip but also the card body with an integrated antenna. In addition to security and functional testing, dual-interface cards are also tested for performance (e.g., speed and reliability of contactless transaction) using approved reference contactless readers.	• Contact only card: card or chip vendor • Dual-interface card: card vendor
Data Level • Personalization data	• Payment brands validate the card personalization prior to production issuance.	• Issuer

3 Roadmap Options

The move toward EMV is accelerating with a number of significant announcements since August, 2011. With Visa taking the lead with its announcement on August 9, 2011, MasterCard and Discover quickly followed suit with announcements on January 30, 2012 and March 15, 2012, respectively; American Express announced their U.S. EMV roadmap on June 29, 2012.

EMV deployment milestones include:

- **PCI Audit Relief**: the date by which, if more than 75% of transactions originate from EMV-compliant contact and contactless POS terminals, the merchant may apply for relief on the audit requirement for PCI compliance (but is still mandated to be PCI compliant).
- **PCI Account Data Compromise Relief**: the MasterCard milestones by when merchants are relieved of all or a portion of penalties for account data compromise (aka "hacking") if a certain percentage of transactions originate from EMV-compliant contact and contactless POS terminals.
    - **75%-50%:** If at least 75% of transactions originate from EMV-compliant POS terminals, the merchant is relieved of 50% of account data compromise penalties
    - **95%-100%:** If at least 95% of transactions originate from EMV-compliant POS terminals, the merchant is relieved of 100% of account data compromise penalties
- **Acquirer/Sub-processor Compliance**: the date when acquirers and acquirer processors must be enabled to handle full chip data in transactions for authorizations and, for some payment brands, clearing and settlement.
- **Counterfeit Liability Shift:** the date when the party that has made investment in EMV deployment is protected from financial liability for card-present counterfeit fraud losses. If neither, or both parties are EMV compliant, the fraud liability remains the same as it is today.
- **ATM Counterfeit Liability Shift**: The date that MasterCard's liability hierarchy will take effect for ATM transactions.
- **Lost or Stolen Liability Shift**: The date that the MasterCard liability hierarchy takes effect for lost/stolen cards. The party that has made the investment in the most secure EMV options is protected from financial liability for card-present fraud losses for lost, stolen and non-receipt fraud on this date.

American Express, Discover, MasterCard and Visa have harmonized their U.S.-specific compliance and liability shift dates.[22] Table 3 shows the milestones that have been announced as of the publication date of this white paper.

[22] Liability shifts differ depending on country pairs and technology: magnetic stripe skimming vs. PIN.

Table 3: EMV Deployment Milestones by Payment Network[23]

EMV Deployment Milestones	Key Dates	Visa	MasterCard	Discover	American Express
PCI Audit Relief	October, 2012	Y	Y	N	N
	October 2013			Y	Y
PCI Account Data Compromise Relief					
75%-50%	October, 2013	N	Y	N	N
95%-100%	October, 2015	N	Y	N	N
Acquirer/ Sub-processor Compliance	April, 2013	Y	Y	Y	Y
Counterfeit Liability Shift (excluding fuel dispensers)	October, 2015	Y	Y	Y	Y
ATM Counterfeit Liability Shift	April, 2013	N	Y – cross border Maestro	tba	N
	October, 2016	N	Y – all MasterCard-branded products	tba	N
Lost or Stolen Liability Shift	October, 2015	N	Y	Y	N
Counterfeit Liability Shift for Automated Fuel Dispensers	October, 2017	Y	Y	Y	Y
Lost and Stolen Liability Shift for Automated Fuel Dispensers	October, 2017	N	Y	Y	N

All payment networks allow issuer choice on issuance dates, cardholder verification methods, and online vs. offline authentication/authorization. However, there are some differences in implementation guidelines among the networks:

- Visa emphasizes the zero floor limit environment of the U.S. payments market, and takes steps to ready the nation's payment infrastructure for mobile. In keeping with deployment dates that are more aggressive than other parts of the world, Visa advocates keeping the infrastructure as straightforward as possible through the following guidelines:
  - For issuers, Visa recommends online-only authorization, online card authentication, and signature preferring cards with online PIN support for debit.
  - Visa requires dual-interface POS terminals in order for merchants to qualify for PCI audit relief.
  - For online-only terminals, Visa does not require support for chip data in the clearing and settlement records, as this is deemed unnecessary in a zero floor limit environment.
- Visa will not require terminals to support contactless MSD after October, 2015, and does not encourage any new deployments of these types of "contactless-only" cards. In addition, "contactless only cards"[24] will not qualify for liability shift protection.

[23] The milestones in Table 3 are based upon Smart Card Alliance Payments Council analysis as of publication time. Continued analysis or updates from any of the key stakeholders may result in modifications of the milestones. Any changes will be communicated in future publications or on the EMV Connection web site (http://www.emv-connection.com), as needed.

- MasterCard introduced a hierarchy of liability shift to the party with the higher risk environment, e.g., magnetic stripe vs. EMV and PIN vs. signature.
- MasterCard requires combined data authentication (CDA) for contactless EMV cards that support offline transactions.
- American Express announced a fraud liability shift policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology.
- American Express mandates that all new EMV card issuers must use dynamic data authentication (DDA) technology and authentication.

3.1 Roadmap Considerations

Many interconnected factors and developments must be considered to construct an EMV migration roadmap for the U.S., including the current contactless implementation, use of contact or contactless EMV, selection of options from the EMV standard to suit the U.S. environment, convergence with NFC mobile contactless payments, and the use of a PIN as opposed to a signature CVM.

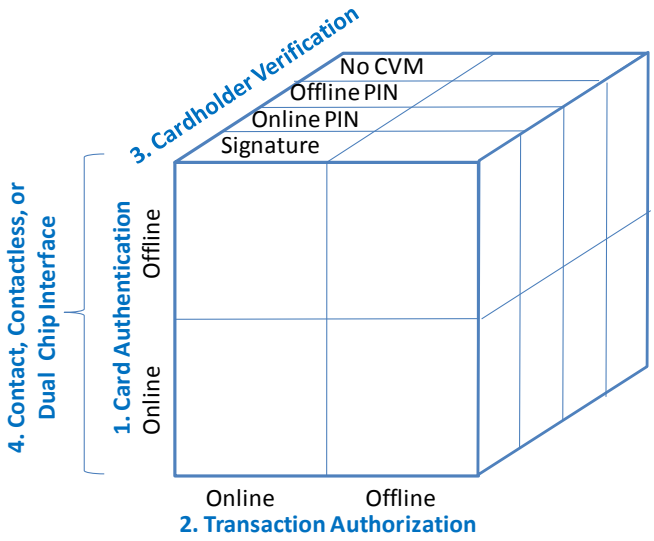
Planning for an EMV implementation requires choices in four key areas:

1. Card interface
2. Card authentication method
3. Transaction authorization
4. Cardholder verification method

Issuers may also need to address four additional areas: key management, PIN management, script processing and fraud risk management parameters. Discussion of issuer considerations is included Section 4.

While each choice must be made independently, some are interconnected, and some choices may vary dynamically depending on the circumstances. In other words, there are numerous possibilities.

Figure 3 highlights the potential complexity of selecting implementation options.



[24] A "contactless only" card is a card with contactless capability and a magnetic stripe, but with no support for an EMV contact chip.

Figure 3. Implementation Options for EMV

One further complication can be the distinction between authentication and authorization. Authentication checks the authenticity of the card itself. Authorization validates the issuing bank's approval of a transaction, considering the status of the cardholder's account (e.g., "open to buy" balance) and the results of fraud checks. As shown in Figure 4, if a card is authenticated offline (A), the transaction can also be authorized offline, subject to certain issuer and payment brand parameters (such as transaction amount); however, if the card is authenticated offline (B) but the transaction must be authorized online, then the card can be authenticated a second time online.

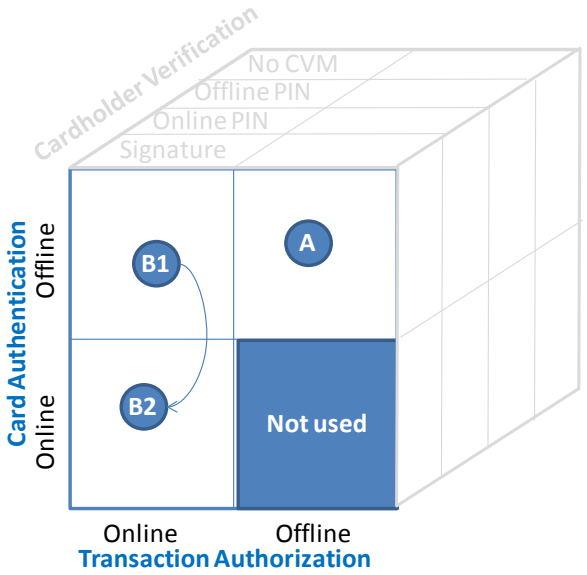


Figure 4. Authorization vs. Online and Offline Authentication

To simplify the analysis, the remaining sections organize and discuss the different options shown in Table 5 for each stakeholder group.

Table 4. Roadmap Options

Roadmap Option		Description
1. Card Interface	a) Contact	• Standard EMV chip card. • Requires contact reader.
	b) Contactless	• RF card, NFC on a mobile phone, or various form factors, including stickers. • Requires contactless reader. • Leverages EMV-based contactless cards being deployed in the U.S. and Canada. • Inability to inject scripts post-issuance, except with second tap, or using over-the-air capabilities with mobile devices.
	c) Dual interface	• Card containing both contact and contactless interfaces. • Works with either contact or contactless reader.
2. Card Authentication	a) Online	• Uses symmetric cryptography for the cryptogram (such as Triple DES). • For online-only contact card, no requirement for SDA, DDA, or

Roadmap Option		Description
		PKI cryptographic co-processor.*
	b) Offline	• Uses SDA, DDA and/or CDA. • Requirement for PKI cryptographic co-processor (for DDA and CDA only).
3. Transaction Authorization	a) Online	• Authorization message, including Field 55, is sent to issuer.
	b) Offline	• Terminal and card negotiate the method for authorization based on the acquirer, issuer and payment brand risk management parameters. The issuer (card) makes the final decision. • May be forced online, depending on limits and other factors.
4. Cardholder Verification	a) Signature	• No special POS requirement beyond current requirements.
	b) Online PIN	• Requires POS PIN pad, secure access module (SAM) linked to hardware security modules (HSM) at every network node, and network capable of supporting PIN block. • Not readily supported by credit card standard messages[25]
	c) Offline PIN[§]	• Requires POS key pad.[26] • Two types of offline PIN: plain text and enciphered. Requirement for PKI cryptographic co-processor for enciphered PIN. • Requires ability to synchronize offline and online PIN
	d) No CVM	• No special POS requirement. • Usually reserved for low value transactions and unattended terminals.

***** All microprocessor cards used for EMV support the appropriate symmetric cryptography algorithm and keys. Symmetric cryptography is employed as a core part of chip security and is used in the personalization process and in any post-issuance EMV scripts from the issuer that are used to change EMV settings on the card.

[§] Offline PIN can be either enciphered or plain text.

3.1.1 Card Interface Options

Each of the three card interface options, contact, contactless, or dual-interface, has advantages and disadvantages for industry stakeholders in an EMV migration.

The contact interface requires the issuance of contact chip cards and the installation of contact chip readers at merchants and ATMs and is required if merchants wish to protect themselves from counterfeit magnetic stripe liability shift.

Dual-interface cards carry both contactless and contact EMV interfaces. Selecting a dual interface card allows the same card to be used both at contactless and contact POS readers. This interface would be ideal for cardholders who travel internationally and where contactless is part of the value proposition.

The U.S. industry is being encouraged to support both contact and contactless EMV at the POS, with issuers able to choose which to support. Contactless cards can leverage current investment in

[25] Standard credit card message 1100 does not support the field required for online PIN support

[26] See PCI specification for POS PIN support requirements for online and offline PIN, https://www.pcisecuritystandards.org/security_standards/documents.php?association=PTS

contactless terminals and cards and prepare the industry to support NFC mobile contactless payments.[27] On the other hand, since much of the rest of the world is implementing contact EMV (and, in some markets, both contact and contactless EMV), the U.S. chip card acceptance infrastructure would be incompatible. (For a further discussion of this issue for international travelers, see Section 3.2.)

For the foreseeable future, all cards will continue to carry a magnetic stripe to ensure acceptance in areas of the world that still have terminals that do not support EMV.

3.1.2 Card Authentication and Transaction Authorization Options

It is important to differentiate between offline *authentication* and offline *transaction authorization*. EMV is designed so that both offline and online authentication can be leveraged in a single transaction. Even when transactions are authenticated online, if the card supports SDA, DDA, or CDA, offline authentication procedures will be performed as part of the EMV transaction. Performing offline authentication neither requires nor implies that the transaction be performed completely offline. With EMV, a card can perform transactions offline even when terminals are online-capable until a certain dollar amount or number of consecutive transactions is reached, at which time the transaction goes online.

Online card authentication and online transaction authorization together (referred to as online EMV in this white paper), is a streamlined implementation with 100 percent online authentications. Online EMV may be appropriate for countries with a fast, reliable telecommunications infrastructure, such as the U.S. For online authentication, the EMV standard specifies that the card use symmetric keys. An online only EMV implementation does not need to support SDA and/or DDA. Implementation of online EMV, especially if contactless, leverages the industry's investment in contactless terminals,[28] contactless cards, and implementation of new fields in the authorization message to carry the 8-byte cryptogram and related chip data.

Another option is to implement offline-capable EMV but require the majority of transactions to be online. In Canada, only a few acquirers are offline-capable. The others are "online preferring" and set their risk parameters to require an online attempt, but have non-zero floor limits to allow offline (within limits) if online is not available. However, POS terminals installed at Canadian merchants all support the full complement of SDA, DDA, and CDA. See Section 2.1.4 for more information on offline-capable and online-preferring implementations.

3.1.2.1 Clearing and Settlement

Offline authorization has additional implications for clearing and settlement; this may require the acquirer to make software modifications to support full chip record data in the clearing message.

Acquirers will need to make this change in clearing and settlement since some payment brands require support.

3.1.3 Cardholder Verification

The cardholder verification methods – online PIN, offline PIN, signature, or no CVM – will be based on the issuer preference for the card product (i.e., ATM, debit, credit) and terminal capability. Considerations for choosing the CVM are discussed in Sections 4 and 5.

---

[27] For the purposes of this white paper, it is assumed that the CVM for NFC will be the same as for a contactless card; i.e., a PIN for NFC mobile contactless payments uses the POS PIN pad, not the phone itself, for PIN entry. Using the phone to enter a PIN is not yet a defined or standardized approach and would require additional changes to the payments infrastructure.

[28] Contactless terminals deployed in the U.S. operate in contactless MSD mode. To become EMV-capable, these readers typically require a firmware upgrade, including an EMV Level 2 software kernel, and application upgrades. Whether upgrading can be done remotely depends on the terminal management system and its capability for remote downloads. Without remote upgrade capability, a reader may have to be returned to the manufacturer for refit.

3.2 Status of Debit Networks

Four networks are owned by the payment brands (Visa's Interlink®, MasterCard's Banknet® and Maestro®, and Discover's PULSE®). As of the date of this white paper, no specific EMV announcements have been made by the other debit networks (e.g., Accel/Exchange®, Access 24, AFFN®, Alert, Cirrus, Credit Union 24®, Instant Teller, Jeanie®, Money Belt, Most, NYCE®, SHAZAM®, STAR® (including former network brands MAC, Cash Stations, Explore, Honor) or TYME).[29]

In April, 2012, the Secure Remote Payment Council (SRPc) formed a working group to define and adopt a POS and ATM solution for chip and PIN acceptance for PIN debit networks. The goal of this collaborative effort is to provide interoperable adoption of chip and PIN debit payments to the industry, while supporting innovation, choice, and the proven track record of PIN security in reducing payment fraud. The working group includes PIN debit networks STAR, SHAZAM, PULSE, NYCE, AFFN, ACCEL/Exchange, ATH®, Credit Union 24, CO-OP Financial Services and Jeanie.[30]

3.3 Durbin Amendment Implications for EMV and Chip

The following material is not intended to be legal advice, nor is it a comprehensive list of issues that could impact payments industry stakeholder business. If there are questions about the legal implications of this material, please direct them to corporate counsel.

On June 22, 2011, the Board of Governors of the U.S. Federal Reserve System published a final rule on Regulation II, Debit Card Interchange Fees and Routing. This rule implemented the provisions of Section 920 of the Electronic Fund Transfer Act (EFTA) as amended by Section 1075 of the Dodd Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act).

Within the final rule, Section 920(b) of the EFTA required the Board to issue rules that prohibit network exclusivity arrangements and debit card transaction routing restrictions. The final rule, defined under Section 235.7(a):

> ***"prohibits an issuer or payment card network from restricting the number of payment card networks on which an electronic debit transaction may be processed to fewer than two unaffiliated networks, regardless of the method of authentication."***

In layman's terms, the rule requires that debit card issuers participate in at least two unaffiliated debit networks. This could be accomplished by having at a minimum:

1. One signature network and one unaffiliated PIN network
2. Two unaffiliated PIN networks
3. Two unaffiliated signature debit networks

3.3.1.1 Durbin in Magnetic Stripe Environment

In a magnetic stripe environment, the ability to apply this rule is straightforward. Given that almost all debit cards issued within the U.S. carry a signature debit network, the most widely adopted approach to meeting the network exclusivity requirements would be to have one signature debit network on the card, along with one or more unaffiliated PIN debit network, as well as, one additional PIN debit network that is affiliated with the signature debit network. An example would be a card issued with one signature debit network on the front and one or more PIN debit networks on the back.

When a card of this nature is swiped at the point of sale, the merchant has the ability to:

[29] Source: http://www.atmscrip.com/processing_networks.html

[30] Source: Secure Report Payment Council, http://secureremotepaymentcounci.camp8.org/Resources/Documents/120426_SRPc_Chip%20and%20PIN_Network_WG_Press%20Release.pdf

A. Prompt the cardholder to select debit or credit (if that option exists on the terminal).

B. Route the transaction to any of the networks on the card that accept the type of cardholder verification selected (i.e., signature or PIN).

If the cardholder or merchant selects credit as their payment method, the debit transaction is routed to the one signature network affiliated with the card. If instead, a PIN was entered, the merchant has the option to route the transaction to one of the PIN debit networks supported by the card.

3.3.1.2 Durbin in EMV/Chip Environment

Applying this same network exclusivity rule in an EMV or chip card environment introduces a level of ambiguity. Due to the proprietary nature of a network's chip application, typically when an application is selected, the routing of that transaction must go to the network associated with the chip application in order for the chip application to be processed correctly and to ensure application security.

Using the same card example defined above, if the terminal selects a specific payment brand's EMV application/AID, then that transaction must be routed to that payment brand. If the merchant elects to route the transaction to a different payment network, then the terminal must select that payment network's EMV application/AID and route the transaction to the network that supports that application. In essence, the merchant is making the routing choice based on the AID/application they select.

Should Section 235.7 of Regulation II, be interpreted to mean that issuers implementing EMV must offer two unaffiliated chip applications on their cards? While no definitive answer to this question has been given, the Federal Reserve did attempt to provide further clarification in an October 2011 release of frequently asked questions.

> ***§ 235.7 Network Exclusivity and Routing Provisions***
>
> ***Q1. Does a debit card comply with the provisions in § 235.7 if the card is enabled for processing transactions over two unaffiliated card networks but, once the card is swiped, the transaction is required to be authenticated using a specific authentication technology available only through one network enabled on the card?***
> *A1. No. Section 235.7(b) prohibits an issuer or a network from inhibiting the ability of any person that accepts or honors debit cards for payments to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions. If an electronic debit transaction initiated using a debit card enabled for certain authentication technology (e.g., a chip) must, once the card is swiped at the point of sale, be processed over a specific payment card network, that debit card does not comply with the prohibition on merchant routing restrictions under § 235.7(b) if the merchant is unable to direct the cardholder to authenticate the transaction so that it may be processed over at least one other unaffiliated network enabled on the card. (Added October 24, 2011)*[31]"

This response from the Federal Reserve Board could be interpreted by some to mean debit issuers will need to provide two or more chip application options on a card. With no clear answer, it is up to each individual issuer to work with their legal counsel to determine their own interpretation of the law.

3.3.1.3 Durbin Considerations in EMV/Chip Environment

For issuers and merchants contemplating migration to EMV and chip technology, there are several questions issuers and merchants should be asking their industry partners.

Quite possibly the most important question might be what chip application options are available in the market today? This list would include the well-known EMV applications from American Express, Discover, MasterCard and Visa, the royalty-free EMVCo Common Payment Application (CPA)[32] and Common Core Definition (CCD)[33] application specifications published and managed by EMVCo, and domestic payment specifications, such as Interac (Canadian debit brand) and First Data's STAR.

Specific questions that issuers may want to approach their industry partners about include:

[31] http://www.federalreserve.gov/paymentsystems/regii-faqs.htm
[32] Common Payment Application (http://www.emvco.com/specifications.aspx?id=19)
[33] Common Core Definition (http://www.emvco.com/faq.aspx?id=102)

1. Does the chip card vendor offer a chip that can support two or more chip applications that are acceptable to the debit networks with which the cards will be affiliated?
    - Does it support contact only, contactless only and/or both contact and contactless?
2. Can the personalization bureau support personalizing a card with two or more chip applications that are acceptable to the debit networks with which the cards will be affiliated?
    - Can they support requirements for dual contact, dual contactless and/or dual contact and contactless cards?
3. What chip technologies do the various PIN debit networks affiliated with the cards support?
    - Are they EMV compliant?
    - Do they have to be EMV compliant?
    - Can their EMV solution coexist with another chip application on the card?
    - How will their contactless application work on an EMV contactless terminal?

For merchants, questions they should be approaching their industry partners with include:

1. What chip applications does the terminal vendor support?
2. Do these applications support contact, contactless and/or both?
3. How do I maintain routing choices in a chip card environment?

With the investment needed to support an EMV chip migration, it is vital that issuers and merchants have a clear strategy on how they will support debit programs using chip cards while maintaining the rules set forth in the Durbin Amendment and the regulations defined by the Federal Reserve. While several questions still remain at the industry level, it is important to consult and collaborate with industry partners to understand the options available and to best prepare the organization while limiting the financial impact that comes with an EMV chip migration. In addition, cardholder education may be needed to address any confusion that may arise regarding choice of application.

Understanding how EMV has been designed to support multiple payment applications on a single card is necessary when considering the debit strategy and assuring that compliance with Durbin. In the EMV/chip environment a payment application is associated with an application identifier or AID. The AID is assigned by the American National Standards Institute (ANSI) or ISO/IEC through a process defined under ISO/IEC 7816-5:2004 Identification cards – Integrated circuit cards – Part 5: Registration of application providers. A specific AID is selected by employing a process defined by EMV and referred to as “application selection” (described in Section 2.2). One could then assume that the transaction is to be routed through the corresponding AID owner’s network.

In the case where the issuer-supported networks use different payment application specifications (e.g., VIS, M/Chip, D-PAS, AEIPS), the chip must support both, and each AID will be associated with each of the applications. Alternatively a domestic network may be able to license an established application specification and allow the issuer to only create a separate instance of the same application with different AIDs for each affiliated debit network. Domestic networks can also define their own application specification.

In order to comply with Durbin, the payment networks will need to define specific rules governing how the routing decision is to occur. Some payment networks have already had to address this situation in other domestic networks where domestic payment brands or closed loop store cards coexist with international payment brands. These rules could be used as a base for how the requirements defined within Durbin will be satisfied.

Merchants, issuers and acquirers are advised to consult with and encourage their industry partners to define a sensible solution that meet the needs of all stakeholders.

3.4 Payment Brand EMV Implementation Guideline Summary

The preceding sections described the different EMV implementation options. Table 4 summarizes the recommended guidelines provided by the payment networks as of the publication date of this.

Table 5. EMV Options: Recommended Guidelines by Payment Network[34]

EMV Options	Visa[35]	MasterCard[36]	Discover	American Express
1. Card Interface	Issuer choice Dual-interface or contact chip card with companion contactless mobile application POS supports contact and contactless Contactless MSD POS support not required after October 2015.	Issuer choice Dual-interface recommended for best cardholder experience	Issuer choice	Issuer choice
2. Card Authentication	Online	Online DDA/CDA if offline is supported (issuer choice)	Online and offline Issuer choice	Offline and online For offline card authentication, issuer must support DDA or CDA
3. Transaction Authorization	Online	Online Offline if issuer opts to support	Online and offline Offline if Issuer chooses	Online
4. Cardholder Verification	Issuer choice Signature, online PIN (debit), no CVM	Issuer choice Signature, online PIN, offline PIN, no CVM	Issuer choice Online PIN, Offline PIN, signature, no CVM	Online PIN, offline PIN, signature, no CVM

3.5 Implications for International Travelers

Aite Group[37] has estimated that 9.7 million U.S. cardholders experience magnetic stripe card acceptance issues when they travel internationally in 2008, costing banks $447 million in lost revenue. A small percentage of European offline-only POS terminals, mostly located at after-hours and unattended gas stations and train ticketing kiosks, will not accept online-only EMV cards and may not accept chip and signature cards either.[38] While such locations are currently in the minority, there tend to be fairly significant consequences if cardholders are unable to use their payment cards at them. This situation

[34] The milestones in Table 4 are based upon Smart Card Alliance Payments Council analysis and payment brand input as of publication time. Continued analysis or updates from any of the key stakeholders may result in modifications of the guidelines. Any changes will be communicated in future publications or on the EMV Connection web site (http://www.emv-connection.com), as needed.

[35] http://usa.visa.com/download/merchants/bulletin-chip-recommended-practices.pdf

[36] MasterCard has a liability hierarchy.

[37] "The Broken Promise of Pay Anywhere, Anytime: The Experience of the U.S. Cardholder Abroad," Aite Group report, October, 2009, http://www.getfluentc.com/pdf/Aite_Group-Broken_Promise_of_Anytime_Anywhere_Report.pdf

[38] Source: Smart Card Alliance Payments Council

necessitates a critical decision for U.S. issuers. Should they issue online-only EMV cards and accept the risk that their cards will not work in offline locations? If issuers expect cardholders to be able to use their cards at unattended terminals, serious consideration must be given to whether to support offline PIN. Should they configure their cards to go online whenever possible and only allow offline transactions when the terminal indicates that it cannot go online?

The contactless options represent another issue. Since most markets have implemented contact EMV, U.S. international travelers would need dual-interface cards, equipped with both contact and contactless EMV. U.S. merchants who cater to international visitors would need to install contact readers to accommodate internationally-issued contact EMV cards

4 Card Issuer Considerations

EMV provides a variety of options that support implementation flexibility; an issuer can implement the options that best fit the issuer's needs and marketplace. This section discusses the issuer implications for selecting particular implementation options in five key areas: the card (chip) interface, the cardholder verification method, the personalization system, the host system, and the transaction authorization process.

4.1 Card Interface

One of the first decisions an issuer must make in deploying EMV is to decide on the card interface: contact, contactless, or dual. This decision would be based on the individual issuer's goals and objectives for issuance and business plan. The interface decision will also help determine the associated payment brand EMV application that will be personalized on the card to support contact, contactless or dual-interface chip cards. Key considerations in this decision are the target customers and products for EMV migration.

- Contact cards and readers are widely deployed in markets outside of the U.S. To enable cardholders to use EMV payment cards internationally, a contact EMV card would provide global acceptance.
- For contactless payments, U.S. reader infrastructure deployment is currently based on contactless MSD, while the emerging Canadian and European contactless infrastructures are based on contactless EMV. Each brand may have requirements around contactless MSD vs. contactless EMV.
- Dual-interface cards supporting both contact and contactless interfaces would enable the broadest acceptance, but incurs additional cost for supporting both interfaces.

4.2 Offline PIN vs. Online PIN

As discussed in the previous section, the offline PIN is distinct and separate from online PIN and is verified at the POS. Issuers need to weigh the advantages and disadvantages and business and infrastructure impact of supporting signature, online PIN and/or offline PIN for credit and debit products.

Offline PIN can be supported in two ways:

- Plain text offline PIN. The chip reader sends the PIN to the chip on the card as plain text.
- Enciphered offline PIN. Either the secure component in the POS device (for example, the chip reader) or the PIN pad itself enciphers the PIN, using an authenticated encryption public key from the chip. The enciphered PIN is sent to the chip, where the PIN is deciphered using the private key from the chip.

Enciphered offline PIN requires asymmetric (RSA) cryptography support and a card with a cryptographic co-processor. These elements require additional system support.

Additionally, the issuer needs to be able to manage the offline PIN for basic servicing, such as PIN resets and unlocks. This type of servicing requires the ability to support issuer EMV scripts. An issuer should consider how these scripts can be delivered to the card, such as through an in-person branch visit or through the ATM network. For cardholder convenience and ease of use, synchronization between the offline PIN and online PIN may require additional resources and considerations.

4.3 Personalization System

When preparing to issue EMV cards, issuers need to consider the hardware, software and issuance process implications. Issuance of EMV cards requires additional software and a hardware security

module (HSM) for EMV data preparation and key management at the data center and additional hardware and software to be added to the central issuance personalization equipment.

During card issuance, the personalization system will execute 'personalization scripts' in order to load each individual card with the right set of:

- Applications (e.g., EMV application)
- Application data values (e.g., EMV parameters)
- Application cryptographic keys (e.g., EMV cryptographic keys)

These components have been prepared for the card by the data preparation and the key management applications, in addition to the usual track data. Issuers should be aware that personalization scripts will differ by card product and may be greatly affected by modifications of operating system type (i.e., native, Java or MULTOS) or chip type. Issuers should try to anticipate these decisions well ahead in order to avoid delays or rework.

For EMV payment applications, the EMV parameters convey the issuer's implementation choices to the EMV application on the chip. The volume of EMV parameters to be personalized on a chip card is quite large compared to the volume of data that needs to be personalized on a magnetic stripe card. Therefore, issuers should allocate enough time for the definition of the EMV parameters.

In some cases, it may be possible for issuers to update some of the EMV parameters later on during the post-issuance phase – that is, after the cards are issued and in the hands of cardholders. This process, by which the issuer sends parameter updates to the chip either through the payment network or using a POS in a branch, is referred to as 'EMV issuer scripting. '[39] Although a powerful tool in the hands of issuers, this process needs some advanced setup and should not be used by issuers as a reason to postpone their decisions concerning the definition of the EMV parameters.

The cryptographic keys are integral to EMV authentication security and to secure post-issuance updates through EMV issuer scripts. Both the data preparation and the key management applications require an HSM to generate, store and process the EMV cryptographic keys during the data preparation process. The applications can share the same HSM or use separate HSMs.

The EMV data preparation and key management applications can be installed in the issuer's secure data center or issuers can outsource this functionality to a full service personalization bureau that already has them installed and audited by the payment brands that they support.

The central personalization equipment must also add support for chip personalization. If the issuer, or the service bureau, has not yet added support for chip card personalization to their issuing equipment they will need to purchase an IC module upgrade for their existing equipment or may have to purchase new central issuance equipment with chip personalization capability. A chip personalization module can be purchased with either contact or contactless support, and in some cases, one module can support both contact and contactless chips. The personalization equipment provider can recommend the best personalization module configuration based on the issuer's objectives.

An HSM and special EMV personalization software that interfaces to the personalization equipment is also required to support chip programming through the central issuance equipment. HSMs are used to store cryptographic keys, derive keys during personalization, and secure the personalization communication lines.

4.4 Host System

For issuers (or processors) to support chip cards, they must process full chip data or use the data processing service from a payment brand. The service is commonly called the "early chip data option" or

[39] 'EMV issuer scripts' (executed in post-issuance) should not be confused with 'personalization scripts' (executed during card issuance).

"on-behalf chip authentication." This service is available for processing both contact and contactless data. The service offering provides an issuer with the flexibility to process chip cards initially while making the needed changes to support the new fields required by EMV for full chip data migration.

Most of the processing validates the authorization request cryptogram and, if needed, generates an authorization response cryptogram to send back to the chip. To validate the cryptogram, the issuer or processor must hold the symmetric key used by the card. The chip data is then used to recalculate the cryptogram value and match it to the value calculated by the card. This process, known as card authentication method (CAM) validation, is a powerful deterrent to the creation of counterfeit cards.

The on-behalf chip authentication service offering requires the issuer or processor to make few or no changes to the host system, thereby reducing initial implementation expense and potentially speeding up deployment. The disadvantages of selecting this option include reduced issuer visibility at the point of transaction (e.g., the issuer will not get the full chip data in Field 55; however, they could be provided with the cryptogram validation results) and limited flexibility in making changes on the chip such as unlocking and changing an offline PIN through issuer scripting.

The full chip data option requires changes to the host system to process chip transaction data. The benefits of this approach include greater issuer visibility at the point of transaction and immediate flexibility in being able to take appropriate actions. In addition, Field 55 includes chip data that could be used in an issuer's host system for additional risk scoring and fraud evaluation. However, this approach implies that the issuer will incur the cost associated with changing the host system.

4.5 Transaction Authorization Process

The U.S. is primarily a magnetic stripe card environment. The transaction authorization process therefore relies on static data to authenticate transactions and online networks to authorize transactions based on risk parameters. Today, a cardholder swipes a magnetic stripe card at a merchant terminal, the track 1 or 2 data is captured, and the transaction is sent to an acquirer, routed to the appropriate payment brand/network, and ultimately sent to an issuer for authentication and authorization. The issuer validates the track data and determines the authenticity of the card based on the static CVV/CVC/CID data element within the track. Once the card is authenticated, the issuer applies its risk parameters and uses fraud neural networks and the online PIN result (if appropriate) to determine the authorization response.

This processing is facilitated cost effectively through the widely available and robust U.S. telecommunications infrastructure, which delivers nearly all transactions from merchants to issuers online. For a long time, U.S. issuers have been able to leverage this transaction processing model to manage fraud effectively. But the rapidly changing fraud landscape and scale of recent data compromises make EMV migration a compelling long-term solution since EMV devalues the usability of stolen data for the purpose of fraud.

The EMV transaction authorization process relies on dynamic data to authenticate transactions, and certain risk parameters can be managed by the issuer within the card. In an EMV scenario, a cardholder inserts an EMV card into the reader, and the merchant POS terminal identifies which payment brand application is on the card so the terminal uses the appropriate payment brand application protocols. Once an application is selected, the card and terminal enter into a dialog to conduct terminal and card risk management to determine whether the transaction should be performed and approved offline or sent to the issuer for online authentication and authorization.

An issuer can use card risk management and the issuer-defined risk management parameters to decide whether and when a transaction will be authorized offline or require online authorization. If offline transaction processing is implemented by an issuer, a variety of offline features must be considered, such as offline data authorization controls, offline data authentication, and online or offline CVMs. If online transaction processing is implemented by an issuer, the card supports online card authentication and online or offline cardholder verification methods. For online card authentication, the chip generates the EMV cryptogram called the authorization request cryptogram (ARQC). Track 2 equivalent data, the ARQC, the associated signed data, and potentially the CVM's online encrypted PIN or offline PIN comparison results are sent in the authorization message. The issuer validates the authorization

message and authenticity of the card based on the ARQC. The issuer can also use the offline and online risk management results to determine the authorization response.

4.6 Summary

Table 7 summarizes considerations for issuers.

Table 6. Issuer Considerations

Roadmap Option		Consideration
1. Card Interface	a) Contact	• Contact cards and readers are widely deployed in markets outside of the U.S.
	b) Contactless	• Contactless cards and readers are a growing trend in global deployment. • Issuers will need to recognize the difference between contactless MSD and contactless EMV and choose which to support. At this time, some early contactless MSD cards may not be accepted outside of the U.S.
	c) Dual interface	• Supporting both interfaces incurs additional costs.
2. Card Authentication	a) Online	• Issuers must choose whether to validate card data on their own or allow card brands to validate on their behalf. Issuers must choose whether to receive full chip data or early chip data.
	b) Offline	• Issuers must choose whether to support offline card authentication and if they will employ SDA, DDA and/or CDA. • Issuers must support a public key infrastructure for offline card authentication.
3. Transaction Authorization	a) Online	• Issuers must choose whether to receive full chip data or early chip data for card authentication.
	b) Offline	• Issuers can apply various risk parameters to allow the EMV chip to authorize transactions offline on their behalf. Risk parameters may include checking transaction amount limits and the number of consecutive offline transactions before requiring an online authorization to be performed. • Offline authorization has impact on the clearing data and process. • Issuers will need to modify their clearing and settlement systems to receive additional chip data (generally in the same format as Field 55 in the authorization request). Clearing and settlement systems should ensure that offline transactions can be identified.
4. Cardholder Verification	a) Signature	• Signature is included in the CVM list on the chip unless otherwise specified by the payment brands.
	b) Online PIN	• Issuers can include online PIN in the CVM list. The online PIN infrastructure will need to be supported by issuer. ATMs only support online PIN.
	c) Offline PIN	• Issuers can include offline PIN in the CVM list. The offline PIN infrastructure will need to be supported by the issuer for PIN management.

Roadmap Option		Consideration
		• Offline PIN and online PIN should be synchronized to prevent cardholder confusion. • Issuers will need to support Field 55 through full chip data processing in order to perform issuer scripting (for example, for unlocking and changing offline PIN).
	d) No CVM	• No CVM is included in the CVM list unless otherwise specified by the payment brands.

5 Payments Acquirer/Processor Considerations

EMV acceptance represents a dramatic departure from the simple magnetic stripe card for the acquirer, processor, merchant and cardholder. Although there is the promise of reduced fraud and greater payment security, there is a good deal of cost, systems work, analysis, process, training and patience that will be needed for an acquirer or processor to accept EMV transactions.

In the case of a contact EMV card, the card will be inserted into the reader usually by the consumer and remain there during the entire transaction unlike a magnetic stripe transaction where the card is swiped. This will require a change in merchant and consumer behavior.

In the case of an EMV contactless card, even those U.S. merchants that installed contactless peripherals will need to update clerk training as most cardholders are not using the readers for contactless cards at this time. This will require merchant investment and clerk acceptance training.

In most cases, a merchant's terminal or POS hardware will require updating to accept EMV contact and contactless cards. Those merchants with Tranz, Omni, T7 and other legacy terminals will need to "throw out the old and bring in the new," replacing non-EMVCo certified terminals with EMVCo-listed terminals and peripherals that provide contact and contactless EMV acceptance in addition to magnetic stripe.

In view of the coming payment brand acquirer/processor liability shift, merchants will need to consider upgrading their terminals, thus compelling the acquirer or ISO to invest in marketing and sales training to answer inquiries such as: "if I invest in EMV will my cost of payment be reduced?," "will my customer have EMV cards and use them in my store?," "why is this any different than when I installed the contactless reader, nobody is using the readers?," "what happens if I don't purchase a new terminal to accept these new cards?," and "are magnetic stripe cards going away?" Answering these questions will require customer support and sales training, along with an investment in marketing.

As of the date of publication, there are still some questions about the specific requirements for acquirers and processors implementing EMV and there appears to be little consistency among the brands in regards to acceptance and processing of EMV transactions. Nonetheless, acquirers and processors need to be ready for April, 2013. The following provides high-level considerations for acquirers and processor for migrating to EMV acceptance.

Pre-development Considerations

- EMV education is a key first step for acquirers and processors that need to implement EMV support. Knowledge of EMV will be different for each group within the company – e.g., support, front-end/back-end development, terminal development. Team with knowledgeable training providers that have experience internationally as well as have offices in the U.S.
- The payment brands can also provide training and can help with understanding their versions of the EMV specifications. They can also provide clarification on requirements for supporting online and offline PIN, offline authorization, online and offline card authentication, the choice of cardholder verification method, and other details.
- Both of the above considerations will save an acquirer or processor time and trouble. Since April 1, 2013, is not that far away and since certification testing queues will be crowded, it's even more important for acquirers, processors and their support teams to have a solid plan.

Front-end Authorization Systems

- Front-end systems need to be updated to accommodate the additional fields and logic necessary to support EMV acceptance.
- Obtain access to payment brand EMV specifications, as enhancements will be needed to the front-end systems.
- It is advisable that the processor or acquirer reach out to the payment brands for assistance interpreting those specifications.

- The acquirer or processor will note differences among the payments brands' implementations of EMV and must build those differences into their authorization systems.
- It is also advisable to enlist a consulting company that is familiar with implementing EMV to save time and error.

Key Management

- Acquirers and processors may need to consider the strategy for supporting online PIN-based credit, including, for example, making system software and hardware changes and putting a key distribution and management process in place.
- Acquirers may also need to consider how to manage the public keys associated with offline authentication, as well as offline encrypted PIN, for self-supported terminals and third parties that interface to the acquirer/processor for processing. The equipment and personnel that will be required needs to be determined, as well as a key exchange process implemented.

Back-end Settlement Systems

- Settlement systems must be updated to support required EMV data from new fields in the clearing records for submission to the payment brand networks, to ensure proper interchange qualification and support new interchange categories.

Gateways

- Gateway specifications and peripheral interfaces will need to be enhanced to enable third parties to integrate and certify to the EMV-enabled front-end.
- Gateways will typically need testing and must work with the acquirers and payment brands to ensure compliance with the acquirer and payment brand specifications.

Third-party Developers and POS Systems

- The certification team will need to be fluent in EMV to communicate with customers and third parties looking to update their certification.
- Certification processes and documentation will need to reflect the enhancement to EMV.
- Development-level support personnel will need to knowledgeable about interface specifications.

Attended Terminal Hardware

- Hardware providers are either going to need to leverage the terminals they sell and support internationally for the U.S. market or provide PIN pads that interface to legacy terminals or both. Meet with the terminal providers to understand their EMV migration plans.
- Acquirers and processors will need to check EMVCo's list of Level 1 and 2 certified hardware to ensure that future terminal hardware purchased is EMV-ready.

Attended Terminal Software

- If the acquirer or processor leverages a vendor's attended terminal software, the version of the vendor's software that supports EMV to the front-end or gateway will need to be enhanced. That combination of hardware and application will need to be certified according to the payment brand requirements.
- If the acquirer or processor has developed an attended terminal application or POS system, the front-end or gateway specification will need to be referenced to make enhancements to the application for EMV acceptance.
- Check with the payment brand representative to ensure that their requirements for certification of attended terminals and POS systems are met before going to market.

Customer Support

- An acquirer/processor will need to spend considerable time educating their customer service groups about the workings and benefits of EMV for the merchant. Merchants will have many questions after updating their brick-and-mortar terminals, even after store-level training.
- Those merchants with POS systems for which the software was written by a third party will also call the acquirer or processor help desk seeking answers to transaction acceptance questions.
- Collectively, an investment in course development or acquisition of an EMV 101 course from a third party will be needed.

Sales and Sales Support

- In addition to customer support training, the sales force and sales support team will need to be educated. These groups are on the front line and will need to understand EMV's value proposition for the merchant in addition to being aware of the operational needs of a merchant with EMV.
- In addition to EMV training, sales and sales support will have new terminals, EMV peripherals and EMV-enabled software with which to become accustomed. This training will take time and the acquirer/processor might want to consider enlisting a third party resource to help with this effort.

Marketing

- The processor's or acquirer's marketing group will have a central role in making the migration to EMV a success. Marketing will need to be educated on the elements of EMV, its value proposition for merchants, and the "trials and tribulations" that a merchant is going to encounter when migrating to EMV.

The following sections describe the changes to the acquiring/processing infrastructure that are required to support contactless EMV and contact EMV transactions.

5.1 Contactless EMV

In a contactless EMV transaction, presenting the contactless card to the POS device sends the chip data from the card to the POS device. The processor must be able to receive all possible types of chip data from the POS device and place the data in the appropriate Field 55 tags and in any custom tags used by a particular payment brand.

In addition, processors will need to support new fields and values to identify the POS entry method (for example, ISO/IEC 8583 Field 22) and the card sequence number (Field 23) when obtained from the chip. Terminal vendors and software providers must certify that they will transmit the fields appropriate to contactless EMV transactions to the processors. Processors must certify that they will transmit the appropriate fields to the payment brand networks. Processors must update systems to store the appropriate data from Field 55. Settlement systems must be updated to support required data from fields carrying EMV data in the clearing records for submission to the payment brand networks, to ensure proper interchange qualification and support new interchange categories.

5.2 Contact EMV with Signature or PIN

The changes required by contactless EMV transactions are also required by contact EMV transactions, with the exception that the chip data is only retrieved by the chip reader or the "dip." When the transaction requires a PIN, the PIN is validated using an offline plain text PIN (sending the unencrypted PIN to the card), an offline enciphered PIN (encrypting the PIN entered before sending it to the card), or an online enciphered PIN (encrypting the PIN entered before sending it online to the card issuer). For the online enciphered PIN, the processor must implement the PIN infrastructure and must be able to support receiving the encrypted PIN and passing this encrypted PIN to the payment brand network. Merchants must have the ability for cardholders to enter the PIN.

5.3 Clearing and Settlement Considerations

Acquirers must ensure that they support the sub-elements necessary to clear and settle EMV contact and contactless transactions. The following is a summary of the data elements required for settling EMV transactions:

- Acquirers will need to support all mandatory and applicable data elements within Field 55 for integrated circuit card (ICC) based transactions. These data elements include online authorization request, online authorization request response, online authorization advice, and first presentment clearing records.
- Field 22 represents the point of service data and indicates to the issuer the capabilities of the terminal and whether the terminal was PIN-capable, as well as whether the chip or the magnetic stripe was read. Field 22 is required when Field 55 is present.
- Field 23 represents the card sequence number and distinguishes among separate cards having the same PAN. For chip transactions that include Field 55, Field 23 must be present and contain the Application PAN Sequence Number if provided by the ICC to the terminal.
- Field 40 represents the service code and provides codes that increase the issuer's flexibility in defining card acceptance parameters as well as provide acquirers with the ability to interpret card acceptance preferences for all point-of-interaction conditions. Please note that Field 40 is not necessary for all payment brands. The acquirer/processor will need to check with each payment brand and the debit networks.

5.4 Summary

For all EMV processing, processors must be able to receive authorization response cryptogram data and EMV scripting data in the response messages from the payment brand networks and pass this data to the merchant POS device.

All devices and software must be certified by EMVCo and the payment brands before they can be used to process EMV transactions.

Payment acquirers must decide which readers, devices, and software applications to certify and deploy, based on their merchants' needs. Processors will need to determine operating system support capabilities and certify with the payment brands. Processors with multiple platforms will need to determine each system's capabilities; support may be limited to one platform.

Table 8 summarizes acceptance considerations for acquirers and processors.

Table 7. Acquirer/Processor Considerations

Roadmap Option		Consideration
1. Card Interface	a) Contact	• May require a PIN pad or integrated PIN pad with integrated terminal • Will require customer support and merchant training on use and exception condition handling
	b) Contactless	• PIN debit is not supported by all payment brands for contactless transactions.
	c) Dual interface	• PIN debit is not supported by all payment brands for contactless transactions.
2. Card Authentication	a) Online	• Field 55 and other required and optional fields (e.g., Field 22, Field 23) must be supported in the authorization request and authorization response.

Roadmap Option		Consideration
	b) Offline	• Field 55 and other required and optional fields (e.g., Field 22, Field 23) must be supported in the authorization and/or clearing record. • The public keys of the appropriate payment brands must be loaded and managed within the POS device.
3. Transaction Authorization	a) Online	• Depending on issuer rules, credit transactions may need PIN entry.
	b) Offline	• Offline authorization has impact on the clearing data and clearing and settlement process.
4. Cardholder Verification	a) Signature	• Issuer dependent.
	b) Online PIN	• If online PIN for credit card transactions is required, then credit card processing must change to accommodate the online PIN. • Requires a PIN pad.
	c) Offline PIN	• Requires a keypad.
	d) No CVM	• Transactions at or below a specified amount based on merchant type do not require merchants to obtain and validate the signature at the POS. • Terminals must be configured to *not* request a PIN or signature at the POS if the chip does not require cardholder verification.

6 POS Terminal and Merchant POS System Considerations

The capabilities of the POS terminal play a pivotal role in the success of any payment innovations. Issuers can distribute cards and other payment devices with new functions (such as sophisticated fraud prevention or customer convenience and marketing functions), but the cards are doomed to fail if retailer POS terminals cannot support the innovations. Even the adoption of magnetic stripe technology took years, primarily because of the amount of time it took for appropriate POS terminals to be widely deployed. In the current era of rapid technology innovation, terminal capabilities will have increasing influence over the success of new payment innovations.

The terminal industry itself is going through a revolution that demands greater flexibility and the ability to adapt rapidly to a broad set of possibilities. So, just as retailers need a payments roadmap to plan and develop the POS requirements for their stores, terminal providers need a roadmap for product development to remain relevant and competitive.

In the past, POS terminals in the U.S. were devoted to supporting magnetic stripe technology and, in recent years, contactless MSD transactions (often referred to as U.S. contactless because POS terminals in the U.S. have been programmed to support contactless MSD transactions only, so that even when a contactless card that supports both EMV and MSD is presented, the transaction will be processed as a contactless MSD transaction). However, in the U.S., terminals will need to support contactless EMV, contact EMV, and NFC applications. Given all of these, it is important to consider the following parameters for EMV migration:

- Hardware support
- Software support
- EMV and brand type approval
- Transaction messaging support
- Terminal software upgrade capabilities and plans

6.1 Hardware Support

To support EMV cards, a terminal needs a contact EMV card interface device (IFD) to read the contact EMV card and a contactless reader that supports the ISO/IEC 14443 standard. Contactless MSD, contactless EMV, and NFC mobile contactless payment all use ISO/IEC 14443.

However, all terminals with a contactless reader that is ISO/IEC 14443-compliant cannot necessarily accept all of these types of payments. The terminals must also include software or firmware that supports the contactless applications used by a particular brand or NFC device. This is an important consideration when evaluating terminals and requires an understanding of terminal software and certification requirements.

Due to some payment brands' requirement for supporting offline PIN verification for contact EMV transactions, a popular architecture is to put the contact IFD and the PIN entry device in the same physical unit. Since offline PIN verification is not required for contactless transactions, it is not uncommon (yet not usually desirable from a user experience standpoint) to use a contactless reader that is physically separated from the POS terminal.

6.2 Software Support

The EMV specifications defined by EMVCo form the global baseline requirements for contact and contactless EMV transactions. Specifications from payment brands (e.g., American Express, Discover, MasterCard, Visa) are mainly to clarify the options and areas that are out of scope of the EMV specifications. A single EMV kernel can usually be created to fulfill all mandatory requirements from different payment brands. Any customization and out-of-scope requirements can then be implemented

outside of the EMV kernel at the POS application level. Examples of customization and out-of-scope requirements are user interface, host communications, and receipt printing.

Contactless implementations are more complicated for terminal manufacturers mainly due to the fact that each payment brand has its own processing logic which can be totally different from other payment brands' requirements. Because of this, different contactless kernels are usually created to meet different payment brand's requirements. Merchants and acquirers should ensure that contactless POS devices contain all contactless kernels available. Again customization and requirements that are out-of-scope for the contactless kernel can be implemented in the POS application level.

The multiple contactless kernel situation brings up an interoperability problem: the terminal application does not know which contactless kernel to use until the payment brand of the presented card is known. In order to address this issue, EMVCo created the "Entry Point Specification." The Entry Point module talks to the contactless card first for selecting an application in the card for the transaction. Once the application is selected, the contactless kernel that is responsible for the transaction processing is known. Each payment brand's kernel operates independently and in isolation from other contactless kernels, so the payment brands do not mandate use of the EMVCo Entry Point. Other "traffic director" modules may be built, but as an impartial and recognized source of specifications and standards, EMVCo seems the obvious source for current and future contactless EMV protocols. EMVCo published version 2.2 of their contactless EMV specifications in June, 2012,

Figure 6 illustrates the relationship between application logic and each chip payment type.

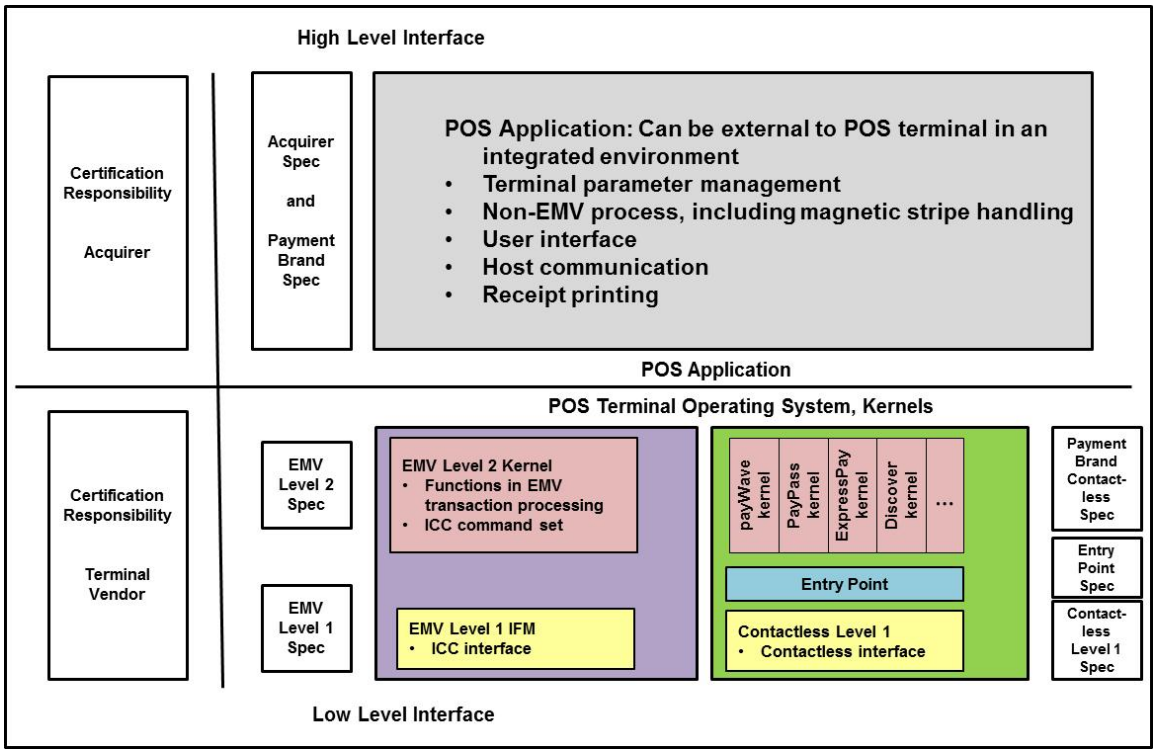


Figure 5. Detailed View of POS Terminal Software Components

NFC-enabled devices can operate in peer-to-peer mode, read/Write mode or card emulation mode. When operated in card emulation mode, the NFC device acts like a regular contactless chip card. The POS terminal does not require specific logic for NFC mobile contactless payments as long as the NFC payment application on the handset emulates a payment brand's contactless EMV or contactless MSD transaction. To avoid imposing new terminal requirements strictly for NFC, NFC applications are leveraging the contactless infrastructure defined for contactless EMV or contactless MSD.

POS Configuration

Not all terminals from a particular terminal brand have the same software support and EMV and brand type approvals. Multiple POS configurations are possible:

- Standalone terminals

  Standalone terminals are not connected to any other cash register system. A standalone terminal can support EMV as long as the acquirer/processor, gateway or independent sales organization (ISO) supports EMV messaging. The terminal vendors themselves may write the EMV terminal application that supports a particular brand.

- Integrated POS systems

  Large retailers often have their own customized cash register software systems with all or portions of the debit and credit card processing logic built in. To support contact EMV, contactless MSD, contactless EMV, or NFC mobile contactless payments, these systems will need additional logic or alterations to leverage the logic in an attached brand-certified terminal.

- Value-added service provider terminals

  These terminals are provided with customized software developed as part of an ISO, acquirer, or terminal reseller service offering.

6.3 EMV and Brand Type Approval

A contact EMV kernel that implements the baseline requirements for contact EMV is required to be certified by EMVCo. There are EMV Level 1 (low level interface) and Level 2 (application level) type approvals. All card brands require EMV Level 1 and Level 2 type approval as a prerequisite of their brand approval. The EMV kernel is usually implemented as payment system independent such that the terminal vendor can get it certified independent of any future POS application implementation. In general, EMV Level 1 and Level 2 certifications are the responsibility of terminal vendors.

A POS application must get brand approval before it can be used in production to process transactions for the payment brand. Brand approval is usually designed to test the acquirer host system and acceptance system from an end-to-end processing perspective (i.e., from terminal to host and back from host to terminal). Brand approval is the responsibility of the acquirer.

Similarly, the terminal vendor is responsible for getting the contactless Level 1 and Level 2 type approvals for the EMVCo and payment brand requirements that the terminal supports. As explained in the previous section, a different contactless kernel (or card handler) is used for each payment brand.

EMVCo has published the EMV Contactless Specifications for Payment Systems Version 2.2 (June, 2012) which includes the provision for multiple kernels. The specification does not refer to any specific payment brand, but provides the command structure needed to support kernels with different requirements. EMVCo has defined the type approval process for contactless Level 2 kernels which include the Entry Point.

Payment brand end-to-end testing and approval for supporting contactless transactions, which is similar to that of contact EMV transactions, is required for POS applications. This approval is the responsibility of acquirers.

6.4 Transaction Messaging Support

Figure 7 shows the communication path between the POS terminal and the issuer's host system. The standard EMV message content for communication between the issuer's host processing systems and the acquirer is defined by Field 55 (see Section 2.2), ISO/IEC 8583 standard and payment brand and acquirer-specific message formats. Communication between the terminal and the acquirer is defined by each acquirer/processor and is not common.

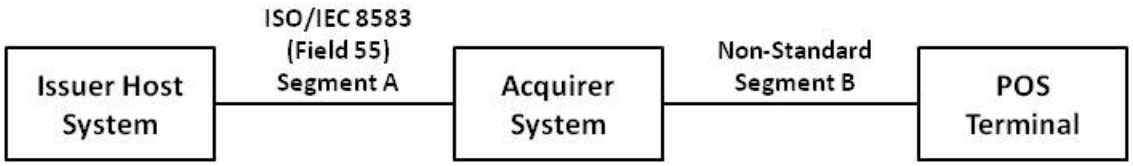


Figure 6: Communication from Host to Acquirer to Terminal

To facilitate rapid adoption of contactless payments in the U.S., the U.S. contactless chip application was designed to require minimal changes to the communication messages exchanged between any of the parties involved. To support online EMV only, at a minimum, the additional new fields described in section 2.3 must be supported in both segments A and B of the messaging illustrated in Figure 7. To support the full EMV messaging specification, which means to support all of the fields carrying EMV data elements, both segments A and B would need to be modified. Changing the messaging in segment B requires changes to the terminal application logic and the acquiring host system.

To provide an additional level of security, end-to-end encryption and the Payment Card Industry Data Security Standard (PCI DSS) are two other initiatives that merchants are implementing, which also affect the payment transaction infrastructure and processes. Implementing each initiative in isolation suggests separate development and POS terminal application release efforts. Entities that are initiating development in these areas are encouraged to implement the messaging changes that support full EMV messaging, even though the fields may not be used immediately.

6.4.1 Clearing and Settlement

The role of POS/merchant system is to provide necessary EMV transaction data to the acquirer for performing clearing and settlement with the issuers. Since the communication between the terminal and the acquirer is not standardized, the clearing and settlement processing in the POS/merchant system is mainly driven by the acquirer's requirements. Please refer to section 5.3 “Clearing and Settlement Considerations" for details of the process from the acquirer's perspective.

6.5 Terminal Upgrade Capabilities and Plans

Merchants should be sure that their acquirer, terminals and in-house infrastructure support remote terminal management and application upgrade.

The state of contact and contactless chip payment adoption in the U.S. is still in flux. For this reason, increasing numbers of acquirers are offering, and retailers are installing, terminals that include the hardware to support contact EMV or contactless EMV payments but that do not include EMV applications. These terminals are designed to facilitate remote application downloads and updates and have received brand-level type approvals for EMV applications that can be downloaded in the future. If an acquirer plans to buy an upgrade that supports EMV, the acquirer must assure the merchant that the upgrade has been certified by the payment brands for the merchant’s specific terminal model. When evaluating POS terminal deployment options, terminal upgrades provide a potentially cost-effective approach to managing the market’s uncertainties when used in combination with a robust terminal management system. However, when evaluating this approach, it is important to consider the acquirer’s software upgrade costs and deployment strategies.

6.6 Summary

The terminal roadmap is tightly coupled with merchant support strategies for each acquirer and ISO in the marketplace. Acquirers and ISOs assess the demand for features and functions demanded by their customers and are required to implement the EMV application logic and messaging changes described to support EMV. In addition, these organizations are responsible for selling terminals that can meet merchant needs for a number of years ahead. A large part of their investment lies in brand-level EMV application development and certification. However, terminals are available that have the required approvals, and some leading acquirers in the U.S. are installing terminals with the hardware to support

contact and contactless EMV transactions. In some cases, these acquirers are activating contact EMV and contactless EMV support; in other cases, they are prepared to download the EMV upgrades as needed.

Table 9 summarizes POS terminal and system acquisition considerations.

Table 8. POS Terminal and System Considerations

Roadmap Option		Consideration
1. Card Interface	a) Contact	• The terminal must have a contact chip reader and be loaded with application software that supports EMV transactions for each of the payment brands. • The terminal must be certified by EMVCo and by each payment brand for which EMV cards will be accepted. The acquirer typically assumes responsibility for ensuring that terminals have the appropriate EMV type approval.
	b) Contactless	• The terminal must have a contactless reader and be loaded with an application that can support contactless MSD transactions, contactless EMV transactions, or both. • The terminal must be certified by EMVCo and each payment brand for which contactless cards will be accepted. The acquirer typically assumes responsibility for ensuring that terminals have the appropriate EMV type approval.
	c) Dual interface	• The terminal must have either a contact or contactless chip reader and must be loaded with application software that supports EMV transactions for each of the payment brands. • The terminal must have a contactless reader and must be loaded with an application that can support both contactless MSD transactions and contactless EMV transactions. • The terminal must be certified by EMVCo and by each payment brand for which EMV cards will be accepted. The acquirer typically assumes responsibility for ensuring that terminals have the appropriate EMV type approval.
2. Card Authentication	a) Online	• The terminal application must be certified by EMVCo and by each payment brand to assure that it follows the specific transaction process defined by each payment scheme. The acquirer typically assumes responsibility for ensuring that terminals have the appropriate EMV type approval. One certification process covers both online and offline card authentication. • The acquirer typically must also obtain a brand network approval. The terminals should be ready to support SDA, DDA, and CDA and online authentication cryptogram.
	b) Offline	• The terminal application must be certified with EMVCo and each payment brand to assure that it follows the specific transaction process defined by each payment brand. The acquirer typically assumes responsibility for ensuring that terminals have the appropriate EMV type approval. One certification process covers both online and offline card authentication. • The acquirer typically also must obtain a brand network approval. The terminals should be ready to support SDA, DDA, CDA, and online authentication cryptogram.

Roadmap Option		Consideration
3. Transaction Authorization	a) Online	• POS terminals and systems must support Field 55 for both authorization and clearing. The terminal application must be tested end-to-end with each payment brand to assure that it follows the specific transaction process defined by each payment brand. The acquirer assumes responsibility for this testing. One process covers both online and offline authorization. • The acquirer also must obtain a brand network approval.
	b) Offline	• POS terminals and systems must support Field 55 for clearing only. The terminal application must be tested end-to-end with each payment brand to assure that it follows the specific transaction process defined by each payment brand. The acquirer assumes responsibility for this testing. One process covers both online and offline authorization. • The acquirer must also obtain a brand network approval.
4. Cardholder Verification	a) Signature	• No change required.
	b) Online PIN	• The terminal must support PIN entry or support a connected PIN pad. If online PIN is used, a PIN block is required to be sent to the issuer host for verification. Key injection will be required and the process is acquirer-specific.
	c) Offline PIN	• The terminal must support PIN entry or support a connected PIN pad with a smart card reader. There is offline plaintext PIN and offline enciphered PIN verification. In the case of enciphered PIN verification, an ICC public key (which is signed by an issuer public key which is in turn signed by a CA public key) will be provided by the card to the terminal for enciphering the PIN. Therefore, for both forms of offline PIN verification, key injection is not required (key is either not required for plaintext PIN or uses the public key for enciphered PIN).
	d) No CVM	• The terminal needs to be able support "no CVM" according to the payment brand rules.

7 ATM Considerations

As part of its EMV roadmap announcement in August 2011, MasterCard stated that there would be a liability shift for Maestro ATMs on April 19th, 2013. Financial institutions that own the ATMs would be liable for any fraud resulting from transactions initiated for international EMV-compliant cards on systems that are not EMV capable. In its announcement of the October 1, 2015 deadline for the liability shift for POS terminals that are not EMV compliant, Visa specifically stated "Note: This liability shift policy change excludes counterfeit fraud at U.S. ATMs. Visa will continue to evaluate the potential for an expansion to U.S. ATMs.

U.S. ATM owners might question whether or not it is worth it to deploy a network of EMV-capable ATMs given that there currently is only a single mandate to do so. Maestro ATM transactions account for an extremely small percentage of overall ATM transactions and ATM owners could opt not to accept Maestro transactions. There are more than 400,000 bank and independently owned ATMs in the United States, all of which would require either replacement or upgrading. It will cost an estimated $500 million to upgrade U.S. ATMs to be EMV capable.[40]

Yet there are reasons to making the change to EMV for ATM owners. An EAST (the European ATM Security Team) study found that ATM-related fraud fell by 7% in 2010 with a total of 12,383 incidents reported, down from 13,269 incidents in 2009.

In order to deploy EMV-compliant ATMs, the ATM owners will have to consider the following:

- The ATM card reader will need to be EMV capable.
- The EMV software kernel will have to be implemented in the ATM application provided by the ATM manufacturer.
- The ATM switch must be configured and tested end-to-end including the hardware and software solution.
- The ATM messaging infrastructure must be changed to accommodate the new data fields required by EMV.

In addition, the ATM is an ideal location to support PIN management for EMV cardholders.

7.1 ATM Hardware

Required ATM hardware includes several components. An ATM needs a contact EMV interface device (IFD) to read a contact EMV card. Optionally, a contactless reader that supports ISO/IEC 14443 for contactless transactions may be deployed. An approved chip-capable reader is essential. Some ATMs may have been sold as EMV ready; however, it is essential to ensure that the installed device has been certified to the latest version of the specification or can be upgraded.

In addition, an ATM must be equipped with a PCI-approved encrypting PIN pad. This feature was included in the mandatory Triple DES upgrade that became effective in 2010.

7.2 ATM Software

ATM software includes the software required to enable all necessary hardware functions.

ATMs must have an approved and certified EMV kernel and support all required extensions to the messaging protocol.

Software enhancements are also needed to enable the specific contactless applications supported by the cards or NFC devices used at the ATM. This is an important consideration when evaluating terminals, and it is helpful to understand terminal software and certification requirements.

[40] Preparing for EMV in the United States, NetWorld Alliance sponsored by Triton, 2011

7.3 Certifications and Type Approvals

EMV contact and contactless terminals are required to receive multiple type approvals (Figure 8):

- EMVCo Level 1 Type Approval tests compliance with the electromechanical characteristics, logical interface, and transmission protocol requirements defined in the EMV specifications. The test examines the physical characteristics of the card reader, such as voltages, timing, dimensions, and contact location.
- EMVCo Level 2 Type Approval tests compliance with the debit/credit application requirements as defined in the EMV Specifications. The test verifies that a terminal can process all types of transactions and transaction variations with an EMV card. All terminals for EMV cards must pass an EMV Level 2 test.
- Payment brand type approval.

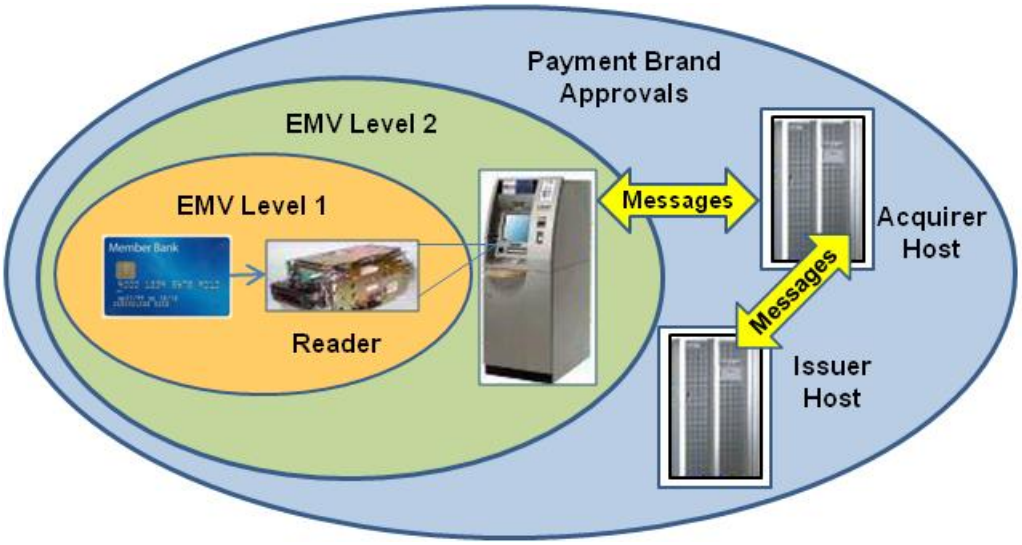


Figure 7. ATM Certification Requirements

To achieve Level 1 and 2 type approval, terminals must undergo lab testing to verify compliance with the electromechanical characteristics, logical interface, and transmission protocol requirements (Level 1) and the debit/credit application requirements (Level 2) defined in the EMV specifications. EMV type approval guarantees that the terminal complies with the baseline EMV specification requirements.

Because EMV supports so many implementation options, multiple implementations of EMV can be required on a single terminal. Each payment brand can implement the EMV standards in a slightly different way, and each brand requires specific programming on the terminal for that brand's implementation. ATM terminals must therefore pass a set of tests defined by each payment brand to receive brand-level approval. There are also terminal approval requirements for both contact and contactless EMV. Accordingly, it is important to understand what payment brand approvals an ATM terminal and terminal applications have received.

Terminal application approvals can be a long process for the terminal application provider. While many of the terminal providers already have terminals that have been approved by the major payment brands, the approval transfers only if the application remains unchanged across implementations. If there are changes for a specific implementation, then a new approval process will be required for that implementation. When purchasing an ATM terminal, ensure that it has an approved software kernel and has implemented the necessary extensions to the messaging protocol.

7.4 Terminal Upgrade Capabilities and Plans

ATMs currently installed in the U.S. today support magnetic stripe cards only. Chip cards are used typically as part of closed campus implementations, rather than at public ATMs; contactless cards are also used for POS transactions, not at ATMs. All ATM vendors report having offered EMV-capable ATMs for the past 5–7 years. Most major manufacturers of ATMs are providing upgrade paths for their installed base of ATMs. Most new ATMs do not need to be replaced to accept EMV cards. Some forward-thinking U.S. deployers already provide chip-enabled readers, and those who do not, may want to do so as a matter of policy. The cost of a chip-enabled reader is about the same as the cost of a non-chip reader, because ATM vendors serve countries where chip-enabled readers are the standard.

ATMs have evolved in the last 10 years from closed proprietary systems to PCs running the standard Windows® operating system. The software on modern ATMs can be upgraded easily. To protect against the uncertainty of what payment instrument types to support, ATM owners are leveraging this future upgrade capability and installing terminals with the hardware to support EMV contact or contactless transactions but without installed or activated EMV applications. These terminals are designed to facilitate remote application downloads and updates and have received brand-level approvals with EMV applications that can be downloaded in the future.

Recent conversion in EMV countries, notably in the U.K. and Canada, has validated that it is also possible to upgrade ATM software for EMV functionality; however previously installed hardware requires verification that all hardware complies with the latest specification and that hardware installed earlier and having sat idle for years has not oxidized.

Below are a few considerations that can assist ATM owners with preparing an assessment of EMV readiness.

1. What is the ATM network inventory? Can the ATMs be upgraded, or do they need to be replaced? Because upgrades are typically less expensive than installing new ATMs, which ATMs can be upgraded?
2. If there is a pending ATM refresh decision, consider models of ATMs where the hardware is compliant to EMV specifications and will only require a software update to enable functions. All major ATM suppliers (e.g., Diebold, NCR, Triton, Wincor) have EMV-ready ATM models.
3. An important consideration is whether the ATM vendor received Level 1 and Level 2 type approval from EMVCo for the devices needed. Ensure that these upgrade paths have already been proven in the field.
4. Even with the right hardware and base software, ATM software still needs to be approved by the various payment brands. Ensure that these approvals have been obtained for the software configuration being purchased.
5. For ATMs processed by a third party processor, the processor will also need to obtain approvals with the individual payment brands in order to ensure that all parts of the system are fully compliant

7.5 Summary

Table 10 summarizes the ATM considerations.

Table 9. ATM Considerations

Roadmap Option		Consideration
1. Card Interface	a) Contact	• The terminal must have a certified contact chip reader and be loaded with application software that supports EMV transactions for each of the payment brands. • The terminal must be certified by EMVCo and by each payment brand for which EMV cards will be accepted. The ATM owner typically assumes responsibility for ensuring the terminal has proper approvals and completing the end-to-end network testing and approvals.
	b) Contactless	• The terminal can also have a contactless reader and be loaded with an application that can support contactless MSD transactions, contactless EMV transactions, or both. • The terminal must be certified by EMVCo and by each payment brand for which EMV cards will be accepted. The ATM owner typically assumes responsibility for ensuring the terminal has proper approvals and completing the end-to-end network testing and approvals.
	c) Dual interface	• The terminal must have either a contact or contactless chip reader and must be loaded with application software that supports EMV transactions for each of the payment brands. • The terminal must be certified by EMVCo and by each payment brand for which EMV cards will be accepted. The ATM owner typically assumes responsibility for ensuring the terminal has proper approvals and completing the end to end network testing and approvals. • The terminal may have a contactless reader and must be loaded with an application that can support both contactless MSD transactions and contactless EMV transactions.
2. Card Authentication	a) Online	• The terminal application must be certified by EMVCo and by each payment brand to assure that it follows the specific transaction process defined by each payment scheme. The ATM owner typically assumes responsibility for obtaining the certifications. • The ATM owner typically must also obtain a brand network approval. The terminals should be ready to support SDA, DDA, and CDA and online authentication cryptogram.
	b) Offline	• Not applicable to ATMs
3. Transaction Authorization	a) Online	• ATM terminals and the ATM network must support Field 55 for authorization. The terminal application must be certified by EMVCo and each payment brand to assure that it follows the specific transaction process defined by each payment brand. The ATM owner typically assumes responsibility for obtaining the certifications • The ATM owner typically also must obtain a brand network approval.
	b) Offline	• Not applicable to ATMs
4. Cardholder	a) Signature	• Not applicable to ATMs

Roadmap Option		Consideration
Verification	b) Online PIN	• The ATM terminal must support PIN entry on a encrypting PIN pad.
	c) Offline PIN	• Not applicable to ATMs
	d) No CVM	• Not applicable to ATMs

8 Conclusions

To reduce counterfeit, lost and stolen card fraud, and to protect cardholder data, nearly every country in the world is widely deploying EMV. As a result, fraud activity is trending more toward the U.S. Led by Visa in August, 2011, the four major U.S. payment brands have harmonized key milestones for U.S. implementation of EMV. The EMV roadmap for debit networks is unclear at this time since most debit networks have not announced their EMV direction. U.S. laws governing debit routing (aka "Durbin Amendment") complicate matters since merchants must have a routing choice of two unaffiliated debit networks.

EMV is an open standard that provides bank card specifications to protect against fraud from counterfeit, lost and stolen cards and to improve the security of the transaction authorization process. EMV is a worldwide common standard that ensures global acceptance and interoperability and supports new form factors beyond cards, including key fobs, microSD memory cards, adhesive stickers, and NFC phones. Card authentication can be performed equally securely using both offline and online techniques. Similarly cardholder verification can be accomplished using online or offline PIN, in addition to signature or in some cases, no verification. Lastly, even the authorization can take place offline between the card and POS terminal, although nearly all transactions will likely be authorized online in the U.S.

EMV requires additional fields in the network message. If offline authorization is supported, issuers and acquirers must also support new chip fields in the clearing and settlement data records. The EMV standard also includes contactless payment transactions, which differ from today's implementation of contactless payments in the U.S. However, these legacy contactless payment implementations are evolving to be compatible with the globally interoperable EMV standard.

The Smart Card Alliance updated its industry-wide roadmap to EMV, originally published in early 2011, to educate the U.S. payments industry stakeholders, including bank issuers, merchants, acquirers/processors and suppliers to the industry, on the actions each stakeholder needs to consider to issue, accept and process EMV transactions. In keeping with the unique characteristics of the U.S. market, the white paper explored potential scenarios with contact and contactless EMV, contactless MSD and NFC.

Planning a roadmap to EMV requires choice of card interface (contact, contactless or dual), card authentication method, cardholder verification method, and transaction authorization approach. The U.S. may evolve to a hybrid combination of options to best support venue, transaction type, and compatibility with the rest of the world.

Banks are under no mandate to issue EMV cards, but are likely to issue both chip cards and NFC applications broadly by 2015 as new product offerings and in readiness for the fraud liability shift. EMV will impact the card interface and the host and transaction authorization processing. Issuers may choose to issue contact, contactless, or dual-interface cards and EMV-compatible NFC applications. Issuer host systems must process full chip data, or as an option, take advantage of an on-behalf-of service from a payment brand, that requires minimal host system changes. Issuers also need to select whether cards are always authorized online or whether offline authorization is also supported. These choices must also be reflected in the cardholder verification methods that are supported. Issuers need to consider key and PIN management, script processing and fraud risk parameters, personalization.

Larger merchants will likely strive to meet the EMV milestones to minimize fraud exposure. To further reap the benefits of accepting all types of payment interfaces from their customers and realizing the PCI audit and account data compromise relief offered by the payment brands, merchants will consider supporting both contact and contactless EMV.

Acquirers/processors will need to modify their systems to receive all possible types of chip data from POS devices and place the data into appropriate message fields. If any of its merchants elects to accept offline authorization, acquirers must also support new chip fields in the clearing and settlement data records. Acquirers need a strategy for supporting online PIN-based credit cards and management of

public keys for offline PIN. They will also be required to certify they are transmitting the appropriate fields to the payment networks.

Many new POS terminals in the market today are built with a smart card chip reader and other hardware components to support EMV. These chip-ready POS terminals that are already in use will simply require a software or firmware upgrade to be fully EMV capable. Additionally, contactless readers currently deployed may require software or firmware upgrade to support EMV contactless. The POS software requires an EMV kernel that is certified by a lab to demonstrate compliance with baseline EMV requirements, and approval by the various payment brands, each of which has different requirements. Standalone POS terminals can be supported by ISOs and acquirer EMV messaging, but integrated POS systems are customized by larger retailers and will need software modifications to support the EMV messaging changes. In some cases, retailers are installing hardware that is EMV-capable but not enabled. Ideally these terminals can be upgraded remotely.

ATMs offer a compelling case for EMV since they are targets for fraudulent cash withdrawals. Although U.S. ATMs are not EMV ready today, all major ATM vendors offer EMV-capable ATMs, and in some cases, existing ATMs can be upgraded rather than replaced. ATM owners need to review their equipment's hardware, software, approval, and upgrade capabilities. The ATM will need a contact and, optionally, a contactless reader that is type approved for EMVCo Levels 1 and 2, plus meet brand-specific requirements. Online PIN is the only cardholder verification method supported by ATMs, and approved PIN pads are already in place from the mandated Triple DES upgrade. The software needs to contain a certified EMV kernel and optionally support contactless.

With the announcements from the major payment brands, we anticipate fairly rapid deployment of EMV in the U.S., harmonized with contactless and NFC payments acceptance. This positions the payments industry well to deflect fraud.

9 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Payments Council to educate stakeholders across the payments value chain about the critical aspects of deploying an EMV solution in their business environments in the U.S. The document is an update to a 2011 white paper, with new content on payment brand guidance and milestones and new and revised content on EMV implementation considerations.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Payments Council members for their contributions. Participants involved in the development of this white paper included: Accenture LLP; American Express; Apriva; Bank of America; Bell Identification B.V.; Booz Allen Hamilton; Capgemini; Chase Card Services; Connexem Consulting; CorFire; Discover Financial Services; First Data Corporation; FIS; Fiserv; Gemalto; Giesecke & Devrient; Heartland Payment Systems; Infineon Technologies; Ingenico, North America; INSIDE Secure; Interac Association/Acxsys Corporation; JPMorgan Chase; MasterCard Worldwide; Morpho; NACHA – The Electronics Payments Association; NagraID Security; NXP Semiconductors; Oberthur Technologies; Quadagno & Associates; Thales e-Security; Toni Merschen Consulting; TSYS; VeriFone Systems; Visa Inc.; Watchdata; Wells Fargo.

Special thanks go to the following Council members who contributed to writing and reviewing this white paper update:

- **Philip Andreae**, Accenture
- **Debbie Bartoo**, Bank of America
- **Nancy Baunis**, Connexem Consulting
- **Deborah Baxley**, Capgemini
- **Troy Bernard**, Discover Financial Services
- **Louis Bianchin**, Watchdata
- **Matt Bowe**, Morpho
- **Brent Bowen**, INSIDE Secure
- **Eddie Chu**, Ingenico
- **Deana Cook**, Chase Card Services
- **Fred Csaky**, FIS
- **Jo Ann Davaris**, American Express
- **Michael English**, Heartland Payment Systems
- **Frazier Evans**, Booz Allen Hamilton
- **Todd Freyman**, Bell Identification B.V.
- **Allen Friedman**, TSYS
- **Ron Hempel**, Chase
- **Ian Hermon**, Thales e-Security
- **Peter Ho**, Wells Fargo
- **Simon Hurry**, Visa Inc.
- **Hap Huynh**, Visa Inc.
- **Liz Jackson**, American Express
- **Jack Jania**, Gemalto
- **Ryan Julian**, Discover Financial Services
- **Grace Jung**, Interac Association/Acxsys Corp.
- **Hal Klein**, Fiserv
- **Brintha Koether**, NXP Semiconductors
- **Mike Kutsch**, MasterCard Worldwide
- **Edwin Lam**, Interac Association, Acxsys Corp.
- **Peter Lee**, CorFire
- **Paul Legacki**, Infineon Technologies
- **James Lock**, JPMorgan Chase
- **Laurie Macnamara**, Booz Allen Hamilton
- **Don Malloy**, NagraID Security
- **Oliver Manahan**, MasterCard Worldwide
- **Janette McGrath**, Discover Financial Services
- **Kenneth Mealey**, American Express
- **Cathy Medich**, Smart Card Alliance
- **Toni Merschen**, Toni Merschen Consulting
- **Andra Munteanu**, Discover Financial Services
- **Susan Pandy**, NACHA
- **Joe Pilozzi**, STMicroelectronics
- **Nick Pisarev**, Giesecke & Devrient
- **Louis Portillo**, American Express
- **Peter Quadagno**, Quadagno & Associates
- **Sanjiv Rawat**, Giesecke & Devrient
- **Bill Robertson**, Apriva
- **James Savage**, American Express
- **Dori Skelding**, Chase Card Services
- **Garfield Smith**, Oberthur Technologies
- **John Smith**, First Data Corporation
- **Ross Snailer**, Visa Inc.
- **Brian Stein**, Accenture
- **Sree Swaminathan**, First Data Corporation
- **Erik Vlugt**, VeriFone Systems
- **Astrid Wang-Reboud**, Gemalto

Individuals who participated in the development and review of the first version of this white paper, published in February, 2011, included: Deborah Baxley, Capgemini; Troy Bernard, Discover Financial Services; Guy Berg, Datacard Group; Louis Bianchin, Watchdata; Donna Colella, First Data Corporation; Deana Cook, Chase Card Services; Jo Ann Davaris, American Express; Joe DeFilippo, Capital One; Jason Dell, First Data Corporation; Willy Dommen, Booz Allen Hamilton; James Ellis, HID Global; Michael English, Heartland Payment Systems; Jacob Greene, Discover Financial Services; Sabrina Hapberg, First Data Corporation; Ian Hermon, Thales e-Security; Bengt Horsma, First Data Corporation; Simon Hurry, Visa Inc.; Hap Huynh, Visa Inc.; Ryan Julian, Discover Financial Services; Mohammad Khan, ViVOtech; Kevin Krest, Smartcard Marketing Solutions; Michelle Lehouck, CPI Card Group; James Lock, JPMorgan Chase; Oliver Manahan, MasterCard Worldwide; Don Malloy, NagraID Security; Joshua Martiesian, LTK Engineering Services; John McNulty, Fiserv; Cathy Medich, Smart Card Alliance; Jean-Louis Meyer, Datacard Group; Barry Mosteller, Oberthur Technologies; Melissa O'Brien, Apriva; Mira Olson, First Data Corporation; Ron Pinkus, Giesecke & Devrient; JC Raynon, ViVOtech; Gregory Riche, IBM; John Shaw, epay Worldwide, Inc.; Dori Skelding, Chase Card Services; Brian Stein, Accenture; Jeffrey Stroud, Gemalto; Tom Zalewski, ViVOtech.

Trademark Notice

About the Smart Card Alliance Payments Council

The Smart Card Alliance Payments Council focuses on facilitating the adoption of chip-enabled payments and payment applications in the U.S. through education programs for consumers, merchants, issuers, acquirers/processors, government regulators, mobile telecommunications providers and payments service providers. The group is bringing together payments industry stakeholders, including payments industry leaders, merchants and suppliers, and is working on projects related to implementing EMV, contactless payments, NFC-enabled payments and applications, mobile payments, and chip-enabled e-commerce. The Council's primary goal is to inform and educate the market about the value of chip-enabled payments in improving the security of the payments infrastructure and in enhancing the value of payments and payment-related applications for industry stakeholders. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

10 Glossary

Card authentication method
In the context of a payment transaction, the method used by the terminal and/or issuer host system to determine that the payment card being used is not counterfeit.

Card security code
Codes either written on the payment card magnetic stripe or printed on the card that are used by the financial payment brands for credit and debit transactions to protect against card fraud.

Card verification code (CVC) / card verification value (CVV)
Terms used by MasterCard and Visa for the card security codes used for credit and debit transactions to protect against card fraud.

Cardholder verification method (CVM)
In the context of a payment transaction, the method used to authenticate that the person presenting the card is the valid cardholder. EMV supports four CVMs: offline PIN, online PIN, signature verification and no CVM.

Chip card
A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, chip cards have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a card reader. Chip card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, key fobs, subscriber identity modules (SIMs) used in mobile phones, and USB-based tokens.

Combined DDA with application cryptogram (CDA)
An authentication technique used in EMV transactions that combines DDA functionality with the application cryptogram used by the issuer to authenticate the card online. The application cryptogram is used to assure that the data in the transaction maintain integrity even after the transaction is completed.

Contact chip card
A chip card that communicates with a reader through a contact plate. The plate must come into contact with a terminal, usually through a dip reader into which the card is inserted.

Contactless magnetic stripe data (MSD)
The U.S. approach for implementing contactless payments. With contactless MSD, the message layout for Track 1 and Track magnetic stripe data remained intact, with one notable difference. The chip on the card allows for the calculation of a dynamic card verification value based on a card-unique key and a simple application transaction counter. The dynamic card verification value is passed in the message in the same field that was used for the original card verification value. The application transaction counter (ATC) is passed in the area reserved on the track layout for issuer discretionary data.

Contactless payments
Payment transactions that require no physical contact between the consumer payment device and the physical point-of-sale (POS) terminal. In a contactless payment transaction, the consumer holds the contactless card, device or mobile phone in close proximity (less than 2-4 inches) to the merchant POS terminal and the payment account information is communicated wirelessly (via radio frequency (RF)).

Contactless chip card
A chip card that communicates with a reader through a radio frequency interface.

CVC
See card verification code.

CVV
See card verification value.

Dual-interface chip card
A chip card that has both contact and contactless interfaces.

Dynamic card security code
A security code which changes for each transaction, replacing the static magnetic stripe-based card security code.

Dynamic authentication data
Information that is used during a transaction to verify the card or the cardholder participating in the transaction and that changes from transaction to transaction.

Dynamic data authentication (DDA)
An authentication technique used in EMV transactions that calculates a cryptogram for each transaction that is unique to the specific card and transaction. DDA protects against card skimming and counterfeiting.

EMV
Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

EMV tags
EMV configuration parameters that convey the issuer's EMV implementation choices to the EMV application on the chip.

EMVCo
The organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. EMVCo is currently owned by American Express, JCB, MasterCard Worldwide, and Visa, Inc.

Magnetic stripe card
A plastic card that uses a band of magnetic material to store data. Data is stored by modifying the magnetism of magnetic particles on the magnetic material and is read by "swiping" the magnetic stripe through a reader.

Near Field Communication (NFC)

A standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate smart chips (called secure elements) that allow the phones to securely store the payment application and consumer account information and to use the information as a “virtual payment card.” NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by EMV and contactless credit and debit cards.

Offline authorization
Authorizing or declining a payment transaction through card-to-terminal communication, using issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized without going online to the issuer host system.

Offline PIN
In an EMV transaction, the process of comparing of the cardholder's entered PIN with the PIN stored on the EMV payment card, without going online to the issuer host for the comparison. Only the result of the comparison is passed to the issuer host system.

Online authorization
Authorizing or declining a payment transaction by sending transaction information to the issuer and requesting a response.

Online EMV
A streamlined implementation of EMV that uses online card authentication and online transaction authorization together and requires 100 percent online authentication/authorization. Online EMV may be appropriate for countries with a fast, reliable telecommunications infrastructure, such as the U.S.

Online PIN
In an EMV transaction, the process of comparing the cardholder's entered PIN with the PIN stored on the issuer host system. The PIN is encrypted by the POS terminal PIN pad before being passed to the acquirer system. The PIN is then dycrypted and reencrypted as it passes between each party on its way to the issuer.

Payment Card Industry Data Security Standard (PCI DSS)
A framework developed by the Payment Card Industry Security Standards Council for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents

Personal identification number (PIN)
A secret that an individual memorizes and uses to authenticate his or her identity.

PIN
See personal identification number.

Public key infrastructure (PKI)
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

Smart card
See chip card.

Static data authentication (SDA)
An authentication technique used in EMV transactions that uses a cryptogram using a static public key certificate and static data elements. With SDA, the data used for authentication is static—the same data is used at the start of every transaction.

Symmetric key technology
Keys that are used for symmetric (secret) key cryptography. In a symmetric cryptographic system, the same secret key is used to perform both the cryptographic operation and its inverse (for example to encrypt and decrypt, or to create a message authentication code and to verify the code). The secret key shared between the sender and the receiver or the card and the issuer.