Smart Card Alliance

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

A Smart Card Alliance Payments Council White Paper

Publication Date: February 2011

Publication Number: PC-11001

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 Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

TABLE OF CONTENTS

1 Introduction

The EMV specification[1] defines technical requirements for bank cards with embedded microchips and for the accompanying point-of-sale (POS) infrastructure. With few exceptions (primarily in the United States), financial institutions worldwide issue EMV bank cards to businesses and consumers. Approximately 1 billion EMV cards have been issued globally and 15.4 million POS terminals accept EMV cards.[2] The primary purposes of including a chip in a bank card are to store cardholder data securely, protect data stored on the chip against unauthorized modification, and reduce the number of fraudulent transactions resulting from counterfeit, lost, and stolen cards.

The United States did not choose to implement EMV while Europe, Canada, Latin America, and Asia are in various stages of EMV chip migration. The U.S. has historically had relatively low fraud rates, due to nearly 100 percent online authorization and sophisticated real-time fraud detection by the issuer authorization systems. In addition, substantial costs are associated with the deployment of an EMV infrastructure. Chip cards are more expensive than magnetic stripe cards, POS terminals require additional features to read the card, and legacy back-office systems must be upgraded. Without a perceived fraud problem and given the cost of implementation, U.S. financial institutions and merchants did not make the investment required to convert the legacy bank card issuance and acceptance infrastructure to the EMV standard.

Today, however, several factors are driving the U.S. payments industry to reconsider implementation and deployment of EMV for payments. Most important are the increasing amount of card-related fraud losses[3] and the cost of enhancing security features incrementally. In addition, the investment being made by merchants to comply with the Payment Card Industry Data Security Standard (PCI DSS) and by the industry to implement new capabilities for contactless and NFC mobile payment transactions provides an opportunity to move to EMV in the U.S. Moreover, U.S. travelers abroad are discovering that their magnetic stripe bank cards are sometimes rejected. Finally, as other markets have adopted chip cards, the per-unit costs for cards and devices have decreased. Some POS device manufacturers now sell only hybrid devices with both chip and magnetic stripe capabilities.

1.1 Objective

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:

- Describes the current state of the payments infrastructure in the U.S.
- Identifies actions stakeholders need to take to issue EMV cards, and to accept and process EMV transactions.
- Defines and discusses the possible relationship between U.S. contactless bank card transactions and EMV and the relationship between the Near Field Communications (NFC) standard and EMV.
- Discusses the impact of the global deployment of EMV on possible roadmap options for the U.S.

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 specification can resolve key issues that challenge financial institutions. The majority of work on EMV was conducted in the late 1990s. Over the years, EMVCo[4] has maintained and revised the

[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] "Over 1 billion EMV cards now active," EMVCo, http://www.finextra.com/News/Fullstory.aspx?newsitemid=21870

[3] *The Nilson Report*, "Global Card Fraud," June 2010

[4] 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

specification to sustain the highest level of security. EMVCo also develops and manages new functionality required by the market.

U.S. 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. When compared to other regions, the U.S. market has unique characteristics, such as low cost telecommunications and the presence of contactless chip cards. Industry stakeholders are exploring which implementation options in the EMV specification will be required to meet U.S. market needs in the most cost-effective manner.

1.2 U.S. Bank Card Market Overview and Card-Based Fraud

The size and complexity of the U.S. credit and debit card market make changes to the payments infrastructure costly and difficult to implement.

Over 1 billion credit and debit cards were in use in the United States in 2009, generating over 52 billion of purchase transactions (see Table 1 and Table 2). Credit and debit cards are accepted at over 10 million merchant POS terminals. Terminal functionality varies by merchant, with increasing numbers supporting PIN pads and contactless readers. Some merchants are also starting to purchase POS terminals with hardware support for contact EMV cards.

Table 1. U.S. Credit and Debit Card Statistics (Nilson Report, 2009)

Card Type	Number (millions)	Purchase Transactions (billions)	Average Transaction Value/Card
Credit	576.4	20.16	$87.40
Debit	507	32.25	$37.50

Table 2. U.S. Debit and Prepaid Card Issuance (Nilson Report 2009)

Card Type	Number (millions)
Debit card (top 50 issuers)	326.8
Prepaid card (top 50 issuers)	136.9
Total (top 50 issuers)	462.7
Total U.S. (97 issuers)	507

The U.S. has historically had relatively low fraud rates, implementing online authorizations as well as other online techniques to detect and react to fraud. There are no reliable, precise, consistent statistics for U.S. payment fraud. Rather, the industry relies on surveys and extrapolations to gauge the levels and trends for payment fraud. By any account, however, the value of losses are significant.

At a global level, the Nilson Report estimated card fraud losses of $6.89 billion on $14.6 trillion in purchases of goods and services and cash advances in 2009.[5] According to the Nilson Report, while the global fraud rate has remained steady, the amount of fraud losses is rising and, at current growth rates, estimated to be $10 billion by 2015.[6] Aite Group estimates the total cost of fraud in the United States is

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.

[5] *The Nilson Report*, Issue 951, June 2010

[6] Ibid.

$8.6 billion per year (0.4% of the $2.1 trillion card payment industry); Aite estimates that counterfeit card fraud accounts for 15.9% of the total, $1.35 billion.[7] Mercator Advisory Group reports that fraud losses are probably dramatically underreported and may actually be as high as $16 billion, especially when all of the associated costs such as data breach forensics, lawsuits, undetected fraud, and misclassified issuer losses are considered.[8]

The true cost of fraud, however, exceeds the actual dollar amount of losses. Financial services companies incur damage to their reputations, higher overall operating costs for increased vigilance (including transaction monitoring), reduced productivity, and higher staff expenditures; they also bear the cost of reissuing cards after a fraud incident. An often overlooked and less well understood cost is the impact that fraud has on card usage and lost revenue, with issuers seeing reduced activation rates on re-issued cards and decreased transaction volumes.[9]

Merchants and processors/acquirers also incur damage to their reputations and bear the cost of Payment Card Industry Data Security Standard (PCI DSS) compliance.

As an example of the impact of EMV, the UK Cards Association reports a dramatic reduction in fraud since the introduction of EMV cards. "Fraud on lost and stolen cards is now at its lowest level for two decades and counterfeit card fraud losses have also fallen and are at their lowest level since 1999. Losses at U.K. retailers have fallen by 67 per cent since 2004; lost and stolen card fraud fell by 58 per cent between 2004 and 2009; and mail non-receipt fraud has fallen by 91 per cent since 2004."[10]

The experiences of the U.K. and other countries that have adopted chip have shown a reduction of domestic card-present fraud. But their experiences have also shown a migration to other types of fraud, namely card-not-present (CNP) fraud and cross-border counterfeit fraud (particularly ATM fraud). Fraud migration offsets some of the savings from the decrease in domestic card-present fraud. This reality reinforces the need for a layered approach to security, even with EMV deployment, to address fraud migration and other security vulnerabilities.

Criminals are known to exploit the weakest link, moving from locations where stronger authentication is present to those where it is not, or from financial institutions and merchants who have more sophisticated fraud detection and prevention tools to those with less. With over 1 billion EMV cards issued in the rest of the world and projections for continued growth in EMV card issuance outside of the U.S., criminals are more likely to move counterfeit magnetic stripe card activities to the U.S., leading to an increase in cross-border counterfeit fraud acquired in the U.S. The U.S. payments industry needs to determine whether it is prepared for the potential of significantly higher payment card fraud if fraud migrates to the U.S. from EMV-enabled locations.

The adoption of EMV chip cards and POS terminals in the United States would have a dual benefit. Not only would American merchants, acquirers and issuers benefit from smaller losses and improved cost management controls, but all EMV-enabled issuers globally could experience reduced losses and decreased operational impact from payment card fraud.

[7] "Card Fraud Costs U.S. Payment Providers $8.6 Billion Per Year," *Bank Systems and Technology*, January 13, 2010, http://www.banktech.com/payments-cards/showArticle.jhtml?articleID=222300752

[8] “Fraud to the Left of Me, Risk to the Right,” Mercator Advisory Group, October 2008

[9] “The True Cost of Fraud,” First Data Corporation white paper, March 2009

[10] "New Card and Banking Fraud Figures," The UK Cards Association, March 10, 2010, http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/

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 phones can all accommodate the same basic technologies. The chip is typically powered by a reader and requires the reader to function.

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

Figure 1 shows a typical 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.

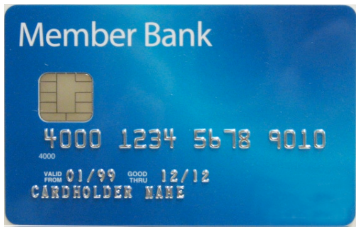

Figure 1: Contact EMV Smart Card

2.1 EMV and Card 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.[11] The specifications address interoperability at two levels. Level 1 defines the electromagnetic and physical characteristics of cards and readers, while Level 2 defines data elements and protocols.

EMV's primary purpose is to ensure that standards for smart card-based payments are interoperable globally. The standards were initially limited to contact cards; however, certain contactless card standards are included.

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 areas:[12]

1. Card authentication, protecting against counterfeit cards
2. Cardholder verification, authenticating the cardholder and protecting against lost and stolen cards
3. Transaction authorization, using issuer-defined rules to authorize transactions

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.

[11] http://www.emvco.com/about_emvco.aspx

[12] 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.

2.1.1.1 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 a cryptogram using a shared secret key. This cryptogram, 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 counterfeit fraud protection. The chip generates this cryptogram by applying an algorithm to the card, device, and transaction data, and then encrypting all data with a Triple Data Encryption Algorithm (TDEA)[13] key (referred to as the Unique Derivation Key (UDK)), that 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. 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)

2.1.1.2.1 Static Data Authentication

As of 2009, most cards issued worldwide support SDA. SDA calculates a cryptogram using a static public key certificate and static data elements. 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 personalization, the issuer uses the issuer's private key to sign a set of card-specific data and loads the signed data onto the card along with the issuer's public key certificate.

To authenticate a card, a terminal loads the payment brand's public root key. 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. The terminal uses the extracted public key to validate the static card data (which has been signed by the issuer).

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 can be used to recreate a transaction.

SDA is the simplest method of chip card authentication and provides the lowest level of protection against counterfeit fraud. Although the current level of chip card counterfeit fraud is low, it can increase as chip card markets become more mature and other opportunities for fraud are removed.

2.1.1.2.2 Dynamic Data Authentication

DDA is similar to SDA but goes one step further. DDA calculates a cryptogram for each transaction that is unique to the specific card and transaction. In addition to the issuer key pair, an asymmetric (RSA) 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 basically the same process as for SDA, except that a random number is also sent to the card to be signed by the card private key. The terminal then validates the signature using the card public key.

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

DDA protects against card skimming and counterfeiting. The technique is similar to the dynamic card verification value (dCVV) and dynamic card verification code (dCVC) which are used in online contactless magnetic stripe data (MSD) transactions.

2.1.1.2.3 Combined DDA with Application Cryptogram

CDA combines DDA functionality with an additional application cryptogram at the end of the transaction. This final application cryptogram is used to assure that the data in the transaction maintain integrity even after the transaction is completed. In other words, the use of a final application cryptogram prevents the type of fraud in which data are manipulated after host authentication.

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) that authenticates the cardholder and protects against the use of a lost or stolen card. EMV supports four CVMs:

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

Depending on payment brand rules 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. Different terminal types support different CVMs. For example, attended POS devices, in addition to supporting signature, may support online or offline PINs (or both), while some unattended card-activated terminals may support "no CVM."

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, which can then either approve the transaction offline or send the transaction and PIN verification result to an issuer host for authorization. The offline PIN is never sent to the issuer host—only the result of the comparison is passed.

Online PIN is not stored on the card because the PIN is being sent online for the issuer to validate. Online PIN is currently supported on magnetic stripe cards and widely available at POS terminals and ATMs in the U.S. today. 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 based on Triple Data Encryption Standard (TDES) and standardized across the globe. For an ATM, online PIN is required and is the only valid CVM. As a result, any implementation of offline PIN will 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. Synchronization is important, because when cardholders are asked to enter a PIN, they do not know whether they should enter their offline PIN or online PIN.

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.

EMV also supports transactions that require "no CVM." No CVM is typically used for low value transactions or for transactions at unattended POS locations.

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

2.1.3 Transaction Authorization

EMV transactions can be authorized online or offline. For an online authorization, transactions proceed as they do today in the U.S. 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 issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized. Offline transactions are used when terminals do not have online connectivity (e.g., at a ticket kiosk) or in countries where telecommunications costs are high.

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.

2.2 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 new network message field that transports chip data. In the U.S., this field is often referred to as Field 55. Outside of the U.S., the data is sometimes carried in a bitmap format known as "third bitmap."

Field 55 is a generic, flexible, variable length container that conforms to tag-length-value (TLV) encoding. 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 authorization request cryptogram, the terminal unpredictable number, the transaction amount, and the form factor indicator are typical of the types of data passed in this field.

Field 23 carries the card sequence number. 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 authorized message.

Issuers, acquirers, and merchants will all need to change their infrastructure to support Field 55 in the authorization request and response messages and Field 23.[14]

Table 3. Field 55 Common Tag Values

Tag	Tag Descriptor	Functionality	Details
9F26	Application cryptogram	Card authentication	Contains the cryptogram used to authenticate the transaction.
9F36	Application transaction sequence counter	Card authentication	Contains the value of the POS terminal transaction sequence counter. The POS terminal maintains a transaction sequence 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.*

[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
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.
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. Is updated by the issuer in the response message.
9F37	Unpredictable number	Card authentication	Contains the POS terminal unpredictable number value. POS terminal generates the number value that may be used as input to the application cryptogram algorithm.

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

Table 4. 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.

2.3 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 differ in the U.S. and in countries implementing EMV.

2.3.1 EMV Contactless

The EMV specifications provide a basis for contactless EMV payments, but do not specify all payment application functionality. 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.

Given that one of the primary goals for contactless EMV is to capture micropayment transactions, DDA and CDA are is typically required by the payment brand. Contactless EMV applications may also leverage the EMV velocity counters to limit the number or dollar value of consecutive offline transactions.

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 developed the common contactless terminal roadmap. In Phase 1, EMVCo is creating a combined set of terminal specifications from the existing four payment brands' specifications and will manage the testing and approval of the contactless kernels according to these specifications.

2.3.2 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. Contactless MSD does not support offline authentication or offline authorization.

The dynamic card verification value significantly 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).

A new generation of contactless cards moves closer to the EMV standard. These cards support a full EMV-based cryptogram that is validated by the issuer in the authorization message. The new contactless cards require a network message change. New fields in the authorization message are needed to carry the 8-byte cryptogram and related chip data.

The requirement to change the message infrastructure for new contactless cards provides a bridge to support future contactless, contact, or mobile NFC EMV chip-based products. Even though different reader interfaces are required for contact transactions as opposed to contactless transactions, the protocol and messaging infrastructure are identical. Merchants and acquirers/processors who upgrade their networks to support the new generation of contactless cards will prepare themselves to support the network messaging required by EMV contact chip cards.

2.3.3 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]

[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.

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 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 payment brand specifications for the region of the world where the "virtual payment card" is being issued.[17] As an example, in Europe, a contactless payment application supporting EMV transactions will be used, while in the U.S. a contactless MSD payment application will be used. This allows consumers to use their NFC-enabled mobile phones for payment at the existing installed base of contactless credit and debit terminals.

EMVCo has been active in defining the architecture, specifications, requirements and type approval processes for supporting EMV mobile contactless payments. This 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:[18]

- 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.

2.4 EMV Certifications

EMV certification and evaluation schemes use an industry standardized and layered approach which is stepwise applied to the integrated circuit (IC), then operating system, then application. Each piece of the value chain can reuse the prior step’s certification to achieve its own. EMVCo evaluates all EMV-based smart card ICs and implementations of the EMVCo Common Payment Application to ensure they conform to EMVCo security guidelines, including firmware and software routines required to access the security functions of the IC. Individual payment brands – American Express, Discover, JCB, MasterCard, and Visa – evaluate the security of their payment applications. These evaluations, which are performed by recognized external security laboratories, provide a high level of assurance that the security functions deal with known attack methods and result in a dated EMVCO Compliance Certificate specifying traceability from manufacturer to issuer.

Figure 2 illustrates the EMV software architecture and the evaluations and certifications that are used with each layer. Certification of POS and ATM terminals are discussed in Sections 6.3 and 7.3, respectively.

[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.

[17] Two examples of EMV NFC trials are: NFC EMV trial in Kuwait, with National Bank of Kuwait, Visa, Zain, and ViVOtech, http://www.vivotech.com/newsroom/press_releases/NBK_Visa_Zain_Middle%20East.asp; NFC trial at the 2010 Mobile World Congress that included GSMA, Telefonica, Visa, Samsung, Giesecke & Devrient, Ingenico, ITN International and La Caixa, http://www.nearfieldcommunicationsworld.com/2010/02/15/32738/nfc-trial-begins-at-mobile-world-congress/

[18] "Contactless Mobile Payment Architecture Overview," Version 1.0, EMVCo, June 2010, http://www.emvco.com/best_practices.aspx?id=162

Figure 2. EMV Chip Software Certifications

EMV Chip Architecture	Evaluations and Certifications
Data Level • Personalization data • Risk management parameters • Cardholder data • Cryptographic keys and certificates	• Payment brands validate the card personalization prior to production issuance.
EMV Application Level • American Express AEIPS, ExpressPay • Discover D-PAS • JCB J Smart • MasterCard Mchip, PayPass Mchip / Magstripe • Visa VSDC, payWave qVSDC / MSD	• Payment brands certify the applications.
Operating System Level • MULTOS • GlobalPlatform Java Card • Native	• EMVCo or MULTOS certify the open chip operating systems. • Payment brands certify native OS EMV implementations.
Chip Hardware • EEPROM • ROM • Cryptographic engine (DES, PKI) • Memory protection logic	

Source: Datacard Group, Smart Card Alliance

3 Roadmap Options

For the past year, the Smart Card Alliance has been providing educational material on the considerations for migrating to EMV. Over the past decade, the benefits of migration have increased, while the costs and implementation difficulties have decreased. Many of the terminal providers and some acquirers/processors have already put in place the EMV features and infrastructure to support customers in Canada and other countries.[19]

The benefits of migrating to EMV include:

- Improving the security of the U.S. payments infrastructure and eliminating the U.S. as a destination for criminals and global magnetic-stripe fraud activity.
- Increasing the satisfaction of cardholders, especially when traveling internationally. In 2008, U.S. payment card issuers missed out on nearly $4 billion in charge volume, including $78.7 million in interchange fees, because of problems cardholders had with their cards while traveling abroad.[20]
- Increasing the satisfaction of international customers, who will be using EMV cards at U.S. merchants and ATMs.
- Maintaining interoperability with the rest of the world as it migrates to EMV.
- Leveraging commercially available EMV-compatible products and services for a low risk, proven approach to fraud reduction.
- Positioning the industry for other forms of payment, notably NFC mobile contactless payments.

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 EMV implementation requires choices in four areas:

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

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.

[19] It is important to note that acquirer/processor support may be platform-specific and may not be available in the U.S. Merchants and issuers should contact their acquirers/processors to determine if they support EMV.

[20] "Card Problems Cost U.S. Issuers Hundreds of Millions Overseas," *Digital Transaction News*, October 2009.

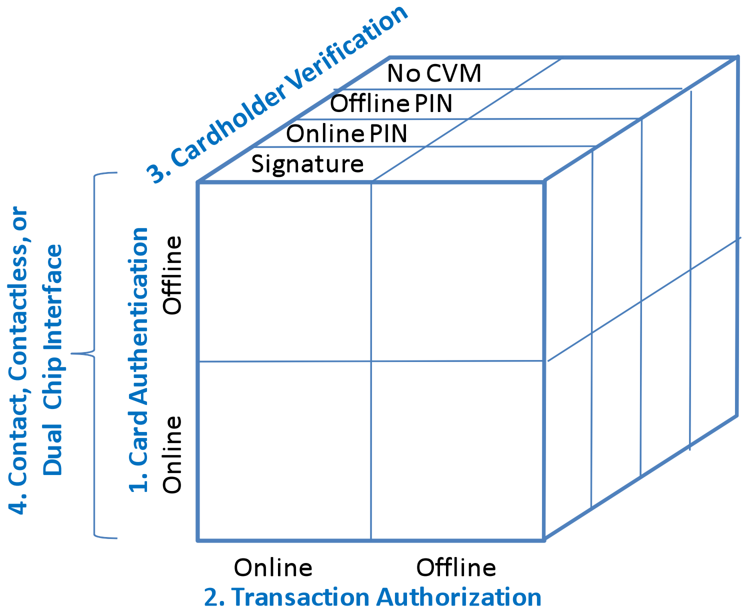
3. Cardholder Verification
No CVM
Offline PIN
Online PIN
Signature
4. Contact, Contactless, or Dual Chip Interface
1. Card Authentication
Offline
Online
Online
Offline
2. Transaction Authorization

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 predetermined limits (such as transaction dollar size); however, if the card is authenticated offline (B) but the transaction must be authorized online, then the card will be authenticated a second time online.

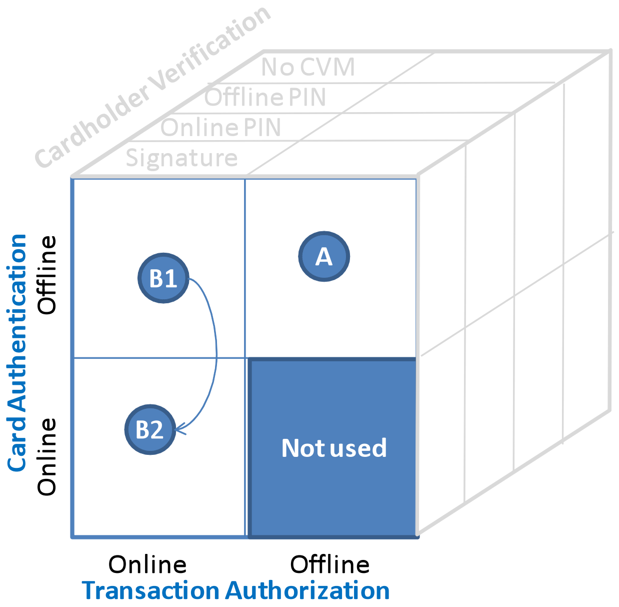

Figure 4. Authorization vs. Online and Offline Authentication

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

Table 5. 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 second-generation contactless cards being deployed in the U.S. and Canada.
	c) Dual interface	• Card containing both contact and contactless interfaces. • Works with either contact or contactless reader.
2. Card Authentication	a) Online	• Uses 8-byte Triple DES cryptogram. • No requirement for SDA, DDA, or PKI cryptographic co-processor.*
	b) Offline	• Uses SDA, DDA and/or CDA and PKI. • Requirement for PKI cryptographic co-processor (for DDA and CDA only).
3. Transaction Authorization	a) Online	• Authorization message sent to issuer as currently implemented for magnetic stripe card transactions.
	b) Offline	• Authorization determined by EMV risk assessment and communication between card and terminal. • May be forced online, depending on limits and other factors.
4. Cardholder Verification	a) Signature	• No special POS requirement.
	b) Online PIN	• Requires POS PIN pad.
	c) Offline PIN[§]	• Requires POS PIN pad. • Uses SDA for plain text PIN, and/or DDA or CDA and PKI for enciphered PIN. • Requirement for PKI cryptographic co-processor (for DDA and CDA only).
	d) No CVM	• No special POS requirement. • Usually reserved for low value transactions.

* All microprocessor cards used for EMV include a DES cryptography engine. DES 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. Contact EMV card security features cannot be used with today's contactless POS readers.

The contactless interface provides a bridge to implementation of NFC-enabled mobile contactless payments. The disadvantage of choosing only a contactless interface is the limited deployment of contactless implementations outside of the U.S. and Canada.

Dual-interface cards carry both contactless and contact EMV interfaces. Selecting a dual interface card allows the same card to be used both at domestic contactless POS readers and contact readers outside of North America. This interface would be ideal for cardholders who travel internationally.

Whether the industry will evolve toward contact or contactless EMV is an open question. Contactless cards can leverage current investment in contactless terminals and cards and prepare the industry to support NFC mobile contactless payments.[21] 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 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 regions without EMV. To remedy chip card incompatibility, some merchants could choose to install contact chip POS readers to accommodate non-U.S. EMV cards, and those cards could be accepted by falling back to signature or no CVM, if the POS were unable to accommodate offline PIN.

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 are performed as part of the EMV transaction. Performing offline authentication neither requires nor implies that the transaction be performed completely offline. Offline capability is designed into EMV to address environments where reliable online communication is not available or is expensive. With EMV, a card can be required to 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. The same offline parameters are used for terminals that are completely offline.

Online card authentication and online transaction authorization together are known as "online EMV," a streamlined implementation with 100 percent online authentication that is compatible with EMV deployments everywhere. 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 generate an 8-byte cryptogram using Triple Data Encryption Standard (TDES)[22] symmetric keys, rather than using the more complex RSA[23] public key infrastructure. Online EMV implementation does not need to support SDA, DDA, or offline PIN. This implementation avoids the additional cost of cards with crypto co-processors to support DDA or CDA, certificate authorities, and PKI support in POS terminals. Implementation of Online EMV, especially if contactless, leverages the industry's investment in contactless terminals,[24] contactless cards, and implementation of new fields in

[21] 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.

[22] Triple Data Encryption Standard (TDES) block cipher applies the DES cipher algorithm three times to each data block. For further information, see http://en.wikipedia.org/wiki/Triple_des

[23] RSA is an algorithm for public-key cryptography. For further information, see http://en.wikipedia.org/wiki/Rsa and http://en.wikipedia.org/wiki/Public_key_infrastructure

[24] 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

the authorization message to carry the 8-byte cryptogram and related chip data. These cost savings should be a factor when comparing the cost of implementing online EMV to the cost of implementing offline-capable EMV in other markets.

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 floor limits to zero, in effect forcing all transactions online. However, POS terminals installed at Canadian merchants all support the full complement of SDA, DDA, and CDA.

3.1.3 Cardholder Verification

The choice of cardholder verification methods – online PIN, offline PIN, signature, or no CVM – is more straightforward. (See Section 2.1.2 for additional details on EMV cardholder verification methods.) Selecting signature verification avoids the requirement to install PIN pads and eliminates certain cardholder behavioral change and training requirements. Selecting the PIN option requires the installation of PIN pads at merchant locations. The choice of PIN also impacts the EMV authorization process for issuers and acquirers/processors (which is discussed in Sections 4 and 5).

3.1.4 Hybrid Options

It is likely that the U.S. EMV implementation would combine options, depending on venue and transaction type. Depending on what product is being offered, individual issuers might choose to implement multiple approaches, the acquirer infrastructure will support all of them, and merchants will choose which EMV features they want to support. This is the situation in most other markets today, as well as in the current U.S. environment with magnetic stripe for cardholder verification.

A hybrid solution could incorporate the benefits available with all of the options, leverage the existing contactless infrastructure, and ensure compatibility with cards from the rest of the world. While at first glance this solution may appear complicated, the flexibility it offers would ease the transition to EMV by accommodating unique merchant, venue, and issuer objectives.

3.2 Implications for International Travelers

Aite Group[25] 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 in Spain, France, and the U.K., will not accept online-only EMV cards.[26] 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 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? 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

remote downloads. Without remote upgrade capability, a reader may have to be returned to the manufacturer for refit.

[25] "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

[26] Source: Smart Card Alliance Payments Council

3.3 EMV Implementation Costs

In the past, one area of great concern has been the incremental cost of supporting EMV, estimated to be between $5–$13 billion for U.S. industry as a whole.[27] This cost cannot support a business case for EMV migration. However, there is a benefit to being late to implement: much of the investment has already been made, and much of the required functionality is being manufactured into the devices—it just needs to be turned on and used.

As a basis for comparison, the Smart Card Alliance project team conducted an informal survey to determine the relative cost differences between today's magnetic stripe infrastructure and an EMV environment. The results are shown in Table 6. Some of the data was provided by Canadian payment executives, based on their recent EMV implementation experiences.

Table 6. Illustrative Costs of EMV Implementation

Cost	Magnetic Stripe Infrastructure	EMV
Card, personalization, and mailing	$1.11[28]	Actual costs will vary, depending on volume, purchasing power, card functionality/interface and other selected options.
Public key infrastructure		Setup of key management for issuers for SDA and DDA not particularly costly. Most personalization bureaus have SDA, DDA and CDA as standard functions.
Reader cost, set-up, and life-cycle management	Sunk cost of mandate to support Triple DES. Terminals can manage keys and PKI as a standard function. Cost of contact chip reader is a minimal incremental cost; most terminals now support both contact chip and magnetic stripe.	

In general, all options described above will also require changes to customer service, marketing and promotion. This will require education of customers, merchants and customer service representatives, and new procedures and facilities for emergency card replacement and PIN change. These across-the-board impacts are not detailed in subsequent chapters; instead the white paper discusses stakeholder impacts, such as form factor, cryptography, readers and other software and hardware requirements, resulting from the four options described in the Table 5 above.

[27] "U.S. Migration to EMV: Javelin Identity Fraud Data Indicates Lack of ROI and Minimal Benefits to Those Bearing the Brunt of Investment," Javelin Research, August, 2009, and estimate from Aite, *Digital Transactions*, February 2010.

[28] "What's it cost to get a credit card in your pocket?," http://www.creditcards.com, August 2010

4 Card Issuer Considerations

EMV provides a variety of options that support implementation flexibility; an issuer can implement only 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. Issuers will need to determine whether to support contactless MSD, contactless EMV, or both. A contactless MSD card may not work with a European contactless EMV terminal (and vice versa), unless the terminal supports both.
- Dual-interface cards supporting both contact and contactless interface 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 deployed at the POS. For U.S. issuers, the cost and complexity of an overall offline PIN infrastructure should be evaluated because this infrastructure does not currently exist.

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 PKI support and a card with a cryptographic co-processor. These elements can add to the cost of the card and requires 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.

The EMV data preparation and key management applications provide the ability to configure EMV tags and prepare both the EMV tags and cryptographic keys for loading to the chip. EMV tags are the EMV configuration parameters that convey the issuer's EMV implementation choices to the EMV application on the chip. The cryptographic keys are integral to EMV authentication security and to secure EMV script updates after the card is issued and in the hands of cardholders. 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." This services is available for processing both contact and contactless data. The "early chip data option" provides an issuer with the flexibility to process chip cards initially while making the needed changes to support Field 55 and Field 23 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 "early chip data option" 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 are 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 block applications. 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.

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 identify the risk management process and determine whether the transaction should be performed offline or online.

An issuer can use the card profile to implement whether and when a transaction must go online or offline. 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, 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 7. 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 not widely deployed globally, but some U.S. and Canadian issuers have adopted the technology, and European issuance is expected to increase. • Issuers will need to determine whether to support contactless MSD, contactless EMV, or both. 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.
	b) Offline	• Issuers must choose whether to allow the card to authenticate

Roadmap Option		Consideration
		chip data. SDA or DDA can be used by the issuer. • Supporting the public key infrastructure incurs additional costs.
3. Transaction Authorization	a) Online	• Issuers must choose whether to receive full chip data or early chip data.
	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 also affects transactions downstream. • 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 be modified to allow for easy identification of offline transactions vs. online transactions.
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. • Issuers should be aware that the offline PIN may differ from the online PIN; therefore, PIN management is critical to avoid cardholder confusion. It is strongly recommended that the offline PIN and online PIN 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 unlocking and changing offline PIN. • Supporting the offline PIN infrastructure incurs additional costs.
	d) No CVM	• No CVM is included in the CVM list unless otherwise specified by the payment brands.

5 Payments Acquirer/Processor Considerations

Current magnetic stripe platforms operate in both the dual- and single-message format environments. A POS device or card-not-present merchant system transmits transaction messages for authorization or approval to the acquiring processor or, in some cases, directly to the payment brand network. These messages include, but are not limited to, cardholder track data and cardholder PIN for PIN debit transactions when a card is swiped, or primary account number (PAN) and expiration date if the card is key entered (PIN debit transactions can only be swiped).

Additional data can be submitted with the transaction message for-card-not-present transactions to assist merchants in preventing fraud (e.g., CVV2/CVC2 or address verification service (AVS) data). The messages are based on proprietary message systems and ISO/IEC 8583 standard.

Magnetic stripe data must not be stored after authorization. In the dual-message process, only the PAN and expiration date are retained by the merchant processor to create the settlement record. The authorization response data indicates the presence of magnetic stripe data at the POS. The PIN is never retained and must always be encrypted using Triple DES encryption.

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

5.1 Contactless MSD

For a contactless MSD transaction, the message from the POS device or merchant host system to the processor or payment brand network is basically the same as the message sent when the transaction is initiated by swiping the card. The differences are:

- The values sent in the POS Entry Mode and Terminal Capability fields. These fields contain values that identify the POS entry method used to capture the cardholder data and whether the terminal is capable of reading a chip.
- The dynamic card verification value/code (dCVV/CVC3), which is passed in the message in the same field that was used for the original card verification value, and the application transaction counter (ATC), which is passed in the area reserved on the track layout for issuer discretionary data.

The contactless chip provides the magnetic stripe equivalent data to the POS terminal through the RF interface.

Terminal vendors and software providers must certify that they will transmit the appropriate fields to the processors for contactless transactions. Processors must certify that they will transmit the appropriate fields to the payment brand networks.

5.2 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 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 55 and 23 in the clearing records for submission to the payment brand networks, to ensure proper interchange qualification and support new interchange categories.

5.3 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 be able to support receiving the encrypted PIN and passing this encrypted PIN to the payment brand network.

5.4 Summary

For all EMV processing, processors must be able to receive application 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.

It is important to note that many acquirers/processors have already put in place the EMV infrastructure to support customers in Canada and other countries.

Table 8 summarizes considerations for payments acquirers and processors.

Table 8. Payments Acquirer/Processor Considerations

Roadmap Option		Consideration
1. Card Interface	a) Contact	• Does not support NFC mobile contactless payments. • May require a PIN pad.
	b) Contactless	• PIN debit is not supported by Visa for contactless transactions. • Limited contactless deployment outside of the U.S. and Canada.
	c) Dual interface	• PIN debit is not supported by Visa for contactless transactions. • Limited contactless deployment outside of the U.S. and Canada.
2. Card Authentication	a) Online	• Optional fields must be supported if received from the issuer.
	b) Offline	• Any data indicator in Field 55 that provides information about authentication will contribute to the success of the authentication.
3. Transaction Authorization	a) Online	• No change required.
	b) Offline	• Most transaction types require authorization to be obtained online. • Offline authorization affects transactions downstream

Roadmap Option		Consideration
		(interchange qualification and operating rules).
4. Cardholder Verification	a) Signature	• Transactions at or below a specified amount based on merchant type do not require merchants to obtain and validate the signature at the POS.
	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	• Processors will need to support Field 55 to identify the result of offline PIN validation. • Requires a PIN pad.
	d) No CVM	• 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 cards (often referred to as U.S. contactless). However, in the near future in the U.S., terminals may also need to support contactless EMV, contact EMV, and NFC applications. Given all of these possibilities, it is important to consider the following parameters:

- Hardware support
- Software support
- EMV and brand certification
- 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 (CID) 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.

6.2 Software Support

POS terminal software is more complex than hardware, because it varies among payment brands. Figure 5 is a simplified view of the relevant POS terminal software components.

<table>
<tr><td><b>Brand contact EMV logic</b></td><td><b>Brand contactless EMV logic</b></td><td><b>Brand contactless MSD logic</b></td></tr>
<tr><td colspan="2"><b>EMV kernel</b></td><td><b>Magnetic stripe logic</b></td></tr>
</table>

Figure 5. Simplified View of POS Terminal Software Components

The EMV kernel provides the payment terminal's EMV foundation logic. The brand contact EMV logic and brand contactless logic leverage the EMV kernel, but also incorporate brand-specific EMV processing options. EMV provides multiple implementation options for payment brands like American Express, Discover, JCB, MasterCard, and Visa. Each payment brand has implemented the EMV standards differently, and a terminal requires specific software logic for each implementation. Because EMV supports implementation flexibility, POS application vendors must have their applications certified by each payment brand before the applications are approved for use in the market. Accordingly, it is important to understand what payment brand certification approvals the terminal and terminal applications have received. Terminal application certification can be a lengthy process. Many terminal providers offer terminals that have been certified at a minimum by both MasterCard and Visa.

The contactless MSD logic is not an EMV implementation but was designed to leverage the current magnetic stripe infrastructure and messaging. This is why add-on contactless readers can be attached to a magnetic stripe POS terminal without requiring EMV logic or certifications.

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

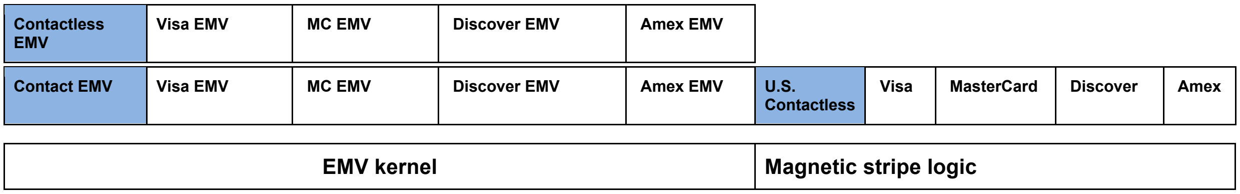

Figure 6. Detailed View of POS Terminal Software Components

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 EMV contactless or U.S MSD contactless.

6.3 EMV and Brand Certification

EMV contact and contactless terminals require multiple certifications. The first certification is EMV certification. To achieve this certification, the terminals must be submitted for lab testing to verify that all of the EMV kernel functions are operating correctly. EMV certification means that the terminal meets the baseline EMV specification requirements.

After receiving EMV certification, a terminal must receive brand certification. The terminal must pass a specific and unique set of tests defined by the payment brand network. When considering the deployment of EMV-compliant terminals, it is important to be sure that the terminals are certified by each of the brands. There are terminal certification requirements that apply to both contact and contactless EMV. It is critical for merchants to make sure that the terminals purchased have current certifications for all capabilities that need to be supported and each of the payment brands that they accept.

POS Configuration

Not all terminals from a particular terminal brand have the same software support and EMV and brand certifications. 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 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.

6.4 Transaction Messaging Support

Figure 7 shows the communication path between the POS terminal and the issuer's host system. The standard EMV message format for communication between the issuer's host processing systems and the acquirer is defined by Field 55 (see Section 2.2) and ISO/IEC 8583 standard. Communication between the terminal and the acquirer is not standardized.

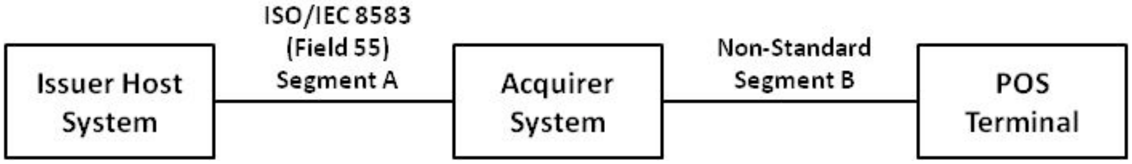

Figure 7: Communication from Host to Acquirer to Terminal

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 field that carries the cryptogram would need to be increased in size 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 Field 55 and Field 23 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.

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.

6.5 Terminal Upgrade Capabilities and Plans

Merchants should be sure that their acquirer and terminals 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 certifications 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. 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 the next 3–5 years. A large part of their investment lies in brand-level EMV application development and certification. However, terminals are available that have the required certifications, 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 9. 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 should be certified by EMVCo and by each payment brand for which EMV cards will be accepted. The acquirer typically assumes responsibility for obtaining the certifications.
	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 should be certified by EMVCo and by each payment brand for which EMV cards will be accepted. The acquirer typically assumes responsibility for obtaining the certifications.
	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 should be certified by EMVCo and by each payment brand for which EMV cards will be accepted. The acquirer typically assumes responsibility for obtaining the certifications. • The terminal must have a contactless reader and must be loaded with an application that can support either contactless MSD transactions, contactless EMV transactions, or both.
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 obtaining the certifications. One certification process covers both online and offline. • The acquirer typically also must obtain a brand network certification. 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 obtaining the certifications. One certification process covers both online and offline. • The acquirer typically also must obtain a brand network certification. 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 certified by 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 obtaining the certifications. One certification process covers both online and offline. • The acquirer typically also must obtain a brand network certification.
	b) Offline	• POS terminals and systems must support Field 55 for clearing only. 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 acquirer typically assumes responsibility for obtaining the certifications. One certification process covers both online and offline. • The acquirer typically must also obtain a brand network certification.
4. Cardholder Verification	a) Signature	• No change required.
	b) Online PIN	• The terminal must support PIN entry or support a connected PIN pad.
	c) Offline PIN	• The terminal must support PIN entry or support a connected PIN pad with a smart card reader.
	d) No CVM	• No change required. • The terminal needs to be able support "no CVM" according to the payment brand rules.

7 ATM Considerations

ATMs have long been synonymous with quick and convenient access to cash. The simplicity and ubiquity of these devices also make them a prime target for fraud. Because one of an EMV card's key features is the inclusion of a secure chip, supporting EMV cards at ATMs would require widespread change.

Nevertheless, there are compelling reasons for the financial services industry to adopt the use of EMV cards at ATMs. As a result of countries implementing EMV, ATM fraud (such as ATM skimming) is migrating from countries implementing EMV to areas that are not currently EMV enabled. The use of EMV chip and PIN cards reduced ATM fraud by 36 percent in Europe in 2009 compared with 2008, according to the European Payment Council[29].

ATM owners, banks, and ISOs, in conjunction with their providers, will want to review carefully the equipment they have in place. Because ATMs are typically on a 7-year upgrade or replacement cycle, a significant portion of the installed base will need to be visited during a transition to EMV. Because online PIN verification is mandatory for ATMs, the implementation option will have fewer variations. In addition to magnetic stripe cards, the ATM terminals may now need to support contactless MSD cards, contactless EMV, contact EMV, and NFC mobile contactless payments. While support for fully inserted cards has been the typical focus of initial ATM EMV conversions, new contactless options are available. ATMs must therefore be examined for the following:

- Hardware capabilities
- Software capabilities
- EMV and brand certifications
- Terminal software upgrade capabilities and plans

7.1 ATM Hardware

Required ATM hardware includes several components. An ATM needs a contact EMV CID to read a contact EMV card and a contactless reader that supports ISO/IEC 14443 for contactless transactions. 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 an approved encrypting PIN pad. This feature was included in the mandatory Triple DES upgrade that took place a few years ago in the U.S.

7.2 ATM Software

ATM software includes the software required to enable all necessary hardware functions. In addition, specific software or firmware is 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.

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

7.3 Certifications

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

- EMVCo Level 1: interface/card reader function certification
- EMVCo Level 2: terminal software application function certification

[29] European Payments Council Report, April 2010, http://www.europeanpaymentscouncil.eu/article.cfm?articles_uuid=3EBDA5B6-CB2E-179D-211BE1EBB4A0CE0C

- Payment brand certification

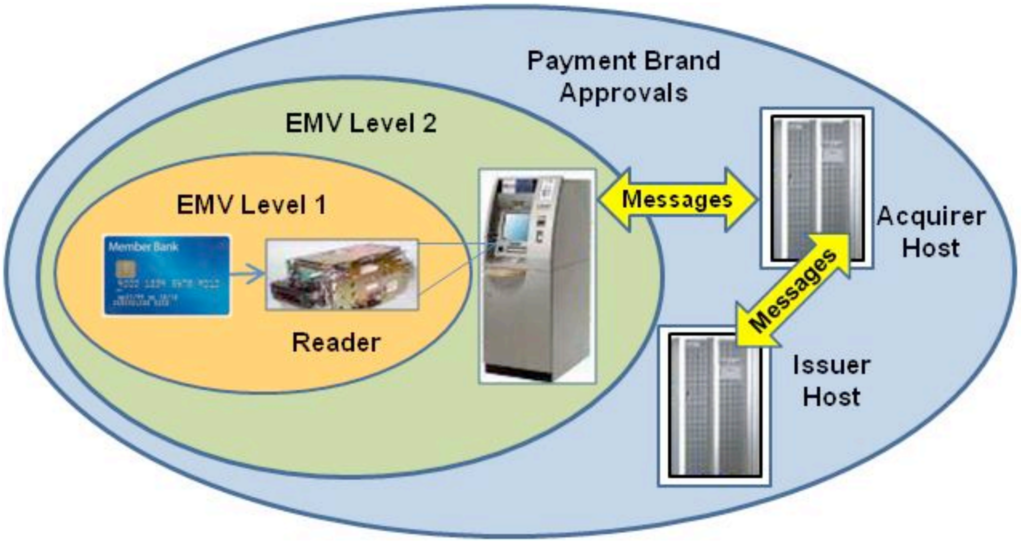

Figure 8. ATM Certification Requirements

To achieve Level 1 and 2 certification, 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 certification guarantees that the terminal complies with the baseline EMV specification requirements. EMVCo provides only Level 1 and 2 certification.

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 certification. There are also terminal certification requirements for both contact and contactless EMV. Accordingly, it is important to understand what payment brand certifications an ATM terminal and terminal applications have received.

Terminal application certification can be a long process for the terminal application provider. While many of the terminal providers already have terminals that have been certified by the major payment brands, the certification 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. While there are no EMV-capable ATMs in the U.S. today, all ATM vendors report having offered EMV-capable ATMs for the past 5–7 years. 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 certifications 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 certification 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 certified with the various payment brands. Ensure that these certifications 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 certification 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 10. 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 should 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 certification and completing the end-to-end network certifications.
	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 should 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 certification and completing the end-to-end network certifications.

Roadmap Option		Consideration
	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 should 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 certification and completing the end to end network certifications. • The terminal must have a contactless reader and must be loaded with an application that can support either contactless MSD transactions, contactless EMV transactions, or both.
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 also must obtain a brand network certification. 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 certification.
	b) Offline	• Not applicable to ATMs
4. Cardholder Verification	a) Signature	• Not applicable to ATMs
	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. Due to historic low fraud rate and high implementation cost, the U.S. is a late-comer to EMV, but increases in fraud losses and the declining cost of adoption are now driving the U.S. toward broad deployment of EMV.

EMV is an open standard that improves the security of card authentication against counterfeiting, cardholder verification against lost/stolen cards, and transaction authorization against interception and replay. There is movement to adopt EMV, a worldwide common standard that ensures global acceptance and interoperability, for 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 transactions are required to be authorized online in the U.S. The industry should carefully weigh the costs against the benefits of supporting offline authorization for U.S. transactions.

EMV requires an additional field in the network message. In the U.S., this field is often referred to as “Field 55”. In Europe an older variant known as “third bitmap” is more common. The EMV standard also includes contactless payment transactions, which differ from today’s implementation of contactless payments in the U.S. However, these legacy implementations are evolving to support NFC mobile contactless payments and to be compatible with the globally interoperable EMV standard.

The Smart Card Alliance researched the topic of an industry-wide roadmap to EMV 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 , 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.

Issuers and merchants may choose to implement only the options they need. EMV will impact the card interface and the host and transaction authorization processing. Issuers may choose to issue contact, contactless or dual interface cards. 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.

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 Field 55 tags. 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 with a lab to demonstrate compliance with baseline EMV requirements, and certified with 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, certification, and upgrade capabilities. The ATM will need a contact and contactless reader that is EMV certified for EMVCo levels 1 and 2, plus brand-specific certifications. 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 support contactless.

Although the enormous size of the U.S. payment industry makes widespread change costly and difficult, the true cost of fraud is increasing and threatens to damage the industry's reputation. This damage could accelerate as criminals move to the U.S. as the weakest link. The cost of EMV implementation in the U.S. has likely declined from original estimates due to maturation of the technology. Ad hoc comparison to representative costs from Canada support this premise. The roadmap outlined in this white paper demonstrates that various options are available to migrate to EMV. Due to the maturity and wide availability of EMV technology and products, migration will be less complicated than it would have been a decade ago.

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.

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; Booz Allen Hamilton; Capgemini; Capital One; CPI Card Group; Datacard Group; Discover Financial Services; epay Worldwide, Inc.; First Data Corporation; Fiserv; Gemalto; Giesecke & Devrient; Heartland Payment Systems; HID Global; IBM; JPMorgan Chase; LTK Engineering Services; MasterCard Worldwide; NagraID Security; Oberthur Technologies; Smartcard Marketing Solutions; Thales e-Security; Visa Inc.; ViVOtech; Watchdata.

Special thanks go to the following Council members who contributed to the development of this white paper:

- **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

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 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 GSM mobile phones, and USB-based tokens.

Combined DDA with application cryptogram (CDA)
An authentication technique used in EMV transactions that combines DDA functionality with an additional application cryptogram at the end of the transaction. This final 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 U.S. 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 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 issuer host system.

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).