A CU24 White Paper

Understanding EMV For Credit Unions

Published by Credit Union 24, Inc.

April 2013

CU24

OVERVIEW

EMV is an advanced payment card technology with improved security and enhanced fraud protection that is globally compatible and more flexible than traditional magnetic stripe technology. The major card payments networks are leading the U.S. migration to an EMV infrastructure to replace our traditional magnetic stripe technology. While EMV is not mandated, the migration is being encouraged through a series of liability transfer milestones, whereby a party to a payment transaction that is not EMV compliant will be held financially responsible for fraudulent transactions. There continues to be progress across the industry to support the general immigration to EMV; however, there remain some important issues to be resolved, and these will be played out over the coming months and years.

This CU24 White Paper provides fundamental information for credit unions to understand the issues related to EMV, the benefits and cost considerations associated with the migration to EMV, and the plans and activities that will be necessary to establish EMV compliance for a credit union's acquiring and card issuing services.

BACKGROUND

EMV is named for the three companies that initially developed global specifications for chip-technology payment cards in 1994: Europay, MasterCard and Visa. The three founders were joined by the Japanese card company JCB and formed a joint venture company called EMVCo which now manages EMV specifications and standards worldwide.

As an advanced payment card technology that offers improved security and fraud protection, EMV is commonly used outside of the United States and provides more flexibility than the magnetic stripe-based card system. Since chip card technology was readily available when markets outside the U.S. were going through their major developmental periods, these markets implemented chip, or EMV, based infrastructures. In the U.S., where the payment card infrastructure was already well-developed, and where magnetic stripe authorization technology was reliable and relatively inexpensive, the magnetic strip infrastructure

continued to serve the industry. As global payment networks and markets have developed, EMV compliant cards and terminals are more and more common, magnetic stripe cards are less often utilized or even accepted in international markets, and card fraud is trending toward the U.S. as the weakest point for card fraud in the face of chip card technologies used around the world.

In addition to enhanced security features, the programmable nature of chip technology enables more flexibility for payment cards, including support for different applications such as identification, rewards and loyalty programs.

These dynamics are spurring the migration to EMV in the U.S.

WHY ADOPT EMV?

Enhanced fraud protection. Card verification — the practice of ensuring the user of a payment card is actually who he says he is — reduces losses from card-related fraud but is time-consuming at the point of purchase. With more powerful processing capabilities and dynamic information, the microprocessor chip enables more robust, complex and secure cardholder verification to protect against consumer-level fraud involving counterfeit, lost or stolen cards.

Reduced skimming. Magnetic-stripe cards are increasingly subject to card skimming -- the practice of capturing data that is encoded on the magnetic stripe and using it to create and use counterfeit cards. When used in properly equipped readers, EMV chip cards are nearly impossible to counterfeit.

Global standard. EMV is the global standard for credit and debit payment cards and terminals. Over 50 countries are in various stages of migrating to EMV. American travelers are finding it increasingly difficult to use their traditional magnetic stripe cards in overseas markets. The United States remains the last significant global market to adopt EMV.

Dynamic data. The secure microprocessor chip on the EMV card contains the information needed for payment and additional protection features, making it significantly more secure than a traditional magnetic-stripe card.
The microprocessor chip adds a bit of dynamic data to each

individual transaction, much like a single-use password that protects each transaction. The information changes with each use. By comparison, magnetic stripe data is static and does not change.

Application flexibility. With the power of the embedded computer chip, EMV cards are more flexible for payments and other applications. The cards can be adapted to provide security and identification applications, as well as support for loyalty and rewards programs

THE TECHNOLOGY

EMV is based on an integrated chip card, or "smart card" technology. Also known as a smart card or Integrated Circuit Card, an EMV card contains an embedded microprocessor chip and enables functions similar to a mini computer. EMV technology replaces the magnetic stripe on the back of debit and credit cards with a powerful computer chip. The microprocessor chip in an EMV card has dynamic data as well as built-in security features, enabling greater security and increased flexibility in applications and utilization.

Through the integrated chip, the card is able to carry out programmable instructions. Information needed to validate, authorize, and process a payment or ATM transaction is stored and accessible on the chip, and can be read by compliant card readers. The integrated chip is protected through various security features, and is embedded within layers of the card plastics, and connected to an antenna that allows communication with contactless terminals (Fig. 1)

By contrast, magnetic stripe cards store only static, unchangeable data that essentially supports only the payment transaction, such as the PAN, expiration date, service code, and some static discretionary data. Magnetic-stripe data is more easily captured and used for fraudulent purposes.

Magnetic Stripe vs. Chip Card Technology

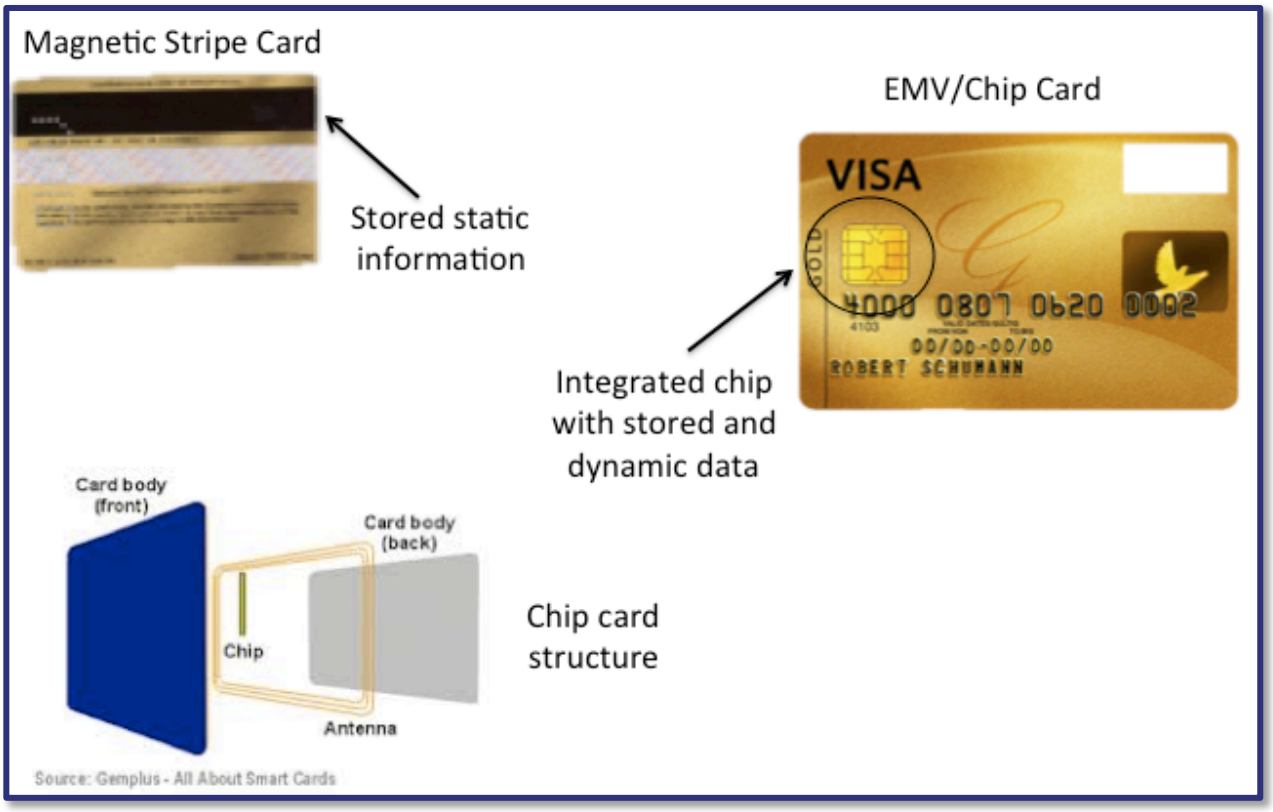


Fig 1

APPLICATION IDENTIFIERS (AIDs)

EMV payment cards generally work according to a series of instructions programmed into the chip called an Application Identifier (AID). The AID determines the processing attributes and characteristics of a specific card utilized at a compatible card terminal (e.g., merchant terminal or ATM). The AID programmed into the card determines how a transaction will be authorized and processed or routed. An AID is essentially a set of features, schemes or characteristics that apply to that particular card. The card issuer determines the AID to be programmed onto the card.

Although an EMV card may contain several AIDs, the terminal where it is used must support the same AID in order for the card to work. Therefore, in order for EMV cards to be generally useable, terminal deployers and card issuers must have mutually compatible AIDs programmed into their respective systems. A card that is presented

at a terminal must have the same AID as the terminal in order for a transaction to be executed.

For example, an AID may require online PIN authorization of a transaction, while a different AID may allow both online and offline PIN authorization.

When an EMV card is presented at a terminal, the terminal determines if there is a common AID. If so, the merchant terminal will process the card according to the processes prescribed by the AID. If there is more than one AID on the card, the terminal must determine which AID it has in common. If there is more than one AID in common, the terminal will determine which AID to use based on the policies and practices of the terminal owner (merchant). (Fig. 2)

This sequence and the rules governing AID recognition, selection and processing are the subject of continuing discussion within the industry.

How It Works At An EMV Device

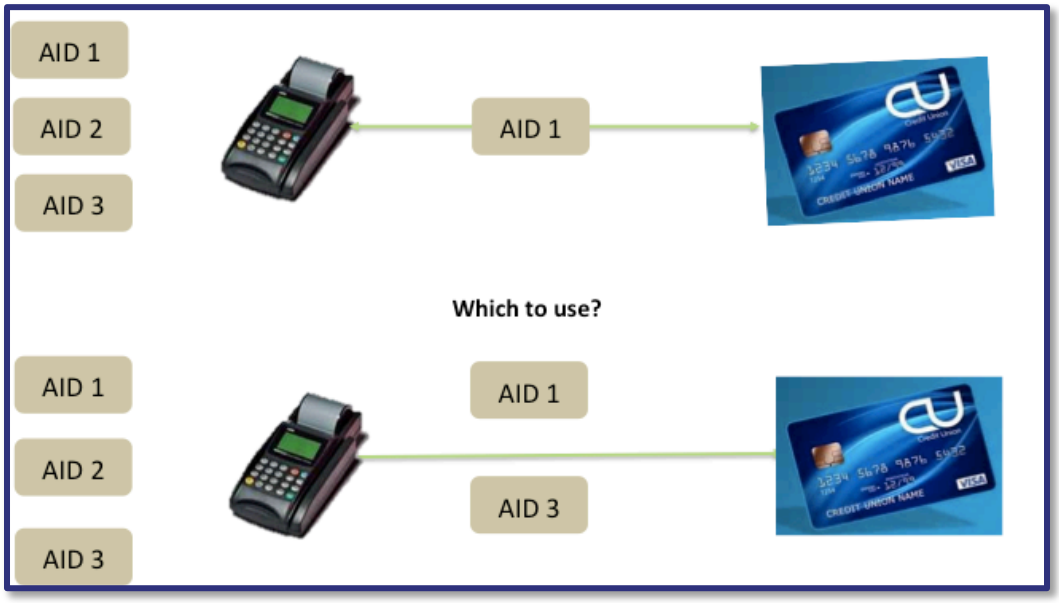


Fig 2

In March, 2013 most of the U.S. debit networks (including CU24) agreed to adopt a common debit AID to clarify, simplify and make more efficient the migration to EMV. Nevertheless, there remain some important issues to be resolved to support the general rollout of EMV. There are efforts underway to formulate an entity to manage and govern a common approach to EMV across the country.

CARDHOLDER VERIFICATION METHODS (CVM) and CONTACT vs. CONTACTLESS AUTHENTICATION

A Cardholder Verification Method (CVM) is a means of authenticating the cardholder, or ensuring that the user of a card is the genuine cardholder. During CVM, the terminal determines which CVM approach is required (according to the appropriate AID), if any. There are several possible approaches for Cardholder Verification:

- **Signature –** The card verification method may require the cardholder's signature.
- **Online PIN –** When online PIN authorization is used, data from both the chip card and the terminal are input to an algorithm that generates dynamic, unique encryption for each transaction. The issuer's host system validates the encryption. This is arguably the most secure authentication method.
- **Offline PIN –** 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 – at a ticket kiosk, for example.

Cards can be configured to allow both online and offline authorization, depending on the circumstances.

Although rare and with risk, cards may require no authentication at all.

There are two access methods available to issuers for cardholder verification – 'contact' or 'contactless' access. Issuers may choose between these implementation options based on their needs, service objectives and risk considerations.

With 'contact chip card technology', the distinctive and visible gold square that is mounted in the card is the actual card contact. It is positioned in the same location on every smart card. Embedded in a cavity directly behind the gold plate and protected by a thin capsule, the contact itself allows the chip to connect to, and exchange data with, a reader when inserted in a card acceptance device. This connection also enables the chip to receive power from the terminal. The gold-plated contact pad on the card must make contact with the card reader. These pads provide electrical connectivity when inserted into a reader,

which is use as a communications medium between the smart card and terminal. With contact, the card is inserted into the terminal, similar to how a hotel key is dipped into a slot to be read. The terminal communicates with the card via the chip.

For 'contactless' acceptance, the chip card communicates with, and is powered by, the reader through Near Field Communications (NFC) technology. This radio technology does not actually require contact between the card and the reader. Instead, connectivity is provided by the card-embedded antenna to near-field communications. (Fig. 3)

Chip Card Structure

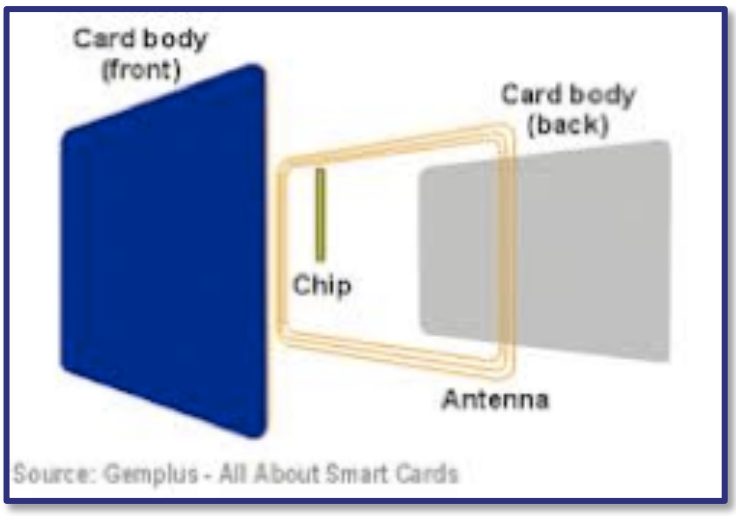


Fig 3

It may be advisable that issuers issue cards that support both methods, called "dual interface" cards.

COMPLICATIONS OF IMPLEMENTING EMV

Despite the enhanced security protections and advantages of smart-card technology, both card issuers and acquirers face complications in implementing EMV.

Unlike most other countries that have one major payment network and a single authority to manage standards, the United States has neither a single payment network (in fact, it has 18) nor a decision-making authority to establish standards for EMV implementation. These issues are the subject of much discussion and debate

across the industry, and there are currently efforts to establish an independent entity to manage EMV standards for a common debit network AID.

The Dodd-Frank legislation's Durbin Amendment not only allows, but requires, issuers to enable at least two unaffiliated debit networks on their cards. Issuers are often members of multiple networks. Original EMV standards do not accommodate such choices, creating a significant complication for implementing EMV in the U.S.

Most of the debit networks, including CU24, have agreed on a common AID, or standard, for debit in the U.S. Despite the agreement, there remain some issues of compatibility and cooperation to be resolved, and these industry discussions are ongoing. Without full resolution, issuer choices could be limited, rendering it cumbersome, difficult and expensive to change network affiliations as issuer needs develop and change.

Multiple AIDs loaded at the terminal add complexity. Today's terminals are not generally equipped for transaction-routing decisions, which are typically dictated by BIN tables loaded at the processor level. The selection of an AID to use for the transaction is made during the initial interaction between terminal and card, with the terminal determining which AID to execute. Original EMV specifications do not support multiple AID and routing decision-making.

'Standard EMV' relies on an issuer choosing from a list of available networks if the terminal identifies multiple matching AIDs, again conflicting with U.S. regulations that require a minimum of two debit networks to be available on a card, and which empower the merchant to choose the network for routing.

ATM acquirers use multiple BIN files and issuer priority flags to determine routing of the transactions. This is contrary to fundamental EMV specifications that determine routing at the source of the transaction; currently, a solution providing for multi-option routing does not exist.

If the industry ends up with multiple AIDs, issuer processors, acquirer processors, vendors, manufacturers, and networks will all be required to perform multiple cumbersome, time-consuming, and expensive certifications.

In the absence of a single authority, multiple industry workgroups have formed to analyze and debate these and other related issues. Inability of the U.S. payment network industry to simplify this situation for issuers and acquirers could inhibit EMV deployment, resulting in possible delays until clarity and a common AID and standards are available. Discussions are underway to create a single independent entity to manage EMV standards in the U.S.

MANDATES AND LIABILITY SHIFTS

EMV is not mandated in the U.S.; rather, the migration to EMV is being encouraged by the major payments companies through a series of liability shifts. That is, based on an announced schedule for each of the major payments networks, financial liability for transactions will shift to the non-EMV compliant party to a fraudulent transaction.

The four major payment brands established a calendar of liability shifts, as follows:

EMV Liability Shift Key Dates

	AMERICAN EXPRESS	DISCOVER	MasterCard	VISA
April 2013 Acquirers Must Support EMV	Y	Y	Y	Y
April 2013 ATM Counterfeit Cross-Border Liability Shift			Y	
October 2015 POS Lost or Stolen Liability Shift			Y	
October 2015 POS Counterfeit Liability Shift (Excl AFDs)	Y	Y	Y	Y
October 2016 ATM Counterfeit Liability Shift			Y	
October 2017 POS AFD Counterfeit Liability Shift	Y	Y	Y	Y

Since EMV compliance is encouraged through liability shifts instead of a mandate, issuers and acquirers may make cost and investment based judgments as to when and whether they wish to convert to EMV technology.

For example, consider the liability shift date for cross-border ATM transactions. If cross-border transactions are only a small portion of an ATM acquirer's transaction volume, the acquirer may choose to defer upgrading its ATMs until a later date (after the established liability shift date), and accept the limited risk associated with a small portion of their transactions.

Credit unions should note, however, that fraudulent activity tends to move to the weakest link in the payment chain, so ignoring the liability shift calendar should not be taken lightly.

FIVE MYTHS ABOUT EMV

There are some common misconceptions about EMV. A brief review of some of these issues can help credit unions better understand the migration to EMV here in the U.S.

- **EMV is mandated.** *Not true.* There is no single U.S. authority that can mandate a shift to EMV for card issuers, merchants or payment networks. Instead, the major payment networks have established a series of transaction liability shifts as incentives for industry participants to adopt EMV. That is, upon the date established for a liability shift, say, ATM acquired transactions, the party (issuer or acquirer) that is not EMV compliant will be held financially responsible for any fraudulent card transactions. Issuers will evaluate the level and cost of exposure related to non-compliance with EMV. Each of the major card networks has announced the initial dates for the shifts in liability.
- **EMV simply replaces the magnetic stripe on existing cards.** *Not true.* The migration to EMV involves more than simply replacing the card. EMV processing is significantly more complicated, and it is specific to each AID or network. That process is much different in today's environment where the magnetic stripe is used by all networks in the same way.

- **United States is behind in EMV adoption.** *Not true.* Magnetic stripe technology was implemented in the U.S. long before EMV technology was developed, and long before card infrastructures were developed in other countries. The magnetic stripe has served the U.S. well and cost-efficiently for many years. Until recently, it has been unnecessary for the U.S. to implement EMV. With advances in security, and the need for compatibility with the rest of the world, the U.S. is now moving toward EMV migration.

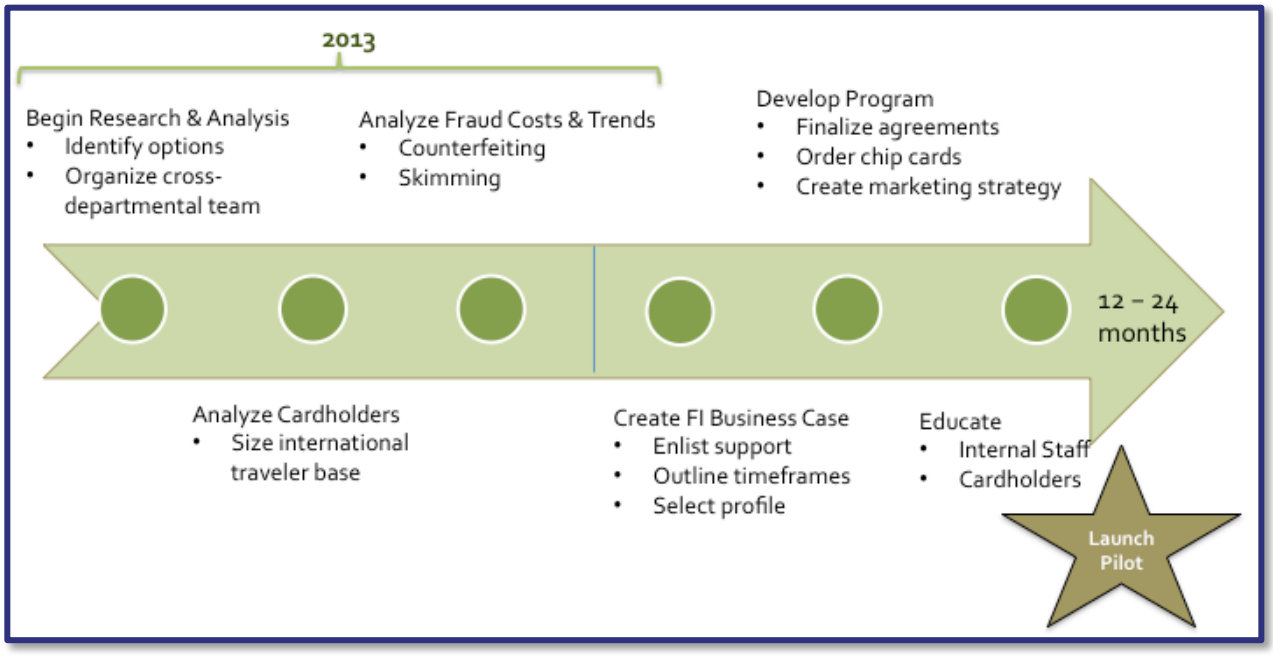
- **U.S. adoption will mirror the rest of the world.** *Not true.* There are important differences in the U.S. that will make EMV implementation unique and more complex. Key among these factors is that the U.S., unlike most other markets, does not have a single payment network or authority that governs transaction processing and these markets are highly competitive, each with its own features and interests. In addition, U.S. regulations impose choice in the U.S. network and card marketplace, making EMV implementation more complex. EMV was not originally designed for this kind of competitive environment.

- **EMV adoption solves all fraud problems.** *Not true.* While EMV technology offers much more security than magnetic stripe cards, no technology is completely secure. Criminals are working on methods to overcome EMV security barriers. Fraud generally moves to the weakest link in the chain, and transaction processing technologists continue to work to keep ahead of criminal elements. There continue to be specific challenges to card-not-present activity.

A ROAD MAP TO PREPARE FOR EMV

As the more general payments industry migrates to an EMV infrastructure, and even as industry groups move toward resolution of remaining issues, credit unions should proceed with their plans for EMV migration. A basic roadmap is depicted below, but it will surely have to be adapted to fit the needs of individual credit unions, as well as coordinated with processors and suppliers.

Sample EMV Roadmap



- Organize cross-departmental teams, including all departments of the credit union that will be affected, to begin analyzing options and requirements. You might begin by researching and identifying credit card members who are international travelers. International travelers are the first to encounter difficulty in trying to use magnetic stripe cards in overseas EMV infrastructure markets. With care, they can serve as a good initial experience with EMV issuance. You might also consider in-house staff for initial tests.
- Analyze your credit union's fraud costs and trends, and determine exposure or experiences with counterfeiting or skimming. This will begin to give you a sense of the return on your investment and urgency with which you might approach

EMV implementation. Be mindful that, traditionally, fraud migrates to the weakest link.

- Create a business case, outlining the various component one-time costs, ongoing expenses and any incremental fee-based revenue associated with EMV implementation. Include estimates or projections on reduced fraud costs. Outline projected timeframes for credit card issuance in a first phase, and debit cards in a second phase, including an assessment of basic costs of preparation, issuance and certification. Credit unions will want to confer with their processors and suppliers on these issues.

- Develop your program. Finalize agreements with your processor and manufacturers. Create a marketing strategy to educate both your staff and your members. The cardholder experience will be different; ensuring a successful transition will require education and time across all program participants.

- Launch a pilot. Identify a small group of prospective cardholders. Internal staff and/or your international travelers may be the best early segments. Review the cardholder experience and the effects on your operations. Learn about lead times and customer support requirements. Confer with other credit unions, your processor, and your network partners to learn from the experience of others. Analyze what went well and what needs to be improved. Understand the results of your pilot before committing to broad issuance or large orders.

- Finally, early on, identify someone in the organization whose responsibility it is to monitor developments regarding EMV. It will help to have an "in-house" expert as the industry moves forward. There are numerous sources of information. Much is published across the Internet, and many payments companies (including CU24) offer Webinars, White Papers and additional resources to help keep you abreast of events.

SUMMARY

EMV is an open-standard set of specifications for smart card payments and acceptance devices. The EMV specifications were developed to define a set of requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards.

The most important benefit of EMV is the reduction in card fraud from counterfeit, lost and stolen cards. EMV also provides interoperability with the global payments infrastructure–consumers with EMV chip payment cards can use their cards at any EMV-compatible payment terminal around the world. EMV technology supports enhanced cardholder verification methods and, unlike magnetic stripe cards, EMV payment cards can also be used to secure online payment transactions.

Regardless of the benefits or complications of EMV implementation, it appears clear that the U.S. payments industry is moving forward with migration to an EMV based infrastructure. It is important for all participants in the payments arena, including credit unions, to be aware of the coming changes, and to effectively prepare for a smooth transition to this new payment environment.

AN EMV GLOSSARY

The EMV Migration Forum recently published this list of standard EMV Terminology. The EMV Migration Forum is a cross-industry body focused on supporting an alignment of the EMV implementation steps required for global and regional payment networks, issuers, processors, merchants, and consumers to ensure a successful move from magnetic stripe technology to more secure EMV contact and contactless technology in the United States.

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

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

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

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

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

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

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

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

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

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

CVC - See card verification code.

CVV - See card verification value.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PIN - See personal identification number

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

Smart card - See chip card.

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

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

ABOUT CU24

CU24 is a credit union-owned, full-service payments cooperative that brings nationwide ATM and point-of-sale (POS) access to credit unions. Founded as a credit union alternative, CU24 offers a flexible, cooperative EFT environment designed to empower credit unions to attract and retain members. CU24 is the nation's largest credit union-owned POS network, and also offers access to 300,000 ATM locations nationally and internationally, many of them deposit-taking. In addition, CU24 offers access to the largest network of surcharge-free ATMs with nearly 70,000 locations.

CU24 offers the services and expertise that helps credit unions compete and improve their members' lives.

For more information about CU24, please visit www.cu24.com.