A Guide to EMV

Version 1.0

May 2011

Table of Contents

List of Figures

1 Introduction

1.1 Purpose

The purpose of this paper is to provide an overview of the EMV[1] specifications and processes. The document is intended to describe the "what" and the "why" of EMV within the context of the wider payments industry.

Additionally, the document describes the role of EMVCo LLC (EMVCo), and how various payment industry stakeholders may interact with EMVCo to participate in the ongoing management of the EMV specifications.

1.2 References

Information for this document has been drawn from several sources, including the following -:

- The EMVCo web site www.emvco.com
- *EMV Integrated Circuit Card Specifications for Payment Systems, version 4.2, June 2008* (EMVCo LLC)
- *EMV Contactless Payment Specification For Payment Systems, version 2.1, September 2010* (EMVCo LLC)
- Type Approval Process Documentation for terminals and cards available from EMVCo LLC.
- *EMV Security Guidelines, version 4.0, December 2010* (EMVCo LLC)

[1] EMV Integrated Circuit Card Specifications for Payment Systems

2 Background

2.1 What is EMV

The EMV Integrated Circuit Card Specifications for Payment Systems are global payment industry specifications that describe the requirements for interoperability between chip based consumer payment applications and acceptance terminals[2] to enable payment. The specifications are managed by the organisation EMVCo.

Named after the original organisations that created the specification, **E**uropay, **M**asterCard and **V**isa, the EMV specifications were first published in 1996. Fourteen years later, there are now one billion active EMV chip cards used for credit and debit payment, at 15.4 million EMV acceptance terminals deployed around the world[3].

The distinguishing feature of EMV is that the consumer payment application is resident in a secure chip that is embedded in a plastic payment card, often referred to as a chip card or smart card, or in a personal device such as a mobile phone. The chip provides three key elements - it can store information; it can perform processing; and because it is a secure element, it is able to store secret information securely, and perform cryptographic processing. These capabilities provide the means for secure consumer payments.

In order to execute a payment, the chip must connect to a chip reader in an acceptance terminal. There are two possible means by which this physical connection may be made which are often referred to as *contact* or *contactless*. With contact, the chip must come into physical contact with the chip reader for the payment transaction to occur. With contactless, the chip must come within sufficient proximity of the reader, (a maximum of 4cm), for information to flow between the chip and the acceptance terminal. In both scenarios, the

[2] Acceptance terminals include attended and unattended point of sale (POS), and automatic teller machines (ATMs).

[3] These figures were reported by EMVCo as of 1 September 2010 and represent the latest statistics from American Express, JCB, MasterCard and Visa as reported by their member financial institutions globally. They translate into 36 percent of total cards and 65 percent of total terminals in circulation based on the EMV standard.

acceptance terminal provides power to the chip to enable the chip to process.

Chips that are embedded in form factors such as plastic payment cards may support only a contact interface, only a contactless interface, or both contact and contactless. Chip cards that support both contact and contactless interfaces are referred to as dual interface. When the chip is installed inside a non-card form factor, such as a mobile phone, contactless is typically the only option for connection to the acceptance terminal.

2.2 Why EMV

EMV is designed to significantly improve the security for consumer card payments by providing enabling features for ***reducing*** fraudulent payment that results from ***counterfeit*** and ***lost and stolen*** cards.

The features that are defined by EMV are as follows -:

1. ***Authentication of the chip card*** to verify that the card is genuine so as to protect against counterfeit fraud for both online authorised transactions and offline transactions.

2. ***Risk management parameters*** to define the conditions under which the issuer will permit the chip card to be used and force transactions online for authorisation under certain conditions such as offline limits being exceeded.

3. Digitally signing payment data for ***transaction integrity***.

4. More robust ***cardholder verification*** to protect against lost and stolen card fraud for EMV transactions.

Counterfeit and lost and stolen card fraud represents significant cost to all participants in the payment process, including retailers, acquiring banks, card issuers and cardholders. Costs are realised through the processing of cardholder disputes, research into suspect transactions, replacement of cards that have been counterfeited or reported as lost and stolen, and eventual liability for the fraudulent payment itself. By reducing counterfeit and lost and stolen card fraud, EMV offers real benefits to retailers, acquirers, card issuers and cardholders.

☞ Why become involved in the EMVCo process?
EMV can help deliver real benefits – whether you are a retailer, an acquirer, or a card issuer, it can assist making a measurable impact to your bottom-line.

Why not have a say in the ongoing development of the EMV specifications? Become an EMVCo Technical Associate. For more information refer to the EMVCo website www.emvco.com.

3 The History of EMV

3.1 Timeline

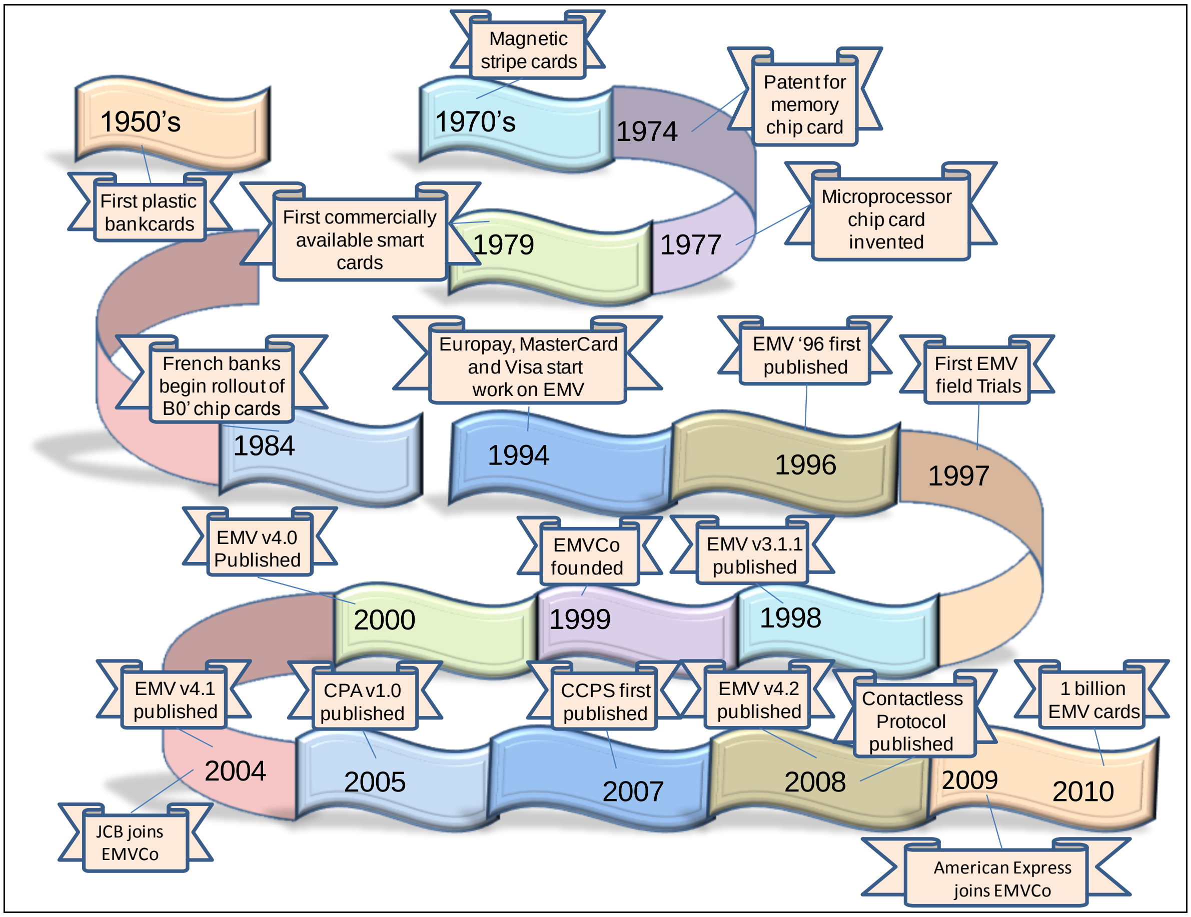


Figure 1: EMV Timeline

3.1.1 The Need for a Global Chip Card Standard

Chip cards have actually been with us for close on forty years. From the first inventions and patents of the early 1970s through to the initial commercial deployments in the 1980s, chip cards predate the delivery of the EMV specifications by more than a decade.

The first mass deployment of chip cards for payment by the banking industry was in France. Driven by a need to reduce high levels of fraud due to counterfeit and lost and stolen magnetic stripe cards, the French banks conducted field trials of microprocessor chip cards embedded in plastic bank cards in 1984.

By 1994, all French bank cards carried a chip using a French developed specification for chip card credit and debit payment known as *B0′*. Through issuing chip cards with PINs, the French banks were able to dramatically reduce fraud due to counterfeit and lost and stolen cards.

Following the French success, a number of European markets issued chip based bank cards through the 1990s to counter the growing fraud due to counterfeit and lost and stolen cards. However, all of these programs were based on domestic market specifications that were not interoperable. This trend of establishing proprietary domestic chip specifications in Europe through the early 1990s created a situation where chip technology helped protect against fraud for domestic transactions but magnetic stripe was the only method of acceptance when the cardholder travelled outside their local market.

In the early 1990s, the United Kingdom and Japan were considering the migration of their bank cards from magnetic stripe to chip. Both markets were reluctant to continue the propagation of non-interoperable domestic chip environments and so the driver for a global chip standard was born.

3.1.2 The Evolution of the EMV Specifications

In 1994, three international payment systems, Europay, MasterCard and Visa began the development of a global chip specification for payment systems. This globalisation continued when in 2004, JCB joined in participating with EMV, and American Express in 2009.

An initial version of the specification titled *EMV '96 Integrated Circuit Card Specification for Payment Systems,* was released in 1996. The first production version of the EMV specifications, version 3.1.1 was subsequently published in 1998.

The most recent version of the EMV specifications is version 4.2, published in 2008. Over the preceding ten years the EMV specifications evolved to meet the changing requirements of the payment industry, and benefited from over a decade of implementation experience in multiple markets across the globe.

Despite the ongoing change, a driving principle that stands behind the evolution of the EMV specifications has been that each new release or version is always backwards compatible with prior releases. This helps protect the investment in EMV infrastructure made by payment industry stakeholders.

3.1.3 Common Core Definitions

The EMV specifications allow the issuer the flexibility to define their own risk management processing that occurs in the chip card and the issuer host, and the information content (known as Issuer Application Data) that flows between the chip and issuer host. This has resulted in each payment system defining its own EMV chip card payment application specification[4] which requires an issuer to implement different card personalisation and host authorisation systems per card payment system.

In 2004, Common Core Definition (CCD) was introduced as part of the version 4.1 EMV specification. CCD defines a set of card application implementation options, card application behaviors, and data element definitions sufficient to accomplish an EMV transaction. Should an issuer wish to comply with CCD, it allows an issuer to define a common EMV chip based payment application that may be applied to all payment systems.

In 2005, EMVCo published a functional specification for an issuer payment application, called *EMV Integrated Circuit Card Specification for Payment Systems Common Payment Application* (CPA) that complies with the CCD requirements, and defines card applications, implementation options and card application behaviours. Issuers could choose to deploy CPA compliant chip cards as an alternative to chip cards that comply with the respective international payment system EMV card payment application specifications.

3.1.4 Extending EMV to Contactless and Mobile

The evolution of contactless chip has transpired in quite a different way when compared with EMV contact chip. While the development of contact chip occurred collaboratively amongst payment industry organisations from the onset, contactless development has occurred in a competitive environment with individual payment systems delivering implementations and specification development unilaterally.

In 2007 the *EMV Contactless Communication Protocol Specification* (CCPS) was published so that the hardware and firmware specifications (known as contactless Level 1) would be common for all payment system contactless payment applications.

This was followed in 2008 by the *EMV Contactless Specifications for Payment Systems – Entry Point Specification*, which facilitated multiple payment system contactless applications in the one contactless reader.

In addition to accepting EMV contactless chip cards, contactless readers that are compliant with the above EMV specifications can be designed to also accept contactless chips embedded in other form factors such as mobile phones. This is possible with the implementation of Near Field Communications (NFC) support in the mobile phone or equivalent device.

[4] International payment system EMV based card specifications include American Express AEIPS, JCB J/Smart, MasterCard M/Chip and Visa VIS.

3.2 EMV Around the World

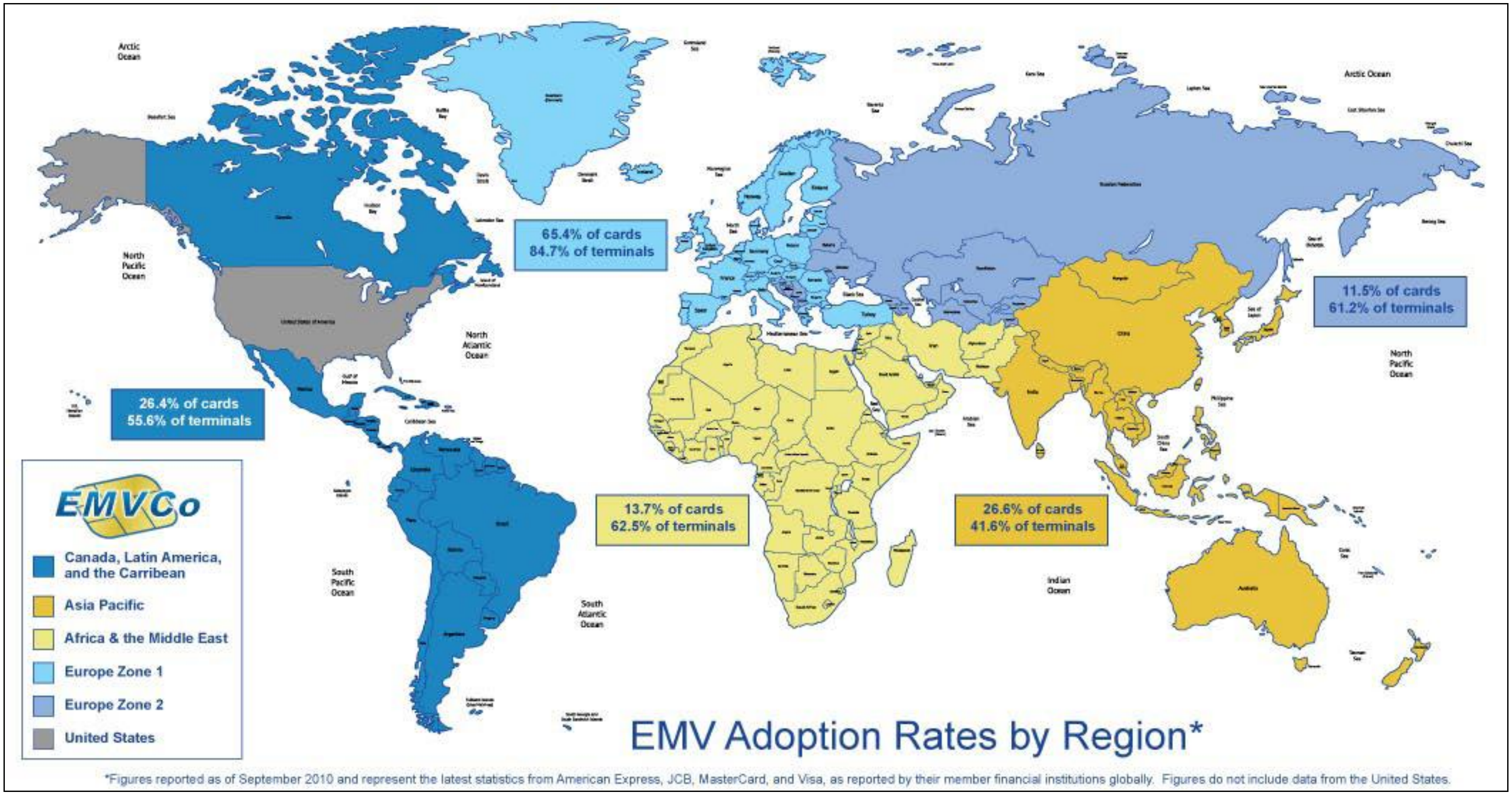
From the earliest field trials in 1997, to the progression of national migrations from magnetic stripe to EMV chip in various markets around the world, EMV is a global standard for chip payment and continues to grow in usage.

Today, 36 percent of total cards, and 65 percent of total terminals deployed are based on the EMV standard[5]. The following diagram provides an overview of the global adoption of EMV by major region.

☞ Protect your investment in EMV infrastructure.
The EMV specifications continue to develop to meet the changing needs of the payment industry.

Make sure you can provide input into the future development of the EMV specifications. Become an EMVCo Technical Associate. For more information refer to the EMVCo website www.emvco.com.

[5] These figures were reported by EMVCo as of 1 September 2010 and represent the latest statistics from American Express, JCB, MasterCard and Visa as reported by their member financial institutions globally.



EMV Adoption Rates by Region*

*Figures reported as of September 2010 and represent the latest statistics from American Express, JCB, MasterCard, and Visa, as reported by their member financial institutions globally. Figures do not include data from the United States.

Figure 2: Global EMV Adoption Rates by Region – Status September 2010

4 EMVCo LLC

In February 1999, Europay, MasterCard and Visa created the limited liability company, EMVCo, as a separate entity to manage, maintain, and enhance the EMV specifications.
In 2002, Europay was acquired by MasterCard.
In 2004, JCB joined with MasterCard and Visa as co-owners of EMVCo, and in 2009, American Express joined as the fourth owning entity.

4.1 EMVCo Mission

The primary goal of EMVCo is to facilitate the interoperability of chip based consumer payment applications with acceptance terminals to perform payment transactions. This is achieved through two primary activities -:

1. The management, maintenance and ongoing enhancement of the EMV specifications.

2. Managing testing and approval procedures for all EMV chip capable terminals and certain aspects of EMV chip cards to assess compliance with the EMV specifications.

The scope of EMVCo's mandate in these areas of activity is to support EMV payments for transactions through any payment channel, both existing and those that may evolve in the future. Traditionally the focus has been on card present transactions via contact chip cards. More recently, this has been extended to the acceptance of contactless chip cards, and support is being developed for evolving form factors such as mobile phones.

4.2 Structure of EMVCo Management and Operations

The structure of EMVCo's management and operations, and interactions with third party advisors is illustrated in the following diagram.

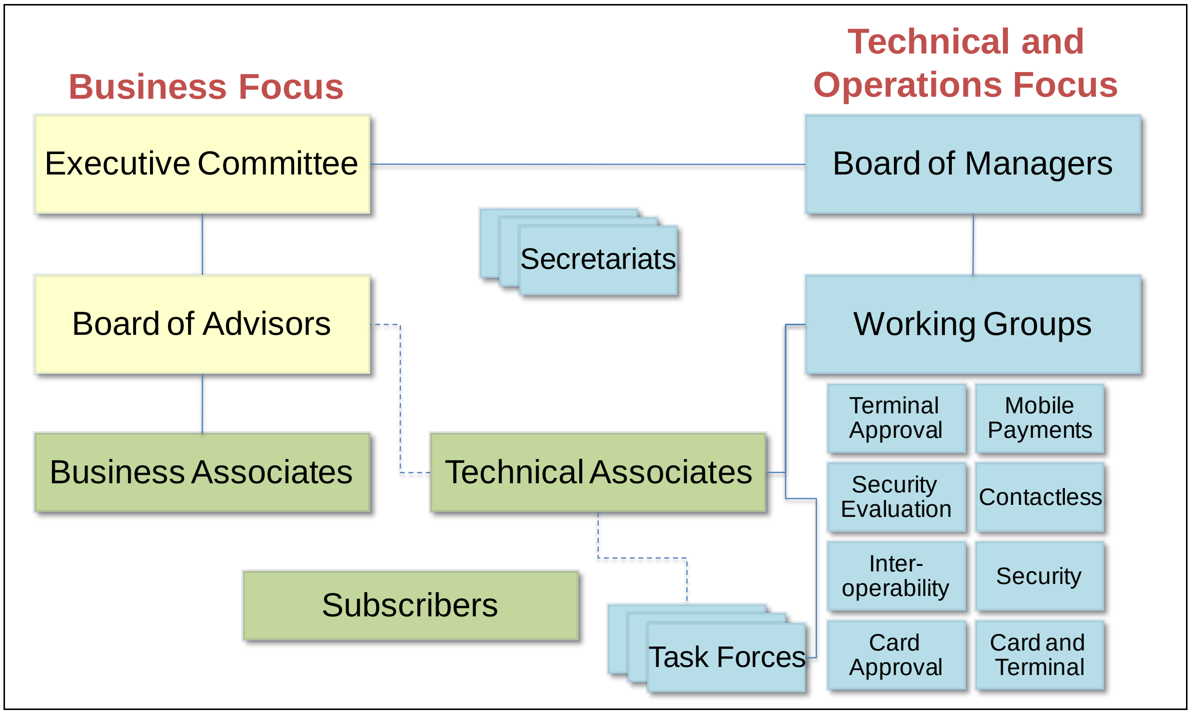


Figure 3: EMVCo Interaction Structure

American Express, JCB, MasterCard and Visa have appointed individuals to work at both management and working group levels within the EMVCo organisation. The Board of Managers, comprised of an individual appointed by each of EMVCo's four owners, generally manages EMVCo. In addition, regarding certain limited matters, EMVCo's owners make management decisions for EMVCo. The Executive Committee, comprised of individuals appointed by each of EMVCo's owners, provides advice to the Board of Managers and helps to resolve disputes among the Board of Managers or EMVCo's owners, but does not have management authority over EMVCo.

EMVCo maintains the EMVCo Associates Program, in which third parties can provide input to EMVCo and participate in certain EMVCo activities as a Business Associate or Technical Associate. Business Associates provide EMVCo with input on strategic business and implementation matters related to the use of the EMV specifications. Eligible candidates for the Business Associate role are payment service providers (i.e., payment card issuers and acquirers carrying the risk of payment transactions) as well as their representative associations and networks. Each Business Associate may appoint an individual to serve on the Board of Advisors and, accordingly, advise the EMVCo Executive Committee.

Any payment industry stakeholder may participate as a Technical Associate and provide EMVCo with input and receive feedback on detailed technical and operational considerations connected to the EMV specifications and related processes. Technical Associates are able to engage with all eight of the EMVCo technical Working Groups and receive updates or provide input on the Working Group activities and specifications. Six seats on the EMVCo Board of Advisors are reserved for Technical Associates representing distinct market sectors. Technical Associate representation on the Board of Advisors is determined through an annual election process.

Organisations that currently participate in EMVCo as Business Associates or Technical Associates are listed on the EMVCo website.

EMVCo also maintains the EMVCo Subscriber Program, which anyone can join as a Subscriber to receive advance notice of pending developments and changes, submit queries to EMVCo, and participate in a more regular dialogue with EMVCo. Organisations that may benefit from being Subscribers are participants in the global payment industry, including vendors, consultants, laboratories, payment systems, retailers and regional associations.

EMVCo hosts an annual User meeting for Associates and Subscribers.

4.3 The Role of the Payment Systems versus EMVCo

EMVCo is a standards body for the payments industry that manages, maintains and enhances the EMV specifications and associated approval procedures. EMVCo does not define or issue products, and has no mandate to enforce EMV compliance within the marketplace.

EMVCo operates separately from the international payment systems that own EMVCo, with its own separate approval and decision making processes. These payment systems do however, assume the role of defining and issuing products, and enforcing EMV compliance for products that carry their respective brands.

Additionally, the individual payment systems publish their own EMV chip card payment application specifications which define the options for card risk management processing for their respective branded chip card products. Also, the payment systems maintain the responsibility for the functional testing and type approval for cards that are compliant with their own product specifications.

The individual payment systems have to personalise the EMVCo kernel to ensure product acceptance matches global and regional rules.

4.4 EMVCo Relationship with Other Standards Bodies

The EMV specifications cannot be considered in isolation, and to this end, EMVCo collaborates with other industry bodies and standards organisations as follows.

1. **International Organisation for Standardisation (ISO)** - The EMV specifications are based on underlying International Organisation for Standardisation (ISO) standards as follows -:

   - ISO/IEC 7816: Identification Cards – Integrated Circuit(s) Cards
   - ISO/IEC 14443: Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards

2. **Payment Card Industry Security Standards Council (PCI)** is primarily concerned with the protection of sensitive payment information such as account information and personal identification numbers (PINs). EMV and PCI are complementary in enhancing payment security and reducing fraud due to counterfeit and lost and stolen cards.

3. **The Near Field Communication (NFC) Forum** – EMV is working to extend EMV payments to the contactless and mobile channels. This requires alignment with the NFC Forum which is responsible for developing the specifications for communication between NFC devices and services.

4. **GlobalPlatform** - Part of EMVCo's activities is to review the functionality and security of platforms on which an EMV payment application will reside. Alignment with standards bodies such as GlobalPlatform are important as EMV payment applications are increasingly implemented on shared chip platforms that support multiple applications, each from a different application owner.

5 EMV – How it Works

5.1 Stepping Through an EMV Transaction

There is a fundamental difference between a magnetic stripe read, and an EMV chip transaction. For magnetic stripe, the card is simply a data store that is read by the terminal and then the card is no longer used. The terminal performs all the processing and applies the rules for payment.

During an EMV transaction, the chip is capable of processing information and actually determines many of the rules for the payment. The terminal helps enforce the rules set by the issuer on the chip. These rules can include enforcing services such as offline data authentication, verifying the cardholder identity via PIN or signature, online authorisation and so on. It is up to the issuing bank to define which of these services is required for the current transaction, via the rules placed on the chip. If the terminal is unable to provide the services requested by the chip, the issuer can set rules that will result in the chip declining the transaction.

Accordingly an EMV transaction requires interaction between the chip and the terminal which is a protocol that is defined by the EMV specifications. The protocol defines a series of steps, which are described in the following sections.

5.1.1 Steps for an EMV Contact Transaction

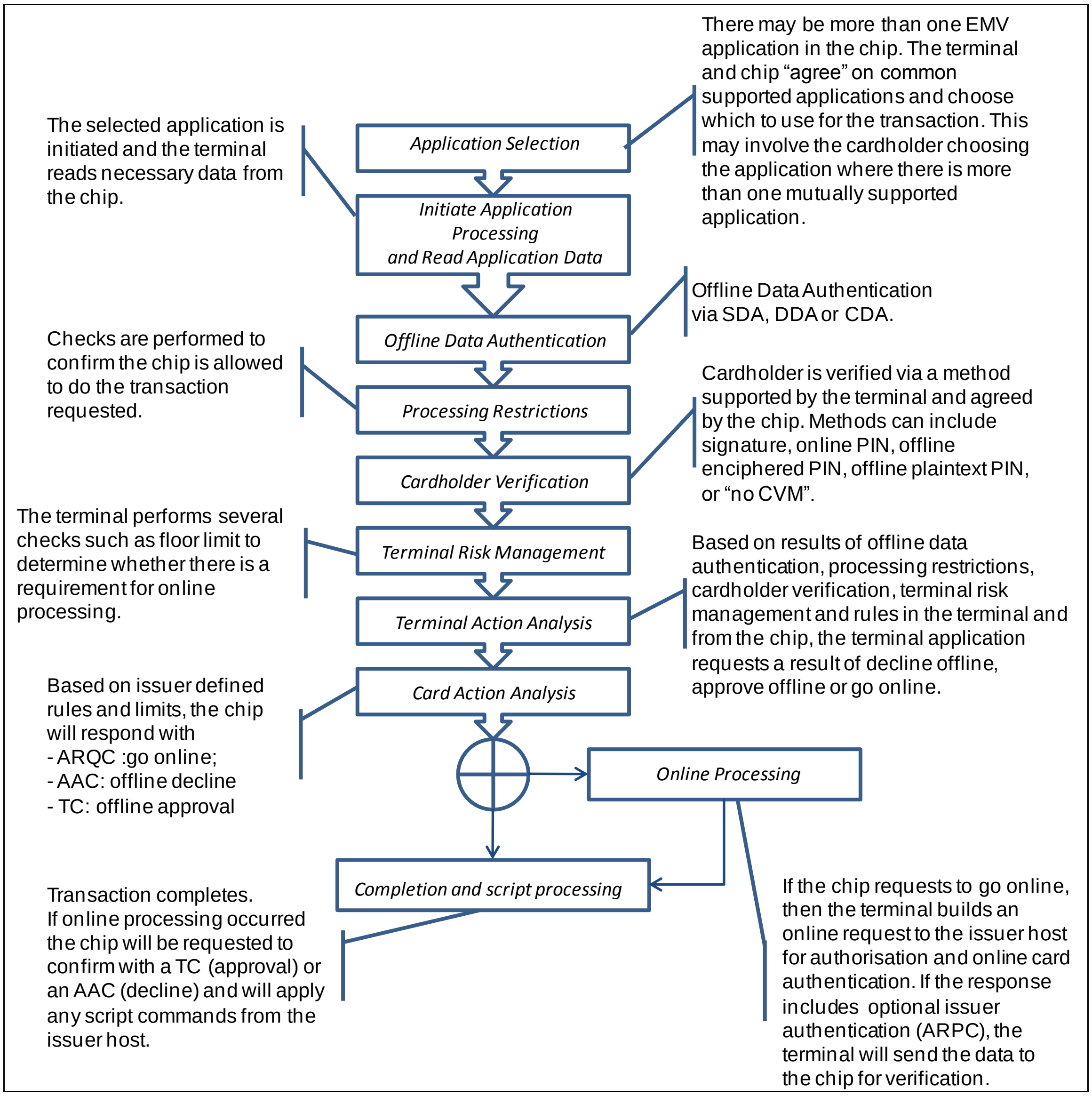

Application Selection
Initiate Application Processing and Read Application Data
Offline Data Authentication
Processing Restrictions
Cardholder Verification
Terminal Risk Management
Terminal Action Analysis
Card Action Analysis
Online Processing
Completion and script processing
There may be more than one EMV application in the chip. The terminal and chip "agree" on common supported applications and choose which to use for the transaction. This may involve the cardholder choosing the application where there is more than one mutually supported application.
The selected application is initiated and the terminal reads necessary data from the chip.
Offline Data Authentication via SDA, DDA or CDA.
Checks are performed to confirm the chip is allowed to do the transaction requested.
Cardholder is verified via a method supported by the terminal and agreed by the chip. Methods can include signature, online PIN, offline enciphered PIN, offline plaintext PIN, or "no CVM".
The terminal performs several checks such as floor limit to determine whether there is a requirement for online processing.
Based on results of offline data authentication, processing restrictions, cardholder verification, terminal risk management and rules in the terminal and from the chip, the terminal application requests a result of decline offline, approve offline or go online.
Based on issuer defined rules and limits, the chip will respond with
- ARQC :go online;
- AAC: offline decline
- TC: offline approval
Transaction completes.
If online processing occurred the chip will be requested to confirm with a TC (approval) or an AAC (decline) and will apply any script commands from the issuer host.
If the chip requests to go online, then the terminal builds an online request to the issuer host for authorisation and online card authentication. If the response includes optional issuer authentication (ARPC), the terminal will send the data to the chip for verification.

Figure 4: Processing Steps for an EMV Contact Transaction

5.1.2 Steps for an EMV Contactless Transaction

The major difference between an EMV contactless transaction and an EMV contact transaction is that the transmission of information between the chip and the terminal is faster for contactless and some of the transaction steps may be performed after the chip has left the proximity of the reader (i.e., online authorisation). The goal is to minimise the amount of time that the chip must be held within proximity of the reader.

5.2 EMV Features

The specific features defined by EMV that achieve the protections and controls to reduce counterfeit and lost and stolen card fraud are described in the following sections.

5.2.1 Application Cryptogram

During an EMV transaction, an application cryptogram is generated using two-key triple DES cryptography. This is a signature generated from critical data elements contained in either the online authorisation request to the card issuer (if online authorisation is required), or the final financial transaction required for clearing and settlement.

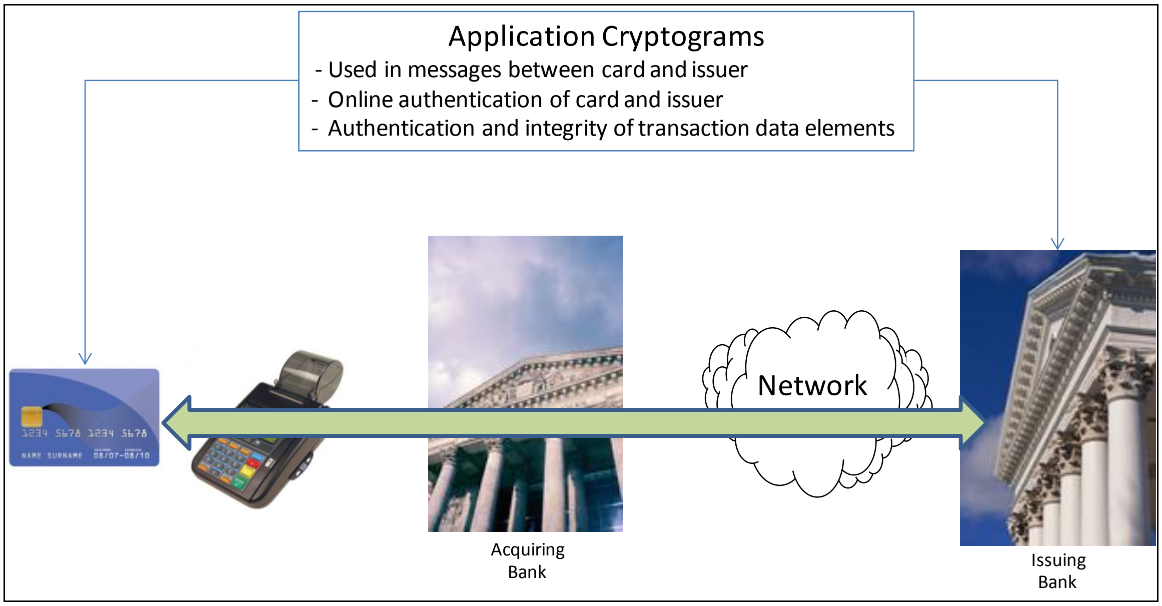

Application Cryptograms
- Used in messages between card and issuer
- Online authentication of card and issuer
- Authentication and integrity of transaction data elements
1234 5678 1234 5678
NAME SURNAME
08/07-08/10
Network
Acquiring Bank
Issuing Bank

Figure 5: Application Cryptograms

The cryptogram that is generated for the online authorisation request is termed the Authorisation Request Cryptogram (ARQC) and the cryptogram that is generated by signing data elements when a chip approves the payment for clearing and settlement is known as the Transaction Certificate (TC). If the transaction is declined, the chip will generate a cryptogram known as an Application Authentication Cryptogram (AAC).

The purpose of these application cryptograms is twofold-:

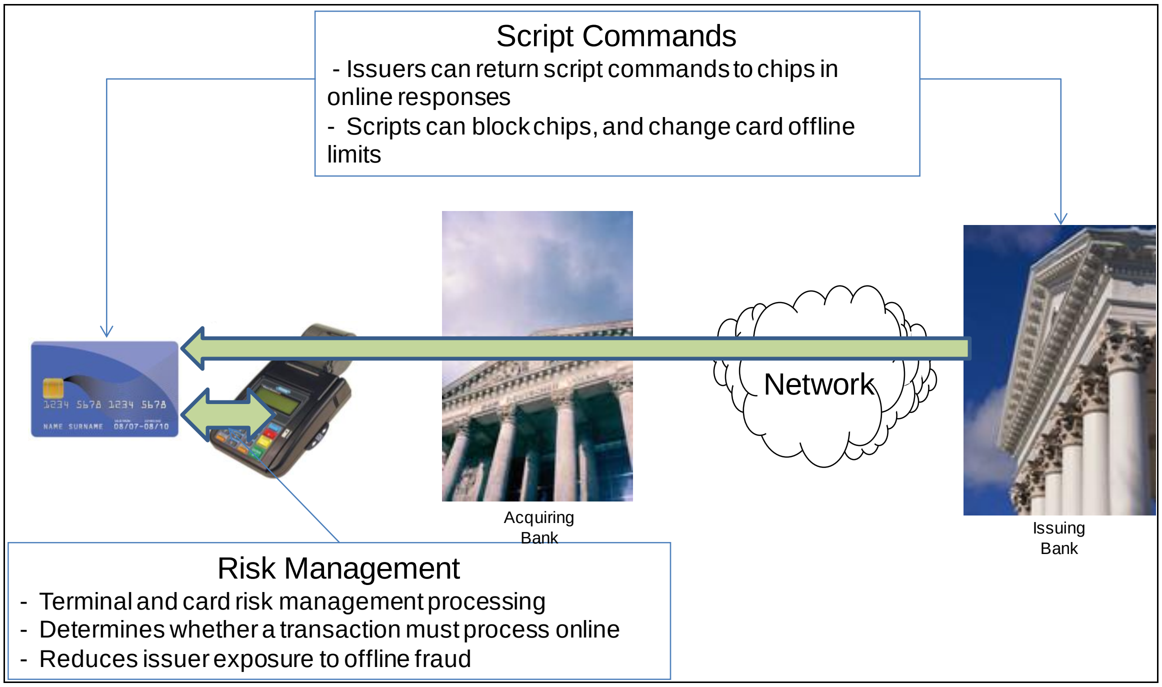
1. ***Online card and issuer authentication***
   The chip generates an ARQC which is sent in the authorisation request when an EMV payment transaction proceeds online to the issuer host. The ARQC can be verified by the issuer host and this confirms that the chip is not counterfeit.

As part of the authorisation process, the issuer host may generate a return cryptogram known as the Authorisation Response Cryptogram (ARPC) which is sent back to the chip in the authorisation response. The verification of the ARPC allows the chip to confirm that the approval was received from the actual issuer host, and therefore that any counters or offline limits on the chip may be reset.

2. ***Signing transaction data elements for transaction authentication and integrity***
   The following cryptograms are generated by signing critical data elements in the respective transaction messages. Validation of the cryptograms by the recipient helps to confirm the data elements are not altered.
   - ARQC – online authorisation request;
   - ARPC – online authorisation response;
   - TC – financial message for clearing and settlement for an approved transaction;
   - AAC – declined transaction.

5.2.2 Risk Management and Authorisation Controls

EMV provides the issuing bank with controls at the point of sale which helps enable the issuer to reduce exposure to fraud and credit risk for offline and below floor limit transactions. The issuing bank can set limits in the chip card that restrict the number of consecutive offline transactions that may be processed.



Script Commands
- Issuers can return script commands to chips in online responses
- Scripts can block chips, and change card offline limits

Risk Management
- Terminal and card risk management processing
- Determines whether a transaction must process online
- Reduces issuer exposure to offline fraud

Figure 6: Risk Management and Script Commands

Additionally, EMV defines script commands that can be returned to the card in an online authorisation response that allows the issuer to change the card limits, perhaps even reducing them to zero depending upon assessed risk profiles. Issuers may also issue scripts to block or disable a lost or stolen card.

Under acquirer control, EMV provides a means for acceptance terminals to select transactions for online approval, based not only on floor limit, but also domestic or retailer criteria, as well as employing a random selection of below the floor limit transactions to be sent online.

Together, these measures provide protection against the use of lost and stolen or fraudulent cards which attempt to stay beneath the floor limit and provide the issuers with a means of permanently blocking a stolen card.

5.2.3 Cardholder Verification Processing

As well as continuing to support all the cardholder verification methods available for magnetic stripe, EMV defines two new features which provide issuers with greater flexibility in determining and enforcing methods for verifying the cardholder is the actual owner of the card during a payment. These features can help reduce fraud due to lost and stolen cards.

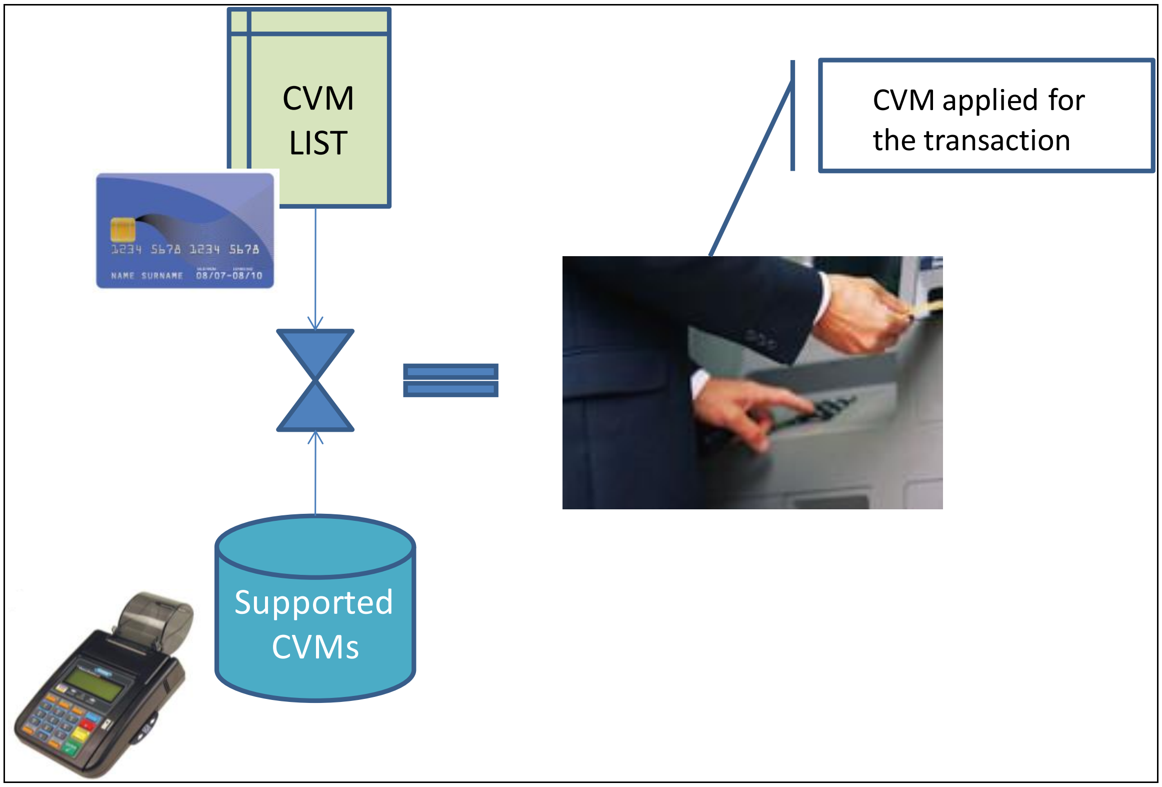


Figure 7: Cardholder Verification Processing

The first feature is the **Cardholder Verification Method (CVM) List** which is defined by the issuer in the chip card. The CVM list allows the issuer to specify in order of priority, the cardholder verification methods to be applied for particular acceptance conditions, allowing a CVM to be applied when supported by the terminal, but providing an alternative when the preferred CVM is not supported. For example, this allows an issuer to require the cardholder to use PIN in acceptance terminals that support PIN (perhaps domestically), but allow the cardholder to sign when travelling to markets that do not support PIN.

The second feature is a new CVM of **offline PIN**. While the use of offline PIN is entirely optional, it is possible to use an EMV chip card to verify a PIN entered into the terminal PIN pad by the cardholder and therefore provide a PIN based cardholder verification method available for all offline and online transaction acceptance environments, including below the floor limit and offline only.

There are two flavours of offline PIN defined by EMV: enciphered offline PIN where public key cryptography is used to protect the PIN as it is sent from the acceptance terminal to the card for verification and plaintext offline PIN where the PIN is sent in the clear from the acceptance terminal to the card for verification.

5.2.4 EMV Offline Data Authentication

EMV describes a feature known as offline data authentication to combat counterfeit fraud for card payments that are performed at offline card acceptance terminals. Offline data authentication uses public key cryptography to perform payment data authentication without the need to go online to the issuer host.

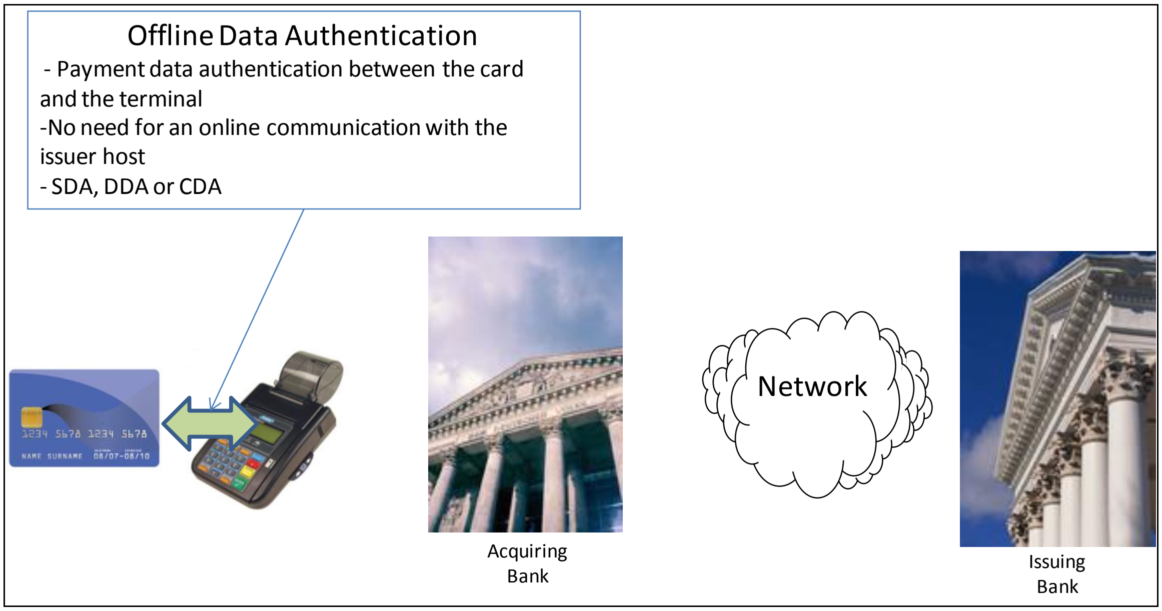

Offline Data Authentication
- Payment data authentication between the card and the terminal
-No need for an online communication with the issuer host
- SDA, DDA or CDA
1234 5678 1234 5678
NAME SURNAME 08/07-08/10
Network
Acquiring Bank
Issuing Bank

Figure 8: Offline Data Authentication

There are essentially two flavours of off-line data authentication - Static Data Authentication (SDA), and Dynamic Data Authentication (DDA). Combined Data Authentication (CDA) is a variation on DDA.

During a payment transaction, the chip card and the terminal agree to perform SDA, DDA or CDA. Only one method of offline data authentication is performed for a particular transaction. When offline data authentication is not performed, an EMV transaction must go online for authorisation.

The essential difference between SDA and DDA is that while SDA indicates that the payment application data read from the chip has not been manipulated or changed, SDA does not mean that the card is authenticated offline. It is possible to copy the chip card data, including the SDA cryptogram, and write it to another chip card to create a counterfeit card that could successfully pass SDA at the point of sale. DDA indicates that the chip card, and the information on the card, has not been altered since being issued to the cardholder, and that the card is not a copy of the original chip card issued. DDA is a stronger form of offline data authentication than SDA because DDA indicates that the card has been authenticated offline.

CDA, as a variation of DDA, is designed to combat a sophisticated method of attack at the point of sale in which the attacker attempts to use a valid chip card to pass offline data authentication, but from then on during the payment, simulates card actions in order to obtain authorisation.

Card issuers will choose an offline data authentication method based on factors such as cost per card and speed of transaction. These costs are weighed against the risk of fraudsters attacking chip cards using the less robust authentication methods such as SDA, while the much easier target represented by magnetic stripe cards is still prevalent.

EMVCo is constantly monitoring the strength of cryptography and on a regular basis issues key length recommendations published in EMVCo Notice Bulletins.

If an issuer chooses to issue a chip card that only permits transactions that are authorised online to the issuer host, the chip would not require offline data authentication support at all.

6 EMV Testing and Approval

6.1 Key EMVCo Objective

In addition to maintaining and evolving the EMV specifications, the other key and complementary EMVCo role is to assess the compliance of products developed to the EMV specifications, and approve products that pass testing prior to deployment in the field.

There are numerous activities that are performed by EMVCo in support of this objective which include defining and implementing test plans based on the EMV specifications and defining and implementing a process for the qualification of test tools to implement EMVCo test cases.

The actual testing is performed by EMVCo accredited external test laboratories located in numerous locations around the world. This is facilitated through an EMVCo managed laboratory accreditation program with an associated ongoing monitoring process.

The payment systems specify the rules regarding how long approved products may be used in the field.

The components that comprise the EMV approval process are described in the following sections.

6.1.1 Terminal Type Approval

Terminal type approval is defined and administered by the EMVCo Terminal Approval Working Group (TAWG) and is designed to assess whether EMV enabled acceptance terminals sufficiently conforms to the functional requirements defined in the EMV specification. There are two separate and independent processes involved.

EMV Level 1 terminal type approval is designed to verify whether the terminal chip reader demonstrates sufficient conformance to Level 1 of the EMV mechanical and electrical protocol specifications which covers the transfer of data between the terminal and the card.

EMV Level 2 terminal type approval is designed to verify whether the software residing in the acceptance terminal that performs the EMV processing, referred to as the EMV Level 2 kernel, demonstrates sufficient conformance to the EMV specifications. EMV defines the kernel as the terminal application software that supports the EMV payment application functions as defined in the EMV specifications. The non-EMV application functionality that supports functions like the printer and display, and building messages to send to the acquirer, is not considered part of the kernel.

The TAWG monitors the ongoing operation of the terminal type approval process and the application of test tools and tool updates. This allows the required improvements to be identified and the process to be improved as required.

Additionally, the TAWG manages a contractual process for terminal vendors seeking approval of their products. Vendors are issued a Letter of Approval for each product that successfully passes type approval.

6.1.2 Card Type Approval

Card type approval is defined and administered by the EMVCo Card Approval Working Group (CAWG) and is designed to assess whether the chip hardware and embedded EMV functionality sufficiently conforms to the electro-mechanical and functional requirements defined in the EMVCo specifications.

It is important to note that EMVCo does not manage the type approval process for chip cards that comply with international payment system card specifications. The payment systems directly manage card type approval processes for cards that comply with their respective EMV-based card specifications.[6]

However, EMVCo does manage the type approval process for chip-resident payment applications that are designed to be compliant with the EMV Common Core Definition (CCD) and Common Payment Application (CPA).

6.1.3 Chip Security Evaluation

The EMVCo chip security evaluation is designed to assess whether a chip demonstrates sufficient assurance of certain minimum levels of security required for EMV payment, including security mechanisms and protections designed to withstand known attacks. The results of the EMVCo chip security evaluation are then used by each payment system in their card approval process.

Card functional security evaluation is out of scope for EMVCo and is run by the payment schemes.

[6] International payment system EMV-based card specifications include American Express AEIPS, JCB J/Smart, MasterCard M/Chip and Visa VIS.

7 Implementation Considerations

The migration from magnetic stripe to EMV requires investment in changing the payment infrastructure and associated processes. Changes are required from the acceptance terminals installed at retailers, through acquirer switches and networks, right up to issuer authorisation hosts and card production systems.

It is important to note that the implementation of chip infrastructure is not an EMVCo role. It falls to the international and domestic payment systems, card issuers and card acceptors.

7.1 Issuer Considerations

An issuer migrating to EMV chip card issuance needs to consider at least three main areas of implementation activity as illustrated in the following diagram.

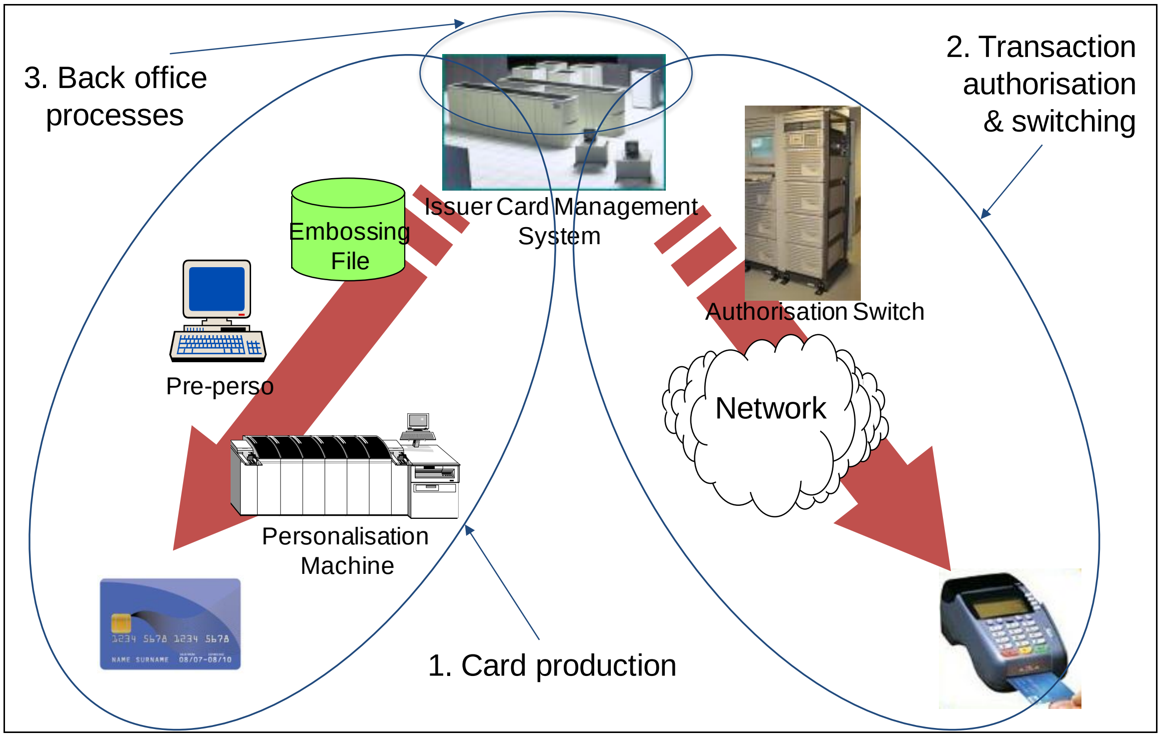


Figure 9: Issuer EMV Implementation Activities

These implementation activities are described in more detail in the following table.

Activity	Description
Upgrade card production and personalisation processes and infrastructure for chip.	Choosing a chip card platform with the necessary hardware that meets the requirements for issuing chip cards. These requirements may include single application, or multi-application, payment only, or payment plus other applications, contact only, or dual interface, and support for cryptographic processing such as public key.
	Determine the parameters and rules that must be personalised into the chip payment application that will meet the card issuer's requirements for reducing counterfeit and lost and stolen card fraud.
	Generate the EMV cryptographic keys required to support the card issuer's application features for reducing counterfeit and lost and stolen card fraud.
	Upgrade existing card production systems from the existing magnetic stripe delivery processes to enable the production and delivery of EMV chip cards.
Upgrade authorisation and settlement systems for chip.	Authorisation and clearing and settlement messages resulting from chip card transactions at the point of sale will carry new chip information. Changes are required to issuer systems to issue, manage, and authorise and settle transactions for EMV chip cards and to support the necessary operational processes that can take advantage of the enhanced chip data such as customer service, chargebacks and disputes, fraud, credit risk management, and management reporting.
Re-engineer internal processes in support for chip.	Update issuer customer service and back office operations. This includes updating processes to enable customer service representatives to support cardholders with EMV chip cards. Tools need to be provided to customer service representatives to enable them to have the necessary information to handle queries from cardholders with EMV chip cards. Systems and processes need to be enhanced to support chip cards back office operations such as chargebacks and disputes, fraud investigation and credit risk management

Table 10: Issuer Implementation Considerations

7.2 Retailer and Acquirer Considerations

An acquirer or retailer migrating to EMV chip card acceptance needs to consider at least three main areas of implementation activity as illustrated in the following diagram.

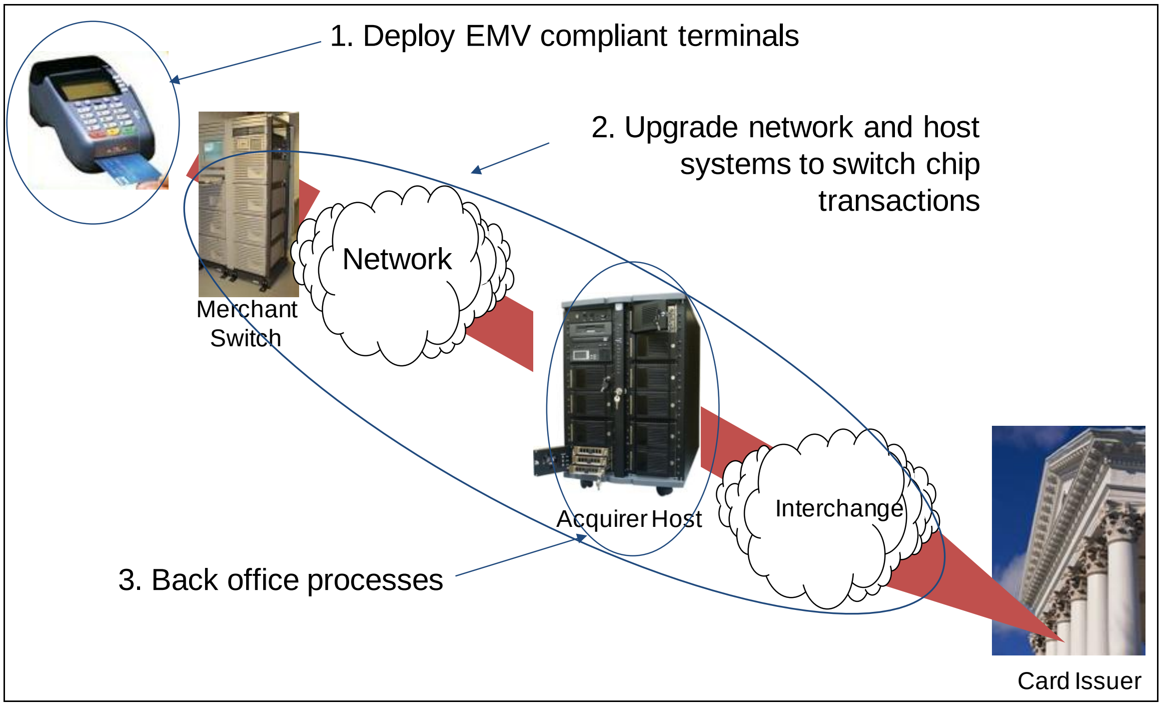

1. Deploy EMV compliant terminals
2. Upgrade network and host systems to switch chip transactions
Network
Merchant Switch
Acquirer Host
Interchange
3. Back office processes
Card Issuer

Figure 11: EMV Acceptor Implementation Activities

These implementation activities are described in more detail in the following table.

Activity	Description
Deploy EMV acceptance terminals, and retrain terminal operators and upgrade retailer support services	Procure approved EMV acceptance terminals. This means talking to vendors to agree on the EMV parameters to be installed in the terminals to meet retailer and acquirer requirements for accepting chip cards and ensuring the terminals are EMV Level 1 and Level 2 type approved.
	Ensure that existing terminal applications are integrated with the new EMV functionality provided by the EMV Level 2 application kernel.
	Upgrade terminal management systems so that EMV configurations and parameters may be managed efficiently and remotely.
	Deploy terminals in the field. This involves upgrading or replacing hardware to incorporate chip readers and upgrading software to include the EMVCo approved EMV functionality.
	Train terminal operators and cashiers to accept a

	chip card – to insert the chip card instead of swiping the magnetic stripe. Additionally, retailer field training staff, and retailer support staff need to be up-skilled to perform their tasks for chip implementation and support.
Upgrade host systems to switch chip transactions for authorisation and settlement.	Upgrade terminal to acquirer host interface. This means the message format for the interface between the terminal and the retailer and/or acquirer host will need to be upgraded to carry new EMV chip data elements.
	Upgrade host and interchange interfaces. This means the retailer and/or acquirer host will need to be upgraded to switch messages containing new EMV data elements from the terminals to outgoing interchange links to the card issuers. This will require mapping data elements from incoming messages on the terminal links to outgoing messages on the interchange links.
Re-engineer internal processes in support for chip.	Update back office operations and retailer service to take advantage of enhanced chip information available in the transaction messages from terminals. This includes upgrading procedures and staff operations to support the following functions. - Chargeback and transaction dispute procedures - Retailer service - Fraud Detection

Table 12: Acquirer Implementation Considerations

8 The Future

8.1 EMV Vision

EMVCo's vision is for all payment transactions through any payment channel, both existing, and those that may evolve in the future, to be able to benefit from the security features provided by EMV.

With input from the EMVCo Associates, EMVCo is currently shaping changes which fall broadly into two areas: enhancing the existing EMV protocol to meet future requirements, and creating global and industry standards for EMV-based transactions for contactless chip and mobile.

8.1.1 Contactless Roadmap

Building on the foundation of a common contactless reader that supports all payment system applications provided by the *EMV Contactless Communication Protocol Specification* and the *EMV Contactless Specifications for Payment Systems – Entry Point Specification*, EMVCo is now working on a combined contactless kernel specification and a single EMVCo administered contactless acceptance terminal type approval process for both Level 1 (hardware) and Level 2 (contactless payment application). This will be defined by the *EMV Contactless Payment Specification for Payment Systems*, currently in draft and undergoing a review process.

EMV will still support multiple contactless kernels in the one reader - each kernel for a payment system's contactless payment application. A goal for the future is to have a single EMVCo-developed common contactless kernel in the one reader, similar to what is currently the case for the contact chip.

8.1.2 Enhancing the EMV Security and Key Management Architecture

EMV relies heavily on cryptographic processing to realise benefits achieved through authentication of the EMV payment application, verification of the cardholder and validating data integrity.

For offline functions, EMV requires use of asymmetric RSA[7] public key cryptography. The challenge with RSA is that key lengths need to periodically be increased to stay ahead of attack techniques. The keys for RSA are becoming relatively large, increasing the time for cryptographic processing. As RSA public key lengths continue to increase, performance may become an issue.

[7] Rivest, Shamir and Adleman algorithm

EMVCo has identified Elliptic Curve Cryptography (ECC) as a viable alternative to RSA. ECC requires smaller keys and is significantly faster to process. The migration to ECC would also see a single dynamic offline data authentication technique replacing the current methods of SDA, DDA and CDA.

EMVCo Working Groups are currently assessing the timeframe and method of migration to ECC.

8.1.3 Mobile

The evolution of contactless payment has allowed the payment industry to contemplate form factors beyond chips embedded in plastic cards. EMVCo is collaborating with numerous industry groups such as the NFC Forum, the GSM Association and GlobalPlatform to define standards and implementation references to further the development of contactless mobile payment.

Work progresses in areas such as defining the architecture for EMV contactless mobile payment, establishing mobile handset requirements, customer user interface requirements, and specifying requirements for the secure element within a handset that contains the EMV payment application.

Additionally EMVCo, in cooperation with other industry players, has started working to initiate the development of a common testing and approval framework for contactless mobile payments.

☞ Help shape the future for EMV.
EMV is continuing to evolve into new channels such as contactless and mobile.

Will your business provide input into the development of these new and exciting channels? Become an EMVCo Associate. For more information refer to the EMVCo website www.emvco.com.

9 Glossary

Term	Description
Acquirer	A financial institution that enters into an agreement with retailers to facilitate acceptance of payment cards and then settles the transaction with the card issuer directly or via a payment scheme.
AEIPS	American Express ICC Payment Specification (Terminal and Chip Card)
Application Authentication Cryptogram (AAC)	A cryptogram generated by the card at the end of offline and online declined transactions to indicate that the card declined the transaction.
Application Cryptogram	A cryptogram generated by the card in response to a GENERATE AC command.
Authentication Request Cryptogram (ARQC)	A cryptogram generated by the card at the end of the first round of card action analysis which is included in the authorization request sent to the card issuer and which allows the issuer to verify the validity of the card and message.
Authentication Response Cryptogram (ARPC)	A cryptogram generated by the issuer and sent in the authorization response that is sent back to the acquirer. The acquirer and terminal provide this cryptogram back to the card which allows the card to verify the validity of the issuer response.
Automated Teller Machine (ATM)	An unattended terminal that has online capability, accepts PINs, and disburses currency.
Cardholder Verification Method (CVM)	The method to be used to verify the cardholder’s identity. This may include signature, PIN or no CVM required.
Certificate Authority (CA)	Trusted third party that establishes a proof that links a public key and other relevant information to its owner.
Combined DDA/Application Cryptogram Generation (CDA)	A type of offline data authentication where the card combines generation of a cryptographic value (dynamic signature) for validation by the terminal with generation of the Application Cryptogram to verify that it came from a valid card.
Common Core Definition (CCD)	A definition of card application implementation options, card application behaviors, and data element definitions sufficient to accomplish an EMV transaction.
Common Payment Application (CPA)	A functional specification for an issuer payment application that complies with the CCD requirements, and defines card applications, implementation options and card application behaviors.
Contactless transaction	A chip transaction where the communication between the card and the terminal does not take place over a contact interface.

Term	Description
Cryptogram	Result of a cryptographic operation which transforms data either to hide the data, or to produce a digital signature that may be used to verify the origin and integrity of the data.
Cryptographic Key	The numeric value entered into a cryptographic algorithm that allows the algorithm to encrypt or decrypt a message.
CVM List	An issuer-defined list in the chip card's payment application profile indicating the hierarchy of preferences for verifying a cardholder's identity.
Data Encryption Standard (DES)	The public domain symmetric key cryptography algorithm of the National Institute for Standards and Technology.
Dynamic Data Authentication (DDA)	A method of offline data authentication used to verify that issuer-selected card data elements and transaction-specific dynamic data elements have not been fraudulently altered and that they come from a valid card.
Elliptic Curve Cryptography (ECC)	A public key cryptosystem which requires smaller keys and is significantly faster to process than RSA. It is used for data encryption and authentication.
EMVCo	EMVCo LLC, a company that manages, maintains, and enhances the EMV specifications jointly owned by the payment systems.
Floor Limit	A currency amount below which an online authorization is not required for a single transaction unless a service code is present which requires online authorization.
International Organization of Standardization (ISO)	The international agency that establishes and publishes international technical standards.
Issuer	A financial institution that issues cards and whose name appears on the card as the issuer (or, for cards that do not identify the issuer, the financial institution that enters into the contractual relationship with the cardholder).
Issuer Application Data	Payment system defined application data for transmission from the chip card to the issuer in an online transaction.
J/Smart	JCB EMV-based ICC Specifications
Kernel	A piece of terminal application software that supports the EMV payment application functions as defined in the EMV specifications. The non-EMV functionality that supports functions like the printer and display, and building messages to send to the acquirer, is not considered part of the kernel.
M/Chip	MasterCard EMV-based ICC Specifications
Near Field Communication (NFC)	A short-range high frequency wireless communication technology which enables the exchange of data between devices over about a 10 centimeter distance. The technology is a simple extension of the ISO/IEC 14443 proximity-card standard (proximity card, RFID) that combines the interface of a smartcard and a reader into a single device.

Term	Description
Offline Data Authentication	A process whereby the card is validated at the point of transaction, using RSA public key technology to protect against counterfeit or skimming. Three forms of offline data authentication are defined by EMV: SDA, DDA and CDA.
Offline Enciphered PIN	A cardholder verification method defined in EMV in which the cardholder PIN is entered at a terminal, encrypted with an ICC public key, and sent to the ICC where it is decrypted and then validated.
Offline only terminal	A chip terminal that is not capable of sending an online authorization request and where all transactions have to be approved offline.
Offline PIN	A cardholder verification method where the card verifies a PIN that is entered by the cardholder; the PIN is stored in the card.
Offline Plaintext PIN	A cardholder verification method defined by EMV in which the cardholder PIN is entered at a terminal and sent to the ICC in plaintext to be validated.
Online capable terminal	A chip terminal that supports both offline and online processing.
Online PIN	A cardholder verification method where the PIN is sent securely from the terminal to the card issuer, or the card issuer’s designated agent, to be verified.
Payment Card Industry (PCI)	A consortium of the major payment schemes, Visa, MasterCard, American Express, JCB and Discover, which became formalized as the PCI Security Standards Council or PCI-SSC and which manages various aspects related to common industry security requirements.
Personal Identification Number (PIN)	A personal identification code that is known only to the cardholder and is entered into the terminal and sent to an authorizing entity for verification. The entity may be either the card issuer, or designated agent, or an ICC.
PIN Entry Device (PED)	A secure device that allows cardholders to enter a PIN.
Point of Sale (POS)	An attended or unattended terminal for the acceptance of payment cards for cash, goods and services.
Private Key	The secret component of an asymmetric key pair. The private key is always kept secret by its owner. It may be used to digitally sign messages for authentication purposes.
Public Key	The public component of an asymmetric key pair. The public key is usually publicly exposed and available to users. A certificate to prove its origin often accompanies it.
Public Key Certificate	An asymmetric transformation of the public key by a Certificate Authority and intended to prove to the public key recipient the origin and integrity of the public key.

Term	Description
Public Key Pair	The two mathematically related keys, a public key and a private key, which, when used with the appropriate public key algorithm, can allow the secure exchange of information and message authentication, without the secure exchange of a secret.
RSA	A public key cryptosystem developed by Rivest, Shamir, and Adleman. It is used for data encryption and authentication.
Skimming	The act of using a device to illegally collect data from the magnetic stripe or chip of a credit, debit or ATM card. This information, copied onto another blank card's magnetic stripe or chip, is then used to make purchases or withdraw cash in the name of the actual account holder.
Static Data Authentication (SDA)	A type of offline data authentication where the terminal validates a cryptographic value placed on the card during personalization. Protects against some types of counterfeit fraud but does not protect against skimming.
Symmetric Algorithm	An algorithm in which the key used for encryption is identical to the key used for decryption. DES is the best known symmetric encryption algorithm.
Terminal Risk Management (TRM)	Offline checks performed by the terminal to determine whether a transaction should proceed further. It includes floor limit checking and exception file checking.
Transaction Certificate (TC)	Cryptogram generated by the card at the end of either an online or offline approved transaction and can be used by the retailer or acquirer as proof that the card approved the transaction.
Triple Data Encryption Standard (TDES)	The data encryption standard used with a double-length DES key. Sometimes referred to as TDEA or DES3.
VIS	Visa EMV-based ICC Specification