A Guide to EMV Chip Technology

Version 2.0

November 2014

Table of Contents

List of Figures

1 Introduction

1.1 Purpose

The purpose of this paper is to provide an overview of the specifications and processes related to EMV chip products and transactions. The document is intended to describe the "what" and the "why" of EMV chip technology 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 various EMV Specifications.

The document was first published in 2011, and this current version (released in 2014) has been updated to focus on the EMV Chip Specifications, as well as reflect the growing ownership of EMVCo.

Information regarding other specifications published by EMVCo can be found at www.emvco.com.

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 4.3, November 2011* (EMVCo, LLC)
- *EMV Contactless Payment Specification For Payment Systems, version 2.4, February 2014* (EMVCo, LLC)
- Type Approval Process Documentation for terminals and cards available from EMVCo, LLC
- *Issuer and Application Security Guidelines, v2.4, April 2014* (EMVCo, LLC)

2 Background

2.1 What are the EMV Chip Specifications?

The EMV Chip Specifications that encompass both Contact and Contactless payments are global payment industry specifications that describe the requirements for interoperability between chip-based payment applications and acceptance terminals[1] 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 Chip Specifications were first published in 1996. Approaching twenty years later, there are now over two billion active EMV chip cards used for credit and debit payment, at over 35 million EMV acceptance terminals deployed around the world[2].

The distinguishing feature of EMV chip transactions is that the 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), a personal device such as a mobile phone or other form factors such as wristbands or watches. The secure chip provides three key elements:

- It can perform processing functions.
- It is able to store confidential information very securely.
- It can 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

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

[2] These figures were reported by EMVCo as of Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay and Visa as reported by their member financial institutions globally.

between the chip and the acceptance terminal. In both scenarios, the 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 Chip Technology?

The EMV Chip Specifications are designed to significantly improve the security for face-to-face payment transactions by providing features for ***reducing*** the fraud that result from ***counterfeit*** and ***lost and stolen*** cards.

The features that are defined within the EMV Chip Specifications that enable this 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 and offline transactions.

2. ***Risk management parameters*** to define the conditions under which the issuer will permit the transaction to be conducted offline and the conditions that force transactions online for authorisation, such as if offline limits have been exceeded.

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

4. More robust ***cardholder verification methods*** to protect against lost and stolen card fraud.

Counterfeit and lost and stolen 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 chip technology offers real benefits to retailers, acquirers, card issuers and cardholders.

Become involved in EMVCo

EMVCo can help deliver real benefits – for retailers, acquirers, card issuers and vendors to the payments industry.

Why not have a say in the ongoing development of the EMV Specifications?

Become an EMVCo Technical or Business Associate. For more information refer to the EMVCo website www.emvco.com.

3 The History of the EMV Chip Specifications

3.1 Timeline

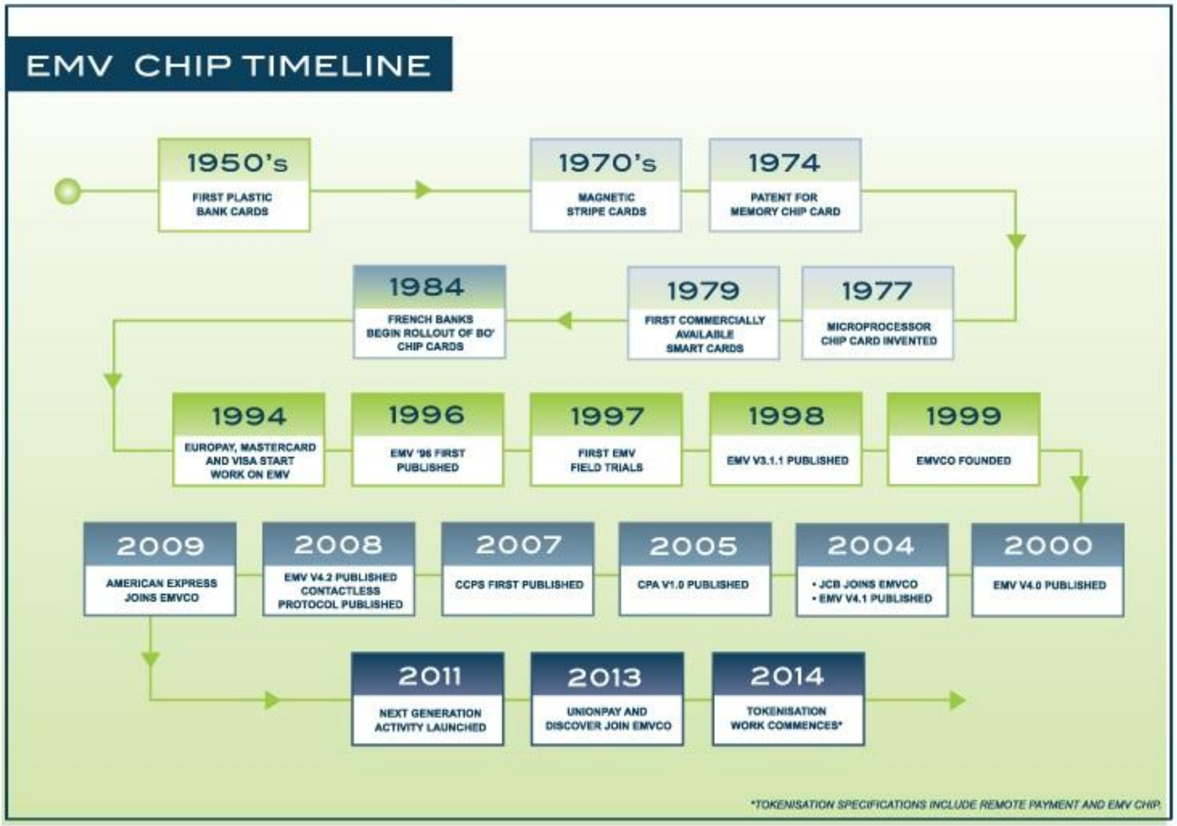

EMV CHIP TIMELINE
1950's
FIRST PLASTIC BANK CARDS
1970's
MAGNETIC STRIPE CARDS
1974
PATENT FOR MEMORY CHIP CARD
1977
MICROPROCESSOR CHIP CARD INVENTED
1979
FIRST COMMERCIALLY AVAILABLE SMART CARDS
1984
FRENCH BANKS BEGIN ROLLOUT OF BO' CHIP CARDS
1994
EUROPAY, MASTERCARD AND VISA START WORK ON EMV
1996
EMV '96 FIRST PUBLISHED
1997
FIRST EMV FIELD TRIALS
1998
EMV V3.1.1 PUBLISHED
1999
EMVCO FOUNDED
2000
EMV V4.0 PUBLISHED
2004
• JCB JOINS EMVCO
• EMV V4.1 PUBLISHED
2005
CPA V1.0 PUBLISHED
2007
CCPS FIRST PUBLISHED
2008
EMV V4.2 PUBLISHED CONTACTLESS PROTOCOL PUBLISHED
2009
AMERICAN EXPRESS JOINS EMVCO
2011
NEXT GENERATION ACTIVITY LAUNCHED
2013
UNIONPAY AND DISCOVER JOIN EMVCO
2014
TOKENISATION WORK COMMENCES*
*TOKENISATION SPECIFICATIONS INCLUDE REMOTE PAYMENT AND EMV CHIP.

Figure 1: EMV Chip Specifications Timeline

3.1.1 The Need for a Global Chip Card Standard

Chip cards have been with us for approximately forty years but have evolved considerably both in terms of functionality and security in that time. 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 Chip 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 Chip 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 over the years, with JCB joining in 2004, American Express in 2009, and both UnionPay and Discover in 2013.

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 Chip Specifications, version 3.1.1 was subsequently published in 1998.

The most recent version of the EMV Chip Specifications is version 4.3, published in 2011. Over the years since their initial publication the specifications have 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 Chip Specifications has been that each new release or version is always backwards compatible with prior releases. This helps protect the investment in the EMV chip infrastructure made by payment industry stakeholders.

3.1.3 Common Core Definitions

The EMV Chip 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 payment application specification[3] which requires an issuer to implement different card personalisation and host authorisation systems per 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 behaviours, 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 cards supporting one of the international payment systems' individual applications.

3.1.4 Extending EMV Chip Technology to Contactless and Mobile

The evolution of contactless chip has transpired in quite a different way when compared with the EMV Contact Chip Specifications. While the development of contact chip occurred collaboratively amongst payment industry organisations from the onset, contactless development has occurred in a competitive environment, with the individual payment systems developing their own specifications.

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 to reside in a single contactless terminal.

In addition to accepting EMV contactless chip cards, contactless terminals that are compliant with the EMV Contactless 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.

[3] International payment system EMV based card specifications include American Express AEIPS, Discover DPAS, JCB J/Smart, MasterCard M/Chip, UnionPay IC Card and Visa VIS.

3.2 EMV Chip around the World

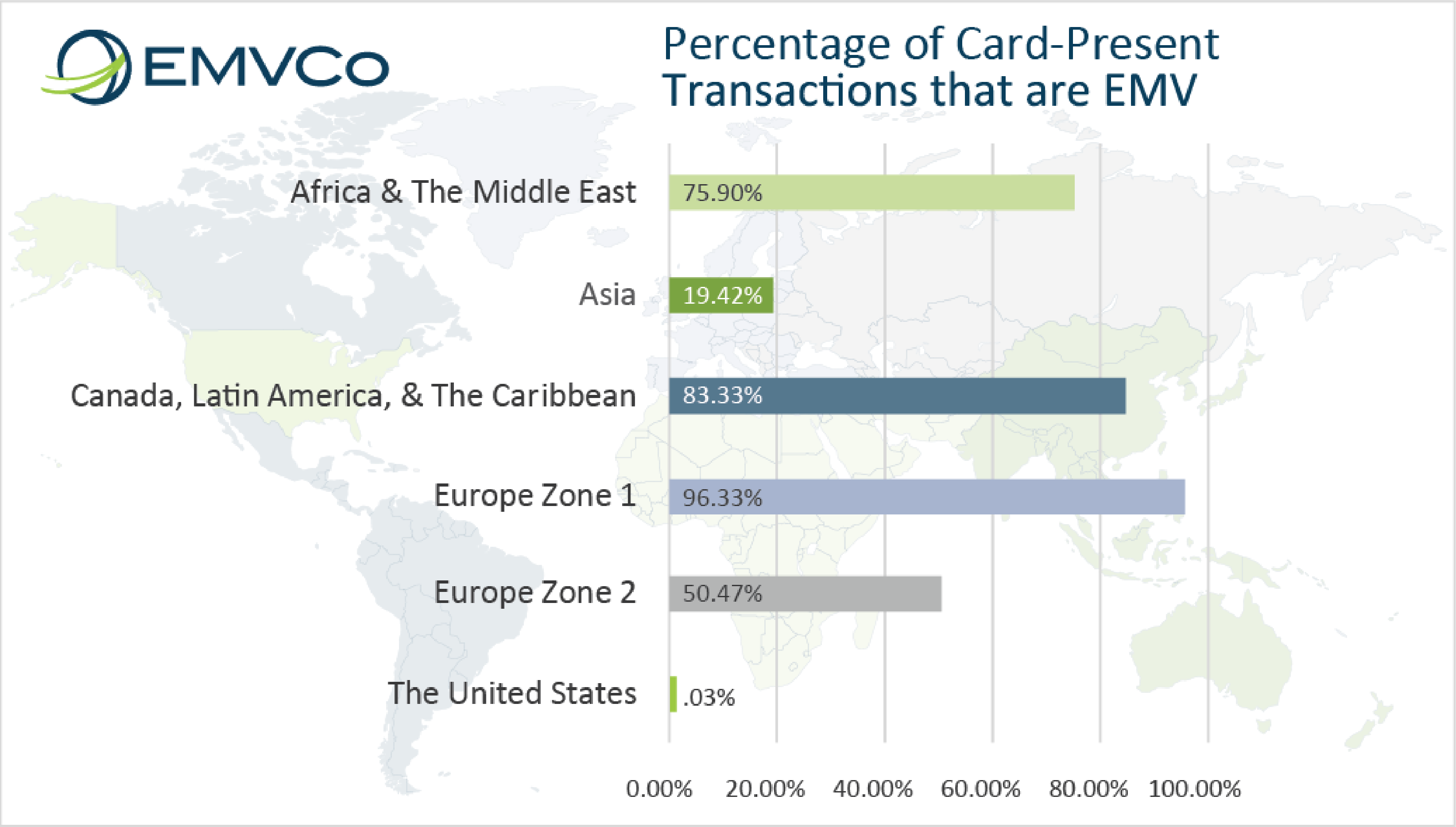
From the earliest field trials in 1997, to the progression of national migrations from magnetic stripe to EMV chip in various markets around the world, the EMV Chip Specifications are a global standard for chip payment, and they continue to grow in usage.

Today there are over two billion active EMV chip cards in circulation and over 35 million EMV acceptance terminals deployed around the world[4]. But, of course the real value proposition is the extent to which EMV transactions actually occur. Accordingly, in 2014 EMVCo transitioned to reporting EMV chip transaction percentages by region. The following diagram provides an overview of the percentage of card-present transactions that are EMV by major region.

Protect your investment in EMV infrastructure.
The EMV Chip 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 Chip Specifications. **Become an EMVCo Technical or Business Associate.** For more information refer to the EMVCo website www.emvco.com.

[4] These figures were reported by EMVCo as of Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay and Visa as reported by their member financial institutions globally.



Figures represent the percentage of all card-present transactions processed by each member institution that are EMV transactions (Contact or Contactless). The reported data is from the twelve months of July 2013 through June 2014 and represents the most accurate possible data that could be obtained by American Express, Discover, JCB, MasterCard, UnionPay, and Visa during this period. To qualify as an "EMV transaction" for the purpose of this methodology, both the card and terminal used during a transaction must be EMV-enabled. Data is reported from the acquirer perspective. These figures do not include offline transactions, "on us" transactions (defined as a transaction handled exclusively by another processor), and/or transactions processed by non-EMVCo-member institutions, such as local schemes.

Figure 2: Percentage of Card-Present Transactions that are EMV

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 Chip 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. In 2013 both UnionPay and Discover became joint owners, giving each payment brand an equal 1/6th ownership of EMVCo, LLC.

4.1 EMVCo Mission

The primary goal of EMVCo was initially to facilitate the interoperability of chip-based transactions. This was achieved through two primary activities:

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

In December 2013 the mission statement of EMVCo was revised to reflect its changing scope following the decision to develop specifications beyond those solely for chip based transactions. The original primary goals detailed above are reflected in the following, updated Mission Statement:

“To facilitate worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV Specifications and related testing processes.”

EMVCo Mission Statement December 2013

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.

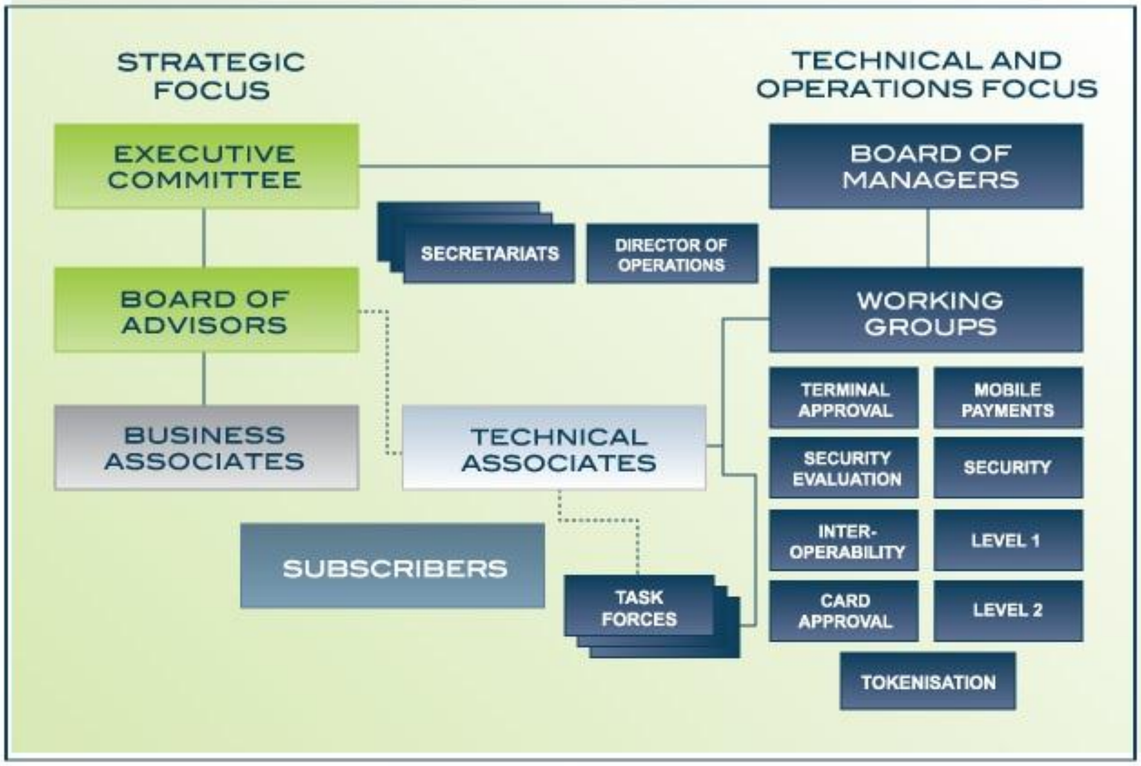


Figure 3: EMVCo Interaction Structure

American Express, Discover, JCB, MasterCard, UnionPay and Visa have appointed individuals to work at both management and Working Group levels within the EMVCo organisation. The Board of Managers, under guidance and direction of the Executive Committee, governs EMVCo. The Executive Committee, in turn, receives input from the EMVCo Advisors on business and strategic issues. The organisation has established several Working Groups, composed of representatives from its members, to carry out the work of EMVCo. The Board assigns work items, functions and responsibilities to the Working Groups as appropriate.

EMVCo maintains the EMVCo Associates Programme, 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. Each Business Associate may appoint an individual to serve on the Board of Advisors and, accordingly, advise the EMVCo Executive Committee.

Payment industry stakeholders 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 of the EMVCo Working Groups and receive updates or provide input on the Working Group activities and specifications. 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 Service, 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.

Eligibility, fee structures, and application details relating to participation in the Associates Programme and Subscriber Service can be found on the EMVCo website, www.emvco.com.

4.3 The Role of the Payment Systems in Contrast to EMVCo

EMVCo is the global technical body that facilitates the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV Chip Specifications and related testing processes. EMVCo does not define or issue products, and it 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. The Payment Systems 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 payment application specifications for their own respective branded chip card products; these define the options for card risk management processing and other features not defined by EMVCo. 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 Chip Specifications cannot be considered in isolation, and to this end, EMVCo collaborates with other industry bodies and standards organisations. Examples of this collaboration are given below.

1. **International Organisation for Standardisation (ISO)** - The EMV Chip 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 SSC)** is primarily concerned with the protection of sensitive payment information such as account information and personal identification numbers (PINs). The EMV Chip Specifications and PCI standards are complementary in enhancing payment security and reducing fraud due to counterfeit and lost and stolen cards.

3. **The Near Field Communication (NFC) Forum** – EMVCo has been working to extend EMV technology to the contactless and mobile channels. This has required 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 chip payment application will reside. Alignment with standards bodies such as GlobalPlatform are important as EMV chip payment applications are increasingly implemented on shared chip platforms that support multiple applications, each from a different application owner.

5 EMV Chip Technology – How it Works

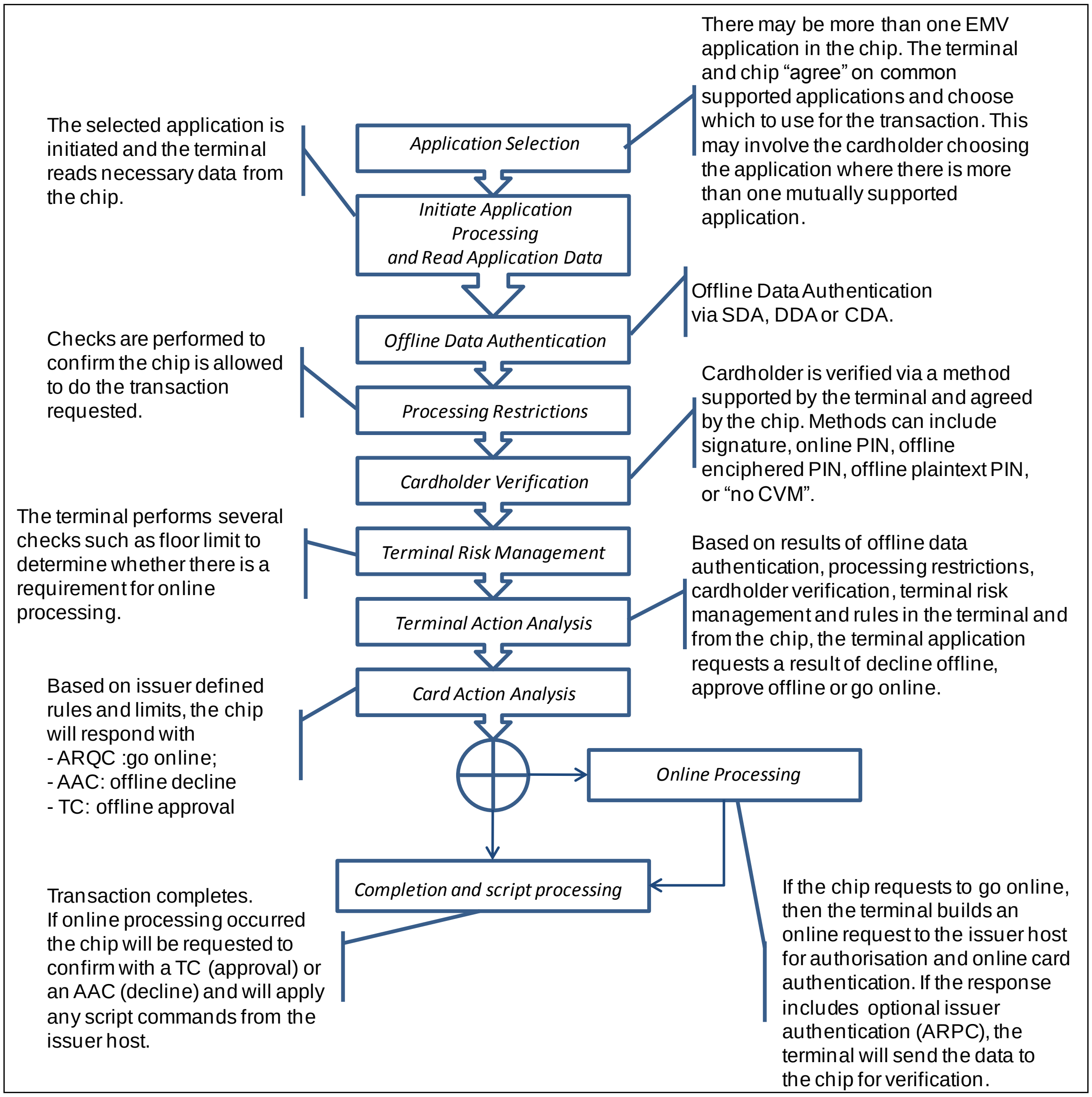
5.1 Stepping Through an EMV Chip Transaction

There is a fundamental difference between a magnetic stripe and an EMV chip transaction. For a magnetic stripe transaction, 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 in conjunction with the issuer and / or payment system and applies the rules for the transaction.

During an EMV transaction, the chip is capable of processing information and determines many of the rules that determine the outcome of the transaction. 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 chip transaction requires interaction between the chip and the terminal which is a protocol that is defined by the EMV Chip Specifications. The protocol defines a series of steps, which are described in the following sections.

5.1.1 Steps for an EMV Contact Transaction



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 Chip Transaction

5.1.2 Steps for an EMV Contactless Chip Transaction

The major difference between an EMV contactless chip transaction and an EMV contact chip 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 Chip Features

The specific features defined by EMVCo 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 chip 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.

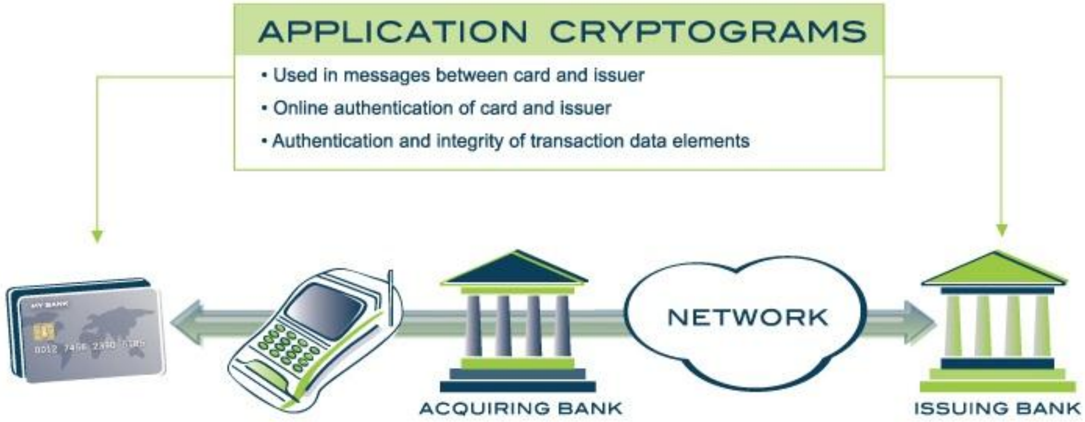

APPLICATION CRYPTOGRAMS
• Used in messages between card and issuer
• Online authentication of card and issuer
• Authentication and integrity of transaction data elements
MY BANK
NETWORK
ACQUIRING BANK
ISSUING BANK

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 chip 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 chip transactions provide 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.

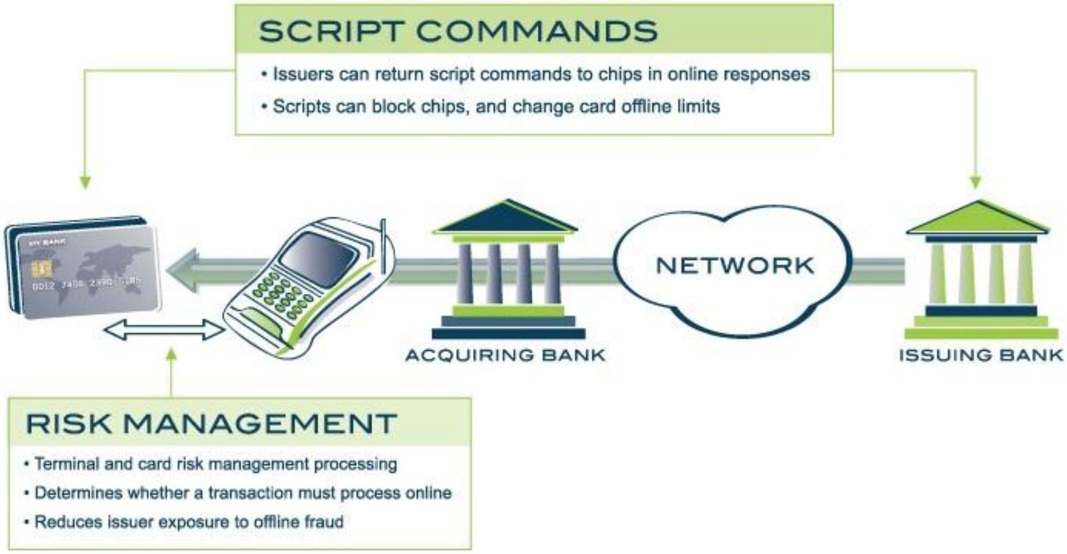

SCRIPT COMMANDS
• Issuers can return script commands to chips in online responses
• Scripts can block chips, and change card offline limits
NETWORK
ACQUIRING BANK
ISSUING BANK
RISK MANAGEMENT
• Terminal and card risk management processing
• Determines whether a transaction must process online
• Reduces 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, the EMV Chip Specifications provide 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, the EMV Chip Specifications define 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.

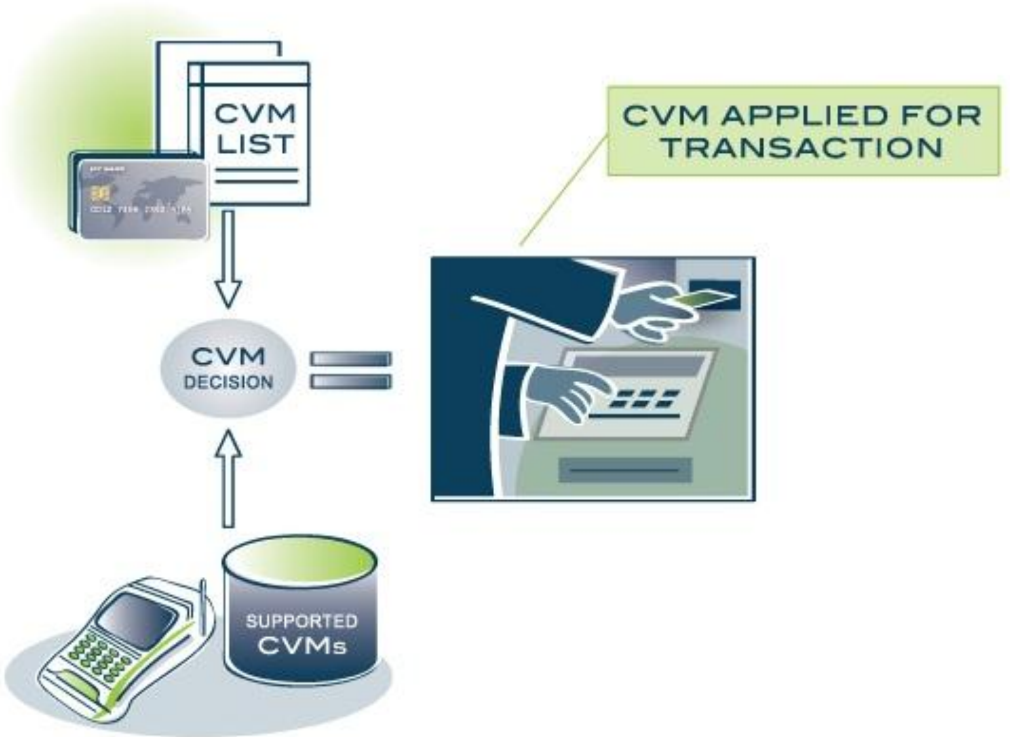


Figure 7: Cardholder Verification Processing

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 in the EMV Chip Specifications: 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 Offline Data Authentication

The EMV Chip Specifications describe 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.

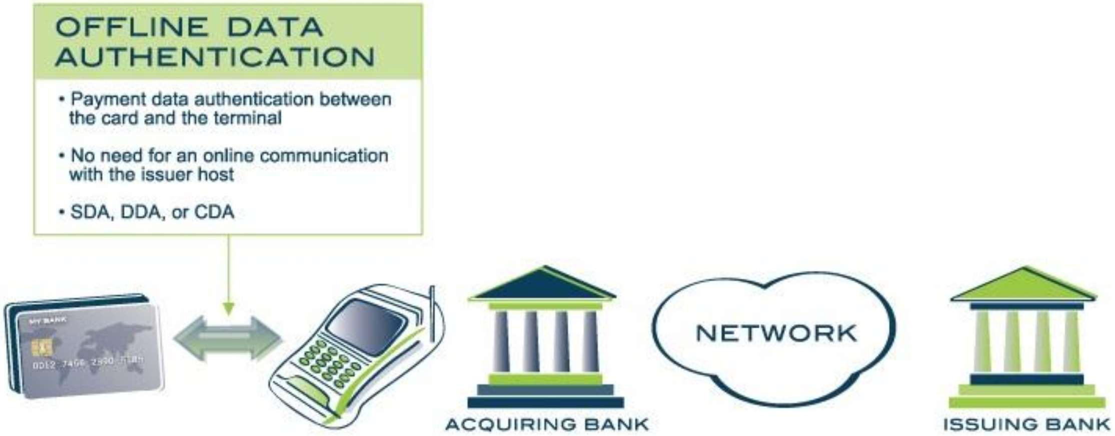

OFFLINE DATA AUTHENTICATION
• Payment data authentication between the card and the terminal
• No need for an online communication with the issuer host
• SDA, DDA, or CDA
NETWORK
ACQUIRING BANK
ISSUING BANK

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 chip transaction must go online for authorisation.

The essential difference between SDA and DDA is that while SDA indicates that the data read from the chip has not been manipulated or changed since it was issued, SDA does not necessarily mean that the card is genuine. 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 offline SDA at the point of sale. It should be noted that any counterfeit card could be detected during online processing.

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 by performing offline dynamic authentication using data from the terminal sent uniquely for each transaction. DDA is therefore a stronger form of offline data authentication than SDA because DDA indicates that the card has been authenticated offline using unique transaction specific data.

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. Individual payment systems may mandate the use of specific offline data authentication methods in particular regions.

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, it is possible that the chip would not require offline data authentication support at all as determined by individual payment systems.

6 Testing and Approval

6.1 EMVCo Objective

In addition to maintaining and evolving the EMV Chip Specifications, the other key and complementary EMVCo role is to assess the compliance of vendor products developed to these 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 Chip 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 chip enabled acceptance terminals sufficiently conforms to the functional requirements defined in the EMV Chip Specifications. 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 Chip Specifications. EMVCo defines the kernel as the terminal application software that supports the EMV payment application functions as defined in the EMV Chip 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 EMV Chip 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.[5]

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 chip 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 systems.

[5] International payment system EMV-based card specifications include American Express AEIPS, Discover DPAS, JCB J/Smart, MasterCard M/Chip, UnionPay IC Card and Visa VIS.

7 Implementation Considerations

The migration from magnetic stripe to EMV chip 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.

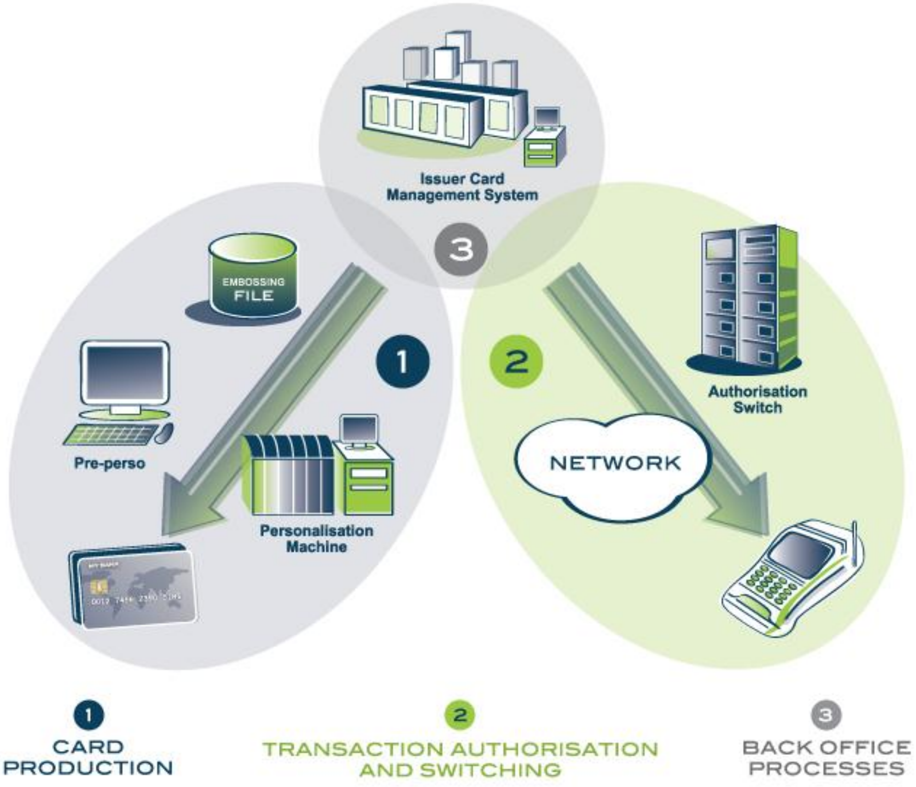


Figure 9: Issuer EMV Implementation Activities

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 the required cryptographic processing.
	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.

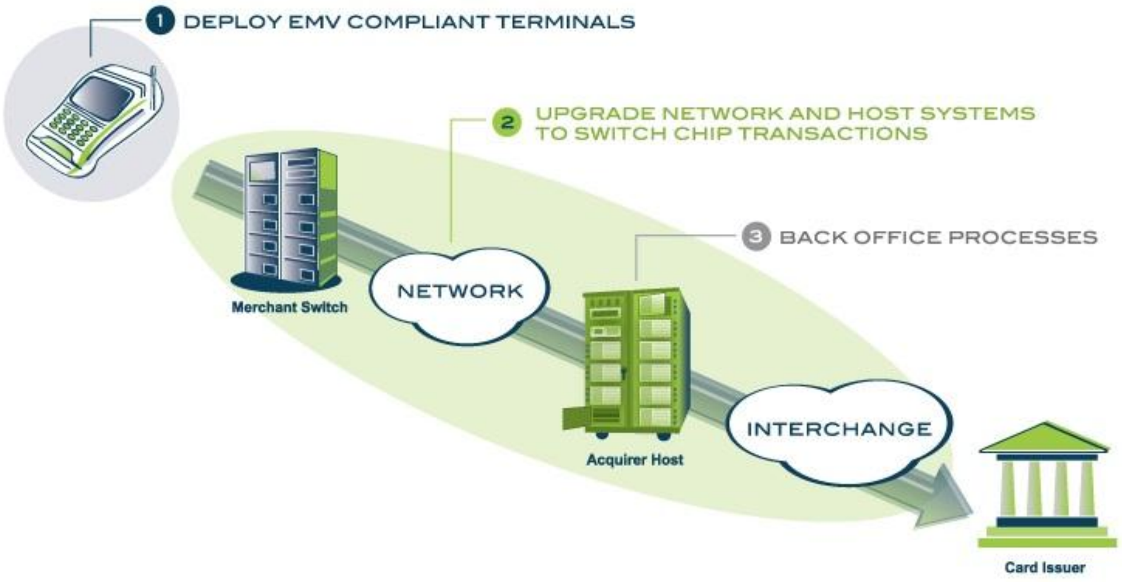

1 DEPLOY EMV COMPLIANT TERMINALS
2 UPGRADE NETWORK AND HOST SYSTEMS TO SWITCH CHIP TRANSACTIONS
3 BACK OFFICE PROCESSES
Merchant Switch
NETWORK
Acquirer Host
INTERCHANGE
Card Issuer

Figure 11: EMV Acceptor Implementation Activities

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

Activity	Description
Deploy EMV chip 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 chip 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 chip 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 Next Generation of EMV Chip Specifications

Many changes have occurred in the payments industry since the initial publication of the EMV Chip Specifications. Specifically, EMVCo has recognised the following:

- Continuous expansion of business requirements and payment technologies (e.g. mobile).
- Convergence of contact and contactless solutions needs to be simplified across the entire payments ecosystem.
- Evolution of public key cryptography (e.g. Elliptic Curve Cryptography).
- Increased requirement to transport additional ‘value add’ data across the networks.

These developments have impelled EMVCo to review the EMV Chip Specifications through a strategic lens and evaluate a roadmap for the future of payments. It formed the Next Generation Task Force which is tasked with designing the solution and leading the development of the next generation of EMV Chip Specifications.

8.1 Business Drivers

There are many reasons why EMVCo’s work in the development of the next generation of EMV Chip Specifications is important. Some of the key business drivers include:

- *Product Time to Market* – Enable a more cost and time efficient deployment of current, future payments
- *Terminal evolution -* Reduce impact on terminal infrastructure as product requirements evolve
- *POS Throughput* – Provide options for improving throughput at the point-of-sale
- *Transaction Quality* – Improve transaction data quality and relevance
- *Transaction and Business Environments* – Address different types of transactions and various business environments
- *Product Selection* – Improve the product selection for the cardholder and merchant
- *Security* – Future-proof EMV security including incorporating ECC and mitigate privacy-related issues

8.2 EMV Next Generation Specifications

The EMV Next Generation (Next Gen) Specifications establishes a common, robust technology platform to support a variety of interfaces—contact, contactless, mobile, etc.—for both online and offline processing, by:

- Enhancing transaction information available to acquirers, networks, and issuers
- Optimising transaction flows to improve throughput at the point of sale and the cardholder experience
- Future proofing EMV chip security by incorporating next generation public key infrastructure and a secure channel between the card and acceptance device
- Supporting multiple communication protocols, with the flexibility to add additional protocols in the future
- Integrating Type Approval processes for contact and contactless

Special attention is given to migration and global interoperability between existing legacy EMV chip products and EMV Next Gen products. It is expected that cards and acceptance devices based on legacy EMV Chip Specifications might remain in the field until 2030.

The coexistence of legacy EMV chip and Next Gen applications (on the card's side) and legacy EMV chip and Next Gen Kernels (on the acceptance device side) facilitates the introduction of new features in response to individual market needs, while providing a natural migration path. Individual payment systems and markets will determine when Next Gen products become relevant for their needs, and may begin migrations well before 2030.

To minimize deployment costs and disruption in the field and to avoid multiple overlapping migrations—especially those that would require changes to acceptance devices and Type Approval testing—EMV Next Gen leverages recent evolutions in smart card, acceptance device, and network technology; incorporating into the Next Generation Kernel System Specifications all the enhancements foreseen to keep EMV chip technology relevant for the next 20+ years. EMV Next Gen is designed so that the overall payment functionality and the cardholder experience should not be impacted by whether Next Gen or legacy EMV chip functionality is used for a particular transaction.

8.3 Milestones

EMVCo continues to progress EMV Next Gen by achieving the following milestones:

2011	Start the EMV Next Generation effort
2012	EMVCo Next Generation scope finalisation
2013	EMV Next Generation high-level architecture completed
2014	EMV Next Generation proof of concept
2015	EMV Next Generation Draft Specification projected
2016	EMV Next Generation Specification projected
2017	Terminal Type Approval Process availability projected
2025	Payment systems may sunset the issuance of legacy contact/contactless cards
2030	Payment systems may remove legacy cryptography (i.e. keys) from terminals
	The timeline and milestones presented are provisional and subject to change

Help shape the future of EMV Technology
EMV is continuing to evolve into new channels such as mobile as well as developing the Next Generation of the EMV Chip Specifications

Will your business provide input into these new and exciting developments? **Become an EMVCo Associate**. For more information please 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 behaviours, 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 behaviours.
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.
DPAS	D Payment Application Specification – The Discover and Diners Club International EMV-based ICC Specifications.
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 Chip 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

Term	Description
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.
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.

Term	**Description**
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.
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