A Guide to EMV

Version 1.0
May 2011
Objective

- Provide an overview of the EMV specifications and processes
  - What is EMV?
  - Why EMV?

- Position EMV in the context of the wider payments industry

- Define the role of EMVCo

- Describe the interaction of various payment industry stakeholders with EMVCo
• What is EMV?
• Why EMV?
• History
• EMV global deployment and adoption
• EMVCo LLC
• EMV – how it works
• EMV testing and approval
• Implementation considerations
• The future
What is EMV?

• EMV Integrated Circuit Card Specifications for Payment Systems

• Developed jointly by Europay, MasterCard and Visa in the mid-1990s

• Open specifications to facilitate interoperability between chip cards and terminals for credit and debit payment
  – Assuming the business rules and agreements are in place, all cards accepted in all devices irrespective of the card issuer, the terminal acquirer, the manufacturers of the card or terminal
What is EMV?
What is EMV?

- Consumer payment application is resident in a secure Integrated Circuit Card (ICC) or chip
  - Contact chips in smart cards
  - Contactless chips in smart cards or personal devices such as smart phones

- Chip key features
  - Store information
  - Perform processing
  - Secure element which stores secrets and performs cryptographic functions
Why EMV?

• Protect against counterfeit fraud through authentication of the chip card, smart phone, fob etc

• Risk management parameters to reduce the risk of unauthorised payment

• Validate the integrity of the transaction through digitally signing payment data

• Reduce lost and stolen cards through robust cardholder verification methods in all acceptance environments
Early Chip Card Milestones

1950’s
- First plastic bankcards

1970’s
- Magnetic stripe cards
- First commercially available smart cards

1974
- Patent for memory chip card
- Microprocessor chip card invented

1979

1984
- French banks begin rollout of B0’ chip cards
The Need for a Global Chip Standard

• The success of the French migration to chip spawned numerous domestic proprietary implementations in Europe

• Chip provided protection for domestic transactions but magnetic stripe was still required for global interoperability

• In 1994, Europay, MasterCard, and Visa began developing a global chip specification for payment systems

• JCB joined in 2004, and American Express in 2009
CCD and CPA

EMV defined Common Core Definitions

Defined by EMV

EMV defined minimum chip data

Acquiring Bank

Network

Issuing Bank
Extending EMV to Contactless and NFC Mobile

EMV Contactless
Level 2

Entry Point Specification

Contactless Communication
Protocol Specification

Payment System
Contactless Applications

EMV Contactless
Level 1
EMV Worldwide Deployment and Adoption

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.
EMVCo LLC

• Created as a limited liability company in 1999 by Europay, MasterCard and Visa

• JCB joined in 2004, and American Express joined in 2009, as owners

• Objectives of EMVCo LLC
  – Own and manage the EMV specifications
  – Maintain and further develop the EMV specifications
  – Manage the type approval processes for terminals
  – Manage the security evaluation process for all EMV chip cards
  – Manage the type approval process for chip cards compliant with CCD and CPA
EMVCo Management and Operation Structure

Business Focus
- Executive Committee
- Board of Advisors
- Business Associates
- Technical Associates
- Subscribers

Technical and Operations Focus
- Secretariats
- Board of Managers
- Working Groups
  - Terminal Approval
  - Mobile Payments
  - Security Evaluation
  - Contactless
  - Interoperability
  - Security
  - Card Approval
  - Card and Terminal

* As of 2011
EMVCo LLC and the Payment Systems

Payment Systems
- Define EMV products
- Define the business rules for the issuing and acceptance of EMV products
- Define the parameters and EMV features that must be deployed
- Enforce EMV compliance in the field
- Maintain and publish payment system card specifications
- Support EMV implementations

EMVCo
- Own and manage the EMV specifications
- Maintain and further develop the EMV specifications
- Manage the type approval processes for terminals
- Manage the security evaluation process for all EMV chip cards
- Manage the type approval process for chip cards compliant with CCD and CPA
EMVCo LLC and other Standards Bodies

- ISO
  - ISO/IEC 7816
  - ISO/IEC 14443

- PCI
  - PCI PTS
  - Payment security

- GlobalPlatform
  - Chip platforms standards
  - Chip security
  - Personalisation
  - Multi-application

- NFC Forum
  - Specifications for NFC devices and services
Stepping Through an EMV 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 card.

Checks are performed to confirm the chip is allowed to do the transaction requested.

The terminal performs several checks such as floor limit to determine whether there is a requirement for online processing.

Offline Data Authentication via SDA, DDA or CDA.

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”.

Terminal Risk Management
Stepping Through an EMV Transaction

Terminal Risk Management

Terminal Action Analysis

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.

Card Action Analysis

Online Processing

Based on issuer defined rules and limits, the card will respond with:
- ARQC: go online;
- AAC: offline decline
- TC: offline approval

Completion and script processing

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.

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.
Differences between EMV contact and contactless transactions

- The goal for contactless is to minimise the amount of time that the card must be held within proximity of the reader.
- Contact requires the card to remain in contact with the reader for the duration of the transaction.

For contactless:

- Transmission of information between the card and terminal is faster.
- Some steps may be performed after the card has left the proximity of the reader:
  - e.g.: online authorisation.
EMV – How it Works

• EMV Features
  – Application Cryptogram
  – Risk Management and Authorisation Controls
  – Cardholder Verification Processing
  – EMV Offline Data Authentication
    • SDA
    • DDA
    • CDA
Application Cryptograms

• The card generates an EMV Application Cryptogram (AC) at key transaction points

  – To indicate if online authorisation is required
    • Authorisation ReQuest Cryptogram (ARQC)

  – At transaction completion
    • Transaction Certificate (TC) for an approval
    • Application Authentication Cryptogram (AAC) for a decline
Application Cryptograms

• Application Cryptograms are signatures created with a card unique DES key composed of critical data elements that indicate the status at the transaction point

• Online authentication of card and issuer
  – ARQC sent in online authorisation request to the issuer.
    • Issuer host validation of the ARQC confirms that the chip has not been copied or changed
  – Optionally in an online authorisation response from the issuer
    • Authorisation ResPonse Cryptogram (ARPC)
    • Chip card validation of the ARPC confirms approval response from the issuer and is typically used to allow the card to reset counters

• Signing transaction data for message authentication and integrity
  – Alteration of AC key elements will fail validation of the signatures
Risk Management and Authorisation Controls

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
Risk Management and Authorisation Controls

• Risk management features under acquirer control to select transactions for online approval
  – Floor limits
  – Domestic or retailer criteria
  – Random transaction selection

• Together with issuer chip card controls, protect against the use of lost and stolen or counterfeit cards which attempt to stay beneath the floor limit
Cardholder Verification Processing

- EMV introduces new features for cardholder verification
  - Cardholder verification method list
    - Issuer can define multiple CVMs in the card and define the conditions under which the CVM must be applied
  - Offline PIN
    - Offline Plaintext PIN
    - Offline Enciphered PIN
- EMV still supports traditional methods
  - Online enciphered PIN, signature, “no CVM”
Cardholder Verification Processing

CVM LIST

CVM applied for the transaction

Supported CVMs
Offline Data Authentication

• Methods of offline authentication available
  – SDA - Static Data Authentication
  – DDA - Dynamic Data Authentication
  – CDA - Combined Data Authentication

• Method supported is chosen by the issuer depending upon card capability

• Only one method of off-line data authentication performed during a transaction
Static Data Authentication (SDA)

- Indicates that the signed data on the chip has not been changed or manipulated
  - Cards **DO NOT** require RSA cryptographic processing capability
  - Each card is personalised with the Issuer public key certificate and *static signed application data*
  - *Static signed application data* is composed of data elements personalised onto the card and signed with issuer private key
  - Terminal performs RSA cryptographic processing using issuer public key to authenticate *signed static application data*
  - *Does NOT* indicate that card is authenticated offline
Dynamic Data Authentication (DDA)

- **Indicates that the actual card issued is present at the point of sale**
  - Cards *DO* require RSA cryptographic processing capability

  - Each card is personalised with the issuer public key certificate, card public key certificate and card private key

  - Card generates unique *signed dynamic application data* per transaction by signing data elements from both the card and terminal with the card private key

  - Terminal performs RSA cryptographic processing using card public key to authenticate *signed dynamic application data*

  - *DOES* indicate that the card is authenticated offline
Combined Data Authentication (CDA)

- Dynamic Data Authentication with Application Cryptogram generation (CDA)
  - The same personalisation requirements as DDA with an additional step during “card analysis”

- Cards **DO** require RSA cryptographic processing capability

- Card generates a “dynamic signature” using card private key, in addition to the “application cryptogram”, to prove that the card authenticated during DDA was the same card that provided the “application cryptogram”

- Assists in the detection of an attempted "man-in-the-middle" attack where the fraudster alters data between card and terminal to try to keep the card offline
EMV Testing and Approval

• EMVCo maintains a testing and approval process to assess whether chip cards and chip accepting terminals comply with the EMV specifications
  – Documented administrative process
  – Definition and implementation of test plans
  – Qualification process for test tools
  – Ongoing monitoring and improvement
  – Published list of approved products
  – Vendor contractual process with letter of approval

• Testing is performed by EMVCo accredited test laboratories
  – EMVCo managed laboratory accreditation process
Terminal Approval

- Defined and administered by the EMVCo TAWG

- EMV Level 1 Terminal Type Approval
  - Designed to verify whether the terminal chip reader sufficiently conforms to Level 1 of the EMV specifications
    - Transfer of data between card and terminal and electromechanical properties

- EMV Level 2 Terminal Type Approval
  - Designed to verify whether the terminal software, known as the EMV Level 2 kernel sufficiently conforms to the EMV specifications
    - EMV payment application functions
    - Non-EMV application functions such as printer, display, building messages to the acquirer host are not considered part of the kernel
Card Approval

• Card Type Approval
  – Process is designed to assess whether the chip hardware and embedded EMV functionality sufficiently conforms to the EMV electro-mechanical and functional requirements
  – Payment Systems perform card type approval for chip applications that comply with their own specifications
  – EMVCo manages the process for CCD and CPA compliant cards

• Chip Security Evaluation
  – EMV functionality and benefits rely on a chip capable of securely storing information such as cryptographic keys and cardholder PINs
  – Process is designed to assess whether chips demonstrate a certain minimum level of security designed to withstand known attacks
  – Results are used by each payment system in their card approval process
1. Card production

2. Transaction authorisation & switching

3. Back office processes

Issuer Card Management System

Embossing File

Pre-perso

Personalisation Machine

Network

Authorisation Switch
Acquirer Implementation Considerations

1. Deploy EMV compliant terminals

2. Upgrade network and host systems to switch chip transactions

3. Back office processes
The Future

• EMVCo’s vision is for all payments through any payment channel, both now and in the future, to be able to benefit from the security features provided by EMV

• Contactless roadmap
  – A combined EMV contactless kernel specification and a single approval process for all contactless readers
  – Ultimately a single EMVCo developed common contactless kernel for all Payment Systems in the one reader

• Enhancing the EMV security and key management architecture
  – Adding Elliptic Curve Cryptography (ECC) for offline cryptographic processing
  – ECC delivers faster processing with smaller keys
The Future

• Mobile
  – Contactless has allowed the delivery of form factors beyond chips embedded in plastic cards
  – EMVCo collaborating with other industry groups to define standards for EMV contactless mobile payment
    • NFC Forum
    • GSM Association
    • GlobalPlatform
  – Work in progress
    • Defining the architecture for EMV contactless mobile payment
    • Handset requirements
    • Customer user interface requirements
    • EMV payment application secure element requirements
Thank you