EMV 101

EMV Migration Forum Webinar
May 7, 2014
Introduction

Cathy Medich
Director, Programs - EMV Migration Forum
About the EMV Migration Forum

Cross-industry body focused on supporting the EMV implementation steps required for global and regional payment networks, issuers, processors, merchants, and consumers to help ensure a successful introduction of more secure EMV chip technology in the United States.

Forum focus: address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States.
Today’s Webinar Topics & Speakers

• **Introduction & EMV Implementation Status:** Cathy Medich, Director - Programs, EMV Migration Forum

• **EMV 101:** Guy Berg, Senior Managing Consultant, MasterCard Advisors

• **Q&A**
Global EMV Adoption*: 2.37 Billion Cards and 36.9 Million EMV Terminals

* Excluding U.S.
Source: EMVCo, as of Q4 2013

Contact EMV Global Adoption*

*Figures reported as of Q4 2013 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. Figures are reported by region and do not imply country-by-country statistics.
U.S. Migration Progress

• Acquirers met 2013 readiness for EMV readiness and are deploying EMV to their merchants as part of the normal upgrade path
• Millions of EMV chip payment cards are in the marketplace from a broad set of issuers
• Merchants are investing in hardware upgrades to accept the payments
• ATM providers are actively deploying EMV-enabled ATMs
• EMV Migration Forum is active in working on issues requiring cooperation to help smooth the migration to EMV for the U.S. payments industry
EMV Fundamentals

I. EMV Payment Transaction Framework
II. Transaction Processing Comparison
   ➢ Magnetic Stripe vs. EMV Transaction Security Points
   ➢ Data Compromise and Skimming Protection Mechanisms

III. EMV Application Fundamentals
   ➢ On-line Card Authentication
   ➢ Off-line Card Authentication
   ➢ Offline Authorization
   ➢ Risk Management
   ➢ Cardholder Verification Method

IV. EMV from a Terminal Perspective
   ➢ Terminal Application and Approvals

V. EMV Debit Support
EMV migration impacts all stakeholders involved in payment transaction processing

- New card data
- New messaging data
- New application logic
- New configuration settings

Issuer

Acquirer

Terminal

Card / Device

EMV Messaging

Contactless

NFC

EMV
Magnetic Stripe Transactions use static authentication data that can be skimmed.

1) Magnetic stripe is easily cloned

2) Terminal performs little or no risk assessment relative to the magnetic stripe

3) Authorization message
   - Track data is often in the clear
   - The authentication data is static

4) Authorization/Authentication
   - Risk assessment performed at the host
   - Host uses static data to perform counterfeit cards
EMV Transaction Processing Introduces dynamic authentication that makes copied data useless at POS

(1) EMV Chip application performs risk assessment

(2) Terminal performs risk assessment

(3) New EMV authentication data

(4) New Issuer Authorization Functions
  - Dynamic cryptogram validation
  - May return an authentication cryptogram
  - Post issuance updates
The AID provides a method for the terminal to recognize what applications exist on a chip card.

So what is an AID?

- **AID**
  - An Identifier that must be registered with ISO
  - Identifies an application owner
  - Identifies technical application logic required for operation
  - Can be specific product offerings

Payment Network (Application owner) **Operating rules** are linked to AIDs.

Role of the AID:
- Provides a way for the chip to tell the terminal what applications reside on it
- Provides the terminal a method to identify if it supports an application on a chip

So what is an AID?
- Can be specific product offerings
  - MasterCard
  - EMV Application (M/Chip)
  - MasterCard Maestro
The terminal and card each maintain a list of AIDs that they support

The terminal keeps a list of AIDs that it can support

An Issuer loads applications and corresponding AIDs to the chip

Application Selection Process

List of AIDs supported by the terminal

<table>
<thead>
<tr>
<th>AID Description</th>
<th>AID Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC Debit/Credit AID</td>
<td>A0000000041010</td>
</tr>
<tr>
<td>MC U.S. Maestro Common AID</td>
<td>A0000000042203</td>
</tr>
<tr>
<td>Visa</td>
<td>A0000000031010</td>
</tr>
<tr>
<td>Visa U.S. Common AID</td>
<td>A00000000980840</td>
</tr>
<tr>
<td>Discover AID</td>
<td>A00000003241010</td>
</tr>
</tbody>
</table>

Logic and configuration data specific to each AID must be added to the terminal
<table>
<thead>
<tr>
<th>EMV Tag</th>
<th>Chip Data</th>
<th>EMV Tag</th>
<th>Chip Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>Issuer Identification Number (IIN)</td>
<td>9F 07</td>
<td>Application Usage Control</td>
</tr>
<tr>
<td>4F</td>
<td>Application Dedicated File (ADF) Name</td>
<td>9F 08</td>
<td>Application Version Number (CARD)</td>
</tr>
<tr>
<td>50</td>
<td>Application Label</td>
<td>9F 0B</td>
<td>Cardholder Name Extended</td>
</tr>
<tr>
<td>57</td>
<td>Track2 Equivalent Data</td>
<td>9F 0D</td>
<td>Issuer Action Code (IAC) - Default</td>
</tr>
<tr>
<td>5A</td>
<td>Application Primary Account Number (PAN)</td>
<td>9F 0E</td>
<td>Issuer Action Code (IAC) – Denial</td>
</tr>
<tr>
<td>5F 20</td>
<td>Cardholder Name</td>
<td>9F 0F</td>
<td>Issuer Action Code (IAC) – Online</td>
</tr>
<tr>
<td>5F 24</td>
<td>Application Expiration Date</td>
<td>9F 11</td>
<td>Issuer Code Table Index</td>
</tr>
<tr>
<td>5F 25</td>
<td>Application Effective Date</td>
<td>9F 12</td>
<td>Application Preferred Name</td>
</tr>
<tr>
<td>5F 28</td>
<td>Issuer Country Code</td>
<td>9F 1F</td>
<td>Track1 Discretionary Data</td>
</tr>
<tr>
<td>5F 2D</td>
<td>Language Preference</td>
<td>9F 20</td>
<td>Track2 Discretionary Data</td>
</tr>
<tr>
<td>5F 30</td>
<td>Service Code</td>
<td>9F 2D</td>
<td>ICC PIN Encipherment Public Key Certificate</td>
</tr>
<tr>
<td>5F 34</td>
<td>Application PAN Sequence Number</td>
<td>9F 2E</td>
<td>ICC PIN Encipherment Public Key Exponent</td>
</tr>
<tr>
<td>5F 50</td>
<td>Issuer URL</td>
<td>9F 2F</td>
<td>ICC PIN Encipherment Public Key Remainder</td>
</tr>
<tr>
<td>5F 53</td>
<td>International Bank Account Number (IBAN)</td>
<td>9F 32</td>
<td>Issuer Public Key Exponent</td>
</tr>
<tr>
<td>5F 54</td>
<td>Bank Identifier Code (BIC)</td>
<td>9F 3B</td>
<td>Processing Options Data Object List (PDOL)</td>
</tr>
<tr>
<td>5F 55</td>
<td>Issuer Country Code (Alpha2 Format)</td>
<td>9F 38</td>
<td>Application Reference Currency</td>
</tr>
<tr>
<td>5F 56</td>
<td>Issuer Country Code (Alpha3 Format)</td>
<td>9F 42</td>
<td>Application Currency Code</td>
</tr>
<tr>
<td>82</td>
<td>Application Interchange Profile (AIP)</td>
<td>9F 43</td>
<td>Application Reference Currency Exponent</td>
</tr>
<tr>
<td>84</td>
<td>Dedicated File (DF) Name</td>
<td>9F 44</td>
<td>Application Currency Exponent</td>
</tr>
<tr>
<td>87</td>
<td>Application Priority Indicator</td>
<td>9F 45</td>
<td>Data Authentication Code (DAC)</td>
</tr>
<tr>
<td>88</td>
<td>Short File Identifier</td>
<td>9F 46</td>
<td>ICC Public Key Certificate</td>
</tr>
<tr>
<td>8C</td>
<td>Card Risk Management Data Object List (CDOL) 1</td>
<td>9F 47</td>
<td>ICC Public Key Exponent</td>
</tr>
<tr>
<td>8D</td>
<td>Card Risk Management Data Object List (CDOL) 2</td>
<td>9F 48</td>
<td>ICC Public Key Remainder</td>
</tr>
<tr>
<td>8E</td>
<td>Cardholder Verification Method (CVM) List</td>
<td>9F 49</td>
<td>Dynamic Data Object List (DDOL)</td>
</tr>
<tr>
<td>8F</td>
<td>Certificate Authority (CA) Public Key Index</td>
<td>9F 4A</td>
<td>Static Data Authentication (SDA) Tag List</td>
</tr>
<tr>
<td>90</td>
<td>Issuer Public Key Certificate (IPKC)</td>
<td>9F 4B</td>
<td>Signed Dynamic Application Data</td>
</tr>
<tr>
<td>92</td>
<td>Issuer Public Key Remainder</td>
<td>9F 4D</td>
<td>Log Entry</td>
</tr>
<tr>
<td>93</td>
<td>Signed Static Application Data</td>
<td>Key</td>
<td>MDK&lt;sub&gt;AC&lt;/sub&gt;</td>
</tr>
<tr>
<td>94</td>
<td>Application File Locator (AFL)</td>
<td>Key</td>
<td>MDK&lt;sub&gt;SMI&lt;/sub&gt;</td>
</tr>
<tr>
<td>97</td>
<td>Transaction Certificate Data Object List (TDOL)</td>
<td>Key</td>
<td>MDK&lt;sub&gt;SMC&lt;/sub&gt;</td>
</tr>
<tr>
<td>9F 05</td>
<td>Application Discretionary Data</td>
<td>Key</td>
<td>MDK&lt;sub&gt;IDN&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key</td>
<td>MDK&lt;sub&gt;CVC3&lt;/sub&gt;</td>
</tr>
</tbody>
</table>
EMV and non EMV security mechanisms combine to provide skimming and data compromise protection.

Multiple protection mechanisms are used in concert to combat card skimming, counterfeit card production and data compromise threats.

- CVC 1 and CVV 1
- CVC 2 and CVV 2
- Chip CVC
- EMV ARQC
- Chip Service Code
Chip security provides both card stock security and transaction security.

### Pre-issuance Security

- EMV Card Configuration Data
- Issuance Security

### Transaction Security

#### EMV Application

- Risk Management Decision Criteria
  - Online Security Functions
    - Symmetric Keys
  - Offline Security Functions
    - Asymmetric Keys

#### Key Management

- EMV Data

#### Cardholder Verification Methods
EMV security functions performed online

1. Online Card Authentication (Online CAM)
2. New Message Data for Authorization Assessment
On-line CAM (Card Authentication)

EMV transaction data

Payment Brand

Acquirer System

Dynamic Authentication Code

3DES cryptography Shared Key

Hardware Security Module and Key Management System

Embedded 3DES crypto processor
EMV message data also increases online fraud detection security

New EMV authentication data

Issuer Auth System

Payment Brand

Field/DE 55

Acquirer System

Terminal EMV transaction analysis data

Chip EMV Transaction Analysis data
New EMV data in the authorization message enhances authorization decisioning.

ISO 8583 – Field or DE 55

<table>
<thead>
<tr>
<th>Field/DE 55</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Cryptogram</td>
</tr>
<tr>
<td>Cryptogram Information Data</td>
</tr>
<tr>
<td>Issuer Application Data</td>
</tr>
<tr>
<td>Application Interchange Profile</td>
</tr>
<tr>
<td>Terminal Verification Result</td>
</tr>
<tr>
<td>Terminal Capabilities</td>
</tr>
<tr>
<td>Cardholder Verification Method Results</td>
</tr>
<tr>
<td>Unpredictable Number</td>
</tr>
<tr>
<td>Application Transaction Counter</td>
</tr>
<tr>
<td>Amount, Authorized (Numeric)</td>
</tr>
<tr>
<td>Transaction Currency Code</td>
</tr>
<tr>
<td>Transaction Date</td>
</tr>
<tr>
<td>Transaction Type</td>
</tr>
<tr>
<td>Transaction Currency Code</td>
</tr>
<tr>
<td>Terminal Country Code</td>
</tr>
</tbody>
</table>

Authorization Rules

Fraud Rules
The new EMV information in the authorization message increases the issuers security tools

Issuer Authorization Tools
- Increased use of authentication security keys
  - EMV dynamic cryptogram (ARQC) validation
- Enhanced Authorization assessment rules
  - Cross check terminal and card results
- Offline PIN Optional for cardholder verification
- Online PIN Optional for cardholder verification
- Post issuance card updates
- EMV Authorization Response Code (ARPC)
EMV Security Functions Performed Offline

1. Offline Card Authentication (Offline CAM)
2. Offline Authorization (Offline Transaction)
3. Offline PIN (Cardholder Verification Option)

Asymmetric Keys
EMV Offline security functions require asymmetric keys and certificates.

Offline Security relies upon Asymmetric Key Technology.

Key Pair

- Public Key
- Private Key
Offline card authentication leverages asymmetric key technology

Public key infrastructure required for EMV offline functions

- Confirms that the card is not counterfeit
- Protects against data manipulation
# Off-line CAM (Card Authentication Method) Options

## Offline Card Authentication Options

<table>
<thead>
<tr>
<th>DDA</th>
<th>CDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Data Authentication</td>
<td>Combined Data Authentication</td>
</tr>
<tr>
<td>Issuer Public Key Certificate</td>
<td>Issuer Public Key Certificate</td>
</tr>
<tr>
<td>ICC Public Key Certificate</td>
<td>ICC Public Key Certificate</td>
</tr>
<tr>
<td>Application Cryptogram (Transaction Certificate)</td>
<td></td>
</tr>
</tbody>
</table>

**Protects Against**
- Counterfeiting
- Skimming

**Protects Against**
- Counterfeiting
- Skimming
- Wedge Attacks

*Dynamic offline card authentication is unique per transaction*
Offline authorization risk parameters are loaded at personalization and updated with post issuance scripts.

2 Offline Authorization (Offline Transaction)

**Offline Risk Management on the Chip**

- Consecutive Transaction Counter
- Last Online Application Transaction Counter
- Lower Consecutive Offline Counter
- Upper Consecutive Offline Counter
- Lower Consecutive Offline Amount
- Upper Consecutive Offline Amount
- PIN
- PIN Try Limit
- PIN Try Counter
- Issuer Action Codes
- Card Issuer Action Codes

Additional Processing Rules

Offline Authorization Parameters
EMV Cardholder Verification Settings

**CVM Options**

- No CVM
- Signature
- On-line PIN at ATM
- On-line PIN at POS
- Off-line PIN plain texted
- Off-line PIN enciphered

**Example: CVM List Selected**

- Online PIN at ATM
- Offline PIN at POS
- Signature
- No CVM

**Priority**
Card profiles and terminal profiles work together to determine the method of cardholder verification.
EMV From a Terminal Perspective

EMV Terminals Become a Workflow Engine

- Signature?
- Online PIN?
- Offline PIN?
- Online CAM
- Offline CAM?
- Offline Authorization
- Other EMV Processing Conditions?
New EMV logic and approvals required for the terminal application.

**Consumer Prompting Logic**

**Merchant Business Line Logic**

- **Visa**
- **MC**
- **AMEX**
- **Discover**

**Contactless Kernels**

(Contactless Card and Mobile NFC) Separate Kernels

**EMV Contact Kernel**

(Common Kernel)

- **Visa**
- **MC**
- **AMEX**
- **Discover**
- **Others**

**EMV hardware and communication components**

**Terminal Operating System**

**Brand Certifications**

- EMVCo Approvals
  - Level 2 Software
  - Level 1 Hardware
Acquirers are required to Brand Certify each terminal type that they deploy.
A U.S. Debit EMV card will have two EMV applications/AIDs in the chip.

To meet Durbin routing option compliance the application selection process changes and two AIDs relate to one funding account.
All stakeholders need to migrate to receive the full benefit of EMV

- New card data
- New messaging data
- New application logic
- New configuration settings
- Enhanced authorization/fraud strategies
Q&A
EMV Resources

EMV Connection web site – http://www.emv-connection.com

EMV Migration Forum Resources
• “Standardization of Terminology” glossary
• “Testing and Certification: Current U.S. Payment Brand Requirements for the Acquiring Community” white paper
• “U.S. Debit EMV Technical Proposal” white paper

Other Resources for Issuers, Merchants and Acquirers/Processors
• EMV FAQ
• “Card Payments Roadmap in the U.S.” white paper
• “How EMV Changes Payment Workshop” recording
• U.S. issuers of EMV chip cards
• Cathy Medich, cmedich@us-emvforum.org
• Guy Berg, guy_berg@mastercard.com