EMV 101

EMV Migration Forum Webinar
March 6, 2014
Introduction

Randy Vanderhoof
Director, 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:** Randy Vanderhoof, Director, EMV Migration Forum

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

• **Q&A**
Global EMV Adoption

EMV Adoption Rates by Region*

*Figures reported as of Q4 2012 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.

Source: EMVCo
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 Webinar

EMV Security Functions - Guy Berg, MasterCard Advisors
EMV Fundamentals

I. EMV Payment Transaction Framework

II. Transaction Processing Comparison
   - Magnetic Stripe vs. EMV Transaction Security Points
   - Data Breach and Skimming Protection Mechanisms

III. EMV Application Fundamentals
   - On-line Card Authentication
   - Off-line Card Authentication
   - Offline Authorization
   - Risk Management
   - Cardholder Verification Method
EMV migration impacts all stakeholders involved in payment transaction processing.

- New card data
- New messaging data
- New application logic
- New configuration settings
Magnetic Stripe Transaction uses 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 cannot recognize cloned 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
Multiple protection mechanisms are used in concert to combat card skimming, counterfeit card production and data breach threats.
EMV introduces new data, cryptographic processes and security keys

<table>
<thead>
<tr>
<th>M/Chip 4 Tags</th>
<th>Chip Data</th>
<th>VSDC Tags</th>
<th>Chip Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>D3</td>
<td>Additional Check Table</td>
<td>9F51</td>
<td>Application Currency Code</td>
</tr>
<tr>
<td>D5</td>
<td>Application Control (Contact)</td>
<td>9F52</td>
<td>Application Default Action</td>
</tr>
<tr>
<td>D7</td>
<td>Application Control (Contactless)</td>
<td>9F53</td>
<td>Cons Trx Counter International Limit (CTCIL)</td>
</tr>
<tr>
<td>D9</td>
<td>Application File Locator (Contactless)</td>
<td>9F54</td>
<td>Cum Total Transaction Amount Limit (CTTAL)</td>
</tr>
<tr>
<td>D8</td>
<td>Application Interchange Profile (Contactless)</td>
<td>9F55</td>
<td>Geography Indicator</td>
</tr>
<tr>
<td>C3</td>
<td>Card Issuer Action Code (CIAC) - Denial</td>
<td>9F56</td>
<td>Issuer Authentication Indicator</td>
</tr>
<tr>
<td>C4</td>
<td>Card Issuer Action Code (CIAC) - Default</td>
<td>9F57</td>
<td>Issuer Country Code</td>
</tr>
<tr>
<td>C5</td>
<td>Card Issuer Action Code (CIAC) – Online</td>
<td>9F58</td>
<td>Cons Trx Counter Limit (CTCL)</td>
</tr>
<tr>
<td>CD</td>
<td>Card Issuer Action Code – Default (Contactless)</td>
<td>9F59</td>
<td>Cons Trx Counter Upper Limit (CTCUL)</td>
</tr>
<tr>
<td>CE</td>
<td>Card Issuer Action Code – Online (Contactless)</td>
<td>9F5C</td>
<td>Cum Total Trx Amt Upper Limit (CTTAUL)</td>
</tr>
<tr>
<td>CF</td>
<td>Card Issuer Action Code – Denial (Contactless)</td>
<td>9F5D</td>
<td>Available Offline Spending Amount</td>
</tr>
<tr>
<td>D1</td>
<td>Currency Conversion Table</td>
<td>9F72</td>
<td>Cons Trx Counter International Country Limit (CTCICL)</td>
</tr>
<tr>
<td>D6</td>
<td>Default ARPC Response Code</td>
<td>9F73</td>
<td>Currency Conversion Parameters</td>
</tr>
<tr>
<td>9F 14</td>
<td>Lower Consecutive Offline Limit (LCOL)</td>
<td>9F77</td>
<td>VLP Funds Limit</td>
</tr>
<tr>
<td>CA</td>
<td>Lower Cum. Offline Transaction Amt (LCOTA)</td>
<td>9F78</td>
<td>VLP Single Transaction Limit</td>
</tr>
<tr>
<td>9F 23</td>
<td>Upper Consecutive Offline Limit (UCOL)</td>
<td>9F79</td>
<td>VLP Available Funds</td>
</tr>
<tr>
<td>CB</td>
<td>Upper Cum. Offline Transaction Amt (UCOTA)</td>
<td>9F7F</td>
<td>Card Production Life Cycle History (CPLC)</td>
</tr>
<tr>
<td>9F6C</td>
<td>Magstripe Application Version Number</td>
<td>Key</td>
<td>MDK_{AC}</td>
</tr>
<tr>
<td>9F62</td>
<td>PCVC3 Track1 (Contactless)</td>
<td>Key</td>
<td>MDK_{SMI}</td>
</tr>
<tr>
<td>9F63</td>
<td>PUNATC Track1 (Contactless)</td>
<td>Key</td>
<td>MDK_{SMC}</td>
</tr>
<tr>
<td>9F64</td>
<td>NATC Track1 (Contactless)</td>
<td>Key</td>
<td>MDK_{IDN}</td>
</tr>
<tr>
<td>9F65</td>
<td>PCVC3 Track2 (Contactless)</td>
<td>Key</td>
<td>MDK_{CVC3}</td>
</tr>
<tr>
<td>9F66</td>
<td>PUNATC Track2 (Contactless)</td>
<td>Key</td>
<td></td>
</tr>
<tr>
<td>9F67</td>
<td>NATC Track2 (Contactless)</td>
<td>Key</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Track1 Data (Contactless)</td>
<td>Key</td>
<td></td>
</tr>
<tr>
<td>9F6B</td>
<td>Track2 Data (Contactless)</td>
<td>Key</td>
<td></td>
</tr>
</tbody>
</table>
Chip security provides both card stock security and transaction security.

**Card Stock Security**
- EMV Card Configuration Data
- Issuance Security

**Transaction Security**

**Pre-issuance Security**
- Key Management
  - EMV Data

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

**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

EMV transaction data

Dynamic Authentication Code

3DES cryptography Shared Key

Issuer Auth System

Online Request (ARQC)

Hardware Security Module and Key Management System

Embedded 3DES crypto processor
EMV message data also increases online fraud detection security
New EMV data in the authorization message enhances authorization decisioning

ISO 8583 – Field or DE 55

<table>
<thead>
<tr>
<th>Application Cryptogram</th>
<th>Application Transaction Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptogram Information Data</td>
<td>Amount, Authorized (Numeric)</td>
</tr>
<tr>
<td>Issuer Application Data</td>
<td>Transaction Currency Code</td>
</tr>
<tr>
<td>Application Interchange Profile</td>
<td>Transaction Date</td>
</tr>
<tr>
<td>Terminal Verification Result</td>
<td>Transaction Type</td>
</tr>
<tr>
<td>Terminal Capabilities</td>
<td>Transaction Currency Code</td>
</tr>
<tr>
<td><strong>Cardholder Verification Method Results</strong></td>
<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 ARQC dynamic cryptogram 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
- ARPC
EMV Security Functions Performed Offline

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

Offline Security Functions

Asymmetric Keys
EMV Offline security functions require asymmetric keys and certificates.
Offline Card Authentication (Simple Example)

Certificate Authority

CA Private Key

CA Public Key

CA Private Key signs
ISS Public key
certificate request data

Issuer PK Certificate

Acquirer loads the Public Key to the Terminal

Loaded to the card before Issuance

Authenticates the card is legitimate

Does not verify who is using it!

Offline DDA/CDA Card Authentication
Off-line CAM (Card Authentication Method) Options

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

Card (Chip) Level Certificate

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

## Offline Authorization (Offline Transaction)

### Offline Risk Management on the Chip

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

### Offline Authorization Parameters
**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.

Card CVM List:

- **CVM 1**: Online PIN at ATM
- **CVM 2**: Online PIN at POS
- **CVM 3**: Signature at POS
- **CVM 5**: No CVM at POS

Terminal Capability Profile:

- **POS Terminal**
  - Signature
  - No “Offline PIN” support
  - No “Online PIN” support
Terminal Perspective – EMV Logic Impact

Each Brand requires EMV terminal certification

Consumer Prompting Logic

<table>
<thead>
<tr>
<th>Visa EMV Config Data, processing rules and AIDs</th>
<th>MC EMV Config Data, processing rules and AIDs</th>
<th>AMEX EMV Config Data, processing rules and AIDs</th>
<th>Discover EMV Config Data, processing rules and AIDs</th>
<th>Other Config Data, processing rules and AIDs</th>
</tr>
</thead>
</table>

EMV Contact Kernel
EMV terminal functions that EMV Co tests against the EMV standards and certifies

Terminal Operating System
Acquirers are required to Brand Certify each terminal type that they deploy.
The AID provides a method for the terminal to recognize what applications exist on a chip card.

So what is an AID?

- An Identifier that must be registered with ISO
- Identifies an application owner
- Identifies application required logic for operation
- 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
The terminals maintain a list of AIDs that it supports

The terminal keeps a list of AIDs that it can support

An Issuer loads applications and corresponding AIDs to the chip

Logic and configuration data specific to each AID must be added to the terminal

### List of AIDs supported by the terminal

<table>
<thead>
<tr>
<th>AID Description</th>
<th>AID Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC Debit/Credit AID</td>
<td>A00000000041010</td>
</tr>
<tr>
<td>MC U.S. Maestro Common AID</td>
<td>A00000000042203</td>
</tr>
<tr>
<td>Visa</td>
<td>A00000000031010</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>
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
EMV leverages card, terminal, messaging and host system security technology to protect against counterfeit fraud.
Q&A
• Randy Vanderhoof, rvanderhoof@us-emvforum.org
• Guy Berg, guy_berg@mastercard.com

www.emv-connection.com