Fundamentals of EMV

- Guy Berg
- Senior Managing Consultant
- MasterCard Advisors’
- guy_berg@mastercard.com
- 914.325.8111
Transaction Processing Comparison
– Magnetic Stripe vs. EMV Transaction Security Points

EMV Application Fundamentals

- Risk Management
- On-line authentication
- Off-line authentication
- Cardholder Verification Method
- Offline Authorization
EMV Component Impact View
Magnetic Stripe Transaction

1) Magnetic stripe is easily cloned

2) Terminal performs little or no risk assessment

3) Authorization/Capture 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 Framework

(1) EMV Chip application performs risk assessment

(2) Terminal performs risk assessment

(3) New EMV authentication data

(4) Issuer Authorization Changes
- Dynamic cryptogram validation
- May return an authentication cryptogram
- Post issuance updates

Payment Brand

Acquirer System

Issuer Auth System

New EMV data

Field or DE 55

ARPC

Field or DE 55

ARPC

New EMV data
EMV Security Components

Card Stock Security
- EMV Configuration
- Issuance Security

Data Preparation
Key Management

EMV Data

Online
PIN

Offline
PIN

Risk Management Decision Criteria
# EMV Chip Data

<table>
<thead>
<tr>
<th>EMV Tag</th>
<th>Chip Data</th>
<th>EMV Tag</th>
<th>Chip Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>9F 26</td>
<td>Application Cryptogram</td>
<td>8E</td>
<td>Cardholder Verification Method List</td>
</tr>
<tr>
<td>9F 42</td>
<td>Application Currency Code</td>
<td>8F</td>
<td>Certification Authority Public Key Index</td>
</tr>
<tr>
<td>9F 51</td>
<td>Application Currency Code VIS</td>
<td>9F 53</td>
<td>Consecutive Transaction Limit International</td>
</tr>
<tr>
<td>9F 44</td>
<td>Application Currency Exponent</td>
<td>9F 72</td>
<td>Consecutive Transaction Limit International</td>
</tr>
<tr>
<td>9F 52</td>
<td>Application Default Action</td>
<td>9F 54</td>
<td>Cryptogram Information Data</td>
</tr>
<tr>
<td>9F 05</td>
<td>Application Discretionary Data</td>
<td>9F 5C</td>
<td>Cumulative Total Transaction Amount Limit</td>
</tr>
<tr>
<td>5F 25</td>
<td>Application Effective Date</td>
<td>9F 49</td>
<td>Dynamic Data Object List</td>
</tr>
<tr>
<td>5F 24</td>
<td>Application Expiration Date</td>
<td>9F 55</td>
<td>Geographic Indicator</td>
</tr>
<tr>
<td>94</td>
<td>Application File Locator</td>
<td>9F 2D</td>
<td>ICC PIN Encipherment Public Key Certificate</td>
</tr>
<tr>
<td>82</td>
<td>Application Interchange Profile</td>
<td>9F 2E</td>
<td>ICC PIN Encipherment Public Key Exponent</td>
</tr>
<tr>
<td>50</td>
<td>Application Label</td>
<td>9F 2F</td>
<td>ICC PIN Encipherment Public Key Remainder</td>
</tr>
<tr>
<td>9F 12</td>
<td>Application Preferred Name</td>
<td>9F 46</td>
<td>ICC Public Key Certificate</td>
</tr>
<tr>
<td>5A</td>
<td>Application Primary Acct Number</td>
<td>9F 47</td>
<td>ICC Public Key Exponent</td>
</tr>
<tr>
<td>5F 34</td>
<td>Primary Acct Number Seq Number</td>
<td>9F 48</td>
<td>ICC Public Key Remainder</td>
</tr>
<tr>
<td>87</td>
<td>Application Priority Indicator</td>
<td>9F 0D</td>
<td>Issuer Action Code – Default</td>
</tr>
<tr>
<td>9F 36</td>
<td>Application Transaction Counter</td>
<td>9F 0E</td>
<td>Issuer Action Code – Denial</td>
</tr>
<tr>
<td>9F 07</td>
<td>Application Usage Control</td>
<td>9F 0F</td>
<td>Issuer Action Code – Online</td>
</tr>
<tr>
<td>9F 08</td>
<td>Application Version Number (ICC)</td>
<td>9F 10</td>
<td>Issuer Application Data</td>
</tr>
<tr>
<td>9F 5D</td>
<td>Application offline Spending Amount</td>
<td>9F 56</td>
<td>Issuer Authentication Indicator</td>
</tr>
<tr>
<td>9F 7F</td>
<td>Card Production Life Cycle History File Identifiers</td>
<td>9F 11</td>
<td>Issuer Code Table Index</td>
</tr>
<tr>
<td>8C</td>
<td>Card Risk Management Data Object List 1</td>
<td>5F 28</td>
<td>Issuer Country Code</td>
</tr>
<tr>
<td>8D</td>
<td>Card Risk Management Data Object List 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5F 20</td>
<td>Cardholder Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9F 0B</td>
<td>Cardholder Name Extended</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EMV Risk Mgmt Data on the Chip

Issuer Interchange Profile
- SDA supported
- DDA supported
- CDA supported
- Cardholder verification supported
- Perform terminal risk management
- Issuer authentication required/or not

Application Usage Control
Valid for:
- Domestic cash transactions
- International cash transactions
- Domestic goods
- International goods
- Domestic services
- International services
- ATMs
- Domestic cashback
- International cashback

Issuer Action Codes
- If issuer authentication failure, do not transmit next transaction online
- If new card, do not decline if unable to go online
- .......
Cardholder Verification

**CVM Options**

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

**CVM List**

- Online PIN at ATM
- Offline PIN at POS
- Signature
- No CVM
EMV Online Transaction Security

- EMV Configuration
- Issuance Security

Data Preparation
Key Management

Risk Management Decision Criteria

Online Transaction Security

Offline Transaction Security
EMV On-line Security

- On-line EMV Authentication
- On-the-Behalf EMV Authentication
On-line CAM (Card Authentication)

Issuer Auth System → Payment Brand → Acquirer System

EMV transaction data

3DES Cryptogram

Shared Key

ARQ Cryptogram

ARQC

Shared Key

Online Request (ARQC)

PIN

EMV transaction data

Shared Key
On-the-be-Half EMV Authentication

Auth Code converted to EMV Response

EMV transaction data

Online Request (ARQC)

Appears as Mag Stripe Transaction

Issuer Auth System

Payment Brand

Acquirer System

Auth Code

Mag Stripe Transaction

EMV Auth Code

EMV Auth Code converted to EMV Response

Auth

Appears as Mag Stripe Transaction

Auth

Online Request (ARQC)
EMV Offline Transaction Security

Card Stock Security
- EMV Configuration
- Issuance Security

Data Preparation
EMV Data
Key Management

Online Transaction Security

Offline Transaction Security

Risk Management Decision Criteria
EMV Off-line Transaction Security

- Offline CAM (Card Authentication)
- Offline CVM (Cardholder Verification)
- Offline Authorization

Public Key Infrastructure (PKI)

User → CA

Issue → Public key certificate

User’s private key

Verifier

Check → CA
Off-line Security Options

Off-line Authentication Options

<table>
<thead>
<tr>
<th>SDA</th>
<th>DDA</th>
<th>CDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Data</td>
<td>Dynamic Data</td>
<td>Combined Data</td>
</tr>
<tr>
<td>Issuer Public Key</td>
<td>Issuer Public Key</td>
<td>Issuer Public Key</td>
</tr>
<tr>
<td>Certificate</td>
<td>Certificate</td>
<td>Certificate</td>
</tr>
<tr>
<td></td>
<td>ICC Public Key Certificate</td>
<td>ICC Public Key Certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Cryptogram</td>
</tr>
</tbody>
</table>

Issuer Level Certificate  Card Level Certificate
Off-line Transaction Authentication
SDA (Issuer level certificate)

SDA (Static Data Authentication)

Certificate Authority

CA Private Key

CA Public Key

CA Private Key
signs
ISS Public key

Issuer PK Certificate

Load Public Key to the Terminal

Load with Issuer Signed Static Data

Authenticated the card is legitimate

Does not verify who is using it!

Verifies the user.

PIN

SDA Card Authentication

Loaded with Issuer Signed Static Data

Verifies the user.

Does not verify who is using it!
Offline Cardholder Verification

- **SDA Cards**
  - Clear Text PIN

- **DDA or CDA Cards**
  - Clear Text PIN
  - Encrypted (Enciphered) PIN
Offline Authorization

Offline Risk Data on the Chip

- Consecutive Transaction Counter
- Last Online Application Transaction Counter
- Lower Consecutive Offline Limit
- Upper Consecutive Offline Limit
- Cumulative Total Transaction Amount
- Cumulative Total Transaction Limit
- PIN
- PIN Try Limit
- PIN Try Counter
- Certification Authority Public Key Index
- Signed Static Application Data
- Signed Dynamic Application Data
- Static Data Authentication Tag List
- Issuer Action Codes

Authorization Parameters
EMV Security Components

Card Stock Security

Issuance Security
Data Preparation & Key Mgmt Security

On-line Transaction Security

Risk Management Decision Criteria
Off-line Transaction Security

[Diagram showing security components and risk management criteria]
EMV Chip Personalization

CMS System

Emboss/Mag Stripe File

Data Prep System

Key Mgmt System

EMV Data & Keys

EMV Issuance

Smart Card Alliance
Card Types

- Contact EMV

- Contactless EMV
  - Contactless Mag Stripe Emulation

- Contact EMV
  - Contactless EMV
  - Contactless Mag Stripe Emulation
Chip OS and Applications

Operating System Level
- MULTOS
- Global Platform JavaCard
- Card Vendor 1 Proprietary
- Card Vendor 2 Proprietary
- Card Vendor 3 Proprietary
- Etc....

EMV Application Level
- MasterCard
  - PayPass Contactless EMV
  - Mchip Contact EMV
- Visa
  - payWave Contactless EMV
  - VSDC Contact EMV
- American Express
- Discover

Data Level
- Personalization Data
- Risk management criteria
- Cardholder data
- Security keys and certificates

- Card Vendors have different chip operating systems
- Brands have different chip application implementations
- Brands have different EMV risk configuration options
Acquirers, Merchants and Terminals
Each Brand has different terminal certification requirements

<table>
<thead>
<tr>
<th>Brand</th>
<th>EMV Terminal Processing Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa</td>
<td>Visa EMV terminal processing functions</td>
</tr>
<tr>
<td>MC</td>
<td>MC EMV terminal processing functions</td>
</tr>
<tr>
<td>AMEX</td>
<td>AMEX EMV terminal processing functions</td>
</tr>
<tr>
<td>Discover</td>
<td>Discover EMV terminal processing functions</td>
</tr>
<tr>
<td>Others</td>
<td>Others EMV terminal processing functions</td>
</tr>
</tbody>
</table>

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

**Terminal Operating System**
## Terminal Profile (EMVCo Type Approval)

<table>
<thead>
<tr>
<th>Unattended Terminal Profile</th>
<th>Unattended Terminal Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supports but does not require PIN</strong></td>
<td><strong>Requires PIN</strong></td>
</tr>
<tr>
<td>➢ Chip only cards</td>
<td>➢ Chip only cards</td>
</tr>
<tr>
<td>➢ Offline plain text PIN</td>
<td>➢ Offline plain text PIN</td>
</tr>
<tr>
<td>➢ Offline enciphered PIN</td>
<td>➢ Offline enciphered PIN</td>
</tr>
<tr>
<td>➢ No CVM</td>
<td>➢ SDA</td>
</tr>
<tr>
<td>➢ SDA</td>
<td>➢ DDA</td>
</tr>
<tr>
<td>➢ DDA</td>
<td>➢ CDA</td>
</tr>
<tr>
<td>➢ CDA</td>
<td></td>
</tr>
<tr>
<td>➢ Issuer authentication supported</td>
<td></td>
</tr>
</tbody>
</table>
EMV Transaction Flow

Technology Selection
  Application Selection
    Processing Options
      Card Authentication
        Processing Restrictions
          Card Holder Verification
            Terminal Risk Management
              Terminal Action Analysis
                Card Action Analysis
                  Go On-line or Not
                    Issuer-to-Card Script Processing

Switch/Acquirer
EMV Transaction Flow

Application Selection
  • What AID?

Card Authentication Method
  • SDA, DDA, CDA, No ODA

Cardholder Verification Method
  • CVM List Preferences

Offline Authorization Support – Y/N

Issuer Action Codes
  • Exception processing rules
Application Selection

Identify mutually supported AIDs

<table>
<thead>
<tr>
<th>Priority</th>
<th>AID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A00000000041010</td>
</tr>
<tr>
<td>2</td>
<td>A0000xyz</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AID</th>
<th>Config Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>A000000000031010</td>
<td></td>
</tr>
<tr>
<td>A00000000041010</td>
<td></td>
</tr>
<tr>
<td>A0000001523010</td>
<td></td>
</tr>
<tr>
<td>A00000000043060</td>
<td></td>
</tr>
<tr>
<td>A000000002501</td>
<td></td>
</tr>
<tr>
<td>A0000xyz</td>
<td></td>
</tr>
</tbody>
</table>
Application Selection Method

**Explicit Selection**
- Displays the choices to consumer

- MasterCard Debit
- XYZ Debit

**Implicit Selection**
- Terminal automatically selects the AID

<table>
<thead>
<tr>
<th>P</th>
<th>AID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A00000000041010</td>
</tr>
<tr>
<td>2</td>
<td>A0000xyz</td>
</tr>
</tbody>
</table>
Cardholder Verification

CVM Options

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

CVM List

Online PIN at ATM → Offline PIN at POS → Signature → No CVM
EMV Message Data

Field or DE 55

Payment Brand

Acquirer System

Issuer Auth System

New EMV authentication data
## EMV Authorization Message

**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>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 (CVM)</td>
</tr>
<tr>
<td>Cryptogram Information Data</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>
EMV Transaction Framework

Issuer Authorization Changes
- EMV ARQC dynamic cryptogram validation
- Authentication cryptogram generation
- Post issuance card updates
- Offline PIN Management
- Online PIN management
- Key Management
- Authorization assessment rules

Payment Brand

Issuer Auth System

Field or DE 55

ARPC

New EMV data

Acquirer System
EMV at a Glance

- Online CAM and CVM
- Offline CAM and CVM
- Offline Authorization
- Chip Risk Management
Smart Card Alliance
191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556–6828
www.smartcardalliance.org

Guy Berg
Mastercard Advisors’
914.325.8111
Guy_berg@Mastercard.com