# EMV 101

EMV Migration Forum Webinar
January 22, 2014
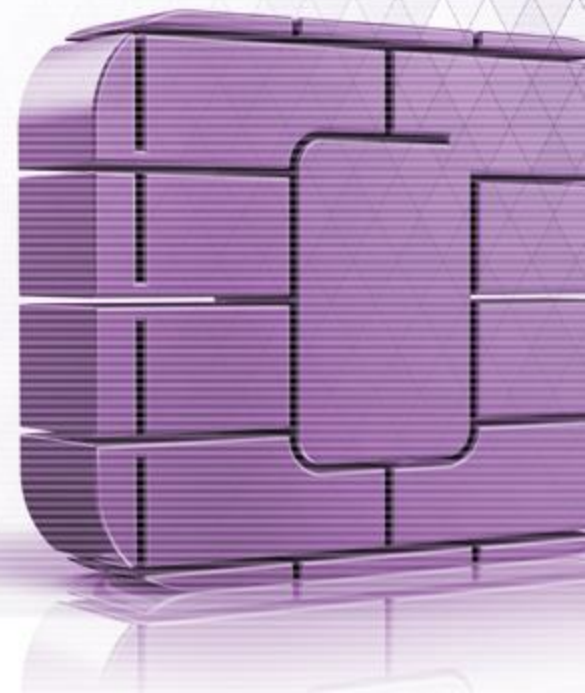
# About the EMV Migration Forum

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.

**EMV**®
Migration Forum
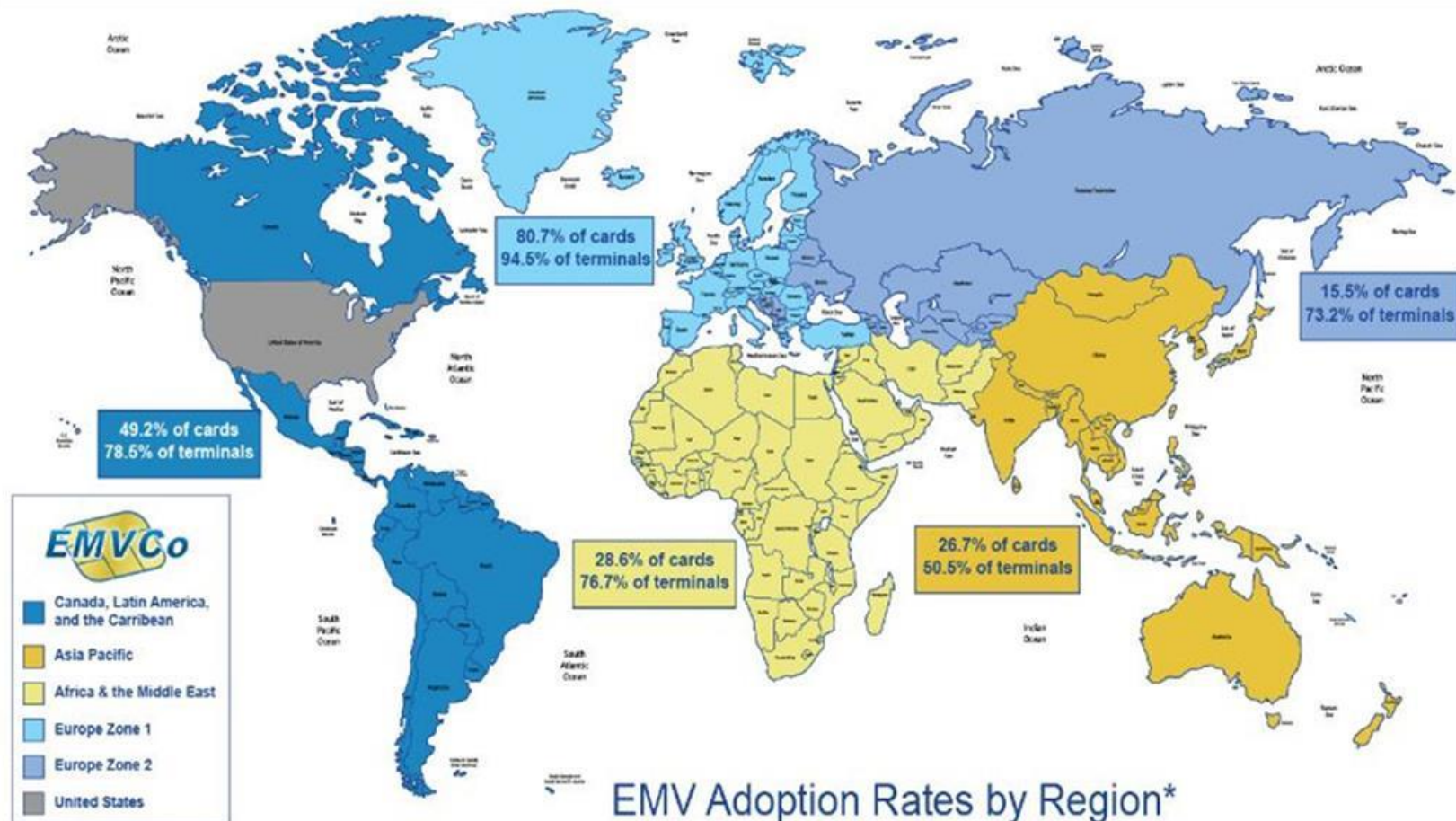
# Today's Webinar Topics & Speakers

- **Introduction & EMV Implementation Status**: Randy Vanderhoof, Director, EMV Migration Forum

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

- **Q&A**

**EMV**®
Migration Forum

# Global EMV Adoption



EMV Adoption Rates by Region*

Legend:
- Canada, Latin America, and the Carribean
- Asia Pacific
- Africa & the Middle East
- Europe Zone 1
- Europe Zone 2
- United States

- 80.7% of cards, 94.5% of terminals
- 15.5% of cards, 73.2% of terminals
- 49.2% of cards, 78.5% of terminals
- 28.6% of cards, 76.7% of terminals
- 26.7% of cards, 50.5% of terminals

*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
- ATM providers are actively deploying EMV-enabled ATMs
- 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
- 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**®
Migration Forum

# EMV Fundamentals

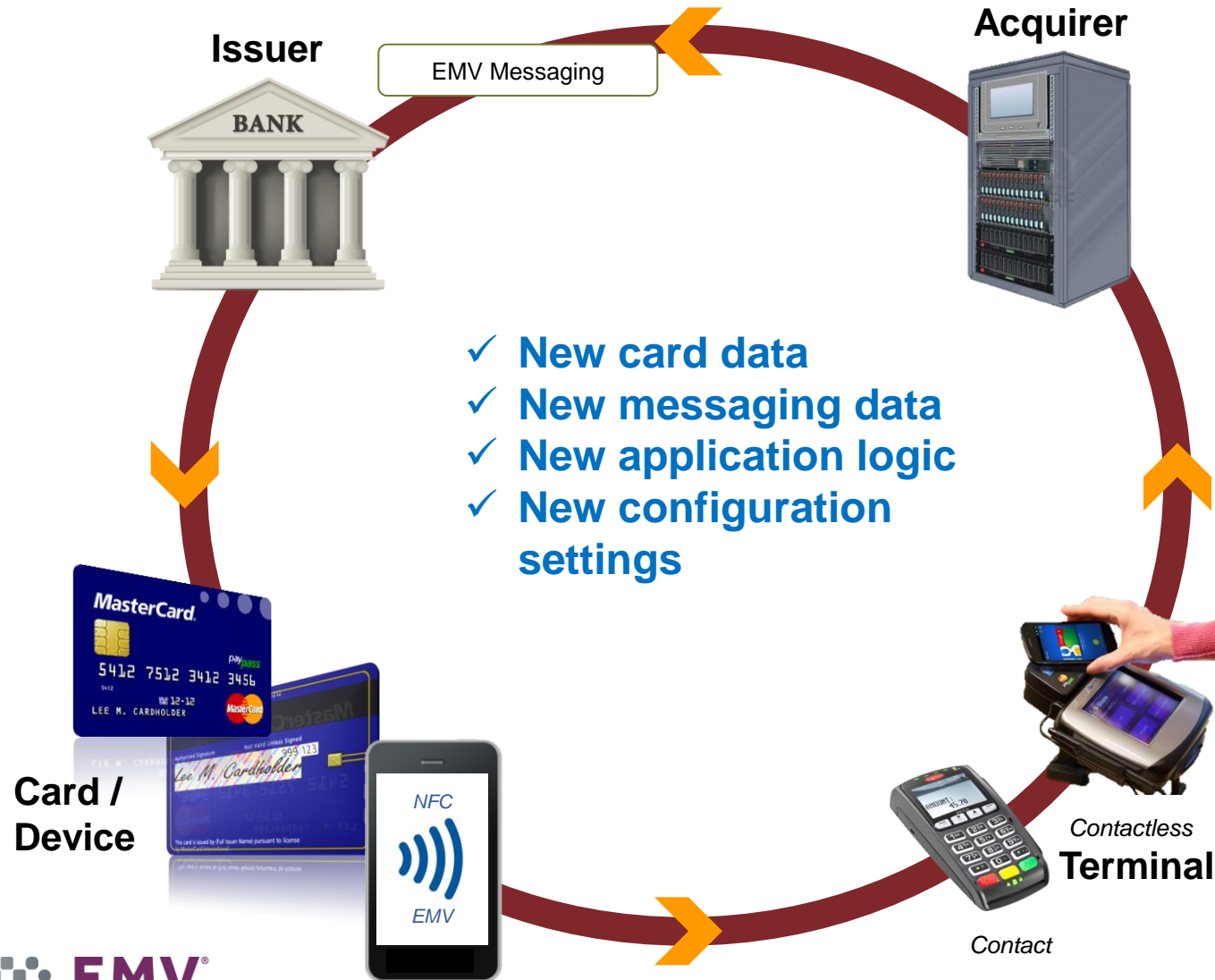I. **EMV Payment Transaction Framework**
II. **Transaction Processing Comparison**
   - Magnetic Stripe vs. EMV Transaction Security Points
   - Data Breach and  Skimming Protection Mechanisms

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

**EMV**®
Migration Forum

# EMV migration impacts all stakeholders involved in payment transaction processing



**Issuer**

EMV Messaging

**Acquirer**

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

**Card / Device**

*NFC*

)))

*EMV*

*Contactless*
**Terminal**

*Contact*

**EMV**
Migration Forum

# Magnetic Stripe Transaction uses static authentication data that can be skimmed

**Track data**

**Auth Code**

**Auth Code**

**Track Data**

## Payment Network

## Acquirer System

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

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

1) Magnetic stripe is easily cloned

## Issuer Auth System

**EMV® Migration**

4) Authorization/Authentication
➢ Risk assessment performed at the host
➢ Host cannot recognized cloned cards

# EMV Transaction Processing Introduces dynamic authentication that makes copied data useless at POS



**Payment Brand**

**Acquirer System**

**Issuer Auth System**

Field/DE 55

ARPC

Field/DE 55

ARPC

Field/DE 55

New dynamic authentication data

(3) New EMV authentication data

(2) Terminal performs risk assessment

(1) EMV Chip application performs risk assessment

(4) New Issuer Authorization Functions
➢ Dynamic cryptogram validation
➢ May return an authentication cryptogram
➢ Post issuance updates

EMV
Migration Forum

# EMV and non EMV security mechanisms combine to provide skimming and data breach protection

Multiple protection mechanisms are used in concert to combat card skimming, counterfeit card production and data breach threats
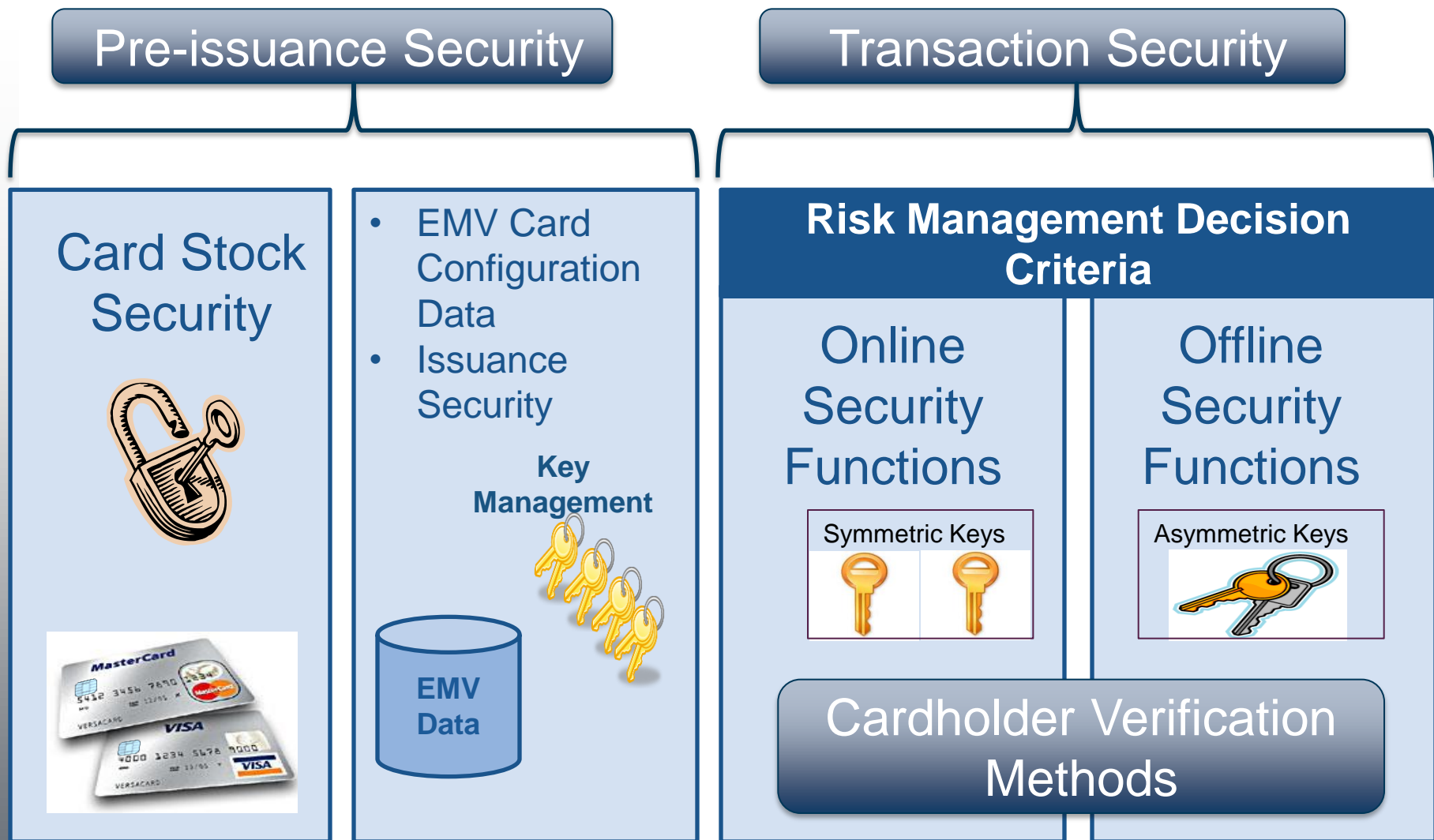
Each of these values are different

Dynamic

| CVC 1 and CVV 1 |
| CVC 2 and CVV 2 |
| Chip CVC |
| EMV ARQC |

Chip Service Code
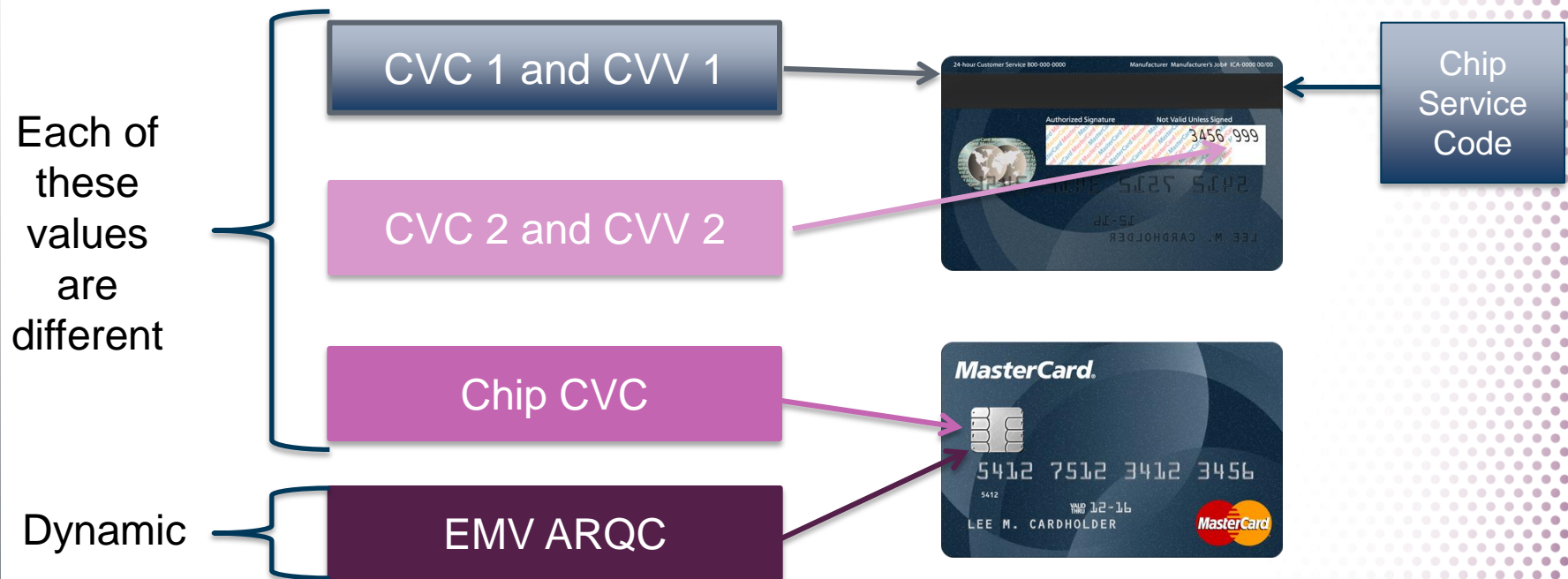
# EMV introduces new data, cryptographic processes and security keys

| M/Chip 4 Tags | Chip Data | VSDC Tags | Chip Data |
|---|---|---|---|
| D3 | Additional Check Table | 9F51 | Application Currency Code |
| D5 | Application Control (Contact) | 9F52 | Application Default Action |
| D7 | Application Control (Contactless) | 9F53 | Cons Trx Counter International Limit (CTCIL) |
| D9 | Application File Locator (Contactless) | 9F54 | Cum Total Transaction Amount Limit (CTTAL) |
| D8 | Application Interchange Profile (Contactless) | 9F55 | Geography Indicator |
| C3 | Card Issuer Action Code (CIAC) - Denial | 9F56 | Issuer Authentication Indicator |
| C4 | Card Issuer Action Code (CIAC) - Default | 9F57 | Issuer Country Code |
| C5 | Card Issuer Action Code (CIAC) – Online | 9F58 | Cons Trx Counter Limit (CTCL) |
| CD | Card Issuer Action Code – Default (Contactless) | 9F59 | Cons Trx Counter Upper Limit (CTCUL) |
| CE | Card Issuer Action Code – Online (Contactless) | 9F5C | Cum Total Trx Amt Upper Limit (CTTAUL) |
| CF | Card Issuer Action Code – Denial (Contactless) | 9F5D | Available Offline Spending Amount |
| C8 | Card Risk Management (CRM) Country Code | 9F5E | Cons Trx International Upper Limit (CTIUL) |
| C9 | Card Risk Management (CRM) Currency Code | 9F68 | Card Additional Processes |
| D1 | Currency Conversion Table | 9F72 | Cons Trx Counter International Country Limit (CTCICL) |
| D6 | Default ARPC Response Code | 9F73 | Currency Conversion Parameters |
| 9F 14 | Lower Consecutive Offline Limit (LCOL) | 9F77 | VLP Funds Limit |
| CA | Lower Cum. Offline Transaction Amt (LCOTA) | 9F78 | VLP Single Transaction Limit |
| 9F 23 | Upper Consecutive Offline Limit (UCOL) | 9F79 | VLP Available Funds |
| CB | Upper Cum. Offline Transaction Amt (UCOTA) | 9F7F | Card Production Life Cycle History (CPLC) |
| 9F6C | Magstripe Application Version Number | | |
| 9F62 | PCVC3 Track1 (Contactless) | Key | $MDK_{AC}$ |
| 9F63 | PUNATC Track1 (Contactless) | Key | $MDK_{SMI}$ |
| 9F64 | NATC Track1 (Contactless) | Key | $MDK_{SMC}$ |
| 9F65 | PCVC3 Track2 (Contactless) | Key | $MDK_{IDN}$ |
| 9F66 | PUNATC Track2 (Contactless) | Key | $MDK_{CVC3}$ |
| 9F67 | NATC Track2 (Contactless) | | |
| 56 | Track1 Data (Contactless) | | |
| 9F6B | Track2 Data (Contactless) | | |

Migration Forum

# Chip security provides both card stock security and transaction security

## Pre-issuance Security

## Transaction Security

### Card Stock Security



- EMV Card Configuration Data
- 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

Online Transaction Security
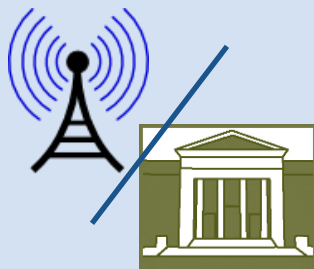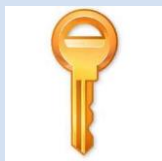
1 Online Card Authentication (Online CAM)

2 New Message Data for Authorization Assessment

EMV® Migration Forum

# On-line CAM (Card Authentication)



EMV transaction data

EMV transaction data

EMV transaction data

ARQC

ARPC

ARQC

ARPC

Payment Brand

Acquirer System

Online Request (ARQC)

ARPC

Dynamic Authentication Code

3DES cryptography Shared Key

Issuer Auth System

Hardware Security Module and Key Management System

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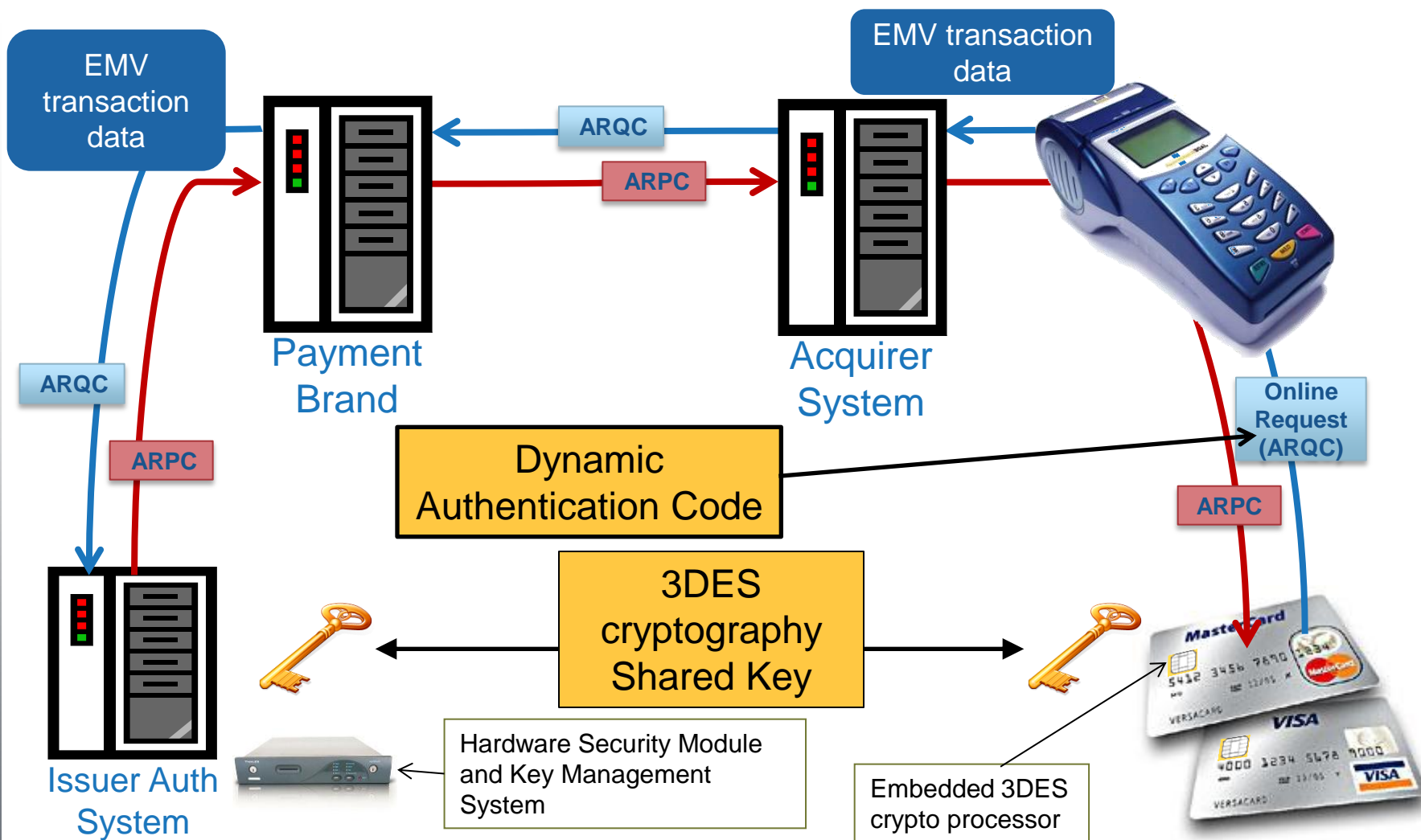
# EMV message data also increases online fraud detection security



**Field/DE 55**

**Payment Brand**

**Field/DE 55**

**Acquirer System**

**Issuer Auth System**

New EMV authentication data

VISA
Visa payWave

MasterCard
paypass
5412 3456 7890 1234
JOHN SMITH

**EMV**
Migration Forum
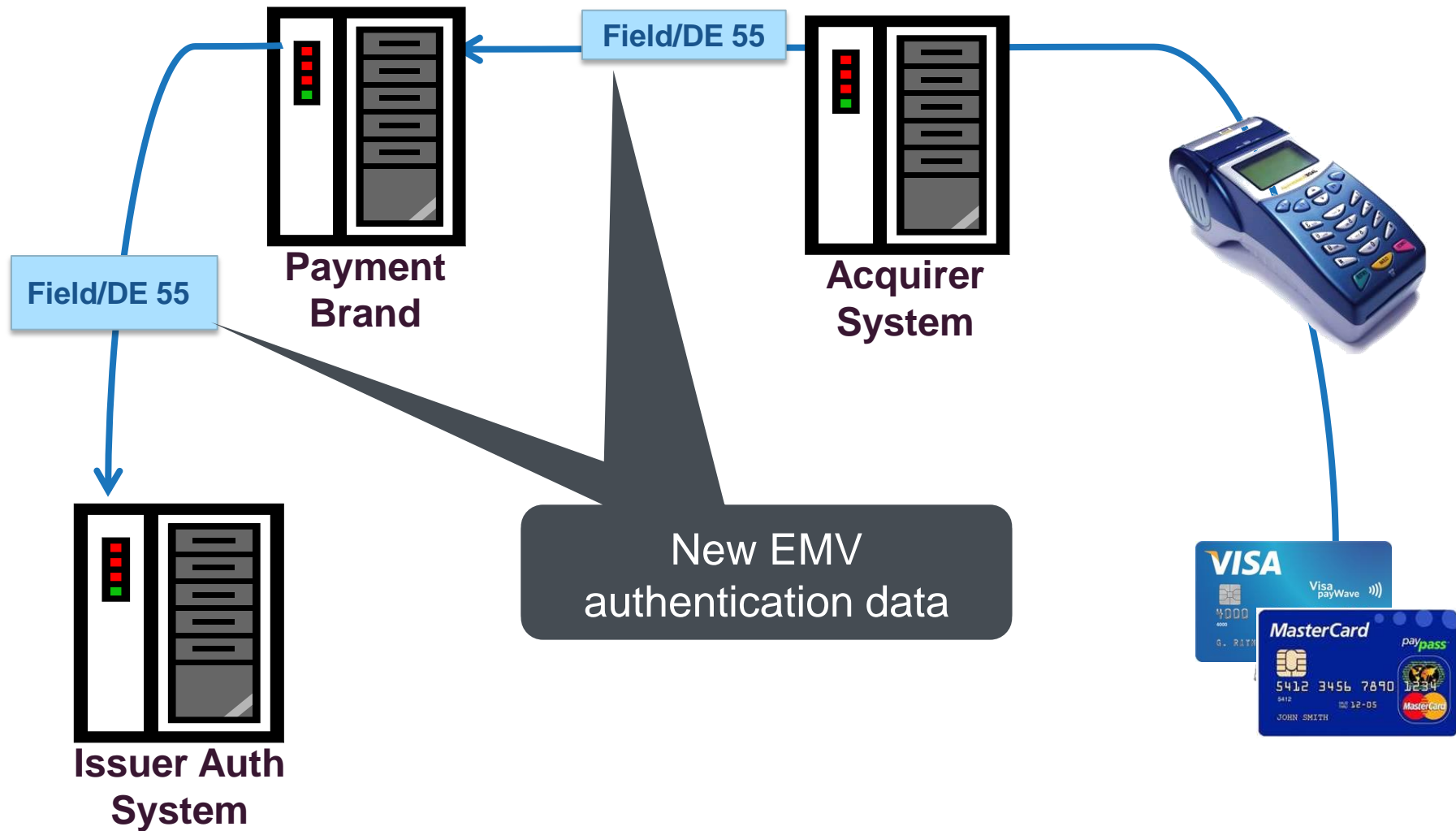
# New EMV data in the authorization message enhances authorization decisioning

## ISO 8583 – Field or DE 55

| |
|---|
| Application Cryptogram |
| Cryptogram Information Data |
| Issuer Application Data |
| Application Interchange Profile |
| Terminal Verification Result |
| Terminal Capabilities |
| Cardholder Verification Method Results |
| Unpredictable Number |
| Application Transaction Counter |
| Amount, Authorized (Numeric) |
| Transaction Currency Code |
| Transaction Date |
| Transaction Type |
| Transaction Currency Code |
| Terminal Country Code |
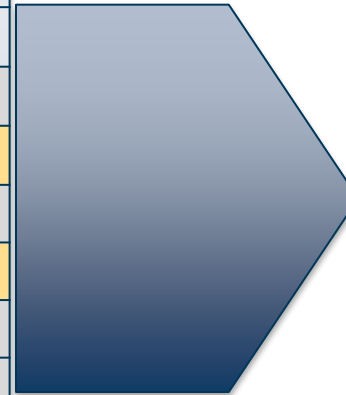
**Authorization Rules**

**Fraud Rules**

EMV® Migration Forum

# The new EMV information in the authorization message increases the issuers security tools
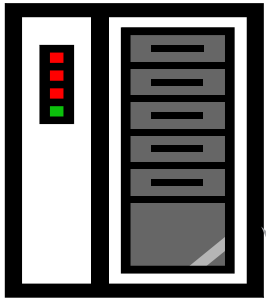
**Issuer Auth System**

**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**®
Migration Forum

# EMV Security Functions Performed Offline

**Offline Security Functions**

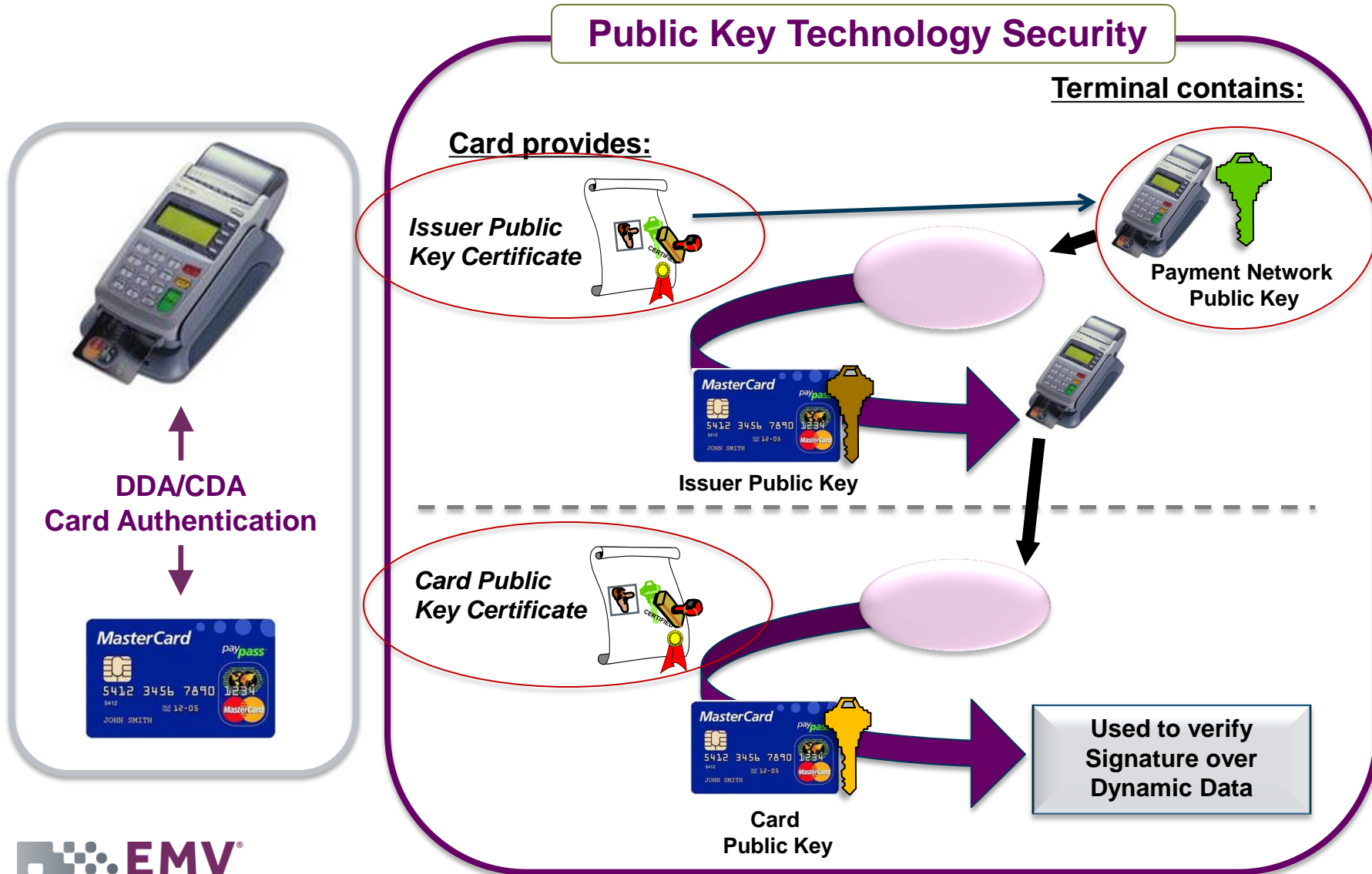Asymmetric Keys

1. **Offline Card Authentication** (Offline CAM)

2. **Offline Authorization** (Offline Transaction)

3. **Offline PIN** (Cardholder Verification Option)

EMV® Migration Forum

# EMV Offline security functions require asymmetric keys and certificates

**Public Key Technology Security**

**Terminal contains:**

**Card provides:**

*Issuer Public Key Certificate*

**Payment Network Public Key**

**Issuer Public Key**

**DDA/CDA Card Authentication**

*Card Public Key Certificate*

**Used to verify Signature over Dynamic Data**

**Card Public Key**

EMV® Migration Forum

# Offline Card Authentication (Simple Example)



**Certificate Authority**

**CA Private Key**

**CA Public Key**

Acquirer loads the Public Key to the Terminal

**CA Public Key**

**CA Private Key signs ISS Public key certificate request data**

**Offline DDA/CDA Card Authentication**

**Issuer PK Certificate**

Loaded to the card before Issuance

Authenticates the card is legitimate

Does not verify who is using it!

EMV® Migration Forum
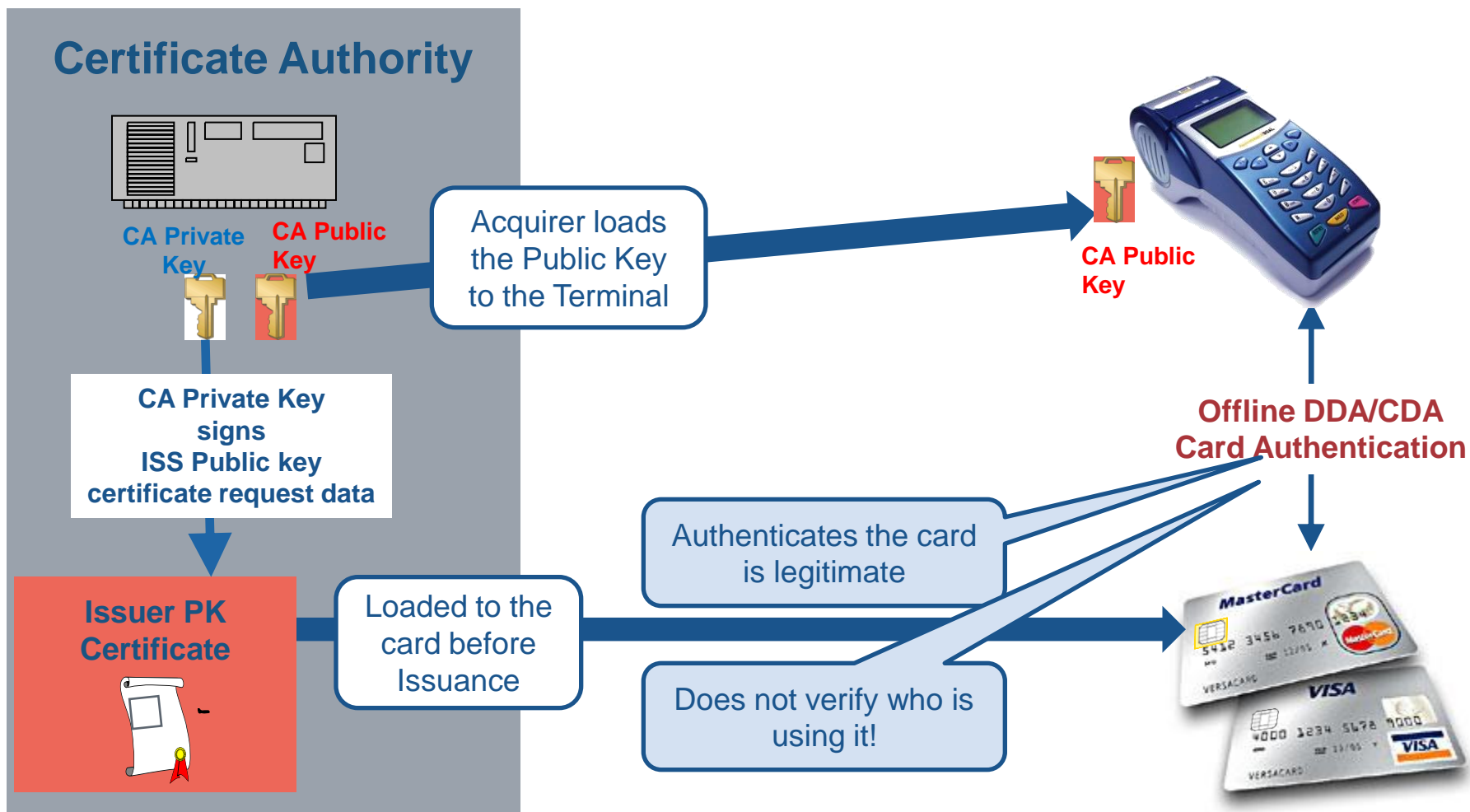
# Off-line CAM (Card Authentication Method) Options

## Offline Card Authentication Options

### DDA

- Dynamic Data Authentication
- Issuer Public Key Certificate
- ICC Public Key Certificate

### CDA

- Combined Data Authentication
- Issuer Public Key Certificate
- ICC Public Key Certificate
- Application Cryptogram (Transaction Certificate)

**Card (Chip) Level Certificate**

**Dynamic offline card authentication is unique per transaction**

EMV®
Migration Forum

# 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 Limit
Upper Consecutive Offline Limit

Lower Consecutive Offline Amount
Upper Consecutive Offline Amount

> Offline Authorization Parameters

PIN
PIN Try Limit
PIN Try Counter

Issuer Action Codes
Card Issuer Action Codes

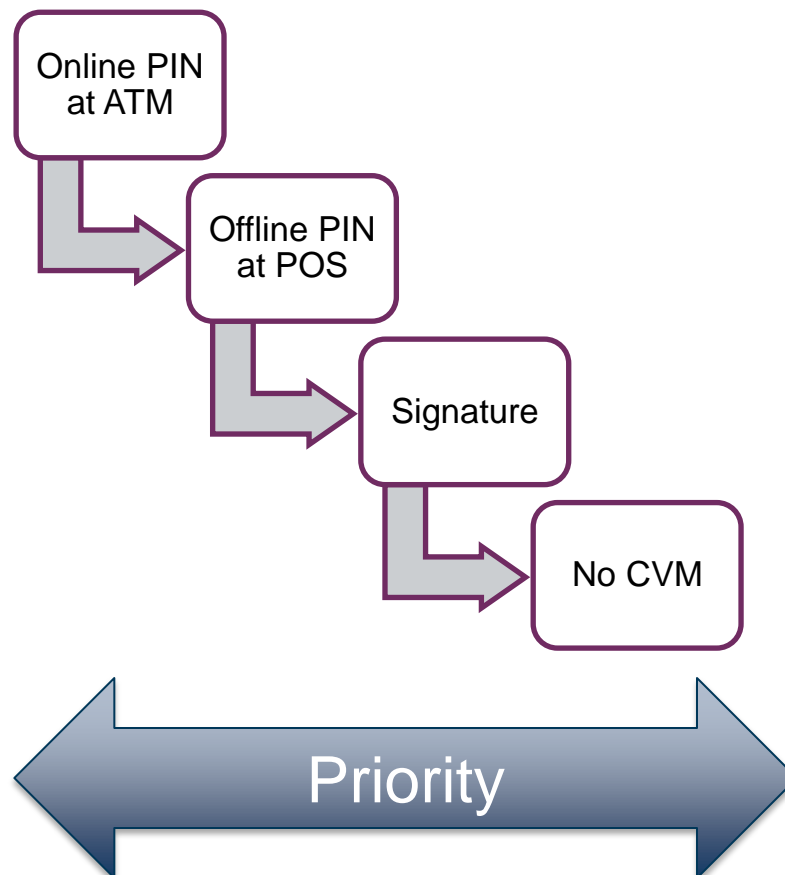**EMV** Migration Forum

# 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

EMV®
Migration Forum

# Card profiles and terminal profiles work together to determine the method of cardholder verification

**Terminal Capability Profile**

| |
|---|
| **POS Terminal** |
| Signature |
| No "Offline PIN" support |
| No "Online PIN" support |

**Card CVM List**

CVM 1 — Online PIN for ATM

CVM 2 — Online PIN

CVM 3 — Signature

CVM 5 — No CVM

**EMV**® Migration Forum

# Terminal Perspective – EMV Logic Impact

Each Brand requires
EMV terminal certification

Consumer Prompting Logic

| Visa EMV Config Data, processing rules and AIDs | MC EMV Config Data, processing rules and AIDs | AMEX EMV Config Data, processing rules and AIDs | Discover EMV Config Data, processing rules and AIDs | Other Config Data, processing rules and AIDs |
|---|---|---|---|---|

## EMV Contact Kernel
**EMV terminal functions that EMV Co tests against the EMV standards and certifies**
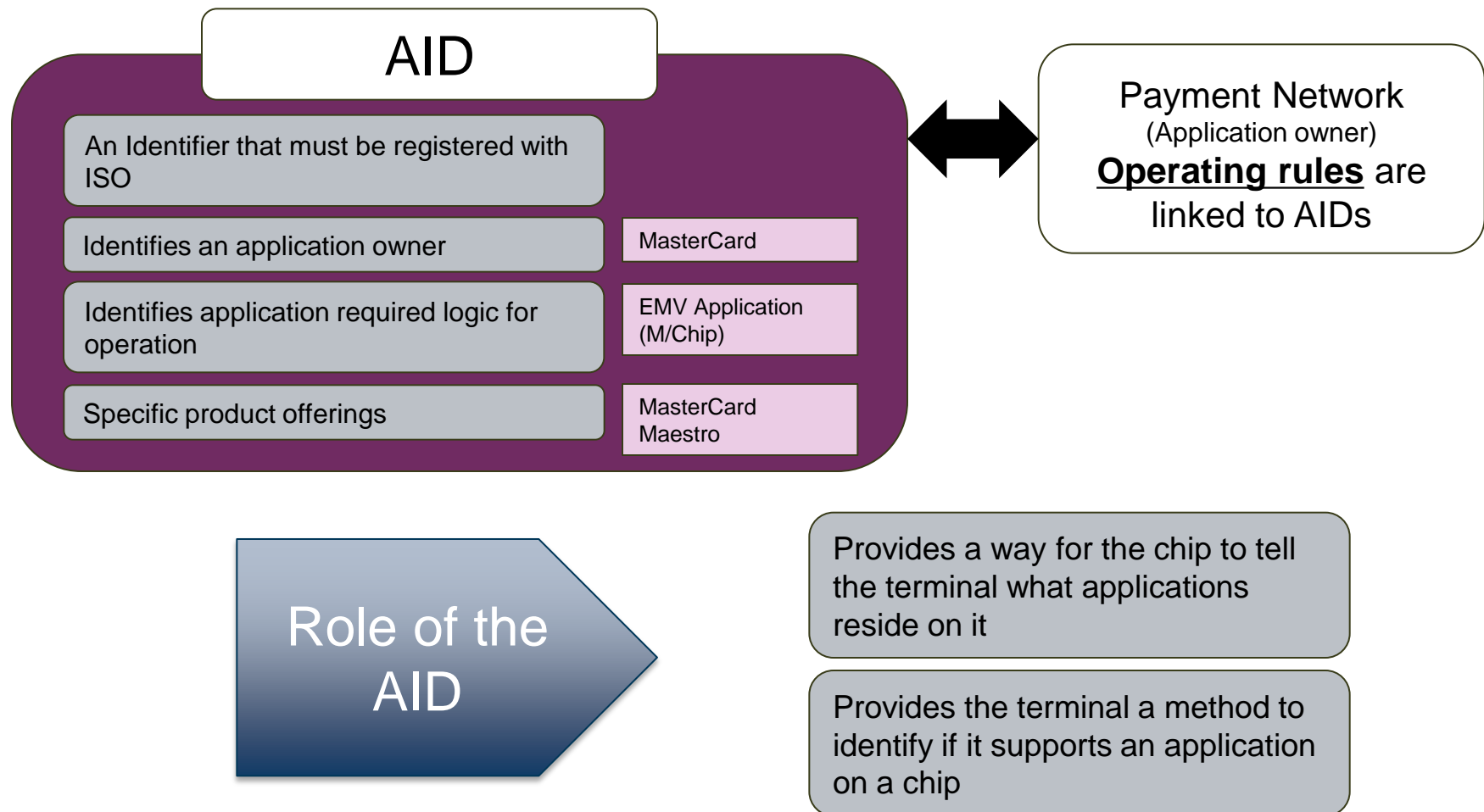
## Terminal Operating System

# Acquirers are required to Brand certify each terminal type that they deploy
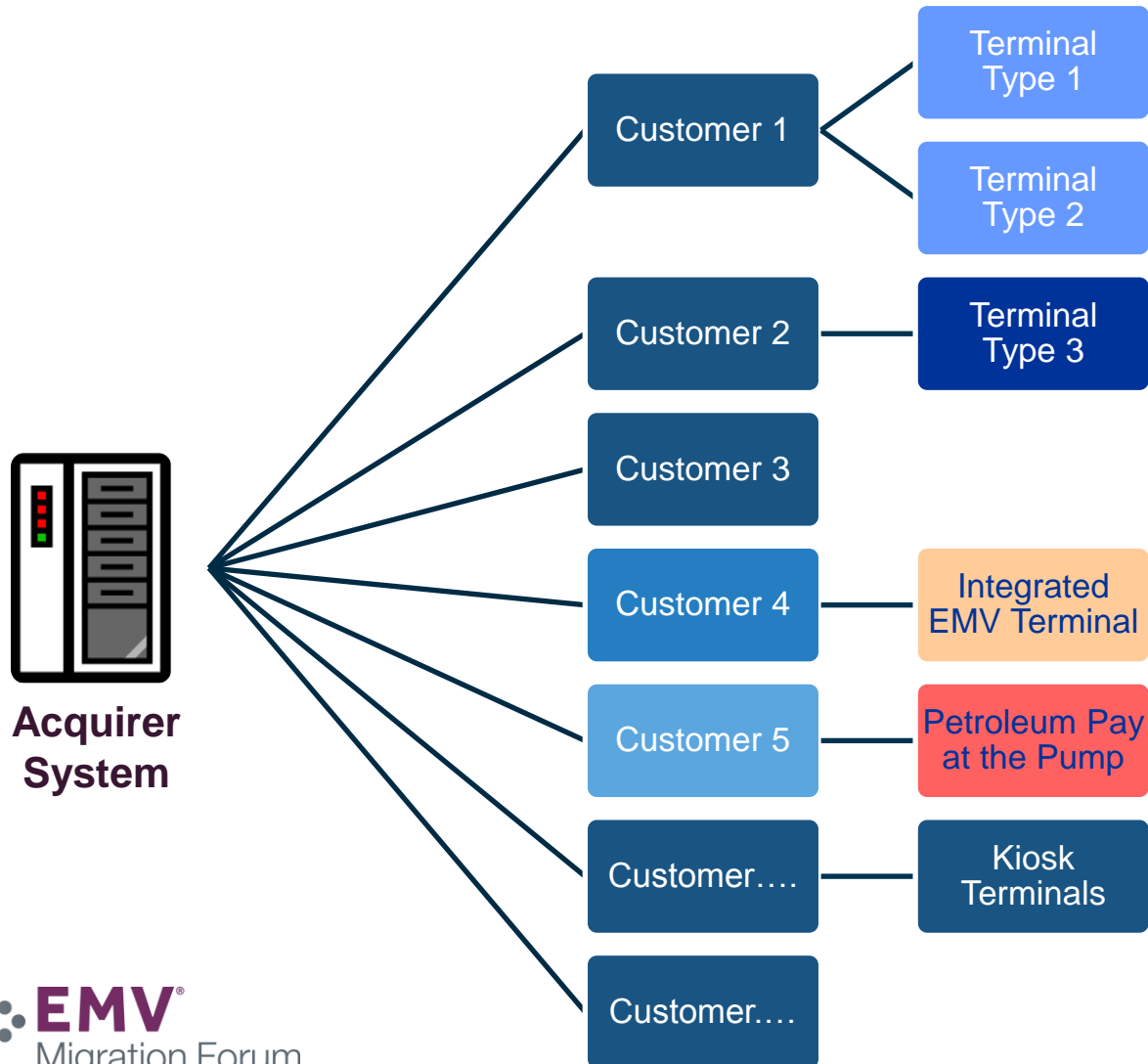
# The AID provides a method for the terminal to recognize what applications exist on a chip card

**So what is an AID?**

## AID

- An Identifier that must be registered with ISO
- Identifies an application owner
- Identifies application required logic for operation
- Specific product offerings

MasterCard

EMV Application (M/Chip)

MasterCard Maestro

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

EMV Migration Forum

# 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

| List of AIDs supported by the terminal | |
|---|---|
| MC Debit/Credit AID | A0000000041010 |
| MC U.S. Maestro Common AID | A0000000042203 |
| Visa | A0000000031010 |
| Visa U.S. Common AID | A0000000980840 |
| Discover AID | A0000003241010 |

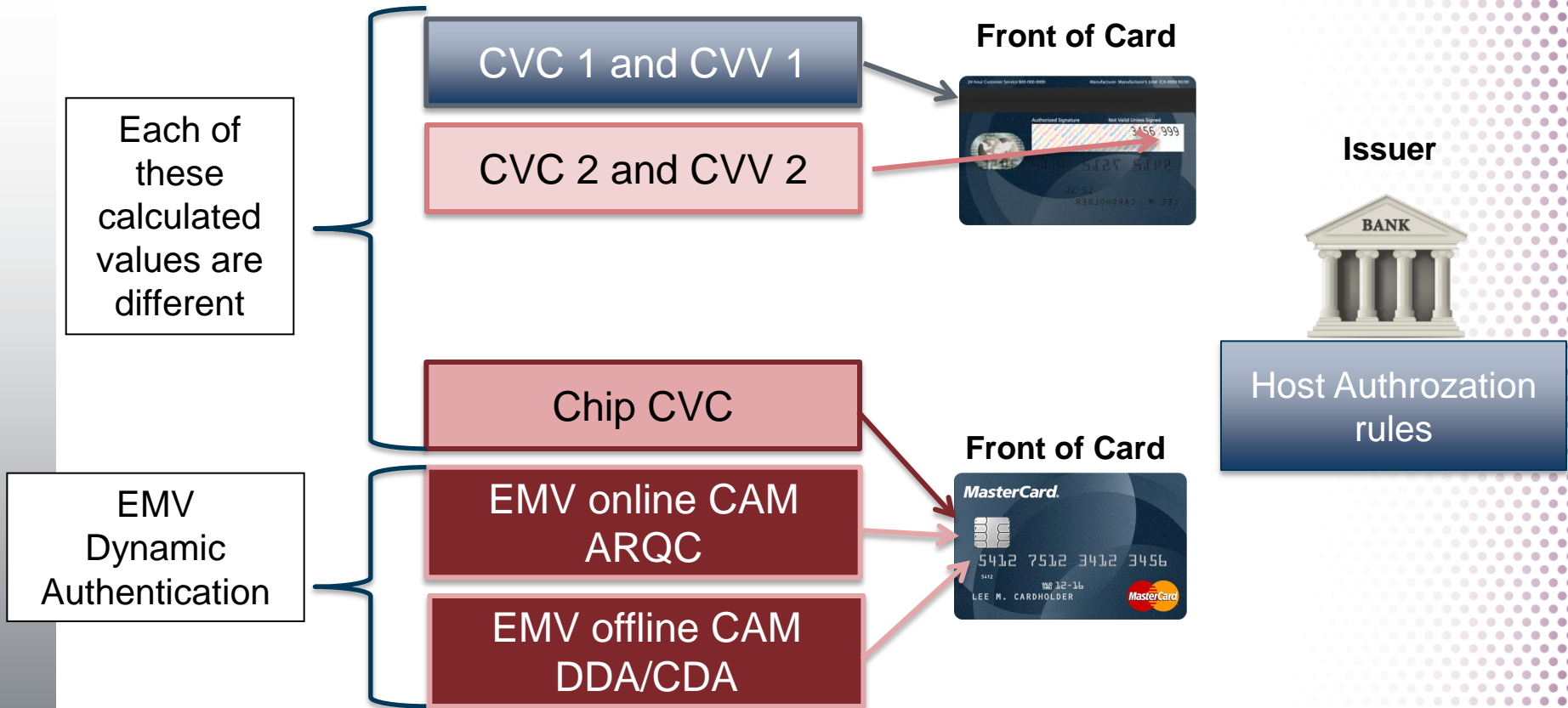Logic and configuration data specific to each AID must be added to the terminal

**EMV**
Migration Forum

# All stakeholders need to migrate to receive the full benefit of EMF

**Issuer**

EMV Messaging

**Acquirer**

- ✓ **New card data**
- ✓ **New messaging data**
- ✓ **New application logic**
- ✓ **New configuration settings**
- ✓ **Enhanced authorization/fraud strategies**

**Card / Device**

*NFC*

*EMV*

*Contactless*

**Terminal**

*Contact*

**EMV**® Migration Forum

# EMV leverages card, terminal, messaging and host system security technology to protect against counterfeit fraud

Each of these calculated values are different

- CVC 1 and CVV 1
- CVC 2 and CVV 2

**Front of Card**

EMV Dynamic Authentication

- Chip CVC
- EMV online CAM ARQC
- EMV offline CAM DDA/CDA

**Front of Card**

**Issuer**

BANK

Host Authrozation rules

**EMV** Migration Forum

# Q&A

- Randy Vanderhoof, rvanderhoof@us-emvforum.org
- Guy Berg, guy_berg@mastercard.com

**EMV®**
Migration Forum

WWW.EMV-CONNECTION.COM