EMV 101

EMV Migration Forum Webinar
May 7, 2014

EMV® Migration Forum

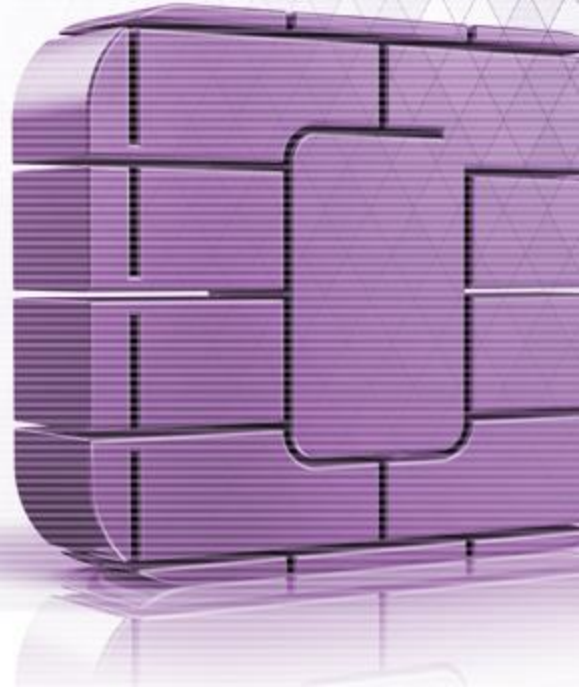
Introduction

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.



EMV® Migration Forum

Today's Webinar Topics & Speakers

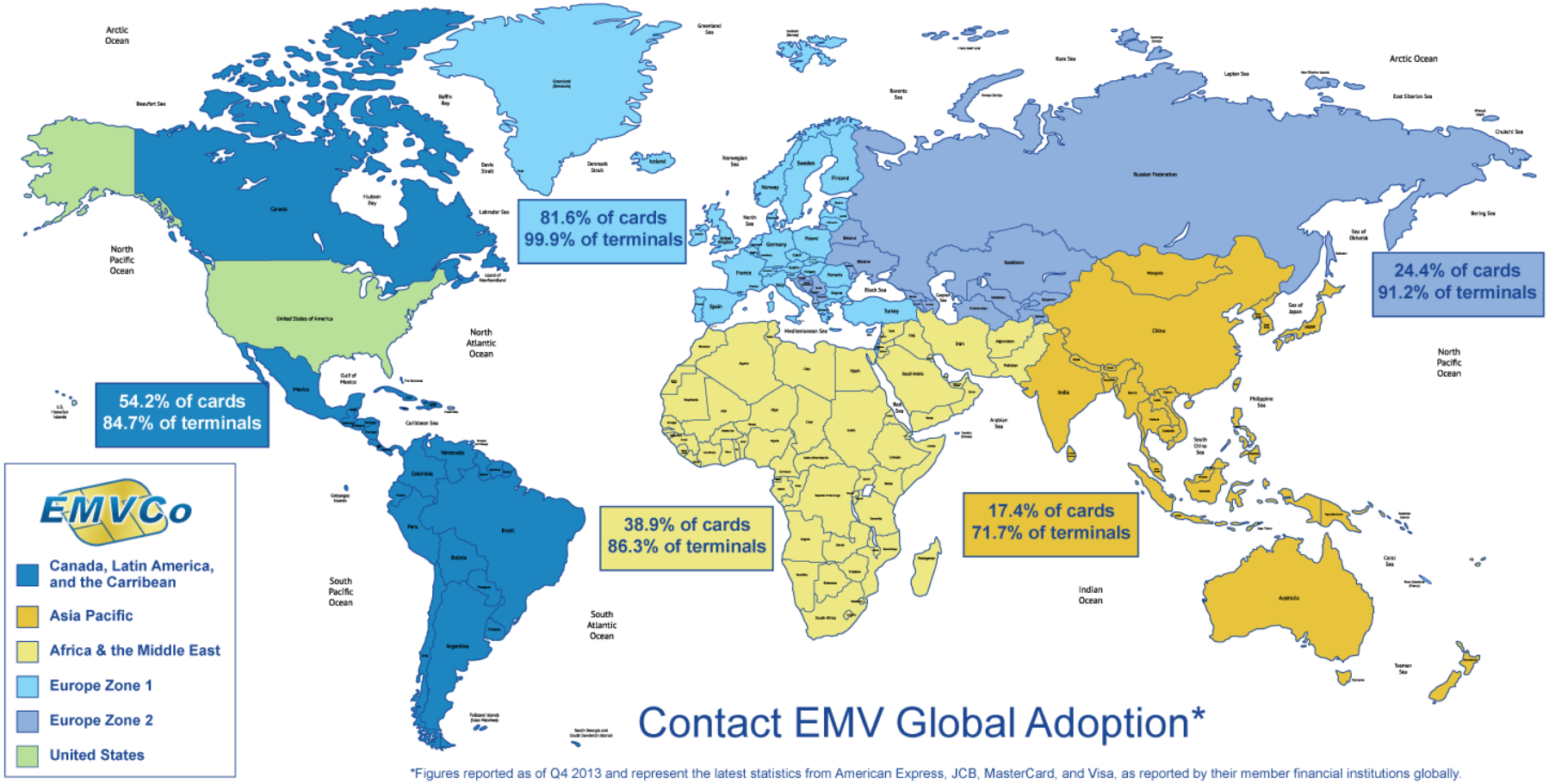
- **Introduction & EMV Implementation Status**: Cathy Medich, Director - Programs, EMV Migration Forum

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

- **Q&A**

EMV® Migration Forum

Global EMV Adoption*: 2.37 Billion Cards and 36.9 Million EMV Terminals



*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.

EMV Migration Forum

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

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® Migration Forum

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 Compromise and Skimming Protection Mechanisms

III. EMV Application Fundamentals

- On-line Card Authentication
- Off-line Card Authentication
- Offline Authorization
- Risk Management
- Cardholder Verification Method

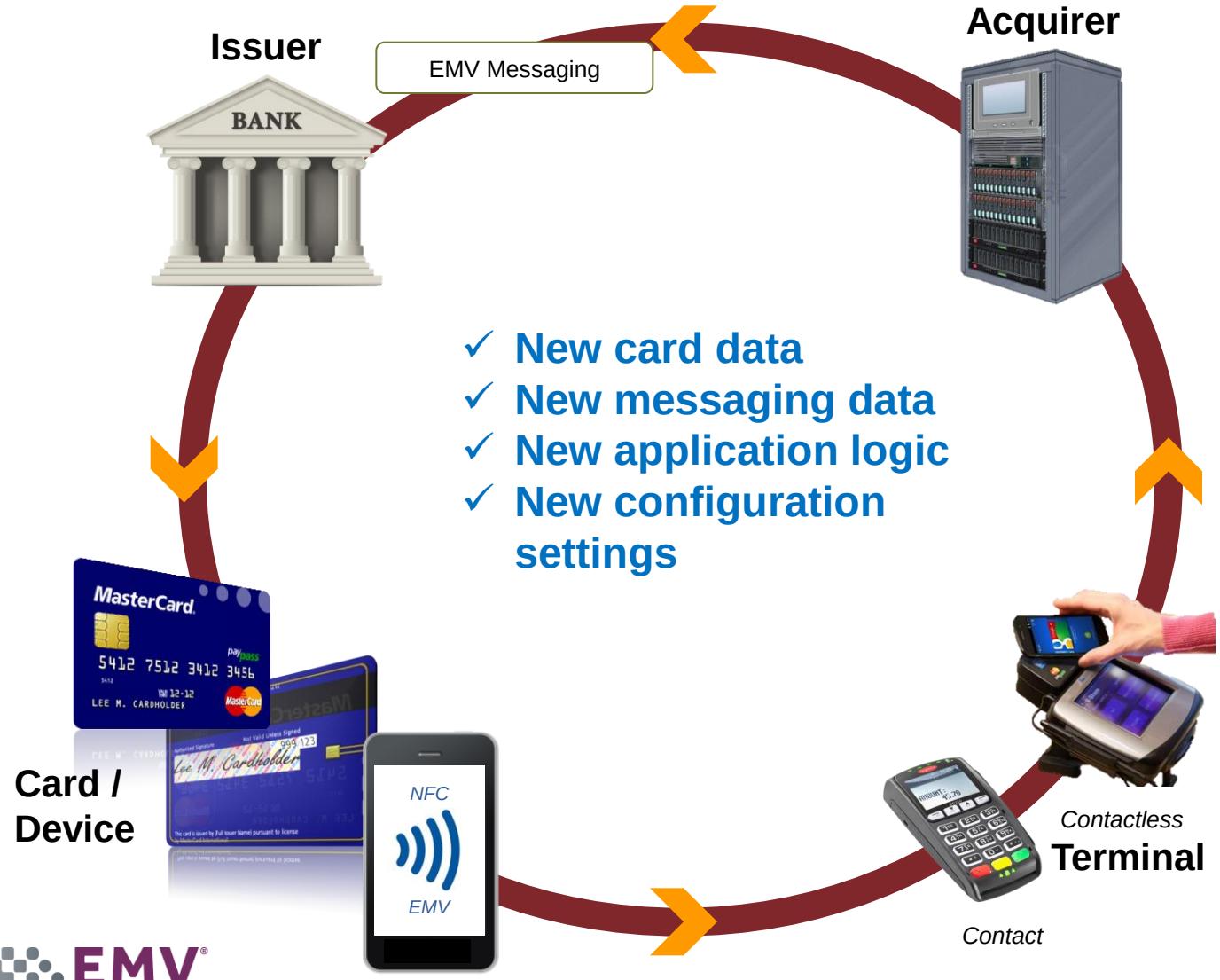
IV. EMV from a Terminal Perspective

- Terminal Application and Approvals

V. EMV Debit Support

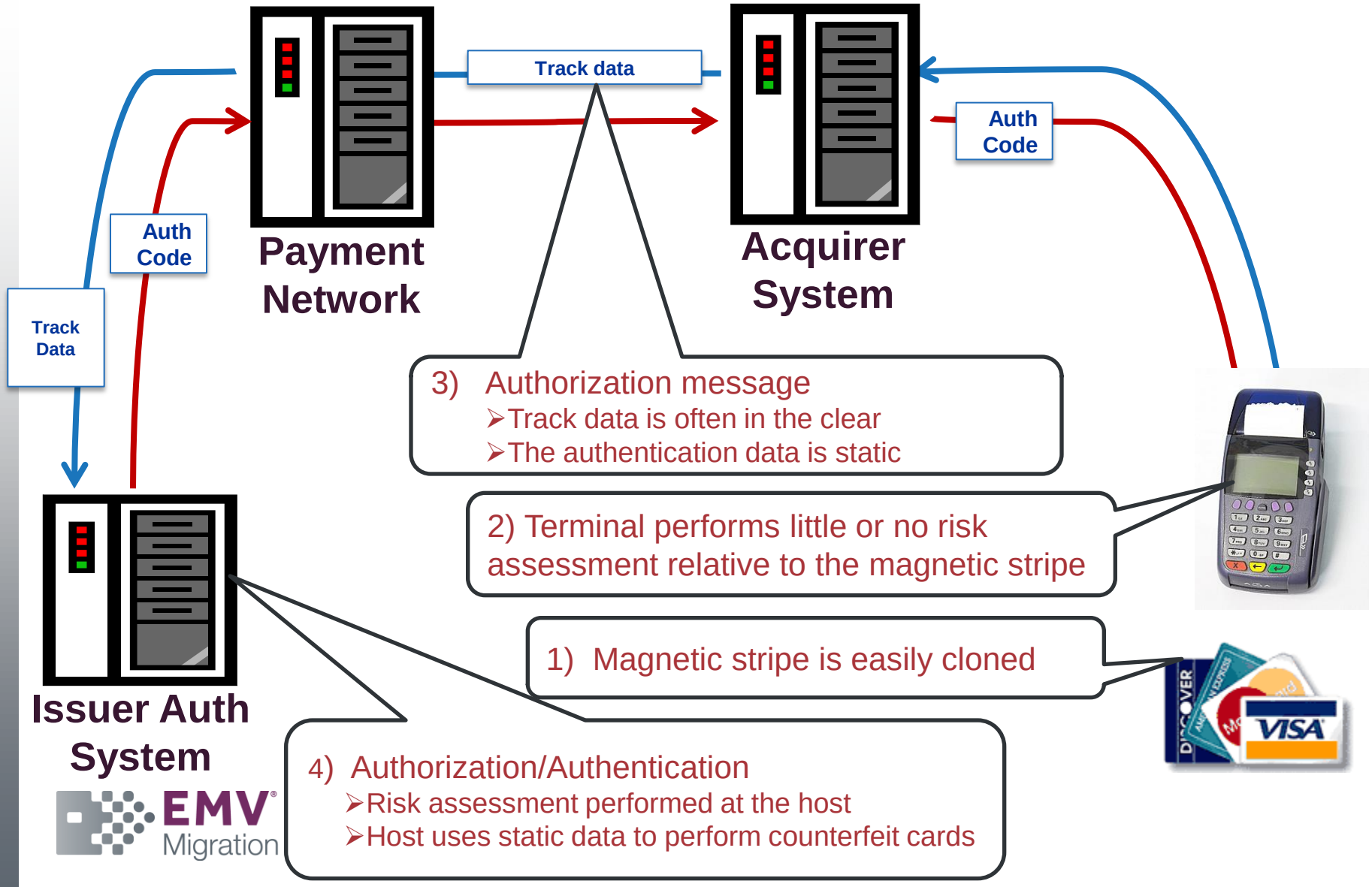
EMV® Migration Forum

EMV migration impacts all stakeholders involved in payment transaction processing

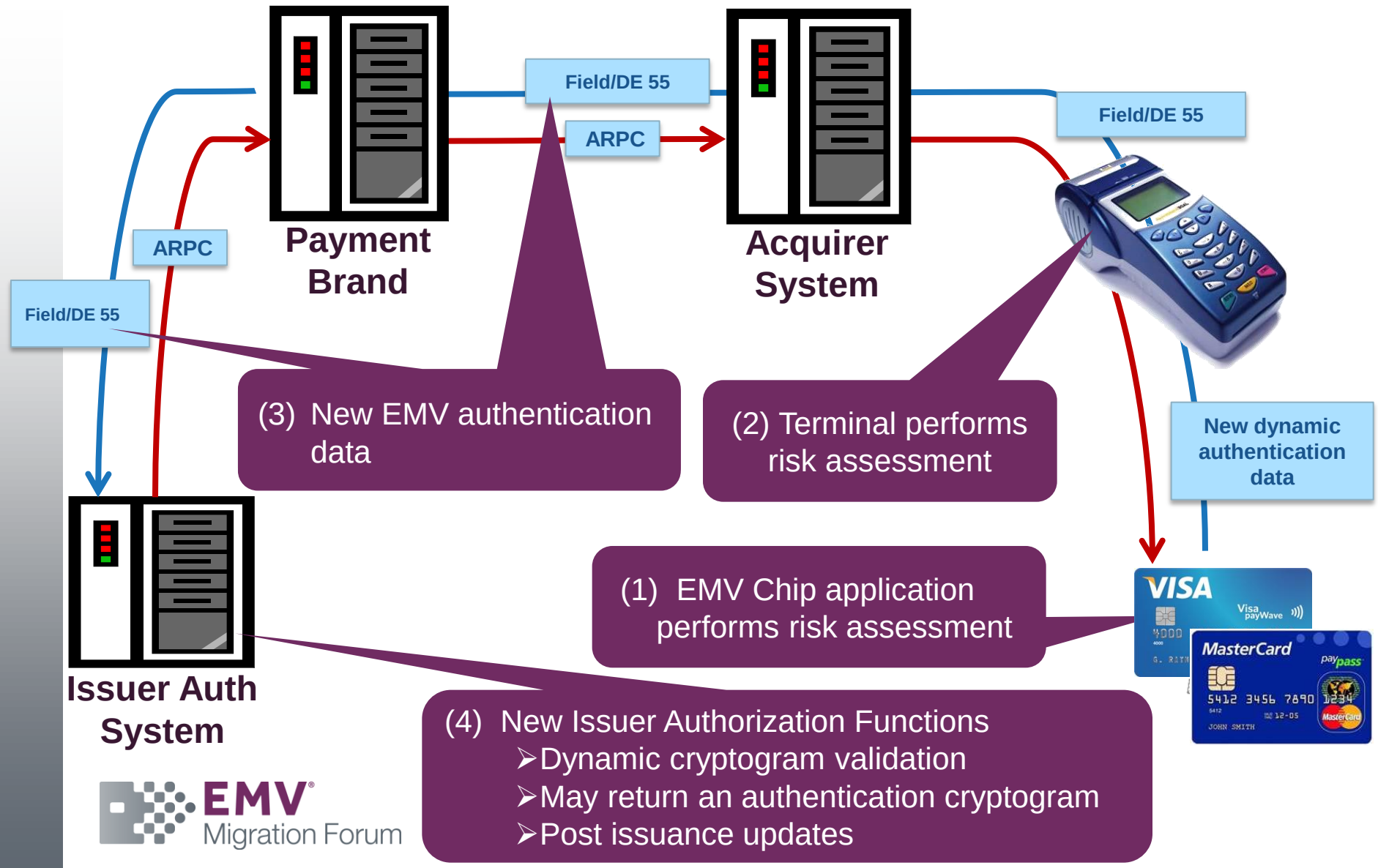


EMV Migration Forum

Magnetic Stripe Transactions use static authentication data that can be skimmed

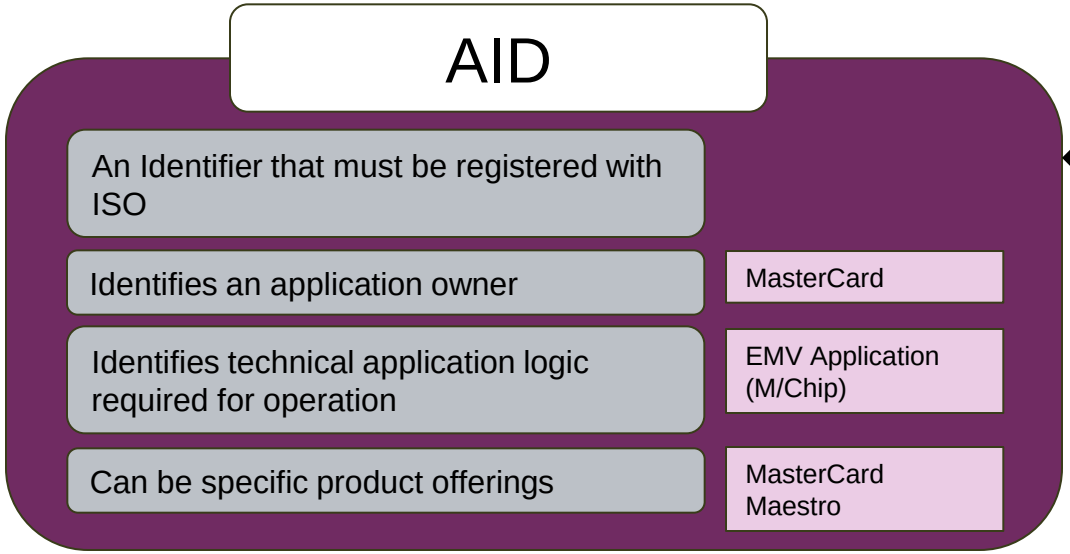


EMV Transaction Processing Introduces dynamic authentication that makes copied data useless at POS



The AID provides a method for the terminal to recognize what applications exist on a chip card

So what is an AID?



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 terminal and card each maintain a list of AIDs that they support

The terminal keeps a list of AIDs that it can support

Application Selection Process

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

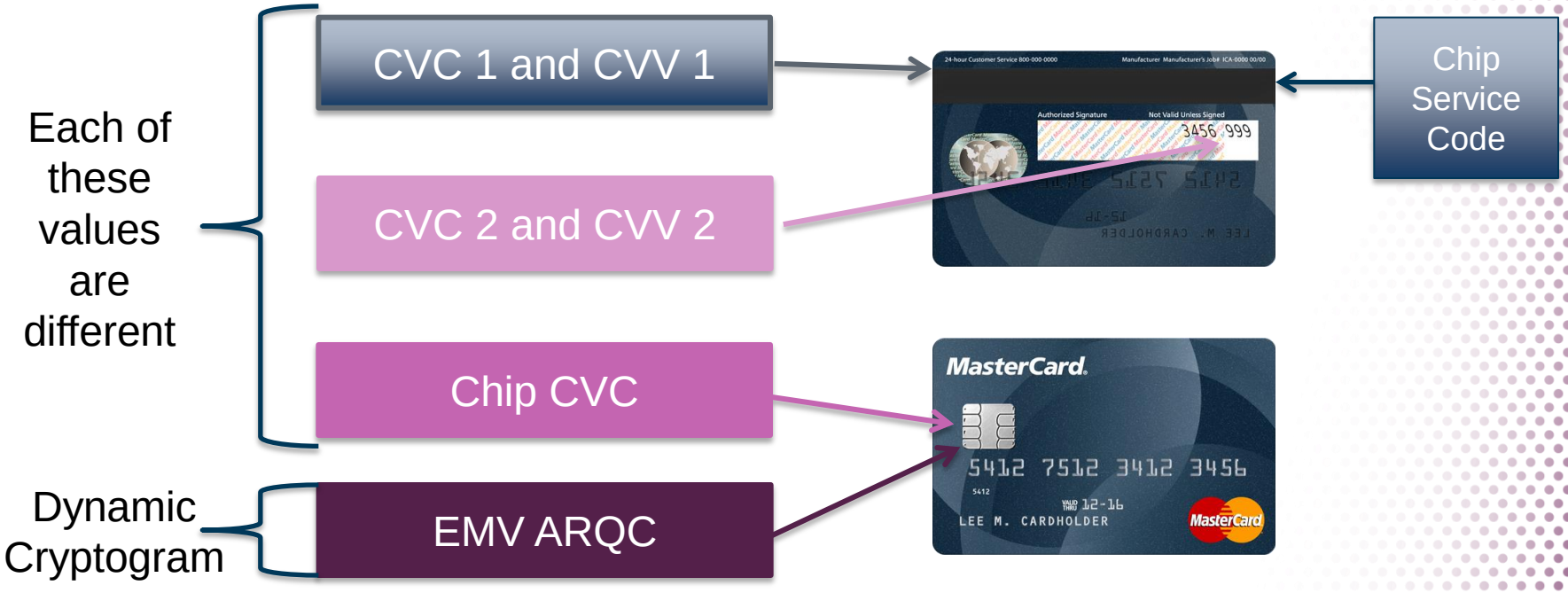
Logic and configuration data specific to each AID must be added to the terminal

EMV Migration Forum

EMV Tag	Chip Data	EMV Tag	Chip Data
42	Issuer Identification Number (IIN)	9F 07	Application Usage Control
4F	Application Dedicated File (ADF) Name	9F 08	Application Version Number (CARD)
50	Application Label	9F 0B	Cardholder Name Extended
57	Track2 Equivalent Data	9F 0D	Issuer Action Code (IAC) - Default
5A	Application Primary Account Number (PAN)	9F 0E	Issuer Action Code (IAC) – Denial
5F 20	Cardholder Name	9F 0F	Issuer Action Code (IAC) – Online
5F 24	Application Expiration Date	9F 11	Issuer Code Table Index
5F 25	Application Effective Date	9F 12	Application Preferred Name
5F 28	Issuer Country Code	9F 1F	Track1 Discretionary Data
5F 2D	Language Preference	9F 20	Track2 Discretionary Data
5F 30	Service Code	9F 2D	ICC PIN Encipherment Public Key Certificate
5F 34	Application PAN Sequence Number	9F 2E	ICC PIN Encipherment Public Key Exponent
5F 50	Issuer URL	9F 2F	ICC PIN Encipherment Public Key Remainder
5F 53	International Bank Account Number (IBAN)	9F 32	Issuer Public Key Exponent
5F 54	Bank Identifier Code (BIC)	9F 38	Processing Options Data Object List (PDOL)
5F 55	Issuer Country Code (Alpha2 Format)	9F 3B	Application Reference Currency
5F 56	Issuer Country Code (Alpha3 Format)	9F 42	Application Currency Code
82	Application Interchange Profile (AIP)	9F 43	Application Reference Currency Exponent
84	Dedicated File (DF) Name	9F 44	Application Currency Exponent
87	Application Priority Indicator	9F 45	Data Authentication Code (DAC)
88	Short File Identifier	9F 46	ICC Public Key Certificate
8C	Card Risk Management Data Object List (CDOL) 1	9F 47	ICC Public Key Exponent
8D	Card Risk Management Data Object List (CDOL) 2	9F 48	ICC Public Key Remainder
8E	Cardholder Verification Method (CVM) List	9F 49	Dynamic Data Object List (DDOL)
8F	Certificate Authority (CA) Public Key Index	9F 4A	Static Data Authentication (SDA) Tag List
90	Issuer Public Key Certificate (IPKC)	9F 4B	Signed Dynamic Application Data
92	Issuer Public Key Remainder	9F 4D	Log Entry
93	*Signed Static Application Data*	Key	MDK_{AC}
94	Application File Locator (AFL)	Key	MDK_{SMI}
97	Transaction Certificate Data Object List (TDOL)	Key	MDK_{SMC}
9F 05	Application Discretionary Data	Key	MDK_{IDN}
		Key	MDK_{CVC3}

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



EMV Migration Forum

Chip security provides both card stock security and transaction security

Pre-issuance Security

Card Stock Security

- EMV Card Configuration Data
- Issuance Security

Key Management

EMV Data

Transaction Security

EMV Application

Risk Management Decision Criteria

Online Security Functions

Symmetric Keys

Offline Security Functions

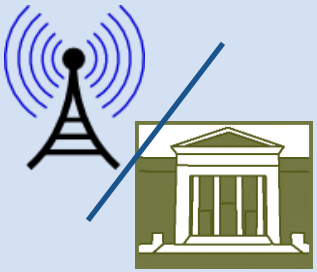
Asymmetric Keys

Cardholder Verification Methods

EMV® Migration Forum

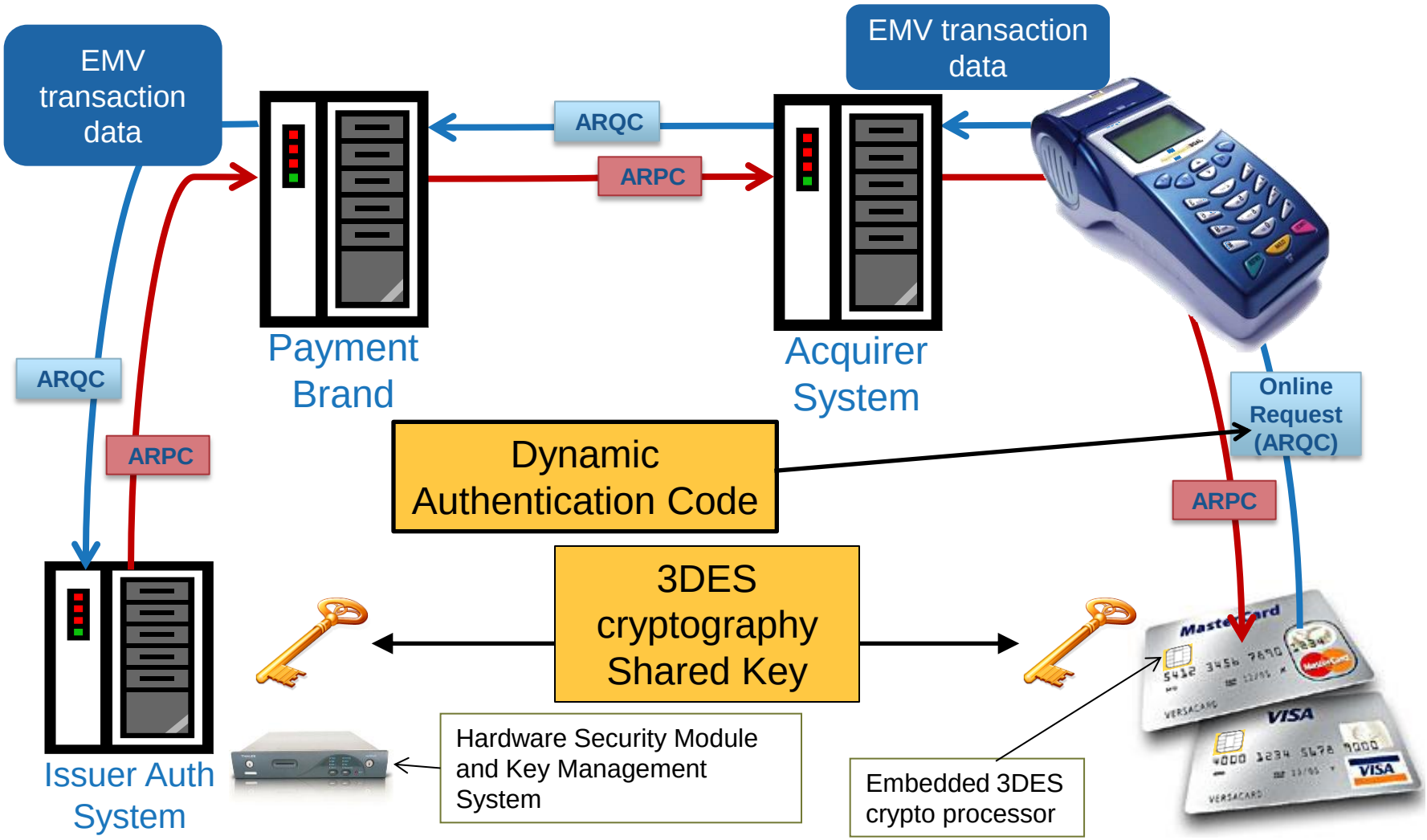
EMV security functions performed online

Online Transaction Security



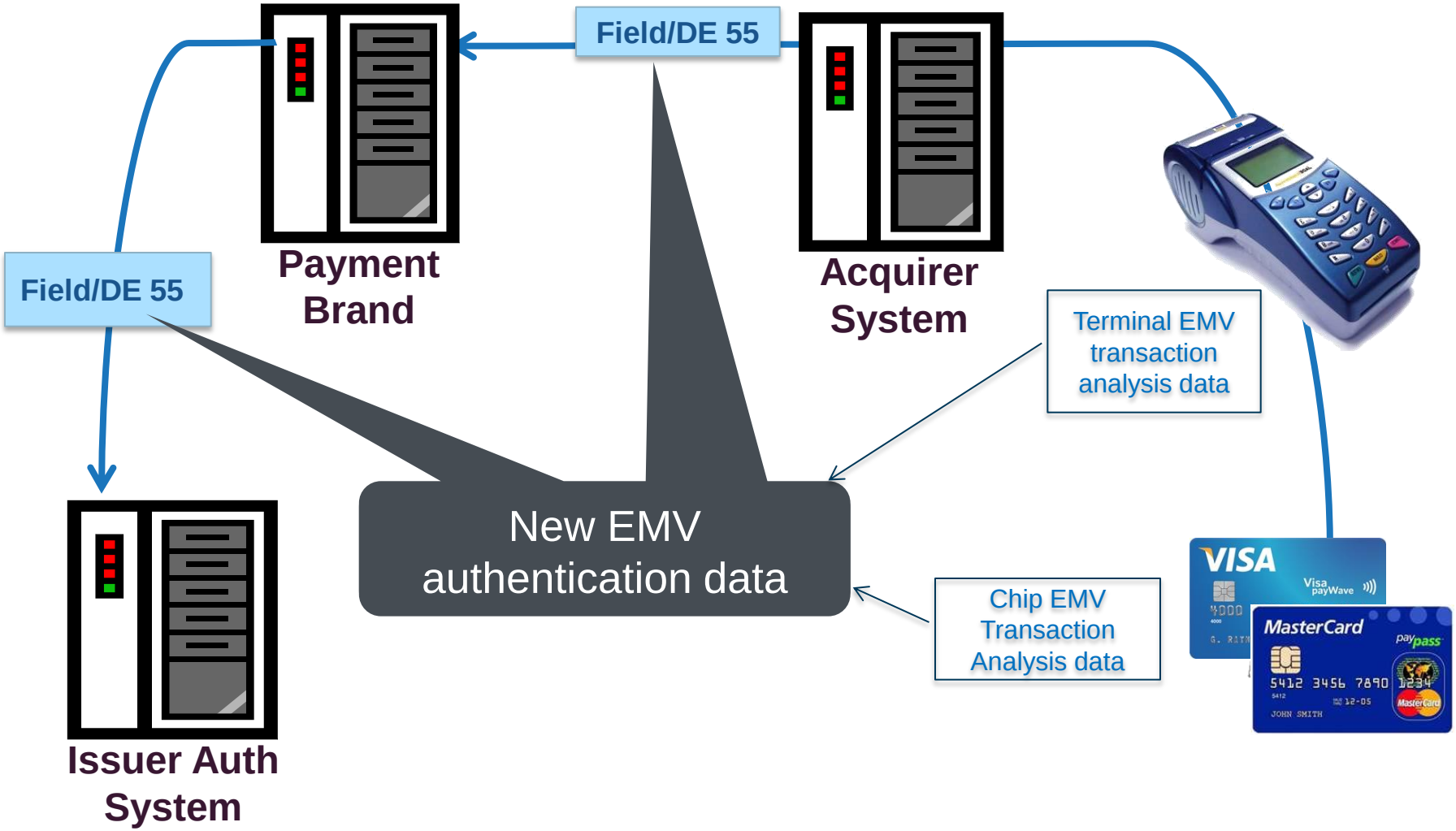
1. Online Card Authentication (Online CAM)
2. New Message Data for Authorization Assessment

On-line CAM (Card Authentication)



EMV Migration Forum

EMV message data also increases online fraud detection security

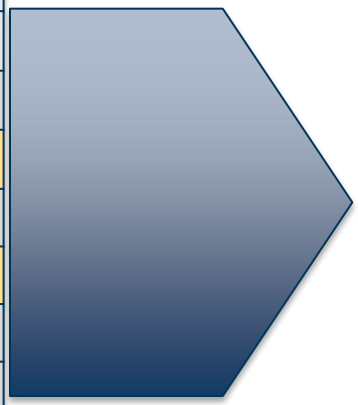


EMV Migration Forum

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

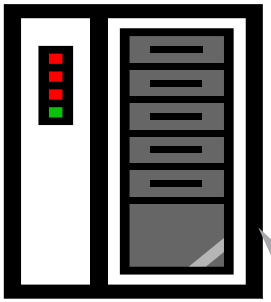


Authorization Rules

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 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® Migration Forum

EMV Security Functions Performed Offline

Offline Security Functions

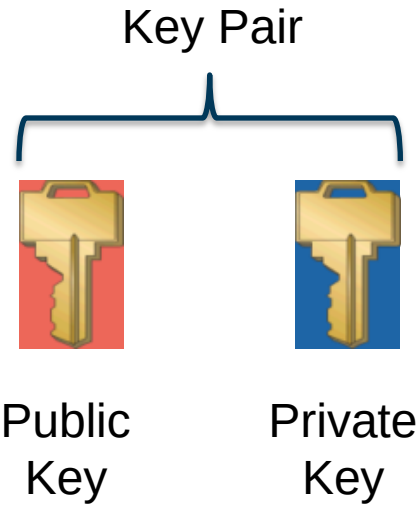
Asymmetric Keys

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

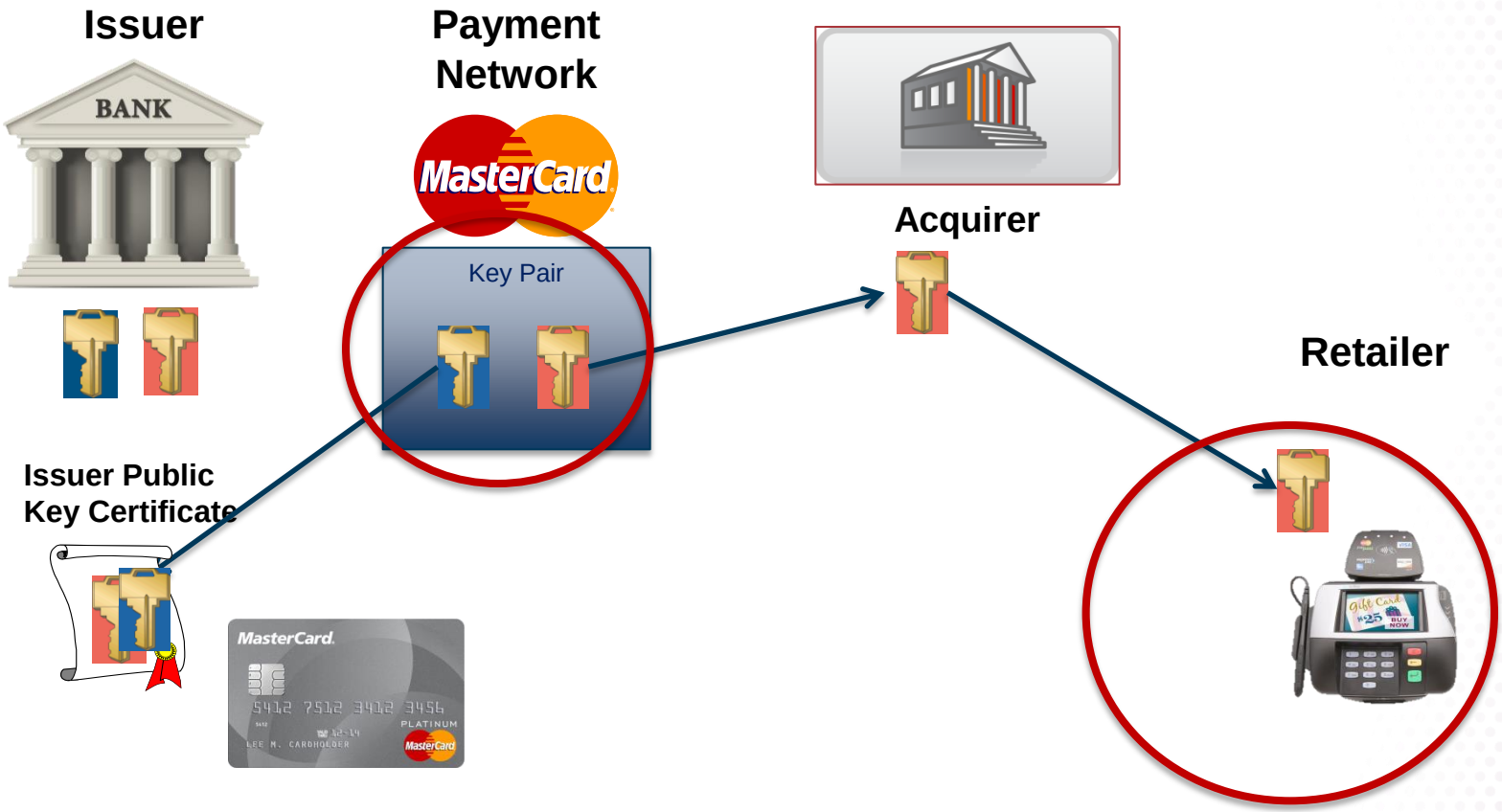
Offline Security relies upon Asymmetric Key Technology



EMV Migration Forum

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

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

Protects Against
- Counterfeiting
- Skimming

CDA

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

Protects Against
- Counterfeiting
- Skimming
- Wedge Attacks

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 Counter
Upper Consecutive Offline Counter

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

Additional Processing Rules

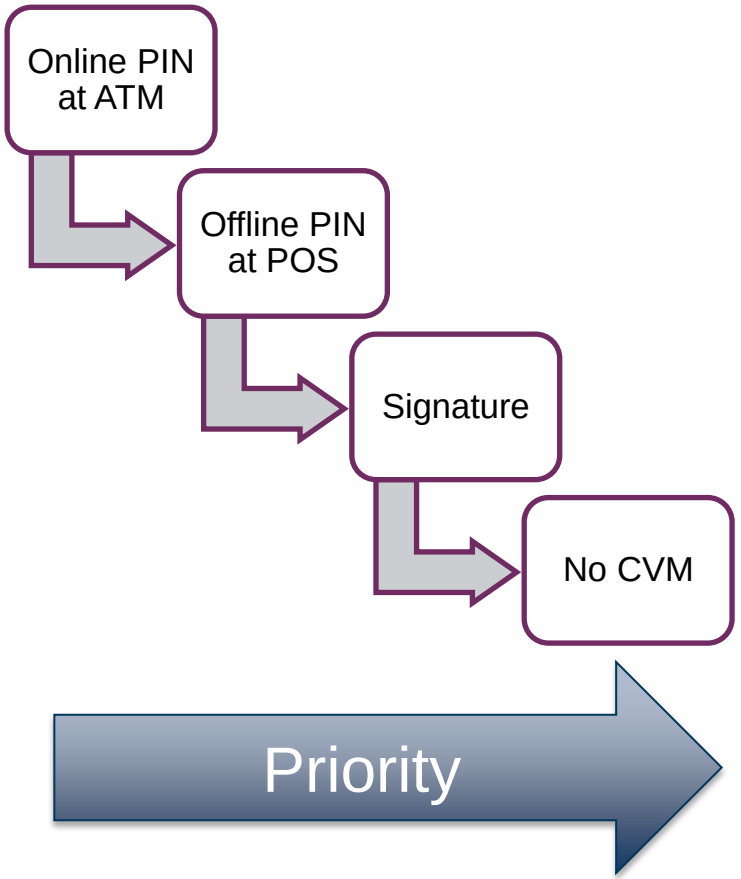
EMV Migration Forum

EMV Cardholder Verification Settings

CVM Options

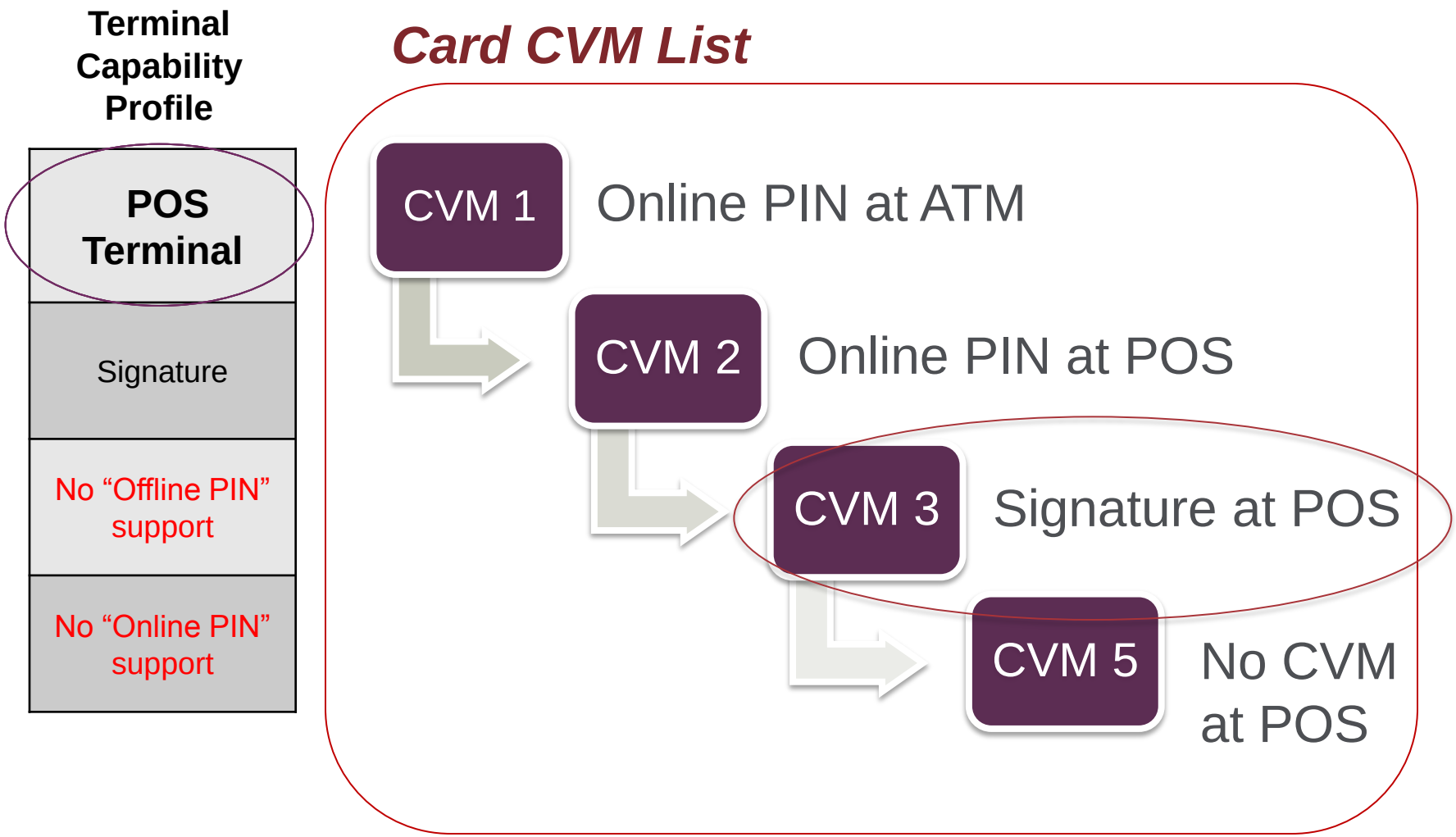
- No CVM
- Signature
- On-line PIN at ATM
- On-line PIN at POS
- Off-line PIN plain texted
- Off-line PIN enciphered

Example: CVM List Selected



EMV Migration Forum

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



EMV From a Terminal Perspective

Issuing Banks

EMV Terminals Become a Workflow Engine

Bank Specific Processing Instructions

Bank Specific Processing Instructions

Bank Specific Processing Instructions

Bank Specific Processing Instructions

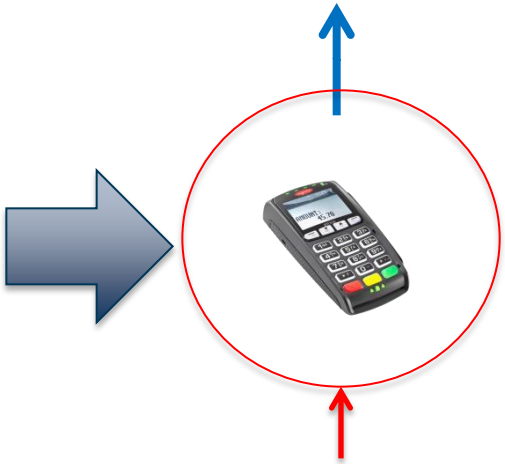
- Signature?
- Online PIN?
- Offline PIN?

- Online CAM
- Offline CAM?
  - DDA, CDA

- Offline Authorization

- Other EMV Processing Conditions?

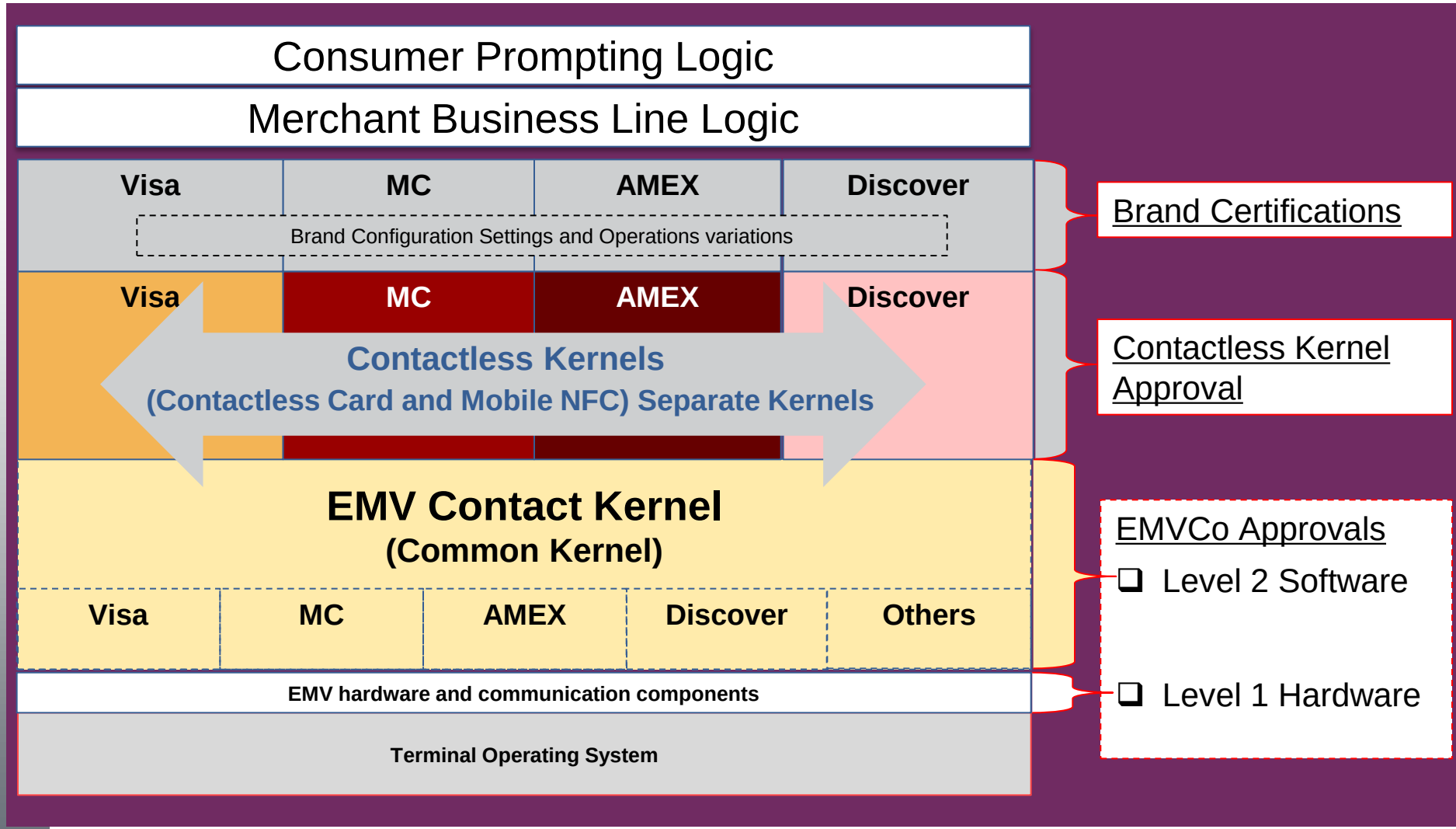
Acquirer



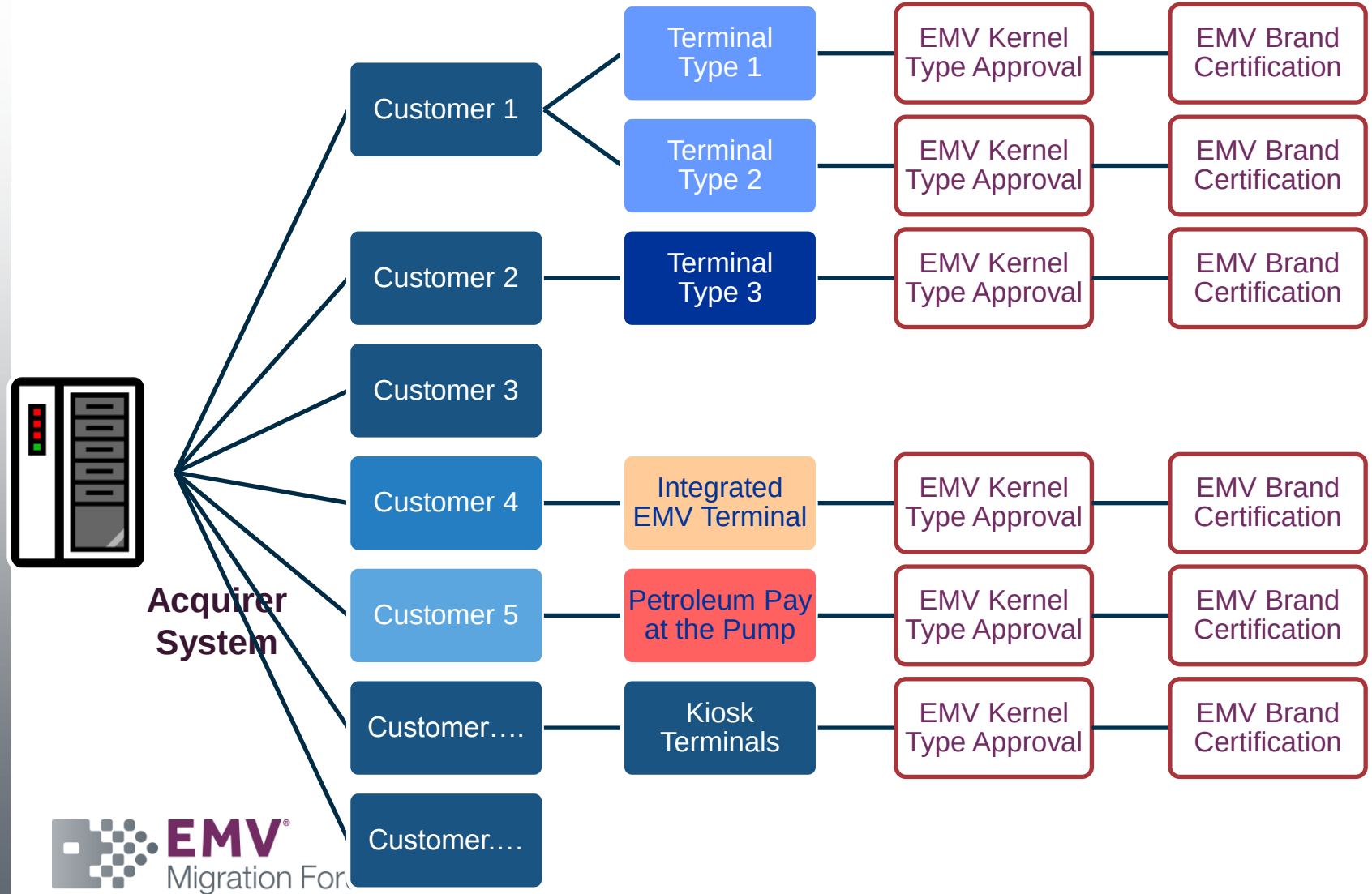
Workflow Engine

EMV Migration Forum

New EMV logic and approvals required for the terminal application



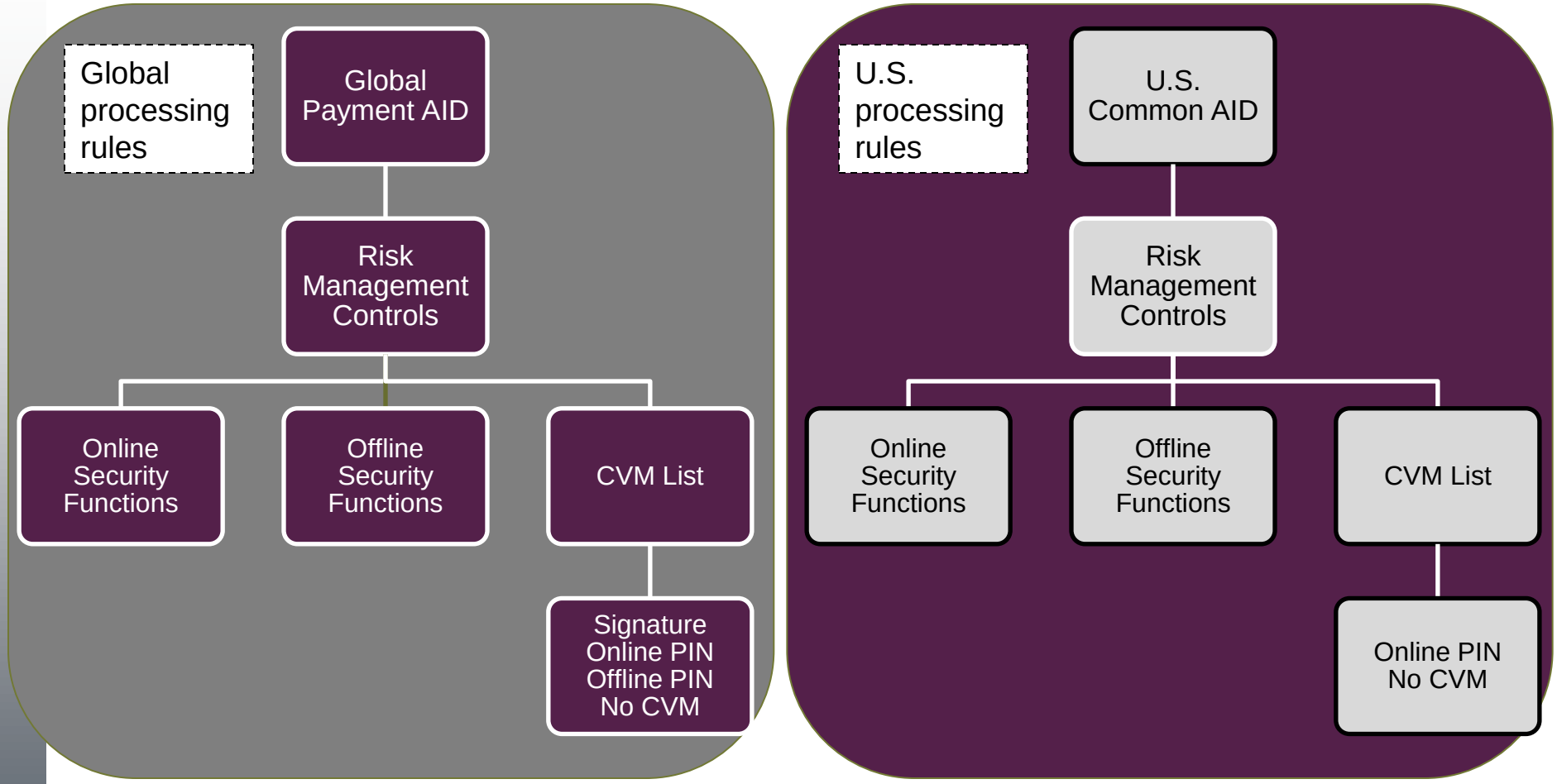
Acquirers are required to Brand Certify each terminal type that they deploy



EMV Migration For

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



EMV® Migration Forum

All stakeholders need to migrate to receive the full benefit of EMV

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

EMV® Migration Forum

- Cathy Medich, cmedich@us-emvforum.org
- Guy Berg, guy_berg@mastercard.com

EMV® Migration Forum

WWW.EMV-CONNECTION.COM