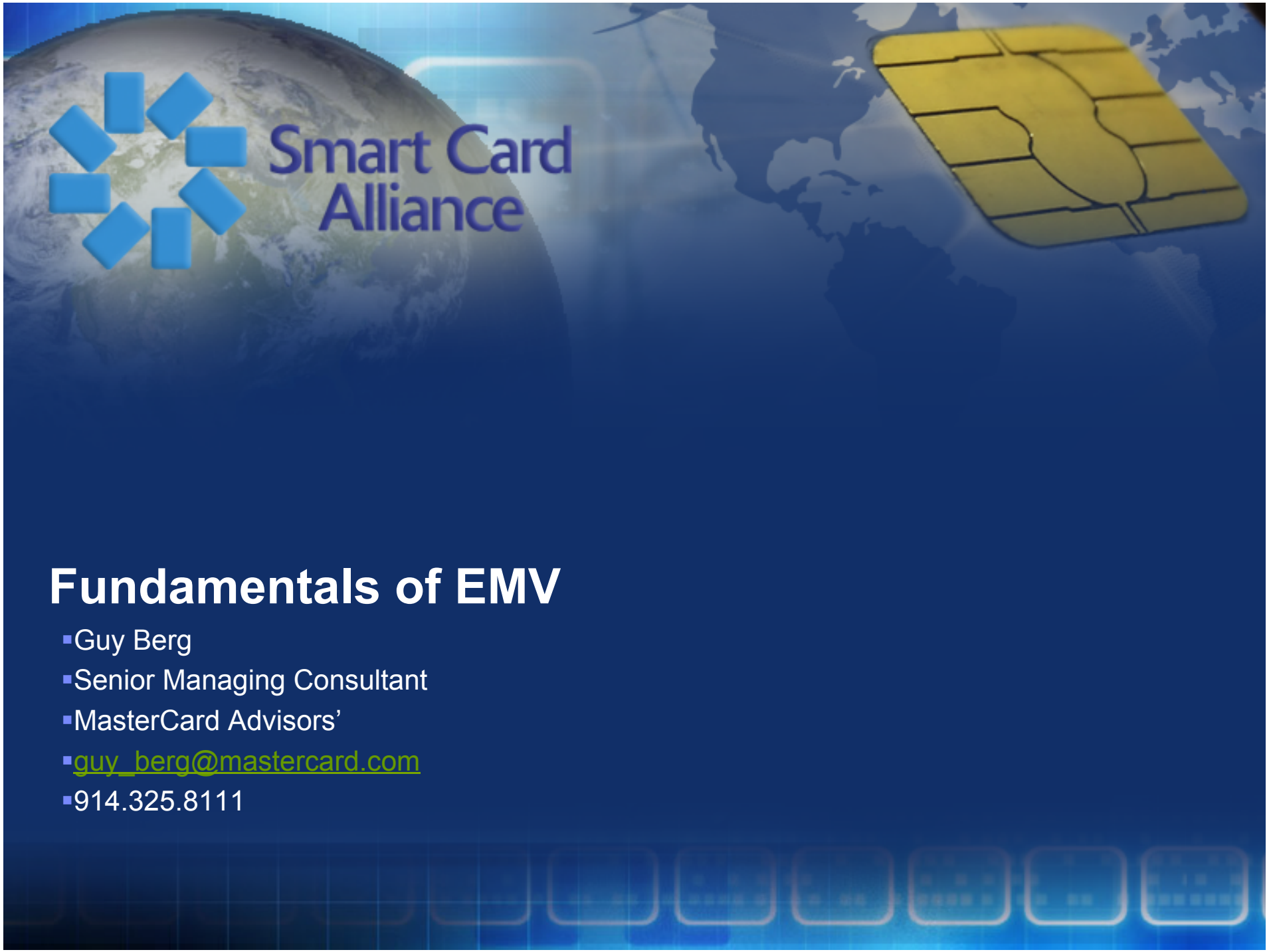


Fundamentals of EMV

- Guy Berg
- Senior Managing Consultant
- MasterCard Advisors'
- guy_berg@mastercard.com
- 914.325.8111

EMV Fundamentals

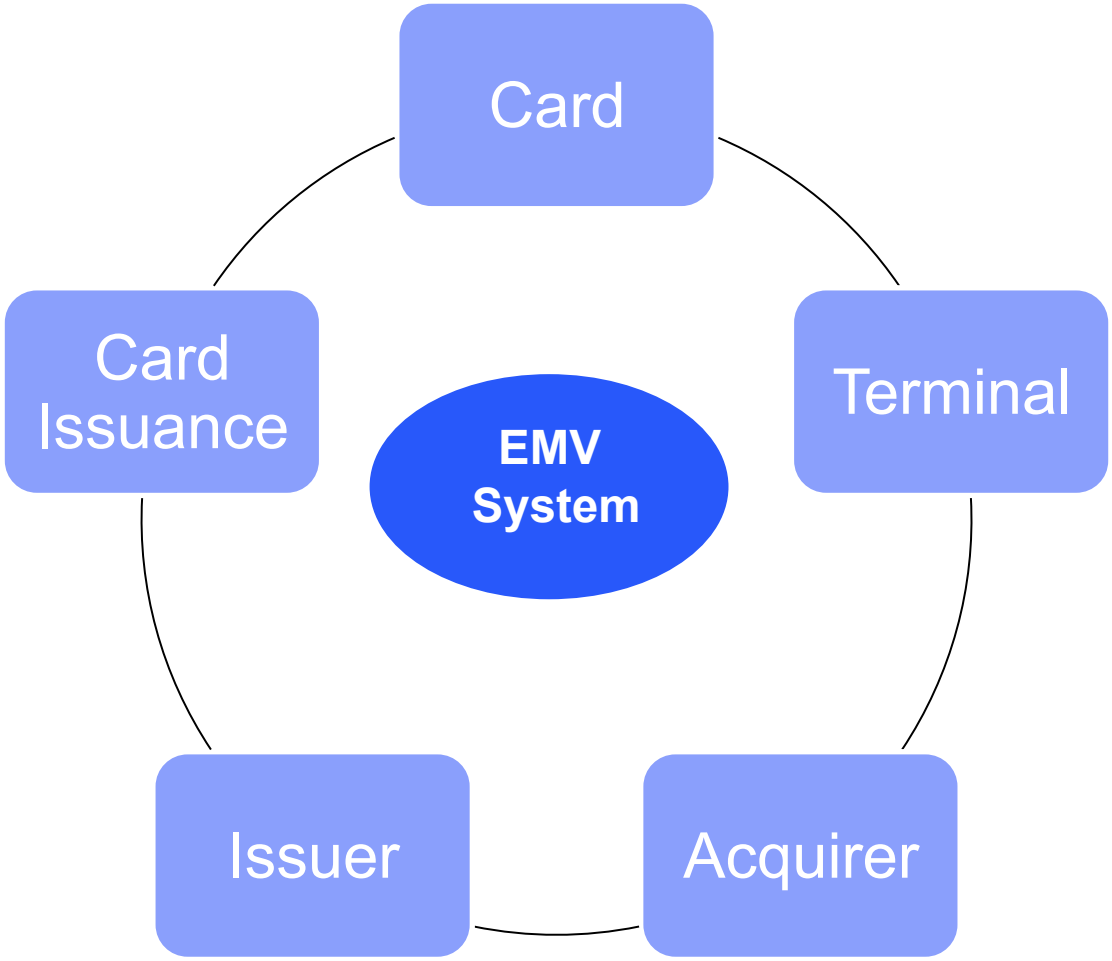
Transaction Processing Comparison

– Magnetic Stripe vs. EMV Transaction Security Points

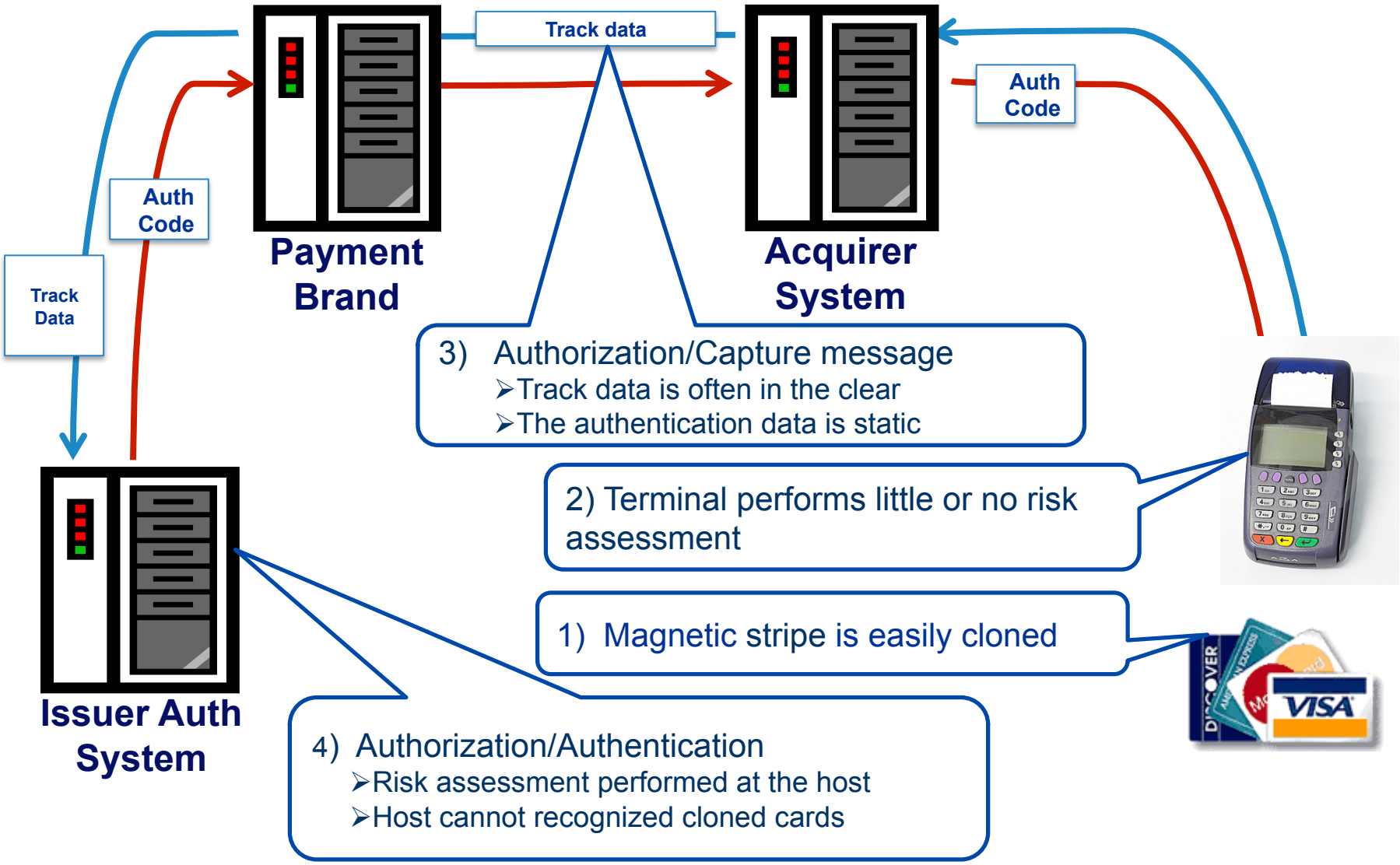
EMV Application Fundamentals

- Risk Management
- On-line authentication
- Off-line authentication
- Cardholder Verification Method
- Offline Authorization

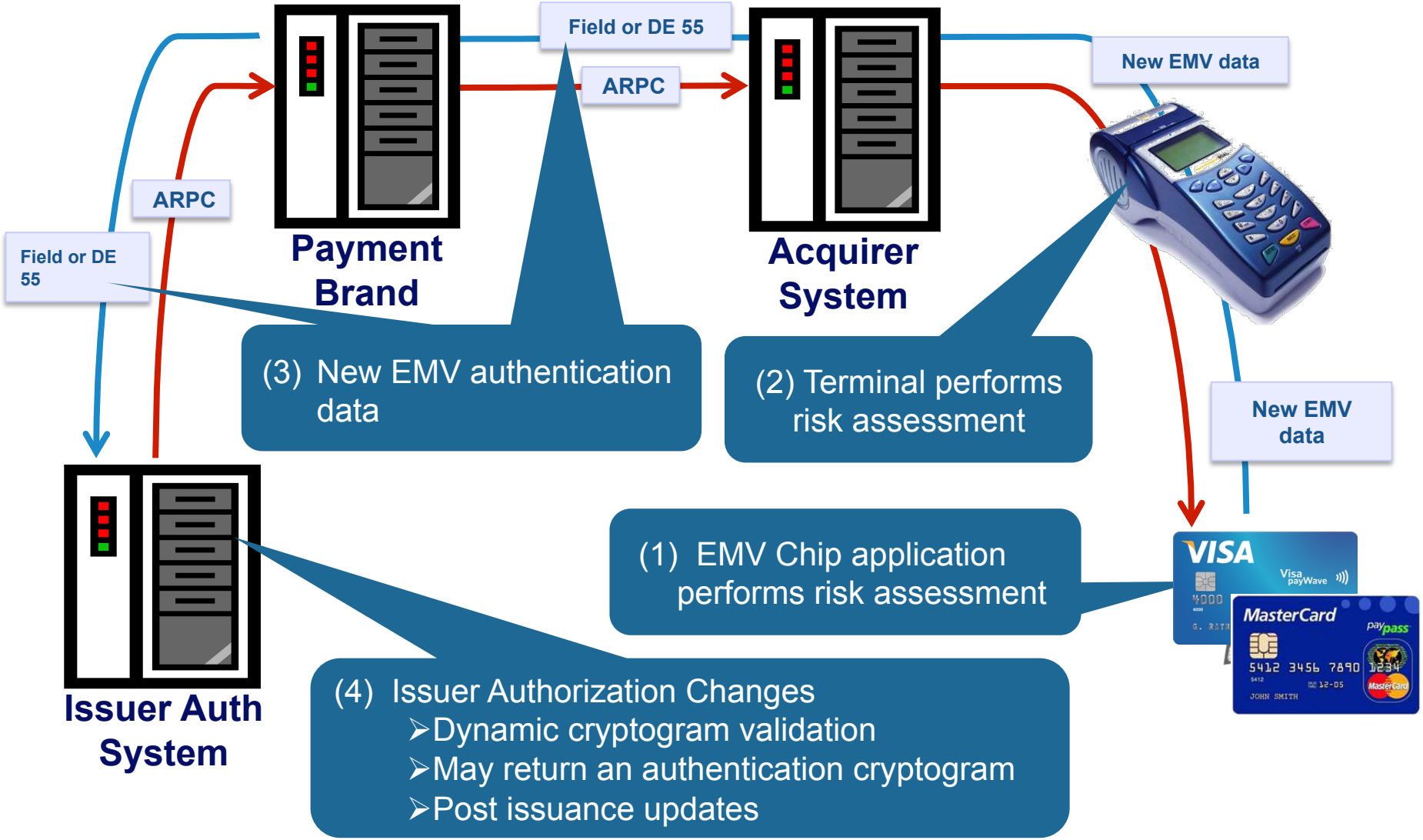
EMV Component Impact View



Magnetic Stripe Transaction



EMV Transaction Framework



EMV Security Components

Risk Management Decision Criteria

Card Stock Security

- EMV Configuration
- Issuance Security

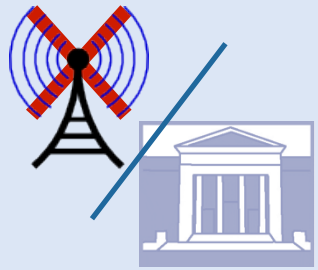
Data Preparation

Key Management

EMV Data

Online

Offline



EMV Chip Data

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

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

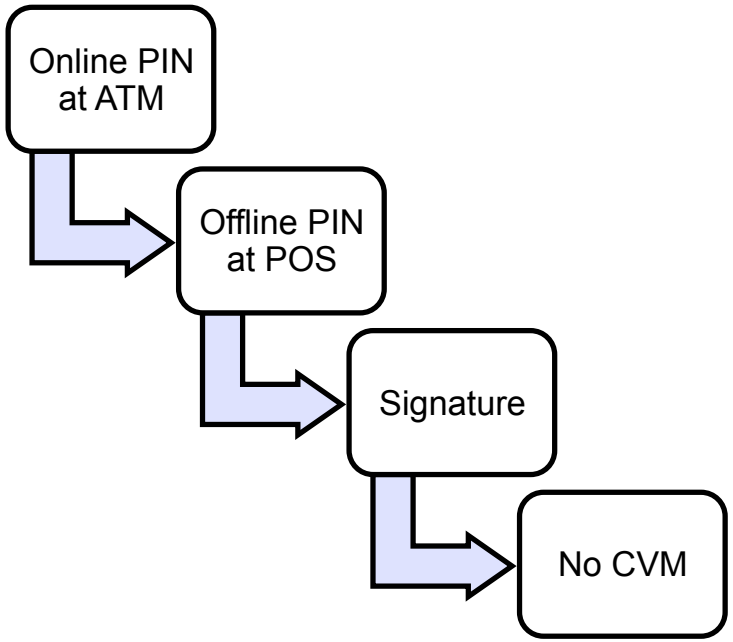
- If issuer authentication failure, do not transmit next transaction online
- If new card, do not decline if unable to go online
- …….

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



EMV Online Transaction Security

Risk Management Decision Criteria

Card Stock Security

- EMV Configuration
- Issuance Security

Data Preparation

Key Management

EMV Data

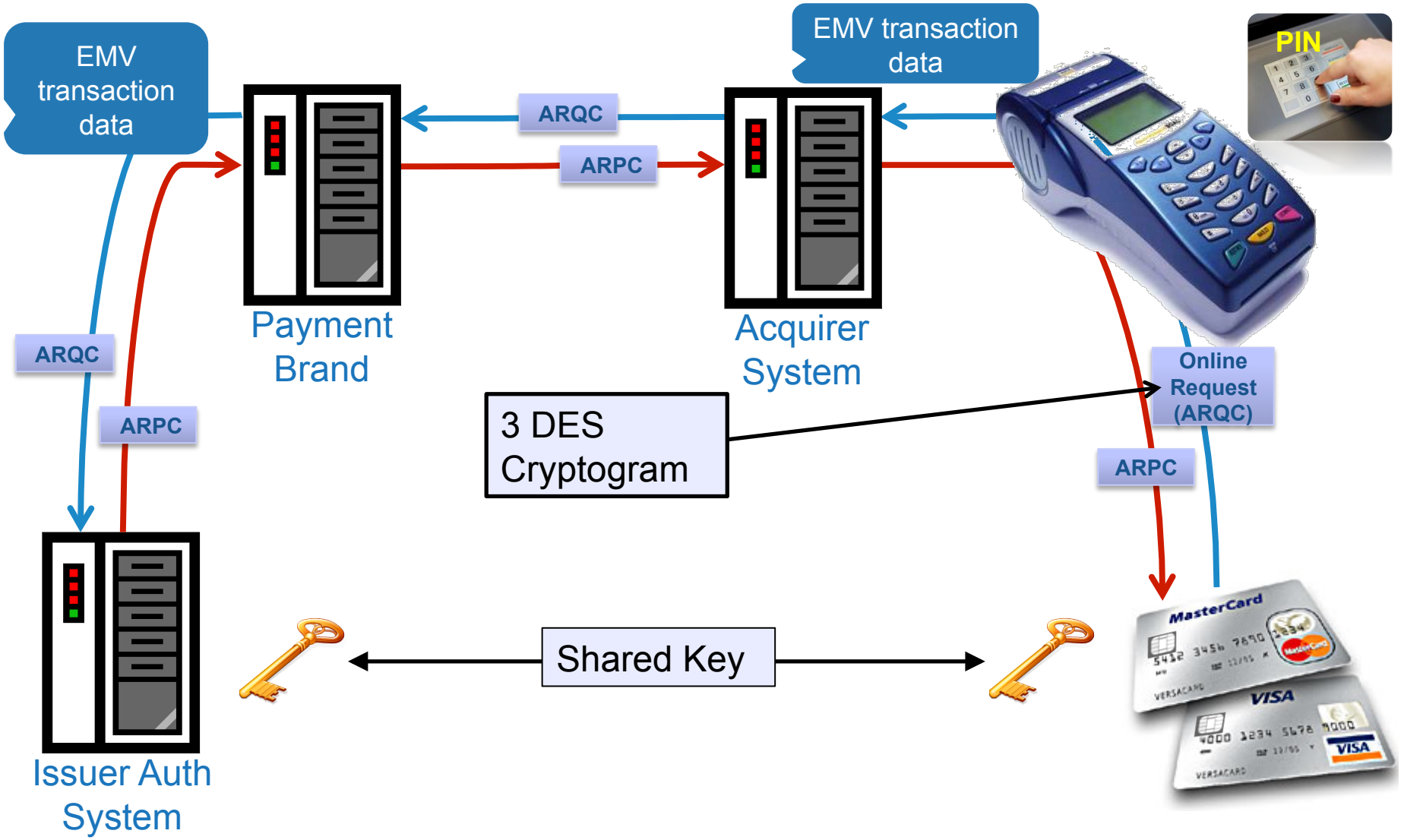
Online Transaction Security

Offline Transaction Security

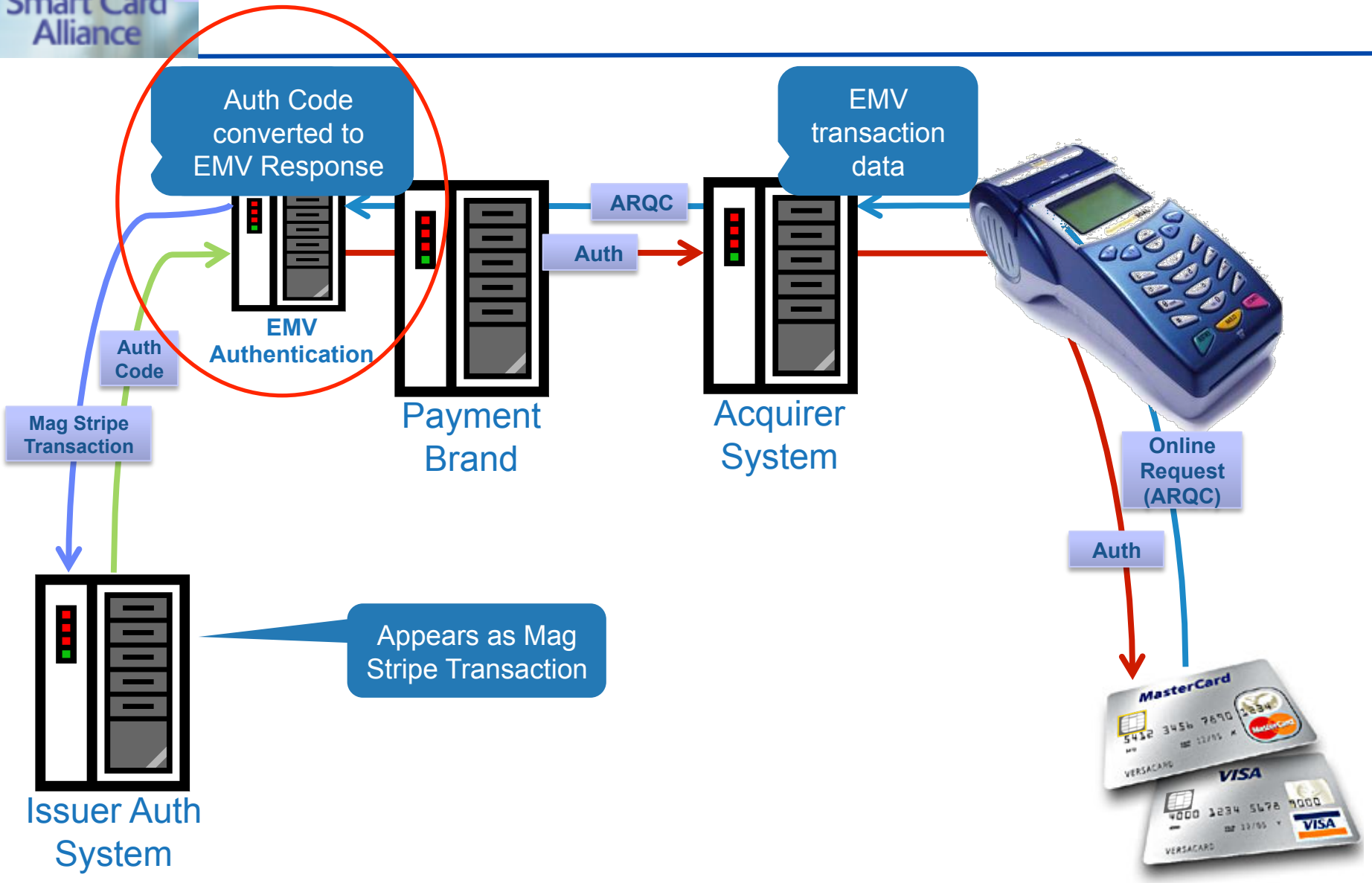
EMV On-line Security

- On-line EMV Authentication
- On-the-Behalf EMV Authentication

On-line CAM (Card Authentication)



On-the-be-Half EMV Authentication



EMV Offline Transaction Security

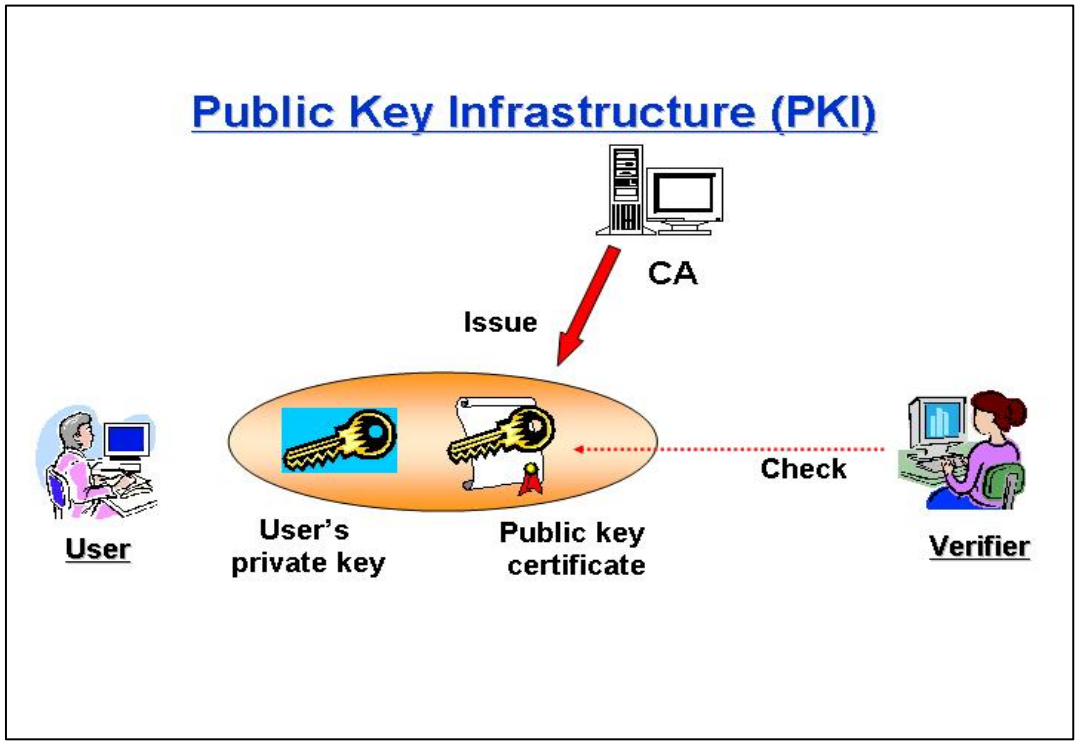
Risk Management Decision Criteria

Card Stock Security	• EMV Configuration • Issuance Security	Online Transaction Security	Offline Transaction Security
	Data Preparation Key Management EMV Data		

EMV Off-line Transaction Security

SDA/DDA/CDA
Card Authentication

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



Off-line Security Options

Off-line Authentication Options

SDA

- Static Data
- Issuer Public Key Certificate

DDA

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

CDA

- Combined Data
- Issuer Public Key Certificate
- ICC Public Key Certificate
- Application Cryptogram

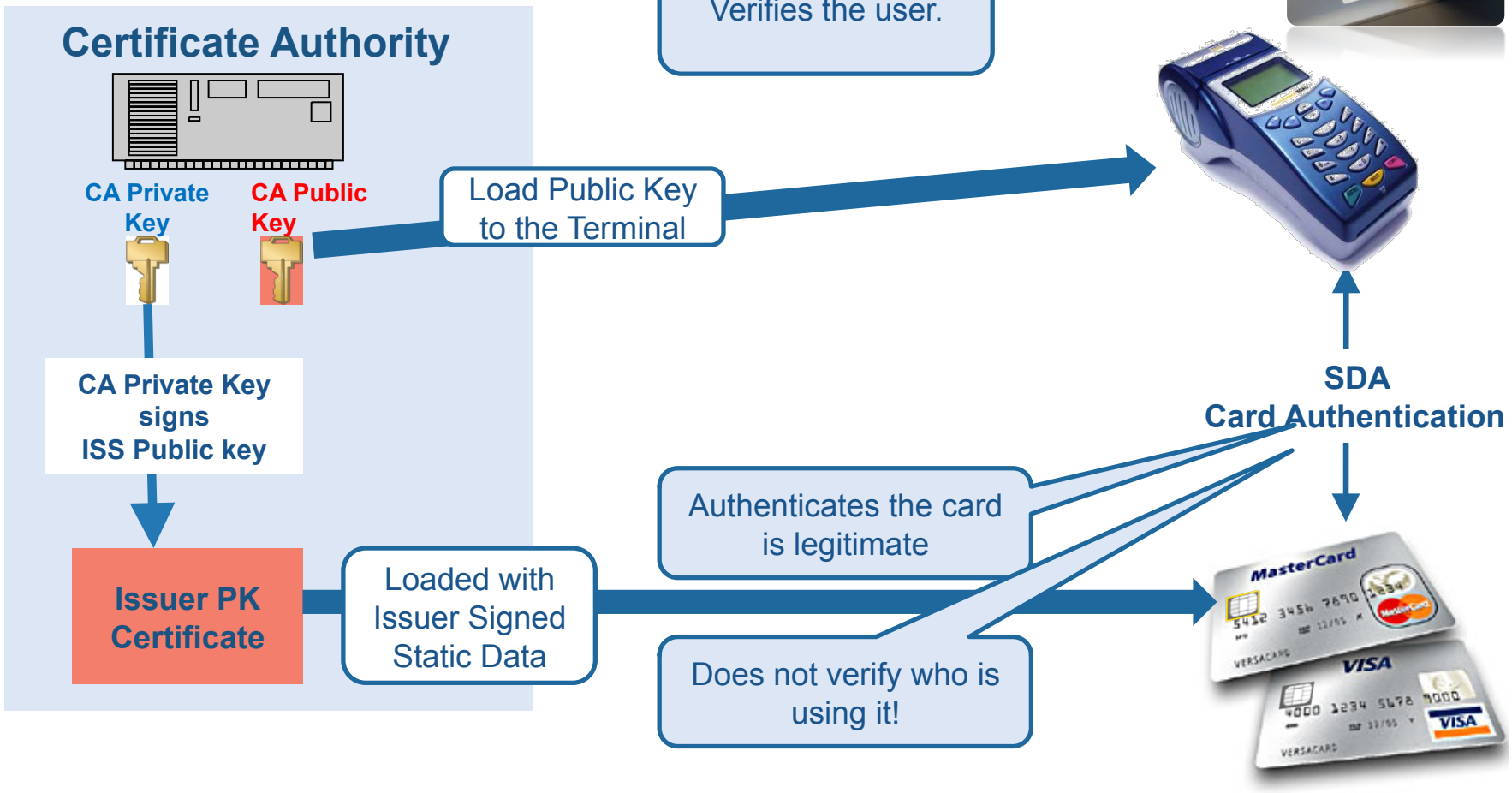
Issuer Level Certificate

Card Level Certificate

Off-line Transaction Authentication

SDA (Issuer level certificate)

SDA (Static Data Authentication)



Offline Cardholder Verification

- **SDA Cards**
  - ✓Clear Text PIN
- **DDA or CDA Cards**
  - ✓Clear Text PIN
  - ✓Encrypted (Enciphered) PIN

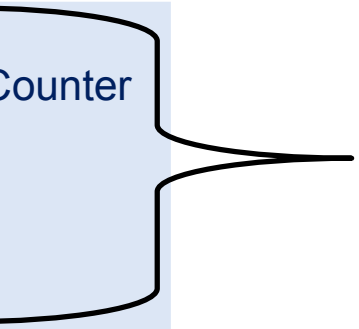
Offline Authorization

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

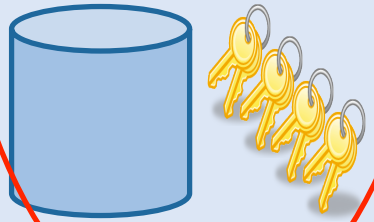
EMV Security Components

Risk Management Decision Criteria

Card Stock Security

Issuance Security

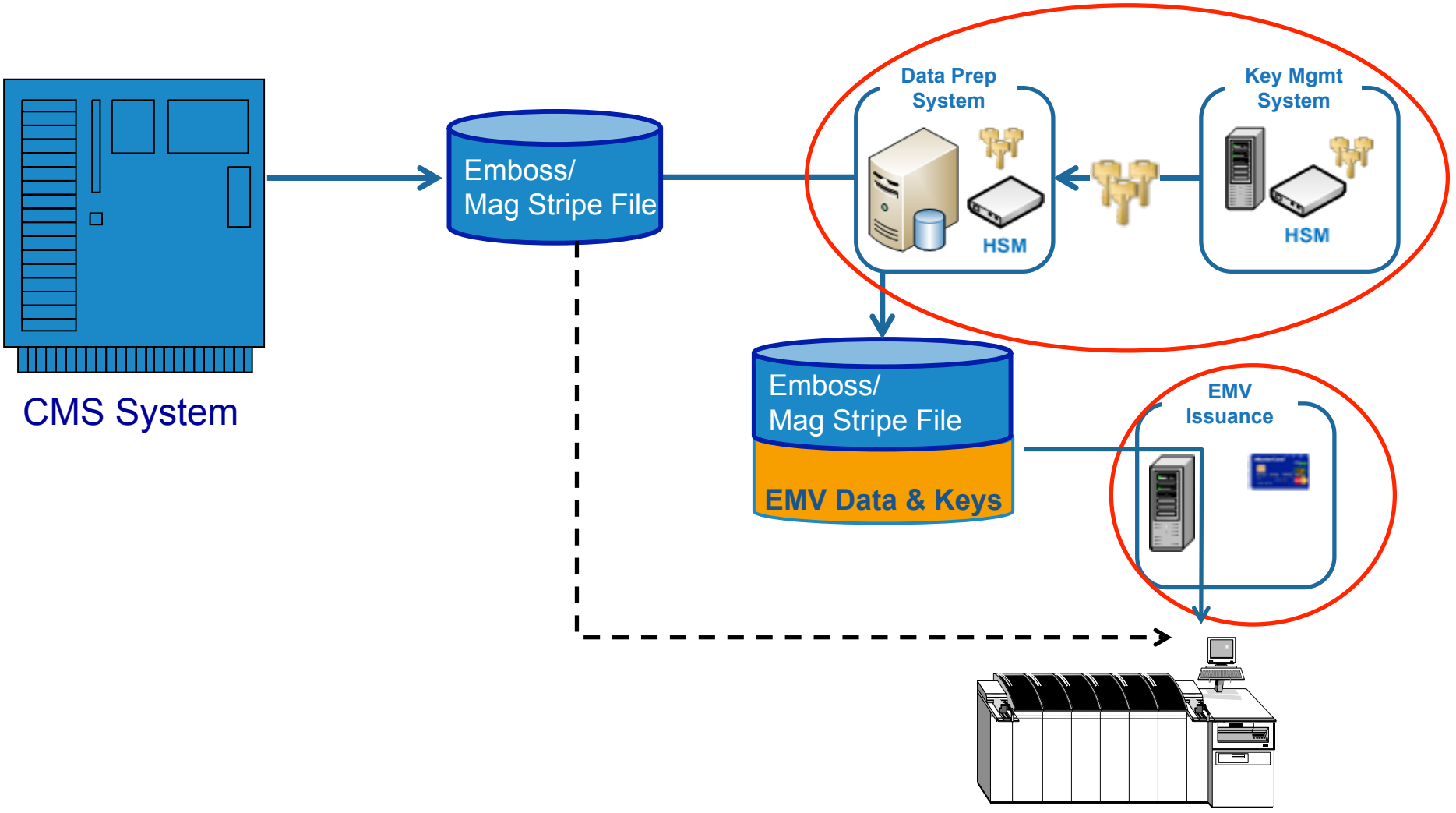
Data Preparation & Key Mgmt Security



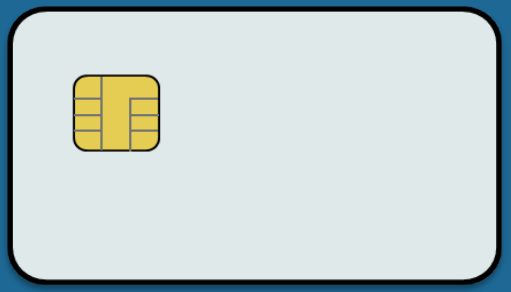
Off-line Transaction Security

On-line Transaction Security

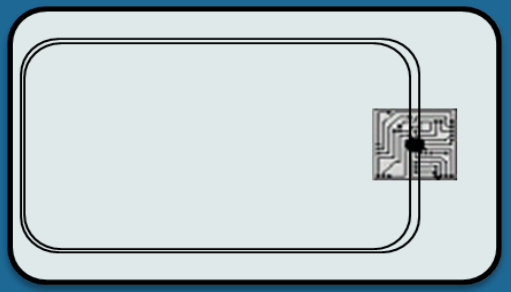
EMV Chip Personalization



Card Types

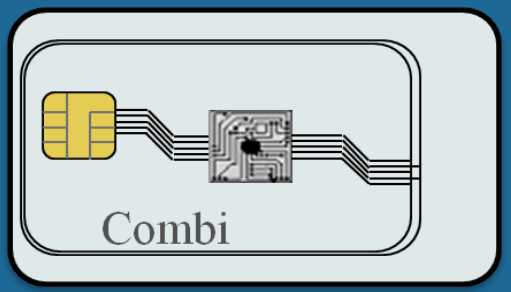


> Contact EMV



> 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

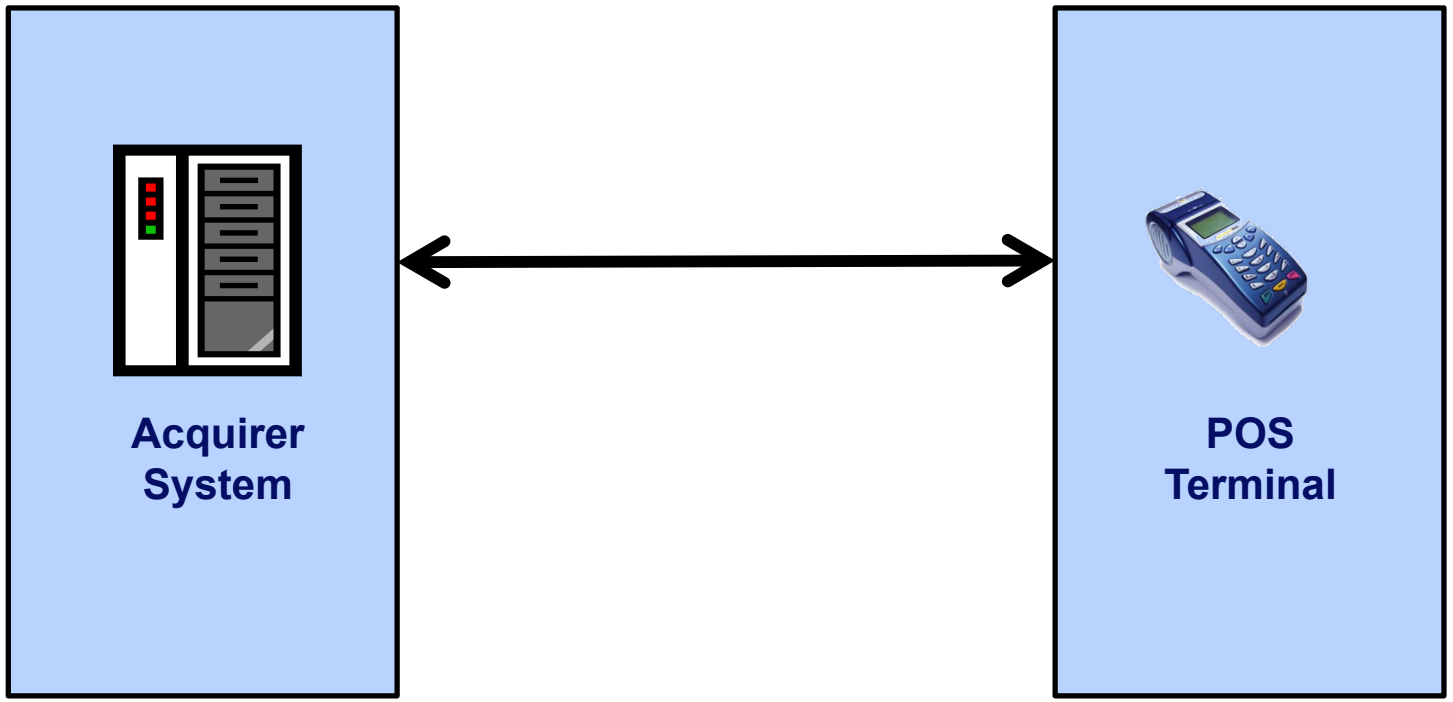
- **MasterCard**
  - ✓PayPass Contactless EMV
  - ✓Mchip Contact EMV
- **Visa**
  - ✓payWave Contactless EMV
  - ✓VSDC Contact EMV
- **American Express**
- **Discover**

- **Card Vendors have different chip operating systems**
- **Brands have different chip application implementations**
- **Brands have different EMV risk configuration options**

Data Level

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

Acquirers, Merchants and Terminals



Terminal Perspective

EMV and AID Based Matching Logic

Each Brand has different terminal certification requirements

Visa EMV terminal processing functions	MC EMV terminal processing functions	AMEX EMV terminal processing functions	Discover EMV terminal processing functions	Others EMV terminal processing functions

EMV Contact Kernel

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

Terminal Operating System

Terminal Profile (EMVCo Type Approval)

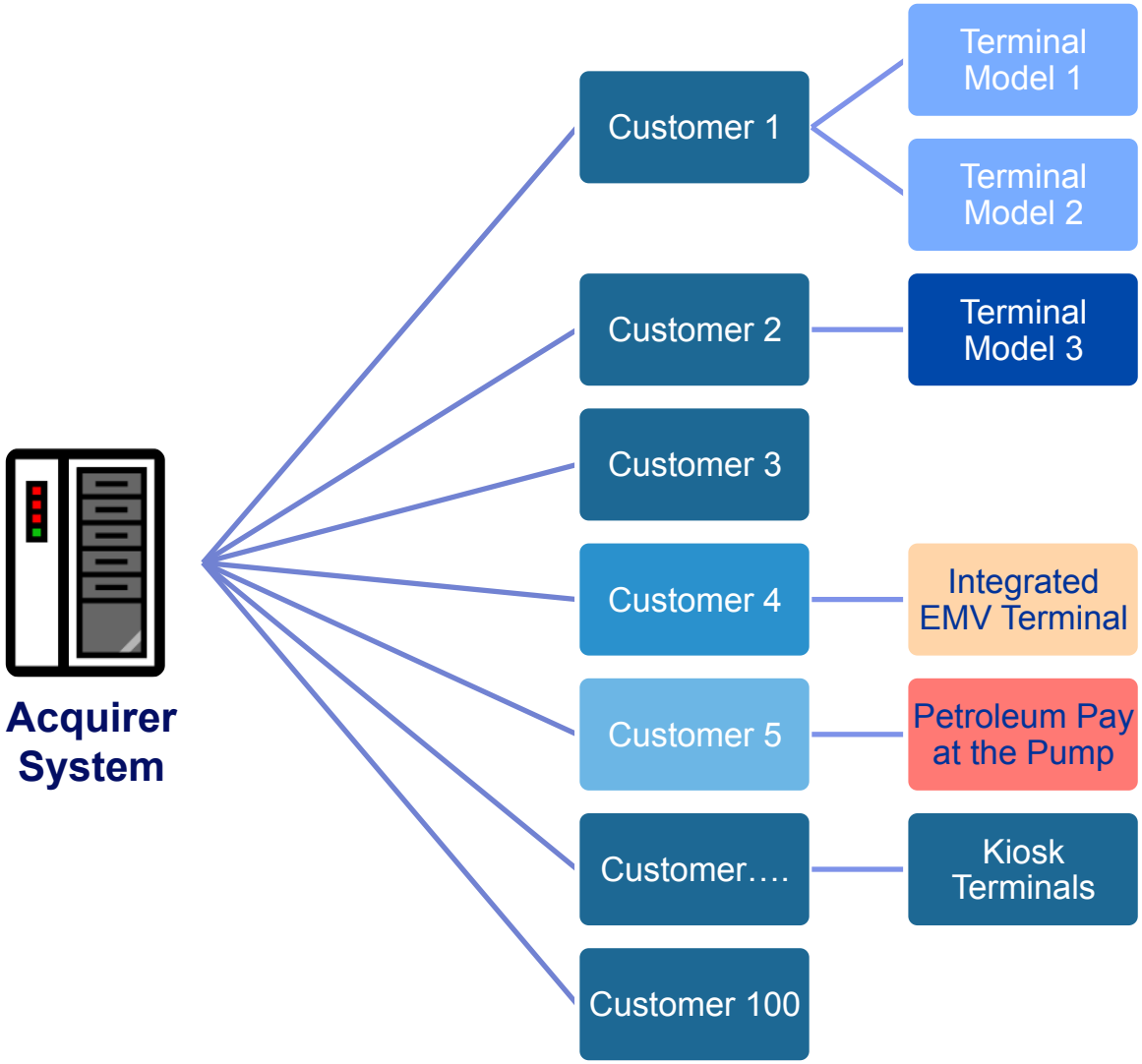
Unattended Terminal Profile
Supports but does not require PIN

- Chip only cards
- Offline plain text PIN
- Offline enciphered PIN
- No CVM
- SDA
- DDA
- CDA
- Issuer authentication supported

Unattended Terminal Profile
Requires PIN

- Chip only cards
- Offline plain text PIN
- Offline enciphered PIN
- SDA
- DDA
- CDA

Acquirers' Perspective



EMV Transaction Flow

Technology Selection

Application Selection

Processing Options

Card Authentication

Processing Restrictions

Card Holder Verification

Terminal Risk Management

Terminal Action Analysis

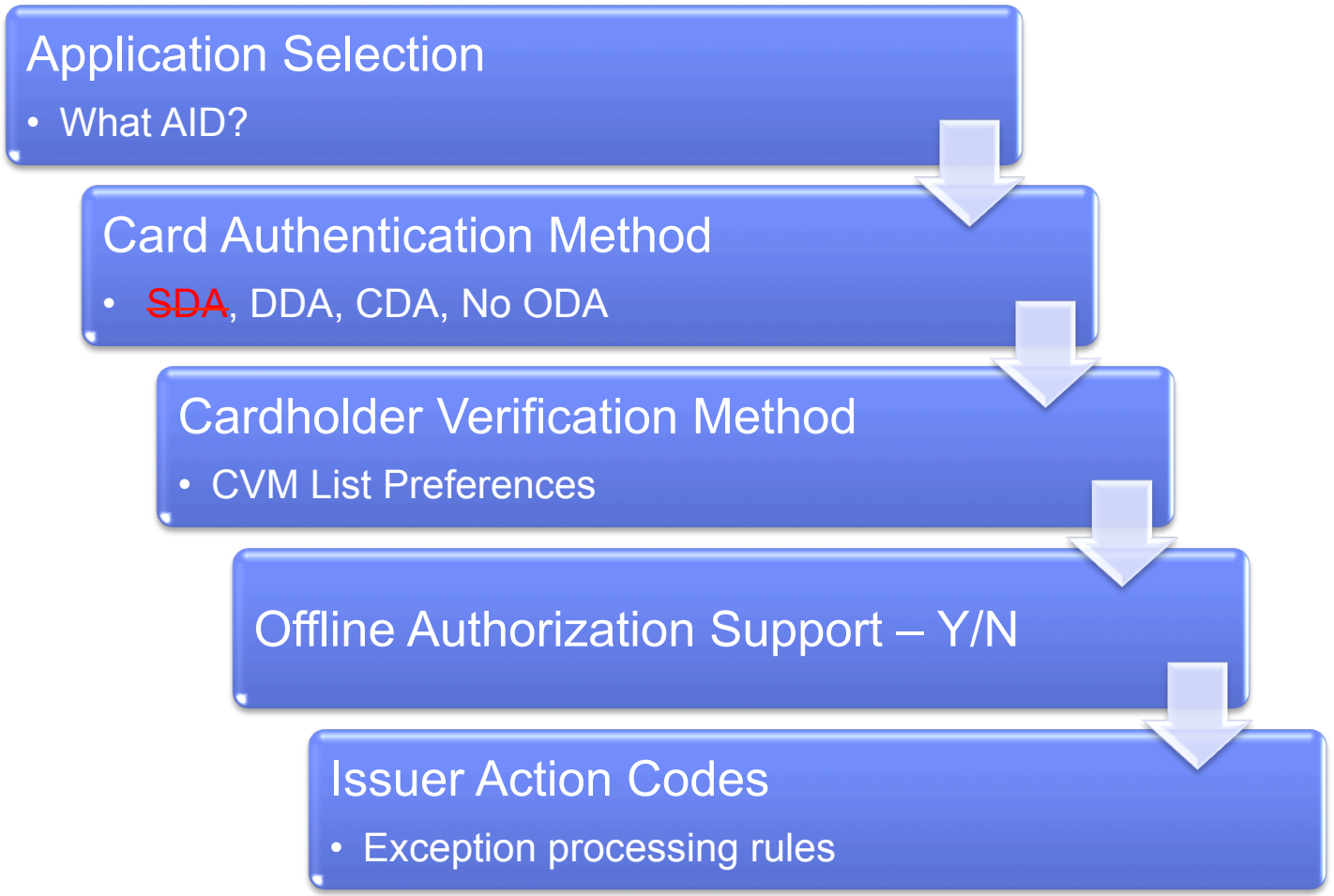
Card Action Analysis

Go On-line or Not

Issuer-to-Card Script Processing

Switch/Acquirer

EMV Transaction Flow



Application Selection

Identify mutually supported AIDs

Priority	AID
1	A0000000041010
2	A0000xyz
3	

AID	Config Data
A0000000031010	
A0000000041010	
A0000001523010	
A0000000043060	
A00000002501	
A0000xyz	

Application Selection Method

Explicit Selection

- Displays the choices to consumer

MasterCard Debit

XYZ Debit

Implicit Selection

- Terminal automatically selects the AID

Selected AID

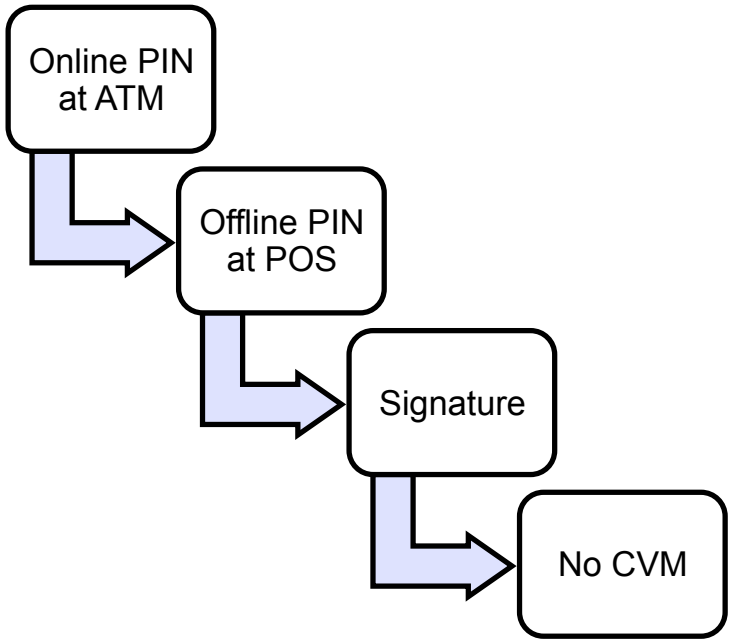
P	AID
1	A0000000041010
2	A0000xyz

Cardholder Verification

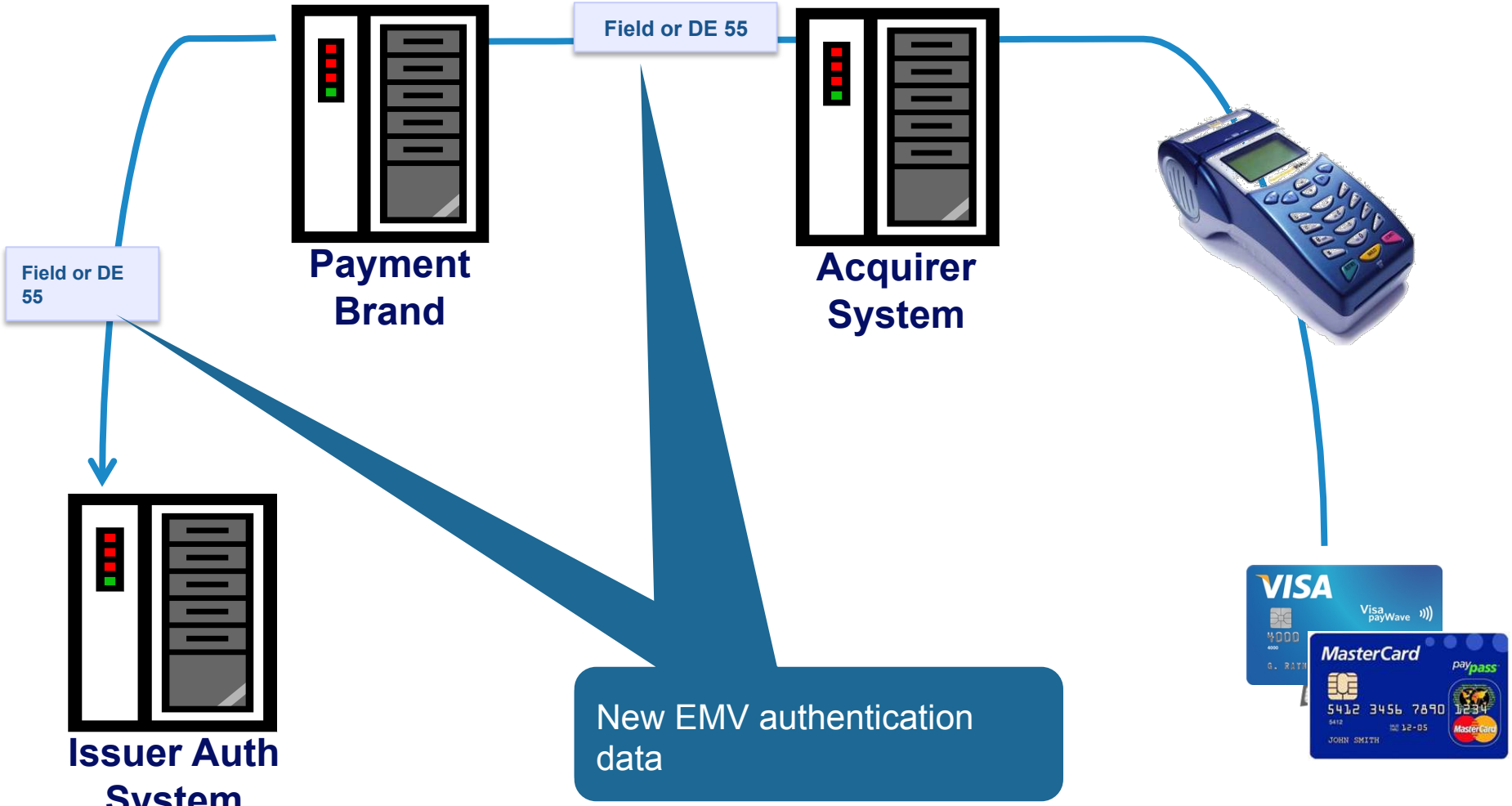
CVM Options

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

CVM List

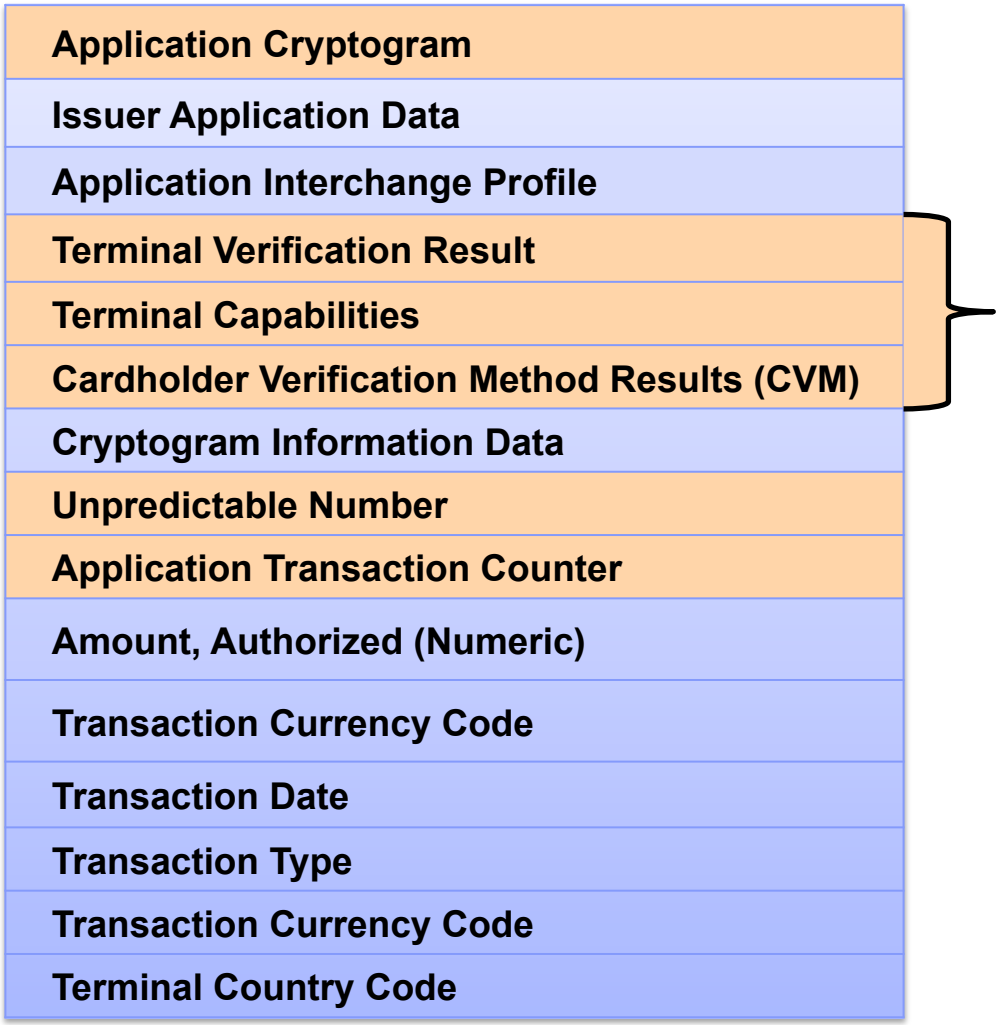


EMV Message Data

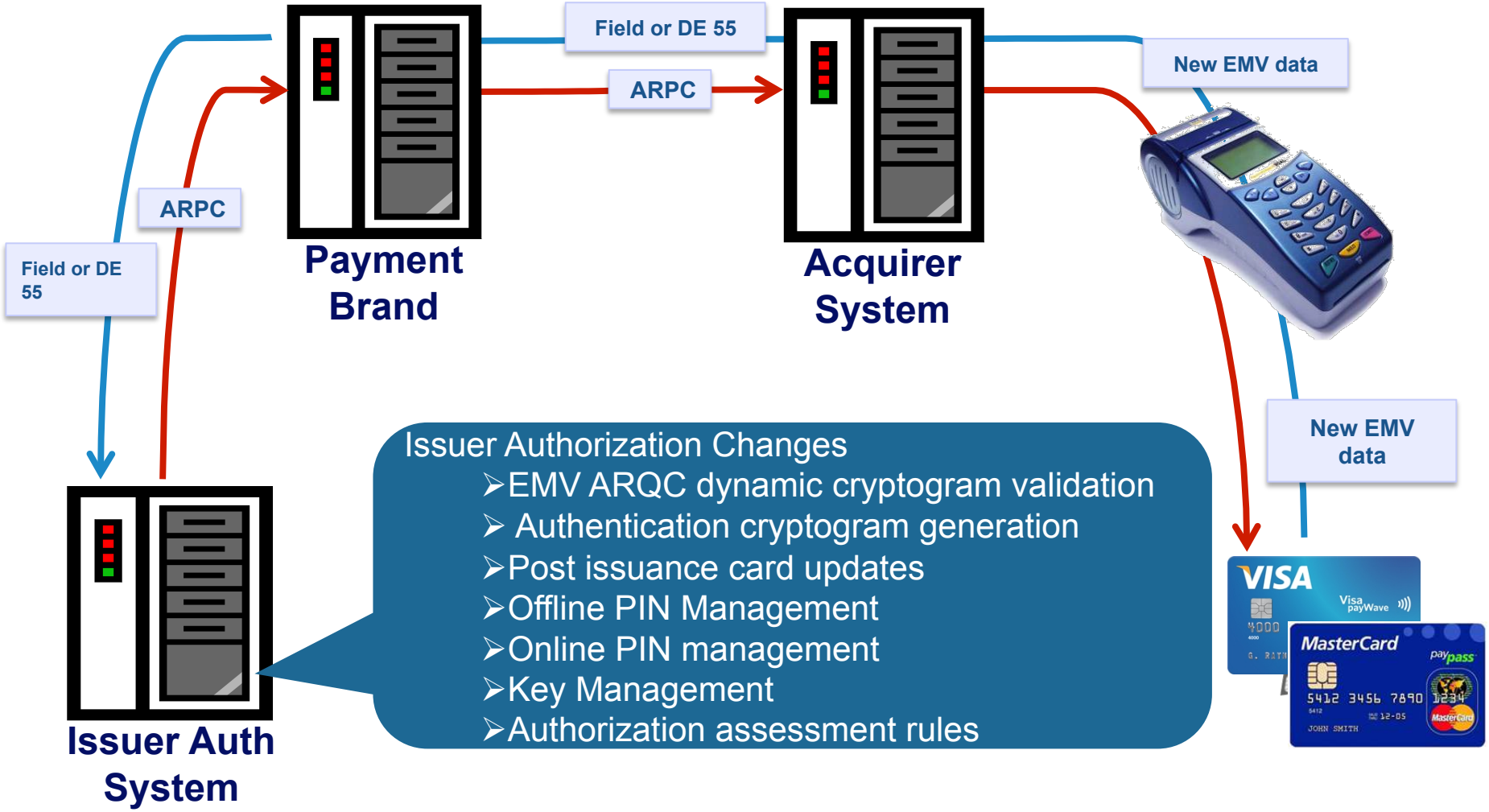


EMV Authorization Message

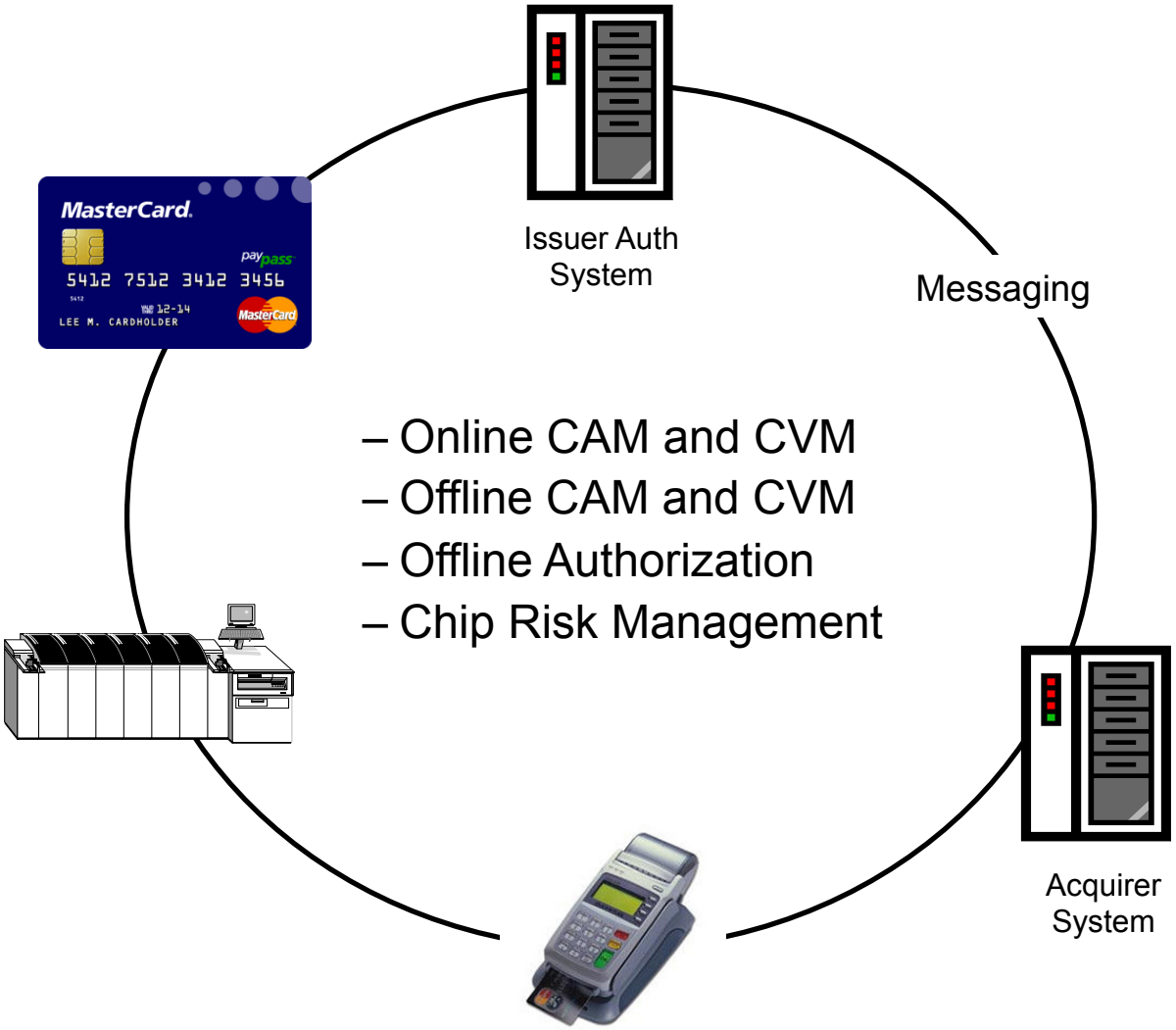
ISO 8583 – Field or DE 55



EMV Transaction Framework



EMV at a Glance



Guy Berg
Mastercard Advisors'
914.325.8111
Guy_berg@Mastercard.com

- Smart Card Alliance
- 191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556-6828
- www.smartcardalliance.org