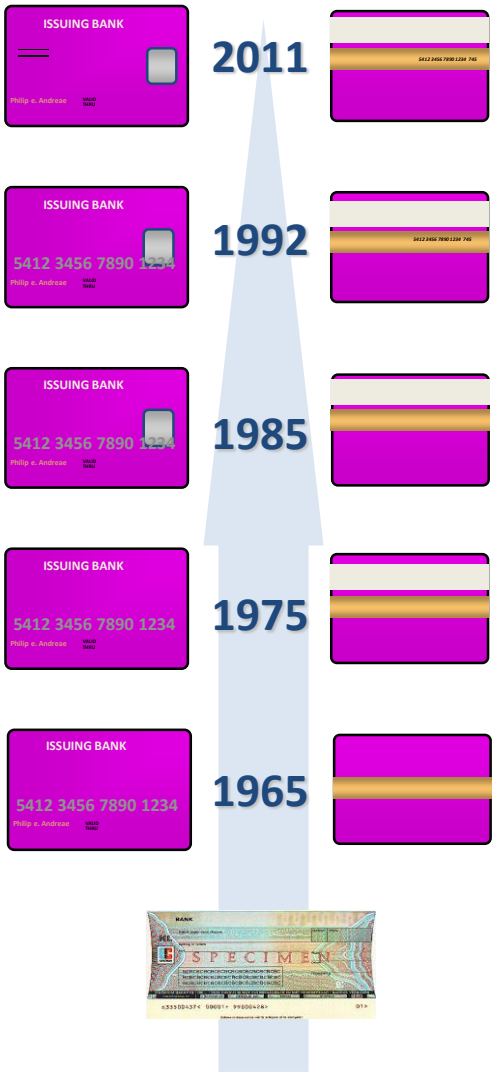
2014 The Year of EMV in the U.S.

Philip Andreae

Oberthur Technologies

Fraud – A Business with Cycles



Card, Embossing, Magstripe, Hologram, CVC & Chip

Card, Embossing, Magstripe, Hologram & CVC

Card, Embossing, Magstripe & Hologram

Card, Embossing & Magstripe

Card, Embossing

Check

CAM
Card Authentication Method

CVM
Cardholder Verification Method

Authentication and Confidentiality Require Cryptography

Symmetric

- One participant establishes a secret and shares the ***secret key S*** with other participants
- Triple DES algorithm is used for online PIN security
- EMV employs Triple DES for online authentication
- Sharing the secret key with too many parties puts the secret key at risk

Asymmetric

- Each participant establishes a unique pair of keys ***public key P*** and ***secret key S***
- Public key cryptography is used to assure authenticity and security on the Internet
- EMV employs RSA for offline authentication
- Each participant has a secret key they do not share

EMV: Global Standard For Credit & Debit Payments

EUROPAY International

MasterCard Worldwide

VISA

In 1993, The International payment brands decided the long-term solution to fraud was the "ICC" and agreed to develop a common specification to assure global interoperability.

They published: ***"The Integrated Circuit Card Specifications for Payment Systems"***

Counterfeit Protection
Off/On-line Authentication

Lost and Stolen Fraud Cardholder Verification

Offline Authorization
Cost Reduction

EMVCo

Revenue Creation
Value Added Services

EMVCo is owned and staffed by Visa, MasterCard, JCB, American Express, UnionPay and Discover

The Specifications Are Almost Stable

- ISO 7816 – Smart Card
  - Part 1: Physical characteristics
  - Part 2: Cards with contacts – Dimensions and location of the contacts
  - Part 3: Cards with contacts – Electrical interface and transmission protocols
  - Part 4: Organization, security and commands for interchange
- ISO 14443 – Contactless
  - Part 1: Physical characteristics
  - Part 2: Radio frequency power and signal interface
  - Part 3: Initialization and anti-collision
  - Part 4: Transmission protocol

Interoperability is the goal

EMVCo and payment brands certification is guaranteed

- EMV Version 4.3 – Contact
  - Book 1: Application independent ICC to terminal interface requirements
  - Book 2: Security and key management
  - Book 3: Application specification
  - Book 4: Cardholder, attendant and acquirer interface requirements
- EMV Version 2.3 – Contactless
  - Book A: Architecture and general requirements
  - Book B: Entry point specification
  - Books C1-6: Kernel specifications
  - Book D: Communications protocol

Payment system specifications define operating rules, network requirements, card application, terminal details, key management and E2E certification requirements

The industry is awaiting DNA and debit network specifications

EMV Provides Three Key Capabilities

Unique serial number and certificates
valid scheme, issuer and card

Authentication

Online authentication with offline option

"What you have"

Verification

PIN verified in chip or on issuer host

"What you know"

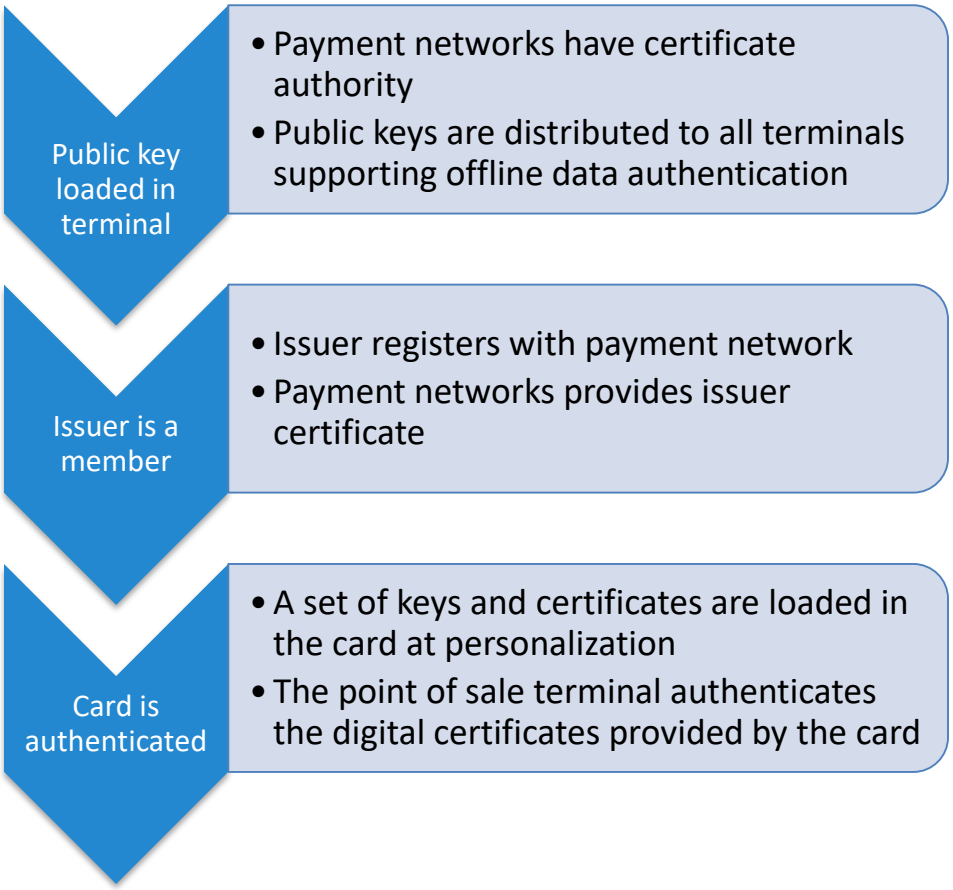
Authorization

"You have the funds"

Card risk management

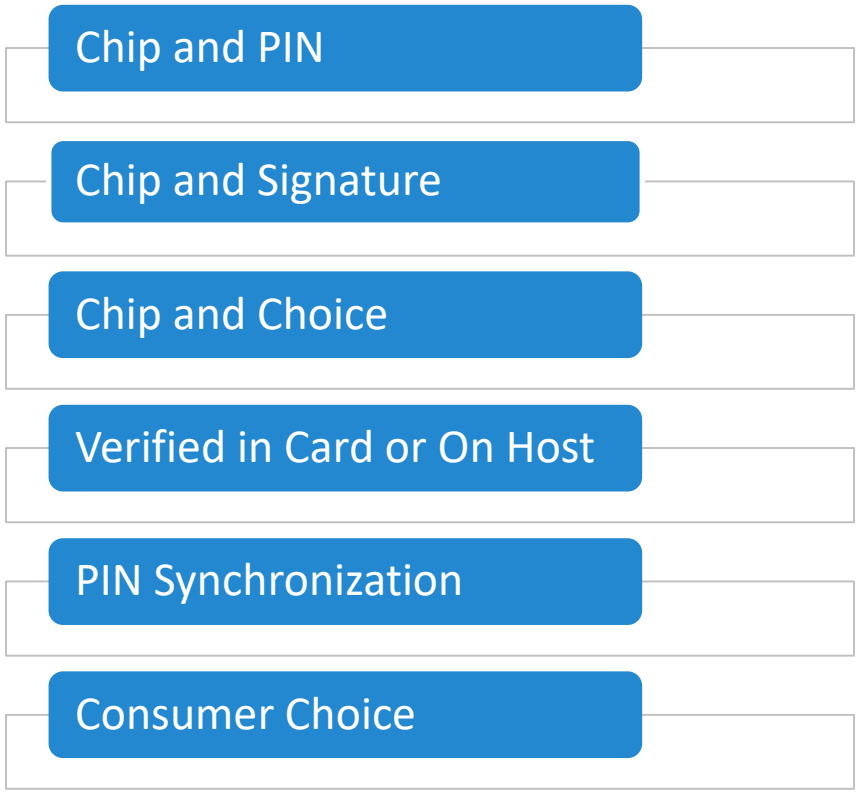
Terminal risk management

Authentication



- EMV supports 3 offline card

Verification



- EMV offers the issuer various cardholder verification methods, like:
  - Online PIN verification
  - In-chip PIN verification
  - Clear text or encipher PIN
  - Signature verification
  - No CVM
- Or any combination, including rules:
  - No CVM below $10
  - Offline PIN between $10 and $100
  - Offline PIN + signature above $1,000
- Phantom PIN is also possible

Authorization

Card Decided

Terminal Requests	TC Offline	ARQC Online	AAC Decline
TC Offline	Yes	Yes	Yes
ARQC Online	Why	Yes	Yes
AAC Decline	Why	Why	Yes

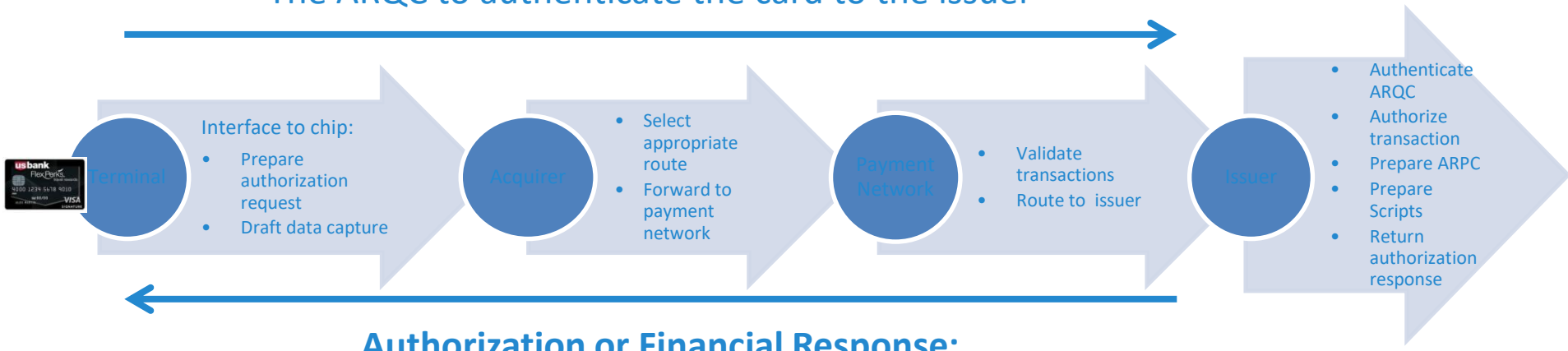
- The design of EMV assured issuer control:
  - **Terminal risk management:** The merchant sets a floor limit under which the terminal will ask the card to approve the transaction
  - **Card risk management**: Issuer defined parameters defined how the card will decide
- The value of offline authorization:
  - The issuer always decides
  - Reduces the cost of authorization
  - Reduced the transaction time
  - Addresses acceptance in Transit
  - Requires Offline Authentication and In Chip Verification

Field 55 – Online Authentication and Card Life Cycle Management

Merchant	Acquiring Bank	Payment Switch	Issuing Bank

Authorization or Financial Request:

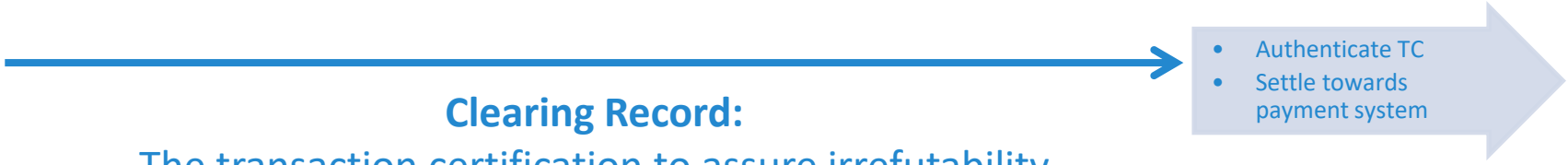
The ARQC to authenticate the card to the issuer



Authorization or Financial Response:

The ARPC authenticates the Issuer to the card

Scripts update Card Risk Management Parameters & the PIN



Clearing Record:

The transaction certification to assure irrefutability

EMV Defined Application Selection
Issuer Control & Consumer Choice

1. Personal Credit Card
2. Corporate Credit Card
3. Family Debit Card
4. Personal Debit Card

Enter 1, 2, 3 or 4 to select payment method?

Consumer Selection

PSE – Payment Systems Environment
AID – Application Identifier

Multi- Access and Multi-Application

AID – Application Identifier

- The AID is the name of the directory in the chip that contains the keys, certificates, parameter, counters and identifies the “application”
- The AID are registered by the payment networks:
  - Visa A0000000031010
    US Common Debit A0000000980840
  - MasterCard A0000000041010
    Maestro Int’l A0000000043060
    US Maestro A0000000042203
  - Amex A00000002501XX
  - JCB A0000000651010
  - Discover A0000003241010
  - DNA Common Debit A000000XXXXXXX

Application

- The Payment Networks’ Card and Terminal specifications defines of the software required in the card and how the terminal will employ the EMV tool kit
- Each Payment Network has invested in in defining, maintaining and certifying implementations of their specifications
  - MasterCard – MChip
  - Visa – VIS
  - Discover - D-Pas
  - Amex – AEIPS
- The Visa and MasterCard specification define methods of sharing data between two or more AIDs to support US Debit requirements
- Card and terminal vendors develop and request type approval of their products

The Debit Conundrum

Issuer

- Sought higher interchange fee income
- Offered signature debit MasterCard or Visa branded on the face of the card
- Selected PIN debit network based on commercial arrangement and regional ATM and POS coverage

Merchant/Acquirer

- Fought the rising cost of Interchange
- If PIN debit was of interest procured PIN capable POS device
- If they supported signature and PIN debit consumer offered the option "like credit" or "as debit"

Challenge

- In EMV the AID is the equivalent of the Payment Brands Logo
- The consumer sees the card as a method of using funds in their checking account
- The consumer does not understand the different Debit Brands and Networks
- EMV assumed a single CVM list per AID

Therefore

- One AID for **Signature Debit** – AID of the brand on the face of the car
- One AID for **PIN Debit** – U.S. debit AID to support PIN debit networks

Dispelling Myths

- EMV does not encrypt data, it uses cryptography to create dynamic digital signatures – the ARQC, ARPC and TC
- To address card not present or shopping on the Internet, an EMV capable card reader (contact or contactless) could be deployed, utilizing 3D-Secure
- Tokenization and EMV compliment each other
- NFC is a communication protocol
- Proximity (NFC) mobile payments are based on EMV
- EMV does not address cyber crime nor stop hackers from breaking into systems
- Once EMV is fully deployed it significantly reduces the value of the data that can be acquired by breaking into payment systems

EMV was designed to address counterfeit and lost and stolen fraud in the physical world