EMV® Migration Forum

EMV 101

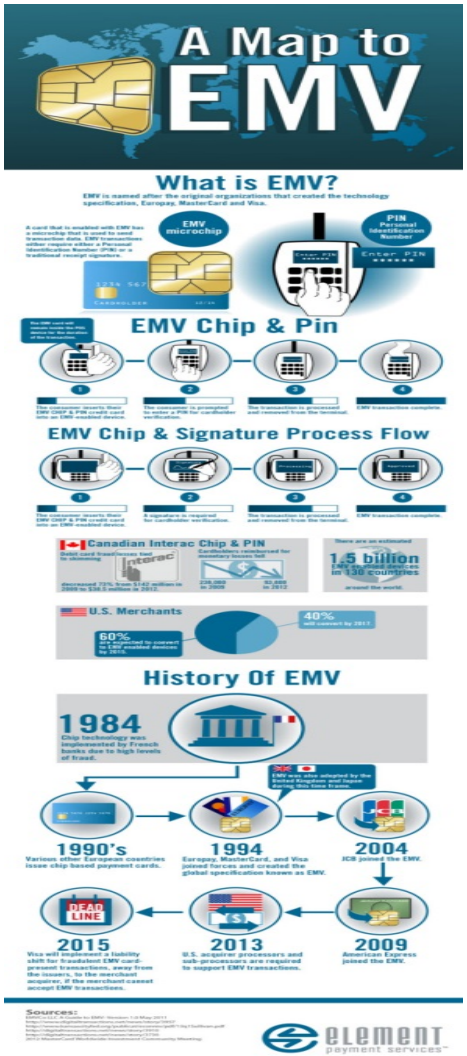
Umesh Kulkarni – Clear2Pay

EMV 101

- What is EMV?
- Benefits of EMV
- Types of Cards
- Terminal (POS / ATM)
- EMV & Applications (AIDs)
- EMV Transaction flow
- EMV & Security
- Changes to the Environment
- Merchant Training
- Lessons Learned
- Risk of improper Testing & Terminal Management

EMV® Migration Forum

What is EMV?



- **Global specification** supporting smart card / terminal interoperability and transaction processing of credit and debit cards
  - Open, industry-wide specification
  - Developed jointly by Europay, MasterCard and Visa (EMV) in the mid-1990s
- **EMVCo** LLC formed in April 1999
  - EMV standards now defined and managed by the public corporation
  - Ownership and promotion of EMV specs
  - Facilitate global interoperability and compatibility of chip-based payment cards and payment terminals
  - Establish unified type approval testing process
  - Now owned by JCB, MasterCard and Visa (+American Express, Discover, and UnionPay as new Members)

Benefits of EMV

Protect against counterfeit fraud through **authentication of the chip** card

Risk management parameters to reduce the risk of unauthorized payment

Validate the **integrity of the transaction** through digitally signing payment data

Reduce lost and stolen cards through robust **cardholder verification** methods in all acceptance environments

Types of cards

Smart card, chip-enabled card, chip card, chip & PIN, EMV card, chip contact card, chip & signature, contactless smart card, VSDC – M/Chip.....

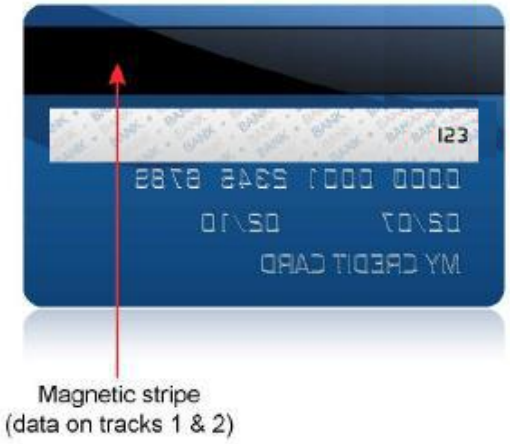
- They all do the same thing
- They all contain an integrated circuit

Three types:

- Magnetic stripe card
- Contact chip
- Contactless/Mobile chip

EMV® Migration Forum

Types of cards: Magnetic stripe



Magnetic stripe (or Magstripe):

- First use on cards : in the early 1960's.
- Not inherently secure (easy to clone)
- 3 tracks maximum (data very limited)
- Very inexpensive and readily adaptable to many functions

"Smart cards" have significantly more memory and processing capacity than their traditional magstripe counterparts.

In the future, magstripe will most likely be gone, with smart cards replacing them.

EMV® Migration Forum

Types of cards: Contact Chip

Plastic card with **embedded microchip** that can process and store data.

IC chip (or ICC) on the surface.

More secure than a magnetic stripe card

- It is very difficult to clone a chip!

Protect customer card information with **improved data encryption**.

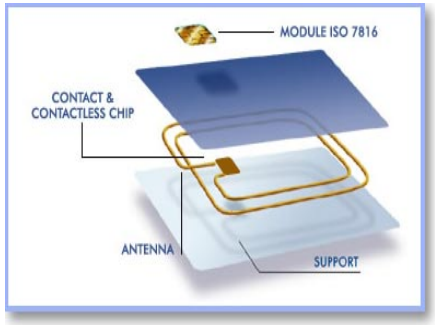
When insert the card into reader, data can transfer to reader.

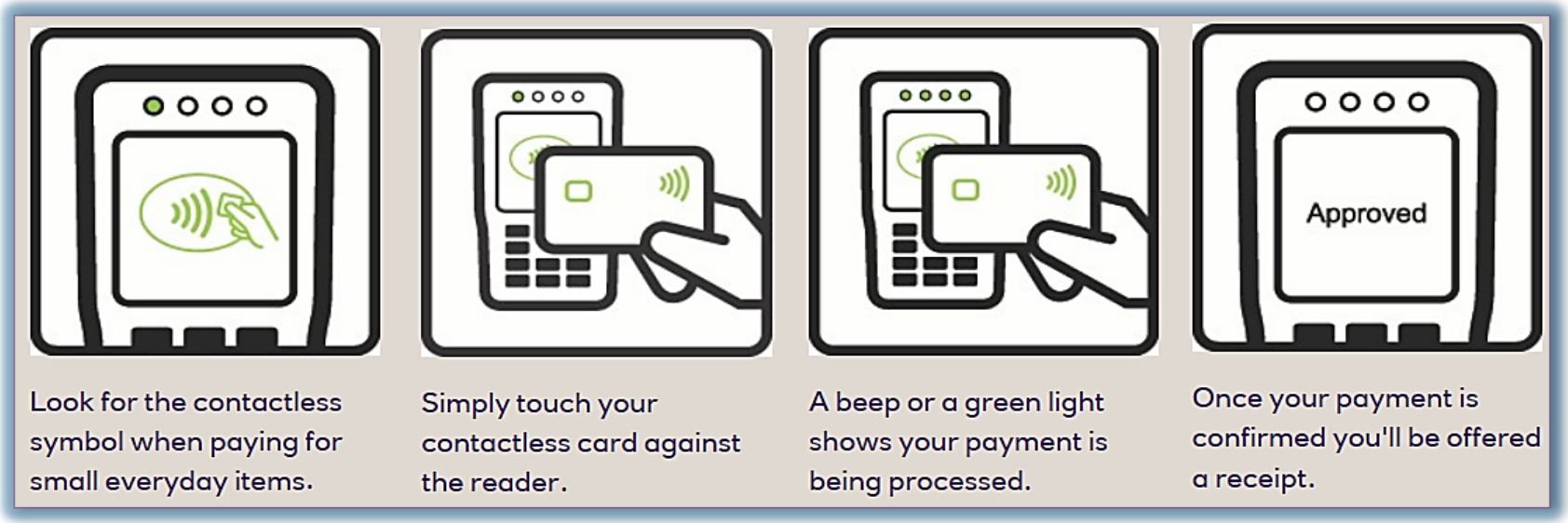
- Can **store a lot of data** - Up to 32 or 64 kilobytes!
- Can be "Chip & PIN" or "Chip & Signature" or both.

EMV® Migration Forum

Types of cards: Contactless/Mobile Chip

Plastic card with embedded microchip
Chip/Antenna integrated to the card
Known as RFID (radio frequency ID)
often used when transactions must be processed quickly or these an also be used in Mobile devices utilizing just the UICC and the Antenna is maintained in the battery or phone cover





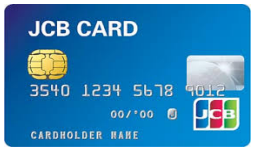
EMV Migration Forum

Types of cards: EMV chip cards

The most widely known chip card implementations of EMV standard are:

- **VSDC** - Visa's EMV specification
- **M/Chip** - MasterCard's EMV specification
- **AEIPS** - American Express's contact EMV specification
- **J Smart** - JCB
- **D-PAS** - Discover/Diners Club International.
- **UICS:** UnionPay International

Each individual specification must first conform to the very detailed EMVCo specifications!



Terminal: POS

Point-of-sale (POS) terminal is an electronic device used to process card payments at retail locations

A POS terminal generally does the following:

- Reads the information off a customer's credit or debit card
- Checks whether the funds in a customer's bank account are sufficient
- Transfers the funds from the customer's account to the seller's account (or at least, accounts for the transfer with the credit card network)
- Records the transaction and prints a receipt

EMV® Migration Forum

Terminal: ATM

ATM

Using an ATM, cardholders can access their bank deposit or credit accounts in order to make a variety of transactions such as:

- Cash withdrawals
- Check balances
- Credit mobile phones
- Loading money on prepaid cards
- Paying bills

ATMs help banks to provide banking services to their customers 24*7 on all 365 days of the year.

Terminal : Terminal Type Approval

EMVCo established the "Terminal Type Approval process" to create a mechanism to test compliance with the EMV Specifications. This certification is normally managed by Terminal or Kernel Vendors.

Two levels of Approval:

- Level 1: compliance with the electro-mechanical characteristics (contact) or the analog characteristics (contactless):
  IFM = Hardware testing
- Level 2: compliance with the application Requirements
  Kernel = Software testing

EMVCo

July 14, 2004

Wayne Yu
ShangHai SAND Information Technology System Co., Ltd.
23 Bin Yang Road
Shanghai, P.R. China 200235

Re: ***EMVCo Letter of Approval -- Terminal Level 1***

Approval Number:	**11780 0704 400 20 FIM**
IFM Identification:	**PS100 Version 1.0**
Hardware:	**SAND-ICC Version 1.3**
Software:	**SAND-SW100 Version 1.0**
As Tested In:	**PS100**

Dear Wayne Yu:

EMVCo, LLC ("EMVCo"), a Delaware limited liability company, has received your request for Level 1 type approval for the interface module identified above. In connection with your request, we have reviewed test file number C04RAP07-02-1 which was generated by FIME.

After assessing such file, EMVCo has found reasonable evidence that the submitted samples of the above referenced interface module sufficiently conform to EMV Specifications, Book 1, Version 4.0 of December 2000 ("EMV 4.0 Specifications").

EMVCo hereby (a) grants your interface module EMVCo Type Approval for Terminal Level 1, based on the requirements stated in the EMV 4.0 Specifications, and (b) agrees to include your Application module in EMVCo's approved interface module list. EMVCo's grant to your interface module is subject to and specifically incorporates (i) the General Terms and Conditions to the Letter of Approval enclosed as Exhibit A, and (ii) the Specific Terms and Conditions to the Letter of Approval attached hereto as Attachment A. Because EMVCo's grant is subject to such limitations, including certain events of termination, you and any third parties should confirm that such approval is current and has not been terminated by referring to the list of approved interface modules published on the EMVCo website (www.emvco.com).

This Letter of Approval is effective on dispatch from EMVCo.

EMVCo, LLC, a Delaware limited liability company

By:
Name: David Mierzwa
Title: EMVCo Type Approval Secretariat

The list of Approved terminals is available on the www.emvco.com website.

EMV Migration Forum

EMV & Applications (AIDs)

EMV cards can be multi-application cards, meaning one card (chip) can contain various applications like:

- One debit application
- One credit application
- One prepaid application

A chip card that conforms to EMV specifications will contain one or more financial applications, each identified by a unique AID:

AIDs e.g. A0000000031010 (Visa credit/debit), A0000000032010 (Visa electron), A0000000042203 (U.S. Maestro AID) etc...

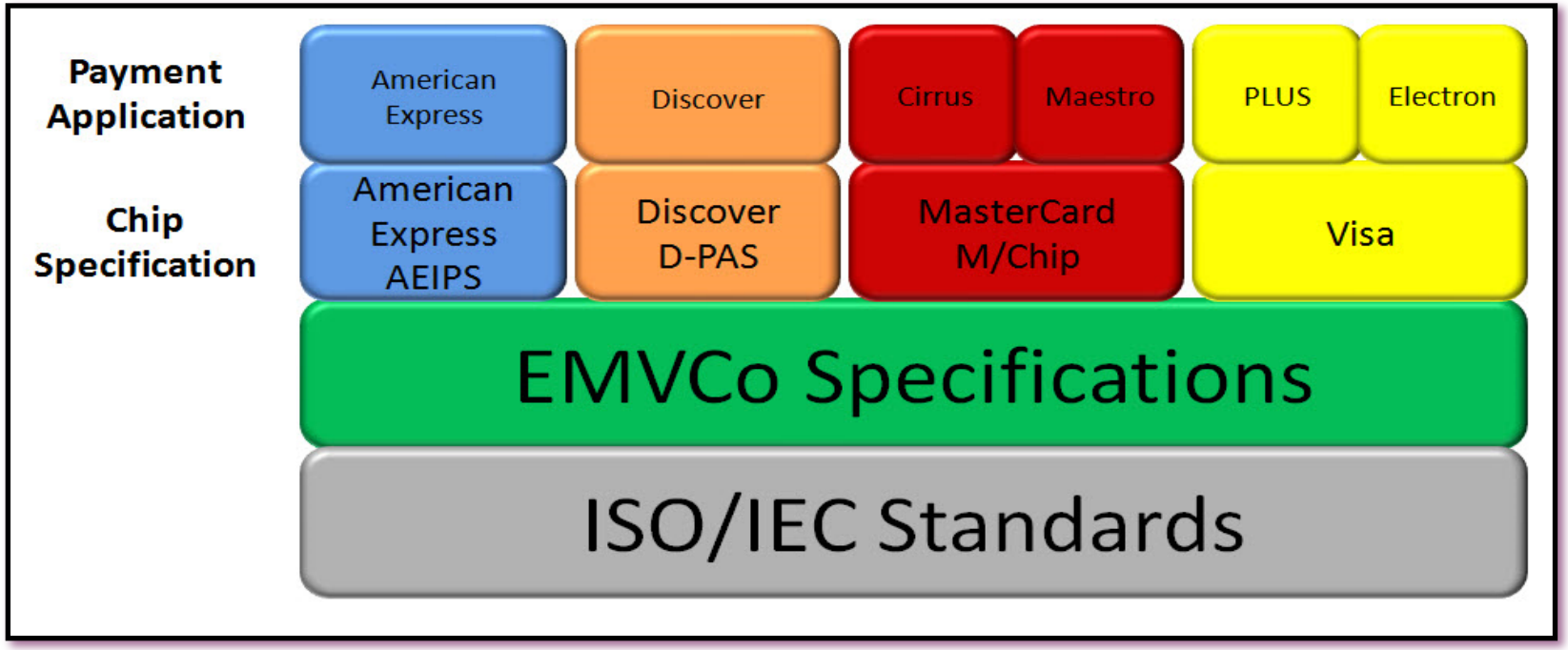
As per EMVCo specifications, when a chip card is used at a chip enabled ATM or POS device, the card and the terminal must have at least one AID in common.

The application can be automatically selected by the card and the terminal if there is only a single matching application or may require cardholder confirmation if there are multiple AIDs support.

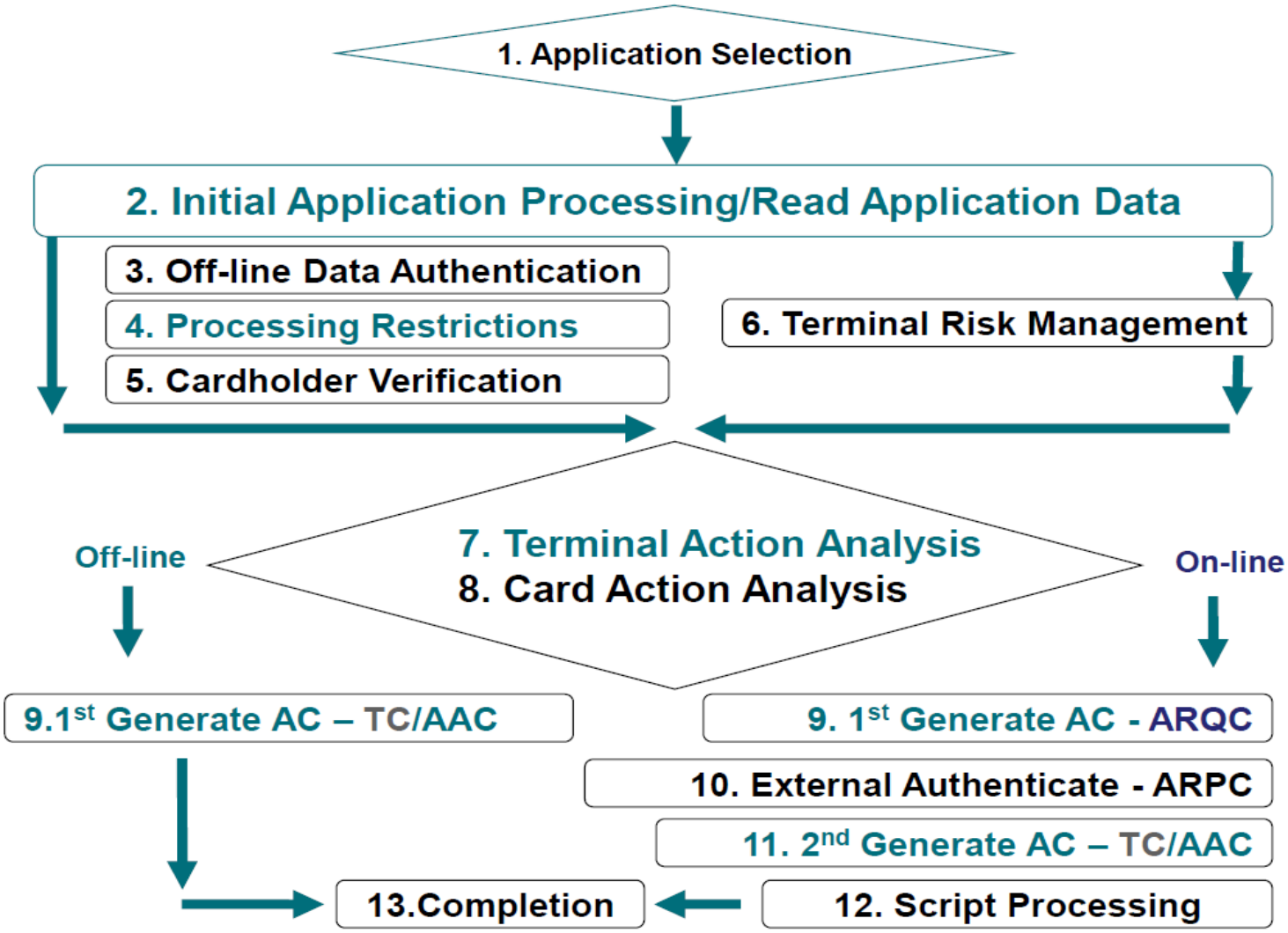
EMV® Migration Forum

EMV & Applications

The chart below is a graphical representation of the relationship between the EMVCo specifications, some of the payment system specifications, and the associated payment system products, which are also called applications (AIDs).



EMV transaction flow



EMV Migration Forum

EMV & Security: Verification method

Issuers can choose from 4 Cardholder Verification Methods (CVM's) based on customer profile and CVM options supported by Payment Brand.

- Online PIN (PIN sent and validated by the card issuer)
- Offline PIN (PIN checked with chip content)
- Signature (for Chip & Magnetic stripe card)
- No CVM (for low value transactions)

EMV® Migration Forum

EMV & Security: PIN vs Signature

Chip & Signature:

- Identity verification with Cardholder Signature

Chip & PIN:

- Identity verification with PIN entry
- PIN must correspond to information on the chip

EMV® Migration Forum

EMV & Security: Authorization method

EMV transactions can be authorized Online or Offline

✓ Online

- The cardholder's PIN (if supported) is encrypted and sent to an issuer bank
- A card cryptogram is sent to an issuer bank (Smart card, EMV, etc.).
- An issuer bank verifies the PIN or card cryptogram.
- An issuer bank makes finance verification (on-time limit, credit limit)
- An issuer bank sends approval/denial/referral(if supported) + response cryptogram

✓ Offline:

- Transactions are authorized between the terminal and the card
- Used where communication infrastructures are not always reliable
- Offline authorization is used for certain low-risk / small value transaction types and may be a consideration for contactless and mobile payments.

EMV & Security: Authentication method

Each EMV transaction request is supposed to contain **ARQC**,(a **cryptogram** generated from the transaction data).

A valid, verifiable cryptogram tells you two things:

- the financial message originated from the source
- the contents of the message have not been altered

Two cryptograms are used in EMV:

- ARQC (Authorization **Request** Cryptogram) : generated by the card
- ARPC (Authorization **Response** Cryptogram) : generated by the issuer

ARQC makes an EMV transaction unique.

Only for EMV Chip transactions.

ARPC is not always present.

EMV® Migration Forum

EMV Merchant Processor Changes

Terminal Apps

Controller Apps

Transaction Authorisation

Merchant Processor Payment Switch

Risk Management

Customer Service

MIS Analysis

Marketing

Gift Card Systems

Loyalty Systems

Merchant Acquirers

Check Services

EMV Migration Forum

= changes required

Card Brands

EMV changes things

Implies changes in every part of your Merchant Services organization, process and infrastructure

- POS Terminal application, hardware and infrastructure development (direct or VAR support)
- ATM application, hardware and infrastructure development – beware the additional rules for EMV!
- Risk management – CVM, Fallback & Interoperability support
- Switch enhancements or replacement
- Acquirer host enhancements or replacement
- Testing Considerations

Key to a successful EMV Migration

Merchant Training

EMV® Migration Forum

Background

EMV is a new and more flexible technology to the merchant

- Multiple application capability
- Offline capability
- Different CVM supports

Operational changes on EMV terminals

- Different in the way payment transactions are done
- Possibility of new types of transaction
- Different CVM requirement

It is important for merchants to be trained to ensure smooth acceptance and higher service level for EMV cards

EMV Knowledge is not a requirement for merchant users but an understanding of the process and do’s and don'ts is key to a smooth operation with minimal Interoperability issues.

EMV® Migration Forum

Message to Merchants

Difference in the cardholder acceptance experience

- Instead of swiping the card, need to insert the card

More secure and will give more confidence to consumer

- Prevents counterfeit cards from being used
- PIN can be implemented to reduce the likelihood of lost and stolen cards from being used

Can be a platform for value-added applications

Most Common Encounters

“Accidental” Fallbacks

- Chip is not detectable because card is inserted incorrectly (e.g. card not fully housed, upside down, incorrect chip etc.)
- Transaction is unable to complete as card is removed
- Terminal Entry Capability value is incorrectly correctly coded to reflect the terminal’s true card-read ability by payment scheme

Offline PIN requirement

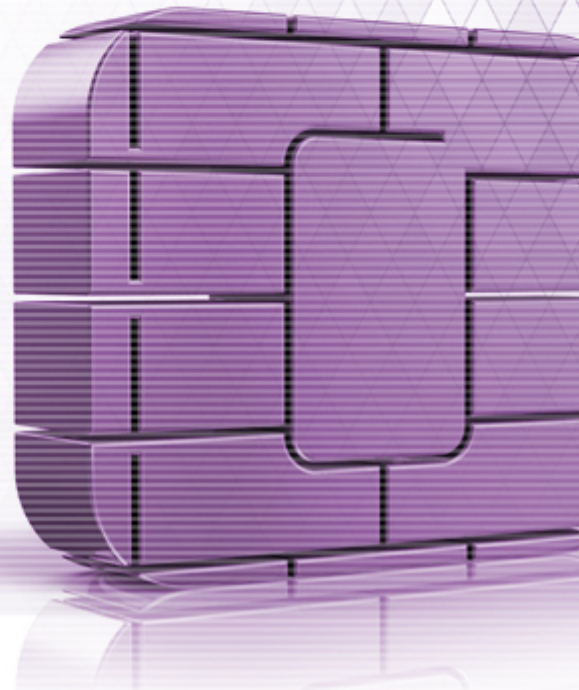
- Currently PINs are not common for credit card transactions (merchant’s choice)
- Merchants not aware of PIN implementation requirements
- Signature optional if PIN is entered

EMV® Migration Forum

Lessons learned from Global EMV Migration

Below is a small list of the most common issues that were encountered by the Brands during the EMV Migration for other regions.

- False Fallback – A very big issue from 2005-2008 for the Brands. This was due to when one Brand certified for Chip the Payment application viewed all other magstripe transactions as fallback which was not correct. It is very important when building the payment application to separate scheme payment modules as their requirements are different.
- Incorrect Terminal Profiles – A constant issue as once terminals are certified for a certain combination of Kernel and Payment Application version, the requirement from the Brand's is that this is the version that will be implemented in the field. This is something the VARs need to understand and secure from certification to Production as if there are differences then the environment will/may be considered as non-compliant.



EMV® Migration Forum

Risk of improper Testing and Terminal Management

Data Accuracy in Authorization and Clearing Messages

Acquirers must ensure the integrity and completeness of chip data in authorization and clearing messages. E.g. Erroneous messages have been seen where some acquirers have failed to ensure the integrity of data, such as:

- Cryptogram Information Data (tag 9F27), invalid value
- Unpredictable Number (tag 9F37), incorrect all zero value
- Issuer Application Data (tag 9F10), invalid padding (applied to extend it to the maximum length permitted)
- Application Interchange Profile (tag 82) (corruption)
- Cardholder Verification Method Results (tag 9F34) (corruption)
- Truncation of Field or DE 55 data (or specific tags within it such as the Application Cryptogram) by padding characters (for example, 40)
- Other tags corrupted (for example, repeated characters instead of correct tag data). Inaccurate information may hinder issuer security processing and in case of dispute, may result in acquirer liability.

EMV® Migration Forum

Summary

There is a lot to do!

Start early

Consider all aspects

Don’t under-estimate testing

Look positively at new things you can do

Work with people who have been there before

Hitch a ride along the EMV Road

Clear2Pay Americas
Umesh.Kulkarni@clear2pay.com
602.617.3871 cell

EMV@Clear2pay.com

EMV® Migration Forum

WWW.EMV-CONNECTION.COM