EMV® Migration Forum

Implementation Best Practices and Considerations

Joe Santana - FIME

Introduction

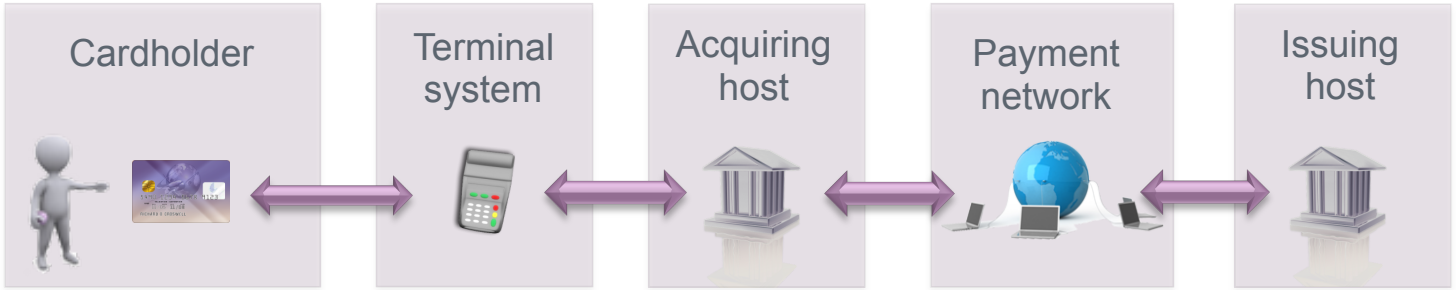
Integration of EMV into the merchant environment

- is very different to mag-stripe
- has broad/wide impacts that touch many participants
- requires an understanding of the wider environment
- planning and EMV skills are vital for successful projects

The aim of this session is to review

- the wide context of a merchant EMV implementation from development and testing perspectives
- considerations for a merchant project for VARs
- some best practices for merchant projects

The payment system context



Contactless-chip tx profiles

Contact-chip tx profiles

Mag-stripe tx profiles

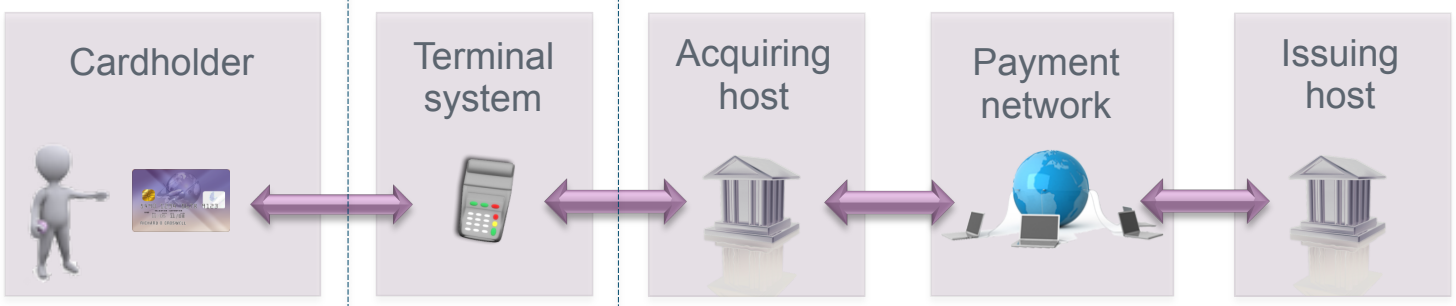
Acquiring E2E operation

Issuing operation ⟷ Card ⟷ Authorisation

- EMV requires all participant systems to operate correctly
- Transaction profiles use the same rails – best evaluated separately
- Merchant system built to acquiring, network and EMVCo rules

EMV® Migration Forum

The payment system context



Application/System — Level 3

Application/Terminal — Level 2

Terminal — Level 1

EMVCo certified components used in L3 implementations (Terminal Vendor responsibility)

- L3 requirements are defined by each payment network
- L3 involves implementation, configuration, test and certification
- L3 certification will include Payment Brand & Acquirer testing after L1/L2 certification
- L3 certification involves VAR/ISV/merchant activity with acquirers/processors

EMV® Migration Forum

The merchant context

- Merchant EMV migration
  - is a wide-impact migration project
  - each merchant situation is different

EMV Migration Forum

The merchant project considerations

- A business review is vital to decide how to manage change
  - On acceptance – brands, contact/contactless, at the POI
  - How fraud and technology will be managed
  - How existing loyalty programs will be integrated at the POI
  - How implementation and security will be managed
- Review the project plan from end to end before starting
  - Choices made early in the project can impact the back end project
  - Confirm the compatibility of business decisions and Brand Rules
    - There are many more rules around chip

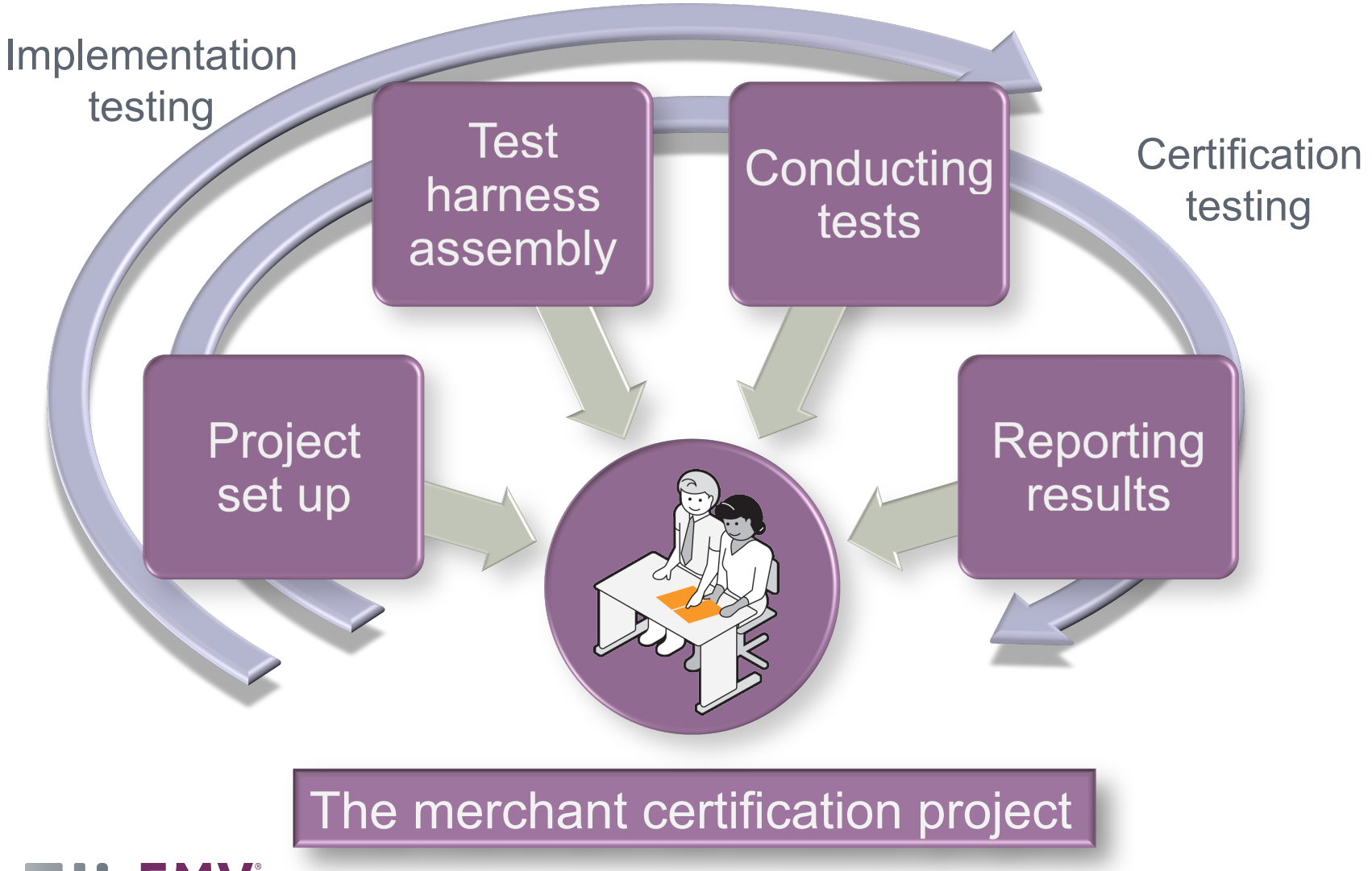
The merchant project considerations

Types of terminals – Use a semi-integrated terminal if you can

Stand-alone terminal	Semi-Integrated terminal	Integrated terminal system
Use: • For small merchants	Use: • Small-medium merchants • Uses a POS/PIN PAD incorporating a kernel, connected to cash machine • Most common solution	Use: • Medium merchants • Kernel in cash machine or backend
-	Pros: • Kernel certified by Terminal Vendor • Least complex solution	Pros: • Flexible
-	Cons: • Limited flexibility	Cons • L1/L2 certification may be required if you build/install a kernel

EMV® Migration Forum

Merchant test project overview



EMV Migration Forum

Best Practices

Ensure you have selected a terminal with:

- EMVCo Level 1 kernel that is still/recently approved
- EMVCo Level 2 kernel that is still/recently approved
- Contactless approvals if applicable
  - (Correctly configured the merchant business needs)
- PCI and any additional Brand approvals

Configuration is very important. Your terminal capabilities must not alter anything that is approved by EMVCo in the kernel.

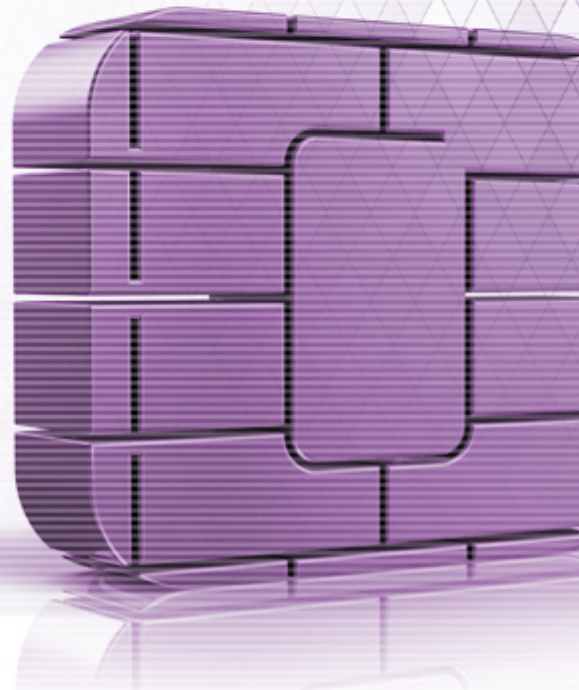
Example: CVM capabilities. If your kernel supports: Online PIN, Offline PIN, Signature and No CVM. Then your application must support this also!

Best Practices: continued…

EMVCo published bulletins explaining which capabilities/aspects of a Level 2 kernel can be changed. Worth being aware of these!!!

Understanding Fallback from Chip to Magstripe will happen.

- In such cases, no Field or DE55 data is sent in authorization messages
- POS Entry mode needs to reflect that it's fallback
- Terminal display needs to indicate to the user that the chip transaction is not possible, and they must swipe the card.



EMV® Migration Forum

Best Practices: continued…

PAN

With Chip, there are now 3 ‘areas’ where PAN data is stored. (1) on the mag stripe of the card (2) in tag 5A of the chip (3) in tag 57.

Common mistake is to continue using the traditional PAN to populate Field or DE002 in ISO EMV authorization message. Field or DE002 = Tag 5A data if it’s a chip transaction.

Just because your application may present the available AID’s for selection and your user selects which application they choose to use, you still need to populate the correct PAN from the chip.

Best Practices: continued…

Multi App Cards

If you support more than one application, then your terminal must present what the terminal & card both support to the user for them to select.

Consider what will appear on the screen

Consider your terminal receipts, any brand requirements which normally mandate that AID, Application label, and the usual PAN truncation is printed.

Best Practices: continued…

Other common issues to be aware of and to address:

Tag 9F33 Terminal Capabilities

Sending this data in authorization messages is now mandatory for some brands.

Tag 5F34 Application Pan Sequence Number

If this populated on the card, you include it in the ISO authorization message. Else, do not send.

Field or DE22 Terminal Type

This should reflect the EMVCo level 2 terminal type as per the kernel's approval.

Unpredictable Number

Being static. This needs to be different per transaction.

And…… Receipts, CA public keys, Incorrect country code, surcharging, error messages on screen

EMV® Migration Forum

FIME

Joe Santana
joe.santana@fime.com

EMV® Migration Forum

WWW.EMV-CONNECTION.COM

FIME®