EMV® Migration Forum

Payments Security Task Force (PST)

Technical Details and Lessons Learned

EMV Migration Forum/Payments Security Task Force
April 2015

About the EMV Migration Forum and the Payments Security Task Force

The EMV Migration Forum is a cross-industry body focused on supporting the 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 U.S. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV chip technology in the U.S.

For more information on the EMV Migration Forum, please visit http://www.emv-connection.com/emv-migration-forum/

Announced in March 2014, **the Payments Security Task Force** is a cross-industry group focused on driving executive level discussion that will enhance payment system security. The Task Force comprises a diverse group of participants in the U.S. electronic payments industry including payment networks, banks of various sizes, credit unions, acquirers, retailers, industry trade groups, and point-of-sale device manufacturers.

EMV® Migration Forum

Introduction: *Technical Details and Lessons Learned*

Welcome to the U.S. EMV Value-Added Reseller Qualification Program's educational webcast series, brought to you by the Payments Security Task Force and EMV Migration Forum.

This is a brief on EMV technical details and lessons learned, presented by Derek Ross of ICC Solutions.

Note: This webcast is one in a series of webcasts which will provide U.S. value added resellers, independent software vendors and merchant organizations with understanding of the U.S. market for EMV migrations, U.S. debit deployment, development preparation, lessons learned and testing considerations to assist with EMV chip migrations.

EMV® Migration Forum

What considerations are in place for more data being sent with each payment transaction?

An EMV transaction will increase the amount of data sent with each transaction. It is relatively incremental and should not impact processing bandwidth and have minimal impact on transaction times and data processing.

How does a chip transaction happen? What is the nature of card/ device/ terminal interaction?

- A chip transaction is a bit like a game of tennis where the card and terminal are players. There are three main steps to a Chip transaction:
  1. Mutual Authentication
  2. Presentation
  3. Decision Making
- For more details on debit, please refer to the Debit Webcast.

When deploying EMV, what other security solutions do I need to consider?

- Recently EMVCo introduced the EMV Tokenization Guidelines which allows replacement of data with tokenized data by taking replayable data out of the messages.
- Ensure your systems are compliant with the PCI DSS standards to reduce vulnerabilities at every point.
- Additionally, consider point-to-point encryption (P2PE) or other types of end-to-end encryption if supported by your acquirer.

What lessons have been learned from earlier implementations and merchant education?

A key success for EMV migration in other markets has been the availability of education materials and training for all stakeholders.

Education and training courses and materials are available from:

- Acquirers
- Payment Networks
- Payments Security Task Force
- EMV Migration Forum
- Smart Card Alliance
- Accredited service providers

Educate all stakeholders in order to reduce interoperability issues and ensure easy adoption of the technology. Communication can be a stronger differentiator.

EMV® Migration Forum

What is a selectable kernel? Do I need to support it?

- A selectable kernel is a piece of software that incorporates various 'switches' to activate or deactivate functionality or behaviors.
- Any merchant eligible under the "No CVM" rules of the individual payment networks and wants to leverage no CVM limit transactions, needs to ensure a selectable kernel is deployed.

What is fallback?

Fallback is the process when there is no capability to process a chip transaction for any reason due to a damaged chip card, terminal or incorrect terminal capability coding.

- It is referred to as fallback because in a list of card authentication priorities, chip has the highest priority.
- If chip is not available, the transaction falls back to magnetic-stripe processing.
- Fallback is a transaction made with a chip card and a chip-reading terminal that is not a chip transaction therefore does not benefit from the security of chip technology.

Consult with your acquirer and payment network for more details on their EMV implementation requirements.

EMV® Migration Forum

ICC Solutions
Derek Ross
info@iccsolutions.com

EMV® Migration Forum

Payments Security Task Force (PST)

WWW.EMV-CONNECTION.COM