EMV® Migration Forum

Payments Security Task Force (PST)

Kernel Management Guidelines

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: *Kernel Management Guidelines*

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 Kernel Management Guidelines, presented by Russell Wolfe of UL.

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

Kernel Management Guidelines

These guidelines are recommendations for kernel management

- Kernel management is linked to managing terminal vendor communications and standardizing solutions.
- Proper management can potentially minimize terminal testing requirements, as well as minimize the overall system impact when necessary updates/changes to existing terminals are deployed in the market.

EMV Terminal Kernel Requirements Background

- Ensure the EMV terminal has EMVCo approvals for the Interface Module or IFM and kernel at time of deployment.
- EMVCo renewal policy states an IFM approval is valid for 4 years and an application kernel approval is for 3 years. This validity period applies to both static and configurable kernels.
- Terminal changes are defined by EMVCo as major and minor based on their impacts. Major changes require EMVCo retesting and new approvals.
- Terminal vendors determine whether changes to approved IFM/kernel are considered major or minor.
- For minor changes, EMVCo retesting or new approvals are not required. The terminal vendor is responsible for managing documentation and internal test results for minor changes to the original EMVCo approval.
- Refer to EMVCo Type Approval Bulletin No. 11, 6th Edition, February 2014.

Kernel Management Guidelines

- "Approved terminals" refer to terminals that contain an EMVCo approved kernel and chip reader IFM. Different models in the same terminal family can share an approved kernel and/or chip reader.
- A terminal can continue to be deployed without risk until the kernel expires (as governed by Payment Network policies).
- Terminals can remain in market beyond the approval expiration as long as there are no changes to the kernel or chip processing logic. Includes existing inventory already in the distribution channel as long as there are no interoperability issues.
- Payment Networks have policies related to terminal approvals for payment network testing requirements.
- EMVCo approved components are largely portable, meaning an EMVCo approved application kernel may run on any terminal that has an EMVCo approved IFM.
- As a best practice, terminal vendor maintenance changes to an existing kernel are usually incorporated into the next version which would require a new certification.
- At expiration of the EMVCo approval, the terminal vendor can request an approval extension.

Testing Considerations

- Payment Networks have positions related to terminal approvals and network testing requirements.
- Acquirers should ensure that any new terminal installations contain IFMs and kernels that have a current EMVCo approval.
- Typically a minor change to a kernel would not require retesting against the Payment Network tests. It is recommended to work with your terminal vendor on kernel change impacts to your terminal configuration.
- Not all kernel changes require an upgrade. Refer to EMVCo Bulletin 11. Depending on the classification, retesting may not be required.
- If an interoperability issue is identified, changes will be required which may include updates to the kernel and payment network testing will be required.
- Anytime there are changes to chip processing impacting the payment application or the EMV kernel, payment network testing will be required.

Recommendations

- Standardize POS solutions by using the same kernel configuration.
- A kernel can be supported on more than one device (terminal family).
- Consult with your terminal vendor to determine if the terminal is the same family which can reduce testing.
- Reduce the number of configurations deployed which can reduce testing efforts.
- The current EMVCo recommendation is expired kernels should be replaced within one year after expiration date. Any new deployments would require a new approved kernel, requiring a separate payment network certification.

Recommendations

- Evaluate kernel updates, when available by the terminal vendor.
- Terminal management systems will allow for EMV configurations and parameter updates to be managed remotely and efficiently.
- The identifiers of kernels with interoperability issues are listed on the EMVCo website.
- Establish ongoing communication with your terminal vendor.
- If an interoperability issue is identified, the acquirer will need to be able to make the necessary changes which may include updates to the kernel. Payment network testing will also be required.

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

UL - Transaction Security Division
Russell Wolfe
Russell.Wolfe@ul.com

EMV® Migration Forum

Payments Security Task Force (PST)

WWW.EMV-CONNECTION.COM