



## **Testing and Certification Working Committee**

# **EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community**

**Version 1.0**

Date: July 2013

## ***About the EMV Migration Forum***

The EMV Migration Forum is a cross-industry body focused on supporting an alignment of the EMV implementation steps required for global and regional payment networks, issuers, processors, merchants, and consumers to ensure a successful move from magnetic stripe technology to more secure EMV contact and contactless technology in the United States. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States. For more information on the EMV Migration Forum, please visit <http://www.emv-connection.com/emv-migration-forum/>.

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION.....</b>	<b>5</b>
<b>2</b>	<b>ACQUIRER HOST TESTING REQUIREMENTS .....</b>	<b>6</b>
2.1	MASTERCARD NIV CERTIFICATION .....	6
2.1.1	Requirements for Testing.....	6
2.1.2	Test Execution .....	7
2.1.3	MasterCard Accreditation Program.....	7
2.2	VISA ACQUIRER HOST TESTING REQUIREMENT.....	7
2.3	DISCOVER ACQUIRER HOST CERTIFICATION .....	8
2.3.1	Prerequisites .....	8
2.3.2	Initiation.....	8
2.3.3	Test Execution .....	9
2.3.4	Review Process.....	9
2.4	AMERICAN EXPRESS HOST CERTIFICATION.....	10
2.4.1	Certification Requirements .....	10
2.4.2	Certification Process .....	10
<b>3</b>	<b>TERMINAL TESTING REQUIREMENTS .....</b>	<b>11</b>
3.1	MASTERCARD TERMINAL TESTING.....	12
3.1.1	Requirements .....	12
3.1.2	Registering the M-TIP .....	12
3.1.3	Test Execution .....	14
3.1.4	M-TIP Service Providers.....	14
3.1.5	Test Tips .....	14
3.1.6	M-TIP Self-Approval .....	14
3.1.7	MasterCard Accreditation Program.....	15
3.2	VISA TERMINAL TESTING REQUIREMENTS .....	15
3.2.1	Acquirer Device Validation Toolkit.....	15
3.2.2	Contactless Device Evaluation Toolkit .....	16
3.2.3	qVSDC Device Module.....	16
3.2.4	Additional Toolkit Requirements.....	17
3.2.5	Chip Compliance Reporting Tool.....	17
3.3	DISCOVER E2E CERTIFICATION TESTING .....	21
3.3.1	Prerequisites .....	21
3.3.2	Initiation.....	21
3.3.3	Test Execution .....	21
3.3.4	Results.....	21
3.3.5	Review Process.....	21
3.4	AMERICAN EXPRESS END-TO-END CERTIFICATION .....	22
3.4.1	American Express Certification Requirements .....	22
3.4.2	Certification Process Steps.....	22
3.4.3	Prerequisites for Device Certification.....	22
<b>4</b>	<b>OTHER REQUIRED TESTING PROCESSES .....</b>	<b>24</b>
4.1	MASTERCARD END-TO-END DEMONSTRATION .....	24
4.2	DISCOVER ACQUIRER PRODUCTION VALIDATION TEST .....	24
4.2.1	Prerequisites .....	24
4.2.2	Initiation.....	24
4.2.3	Test Execution .....	24

EMV Migration Forum: Testing and Certification Committee  
Current U.S. EMV Testing and Certification Requirements for the Acquiring Community

<b>5</b>	<b>WHEN TERMINAL TESTING IS NEEDED .....</b>	<b>25</b>
5.1	ATM USE CASES .....	25
5.2	TERMINAL USE CASES .....	26
5.2.1	<i>Semi-Integrated Terminal Use Cases</i> .....	27
5.2.2	<i>Stand-alone Terminal Use Cases</i> .....	28
5.3	ACQUIRER-PROCESSOR PLATFORM .....	28
5.4	VALUE-ADDED RESELLER .....	29
<b>6</b>	<b>REFERENCES.....</b>	<b>30</b>
<b>7</b>	<b>PUBLICATION ACKNOWLEDGEMENTS .....</b>	<b>31</b>

## 1 Introduction

All payment brands have acquirer host and EMV chip terminal testing processes to maintain and ensure the integrity of the payment brand infrastructure and a frictionless cardholder acceptance experience. The American Express, Discover, MasterCard and Visa testing requirements are global and are therefore relevant to the U.S. market also in order to reduce any potential interoperability issues in production. These processes follow the EMV specification which is the agreed industry standard and each payment brand's application specification, with an objective of ensuring interoperability between all host systems, payment devices, and cardholder devices.

By benefitting from global knowledge and experience, the payment brands have developed, and continually strive to improve, the testing process while maintaining the balance of when to test in order to minimize any risk of deployment issues into production. This document defines the current processes required to test EMV chip transactions with MasterCard, Visa, American Express, and Discover (referred to collectively as the payment brands).<sup>1</sup> Brand-specific issues, concerns, or questions related to these processes should be directed to the appropriate payment brand. This document is intended to provide a clear approach to acquirer host and EMV chip terminal testing and certification, and includes examples of common use cases.

It is important to note that the processes described in this document cover the current acquirer testing requirements for the payment brands referenced above. These testing processes also support direct connect merchants which are directly connected to the payment brands. Merchants not directly connected to the payment brands should work with their acquirer on testing requirements and are out of scope for this document. The white paper does not describe testing for U.S. regional debit payment brands.<sup>2</sup> The EMV Migration Forum plans to provide updates and additional educational resources as other requirements and streamlined testing and certification processes are documented. There will be a separate document providing the payment brand issuer testing requirements.

Throughout this document, you will see the term *required testing*, which the payment brands have agreed to use as a common term. Each payment brand also uses brand-specific references or terms (e.g., certification, qualification, confirmation, approval). The term *required testing* is used in generic areas, and each brand's terminology is used as appropriate in brand-specific sections.

The document is the result of input from Acquirer Systems, American Express, Chase, Discover, ICC Solutions, MasterCard, TSYS, UL Transaction Security, Vantiv, VeriFone, and Visa.

Comments on or recommendations for edits or additions to this document should be submitted to [certification-feedback@us-emvforum.org](mailto:certification-feedback@us-emvforum.org).

---

<sup>1</sup> In addition to the payment brand requirements discussed in this white paper, EMVCo Level 1 and Level 2 terminal type approvals are a prerequisite for the payment brand testing requirements for EMV chip terminals. Refer to page 11 for details.

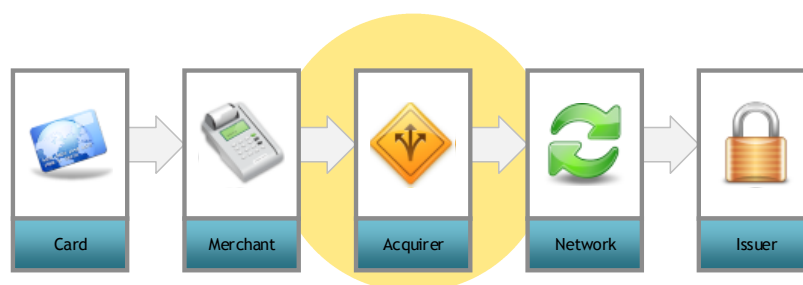
<sup>2</sup> At the time of the creation of this document, the debit network testing specifications were not available.

## 2 Acquirer Host Testing Requirements

This section outlines the host testing requirements for acquirers, acquirer processors, and direct-connect merchants who will process EMV chip transactions and are directly connected to the payment brands. The testing process is designed to test the capability to carry full chip data correctly in Field 55 and related chip values in existing fields to support EMV contact chip and contactless transactions.

The required testing is to be performed once for each platform. Testing with each payment brand was required to be completed by April 2013, as per payment brand mandates.

Figure 1 illustrates the relative position of the acquirer host in the payment process.



**Figure 1. Acquirer Host Position in the Payment Process**

### 2.1 MasterCard NIV Certification

The objective of the MasterCard network interface testing (NIV) process is to validate the interface between the customer host and the MasterCard network(s) with particular emphasis on the following:

- ISO/IEC 8583 interfaces
- EMV contact and *PayPass* M/chip transactions, depending on customer profiles or requirements.

NIV includes test and validation activities for authorization and clearing processing.

#### 2.1.1 Requirements for Testing

**NIV Test Tools.** Depending on their implementation, the NIV test tools comprise physical chip cards or a chip card simulator, and EMV card/terminal trace functionality. Use the latest version of the tools. The manual *M/Chip Qualified Test Tools* lists the relevant test tools (for EMV contact, for EMV Contact-PIN Management and for *PayPass* M/chip) together with contact information about the tool vendors. The manual is available on MasterCard Connect.

**Simulators.** Install the latest version of the MasterCard MAS simulator for the dual message system or the MasterCard Debit Financial Simulator (MDFS) for the single message system and obtain the relevant valid MasterCard simulator license. The MasterCard simulators can be ordered (or upgraded) on MasterCard Connect under Simulator Suite. Online attended testing is available as an option as well for acquirers.

**Chip Terminal.** NIV testing performs a number of chip transactions with the NIV test tool. A chip terminal or chip terminal simulator must be connected to the test bed's acquiring infrastructure to run these transactions.

*Test Specifications.* The latest *Customer Interface Testing Reference* (CITR) is required (available on MasterCard Connect under Member Publications).

### **2.1.2 Test Execution**

Your assigned MasterCard implementation specialist will assist you with technical or testing-related questions or required activities. This assistance includes generating the appropriate NIV test cases.

### **2.1.3 MasterCard Accreditation Program**

MasterCard runs an accreditation program whereby third parties are recognized for their chip-related expertise.

MasterCard customers lacking in-house chip-related expertise usually seek external expert support when implementing chip in their organization. MasterCard's Third Party Accreditation Program helps MasterCard customers identifying suppliers with suitable skills and expertise for supporting them during migration to contact EMV and contactless chip products or deployment of new chip-enabled cards and terminals. Based on their respective expertise and areas of activities, suppliers may be accredited in one or several of the following three categories:

- Guidance
- Technical Support for Issuers
- Technical Support for Acquirers

## **2.2 Visa Acquirer Host Testing Requirement**

Visa's plan to accelerate migration to contact and contactless EMV chip technology in the U.S. required acquirers and acquirer processors to support full chip data including Field 55-Integrated Circuit Card (ICC) related data and additional fields processed in BASE I and VisaNet Integrated Payment (VIP) authorization and full financial messages for Visa Smart Debit and Visa Smart Credit (VSDC) on all host platforms that support face-to-face POS transactions, **effective April 1, 2013.**

The details of the available infrastructure to complete the host requirements are as follows:

- Attended testing is required.
- Use of physical Global Host Test Cards and scripts.
- Managed by a project.
- Testing performed with use of a POS device. A terminal emulator solution was available for acquirers to support the U.S. EMV chip migration mandate deadline. An acquirer will be required to support Visa's terminal testing requirements before deploying a terminal to market.
- Support of both quick Visa Smart Debit Credit (qVSDC) and magnetic-stripe data (MSD) legacy contactless transactions.
- Validation of compliance with VIP authorization and full financial messages for each unique host platform.
- If using a POS device, terminal testing is required before host testing can begin. A production-ready terminal is required to generate online authorization messages for host testing.
- Settlement testing is optional and only required if offline authorization of transactions is supported.
- A testing completion letter is provided when host testing is completed successfully.

- Production activation is required to implement full chip data with Field 55 for the first time, requiring the appropriate Visa paperwork. Visa made default systems changes to enable all U.S. acquirers to support full chip and Field 55 on April 1, 2013. Processor parameters will require the appropriate Visa paperwork.

Acquirers and acquirer processors are required to meet these EMV testing requirements. Support is optional for direct connect merchants.

Contact your Visa representative for more information.

## **2.3 Discover Acquirer Host Certification**

Executing Discover acquirer host certification ensures that the acquirer, acquirer processor, or direct-connect merchant's host system meets the messaging requirements listed in the *Discover Authorization Interface Technical Specifications* and *Discover Sales Data Interface Technical Specifications*.

Discover acquirer host certification includes the D-PAS Acquirer Network Online test and the D-PAS Acquirer Clearing test.

The D-PAS Acquirer Network Online Test ensures that the acquirer's host authorization messaging meets the following criteria:

- Successfully sends and receives authorization requests and responses, including additional chip data, in accordance with the Discover authorization message requirements detailed in the *Discover Authorization Interface Technical Specifications*.
- Successfully processes all chip response data, expected or unexpected, from the network or the issuer.
- Successfully processes PIN management transactions, if supported.

The D-PAS Acquirer Clearing Test ensures that the acquirer's host system meets the following criteria:

- Successfully generates a clearing data file in accordance with the applicable Discover clearing format.
- Successfully sends clearing files in accordance with the *Discover Sales Data Interface Technical Specifications*.

### **2.3.1 Prerequisites**

Discover requires the following activities before beginning acquirer host certification:

- Completion of required network release certification
- Completion of acquirer host system changes required for processing D-PAS authorization and clearing
- Connection to the Discover Release Compliance Tool (RCT) or the Discover Production Assurance (PA) environment

Purchase of a Discover-approved test tool for offline pre-certification testing is optional.

### **2.3.2 Initiation**

The acquirer, acquirer processor, or direct-connect merchant must complete the following documents before starting the certification process:



- D-PAS Certification Request Form. This form provides details on the functions that acquirers intend to support and on their planned timelines for certification testing. Discover assigns necessary test cases based on this information.
- D-PAS Card Request Form. This form is used to request physical test cards.
- CA Security Officer Registration Form. This form is used to register security officers and obtain CA public keys.

All forms can be obtained by contacting the assigned Discover account executive.

### 2.3.3 Test Execution

- **Transaction Generation**

To generate transactions, Discover prefers that acquirers use a physical terminal and test cards or a test card simulator for the D-PAS Acquirer Network Online Test and the DPAS Acquirer Clearing Test. However, Discover will allow the use of a POS simulator or transaction generator if a terminal is not available for these tests.

If the POS simulator or transaction generator used can only generate static data, additional test cases will be required as part of the end-to-end testing process (i.e., test cases validating certain cryptographic scenarios).

- **Test Tools**

Two test tools are available to execute D-PAS Acquirer Network Online testing and D-PAS Acquirer Clearing testing.

During test execution, technical help is coordinated by the assigned Discover account executive.

- A. Release Compliance Tool (RCT)**

The preferred method for executing acquirer host testing is using the Discover RCT.

Acquirers can access the tool at any time, conduct their testing, and view their results immediately. Test log submission is not required; however, a one-to-one correlation of test cases to transactions should be provided to Discover. Participants are required to run a clean test batch for submission.

Acquirers are also required to submit a clearing file containing chip transaction records for assigned tests.

- B. Discover Production Assurance Environment**

In addition to RCT, Discover has an attended online production assurance (PA) environment in which Acquirer Network Online Tests can be executed. Clearing files can also be submitted through the PA environment.

### 2.3.4 Review Process

Discover reviews the results of each test. Results are communicated within agreed service level agreements (SLAs). Following successful testing, a letter of certification is issued to the acquirer, acquirer processor, or direct-connect merchant.

## **2.4 American Express Host Certification**

American Express network requirements for EMV chip-based contact, contactless, and mobile transactions require that U.S. acquirers, and acquirer-processors certify by April 2013.

For additional information on requirements and certification process, please contact your American Express representative.

Certification is also required for merchants connecting directly onto the American Express network in support of EMV chip-based contact, contactless, and mobile transactions. Please contact your American Express representative for additional information.

### **2.4.1 Certification Requirements**

American Express requires the acquirer, acquirer-processor, or merchant to demonstrate their ability to support chip card acceptance as outlined in the *American Express ICC Payment Specification (AEIPS)* and *Expresspay Contactless Specification*.

Requirements in support of EMV contact/contactless include the need to certify acquirer, acquirer-processor, or merchant host connection for authorization and settlement.

For authorization and settlement specifications and additional detail log on to:

<http://www.americanexpress.com/merchantspecs>

### **2.4.2 Certification Process**

The certification process steps are as follows:

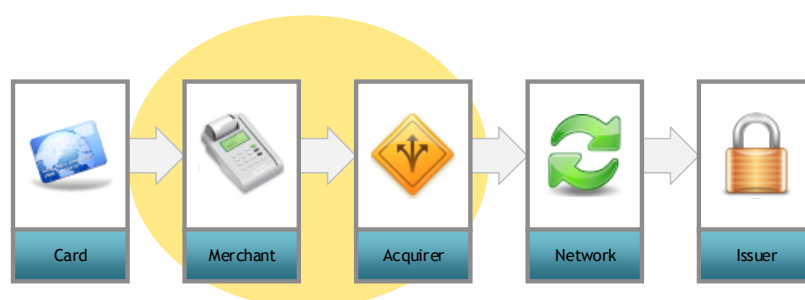
1. The acquirer, acquirer-processor, or merchant notifies American Express they are ready to commence certification.
2. American Express initiates a project request.
3. American Express assigns a certification resource to the project.
4. American Express reviews the certification process and requirements with the acquirer, acquirer-processor, or merchant.
5. American Express reviews test plan and message specifications with the acquirer, acquirer-processor, or merchant.
6. The acquirer, acquirer-processor, or merchant executes test plan successfully.
7. American Express issues an Authorization Test Plan/Certification Summary designating successful completion of host certification.
8. The acquirer, acquirer-processor, or merchant moves into production.

Please contact your American Express representative to start the certification process.

### 3 Terminal Testing Requirements

This section outlines the EMV chip process for completing the required terminal testing for the various payment brands. “Terminals” means all EMV-related terminal types, including POS devices, ATMs, bank branches, unattended devices, and on-board terminals.

Terminal testing is the responsibility of the acquirer. Required terminal testing does not focus solely on the terminal; it examines anything that sits between the card and the payment brand. Figure 2 illustrates what areas are covered by terminal testing.



**Figure 2. Areas Covered by Terminal Testing**

The use of EMV chip (as compared to magnetic stripe) introduces increased complexity into the acceptance process. Terminals deployed in one country or region can experience acceptance problems when used with cards from other countries or regions, even though both the cards and terminals have been EMV or payment-brand approved. These issues may be the result of incorrect terminal configuration, inadequate integration testing, or misunderstandings about EMV.

To help ensure that acquirers deploy terminals that do not contribute to interoperability problems, all payment brands have developed requirements for testing terminals before global deployment of EMV chip terminals.

The payment brand testing outlined in the following sections takes place after both EMVCo Type Approval Level 1 and Level 2 terminal approval and precedes terminal deployment. EMVCo Level 1 Terminal Type Approval measures the conformance of interface modules (IFM) to the EMV-defined set of electrical, mechanical, and communication protocol characteristics. (Interface modules support communication between the device and the chip card.) EMVCo Level 2 Terminal Type Approval measures the conformance of the terminal-resident application software that supports specified EMV functionality, both required and optional. Information about these approvals can be found on <http://www.EMVCo.com>.

Currently, payment brand terminal testing is required in the following situations:

- New hardware, a new EMV-approved kernel, or new payment application software is introduced, or payment-related configuration changes are made.
- Hardware or software is modified significantly, a new communication interface is implemented, or an EMV-approved kernel is changed on a deployed terminal.
- Hardware, software, or parameter settings are changed and the change impacts the payment application.
- Terminal to acquirer messaging is changed.

### **3.1 MasterCard Terminal Testing**

The MasterCard terminal integration process (M-TIP) is MasterCard's process for testing terminals integrated into an EMV environment. This testing can only take place after valid NIV approval is obtained. Testing is performed once on any combination of EMVCo Level 2 kernel and payment application that is intended to be deployed in the field. M-TIP projects can be initiated for a contact and/or contactless terminal.

A MasterCard end-to-end demonstration (ETED) is required for initial chip migration for either ATM or POS (see "MasterCard " on p. 24).

#### **3.1.1 Requirements**

Preparation for an M-TIP project requires the following:

Simulator. Install the latest versions of the MasterCard MAS simulator for the dual message system or the MasterCard Debit Financial Simulator (MDFS) for the single message system and obtain the relevant valid MasterCard simulator license. The MasterCard simulators can be ordered (or upgraded) on MasterCard Connect under Simulator Suite.

In addition, preparation for an EMV contact M-TIP project requires the following:

EMV Level 1 and Level 2 Certificates. Obtain Level 1<sup>3</sup> and 2 certificates from your software vendor/VAR/integrator. These certificates include three pieces of required information: the Issuer Conformance Statement (ICS), approval numbers, and kernel name.<sup>4</sup> The EMV level 1 device is the hardware that accepts the card. This device could be a terminal, a card-reading device on an ATM, or an unattended solution.

Application Details. Obtain the name and version number of the application that handles all payment information and implements the terminal-to-acquirer host protocol. The application version number will appear in the M-TIP letter of approval

Qualified EMV Contact M-TIP Test Tool. The list of qualified EMV contact M-TIP test tools and their suppliers can be found on MasterCard Connect. Procure the latest version.

Preparation for a *PayPass* M-TIP project requires the following:

PayPass Vendor Product Letter of Approval. Obtain this letter from your terminal vendor/VAR/integrator.

Qualified PayPass M-TIP Test Tool. The list of qualified *PayPass* M-TIP test tools and their suppliers can be found on MasterCard Connect. Procure the latest version.

#### **3.1.2 Registering the M-TIP**

Before starting an M-TIP project, go to MasterCard Connect and download the latest M-TIP questionnaire(s), *M-TIP Process Guide*, and relevant test-case user guides. There are separate M-TIP

---

<sup>3</sup> The EMV level 1 device is the hardware that accepts the card.

<sup>4</sup> These certificates are also available on <http://www.emvco.com>. Confirm with your provider that you have the correct certificates so as not to impact certification at a later stage.

questionnaires for EMV contact and for *PayPass*. The questionnaires must be completed by the acquirer and the VAR.

Once all appropriate questionnaires have been completed, you will generate a unique M-TIP reference number and a test plan. This test plan is based on answers to the questionnaire, so it is important that the answers are correct.

Table 1 lists the main questions required to test contact EMV and an explanation of what should be completed.

**Table 1. Information Required for Contact EMV M-TIP Testing**

Information	Explanation	Source
Terminal brand	The brand of payment terminal being tested (for example, Verifone, Ingenico, Equinox)	–
Terminal model	The model number of the terminal being tested (for example, VeriFone VX510)	–
EMVCo Level 1 approval reference	Level 1 approval for the terminal.	Find this number on the certificate from the hardware supplier. Verify that the approval reference is valid by checking this reference on <a href="http://www.emvco.com">http://www.emvco.com</a> .
EMVCo Level 2 approval reference	Level 2 approval for the terminal.	Find this number on the certificate from the kernel provider. (Hardware and software certifications may be supplied by different companies.) Verify that the approval reference is valid by checking this reference on <a href="http://www.emvco.com">http://www.emvco.com</a> .
TQM label or action plan reference	Terminal Quality Management (TQM) is a MasterCard process that payment terminal hardware must go through.	Obtain the reference number from your hardware provider.
PCI-PED approval reference	Security certification of the PIN pad, if any.	Obtain the approval reference from your hardware provider.
EMV kernel name	The kernel name must match the kernel name on the EMV Level 2 certificate.	Obtain the kernel name from the letter of approval.
Payment acceptance application software version	Version number of the software being tested. Minor updates could cause this to change but not affect certification	–

Information	Explanation	Source
Terminal type	The type of EMV terminal being used by the acquirer for the M-TIP: e.g., attended POS, CAT Level 1 terminal	–
Online/offline capability of the terminal type	–	Defined in the EMVCo Level 2 certificate. Use the precise wording in the certificate.
Whether a combined reader is being tested	A combined reader can handle both chip and magnetic stripe transactions. This question is used to define testing for session management.	

### 3.1.3 Test Execution

For the dual message system, tests are run against the MasterCard MAS simulator. For the single message system, tests are run against the MasterCard Debit Financial Simulator (MDFS). For each test, both one card/terminal log and the simulator log must be recorded. The simulator log can either be saved for each transaction or for the test run. The tests require checking a variety of data in both logs to determine success.

### 3.1.4 M-TIP Service Providers

MasterCard has accredited a number of approval service providers who can analyze test results and validate that they are in line with the responses required by MasterCard. The list of accredited M-TIP service providers is available on MasterCard Connect. Once the testing process is complete, the provider issues a letter of approval on behalf of MasterCard. The terminal can then be deployed.

### 3.1.5 Test Tips

The following tips can facilitate testing:

- Use the unpredictable number to match terminal logs and simulator logs. This practice ensures that the correct logs are being used; sometimes transactions are repeated, and logs and data can be confused.
- Make sure the terminal capabilities match what is defined in the applicable EMVCo Level 2 certificate.
- When running tests, save the simulator log after every transaction or after every group of tests. This will ensure that logs are not recorded incorrectly.
- Build the interoperability test pack (which is part of the M-TIP test tool) into the regression testing; the interoperability test pack is based on real cards from international markets.

### 3.1.6 M-TIP Self-Approval

Acquirers who deploy a significant number of different terminal configurations can take advantage of the M-TIP self-approval program. The self-approval program validates, through an audit-based process,

the ability of an acquirer to analyze test results correctly. Acquirers who enroll in this program can be authorized to complete M-TIP on their own, without recourse to an M-TIP service provider.<sup>5</sup>

### **3.1.7 MasterCard Accreditation Program**

As described in Section 2.1.3, MasterCard runs an accreditation program whereby third parties are recognized for their chip-related expertise.

MasterCard customers lacking in-house chip related expertise usually seek external expert support when implementing chip in their organization. MasterCard's Third Party Accreditation Program helps MasterCard customers identifying suppliers with suitable skills and expertise for supporting them during migration to contact EMV and contactless chip products or deployment of new chip-enabled cards and terminals.

## **3.2 Visa Terminal Testing Requirements**

Visa developed the Acquirer Device Validation Toolkit (ADVT) and Contactless Device Evaluation Toolkit (CDET) to provide a separate set of test cards and test cases for EMV contact chip and contactless acceptance validation. The toolkits are used to validate correct terminal configuration, assist with integration testing, and ensure that Visa's terminal requirements are met before terminals are deployed. At a minimum a terminal must meet EMV Level 1 and EMV Level 2 requirements and be listed on the EMVCo website at <http://www.emvco.com>. For details on Visa approved contactless devices, refer to the Visa Technology Partner website at <https://technologypartner.visa.com/>. In addition, the quick Visa Smart Debit Credit Device Module (qVSDC DM) was developed both to address specific product approval self-testing requirements for Visa payWave readers and deployment of stand-alone contactless readers compliant with the Visa Contactless Payment Specification (VCPS) and to support quick Visa Smart Debit and Credit (qVSDC). The test results are submitted to Visa via the Chip Compliance Reporting Tool (CCRT). The requirements for each toolkit are outlined below.

### **3.2.1 Acquirer Device Validation Toolkit**

Acquirers are mandated to use the ADVT prior to initial deployment of EMV chip terminals to ensure that the terminal is configured correctly.<sup>6</sup> The ADVT must also be used if there are major changes to an EMV-approved terminal that affect the payment application, including changes to kernels or interface modules (IFMs) for chip processing or changes to the network infrastructure. Visa also recommends using ADVT when dynamic currency conversion is introduced or if an upgrade or modification to the acquirer's host system may affect the transmission of chip data.

To encourage the deployment of modern kernels and IFMs that are less susceptible to interoperability issues, acquirers must not submit ADVT test results for kernels and IFMs that have expired. This does not affect the deployment of terminals already approved using ADVT. However, it helps prevent the deployment of new or updated terminal configurations that use expired hardware or software.

---

<sup>5</sup> For more information on the self-approval program, contact MasterCard.

<sup>6</sup> In addition, Visa strongly recommends that acquirers use the toolkit on previously deployed terminals to determine whether there are potential acceptance problems.

Visa may ask the acquirer to undertake further ADVT testing if it seems likely that a terminal is causing acceptance or interoperability problems.

Acquirers can also use a subset of the test cards in the toolkit to conduct online transactions through a connection to the VisaNet Certification Management Service (VCMS) or a Visa-confirmed third-party-supplied host simulator.

Further information regarding ADVT can be found in the *Acquirer Device Validation Toolkit User Guide*, which is included in the toolkit.

### **3.2.2 Contactless Device Evaluation Toolkit**

Like the ADVT, the CDET is a set of test cards and an accompanying user guide that allows an acquirer to validate the correct configuration of contactless readers.

The toolkit is also a self-administered solution similar to ADVT. Each test card corresponds to a required test case that has to be performed. For new reader deployments, the intent is for the acquirer to run through each applicable test case and make modifications until the expected outcome is reached.

If Visa or the acquirer suspects there is a problem with a deployed terminal, it is recommended that all applicable tests specified in CDET be performed to assist with the analysis.

If changes are made to the configuration of a previously deployed terminal, it is recommended that an acquirer rerun all applicable test cases to provide a level of confidence in the changes.

Visa rules required that effective April 1, 2013, all new Visa payWave-accepting contactless readers deployed in the U.S. must actively support both magnetic-stripe data (MSD) and qVSDC. Acquirers need to be familiar with the CDET requirements before deploying new terminals.

Further information regarding the use of CDET can be found in the *Visa Contactless Device Evaluation Toolkit User Guide*, which is included in the toolkit.

### **3.2.3 qVSDC Device Module**

The qVSDC DM was developed to address specific product approval self-testing requirements for Visa payWave acquirers deploying stand-alone contactless readers compliant with the Visa Contactless Payment Specification (VCPS) and supporting the qVSDC path. Before activating and deploying stand-alone contactless readers, Visa payWave acquirers must use the qVSDC DM and validate successful results as part of the overall contactless reader approval process. Testing is optional for dual-interface (contact and contactless) integrated readers being deployed in the U.S.

Use of the qVSDC DM is governed by the same rules and policies that apply to ADVT. That is, use of the toolkit is mandatory before deploying a new stand-alone device or when an acquirer has modified software on an existing deployed device to support Visa payWave acceptance. In the specific case of a Visa payWave acquirer deploying a new qVSDC-supporting stand-alone reader into its existing acceptance environment, use of the qVSDC DM is required to complete the self-testing component of the device approval process before deployment.

Use of qVSDC DM is limited to contactless stand-alone readers supporting qVSDC. It does not apply to readers supporting only MSD legacy contactless, such as those currently deployed in the U.S.

For further information regarding the use of qVSDC DM, refer to the *qVSDC Device Module Test Cases* document.



### **3.2.4 Additional Toolkit Requirements**

Acquirers are required to use the ADVT, the CDET, and the qVSDC DM (conditional) toolkit prior to initial terminal deployment (including all variations of hardware, software, and parameter settings) to ensure that the terminal has been set up and configured correctly. It is expected that acquirers will run every applicable test to gain the full benefits of each toolkit. When the acquirer's test results do not match the expected test outcome, the acquirer should work with the terminal vendor (and Visa, if necessary) to correct the problem. The acquirer should repeat the test until the problem is resolved and the test result matches the expected outcome. An acquirer who fails to use the ADVT, the CDET, or the qVSDC DM (conditional) toolkits on a device that causes interoperability issues may be subject to fines, as defined in the Visa Chip Interoperability Compliance Program.

In addition, it is strongly recommended that acquirers use the toolkits on previously deployed EMV contact-chip and Visa payWave-accepting contactless terminals to ascertain whether there are potential acceptance problems.

Use of the ADVT and the CDET is intended to ensure that basic EMV contact chip and contactless functionality is not compromised during application integration, that Visa requirements are met, and to uncover exposure to certain common interoperability issues. Use of the toolkits does not imply or guarantee that a terminal is fully compliant with EMV specifications or Visa requirements.

The ADVT and the CDET can be obtained through Visa's third-party fulfillment service, Merrill Corporation. Substantially similar tools are also available from Visa-confirmed third party vendors. For a list of Visa-confirmed tool vendors, see Products and Toolkits at <https://technologypartner.visa.com/>.

After an acquirer successfully completes ADVT and CDET testing (and qVSDC DM testing if applicable), the Chip Compliance Reporting Tool (CCRT) must be used to submit the test results to Visa. The submission of the applicable test results for compliance reporting needs to be completed to ensure chip and contactless acquirers minimize the risk of interoperability problems.

### **3.2.5 Chip Compliance Reporting Tool**

Visa developed the CCRT as a centralized, server-based solution for the systematic reporting of ADVT, CDET, and qVSDC DM (if applicable) test results. CCRT facilitates an efficient submission and management process for compliance reporting by chip and contactless acquirers. CCRT allows users to:

- Submit new compliance reports
- Review and update draft reports
- Review status online and manage reports submitted to Visa automatically
- Track approved and submitted reports

Use of the CCRT provides Visa-acquiring clients with an appropriate level of security and confidentiality in managing terminal test results; the CCRT service can be consolidated with other services currently provided to Visa clients. CCRT is available on Visa Online, which is Visa's online solution for providing secure access to Visa content and services for clients globally. It reduces potential errors in manual entry by guiding users to choose from applicable options and provide mandatory information. Current reports can be used as a starting point for new reporting, reducing time spent completing the reports.

EMV Migration Forum: Testing and Certification Committee  
Current U.S. EMV Testing and Certification Requirements for the Acquiring Community

Acquirers or their processors are required to use the CCRT to submit terminal test results. Visa will accept test results only if they are submitted using the CCRT. Terminal test results must be submitted for each region separately. Acquirers should discuss enrollment requirements and use of CCRT with their Visa representative. For processors to submit terminal test results on behalf of their acquirers, an Acquirer Acknowledgement Form is required.

Table 2 summarizes the steps required to submit a report using CCRT.

**Table 2. Steps Required to Submit a Report Using CCRT**

Step	Description
Client information	Provide information about the client, including contact details and Visa-related licensing information used for testing.
ADVT/CDET test information	Provide mandatory information on the Compliance Test Information, Payment Application and EMV, Terminal Resident Data Objects, and Terminal Details screens.
qVSDC DM test information	Provide mandatory information on the Reader Details and Reader Configuration Detail screens, if applicable.
Enter data	Provide data, using free-form entry fields and pull-down menus to select prepopulated lists, or using a new feature to use a Visa-confirmed vendor card simulator and the import function, eliminating the need to populate CCRT screens manually. Log files are not required for online tests.
Test results	Provide required data for test results. An option to 'Select All: Pass or Fail,' can save data entry time. In some cases this may be all that is required. You are notified of test result errors, if any, that must be corrected when 'Next' is selected at the end of this step. If no errors are found, you will be taken to the confirm screen.
Confirm	Confirm entries and submit the Compliance Report to Visa for validation. If all mandatory fields are completed, the report can be submitted by selecting 'Submit.' Incomplete mandatory fields are summarized on the 'Confirm' screen. Clicking on a listed item displays the correct location at which to input the values for these fields.
Review	The submitted reports remain in a 'pending' status until Visa has reviewed and validated a first-time submission by an acquirer. The status of the submitted report changes to Accepted or Declined, depending on the outcome of Visa's review. If an acquirer has already undergone a successful first-time review by Visa and has elected for Visa to not review the submission of test results, the status of the submitted report changes to Accepted. Reports can be reviewed using the search capability. A statistical reporting feature is available for previously submitted reports

CCRT enhancements in the U.S. include the following, effective April 2013:

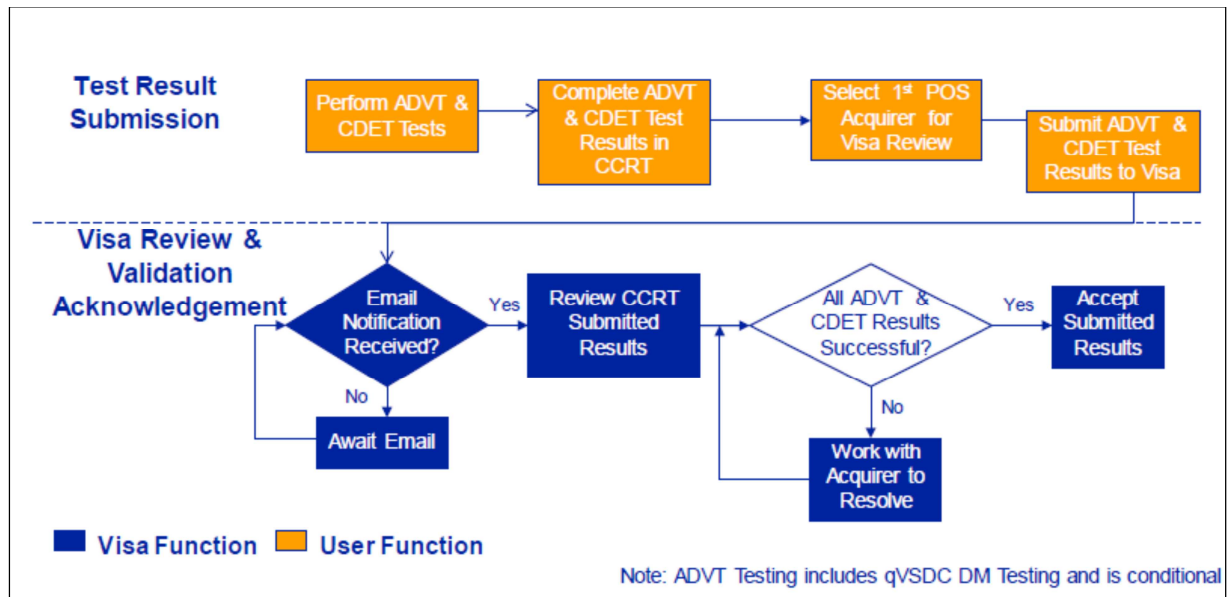
- Streamlined online testing submission requirements to reduce client resource time.
- Visa requires review of the initial submission of test results only for an acquirer or its processor. Updates need not be reviewed. The acquirer or its processor is still required to submit terminal test results, but these results will not require Visa review. The review is optional after the initial submission in CCRT (see Figure 3 and Figure 4 for sample process flows).
- Expanded processor capabilities to support multiple acquirers in one submission.  
A processor is not required to submit terminal test results for each acquirer on the same processing platform as long as the terminal or kernel/IFM configurations are the same. Currently, processors need to notify their Visa representative so that the CCRT Regional Administrator can link all applicable acquirers who will be deploying a terminal on that platform. If any changes to the terminal affect chip processing, a separate submission is required. The Acquirer Acknowledgment Form is needed.
- Acquirer processors have the capability to submit terminal test results for their own Visa-licensed entities.
- qVSDC DM test results are not required when a dual-interface integrated terminal is selected. qVSDC DM testing is still required for a standalone contactless-only device.

Further information regarding the use of CCRT can be found in the *Chip Compliance Reporting Tool User Guide for Chip Acquirers*.

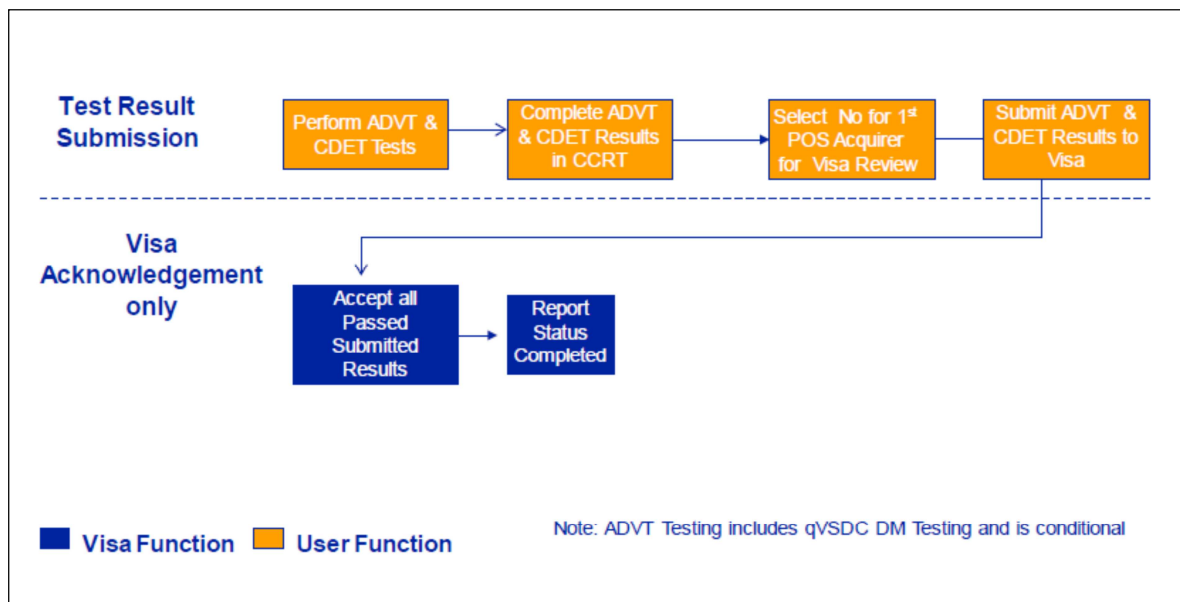
For more information, Visa clients can access Visa documentation on Visa Online. Visa-confirmed tool vendors can access documentation at <https://technologypartner.visa.com/>. Acquirers should consult with their Visa representative for more details.

The following lists the relevant Visa reference documentation:

- Acquirer Device Validation Toolkit (ADVT) User Guide
- Contactless Device Evaluation Toolkit (CDET) User Guide
- qVSDC Device Module Test Cases (VCPS 2.1.1)
- Chip Compliance Report Tool (CCRT) User Guide
- Chip Compliance Report Tool (CCRT) Quick User Guide
- Visa Smart Debit/Credit and Visa payWave US Acquirer Implementation Guide



**Figure 3. Visa CCRT Process Flow for a New Acquirer**



**Figure 4. Visa CCRT Process Flow for a Current Acquirer**

### **3.3 Discover E2E Certification Testing**

Executing the D-PAS Acquirer-Terminal End-to-End (E2E) test ensures that acquirers demonstrate the following:

- That the terminal accepts D-PAS products successfully.
- That authorization requests and responses can be transmitted between a terminal, acquirer host, and the network successfully.
- That the terminal processes chip-based functions, including PIN support, fallback transactions, and the card verification methods supported by the terminal.

#### **3.3.1 Prerequisites**

Discover requires the following activities before beginning acquirer end-to-end certification:

- Completion of acquirer host certification.
- EMVCo Level 1 and Level 2 certification for each terminal model.
- A Discover-approved E2E test tool. To obtain a list of test tools, contact your Discover account executive.
- Discover-supplied test cards (or optionally a Discover-qualified card simulator).

#### **3.3.2 Initiation**

The acquirer or direct-connect merchant must complete the following documents before starting the certification process:

- D-PAS Certification Request Form. This form provides details on the functions that acquirers intend to support and on their timelines for certification testing.
- D-PAS Card Request Form. This form is used to request physical test cards.
- Terminal Data Collection Form. This form is used to provide details about various terminal functions such as CVM methods supported, Offline Data Authentication methods supported, and fallback. Discover assigns E2E tests based on this questionnaire and the D-PAS Certification Request Form.

All forms can be obtained by contacting the assigned Discover Account Executive.

#### **3.3.3 Test Execution**

End-to-end testing is executed using a Discover-qualified E2E test tool. Discover-supplied test cards or a Discover-qualified card simulator should be used. During execution, technical help is coordinated by the assigned Discover account executive.

#### **3.3.4 Results**

Following execution, both the logs generated by the test tool and the terminal receipts should be submitted to Discover. If a card-to-terminal interaction log (i.e., smart spy log or card simulator log) is available, it should be submitted as well.

#### **3.3.5 Review Process**

Discover reviews the results and communicates within agreed SLA timeframes. Following successful completion of the certification test, a letter of certification is issued to the acquirer or direct-connect merchant.

### **3.4 American Express End-to-End Certification**

The American Express POS device certification process is designed to test end-to-end processing of American Express chip card transactions from the POS device, through an acquirer/acquirer processor or merchant network, to the entry point on the American Express network.

Testing includes chip card/POS device interoperability, and the acquirer/acquirer-processor's or merchant's capability to capture, format, and transmit required data, involving contact and/or contactless capabilities. POS device specifications are detailed in the American Express ICC Payment (contact) Specification (AEIPS), and the Expresspay (contactless) Specification documents.

POS device certification must be successfully completed prior to production deployment

POS devices connecting directly to American Express need to support host messaging. For details, access <http://www.americanexpress.com/merchantspecs>.

#### **3.4.1 American Express Certification Requirements**

In support of chip card/POS device interoperability, American Express requires the acquirer, acquirer-processor, or merchant to demonstrate their ability to support chip card acceptance as outlined in the American Express ICC Payment Specification (AEIPS) and Expresspay Contactless Specification.

#### **3.4.2 Certification Process Steps**

Certification process steps are as follows:

1. The acquirer, acquirer-processor, or merchant notifies American Express they are ready to commence certification.
2. American Express initiates project request and assigns a certification resource to the project.
3. The acquirer, acquirer-processor, or merchant executes test plan successfully (unattended testing – American Express is not involved).
4. The acquirer, acquirer-processor, or merchant executes certification (attended testing – American Express is involved).
5. American Express reviews receipts and terminal log provided by the acquirer, acquirer-processor, or merchant.
6. American Express issues certification letter.
7. The acquirer, acquirer-processor, or merchant moves into production.

Contact your American Express representative to start the certification process.

Starting in the third quarter of 2013, the American Express POS Certification Participant Program will be available to acquirer and acquirer-processors. Acquirer and acquirer-processors who choose to participate and meet all Program requirements will be able to streamline the end-to-end certification process. Please contact your American Express representative to receive more information about the Program.

#### **3.4.3 Prerequisites for Device Certification**

The following outlines the prerequisites for contact and contactless device certification.

EMV Migration Forum: Testing and Certification Committee  
Current U.S. EMV Testing and Certification Requirements for the Acquiring Community

*Contact:*

1. EMVCo Level 1 and Level 2\* certification status as completed/current, and not expired or revoked.
2. EMVCo certifications must reference the same device or device family as the device being requested for Level 3 American Express certification.
3. EMVCo Level 2\* certification (EMV contact) must reference the same kernel that is in the POS device being requested for Level 3 American Express certification.

*Contactless:*

1. EMVCo Level 1 certification status as completed/current, and not expired, or revoked.
2. American Express/Expresspay Level 2\* certification must be completed/current, and reference the same device or device family as the device being requested for Level 3 American Express certification.
3. American Express/Expresspay Level 2\* certification must reference the same kernel that is in the POS device being requested for Level 3 American Express certification.

\*NOTE: If Level 2 certification has expired for a POS device previously approved by American Express, the device can continue being deployed provided no device updates have been made.

## **4 Other Required Testing Processes**

Some of the payment brands require tests in addition to those described in “Acquirer Host Testing Requirements” and “Terminal Testing Requirements.”

### **4.1 MasterCard End-to-End Demonstration**

A MasterCard Acquirer End-To-End Demonstration (ETED) is typically required as the last step of an initial acquirer chip migration project for either ATMs or POS terminals. It serves as a final confirmation of acquirer system readiness. ATM and POS terminals are tested by performing a standardized set of transactions (such as cash withdrawals from an ATM or low-value POS purchases) with various live cards from multiple issuers. The demonstration encompasses various card configurations and parameters, covering the majority of the MasterCard branded chip cards (such as cards with T=0 and T=1 protocols, M/Chip 4 and M/Chip 2 cards, 6 digit PIN cards, and cards that generate issuer script messages).

Similarly, an issuer ETED may be required as part of an issuer chip migration project. An issuer ETED confirms the interoperability of an issuer’s cards with the issuer’s authorization network in a production environment. This test involves issuing live cards to an ETED tester, who uses them at production ATMs and POS terminals to withdraw funds and make low-value purchases to check for compliance.

### **4.2 Discover Acquirer Production Validation Test**

Acquirer production validation confirms that terminals in a live environment have been properly configured to accept D-PAS and can pass the necessary D-PAS data for authorization. The test also identifies any interoperability issues.

#### **4.2.1 Prerequisites**

Discover requires the following activities before beginning the acquirer production validation test:

- Completion of acquirer host and end-to-end certifications.
- Assurance that all required terminal parameters are loaded across the terminal base.

#### **4.2.2 Initiation**

The acquirer or direct-connect merchant must fill out the Production Validation Card Request Form before starting the production validation process. The form is used to obtain production validation cards from Discover.

This form can be obtained by contacting the assigned Discover account executive.

#### **4.2.3 Test Execution**

Production validation testing is executed by performing the following steps according to the D-PAS Production Validation Test Plan:




- Complete and document the results of production validation tests on all applicable terminals.
- Work with Discover to resolve any issues identified.
- Return the completed D-PAS Production Validation Form along with required supporting documentation and production validation cards to Discover.



## 5 When Terminal Testing Is Needed

This section provides some common examples in the field of when retesting is required for EMV chip and contactless terminals. The examples listed below are guidelines. They are selected to clarify when required testing must be repeated. (For further clarification, please contact your payment brand representative or acquirer.) It is recommended that acquirers always perform internal testing using the payment brand's testing tools when changes are made.

The issues below are labelled as follows:

	A use case with an exclamation point symbol requires additional testing; this is classified as a major issue.
	A use case with a magnifying glass symbol does not require recertification. However, best practice would be to run an internal test based on the required testing and contact the payment brand if any issues are found.
	For a use case with a check mark symbol, standard internal regression testing only is advised.

### 5.1 ATM Use Cases

This section covers whether changes to ATM devices necessitate the terminal required testing processes by the payment brands.

**Q. I am changing the EMV Level 1 hardware on my device, which impacts neither the EMV chip processing in the payment application nor the kernel. Do I need to repeat required testing with the payment brands?**



*This hardware change is classified as a minor change. Therefore, retesting with the payment brands would not be required. The recommendation is to perform internal regression testing prior to deployment of Interface Module (IFM) changes.*

**Q. If I change my operating system (e.g., Windows XP to Window 7), do I need to repeat required testing?**



*If this is the only change, and there are no changes to the payment application impacting EMV chip processing or the kernel, then no retesting with the payment brands is required.*

## 5.2 Terminal Use Cases

For the purposes of this section, a terminal can be any EMV-capable terminal or PIN pad that is not an ATM (ATM use cases are covered in the previous section). Terminals are all other terminal types as defined in EMV, including POS terminals, bank branch terminal (BBT), unattended terminals, and on-board devices (e.g., handheld terminal on planes).

**Q. My terminal supports different communication types (Bluetooth, General Packet Radio Service (GPRS), dial-up). Do I need to repeat required testing for each communication type?**



*No, one set of required testing per terminal family is needed as long as the communication type is the only change. Consult with the terminal vendor for information on whether a group of terminals fall within the same family. Communication types are out of scope for this testing.*

**Q. If I deploy terminals by multiple terminal vendors, do I have to retest each terminal configuration by vendor?**



*Yes, retesting with the payment brands is required if changes to the payment application affect chip processing or the kernel by terminal configuration.*

**Q. I am changing the EMV Level 1 hardware on my device. Do I need to repeat required testing with the payment brands?**



*This hardware change is classified as a minor change. Therefore, retesting with the payment brands would not be required. The recommendation is to perform internal regression testing prior to deployment (IFM changes).*

**Q. I would like to add an additional service, such as dynamic currency conversion or cash back. Do I need to repeat required testing?**



*Yes. Most of the payment brands require specific testing to support these transaction types, which include host testing. Refer to the applicable payment brand for more details.*

**Q. My EMV Level 2 kernel has expired. Do I need to replace it?**



*No. However, new terminals should be deployed with the updated kernel and with IFM tested appropriately with the payment brands.*

**Q. Do ECR (a cash register with integrated payments) changes that are not payment related require testing?**



*No. Formal testing is not required.*

**Q. Does upgrading to a new version of a PIN pad with a new EMV kernel require retesting?**



*Yes. Rerunning required tests with the payment brands is necessary.*

**Q. I am upgrading to a new version of a PIN pad that does not involve changes to EMV chip processing but does involve other changes, such as adding a tip prompt for use in a restaurant. Do I need to retest with the new version of the PIN pad?**



*No. Formal testing is not required.*

**Q. Does upgrading to a new PIN pad version with changes that affect an EMV chip processing transaction type require testing?**



*Yes. Rerunning required tests with the payment brands is necessary any time EMV chip processing is affected.*

**Q. If I change the transaction path or the data transmitted in transaction packets, do I need to repeat required testing?**



*Yes. Changing the route of the transaction requires you to repeat required testing. With most payment brands, testing is not restricted to the terminal but constitutes end-to-end testing. The payment brands should be involved in this process.*

**Q. Do I need to repeat required testing if the portfolio changes – for example, if my ISO sells or buys a portfolio and changes where the device is pointing or changes my merchant ID or transaction ID?**



*If routing of the transaction is effected with a different gateway then required testing must be performed.*



*If the changes are only related to the terminal management system, required testing is not affected.*

**Q. When Level 1 or Level 2 certification expires, what happens?**



*Internal testing is suggested as a first step. Review with your kernel provider, as the provider may need to update the kernel. The payment brands have specific processes to address this particular issue that fall outside of the scope of this document.*

### 5.2.1 Semi-Integrated Terminal Use Cases

**Q. Does changing connectivity to the PIN pad require retesting?**



*Communication types are out of the scope for repeating required tests.*

**Q. Does upgrading my PIN pad to a new version with changes that affect an EMV chip transaction type require retesting?**



*If there are no changes to the messages exchanged between the PIN pad and the ECR, certification with the merchant is not required. The acquirer needs to complete required testing with the payment brands. Refer to the applicable payment brand for more details.*

**5.2.2 Stand-alone Terminal Use Cases**

**Q. Do changes to non-payment-related applications on the device require certification?**



*No. Other applications are out of scope.*

**Q. Do changes to the payment application that do not affect the EMV chip transaction require certification?**



*No. This would be considered a minor change, and no retesting is required.*

**5.3 Acquirer-Processor Platform**

This section defines an acquirer and the acquirer's processor as an entity with a direct connection to the payment brands.

**Q. When biannual payment brand compliance changes are released, do I need to recertify everything because I am making changes to my platform?**



*Required testing is not necessary unless specifically requested by the payment brands.*

**Q. I am upgrading my switch to support changes from my supplier. Do I need to complete required testing?**



*Retesting may not be required, depending on what areas are affected. The payment brands should be involved in this process.*

**Q. I am changing my payment platform to a different switch vendor's platform. Do I need to complete required testing with the payment brands?**



*Yes. This is a major change, and the payment brands should be involved in this process.*

## **5.4 Value-Added Reseller**

**Q. Value-added resellers (VARs) support an integrated payment application. If there are changes to an inventory management system within the payment application, would this require the terminal to be retested? For example, a retail and restaurant management systems' integrated payment application would include the inventory system. If a change is made to the inventory system, it will impact the payment application but not chip processing.**



*No retesting is required. Modularizing applications is recommended to protect the payment application. Changes to the kernel or chip processing will necessitate a retest.*

**Q. I am using a middleware application for EMV. If I update my API, do I have to repeat required testing?**



*Retesting is only required if the changes impact the payment application for chip processing or the kernel.*

**Q. I am adding mandatory addenda per payment brand enhancements for mag-stripe transactions. Do I need to complete required testing?**



*No. Retesting is not required.*

**Q. I've added a new payment peripheral device to my processing chain. Must I repeat required testing?**



*No. Retesting is not required.*

**Q. The version of my application has changed but the device hardware version has not. Must I repeat required testing?**



*Yes. Retesting is required.*

## **6 References**

The following links provide additional reference material on EMV testing and certification. Please note that the payment brands' sites require registration and login.

### **American Express**

American Express technical specification web site, <http://www.americanexpress.com/merchantspecs>

### **Discover**

Contact your assigned Discover representative.

### **EMVCo**

EMVCo web site, <http://www.emvco.com>

EMVCo Approvals and Certifications, <http://www.emvco.com/approvals.aspx>

### **MasterCard**

MasterCard Connect web site, <https://www.mastercardconnect.com/>

### **Visa**

Visa Online web site for Visa clients, <https://www.visaonline.com>

Visa Technology Partner web site for vendors, <https://technologypartner.visa.com/>

Visa clients: Contact your Visa representative.

## **7 Publication Acknowledgements**

This white paper was developed by the EMV Migration Forum Testing and Certification Working Committee to provide an educational resource on the payment brands' EMV testing and certification requirements for U.S. payments industry stakeholders.

Publication of this document by the EMV Migration Forum does not imply the endorsement of any of the member organizations of the Forum.

The project team who developed this white paper included: Acquirer Systems, American Express, Chase, Discover, MasterCard, TSYS, Vantiv, VeriFone, and Visa.

The EMV Migration Forum wishes to thank the Testing and Certification Working Committee members for their contributions to the white paper. Special thanks go to **Kevin Emery**, Discover, and **Cindy Kohler**, Visa, for leading this project.

The following members participated in the development and review of the white paper:

- **Chiro Aikat**, MasterCard
- **Randy Burnette**, VeriFone
- **Steve Cole**, Vantiv
- **Aidan Corcoran**, Acquirer Systems
- **Maxim Dyachenko**, UL Transaction Security
- **Kevin Emery**, Discover
- **Allen Friedman**, TSYS
- **Manjit Hota**, Discover
- **Cindy Kohler**, Visa
- **Christine Lopez**, Vantiv
- **Fergal Molloy**, Acquirer Systems
- **Ricardo Morales**, UL Transaction Security
- **Derek Ross**, ICC Solutions
- **Ellie Smith**, Discover
- **Clyde L. Van Blarcum**, American Express
- **Paul Vanneste**, MasterCard

## **Trademark Notice**

All registered trademarks, trademarks, or service marks are the property of their respective owners.