AN EMV MIGRATION FORUM TESTING AND CERTIFICATION WORKING COMMITTEE WHITE PAPER

EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community

Version 2.0

Date: April 2016

EMV Migration Forum

191 Clarksville Rd.
Princeton Junction, NJ 08550

www.emv-connection.com

About the EMV Migration Forum

The EMV Migration Forum is a cross-industry body focused on supporting the EMV 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 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/.

Legal Notice

Notwithstanding anything to the contrary in this document, each payment network determines its own testing and certification requirements, and all such requirements are subject to change. Merchants, acquirers, processors and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with their respective payment networks regarding applicable requirements.

While great effort has been made to ensure that the information in this document is accurate and current as of the publication date, this information should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise, and all warranties of any kind, whether express or implied, are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein, and all warranties as to the accuracy, completeness or adequacy of such information. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk. Comments or recommendations for edits or additions to this document should be submitted to: certification-feedback@us-emvforum.org.

Table of Contents

1 Introduction

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

With the benefit of global knowledge and experience, the global payment networks have developed, and continually strive to improve, their respective testing processes and requirements, in order to help minimize potential deployment and production risks. This document defines the current processes required to test EMV chip transactions with American Express, Discover, MasterCard, and Visa (referred to collectively as the global payment networks).[1] Network-specific issues, concerns, or questions related to these processes should be directed to the appropriate global payment network. 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 only cover the current acquirer testing requirements for the global payment networks referenced above. These testing processes also support direct-connect merchants which are directly connected to the global payment networks. Merchants not directly connected to the global payment networks should work with their acquirers on testing requirements and are out of scope for this document. The white paper does not describe testing for U.S. domestic debit payment networks; it is recommended that acquirers contact the domestic debit networks to understand their requirements.

Throughout this document, you will see the term "required testing," which is used in sections that are not global payment network specific to generically refer to testing required by global payment networks. Each global payment network also uses its own network-specific references or terms (e.g., certification, qualification, confirmation, approval). Global payment network specific terminology is used as appropriate in network-specific sections of this document.

This document is the result of input from American Express, Discover, MasterCard, and Visa.

Comments on or recommendations for edits or additions to this document should be submitted to certification-feedback@us-emvforum.org.

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

2 Acquirer Host Testing

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 global payment networks. 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 global payment network was required to be completed by April 2013, as per global payment network mandates. Any new acquirer processor endpoints would be required to perform host testing that includes chip data.

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

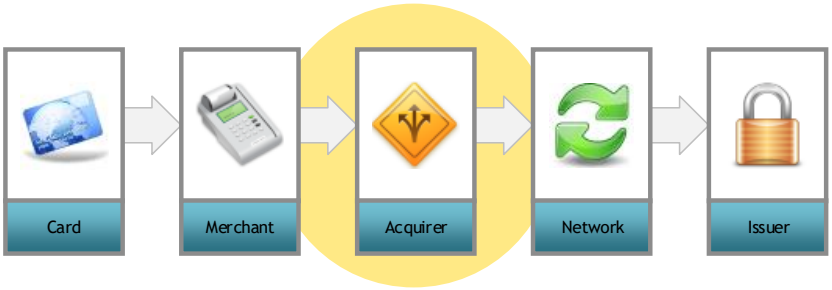

Figure 1. Acquirer Host Position in the Payment Process

2.1 MasterCard NIV Certification

The objective of the MasterCard network interface validation 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 *MasterCard Contactless-MasterCard Contactless* 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. Acquirers and merchants are always required to 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 *MasterCard Contactless-MasterCard Contactless* 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 Authorization Simulator (MAS) 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 via the MasterCard Test Facility (MTF) is available as an option as well for acquirers, but not recommended.

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 environment'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

The assigned MasterCard implementation specialist will assist the acquirer 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 (MEPSA) helps MasterCard customers to identify 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 point-of-sale (POS) transactions.

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

- Requirement for attended testing
- Use of physical global host test cards and scripts
- Managed by a project
- Testing performed with use of a production-ready 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
- Support for quick Visa Smart Debit Credit (qVSDC) contactless transactions
- Validation of compliance with VIP authorization and full financial messages for each unique host platform

Settlement testing is optional and only required if offline authorization of transactions is supported. While chip data is required to be included in the authorization request and authorization response messages, there are no requirements to carry chip data in the clearing and settlement messages, or returns, when supporting Visa's minimum U.S. online-only terminal configuration.

- 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. Processor parameters will require the appropriate Visa paperwork.

Any new acquirers and acquirer processors will be required to meet these EMV testing requirements. Support is optional for direct-connect merchants.

Contact the Visa representative for more information.

2.3 Discover Acquirer Host Certification

Executing Discover acquirer host certification requires the host system of the entity obtaining certification (either an acquirer, acquirer processor, or direct-connect merchant) to meet the messaging requirements 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 confirms 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 confirms 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*

Note: Discover host and clearing certification also covers certification with Discover's network partners or entities using the D-PAS product.

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 Host 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.

- Certificate Authority (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

2.3.3.1 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 D-PAS 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).

2.3.3.2 TEST TOOLS

The Release Compliance Tool (RCT) is 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.

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.

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 the 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 the 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 the acquirer, acquirer processor, or merchant host connection for authorization and settlement.

For authorization and settlement specifications and additional detail log on to: 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 the 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 the 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 global payment networks. "Terminals" mean all EMV-related terminal types, including POS devices, ATMs, bank branch terminals, unattended devices, automated fuel dispensers, and on-board terminals (handheld terminals on planes).

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 network.

Figure 2 illustrates the areas that are covered by terminal testing.

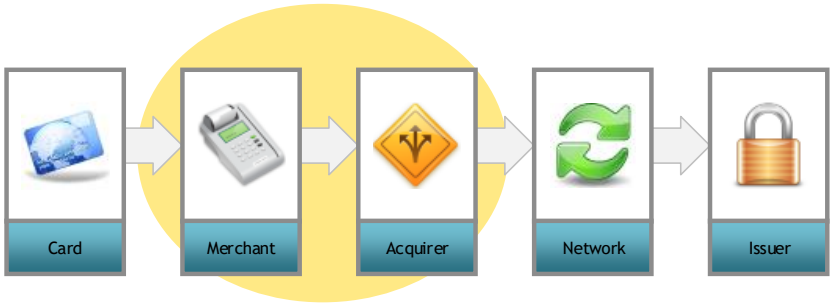

Figure 2. Areas Covered by Terminal Testing

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 EMVCo or global payment network 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 global payment networks have developed requirements for testing terminals before global deployment of EMV chip terminals.

The global payment network 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 www.emvco.com.

Currently, global payment network 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. Any time there are changes to the payment application affecting chip processing or to the kernel by terminal configuration, retesting with the payment network is required.
- Changes are made to the chip payment application processing on the terminal or within the infrastructure.
- Hardware or software is modified significantly or an EMVCo-approved kernel is changed on a deployed terminal. Refer to EMVCo Type Approval Bulletin No. 11 for more details on minor and major changes.
- Hardware, software, or parameter settings are changed and the change impacts the payment application.

- Terminal-to-acquirer messaging is changed affecting chip processing

Kernel management is linked to managing terminal vendor communications and standardizing solutions. Proper management can potentially minimize the terminal testing required, as well as minimize the overall system impact when necessary updates and changes to existing terminals are deployed in the market. Refer to the "Kernel Management Guidelines" webcast available at http://www.emv-connection.com/emv-resources/.

The EMV Migration Forum "Minimum EMV Chip Card and Terminal Requirements" document defines minimum configuration requirements for EMV terminalization (which may vary across payment networks). Following guidance in the document may also minimize terminal testing requirements. The document is available on the EMV Migration Forum website at http://www.emv-connection.com/minimum-emv-chip-card-and-terminal-requirements-u-s/.

Each global payment network offers self-testing and accreditation vendor programs. Refer to each global payment network's section of this white paper for more details. Also, depending on the individual global payment network's requirements, each one allows the use of card and host simulators by accredited vendors.

3.1 Industry Initiatives

Several industry initiatives have focused on streamlining the testing and certification process, both for the U.S. and global payments industries. Collectively, implementing these efforts will streamline and improve the current terminal integration testing processes globally while maintaining a balance for when to test for a stable, near frictionless payment environment and acceptance experience both domestically and globally.

3.1.1 EMV Migration Forum Testing and Certification Working Committee

Through the EMV Migration Forum Testing and Certification Working Committee, the global payment networks collaborated to provide education and clarity on testing requirements and processes as well as individual global payment network strategies to further streamline testing. The following were the Working Committee's key initiatives:

- Hosted EMV training for retail value-added resellers (VARs), independent software vendors (ISVs) and independent service organizations (ISOs) in September 2014, with recording available on http://www.emv-connection.com/emv-workshop-for-vars-isvs-and-isos/.
- Launched testing materials and resources, available on the EMV Migration Forum Knowledge Center website.
- Developed the "EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community" in July 2013 (which this white paper updates)
- Formed the Acquirer Subcommittee which developed a "Framework Document" that identified opportunities to improve acceptance testing processes for migration to chip.

3.1.2 EMVCo Terminal Integration Task Force

In a parallel effort, the EMVCo Terminal Integration Task Force (TITF) was established in September 2013 to also review varied acquirer processes globally, identify areas to align and determine synergies across the global payment networks' testing processes for the integration of EMV contact and contactless acceptance devices into their payment environments.

Working jointly with the Testing and Certification Working Committee Acquirer Subcommittee, eight deliverables were identified associated with network-defined EMV terminal testing requirements for tool automation and alignment of testing processes across all of the payment networks.

The EMVCo TITF published the *EMVCo Brand-aligned Terminal Integration Testing Framework – Process Enhancement* in November 2014. The document is available on http://www.emvco.com.

Industry adoption globally is currently scheduled to be complete by June 2016 and includes American Express, China UnionPay, Discover, JCB, MasterCard, and Visa.

Table 1 outlines the benefits of the eight deliverables:

The Brand-aligned Framework describes the plan for delivery and benefits of alignment on the following 8 items:		Tool Automation	Process Improvement
1	A machine-readable format (in XML) for use in defining and developing the Brands' test card images for the terminal integration testing	√	
2	Aligned principles for defining Test Cases Pass/Fail Criteria (similar to principles defined for EMV Type Approval)		√
3	A machine-readable syntax (in CSV format) for enabling test tools determination of the pass/fail criteria for each test case	√	
4	A common Transaction Log format to assist with test case result determination	√	
5	An aligned Test Plan template for Brand consistency		√
6	Common Terminology Glossary as applied to terms and abbreviations used during terminal integration testing		√
7	Aligned criteria on when terminal integration testing is required vs recommended		√
8	Common Test Report Guidelines and a machine-readable (in XML) file format template	√	√

Table 1. Benefits of the EMVCo Brand-aligned Terminal Integration Testing Framework

The key benefits of these initiatives for the U.S. market are:

- Quicker development and availability of all global payment network qualified test tools to meet market needs.
- Improved credibility and availability of all global payment network accredited service providers to assist merchants and acquirers with their testing requirements.
- Provision of more robust testing analysis by test tools, reducing test debugging and analysis timelines and allowing for quicker deployment to market.
- Standardization of test tool readiness across all global payment networks, allowing for streamlined processes.

3.1.3 U.S. EMV VAR Qualification Program

The Payments Security Task Force joined with the PCI Security Standards Council and the EMV Migration Forum and launched a chip education curriculum and "pre-qualification" program, the U.S. EMV Value Added Reseller (VAR) Qualification Program, in April 2015. The program is designed to help streamline and simplify the EMV testing and certification process for VARs and ISVs. Through this industrywide effort, VARs and ISVs will better understand how to integrate chip cards into small and mid-sized merchants' POS solutions for the payment networks (American Express, Discover, MasterCard and Visa).

The optional program consists of three central components:

- The education series provides U.S. VARs, ISVs and merchant organizations with an understanding of the U.S. market for EMV migration, U.S. debit deployment, development preparation, kernel

management guidelines, lessons learned, and testing considerations to assist with EMV chip migrations. Audio recordings of the six webcasts with accompanying slides are available at http://www.emv-connection.com/chip-education-for-vars-isvs-and-merchants/.

- A list of service providers independently accredited by the payment networks is maintained to provide chip consulting and expertise.
- A pre-qualification process is run by the accredited service providers to help VARs and ISVs begin the implementation and testing process before they work with acquirers to achieve final certification.

Major U.S. acquirers participated in the development of the program and will recognize the pre-qualification status. Many plan to provide fast track certification for VARs and ISVs that have demonstrated the execution of solid chip solutions. Merchants have the ability to prepare their systems today to continue to deliver their customers an even more secure shopping experience.

With that foundation, each VAR and ISV should have the ability to pre-qualify its solution for each of the participating U.S. payment networks. The VAR would then work with its acquirer to receive a final certification of the solutions a merchant would need to process a chip card transaction. The result will be a streamlined, go-to-market process for the thousands of solutions that will provide ongoing value over the next two to three years, as the U.S. migrates to chip.

Section 8 Addendum includes more information about the program. To begin the pre-qualification process, visit:
https://www.pcisecuritystandards.org/approved_companies_providers/var_qualifications_program.php.

3.2 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 the contact interface, the contactless interface, or both.

A MasterCard end-to-end demonstration (ETED) may optionally be performed for either ATM or POS (see Section 4.1).

3.2.1 Requirements

Preparation for an M-TIP project requires the following:

Simulator. Install the latest versions of the MasterCard Authorization Simulator (MAS) 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[2] and 2 certificates from the software vendor/VAR/integrator. These certificates include three pieces of required information: the Issuer Conformance Statement (ICS), approval numbers, and kernel name.[3] 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.

[2] The EMV level 1 device is the hardware that accepts the card.

[3] These certificates are also available on www.emvco.com. Confirm with the provider that certificates are correct so that certification is not impacted at a later stage.

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 *MasterCard Contactless* M-TIP project requires the following:

MasterCard Contactless Vendor Product Letter of Approval. Obtain this letter from the terminal vendor/VAR/integrator.

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

3.2.2 Registering the M-TIP

Before starting an M-TIP project, go to MasterCard Connect and download the latest M-TIP *Process Guide*, Test Selection Engine (TSE) and M-TIP Test Set. TSE is a Windows® application that generates the applicable M-TIP test plans, based on the testing rules defined by the M-TIP Test Set.

The acquirer and the VAR use TSE to describe their terminal configuration and generate a unique M-TIP reference number and a test plan. This test plan is based on answers to questions asked by TSE on the terminal configuration, so it is important that the answers are correct and aligned with the EMVCo Level 2 Kernel terminal capabilities.

Table 2 lists the main questions required to test contact EMV and an explanation of what should be completed.

Table 2. 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 www.emvco.com. Contactless reader deployments must use a proximity coupling device (PCD) that is compliant with EMV Contactless Specifications for Payment Systems—Book D—EMV Contactless Communication Protocol Specification, v2.2 (EMV CL Book D v2.2) or later.

Information	Explanation	Source
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 www.emvco.com. All contactless readers submitted for M-TIP must be compliant with MasterCard Contactless Reader Specification v3.0 (or later) or EMVCo Book C-2.
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 the hardware provider.
PCI-PED approval reference	Security certification of the PIN pad, if any	Obtain the approval reference from the 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	–
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	–

3.2.3 Test Execution

For the dual message system, tests are run against the MasterCard Authorization Simulator (MAS). 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.

3.2.4 M-TIP Service Providers

MasterCard has accredited a number of Formal 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.

3.2.5 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.

3.2.6 M-TIP Fast Track

The Fast Track M-TIP process allows acquirers to obtain, with no testing or with a minimal amount of testing, an M-TIP Letter of Approval for terminals identical to the ones tested by another acquirer in a prior execution of M-TIP (referred to as the “reference M-TIP”).

Third party processors (TPP) have asked MasterCard whether they could avoid retesting a configuration that they previously tested for another acquirer. In such cases, MasterCard usually allows, on a case by case basis, MSPs to perform some form of reduced testing.

The Fast Track M-TIP process formally allows acquirers to complete M-TIP with no or with a limited amount of testing and defines the conditions under which acquirers may opt for such alternative.

3.2.7 Modular M-TIP

In some cases, MasterCard may accept that chip terminals and (parts of) the acquirer host infrastructure are tested and certified as discrete components rather than as an entire acquiring chain. Subsequently, suitable combinations of independently M-TIP-certified components can be deployed without further testing.

The benefit of such an optimized process, known as Modular M-TIP, is to reduce the amount of testing required when the terminal/acquirer infrastructure is re-used in exactly the same configuration.

Acquirers, third party processors (TPP) or terminal vendors that wish to benefit from Modular M-TIP may contact MasterCard and provide the details of their network topology. MasterCard will review their request and, if it is deemed acceptable, will allow them to apply the Modular M-TIP approach.

Modular M-TIP can be applied to both contact and contactless.

3.2.8 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[4].

3.2.9 MasterCard Emerging Payment Support Accreditation Program (MEPSA)

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 MEPSA Program helps MasterCard customers to identify 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.

3.3 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 www.emvco.com. For details on Visa approved contactless devices, refer to the Visa Technology Partner website at https://technologypartner.visa.com/. The test results are submitted to Visa via the Chip Compliance Reporting Tool (CCRT). The requirements for each toolkit are outlined below.

3.3.1 Acquirer Device Validation Toolkit

Visa mandates that acquirers use the ADVT prior to initial deployment of EMV chip terminals to help ensure that the terminal is configured correctly.[5]

The ADVT must also be used if there are major changes to an EMV-approved terminal that impact the payment application or authorization message for chip processing, kernel, interface modules (IFMs), or network infrastructure. Visa also requires the use of ADVT when dynamic currency conversion or cash back is introduced to the EMV POS environment.

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 an expired EMV Letter of Approval (LoA). This requirement does not affect the deployment of terminals already approved against ADVT. However, it will help prevent the deployment of new or updated terminal configurations that use expired IFM hardware or kernel software.

To reduce terminal testing requirements, as well as to minimize the impact when necessary updates/changes to existing terminals are deployed in the market, Visa recommends acquirers and merchants become familiar with the IFM revisions and kernel versions being supported in their terminals to assist in proper EMV kernel management. Kernel management promotes terminal vendor communication and standardization of solutions. Refer to Visa's kernel management guidelines for contact and contactless chip terminal implementations, which are available on www.visachip.com.

Visa may ask the acquirer to undertake specific post-deployment ADVT testing whenever it seems likely that a terminal is causing acceptance or interoperability problems in the field.

---

[4] For more information on the self-approval program, contact MasterCard.

[5] In addition, Visa strongly recommends that acquirers use the toolkit on previously deployed terminals to determine whether there are potential acceptance 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.

The ADVT test results are provided to Visa by submitting the results into the Chip Compliance Reporting Tool (CCRT), a server-based online solution for systematic reporting. Acquirers, their processors or a vendor enabled for the Visa Chip Vendor Enabled Service (CVES) are required to use the CCRT to submit their terminal test results.

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

3.3.2 Contactless Device Evaluation Toolkit

Similar to ADVT, the CDET is a set of test cards and an accompanying user guide that allow acquirers 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 must be performed. For new reader deployments, the acquirer executes each applicable CDET test case to confirm that the expected outcome is achieved.

If Visa or the acquirer suspects a problem with a deployed contactless reader, it is recommended that all applicable tests specified in CDET be performed to assist with the analysis and debugging of the suspected issue.

If changes are made to the configuration of a previously deployed contactless reader, it is required that all applicable CDET test cases are re-performed

As contactless acceptance increases in the U.S. for mobile payments, it is important that merchants, acquirers and vendors remain committed to interoperability and processing integrity for all form factors without compromising cardholder convenience. All contactless readers being deployed must undergo CDET testing.

CDET testing is also required for existing contactless chip-reading terminals that have undergone a significant hardware or software upgrade impacting the kernel or payment application for chip processing.

CDET does not specifically test the performance of the contactless antennae. It focuses on the integration of the payment application to the Level 2 kernel. While there may be variances of Level 1 and Level 2 letters of approval for a terminal family, the Level 2 kernel is often identical within that family. When a deployment supports a Visa payWave terminal family that also shares the same Level 2 kernel, a single Visa payWave reader can be CDET tested to cover the entire terminal family. Consult with the terminal vendor to ensure a terminal falls within a terminal family. This approach allows a general reduction in the number of test iterations without negligible impact to the integrity of the testing process.

The CDET test results are provided to Visa by also submitting the results into the CCRT. Acquirers, their processors or a vendor enabled for the Visa Chip Vendor Enabled Service (CVES) are required to use the CCRT to submit their terminal test results. 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.

3.3.3 Additional Toolkit Requirements

Acquirers must use the ADVT and CDET before initial terminal deployment (including all variations of hardware, software, and parameter settings) to help ensure that the terminal is fully operational and 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 will continue to perform the test until the problem is resolved and the test result matches the expected outcome. An acquirer who fails to use the ADVT and CDET on a device that causes interoperability issues will be out of compliance and will follow requirements 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 in order to analyze and debug any potential acceptance issues. Retesting of offline-capable terminals can increase the duration of testing because of the complexity of debugging issues with these terminals. Refer to *Visa Minimum U.S. Online Only Terminal Configuration* document for more details. 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 and that Visa requirements are satisfied, and to identify 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 fulfilment service, Merrill Corporation. 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.

3.3.4 Chip Compliance Reporting Tool

Visa developed the CCRT as a centralized, server-based solution for the systematic reporting of ADVT and CDET test results. CCRT facilitates an efficient submission and management process of compliance reporting for 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, and allows the CCRT service to be consolidated with other services currently provided to Visa clients. CCRT is available on Visa Online, 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. A user can reuse existing reports as a starting point for new reporting or leverage import functionality generated by Visa-confirmed third party vendors, reducing time spent completing the reports.

Acquirers or their processors are required to use the CCRT to submit terminal test results. The CCRT is the only method under which Visa will accept the test results for ADVT and CDET. Acquirers should discuss enrollment requirements and use of CCRT with their Visa representative. In order for processors or CVES-enabled vendors to submit terminal test results on behalf of their acquirers, an Acquirer Acknowledgement Form is required. Merchants should contact their acquirer for more details on CCRT.

Table 3 summarizes the steps required to submit a report using CCRT.

Table 3. Steps Required to Submit a Report Using CCRT

Step	Description
Client information	Requests information about the client, including contact details and Visa related licensing information used for testing.
ADVT/CDET test information	Complete all mandatory information on the Compliance Test Information, Payment Application and EMV, Terminal Resident Data Objects, and Terminal Details screens.
Enter data	The tool offers free-form entry fields and pull-down menus for selecting pre-populated lists or a new feature providing the ability to use a Visa-confirmed vendor

Step	Description
	card simulator and the import function, eliminating the need to manually populate CCRT screens. Log files are not required for online tests unless using a Visa approved host simulator.
Test results	Complete all required data for test results before submitting to Visa. An option is provided to "Select All: Pass or Fail," which can be used to save data entry time for these columns. In some cases, this may be all that is required. Test result errors that must be corrected, if any, will be provided when 'Next' is selected from this screen. If no errors are found, the 'Confirm' screen will be displayed.
Confirm	The final stage is to 'Confirm' entries and submit the Compliance Report to Visa for validation. Provided all mandatory fields were completed on previous pages, the option to 'Submit' the report will be given. If any mandatory fields are missing, they will be summarized on the 'Confirm' page. Clicking on any of the listed items will return to the correct location to complete the values for these fields, before submitting the report.
Review	The submitted reports remain in a "Pending" status until they have been reviewed and validated for a first-time submission by an acquirer. The status of the submitted report will change to 'Accepted' or 'Declined' depending on the outcome of Visa's review. For an acquirer that already has completed a successful review by Visa, the status of the submitted report will change to an 'Accepted' status. Reports can be reviewed by using the 'Search' capability. A statistical reporting feature is available for previously submitted reports.

CCRT enhancements in the U.S. include:

- A streamlined review process is available to automatically accept reports when all results "pass" for subsequent submissions.
- After the first accepted report is reviewed by Visa, a review of updates is not required. The requirement to submit terminal test results remains, but does not include a Visa review. The review is optional after the initial submission in CCRT. Refer to the two flows in Figure 3 and Figure 4 for examples.
- Processor capabilities have been improved to support multiple acquirers in one submission.
- Submission of terminal test results for each acquirer on the same processing platform is not required as long as the terminal or kernel/IFM configuration is the same. The acquirer processor must link all applicable acquirers that will be deploying the terminal on that platform. If any changes to the terminal impacting chip processing are necessary, a separate submission is required. The Acquirer Acknowledgment Form is required.
- Test results may be submitted by acquirer processors for their own Visa licensed entities.
- Report submission import capability is available for all reporting options generated by third-party card simulator test tools confirmed by Visa.

- It is recommended that large merchants, direct-connect merchants and new endpoints supported by a project complete ADVT and CDET terminal testing using VCMS for the first time. Subsequent terminal testing can support VCMS or a host simulator if available.
- Merchant name has been added as a new data field in CCRT. This will allow for analysis and troubleshooting.
- The January 2016 CCRT release was enhanced to support the Visa minimum U.S. online-only terminal configuration for clients deploying terminals that have online-only capability. If a terminal is not configured for any offline functionality, that terminal can use the subset of ADVT.

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

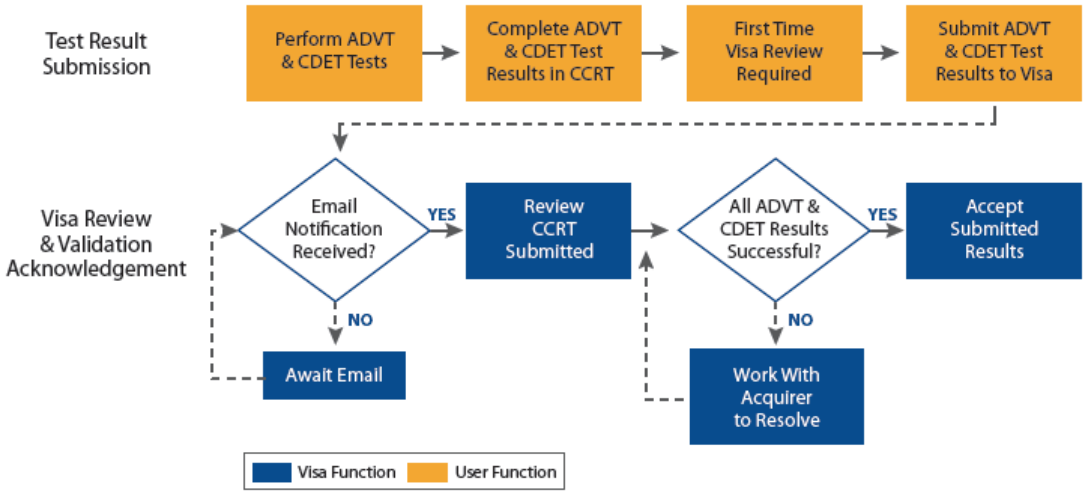

Figure 3. CCRT Process Flow – New Acquirer

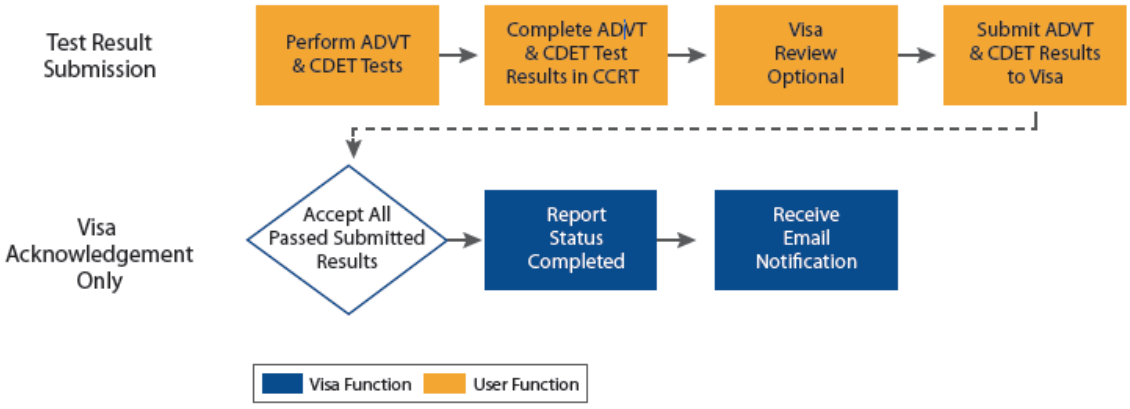

Figure 4. CCRT Process Flow – Existing Acquirer

3.3.5 Chip Vendor Enabled Service

Visa-confirmed third party vendors can help streamline the testing and reporting requirements for deployment of EMV chip ATM and point of sale acceptance devices in the U.S.

The Chip Vendor Enabled Service (CVES) engages third-party chip tool vendors to execute mandatory ADVT and CDET testing on behalf of acquirers and processors, analyze the results, and submit reports to Visa using the CCRT.

Vendors choosing to participate in CVES must complete a confirmation process by which the vendors' eligibility is verified and the ability to effectively deliver the required services is demonstrated. Approved vendors will be included on the Visa-Confirmed Third-party Chip Tool Suppliers list.

3.3.5.1 HOW IT WORKS

Any Visa-recognized chip tool supplier with a product currently listed in the Visa-Confirmed Third-party Chip Tool Suppliers list, also found on the Visa Technology Partner website as confirmed by Visa for ADVT and CDET card simulation, is eligible to participate in the CVES. The vendor must have a valid Visa Business ID (BID), and active Visa Online User ID, organization and user entitlement to the CCRT for test result submissions, and a valid listing on the Visa Technology Partner website as a Visa-confirmed vendor for this service.

To begin engagement with Visa, vendors should submit their request via email to chiptoolkits@visa.com. Once the request is received, Visa will ensure the vendor meets the eligibility requirements and will send the vendor the required paperwork. On completion and approval, a Visa Business ID will be provided by Visa. Results of the first vendor submission will be reviewed by Visa.

The enabled vendor must be a current Visa-confirmed supplier of an ADVT and CDET card simulator and must be confirmed by Visa as being capable of delivering the following services on the client's behalf:

- Utilize their own Visa-confirmed card simulator for test execution
- Execute the required ADVT or CDET tests on the client's acceptance device
- Analyze results and determine pass/fail outcome
- Offer consultation on any failed or inconclusive results as necessary
- Successfully submit test results of behalf of clients into the CCRT
- Monitor terminal deployment for interoperability issues

Clients must complete all required licensing and set-up paperwork as a prerequisite for providing CCRT entitlement to their chosen vendor.

3.3.5.2 BENEFITS TO BUSINESS

Acquirers will benefit from a centralized process that delivers:

- Faster time-to-market with speedy test execution and result submission
- Improved efficiencies of device testing methods mitigating time delays to deployment
- Minimized interoperability problems and poor cardholder experience in market
- "One test" solution for acquirer testing

Additional documentation is available for Visa clients on Visa online. Vendors can access Visa documentation at Visa Technology Partner website https://technologypartner.visa.com and documentation is also publicly available on www.visachip.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

- Chip Compliance Report Tool (CCRT) User Guide
- Chip Compliance Report Tool (CCRT) Quick User Guide
- Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide
- Visa Smart Debit/Credit ATM U.S. Acquirer Implementation Guide
- CVES Benefits
- Visa Chip Bytes
- Visa Minimum U.S. Online Only Terminal Configuration document
- Visa U.S. EMV Chip Terminal Testing Requirements

3.4 Discover Acquirer Terminal End-to-End Certification Testing

The Discover Acquirer Terminal End-to-End (E2E) Certification is managed by accredited E2E service providers. To obtain a list of accredited E2E service providers, contact the Discover account executive.

The purpose of the Acquirer Terminal End-to-End Certification is to ensure that acquirers are able to:

- Demonstrate that the deployed terminals meet the requirements of both the acquirer and Discover
- Demonstrate the terminal's acceptance of D-PAS products
- Send and receive authorization requests and authorization responses between a terminal, acquirer host system, and the network
- Demonstrate that terminals can process chip-based functions including support of PIN, fallback transactions and Cardholder Verification Methods (CVMs), as supported by the terminal

Note: An acquirer must successfully execute the Acquirer Terminal End-to-End Test for every unique POS combination enabled to accept chip cards.

Note: Discover Terminal E2E Certification also covers certification with Discover's network partners, or entities licensed to use the D-PAS product.

3.4.1 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
  - In addition, when the terminal supports a PIN entry device (PED), it must be Payment Card Industry PIN Transaction Security (PCI PTS) approved.
- Acquirer End-to-End Test Tools (see Section 3.4.2)

3.4.2 Test Tools

Table 4 lists the tools used for Acquirer Terminal End-to-End testing.

Table 4. Discover Acquirer Terminal End-to-End Testing Tools

Tool	Description
Fully-configured physical test cards or Discover-qualified smart card simulator	Acquirers can request up to 10 full sets of test cards from Discover, at no charge. Further test cards, if needed, can be purchased from an approved test card provider. Contact the implementation manager to: • Obtain physical test cards or purchase additional sets of physical cards from an approved third party vendor **Important!** The physical cards distributed to acquirers are the property of Discover and may be used only for testing purposes.
Acquirer Terminal End-to-End Test Tool	Acquirers must use a Discover-qualified Acquirer Test Tool that simulates the network and issuer host system.

3.4.3 Obtaining Qualified Test Tools

Discover has prepared a list of qualified test tools to simulate the presence and processing of issuers, networks and terminals. These tools are available from external vendors.

To obtain and verify a test tool:

1. Obtain a list of qualified tools from the implementation manager.
2. Select one or more test tools from the list of qualified tools.
3. Obtain the required tool or tools from the vendor.
4. Set them up in accordance with the vendor's specification.
5. Perform internal, informal tests to verify that the tools function as intended.

3.4.4 Acquirer Terminal End-to-End Testing Architecture

Figure 5 shows the acquirer terminal end-to-end testing architecture that enables the simulation of network and issuer responses.

Transactions are generated at the terminal(s) using either physical cards or a smart card simulator.

Transactions are routed from the terminal through to the acquirer host and to the acquirer test tool, which generates a response for online transactions.

Offline transactions are processed only at the terminal(s) and involve only the physical cards or smart card simulator and the terminal(s).

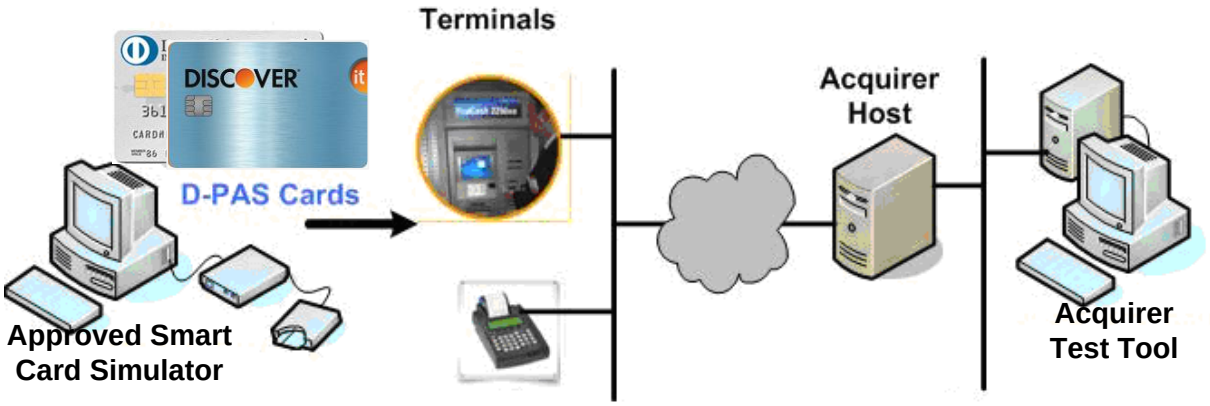

Figure 5. Acquirer Terminal End-to-End Testing Architecture

3.4.5 Initiation

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

- D-PAS Card Request Form – Used to request physical test cards.
  - Cards can be obtained by contacting the assigned Discover account executive.
- E2E Service Provider Order Form – Used to begin the E2E certification project with the chosen E2E service provider.
- D-PAS E2E Certification Request Form – Used to provide details about various terminal functions such as CVM methods supported, Offline Data Authentication methods supported, and fallback. The E2E service provider assigns E2E test cases based on this form.
  - Form can be obtained by contacting an accredited E2E service provider.

3.4.6 Test Execution

The Acquirer-Terminal End-to-End Test must be executed in accordance with the approved Acquirer Certification Response Form, the Acquirer-Terminal End-to-End Test Plan, and the parameters specified in the D-PAS Certification Guide.

3.4.7 Results

Acquirers must record on the Certification Response Form the results of each test case executed and submit the form, together with the card/terminal logs, host logs and receipts (as applicable) to the E2E service provider, for them to validate the successful completion of the test cases.

Acquirers must follow the procedure described in the D-PAS Certification Guide.

3.4.8 Test Case Validation

The E2E service provider validates the test case results and provides feedback to the acquirer for the test cases executed.

3.4.9 Letter of Certification

After all of the required tests have been successfully executed, the E2E service provider sends an e-mail to the acquirer that includes a Letter of Certification for the completed tests. The letter specifies the following:

- Test plans that were completed
- Interfaces that were tested
- Test cases that were excluded from testing (if applicable)

3.5 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's/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 www.americanexpress.com/merchantspecs.

3.5.1 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.

3.5.2 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 the American Express representative to start the certification process.

The American Express POS Certification Participant Program is available to acquirer and acquirer processors interested in conducting self-testing of devices to accept American Express chip card transactions. Acquirers 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 the American Express representative to receive more information about the program.

3.5.3 Prerequisites for Device Certification

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

Contact:

1. EMVCo Level 1 and Level 2* certification status must be 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 must be 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 Testing Processes

Some of the global payment networks require tests in addition to those described in the sections "Acquirer Host Testing" and "Terminal Testing Requirements."

4.1 MasterCard End-to-End Demonstration (Optional)

A MasterCard Acquirer End-To-End Demonstration (ETED) may be performed 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, six -digit PIN cards, and cards that generate issuer script messages).

Acquirer ETED may be ordered from a MasterCard accredited ETED service provider.

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.

Production validation is executed by conducting tests using live D-PAS chip cards and D-PAS enabled terminals deployed in the market.

Acquirers are required to participate in validation testing to confirm that all required D-PAS transaction functionality works as expected.

4.2.1 Purpose

The purpose of acquirer production validation is to confirm that:

- Terminals have been properly configured to accept D-PAS, and
- Acquirers can successfully pass the necessary D-PAS data for authorization.

4.2.2 Prerequisites

Before conducting production validation, acquirers must:

- Complete all required acquirer certification tests.
- Ensure that all of the required terminal parameters are loaded across the terminal base, including:
  - D-PAS Application Identifier (AID)
  - Application Version Number
  - Certificate Authority Public Keys (Production Keys)
  - Terminal Action Codes (TACs)
  - Terminal Floor Limits
  - Default Dynamic Data Authentication Data Object List (if Dynamic Data Authentication is supported).

4.2.3 Requirements

The implementation manager provides an Acquirer Production Validation Test Plan.

The acquirer then:

- Identifies resource(s) to conduct testing
- Identifies the terminals where production validation will be executed
- Submits locations and timeframes for where and when production validation tests will be conducted
- Performs production validation testing, in conjunction with their implementation manager, using the Acquirer Production Validation Test Plan.

4.2.4 Card Request Form

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.

4.2.5 Test Execution

For acquirer production validation, acquirers must:

- Execute the production validation process using the Discover Acquirer Production Validation Test Plan and any acquirer-specific production validation test case scenarios that the acquirer would like to include
- Complete and document production validation test results at all applicable terminals
- Work with their implementation manager to resolve any issues
- Return the following items to their implementation manager:
  - A completed Acquirer Production Validation Test Plan and any required supporting documentation
  - Funded test cards (if used)

Note: Unfunded test cards do not need to be returned.

4.2.6 Results

Acquirers must send the test plan and any supporting documentation to Discover, who reviews the test results.

5 When Terminal Retesting 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 the global payment network representative or acquirer). It is recommended that acquirers always perform internal testing using the global payment network's testing tools when changes are made.

Note: PIN pad references in this document do not have EMV chip processing impacts. Adding a card reader does have EMV chip processing impacts which would have testing requirements.

Use cases are provided in the following categories:

- ATM use cases
- Terminal use cases
- Acquirer processor platform use cases
- Value added reseller use cases
- Gateway use cases
- Unattended/automated fuel dispenser (AFD) use cases

The use case categories for when to test 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 does not require recertification. However, best practice would be to run an internal test based on the required testing and contact the payment network if any issues are found.
	For a use case with a check mark, 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 networks.

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 regardless of terminal vendor or terminal family. Do I need to repeat required testing with the payment networks?

This hardware change is classified as a minor change. Therefore, retesting with the payment networks 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 (Windows XP to Window 7) with kernel changes, do I need to repeat required testing?

Yes. Retesting would be required.

Q. If I change my operating system (Windows XP to Window 7) without kernel changes, do I need to repeat required testing?

No. Formal testing is not required if there are no changes impacting the payment application for chip processing or the kernel.

Q. If I am adding a new AID to an existing terminal configuration, do I need to retest?

Yes. Retesting is required since adding a new AID would change the Level 2 configuration.

Q. I would like to add an additional service, such as cash advance and balance inquiry. Do I need to repeat required testing?

Yes. Most of the payment networks require specific testing to support these transaction types, which include host testing because it impacts the authorization message for chip processing (cryptogram data). Refer to the applicable payment network for more details.

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 terminals (BBT), unattended terminals, automated fuel dispensers and on-board devices (handheld terminals 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 falls 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 networks 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 networks regardless of terminal vendor and terminal family?

This hardware change is classified as a minor change. Therefore, retesting with the payment networks 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 networks require specific testing to support these transaction types, which include host testing because it impacts the authorization message for chip processing (cryptogram data). Refer to the applicable payment network for more details.

Q. If I am adding a new AID to an existing terminal configuration, do I need to retest?

Yes. Retesting is required since adding a new AID would change the Level 2 configuration.

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

No. Existing terminals can remain in market beyond the approval expiration as long as there are no changes to the kernel or chip processing logic. This would include existing inventory already in the distribution channel as long as there are no interoperability issues. Review with your kernel provider, as the provider may need to update the kernel. Refer to the Kernel Management Guidelines webcast available at http://www.emv-connection.com/emv-resources/ and EMVCo Type Approval Bulletin No. 11, 6th Edition, February 2014, for more details.

However, new terminals should be deployed with the updated kernel and with IFM tested appropriately with the payment networks. The global payment networks have specific processes to address this particular issue that fall outside the scope of this document.

Q. I would like to add an additional service, such as refunds or voice authorization. Do I need to repeat required testing?

No. Formal testing is not required since the functionality is considered non-EMV transaction processing.

Q. I would like to add an additional service, such as gratuity. Do I need to repeat required testing?

It depends. If there are changes to the cardholder verification method (CVM), retesting would be required.

Q. I would like to add an additional service, such as PIN Entry Bypass. Do I need to repeat required testing?

Yes. Retesting is required since it impacts changes to the kernel.

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 networks is necessary since this would include a card reader.

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 loyalty program. 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 networks is necessary any time EMV chip processing is affected since this would include a card reader.

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 as it will impact chip processing. With most payment networks, testing is not restricted to the terminal but constitutes end-to-end testing. The payment networks should be involved in this process.

Q. I am implementing terminals which will support Near Field Communication (NFC) (e.g., Apple Pay, Samsung Pay, Android Pay). Are there global payment network terminal testing requirements?

Yes. Each global payment network has test tools that support contactless terminal testing. Refer to each global payment network for more details on their requirements.

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.

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 using a different POS system (that is not part of the payment transaction process but only prints the receipt) with a previously tested semi-integrated payment solution require testing?

No. Formal testing is not required.

Q. Does changing non-EMV related receipt information when integrating a POS system to a previously tested semi-integrated payment solution require testing?

No. However, the acquirer should validate the receipt implementation has not changed the required EMV elements.

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 should consult with the terminal vendor for impacts. If there are changes impacting chip processing, the acquirer needs to complete required testing with the payment networks. Refer to the applicable payment network for more details.

5.2.2 Standalone Terminal Use Cases

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

No. Other applications are out of scope.

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

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

Q. I am an acquirer processor offering a standalone POS solution. Does each merchant that will deploy it need to perform terminal testing?

No. Standalone solutions tested for a given acquiring platform are generally acceptable for deployment at all merchants for that acquiring platform after the first full terminal test.

Q. If an acquirer processor is offering a standalone POS solution for clients on a specific processing platform, do all acquirers need to retest after the first full terminal test?

No. POS solutions tested for a given acquiring platform are generally acceptable for deployment by all acquirers on that platform.

Q. We have certified a standalone terminal with an external PIN pad. Can we deploy the terminal as a standalone device, without the external PIN pad, without any additional testing?

Retesting is only required if the changes impact the payment application for chip processing or the kernel. Disabling a CVM should not require retesting.

Q. My terminal provider has provided the Letter of Approval (LoA) for Level 2 type approval which includes several terminal configurations. Do I have to test all of the configurations listed in the LoA?

No, one set of required testing per terminal family is needed for the unique terminal configuration. Consult with the terminal vendor for information on whether a group of terminals falls within the same terminal family.

Q. I have a previously tested standalone terminal and will be adding an external PIN pad (with a card reader). What type of effort is required for the already certified terminal?

Rerunning required tests with the payment networks is necessary.

Q. I have a previously tested standalone terminal and will be adding an external PIN pad (without a card reader). What type of effort is required for the already certified terminal?

If an online only PIN pad is added, then retesting is not needed.

If an offline PIN pad is added, then retesting would be required.

Q. I am adding contactless functionality to a previously tested contact chip only terminal, what is the scope of required testing when it comes to the contact chip side that was already completed?

It depends on the impacts to the payment application, when adding contactless. If there is no change in the payment application and contactless is enabled by configuration, then regression testing should be performed to ensure no impacts when adding contactless.

If there is a change in the payment application for handling contactless, then contact chip testing would be required.

Q. If I want to disable a CVM on a device previously tested for all CVMS, do I need to retest?

If the device was previously tested with all CVMs, but then you decide to disable one, regression testing is recommended. Consult with the terminal vendor to validate there is no impact.

Q. If I want to add point-to-point encryption (P2PE), will it impact my EMV implementation and require retesting?

Adding P2PE should not impact EMV implementation, and vice versa, assuming that P2PE occurs outside of the EMV kernel (which it always should). Regression testing should be performed to ensure there are no impacts when adding P2PE.

5.3 Acquirer Processor Platform Use Cases

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

Q. When biannual payment network 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 networks.

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. If there are changes to the message format for chip processing, then testing will be required. The payment networks should be involved in this process.

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

Yes. This is a major change as it impacts the message format for chip processing, and the payment networks should be involved in this process.

Q. I am changing processing platforms that support a different message format. Do I need to complete required testing with the payment networks?

Yes. This is a major change as it impacts the message format, and the payment networks should be involved in this process.

***Note**: Payment networks do not recommend acquirer host systems alter chip data elements from the terminal in the terminal-to-acquirer message. If any of the data elements are corrupted or altered by the acquirer host system, the cryptogram will fail.*

Q. I am an acquirer processor making changes to my processing platform impacting chip processing. Do I need to perform any host testing with the payment networks?

Yes. This is a major change as it impacts the message format and the payment networks should be involved in this process.

5.4 Value-Added Reseller Use Cases

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 system's 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. My semi-integrated payment application will be used with multiple terminal vendors. Is retesting required with each terminal vendor and acquirer processor?

Yes. Retesting is required if changes are made to the payment application or kernel. These major changes are defined in Bulletin #11 6th Edition, February 2014, available on www.emvco.com. Changes from one acquirer processor to another typically impact the message format for each processing platform requiring retesting.

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 network enhancements for magnetic stripe transactions. Do I need to complete required testing?

No. Retesting is not required.

Q. I've added a new payment peripheral device (e.g., a cash dispenser module) 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 since changes typically impact the payment application for chip processing.

5.5 Gateway Use Cases

Q. I am a pass-through gateway. Do I need to perform terminal testing with each acquirer processing platform connection?

Retesting may not be required, depending on what areas are affected. The payment networks should be involved in this process. Any time there are changes to the payment application affecting chip processing or the kernel by terminal configuration, retesting with the payment networks is required.

Q. I am a gateway that alters the message format. Do I need to perform terminal testing with each acquirer processing platform connection?

Yes. Retesting is required.

5.6 Unattended/Automated Fuel Dispenser Use Cases

Figure 6 illustrates an example of the petroleum transaction process flow. The following areas are potentially impacted when migrating to EMV:

- Level 1 interface module (IFM)
- Level 2 kernel
- Level 2 contactless kernels
- Implemented kernel configurations
- Payment terminal application
  - Typically there is a POS application that does not play a role in EMV, unless the POS and electronic payment server (EPS) applications are actually the same application.
  - For outdoor transactions, the transaction flow will go through a forecourt controller then into the EPS where the fuel forecourt controller acts as a pass-through.
- Electronic payment server (version, model number, host interface version)
  - Host message formats and interface to the acquirer or possibly to the gateway (which may be different) are impacted.
  - In some cases, there may be a payment gateway in between the EPS and the acquirer.
- Acquirer/processing platform

Q. I have already deployed terminals in-store and now will be upgrading my AFD. Do I need to retest my in-store terminals?

Retesting is only required if the changes impact the in-store payment application for chip processing or the kernel. If upgrading the AFD impacts the in-store flow, then retesting would be required. Typically it is a separate processing flow.

Q. I am making changes to my electronic payment server which will impact chip processing. Is retesting required?

Yes. Retesting is required. The electronic payment server typically impacts chip processing.

Q. I am making changes to my forecourt controller. Is retesting required?

Retesting is only required if the changes impact the payment application for chip processing or the kernel. If the forecourt is only a pass-through that doesn't touch chip processing, retesting is not required.

Q. I would like to add an additional service, such as partial approval to an AFD authorization. Do I need to repeat required testing?

No. Formal testing is not required since the functionality is considered non-EMV transaction processing

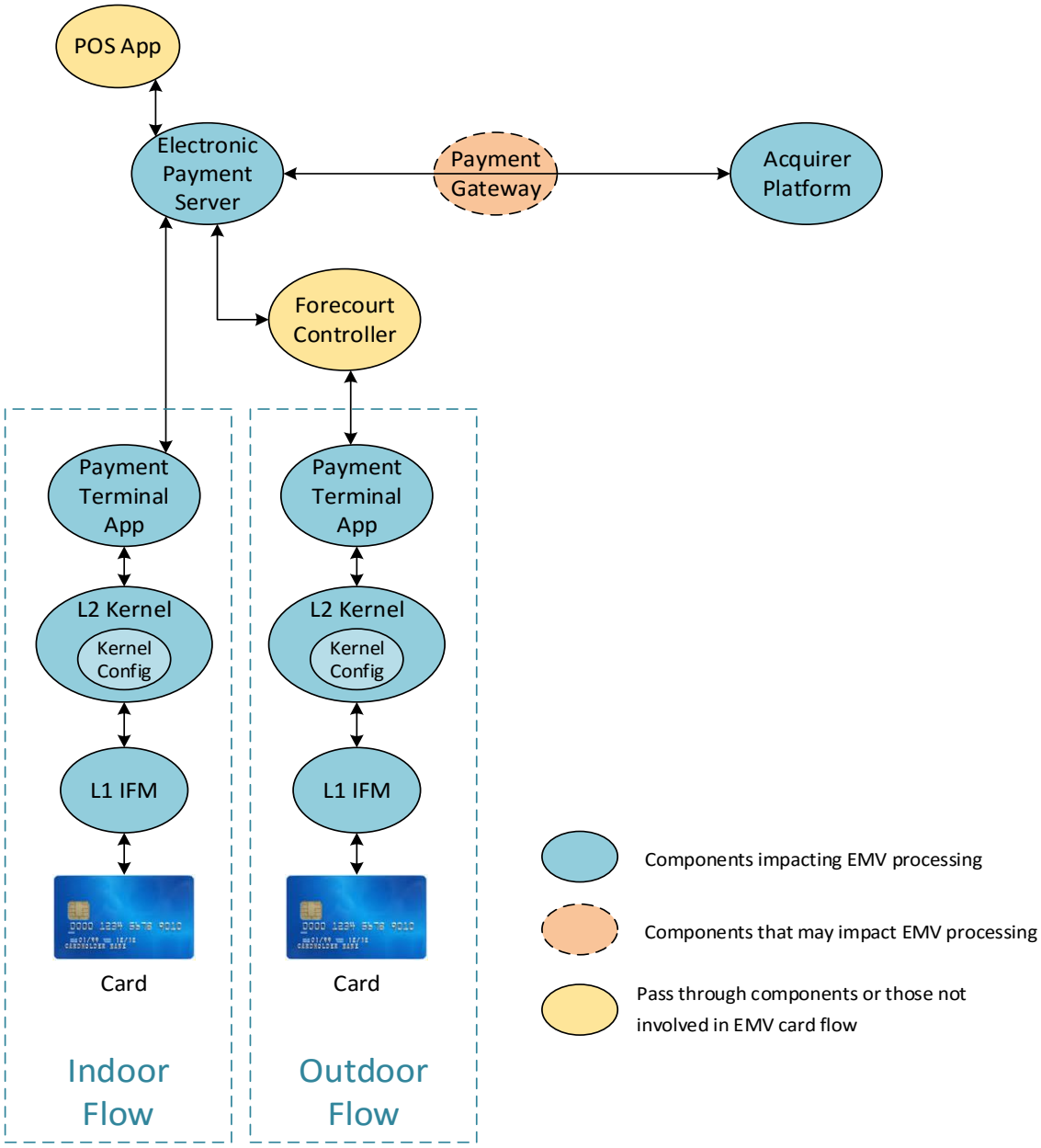

Figure 6. Petroleum Transaction Process Flow with Areas Impacted by EMV Migration

6 References

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

American Express

American Express technical specification web site, www.americanexpress.com/merchantspecs

Discover

Contact your assigned Discover representative.

EMV Migration Forum

EMV Migration Forum web site, http://www.emv-connection.com

Chip Education for VARs, ISVs and Merchants, http://www.emv-connection.com/chip-education-for-vars-isvs-and-merchants/

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/

PCI Security Standards Council

U.S. EMV VAR Qualification Program, https://www.pcisecuritystandards.org/approved_companies_providers/var_qualifications_program.php

Visa

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

Visachip.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 networks' 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 the V1.0 white paper included: Acquirer Systems, American Express, Chase, Discover, MasterCard, TSYS, Vantiv, VeriFone, and Visa. The V2.0 white paper update was developed with input from American Express, Discover, MasterCard and Visa.

The EMV Migration Forum wishes to thank the Testing and Certification Working Committee members for their contributions to the white paper use cases.

The following members participated in the development and review of the V2.0 white paper:

- Dave Blust, Galitt
- Charl Botes, MasterCard
- Eric Bartfield, Elavon
- Mar Castrechini, Cayan
- Steven Cole, Vantiv
- Deana Cook, Chase Paymentech
- Kevin Emery, Discover
- Anne Fairchild, First Data
- Art Harper, PSCU
- Cindy Kohler, Visa
- Ed Learned, MerchantLink
- Tomas Levi, Gilbarco
- Dave Maisey, ICC Solutions
- Andy Patania, First Data
- Ben Potter, Discover
- Todd Smith, Heartland Payment Systems
- Joe Santana, FIME
- Clyde L. Van Blarcum, American Express
- Huy Vu, China UnionPay

Trademark Notice

8 Appendix A: U.S. EMV VAR Qualification Program

PST
Payments Security Task Force | **EMF**
EMV Migration Forum

Value Added Reseller (VAR) Qualification Program: A Streamlined U.S. EMV Terminal Testing and Certification Process to Support Efficient Migration

The VAR Qualification Program was created through collaboration across the industry

The PST Value Added Reseller working group has participants from across the industry

Service Providers
AJB software
VeriFone, A division of Hewlett-Packard

Brands
MasterCard
VISA
American Express
Discover Network

Acquirers
Bank of America Merchant Services
Chase Paymentech
WorldPay
Elavon
TSYS
vantiv
Wells Fargo
citibank
globalpayments
Heartland Payment Systems
First Data

Test Tool Vendors
Galitt
Acquirer Systems
UL ICC Solutions
FIME — the recognised leader in EM test tools and service provi
Clear2Pay

Program Administrator
PCI Security Standards Council

Overview | U.S. EMV VAR Qualification Program

The US EMV VAR Qualification Program officially launched on April 30th, 2015

Objectives

- Accelerate multi-acquirer solution certification
- Provide clear and consistent EMV education content
- Create a central community with better communication
- Accelerate the delivery of EMV for small to midsize merchants

Live Program Components

Standard set of educational materials in the form of a webcast series hosted on the EMV Migration Forum website

See here for more information:
http://www.emv-connection.com/chip-education-for-vars-isvs-and-merchants/

Pre-qualification process for Value Added Resellers (VARs) and Independent Software Vendors (ISVs) to complete brands' test cases with an accredited service provider, supported and facilitated by a public PCI SSC listing system

See here for more information:
https://www.pcisecuritystandards.org/approved_companies_providers/var_qualifications_program.php

The program will benefit stakeholders across the Payments value chain

Service Providers

- Prioritize/expedite process for testing with each acquirer
- Potential to shorten debugging/training time
- Access to accredited service providers across brands that provide additional technical training/education

Acquirers

- Reduce time/resources needed to educate/test VARs
- More predictability in resource scheduling and rollout schedules
- Enhance dialogue with brands

Test Tool Vendors

- Potential to develop deeper long-term relationships with key and new customers
- Ability to leverage education assets in addition to test tools and services

Brands

- Advancement of standardization in execution of testing
- Encouragement of accelerated and higher quality rollout solutions
- Ensure baseline functionality

Merchants

- Completion of final acquirer certification more quickly
- Lower interoperability issues in the field
- Fewer in-field updates and changes necessary

9 Appendix B: EMV Data Elements Impacting Terminal Testing

Table 5 shows the EMV data elements that would impact when global payment network terminal retesting would be required. While there are other EMV tags required for chip processing, these tags impact the terminal testing. For a complete list of tags, refer to individual global payment network documentation. For more Information on EMVCo major and minor terminal changes which can impact global payment network testing, refer to Bulletin #11 *6th Edition, February 2014* available on www.emvco.com.

Table 5. EMV Data Elements Impacting Terminal Testing

Name	Source	Tag	AMEX	Discover	MasterCard	Visa
Application Interchange Profile*	Card	82	M	M	M	M
Application PAN Sequence Number	Card	5F34	M	Field 23	DE23	Field 23/C
Application Transaction Counter*	Card	9F36	M	M	M	M
Card Verification Method Results*	Card	9F34		O	M	O
Dedicated File Name (Card AID)	Card	84		O	M	M
Issuer Application Data*	Card	9F10	M	M	M	M
Amount, Authorized*	Term.	9F02	M	M	M	M
Amount, Other*	Term.	9F03	M	C	O	C
Terminal Capabilities	Term.	9F33	Bit 22	M	M	M
Terminal Country Code*	Term.	9F1A	M	M	M	M
Terminal Verification Results*	Term.	95	M	M	M	M
Transaction Currency Code*	Term.	5F2A	M	M	M	M
Transaction Date*	Term.	9A	M	M	M	M*
Transaction Type*	Term.	9C	M	M	M	M
Unpredictable Number*	Term.	9F37	M	C	M	M
Transaction Category Code	Term	9F53			O	

*The tags denoted with the asterisk in the table above are cryptogram data elements and while provided by the card, they should be provided unaltered.

The values in the tables represent each global payment networks' requirements to support these EMV tags.

Legend:

M = Mandatory data
O = Optional data
C = Conditional
Blank = no requirement

Table 6 identifies the data for an authorization response.

Table 6. Authorization Response Data

Name	Source	Tag	AMEX	Discover	MasterCard	Visa
Issuer Authentication Data	Issuer	91	O	O	M*	C
Issuer Script Template 1	Issuer	71	C	C	C	C
Issuer Script Template 2	Issuer	72	C	C	C	C

Note: Global payment networks do not recommend acquirer host systems alter chip data elements from the terminal in the terminal-to-acquirer message. If any of the data elements are corrupted or altered by the acquirer host system, the cryptogram will fail.

MasterCard Requirements:

*The Issuer Authentication Data must be present in the online response message when the conditions below are met (any transactions originated from MasterCard Stand-In are excluded):

- Subfield 1 of DE 22 (POS Entry Mode) contains a value of 05.
- DE 55 is present including all mandatory tags.
- The ARQC has been validated successfully.
- The Issuer's Response Code indicates an approval.

Issuer Authentication Data from the online response is never delivered to the contactless device/form factor.