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

Version 4.0

Date: December 2017

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

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@uspaymentsforum.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 contact and contactless 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@uspaymentsforum.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 12 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.

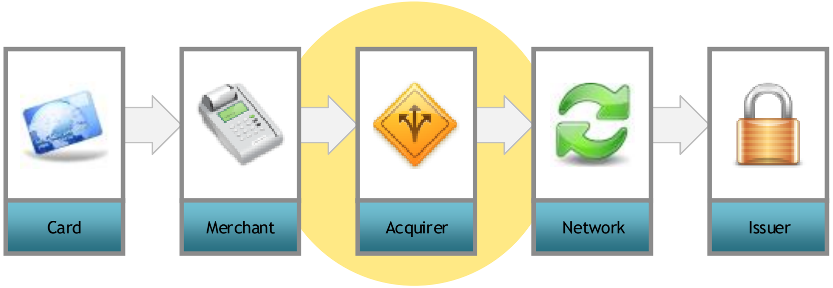

Figure 1. Acquirer Host Position in the Payment Process

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.

Contact your Mastercard account manager for more information and/or initiation of project.

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

Assigned Mastercard project team assists the acquirer with technical or testing-related questions and required activities. Implementation project manager generates the list of appropriate NIV test cases for the particular session. This list includes test cases sufficient enough to perform specific interface validation, but may not cover all scenarios technically possible.

After tests are performed, acquirer submits test logs from the simulator(s) to the implementation specialist. Logs are reviewed by Mastercard teams and results are provided back to the acquirer. Corrections and rerun of some test cases may be requested when needed.

Upon successful completion of NIV, Mastercard provides a Testing Acknowledgement Letter (TAN) that includes details of the validation session. TAN may be used as proof of completed validation during future implementations.

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 EMV contact and contactless 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 (contactless chip) 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 Quick Chip and 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 contact and contactless 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*

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)

As an option, a Discover-approved test tool may be obtained for offline pre-certification testing.

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.
- If an acquirer wishes to obtain physical test cards, they may request them directly from their Discover implementation manager.
- Certificate Authority (CA) Security Officer Registration Form. This form is used to register security officers and obtain CA public keys. CA public keys can also be obtained through encrypted email from your Discover implementation manager.

All forms can be obtained by contacting your Discover implementation manager.

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 implementation manager.

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.

Merchants, acquirers, processors and others (ISOs, ISVs, VARs) can also register on Amex Enabled (https://network.americanexpress.com/globalnetwork/amex-enabled/) and review products and services offered.

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 and Settlement 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.

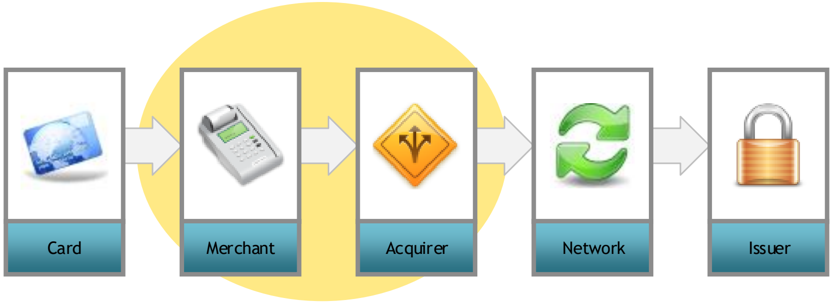

Figure 2. Areas Covered by Terminal Testing

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. (e.g., changes to CVM supported by terminal, addition of new payment methods)
- Terminal-to-acquirer-to-network 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/.

All payment networks support testing on an expired EMVCo approved kernel for a year from the expiration date of the kernel. Refer to each payment network for details on their processes.

Refer to EMVCo new bulletin to extend the validity of Contact Terminal Level 2 Type Approval – Bulletin nº 193, Contact Terminal Level 2 - Four Years LoA Validity on 24 June 2017 at http://emvco.com/news.aspx.

The U.S. Payments 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 U.S. Payments 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.

Through the U.S. Payments Forum Testing and Certification Working Committee, the global payment networks provided education and clarity on testing requirements and processes as well as their 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 U.S. Payments Forum Knowledge Center website.[2]
- Developed the "EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community" in July 2013 and updated version in April 2016 (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.

The Payments Security Task Force joined with the PCI Security Standards Council and the U.S. Payments Forum and launched a chip education curriculum in April 2015. 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/.

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[3] 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.[4] 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] http://www.emv-connection.com

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

[4] 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.

Kernel Management. Mastercard allows M-TIP certification performed on devices using a valid kernel. Kernel is considered valid from inception until 12 months after the kernel expiration date. Mastercard allows an expired EMV Level 2 Kernel used for new M-TIP certifications for a period of 12 months after the kernel expiration.

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. M-TIP test tools scenarios and tools are updated from time to time, based on any requirement changes or interoperability findings. Acquirers should use the latest version of their selected tool for each MTIP session.

Mastercard Contactless Vendor Product Letter of Approval (for contactless terminals). Obtain this letter from the terminal vendor/VAR/integrator.

3.2.2 Registering the M-TIP

Before starting an M-TIP project, go to Mastercard Connect and download the latest M-TIP *documentation*, 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 specifics of the terminal being tested and 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. TSE also allows selection of terminal configuration from a pre-set list of common U.S. Terminal configurations for ease of use. The list of U.S. Standard Terminal Configurations may be found in the documentation available on Mastercard Connect.

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

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

Information	Explanation	Source
Terminal brand	The brand of payment terminal being tested (for example, Verifone, Ingenico, Equinox)	–
Terminal model	The model number of the terminal being tested (for example, Verifone VX510)	–
EMVCo Level 1 approval reference	Level 1 approval for the terminal	Find this number on the certificate from the hardware supplier. Verify that the approval reference is valid by checking this reference on www.emvco.com.

Information	Explanation	Source
		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.
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.

Information	Explanation	Source
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

Acquirers should run all test cases extracted by TSE, using the M-TIP test tool. TSE provides the pass criteria with the details of the test transactions, which determines whether the case is successfully completed or not. Acquirers should validate pass criteria for all test cases were successfully met.

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.
- Consider using a U.S. Standard Terminal Configuration.
- A dry run of all test cases is recommended before starting the final testing for submission.
- Confirm pass criteria are met for each test case before submitting test logs for formal validation.
- 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.

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.[5]

Financial Institutions or MSPs that are performing the acquiring of payment transactions may be willing to perform the activities below without any recourse to an accredited service provider:

a. M-TIP test result analysis and validation
b. M-TIP approval decision before deployment of a new terminal configuration or deployment of a new terminal payment application.

Mastercard has developed the M-TIP Self-Approval accreditation process to accredit financial institutions or MSPs (applicants) and to allow them performing the above activities a) and b) within their own organization instead of ordering the M-TIP service to an accredited service provider.

M-TIP Self-Approval accreditation takes place further to the signature by the applicant of the agreement for M-TIP Self-Approval. Accreditation is primarily performed by means of accreditation audits.

[5] For more information on the self-approval program, contact Mastercard.

The applicant may decide to subcontract operational aspects of the M-TIP process to a support company. A support company has to be accredited by Mastercard for delivery of support services to SACs.

3.2.9 Mastercard U.S. Delegated L3 Testing

Mastercard recommends that acquirers perform regular M-TIP terminal certification, either using accredited M-TIP service providers or on their own through the M-TIP Self-Approval Program.

However, Mastercard offers the ability for U.S. acquirers and their partners to perform internal validation of the POS payment systems they intend to deploy in the U.S. The US Delegated L3 Testing framework is designed to enable Acquirers and their partners – value added resellers (VAR), independent sales organizations (ISO) and gateways – to quickly and efficiently deploy interoperable contact and contactless M/Chip solutions with their merchant customers.

Acquirers willing to participate in U.S. Delegated L3 Testing framework are required to go through a due diligence program with Mastercard to demonstrate they have appropriate testing and quality assurance measures in place, including test tools and processes, and have proven that they have successfully completed M-TIP projects without multiple iterations of testing and corrections in the past. Acquirers operating under the Mastercard M-TIP Self-Approval process can leverage their accreditation as part of the U.S. Delegated L3 Testing Framework due diligence program.

Approved acquirers may perform M-TIP validations internally without using a 3rd party service provider. The program also allows the use of alternate tools for logging and validations.

However, Mastercard requires at all times full compliance with the Mastercard Rules and Requirements (including the M/Chip Requirements). Acquirers are liable for the compliance, quality and interoperability of the terminals they and their merchants deploy under their oversight/approval. Non-compliances and failure to fix them in a timely manner may result in Category A non-compliance assessment (Mastercard Rules 2.1.4).

3.2.10 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 cases for EMV contact and contactless chip 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 requirements for each toolkit are outlined below.

3.3.1 Acquirer Device Validation Toolkit

To help ensure that deployed terminals do not contribute to interoperability problems, Visa developed the ADVT, which is a set of test cards and test scripts that can be used on terminals that have already received EMV Level 1 and Level 2 approval and are configured for deployment (that is, after the country code, floor limits, and other processing parameters are set up in the terminal).

Visa requires using the ADVT before initial deployment of their EMV contact chip terminals to help ensure that the terminal has been configured correctly and is capable of processing various use cases.

3.3.2 Contactless Device Evaluation Toolkit

CDET is an incremental set of contactless chip test cases that accompany ADVT (contact chip) for support of both contact and contactless chip.

Visa has an Android-based mobile app as an alternative and convenient option for performing the latest CDET (currently, Version 2.3) testing requirements using a mobile Near Field Communication (NFC) capable handset.

For new reader deployments, the acquirer executes each applicable CDET test to confirm that the expected outcome is achieved.

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 contactless terminal family that also shares the same Level 2 kernel, a single contactless reader can be CDET tested to cover the entire terminal family.

Consult with your terminal vendor to ensure that a terminal falls within a terminal family. This approach allows a general reduction in the number of test iterations with negligible impact to the integrity of the testing process.

3.3.3 Additional Toolkit Requirements

Use of the ADVT and the CDET is intended to ensure basic EMV contact and contactless chip functionality is not compromised during application integration, that all 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. In addition, Visa strongly recommends that ADVT and CDET toolkits are used on previously deployed terminals when troubleshooting or debugging acceptance issues. Also, both toolkits are required for existing contact and contactless chip-terminals that have undergone a significant hardware or software upgrade impacting the kernel or payment application for chip processing.

Visa Mobile Card Personalization (VMCP) app (Visa's new Android-based mobile app) combines the ability to personalize chip test cards for various testing toolkits (ADVT, CDET, Global Host Test Cards, other specialized test cards). It requires the use of a mobile handset with Near Field Communication (NFC) capability, as well as a Visa-supplied VMCP Utility Card.

3.3.3.1 U.S. Quick Chip and Minimum Online-only Terminal Test Cases

Minimum U.S. online-only terminal configurations may take advantage of the minimum test cases which are a subset of ADVT. These test cases can also be used for new deployments of Quick Chip and regression testing. It will allow for chip projects to proceed with reduced testing cycles, fewer test cases and a faster implementation time.

Contactless chip and Quick Chip can be implemented together with limited development and testing. If a merchant already supports Quick Chip, adding contactless chip (qVSDC) is an incremental development effort. It will require a new CDET certification and only ADVT regression testing on a previously certified POS solution.

Reminder: U.S. clients should only use U.S. versions of test cases.

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.

Details for access to the ADVT and the CDET can be obtained through Visa's third party fulfillment service. Similar tools are also available from Visa-confirmed third party vendors. For a list of Visa U.S. Confirmed Third-party Chip Acceptance Tool Suppliers, refer to https://technologypartner.visa.com. For a list of global products, refer to Visa-confirmed tool vendors, see Products and Toolkits at https://technologypartner.visa.com.

3.3.4 Chip Compliance Reporting Tool

Visa developed the Chip Compliance Reporting Tool (CCRT) as a centralized, server-based solution for the systematic reporting of ADVT and CDET test results. The CCRT facilitates a more efficient submission and management process of compliance reporting by chip acquirers. CCRT is available on Visa Online (Visa's online solution for providing secure access to Visa content and services for clients globally).

3.3.5 Visa Chip Vendor Enabled Service (CVES)

Launched in October 2013, CVES helps streamline the testing and reporting requirements for the deployment of ATM and point-of-sale chip-acceptance devices in the U.S. CVES engages third-party chip tool vendors to execute ADVT and CDET testing on behalf of acquirers and processors, analyze the results and optionally submit reports to Visa using the CCRT.

3.3.6 Visa U.S. Chip Acquirer Self-Accreditation Program

Visa U.S. Chip Acquirer Self-Accreditation Program for U.S. acquirers eliminates the need to use CCRT to report ADVT and CDET terminal test results when they deploy chip POS solutions. The program streamlines acquirers' chip-testing process and removes redundant reporting. It also allows acquirers flexibility to adjust their test plans based on the POS solution, merchant vertical and reiterations of testing, enabling them to perform the Visa-recommended minimum set of test scripts for both contact and contactless chip solutions.

To be eligible for the Visa U.S. Chip Acquirer Self-Accreditation Program, acquirers must:

- Partner with an accredited CVES vendor that can execute, analyze, and validate terminal test results, and has the capability to store test results, receipts and logs for up to five years or have the equivalent chip tool capability available in-house.

- Establish testing processing and requirements (i.e., defined chip terminal test cases).
- Complete the "Visa U.S. Chip Acquirer Self-Accreditation Program Acknowledgement Form."

Refer to ADVT and CDET User Guides as well as the latest versions of "U.S. Quick Chip and Minimum Terminal Configuration ADVT/CDET Use Cases" for more details on specific testing conditions. 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.

3.4 Discover Acquirer Terminal End-to-End Certification Testing

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 your Discover implementation manager.

The purpose of the acquirer terminal E2E certification is to verify that acquirers are able to:

- Demonstrate that the deployed terminals meet the requirements of both the acquirer and Discover Global Network
- 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

3.4.1 Prerequisites

Discover requires the following activities to be completed before beginning E2E certification:

- Acquirer host certification
- Obtain access to CA public keys (see section 2.3.2)
- Confirm device completing certification has relevant EMVCo Level 1 and Level 2 certifications and Discover Type Approval for contactless D-PAS devices.
    - In addition, when the terminal supports a PIN entry device (PED), it must be Payment Card Industry PIN Transaction Security (PCI PTS) approved.
- Obtain acquirer terminal E2E certification Test Tools (see Section 3.4.2)

3.4.2 Test Tools

Table 2 lists the tools used for acquirer terminal E2E Certification.

Table 2. Discover Acquirer Terminal End-to-End Testing Tools

Tool	Description
Physical test cards or Discover-qualified smart card simulator	Acquirers and merchants can request up to **10 full sets of test cards from Discover at no charge**. Additional test cards, if needed, can be purchased from an approved test card provider. Contact your Discover implementation manager to obtain information on these processes.
Acquirer terminal E2E certification test tool	Acquirers and merchants 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 industry 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 each tool up in accordance with the vendor's specification.
5. Perform internal tests to verify that the tools function as intended.

3.4.4 Initiation

An acquirer or direct-connect merchant following the service provider model for E2E certifications must complete the following documents before starting the E2E certification process:

- E2E Service Provider Order Form – used to begin the E2E certification project with the chosen E2E service provider.
- D-PAS E2E Certification Request Form (CRF) – 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.

These forms can be obtained by contacting an accredited E2E service provider.

3.4.5 Test Execution

The acquirer terminal E2E case must be executed in accordance with the approved Certification Response Form, the Acquirer-Terminal E2E Plan, and the parameters specified in the D-PAS Certification Manual for Issuers and Acquirers.

3.4.6 Results

Acquirers complete the CRF and record the results of each test case executed. The CRF is then submitted, 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 procedures described in the D-PAS Certification Manual for Issuers and Acquirers.

3.4.7 Test Case Validation

The E2E service provider validates the test case results sent by the acquirer, and provides feedback to the acquirer on the test cases executed.

3.4.8 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 cases that were completed
- Interfaces that were tested
- Test cases that were excluded from testing (if any)

3.4.9 Acquirer Managed Terminal Certification

From 2013, acquirers have been able to join the Discover Acquirer Managed Terminal Certification program (AMTC) also known as self-certification. Within this program, the acquirer is accredited to complete the E2E certification process, including test case validation, without any direct validation by an E2E service provider or Discover. In addition to the acquirer’s ability to validate its own test case results, the acquirer is also permitted to manage the evidence of its certification completion.

Discover has maintained the AMTC program and has streamlined and provided flexibility to the acquirer terminal E2E certification process. Discover manages each acquirer accreditation on a case-by-case basis.

To meet the certification process requirements set by Discover, acquirers may opt to work directly with a service provider or manage certification internally. If using a service provider that has not previously been accredited by Discover, the service provider will be indirectly accredited during the AMTC accreditation process. For more information on this program please contact your Discover implementation manager

3.4.10 Streamlined D-PAS E2E Test Plan

Discover has consistently demonstrated a focus on continuing to streamline certification processes. As a part of this commitment to acquirers and merchants, Discover released an updated D-PAS E2E Test Plan in Q3 2016.The updated D-PAS E2E Test Plan has a modular format to allow the test cases to be adjusted depending on the terminal functionality.

With this update, the acquirer will be able to take advantage of a more flexible testing approach and an increased ability to selectively execute test cases.

The updated D-PAS E2E Test Plan can be obtained by contacting your Discover implementation manager.

3.4.11 Discover *Contactless D-PAS* Terminal E2E Certification

Discover® *D-PAS* Terminal E2E Certification process is the same for both contact and contactless (CTL) and can be conducted in the same certification.

- Test cases are assigned depending on terminal configuration and include testing of **Consumer Device Cardholder Verification Method** (**CDCVM) and Discover U.S. Common Debit AID.**
- Contactless magnetic stripe data (MSD) 'Zip' support **does not require** D-PAS CTL Terminal E2E Certification.
- Contact test cases are assigned as **regression** when CTL is added to a previously contact certified terminal, providing additional flexibility.

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.

For AEIPS & Expresspay specifications, technical manuals and implementation guides log on to: www.americanexpress.com/merchantspecs

Merchants, acquirers, processors and others (ISOs, ISVs, VARs) can also register on Amex Enabled (https://network.americanexpress.com/globalnetwork/amex-enabled/) and review products & services offered.

3.5.2 Prerequisites for Device Certification

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

- Acquirer host certification.
- EMVCo Level 1 and EMVCo Level 2* (American Express/Expresspay Level 2* in case of contactless) certification status must be completed/current, and not expired or revoked.
  1. EMVCo certifications must reference the same device or device family as the device being requested for Level 3 American Express certification
  2. EMVCo Level 2* certification (for EMV contact) or American Express/Expresspay Level 2* (for Contactless) 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.

- When the terminal supports a PIN entry device (PED), it must be Payment Card Industry PIN Transaction Security (PCI PTS) approved.
- Usage of American Express approved certification Test Tools to conduct POS Device Certification. (See section 3.5.3.)

3.5.3 Approved Test tools

The merchant or processor must at their own cost, obtain licenses and permissions for tools (card/device logging or card simulator) that they select to conduct certification testing. The list of American Express approved test tools can be obtained from https://network.americanexpress.com/globalnetwork/amex-enabled/. (Go to 'Test Tools' and download the latest list.)

3.5.4 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 & provides Live Terminal parameters.
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 (CPP) 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 (CPP).

3.5.5 Self (Acquirer/Processor) Managed Terminal Certification

American Express approved Host Simulator Test Tools are evaluated by American Express to properly simulate the American Express Host System in a testing environment. The American Express Test System ("ATS") is an approved host simulator available at no cost to merchants and processors. ATS evaluates the authorization message sent by the device, and displays the pass or failure of the certification test case criteria.

Processors wishing to use a host simulator other than ATS must comply with the additional requirements defined in Approved Solution Provider Program Requirements Guide. Processors choosing to use a host simulator other than the ATS during certification testing are responsible for additional requirements that include, but are not limited to, ongoing maintenance to support the current version of message specifications and test plans, and support during qualification and approval of the selected host simulator. The processor is responsible for all costs associated with development and required maintenance of the host simulator. Please contact the American Express representative to receive more information about the Approved Solution Provider program.

4. Other Testing Processes

Some of the global payment networks require tests in addition to those described in the sections 2 and 3.

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 during enablement in production. 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). Although many different configurations are tested, this sampling may not cover all possible configurations and different scenarios.

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.
- Load all terminal parameters 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, free of charge.

This form can be obtained by contacting the assigned Discover implementation manager.

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 contact 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 the latest version of EMVCo Type Approval Bulletin No. 11 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. 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. 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 the latest version of EMVCo Bulletin #11 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.

5.4 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.

5.4 Unattended/Automated Fuel Dispenser Use Cases

Figure 3 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.

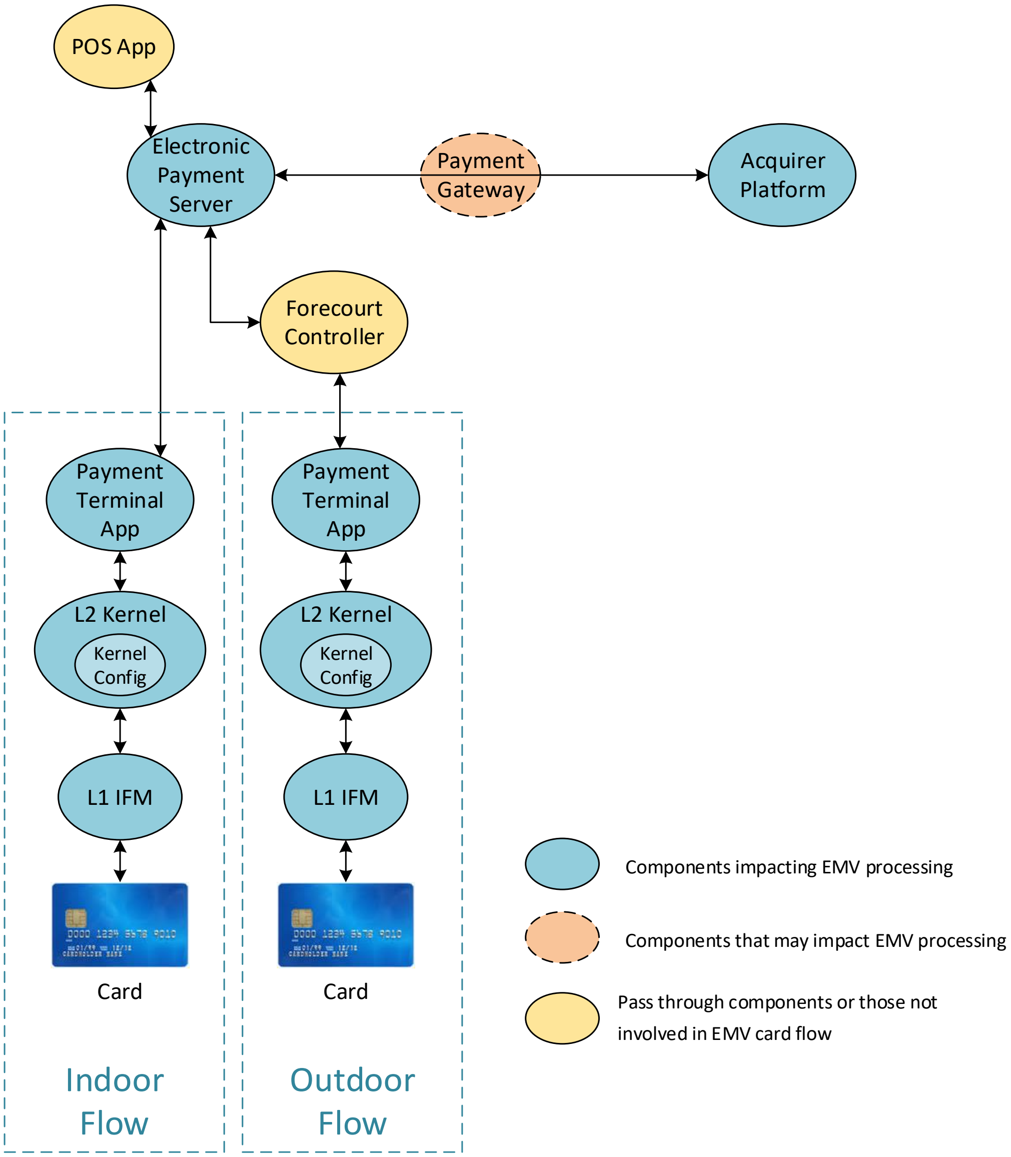

Figure 3. Petroleum Transaction Process Flow with Areas Impacted by EMV Migration

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 implementation manager.

DiscoverNetwork.com/chip-card

U.S. Payments Forum

U.S. Payments 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 U.S. Payments Forum Testing and Certification Working Committee to provide an educational resource on the global payment networks' EMV testing and certification requirements for U.S. payments industry stakeholders.

Publication of this document by the U.S. Payments Forum does not imply the endorsement of any of the member organizations of the Forum.

The V4.0 white paper update was developed with input from American Express, Discover, Mastercard and Visa.

The U.S. Payments 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 V4.0 white paper:

- **Berke Baydu,** Mastercard
- **Charl Botes**, Mastercard
- **Roberto Cardenas**, TSYS
- **Steve Cole,** Vantiv
- **Kevin Emery**, Discover
- **Cindy Kohler**, Visa
- **Alex Pierre,** Visa
- **Derek Ross,** ICC Solutions
- **Clyde L. Van Blarcum**, American Express

Trademark Notice

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

8. Appendix A: EMV Data Elements Impacting Terminal Testing

Table 3 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 the latest version of EMVCo Bulletin #11 available on www.emvco.com.

Table 3. 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		M	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 4 identifies the data for an authorization response.

Table 4. 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.

9. Appendix B: Optimizing Transaction Speed at the POS Certification and Testing Processes

Faster EMV processing has been defined by the payment networks under the names of Amex Quick Chip, Discover Quick Chip, M/Chip Fast, and Visa Quick Chip.

The chip processing solutions are specifically designed for environments where faster transaction times, in addition to security, are particularly important. It prioritizes the parts of the EMV transaction that provide protection against counterfeit fraud and omits certain other EMV features.

As with standard EMV, counterfeit protection is central to the Faster EMV transaction and is accomplished through the generation of a unique one-time cryptogram. Once this cryptogram has been generated by the card and delivered to the terminal, Faster EMV allows completion of EMV processing to be initiated, and the card can be removed from the reader. This improves the cardholder perception of the time it takes to complete the payment transaction.

Faster EMV solutions are defined as online-authorization-only processing scenarios (also referred to as "online-only"). By definition, EMV offline chip-based authorization[6] is not supported. Other options discussed in the U.S. Payments Forum white paper, "Merchant Processing during Communications Disruptions,"[7] still apply.

Currently, each payment brand has approved these Faster EMV solutions only for implementation in the U.S. American Express, Discover, and Mastercard do not permit Faster EMV processing at the ATM.

9.1 Implications for Testing and Certification

Faster EMV functions can be implemented without impacting the EMVCo Level 2 approval of the kernel.

For point-of-sale solutions that *have* been Level 3 EMV certified through the payment networks and wish to enable Faster EMV transactions, all payment networks have recommended regression test cases that can be performed internally to validate Faster EMV functionality. Additional Level 3 certification will not be required. American Express will provide an amendment to the existing American Express Letter of Approval (LOA) upon attestation that inclusion of Quick Chip was the only change made.

For new point-of-sale solutions that *have not* been Level 3 EMV certified through the payment networks, test plans have been updated to reflect Faster EMV acceptance when requested. For new certifications, all payment brands require a streamlined testing approach (subset of test cases) versus a standard full EMV certification. Refer to each payment network's current processes and programs for specifics on requirements.

[6] U.S. Payments Forum, "Merchant Processing during Communications Disruptions," April 2016, http://www.emv-connection.com/merchant-processing-during-communications-disruption/

[7] Ibid.

Table 5. Optimizing Transaction Speed at the POS Certification and Testing Requirements

Payment Network	**If Previously Certified Terminal Configuration**	**New Terminal Configurations**
American Express	Recommend regression testing	Complete subset of AEIPS end-to-end test cases
Discover	Recommend regression testing	Complete subset of D-PAS end-to-end test cases
Mastercard	Recommend regression testing	Require M/Chip Fast subset of M-TIP
Visa	Recommend regression testing	Complete subset of ADVT

Refer to each payment networks' existing processes and programs for review and reporting requirements.

Note: Any EMVCo approved Terminal Type value can be used as an U.S. online only configuration via a zero floor limit for Quick Chip and M/Chip Fast implementations. Testing requirements would be performed based on the implemented capabilities. Refer to the latest version of EMVCo Bulletin #11 for more details.

9.1 Optimizing Transaction Speed at the POS Certification and Testing Processes Frequently Asked Questions

This section provides clarification on some common testing examples in the field for Faster EMV (M/Chip Fast and Quick Chip) certification and testing requirements.

Q. What are the differences with generating a Quick Chip / M/Chip Fast Level 3 certification project compared to standard full EMV certification?

Since these implementations support online-only solutions, scripting and some offline EMV functionality are removed from the testing requirements depending on the payment network. There are fewer test cases to be executed across each of the payment networks.

Q. Is a standard full certification required if I move from Quick Chip / M/Chip Fast to standard EMV?

Yes. However, there is not a requirement to migrate to standard full EMV after implementing Quick Chip / M/Chip Fast. This will be determined based on business needs.

Q. Will Quick Chip / M/Chip Fast terminal configurations impact the kernel and increase the number of certifications due to the changes?

Faster EMV functions can be implemented without impacting the EMVCo Level 2 approval of the kernel.

Q. Can I certify Quick Chip / M/Chip Fast only?

Yes. You can develop and certify a Faster EMV solution only. For more details on different merchant verticals, refer to the "Optimizing Transaction Speed at the POS" white paper.[8]

[8] http://www.emv-connection.com/optimizing-transaction-speed-at-the-point-of-sale/

Q. Is there a requirement for Level 3 testing to certify standard full EMV prior to Quick Chip / M/Chip Fast?

No, there is not a requirement to certify standard full EMV prior to Quick Chip / M/Chip Fast. A terminal configuration can complete certification with each payment networks' subset of test cases for Quick Chip / M/Chip Fast configurations. Refer to each payment network for more details on their streamlined testing requirements.

Q. If there are no changes to the kernel, why is additional testing required for a previously certified terminal configuration?

Since there are minimal software changes, all payment networks have recommended that regression testing can be performed internally to validate Faster EMV functionality.

Q. Why did accredited test tools need to be updated to support Quick Chip / M/Chip Fast?

Chip tools required updates with each of the payment networks to remove unnecessary testing and align with the subset of test cases. Chip tools currently support all payment networks' specifications and testing requirements.

For more details on implementation, refer to the "Optimizing Transaction Speed at the POS" White Paper.[9]

[9] Ibid.

10. Appendix C: Contactless Certification and Testing Processes

This section provides clarification on contactless[10] testing and when to test use cases.

Q. I am implementing terminals which will support Near Field Communication (NFC) (e.g., dual-interface chip cards or mobile devices). Are there global payment network terminal testing requirements?

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

Q. Do global payment networks recognize terminal family for contactless EMV when the only difference is the antennae and reader size?

Yes, global payment network terminal testing requirements do not specifically test the performance of the contactless antennae or differences in reader size.

- Focus is 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, often the Level 2 kernel is identical.

A single contactless reader can be tested to cover the entire terminal family, sharing the same Level 2 kernel.

Consult with your terminal vendor to ensure a terminal falls within a terminal family. This approach allows a general reduction in the number of test iterations with negligible impact to the integrity of the testing process.

[10] A contactless payment is a payment transaction that does not require physical contact between a consumer's payment device and a point-of-sale terminal. The consumer holds a payment device (dual-interface chip card or a mobile device) in close proximity to the terminal (less than 1-2 in. away), and payment account information is transmitted wirelessly, over radio frequency (RF). The consumer's contactless payment device can assume a variety of form factors, including cards, Near Field Communication (NFC)-enabled smart phones, and wearables. Contactless transactions are cryptographically secure and generate a unique code for each transaction.

NFC is not a payment technology; it is a set of standards that enables proximity-based communication between consumer electronic devices and is compatible with the current contactless payment acceptance infrastructure. Each global payment network independently has its own specification. An NFC-compliant mobile device or card can communicate with a point-of-sale (POS) system that currently accepts contactless payment cards.

NFC and EMV are companion technologies. NFC applies to how devices communicate; EMV applies to payments made with contact and contactless chip cards or with a mobile NFC device emulating a contactless chip card. Contactless payment transactions made using mobile NFC devices or cards use the same infrastructure as contact and contactless EMV chip card transactions.

Additional information can be found in the Secure Technology Alliance Payments Council white paper, "Contactless Payments: Proposed Implementation Recommendations," available at http://www.securetechalliance.org.

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

When adding contactless EMV to a previously certified chip terminal, perform contact EMV regression testing and perform a new contactless EMV certification using the applicable payment network's chip tools.

Q. Is there benefit when adding contactless EMV to a POS solution that supports Faster EMV processing?

Yes, faster EMV at the POS solutions from payment networks support contactless EMV and can reduce scope of testing.

Q. Can I test contact and contactless EMV at the same time with an acquirer during Level 3 certification?

Yes, contactless EMV deployments can be accelerated by implementing contact and contactless EMV together which would be supported in one acquirer certification project.

Q. Can I test and deploy terminals that support contactless magnetic stripe data (MSD) only?

Yes, however, given the U.S. transition to EMV, some global payment networks may have requirements to migrate terminals to contactless EMV (which are considered more secure) if accepting contactless payments. Refer to each global payment network for more details on their requirements.

Q. My terminals support contactless magnetic stripe data (MSD) already. Do I need to perform certification to migrate to contactless EMV?

Yes, each global payment network has testing requirements to migrate terminals to contactless EMV, which are a part of their EMV terminal testing process. Refer to each global payment network for more details on their requirements.