Visa Smart Debit/Credit

Acquirer Device Validation Toolkit User Guide

Version 6.1.1

02 March 2015

Important Information on Confidentiality and Copyright

© 2014 Visa. All Rights Reserved. 2004-2014

Notice: This information is proprietary and CONFIDENTIAL to Visa. It is distributed to Visa participants for use exclusively in managing their Visa programs. It must not be duplicated, published, distributed or disclosed, in whole or in part, to merchants, cardholders or any other person without prior written permission from Visa.

The trademarks, logos, trade names and service marks, whether registered or unregistered (collectively the "Trademarks") are Trademarks owned by Visa. All other trademarks not attributed to Visa are the property of their respective owners.

Note: This document is not part of the Visa Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Rules, the Visa Rules shall govern and control.

Contents

Tables

Figures

Acquirer Device Validation Toolkit (ADVT) User Guide Introduction

This chapter provides the following information:

- Introduction to the Acquirer Device Validation Toolkit (ADVT) User Guide
- Contact Information
- Summary of Changes
- Disclaimer

Introduction

Visa Smart Debit/Credit (VSDC) provides a global chip-based payment service that allows clients to strategically and competitively position themselves for the future. The program is based on the underlying specifications developed by EMVCo LLC to ensure that all chip-based debit and credit cards can be accepted in any EMV chip reading terminal worldwide.

From an acquiring perspective, chip introduces additional features and complexities to the card acceptance process. During a chip-based transaction, the card and terminal proceed through a series of steps to determine the final outcome of the transaction. These steps require additional data and processing capabilities at the terminal level.

The interaction of cards issued in other countries and regions with a terminal deployed in a specific location can often result in acceptance issues, even though both the cards and terminals would have been EMV and Payment Scheme approved. These issues may often be the result of an incorrectly configured terminal, inadequate integration testing, or misunderstandings about EMV and Visa requirements.

To help ensure that the terminals acquirers are deploying do not unduly contribute to interoperability problems, Visa has developed the Acquirer Device Validation Toolkit—a set of test cards or simulated test cards and test cases to be used on new or upgraded EMV terminals to ensure correct terminal configuration, to assist with integration testing, and to ensure that Visa’s terminal requirements are being met.

In addition to ensuring card acceptance, these tests also enable the User Interface of live terminals to be tested. This is necessary to make sure that user prompts such as error messages, Application Selection menus, and PIN Entry messages are appropriate and readily comprehensible to the cardholder and merchant.

Contact Information

For more information on the ADVT, contact your Visa representative using the following email addresses according to your geographical location:

- Visa Inc.:
  - For copies of the ADVT, contact: STCVisaFulfillment@merrillcorp.com
  - For general information, contact: chiptoolkits@visa.com
- Visa Europe:
  - For copies and general information, contact: ADVTK_EU@visa.com

Visa Inc. consists of the following regions:

- Asia Pacific (AP)
- Canada
- Central Europe Middle East and Africa (CEMEA)
- Latin America
- United States (U.S.)

Visa Europe consists of the following countries and territories:

Andorra, Austria, Bear Island, Belgium, Bulgaria, Channel Islands, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faeroe Island, Finland, France (including its "DOM-TOMs"), Germany, Gibraltar, Greece, Greenland, Hungary, Iceland, Ireland, Isle of Man, Israel, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Vatican City, and the United Kingdom.

Summary of Changes to the Document Since Version 6.1 (Dated September 2014)

This section provides an overview of the changes made since the last publication.

For a summary of changes related to the test cards, refer to the Table 2: Summary of Changes to the Test Cards.

Table 1: Summary of Changes to the Document

Section	Change	Description
Section1.10 EMVco Brand-aligned Terminal Integration Testing Framework	New Section	Introduced to describe Visa's ADVT compliance plans with the EMVCo Terminal Integration Testing Framework.
Section 3.4 Test Case 4: Terminal Risk Management – Expected Results	Correction	Under the "Online-only Devices That Do Not Support Terminal Risk Management (TRM)" section, text replaced with "Not Applicable"
Section 3.5.1 Test Case 5: Application Selection – Expected Results, Terminal Scenario 3	Clarification	Second paragraph clarified to state that: "If a receipt is printed, the Visa AID must be on the receipt and it is strongly recommended that the Application Label (Visa Credit) be printed as well."
Section 3.8 Test Case 8: Fallback – Expected Results	Deletion	Note 3 deleted.
Section 3.17 Test Case 17: Magnetic Stripe Image – Expected Results - ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):	Correction	Second sentence of the first paragraph, change to: "The transaction must be **declined** online."
Section 3.21 Test Case 21: PIN Try Limit Exceeded (1) – Expected Results	Correction	Under the "Devices That Do Not Support Offline PIN" section, text replaced with "Not Applicable"
Section 3.22 Test Case 22: PIN Try Limit Exceeded (2) – Expected Results	Correction	Under the "Devices That Do Not Support Offline PIN" section, text replaced with "Not Applicable"

Section	Change	Description
Section 3.25 Test Case 25: No PAN Sequence Number – Expected Results – ADVT Online Testing	Clarification	Second paragraph clarified to indicate that: "Since the Application PAN Sequence Number is not present on the card, the acquirer may either exclude the field entirely from the request message or include it with all zeroes"
Section 3.27: Test Case 27: 1144-Bit Issuer Public Key – Expected Results	Correction	Under the "Devices That Do Not Support SDA" section, text replaced with "Not Applicable"
Appendix A (Visa CA Test Public Keys for VSDC)	Addition	Add a note in the second paragraph as follows: "**NOTE**: Expiration dates are not defined for test CA Public Keys, and it should not be assumed that a test key has the same expiry date as the live key of the same length. If your Terminal Management System requires expiry dates to be provided for CA PKs then please set the expiry date to 31 December 2025 for all test keys."

Summary of Changes to the Test Cards Since Version 6.1 (Dated September 2014)

This section provides an overview of the changes made to the test cards since the last publication.

Refer to the *ADVT Card Profiles* for details.

Table 2: Summary of Changes to the Test Cards

Change	Description
Card # 28	Conversion from support of Cryptogram Version Number 10 (hex '0A') to Cryptogram Version Number 18 (hex '12')
Card # 6, 11, 18 & 27	Corrections of minor personalization errors are defined in the "*Corrections and Clarifications within ADVT v6.1*" bulletin, dated February 5th, 2015.

ADVT Support Documentation

ADVT support documentation now consists of two documents: This user guide and the card profiles (the card profiles have been removed from this guide and placed in a separate document).

Table 3: ADVT Support Documentation

Document Name	Description	Audience
Acquirer Device Validation Toolkit User Guide (This Document)	This document provides: • An overview of the ADVT including a description of the components and usage criteria • Test cases • Appendices providing details of the Visa CA test keys, Terminal Action Code (TAC) values, VisaNet Stand-in (STIP) options, an overview of merchant terminal environments, and terminal testing use cases.	This document is primarily intended for users of the ADVT, including acquirers, processors, merchants, and third party service providers on behalf of acquirers.
Acquirer Device Validation Toolkit Card Profiles	This document provides the details required to personalize each of the ADVT test cards.	This document is intended for personalization bureaus and chip tool vendors responsible for developing ADVT test cards or simulated/scripted equivalents.

Disclaimer

The Acquirer Device Validation Toolkit described herein provides a means for a Visa Acquirer (or its agent) implementing a chip program to test their terminals before deployment. The tests prescribed herein do not supersede the requirement for the terminals to undergo type approval testing at an accredited EMVCo laboratory.

The Acquirer Device Validation Toolkit tests must be included in a Visa Acquirer's chip migration project plan as they provide additional testing and review methods that are particularly important after the terminal has been re-configured to suit the acquirer's requirements.

The Acquirer Device Validation Toolkit test cards and test cases are designed to determine whether the terminal can process certain card profiles that are known to cause acceptance issues. Visa reserves the right to add or remove tests and test requirements in its sole discretion.

The Acquirer Device Validation Toolkit is provided as a service to Acquirers to help reduce card acceptance problems. Visa does not warrant the Toolkit or any Toolkit test results for any purpose whatsoever, and expressly disclaims any and all warranties relating to the Toolkit. No vendor or other third party may refer to a product, service or facility as "Visa-approved", nor otherwise state or imply that Visa has, in whole or part, approved any aspect of a vendor or its products, services or facilities, except to extent and subject to the terms and restrictions expressly set forth in a written agreement with Visa or in an approval letter provided by Visa. All other references to "Visa approval" are strictly prohibited by Visa.

All references to Visa operating regulations in this document are deemed to be references to both *Visa International Operating Regulations* and/or *Visa Europe Operating Regulations*, as appropriate.

1 Acquirer Device Validation Toolkit User Guide Overview

This section provides an overview of the Acquirer Device Validation Toolkit and its associated User Guide (this document).

1.1 Objective

The objective of this document is to define a toolkit that provides Visa acquirers with a high level of confidence that the chip terminals they are deploying will not unduly contribute to interoperability problems.

1.2 Audience

The audience for this document is Visa acquirers, their agent(s), and third-party service providers responsible for deploying terminals in their marketplace that accept Visa Smart Debit/Credit (VSDC) cards. It shall not be shared with or distributed to any other parties.

The term *acquirer* in this document is used generically to represent the entity in the marketplace responsible for terminal deployment. Depending on the marketplace, it could represent the acquirer, acquirer processor, merchant, or a third party service provider on behalf of an acquirer or merchant.

1.3 Document Organization

This document contains the following chapters:

Table 1–1: Document Organization

Chapter	Description
ADVT User Guide Introduction	This chapter provides background information highlighting the need for the ADVT. It also includes: • Contact Information • Summary of Changes • Disclaimer
Chapter 1: ADVT User Guide Overview	This chapter provides an overview of the document including objective, audience, document organization, components, usage, scope, and related documents.

Chapter	Description
Chapter 2: Test Cases Introduction	This chapter provides an introduction to the test cases. It includes pre-requisites that need to be in place before testing can begin as well as instructions for performing ADVT tests.
Chapter 3: Test Cases	This chapter outlines each ADVT test case, its associated test card, objective, business justification, applicable terminal device type, document reference, and pass criteria/user validation.
Appendix A: Visa Certificate Authority (CA) Public Test Keys for Visa Smart Debit Credit (VSDC)	This appendix provides the VSDC public test keys that need to be loaded into the terminal to support the tests associated with Offline Data Authentication (ODA) and Offline Enciphered PIN.
Appendix B: Terminal Action Code (TAC) Settings	This appendix outlines the Terminal Action Codes (TACs) that need to be configured in the terminal to be in compliance with Visa rules.
Appendix C: VSDC Stand-in Processing Conditions	This appendix provides the VSDC Stand-in processing conditions that can be used to provide valuable insight into the reason that VisaNet Certification Management Service (VCMS)/Visa Member Test System (VMTS) either approved or declined an online-initiated transaction.
Appendix D: Merchant Terminal Infrastructures	This appendix provides an overview of some of the most commonly configured terminal infrastructures at the merchant level.
Appendix E: ADVT Testing Use Cases	This appendix provides use cases in a Questions & Answers format that address commonly asked questions related to ADVT usage.
Appendix F: Acronyms	This appendix provides a list of commonly used acronyms in this User Guide and in the EMV environment.

1.4 ADVT Components

The ADVT consists of:

- **Test Cards or Test Card Simulators**—Cards or simulators personalized with specific settings that are intended to identify incorrectly coded or configured chip card acceptance devices.
- **Documentation**—Two documents:
  - **ADVT User Guide (This Document)**—A document that outlines each test case, a description of the test card to be used with each test case, and the expected test results. This document is used by the acquirer or acquirer's agent to perform testing.
  - **ADVT Card Profiles Definitions (Separate Document)**—A document that outlines the card personalization requirements for each test card that can be used by card personalization bureaus and card simulator vendors to personalize the physical test cards or to develop simulated test card scripts.

Acquirers may obtain additional ADVTs (including test cards) from their Visa representative. Refer to the Contact Information section in the ADVT User Guide Introduction chapter for details.

1.5 ADVT Usage

Important: An acquirer must utilize the ADVT before deploying a new chip card acceptance device or after performing significant upgrades to an existing device.

As described in the *Visa Core Rules and Visa Product and Service Rules (*formerly *Visa International Operating Regulations)* and the *Visa Europe Operating Regulations*, an acquirer that fails to utilize the ADVT on a device that later causes a chip interoperability issue, may be subject to fines and penalties as defined in the Visa Chip Interoperability Compliance Program.

Note: There is no Visa requirement that ADVT testing must be conducted for each merchant location; however, testing is required for each unique terminal configuration.

Acquirers are required to use the ADVT before initial terminal deployment (including all variations of hardware, software, and parameter settings) to ensure that the terminal has been set up and configured correctly. It is expected that acquirers will run each applicable test to gain the full benefit of the ADVT. When a test result does not match the required outcome (“Expected Results”) of the test, it is anticipated that the acquirer will work with its technical support team (and Visa, if necessary) to correct the problem. The acquirer will continue to perform the test until the problem is resolved and the acquirer’s result matches the Expected Results.

In addition, since new versions of the ADVT are periodically released by Visa, it is always good practice for acquirers to use the most recent version on terminals already deployed in the field. This helps to further minimize potential acceptance problems with those previously deployed terminals.

1.5.1 ADVT Usage Guidelines

This section outlines the scenarios where ADVT usage is:

- Required
- Recommended
- Not Required

Where ADVT usage is required, the latest version of the ADVT shall always be used. If this is not possible due to upgrade schedules, etc., ADVT users must consult with their Visa representative to determine regional policies regarding proposed use of an earlier version of the ADVT.

Note: If the device integrator wishes to see the ADVT test results recognized in multiple regions, they will need to submit a request to Visa. Granting the request is at the sole discretion of Visa, and may not be allowed under regional policies. If the request is accepted, the compliance report will be accessible via Chip Compliance Reporting Tool (CCRT). For information on CCRT, refer to Section 2.2.13: Chip Compliance Reporting Tool.

Refer to Appendix E: ADVT Testing Use Cases for further information.

1.5.1.1 ADVT Usage: Required

This section outlines scenarios where use of the ADVT is required:

- **New Device**—Deployment of a new EMV card accepting device containing any of the following:
  - New EMV kernel
  - New version of payment application
  - New terminal-to-host message protocol
- **Modified Device**—Modification or reconfiguration of an existing device to make any of the following changes:
  - Major changes to the EMV-approved kernel (as defined in EMV Bulletin 11 available on www.emvco.com)
  - Changes to the payment component of the terminal application, affecting EMV processing
  - Changes to the Cardholder Verification Method (CVM) capabilities
- **Merchant/Acquirer Network Architecture Change**—Changes to a merchant's or acquirer's network architecture. For example, in a case where a merchant has switched acquirers, even though their terminal configuration might remain the same.
- **New Terminal Hardware Model**—Introduction of a new model[1] of terminal hardware.
- **Dynamic Currency Conversion**—Introduction of Dynamic Currency Conversion (DCC) functionality.
- **Cash-Back**—Addition of cash-back functionality.
- **Visa Request**—As requested by Visa based on evidence of an acceptance or interoperability problem affecting the device or connectivity to VisaNet.

1.5.1.2 ADVT Usage: Recommended

This section outlines scenarios where use of the ADVT is recommended:

- **Acceptance/Interoperability Problem**—A strong suspicion by Visa or an acquirer of the presence of an acceptance or interoperability problem affecting the device or connectivity to VisaNet.
- **Minor Modifications**—Minor modifications or reconfiguration of existing terminals for any of the following:
  - Change of Language Support
  - New communications interface (e.g., from dial-up to high-speed)

[1] It is possible to have "families" of terminals which are identical from a payment point of view. Here a new "model" is taken to mean a change which may affect card acceptance. This includes the user interface presented to either the cardholder or merchant.

- Upgrades or modifications to the acquirer host systems which affect the transmission of chip data (at a minimum, the ADVT online tests must be performed on at least one EMV chip-reading device; refer to Section 2.2.10: ADVT Online Testing for further information)

1.5.1.3 ADVT Usage: Not Required

This section outlines scenarios where use of the ADVT is **not** required:

- **Terminal in Same Family**—On individual terminals that all fall within the same terminal family (e.g., payment application, EMV kernel, and chip transaction flows are all the same). Consult with your terminal supplier to verify that the terminals fall within the same terminal family.
  Note: Third party processors implementing "terminals in the same family" for different clients within the same country or for different clients in a different country are not required to use the ADVT on these devices.
- **Currency Code/Country Code Change**—Change of supported Currency Code/Country Code on the same acquirer host platform. If on a different host platform or different protocol, testing is required.
- **Minor EMV Kernel Changes**—Minor changes to the EMV-approved kernel (as defined in EMV Bulletin 11 available on www.emvco.com).
  Note: Replacing the Interface Modules (IFM) with another approved module is defined as a minor change.
- **Non-Payment Processing Software Change**—Change to software that does not affect payment processing (e.g., screen layout and report generation on a POS terminal, advertising graphics on an ATM).
- **New Peripheral Device**—Addition of a new peripheral device not requiring changes to the existing code (e.g., a new printer or cash dispenser module).
- **Online PIN-Only PIN Entry Device (PED)**—Addition of a new Online PIN-only PED.
- **Terminal-to-Host Message Protocol Change**—Change to the terminal-to-host message protocol which does not affect authorization messages.
- **CA Public Key Change**—Change to CA Public Keys used for Offline Data Authentication (ADVT testing does not use production keys).
- **New Version of ADVT**—Introduction of a new version of ADVT by Visa provided the device has already undergone successful validation using an earlier version of ADVT in accordance with these guidelines.

1.6 New ADVT Version

On release of a new version of the ADVT, acquirers will be given a six month grace period to upgrade to the new version. During this grace period, testing will still be allowed with their existing version of the ADVT. However, on expiration of the grace period, it is expected that acquirers will have completed their upgrade to the latest version of the ADVT and results from earlier versions will no longer be accepted.

Some Visa regional offices, however, may apply more stringent policies governing the period by which earlier versions of the ADVT must be phased out and replaced by the most recent version. Contact your Visa representative for details.

1.7 Scope of ADVT Testing

This section outlines the scope of ADVT testing comparing it to both acquirer host certification and EMV-Level 2 testing.

Table 1–2: Scope of ADVT Testing

Within Scope	Out of Scope	Explanation
Terminal Testing	Acquirer Host Certification	The ADVT focuses on helping to ensure terminals deployed in the field are configured in a way that promotes the best potential for global interoperability. While some of the cards in the ADVT are to be used for online testing, the ADVT is not specifically designated as a host certification toolkit. Acquirers will continue to perform host system certification using current procedures. Contact your Visa representative to obtain the requirements for acquirer host certification.
Complement to EMV Level 2 Testing	Replacement of EMV Level 2 Testing	It is assumed that acquirers and/or terminal vendors will perform these tests on terminals that have already passed EMV Level 1 and Level 2 testing. ADVT complements EMV testing to ensure that terminals have been configured correctly prior to deployment.

1.8 Future Enhancements

The ADVT may be expanded in the future to include additional device and/or online tests.

1.9 Related Documents

This section lists documents that may be read and/or referred to in conjunction with this document:

- Europay, MasterCard, Visa (EMV) (latest version)
- Visa Core Rules and Visa Product and Service Rules (formerly Visa International Operating Regulations) (latest version)
- Visa Europe Operating Regulations (latest version)
- Transaction Acceptance Device Requirements (TADR)—Requirements (latest version)
- Transaction Acceptance Device Guide (TADG)—Requirements and Best Practices (latest version)
- EMV Brand-aligned Terminal Integration Testing Framework (latest version)

1.10 EMVCo Brand-aligned Terminal Integration Testing Framework compliance

Visa, in collaboration with the five other EMVCo member payment organizations, has agreed upon compliance with the recently published *EMVCo Brand-aligned Terminal Integration Testing Framework*. This Framework was developed by the EMVCo Terminal Integration Task Force (TITF) - established by EMVCo in September 2013 for the purpose of examining the various payment systems' (Brands) testing processes for the integration of EMV contact and contactless acceptance devices into their payment environments. The Framework defines the areas within the respective Brands integration testing processes where agreement was reached on aligning of key elements, along with a plan for implementation.

The main impacts of the TITF Framework on Visa's ADVT process, specifically as being introduced in this version of the User Guide, will be on the Test Case definitions in Section 3.

For more information on the EMVCo Terminal Integration Task Force's (TITF) efforts or to download the Framework document, please visit the EMVCo website as follows:
http://www.emvco.com/approvals.aspx?id=272

2 Test Cases Introduction

This chapter provides an introduction to the test cases. It includes pre-requisites that need to be in place before testing can begin as well as instructions for performing ADVT tests.

2.1 Pre-requisites

Prior to running the ADVT test cases, acquirers must ensure that the prerequisites in this section are fulfilled.

2.1.1 Terminal Capabilities

Before beginning any of the tests, it is important to understand the capabilities of your terminal. This will help you ensure you are performing the tests correctly for your specific device.

- **Terminal Type**—Determine if your terminal is an Automated Teller Machine (ATM) machine, stand-alone Point of Sale (POS) device, integrated POS device, or Cardholder Activated Terminal (i.e., an unattended device).
- **Cardholder Verification Methods**—Determine the Cardholder Verification Methods that your terminal supports: Online Personal Identification Number (PIN), Offline Enciphered PIN, Offline Plaintext PIN, Signature, No CVM Required (this CVM allows you to accept a card without any verification of the cardholder). This is important since the expected results associated with some of the tests is specific to the Cardholder Verification Method.
- **Offline Data Authentication**—Determine if your terminal supports Static Data Authentication (SDA), Dynamic Data Authentication (DDA), and/or Combined Dynamic Data Authentication/Generate Application Cryptogram (CDA). This is important since the expected results associated with some of the tests is specific to Offline Data Authentication.
- **Floor Limit**—Determine the floor limit of your terminal. For devices with a floor limit, always use an amount below the floor limit during testing unless the test case description specifically states that it must go online.

2.1.2 Terminal Log

It is very useful to the testing process for the terminal to have the ability to make the values of certain data objects (such as the Terminal Verification Results (TVR) and Transaction Status Information (TSI)) generated during the transaction available to the tester. This could take the form of a log file or some means of printing this information on a receipt or displaying it on the screen. In some cases, a log produced through online interaction with a host can be used.

2.1.3 Visa CA Test Public Keys

During use of the ADVT, terminals that support offline functionality (e.g., Offline Data Authentication, Offline Enciphered PIN) must be configured with the Visa CA Test Public Keys. These test keys are located in Appendix A: Visa CA Test Public Keys for VSDC.

Important: Prior to terminal deployment, the acquirer must ensure that the Visa CA Test Public Keys are removed from the terminals and the production Visa CA Public Keys are installed.

2.1.4 Terminal Action Codes (TACs)

Visa supports one set of TACs for acquirers. The TACs must be loaded into the terminal and acquirers must ensure that the TAC settings are correct. The TAC settings are provided in Appendix B: TAC Settings. See also, *Transaction Acceptance Device Requirements* (latest version).

2.1.5 Configured for Operational Use

The terminals must be configured for operational use. For example, the terminal must include the Visa Application Identifiers (AIDs) (for Visa Credit/Debit and Visa Electron, where appropriate), terminal country code, correct date/time, and floor limits.

2.1.6 EMVCo Level 1 and 2 Approval

Prior to deployment, terminals must have passed the EMVCo Level 1 and Level 2 approval process.

2.2 Instructions

This section provides instructions for using the ADVT.

2.2.1 Mandatory vs. Conditional Test Cases

ADVT 6.1 contains 29 test cases.

Important: All devices must perform **all** ADVT test cases except for the following:

Test Case	Test Case Description	Requirement
4	Terminal Risk Management	Only applicable to devices that support Terminal Risk Management
8	Fallback	Only applicable to devices that support fallback

Test Case	Test Case Description	Requirement
19	Plus and Interlink	Only applicable to devices that support Plus and/or Interlink
20	Visa Electron	Only applicable to devices that support Visa Electron
21	PIN Try Limit Exceeded 1	Only applicable to devices that support Offline PIN
22	PIN Try Limit Exceeded 2	Only applicable to devices that support Offline PIN
27	1144-Bit Issuer Public Key	Only applicable to devices that support SDA

Important: Although all test cases (except 8, 19, and 20) are mandatory for all devices, the expected results may differ based on the device's capabilities. For example, for a test that focuses on Combined DDA/AC Generation (CDA) (Test Case 10), the expected results differs based on whether the device supports CDA:

- **Devices Supporting CDA**—Must successfully perform CDA.
- **Devices that do not Support CDA**—CDA is not applicable but the device must perform a complete transaction without any errors. This ensures that even though the device does not support CDA, a card with CDA does not pose any acceptance problems for the device.

2.2.2 Self-Administered Tool

The ADVT is a self-administered tool. Users must work to fix the problems on their own whenever possible and only use Visa assistance for problems that cannot be resolved between the terminal vendor and the acquirer's technical team.

2.2.3 Initially Deployed Terminals

For terminals being initially deployed, the intent is for acquirers to run each applicable test and make modifications to the terminal configuration until the terminal meets the expected results of the test. Acquirers need to run these tests on each terminal type as well as each terminal hardware and/or software configuration.

After running all tests and making the appropriate terminal configuration modifications, acquirers need to submit their results to Visa in accordance with the information outlined in Section 2.2.13: Chip Compliance Reporting Tool.

See "For Information Gathering Purposes Only Tests" for the test scenarios that do not require acquirer action.

2.2.4 Previously Deployed Terminals

If there is a need to perform ADVT testing on terminals that have already been deployed, acquirers should run all relevant tests, gather the results, and report them to Visa in accordance with the information outlined in Section 2.2.13: Chip Compliance Reporting Tool.

2.2.5 For Information Gathering Purposes Only Tests

Occasionally, select test cases in the ADVT may be defined as “for information gathering purposes only.” If a terminal fails any of these tests, acquirer action to resolve the issue is not always necessary.

However, there may be some instances where Visa strongly recommends an update to the terminal to comply with the test case. Oftentimes, this is because the functionality, although currently optional, may later become mandatory; in all cases, the acquirer must submit the test result to Visa.

2.2.6 Changes to Terminals

If changes are made to terminal configuration or settings, the acquirer/tester must re-run the ADVT tests as described in Section 1.5.1: ADVT Usage Guidelines.

2.2.7 Decline Responses vs. Other Errors

A decline response is different from an error message. In some cases, a decline response by the terminal is an acceptable outcome of the test case. Error messages, where the terminal is unable to complete the transaction (e.g., unable to perform a complete EMV transaction from Application Selection to Completion), are generally unacceptable and can indicate a problem with the terminal or an incorrect terminal setting/configuration. Testers should not be alarmed if decline responses occur (as long as a decline is allowed in the expected results) but must investigate error messages (such as “Card Error” and “Not Accepted” or the equivalent). For further information on these error messages, refer to EMV 4.3, Book 4 - Section 11.2: Standard Messages.

2.2.8 Transaction Amount

For terminals with offline authorization capability, it is recommended to enter an amount below the floor limit. Where the test requires an online transaction, an amount above the floor limit should be entered.

2.2.9 PIN-Based Transactions

For Offline or Online PIN, a PIN value of ‘1234’ must be used, except for Test Case 13 which uses a PIN of ‘123412’.

Note: When PIN is used for the transaction, the signature line does not need to be printed on the receipt (if applicable) nor obtained from the cardholder (unless the combination CVM of Offline PIN and signature applies).

2.2.10 ADVT Online Testing

In this version of the ADVT, 10 test cases (1, 2, 3, 13, 17, 19, 24, 25, 26, 28) are designated for online testing. These tests are identified in Table 2-1: Test Case Summary and in Chapter 3: Test Cases.

This section outlines the requirements for ADVT Online Testing:

- **Devices**—All online-capable devices must perform these tests. This includes:
  - POS devices that support both offline and online transactions
  - Zero floor limit POS devices
  - ATMs
- **Connection to VCMS/VMTS/Test-Host Simulator**—Online-capable devices must connect their device to their test host system and generate transactions through one of the following:
  - VisaNet Certification Management Service (VCMS) (for Visa Inc. clients)
  - Visa Member Test System (VMTS) (for Visa Europe clients)
  - Visa-confirmed third party supplied test-host simulator which mimics VCMS/VMTS (refer to Section 2.2.12: Simulators for information on third party test-host simulators)
- **Online Card Authentication**—Online Card Authentication (i.e., ARQC validation) must be performed and be successful (Field 44.8 = 2) (except Test Case 17 where the card has a proprietary cryptogram version).
- **Retrieval Reference Number (RRN)/Host Logs**—Additional requirements for ADVT online testing (such as providing an RRN or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via the Chip Compliance Reporting Tool. For information on CCRT, refer to Section 2.2.13: Chip Compliance Reporting Tool (CCRT).

To help you determine the reason VCMS/VMTS (or the third party test host simulator) approved/declined the online transaction, refer to Appendix C: VSDC Stand-in Processing Conditions.

Note: Access to VCMS or VMTS is provided to Visa clients only.

Important: Online-only devices (such as ATMs and U.S. POS devices) must perform the ADVT Online Testing test cases in addition to all mandatory test cases.

2.2.11 Test Cards

If physical test cards are being used to perform ADVT testing, acquirers must use the applicable test card provided to run the test case. For convenience, one card is used for each test case with the test card number matching the test case number (i.e., for Test Case 1, the acquirer will use Test Card 1).

2.2.12 Simulators

Simulators are available to support ADVT testing:

- **Card Simulators**—As an alternative to using the physical test cards, acquirer can use a Visa-confirmed third-party vendor supplied card simulator for ADVT testing. Acquirers must execute each applicable simulated script to run the test cases. Typically, a single script is used for each test case with the script number matching the test case number (i.e., for Test Case 1, the acquirer will use simulated card script 1).
- **Test-Host Simulator**—As an alternative to connecting to VCMS or VMTS for online testing, acquirers can connect to a Visa-confirmed third party supplied test tool which mimics VCMS/VMTS.
    - **Important:** To allow Visa to review the tests performed with host simulators, acquirers using these simulators must provide Visa with the host simulator's log of each ADVT online test. For a list of the ADVT online test cases, refer to Section 2.2.11: ADVT Online Testing. Acquirers submit the logs to Visa via the Chip Compliance Reporting Tool (CCRT). Refer to Section 2.2.13 for more information on CCRT.

A list of available Visa-confirmed ADVT card and test-host simulators is posted on the Visa Technology Partner website under the Product Toolkits section in the document *Visa Confirmed Third-Party Chip Tool Suppliers:* https://technologypartner.visa.com/Toolkits/

Note: For entities using card simulators, a simulator may not behave in exactly the same manner as the physical test cards (for example, the CVR bit settings may not represent the disposition of the previous transactions). However, this has no effect on test case results. Where a host simulator is used, RRN values will not be available.

2.2.13 Chip Compliance Reporting Tool (CCRT)

Once the ADVT test cases have been completed, acquirers need to submit the results to Visa using the Chip Compliance Reporting Tool (CCRT). CCRT is a web-based tool that allows chip acquirers or their processors to complete and submit the mandatory compliance reports via a global automated online system. Hosted on Visa Online (VOL), CCRT is designed in accordance with Visa's three-tiered architectural requirements and provides a high-level of application and data security.

CCRT allows users to:

- Submit new compliance reports.
- Submit logs when using test-host simulators.
- Review and update draft reports.
- Check on the status of pending reports submitted to Visa.
- Track approved reports.
- Upload reports as XML files generated by test tools (thus avoiding the need to retype report details).

It benefits users by:

- Providing a convenient and secure online solution for ADVT results reporting.
- Reducing potential for errors in manual entry by guiding users to choose from applicable options and providing mandatory information requirements.
- Allowing the "re-use" of reports as a starting point for new reporting, reducing time spent completing the reports.
- Supporting online status review and automated management of reports submitted to Visa, expediting communication between Visa and clients.

For more details on CCRT, contact your Visa representative.

2.3 Test Case Summary

The following table provides:

- **Description**—A brief description of each test case.
- **Mandatory vs. Conditional**—Whether the test case is mandatory or conditional (refer to Section 2.2.1: Mandatory vs. Conditional Test Cases for more information).
- **ADVT Online Testing**—Whether the test case is part of ADVT Online Testing (refer to Section 2.2.10: ADVT Online Testing for more information).

Important:

- Mandatory test cases must be performed by all devices.
- Mandatory test cases may have an ADVT Online Testing component:
  - **Online-Capable Devices**—ADVT Online Testing requirements must be fulfilled by all online-capable devices.
  - **Offline-Only Devices**—ADVT Online Testing requirements are **not** applicable to offline-only devices.

Table 2–1: Test Case Summary

Test Card Number	Test Case Description	Mandatory vs. Conditional (M/C)	ADVT Online Testing
1	**Basic VSDC**—Basic VSDC card personalized with a unique Primary Account Number (PAN) and the card is personalized to require successful Issuer Authentication on online transactions.	M	✓
2	**19-Digit PAN**—Card personalized with a 19-digit PAN.	M	✓
3	**T=1, DDA, OEP, and Issuer Authentication**—Card supports the T=1 protocol and is personalized to support the following: • Dynamic Data Authentication (DDA) with an 1024-bit ICC key • Offline Enciphered PIN (OEP) • Requires successful Issuer Authentication on online transactions	M	✓
4	**Terminal Risk Management**—Card personalized without Terminal Risk Management and configured to decline when the Terminal Floor Limit is Exceeded.	M	

Test Card Number	Test Case Description	Mandatory vs. Conditional (M/C)	ADVT Online Testing
5	**Application Selection**—Multi-application card containing five applications, each with a unique suffix and an Application Preferred Name containing non-ASCII characters. The first three applications are intentionally expired to trigger an offline decline, and Applications four and five both have a unique PAN for transaction identification.	M	
6	**Dual Interface**—Dual interface card supporting the following: • **Contact Interface:** An extended length Processing Options Data Object List (PDOL) (45 bytes) and Language Preferences (Japanese, Korean, and Chinese) supported • **Contactless Interface:** Supporting both MSD and qVSDC (CVN 10) contactless transactions	M	
7	**Terminal Action Codes**—Test ensures the Terminal Action Codes (TACs) are correctly set up in the terminal.	M	
8	**Fallback**—Card created to allow magnetic stripe fallback testing on a faulty chip.	C (only applicable to devices that support fallback)	
9	**"Reserved For Future Use" CVM**—Card contains an unrecognized method code in the CVM List ('Reserved for Future Use') with instructions to apply the next CVM when the CVM fails.	M	
10	**CDA**—Card supporting Combined DDA/AC Generation (CDA).	M	
11	**Multiple Applications**—Dual interface card supporting the following: • **Contact Interface**—Three payment applications; First with unknown Application ID, second with a blocked application, and the third with a valid application • **Contactless Interface**—Supporting both MSD and qVSDC (CVN 17) contactless transactions	M	
12	**Geographic Restrictions**—Card is restricted to domestic transactions through the use of the card's internal Geographic Restrictions feature.	M	

Test Card Number	Test Case Description	Mandatory vs. Conditional (M/C)	ADVT Online Testing
13	**Proprietary Data and 6-digit PIN**—Card contains: • PSE and has proprietary tag data within the PSE • Proprietary data within the application • 6-digit PIN	M	✓
14	**Long PDOL and Unrecognized Tag**—Card requests a long string of data (0x64 bytes) and an unrecognized tag in Processing Options Data Object List (PDOL).	M	
15	**Data Element with 2-Byte Length Field**—Card with a record length of 2 bytes (Issuer Public Key Certificate). As a negative test, it also contains a data element (Issuer Public Key Remainder) where its length is zero bytes.	M	
16	**Two Applications and Cardholder Confirmation**—Card contains two applications: • **Visa Credit:** Requires cardholder confirmation • **Visa Debit:** Does not require cardholder confirmation	M	
17	**Magnetic Stripe Image**—Card supports the minimum set of VSDC data elements (Magnetic Stripe Image) and a Cryptogram Version Number of 12.	M	✓
18	**T=1 and DDA with 1984 Certificate**—Card supports the T=1 protocol and contains an Issuer Public Key Certificate signed by Visa's 1984-bit CA test key.	M	
19	**Plus and Visa Interlink**—Card containing the following: • Visa RID (A00000003) with the Plus PIX (8010) and a suffix of '01' • Visa RID (A00000003) with the Interlink PIX (3010)	C (only applicable to devices that support Plus and/or Interlink)	✓
20	**Visa Electron**—Card is a Visa Electron card with a unusable magnetic stripe.	C (only applicable to devices that support Visa Electron)	
21	**PIN Try Limit Exceeded (1)**—Card contains a CVM List with Offline PIN as the first method in the list. The PIN Try Limit is exceeded and the CVM List provides instructions to apply the next CVM (signature) when the first CVM fails.	M	

Test Card Number	Test Case Description	Mandatory vs. Conditional (M/C)	ADVT Online Testing
22	**PIN Try Limit Exceeded (2)**—Card contains a CVM List with Offline PIN as the first method in the list. The PIN Try Limit is exceeded and the CVM List provides instructions to fail cardholder verification and stop CVM processing when the first CVM fails. The Issuer Action Codes (IACs) require an offline decline when the PIN Try Limit is exceeded.	M	
23	**Combination CVM and Visa Fleet Chip**—Card contains: • CVM List where the first CVM is the combination CVM of Signature and Offline PIN • Visa Fleet Chip (VFC) feature to ensure cards with this feature can be accepted at standard EMV devices	M	
24	**Account Number with Padded Fs**—Card with a 16-digit account number padded with hexadecimal "F's" up to a maximum account number length.	M	✓
25	**No PAN Sequence Number**—Card without a PAN Sequence Number.	M	✓
26	**PAN Sequence Number of 11**—Card with a PAN Sequence Number of 11.	M	✓
27	**1144-Bit Issuer Public Key**—Card with an Issuer Public Key Certificate based on an 1144-bit Issuer Public Key.	M	
28	**Multiple Features**—Card contains a PSE, with an issuer URL in both the PSE and application data, extra Issuer Application Data in tag 9F 10, an Application Expiration Date of December 31, 2025, a CVM List which does not contain Signature, and Cryptogram Version Number 18 (hex '12).	M	✓
29	**Blocked Card**—Card that is blocked from use.	M	

3 Test Cases

This chapter outlines each ADVT test case.

Important: Prior to beginning the tests, be sure to read the following sections:

- Section 2.1: Pre-requisites
- Section 2.2: Instructions
  (especially Section 2.2.1: Mandatory and Conditional Test Cases and
  Section 2.2.10: ADVT Online Testing)
- Section 2.3: Test Case Summary

These sections contain critical information.

The following information is provided with each test case:

- **Test Case Number**—The number of the test case.
- **Test Case Name**—The name of the test case.
- **Objective**—The objective of the test case.
- **Regional Requirement**—Whether the test applies to all regions or is specific to sub-set of regions. (Currently, all of the tests apply to all regions).
- **Business Justification**—The business reason for the test.
- **Pre-requisite**—Any specific terminal conditions that apply or configuration requirements needed for the test case.
- **Applicable Terminal Device Type**—Indicates the device type that needs to be tested.
- **Applicable Terminal Interface**—Indicates the interface type that needs to be tested.
- **Test Card**—A number used to uniquely identify the test card required to execute the test. There is a one-to-one correlation between the Test Case Number and the Test Card Number (i.e., Test Case 1 uses Test Card 1).
- **Test Evidence to be submitted**—Evidence to be submitted with results on completion of the test case.
- **Document Reference**—References to the specification or rule that acquirers may refer to for background information on the test. This information is especially important in the event that the test fails.
- **Pass Criteria/User Validation**—The success/failure criteria for the test.

3.1 Test Case 1: Basic VSDC

Test Case 1/Test Card 1 (Mandatory; ADVT Online Testing)	
Test Case Number:	1
Test Case Name:	Basic VSDC
Objective:	To ensure acceptance of a basic VSDC card. This card contains the most commonly used VSDC features. It is personalized to require successful Issuer Authentication on online transactions. **Note:** This is a T=0 test card that is personalized without the Payment System Environment (PSE). If the terminal has difficulty with this test, ensure your terminal can accept cards supporting the T=0 protocol and personalized without the PSE. **Note:** Card contains an Application Label of "Visa Credit" and an Application Preferred Name of "Credito de Visa."
Regional Requirement:	Mandatory All Regions ADVT Online Testing Required (see part 1d)
Business Justification:	This represents a card containing some of the most commonly used VSDC features. For this reason, it is important to ensure universal acceptance of this card.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	1
Test Evidence to be Submitted:	☒Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	EMV 4.3, Book 1, Section 12.3.2: Using the Payment Systems Environment Transaction Acceptance Device Requirements
Pass Criteria/User Validation	This test has four parts (1a-1d). Complete the parts that apply to your device as follows: • 1a: All Devices • 1b: Devices that have separate insertion areas for chip and magnetic stripe • 1c: Non-Zero Floor Limit Devices (i.e., devices that have a floor limit) • 1d: ADVT Online Testing (for online-capable and online-only devices) **Important:** Please ensure that all applicable cases 1a-d are performed as separate, consecutive transactions.

Test Case 1/Test Card 1 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**1a) All Devices:** **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test. Devices Supporting Offline Data Authentication: For devices supporting SDA, the device log must show that: • Transaction Status Information (TSI), byte 1, bit 8 = 1 (Offline Data Authentication was performed) • TVR, byte 1, bit 8 = 0 (Offline Data Authentication was performed) • TVR, byte 1, bit 7 = 0 (SDA did not fail) Application Name and Receipt Requirements: • If the application name is displayed and the device supports the Issuer Code Table Index of 01, the device must display the Application Preferred Name of Credito de Visa. For these devices, the Visa AID (A0000000031010) must be printed on the receipt and it is strongly recommended that the Application Preferred Name (Credito de Visa) also be printed on the receipt. • If the application name is displayed and the device does not support the Issuer Code Table Index of 01, the Application Label of Visa Credit must be displayed. For these devices, the Visa AID (A0000000031010) must be printed on the receipt and it is strongly recommended that the Application Label (Visa Credit) also be printed on the receipt. **Note:** It is a Visa Best Practice to print the application name (either Application Preferred Name or Application Label depending on support for the Issuer Code Table Index) on the receipt. Refer to the *Transaction Acceptance Device Guide* for details.
	1b) Devices that Have Separate Insertion Areas for Chip and Magnetic Stripe Transactions: **Note:** This part of the test (1b) is **not** applicable to Combined Readers such as ATMs where the card is inserted into a single slot for both chip and magnetic-stripe transactions. Attempt to read the card via its magnetic stripe. Ensure that the device prompts the user to insert the card into the chip reader. This ensures that the device does not allow functioning EMV chip cards to be processed as magnetic stripe.
	1c) Non-Zero Floor Limit Devices (Devices that have a Floor Limit): Perform an online transaction (above the floor limit) to help ensure that the floor limit is set up correctly. The device must attempt to send the transaction online: • TVR, byte 4, bit 8 = 1 (Transaction Exceeds Floor Limit) **Note:** You will not be able to perform this test if you do not successfully pass part 1a.

Test Case 1/Test Card 1 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**1d) ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):** Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator where VCMS/VMTS/approved host simulator will perform Online Card Authentication. Online Card Authentication must pass (Field 44.8 = 2). VCMS/VMTS/approved host simulator will respond with an Issuer Authentication cryptogram (Authorization Response Cryptogram—ARPC). The device must be able to receive the cryptogram in the response data and forward it to the card where the **transaction must be approved**. If the online transaction results in a decline, the user has failed the test (indicating that the device either did not forward the cryptogram to the card or incorrectly forwarded the cryptogram to the card). The device log must show: • CVR, byte 2, bit 4 = 0 (Issuer Authentication performed and not failed) For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

3.2 Test Case 2: 19-Digit Account Number

Test Case 2/Test Card 2 (Mandatory; ADVT Online Testing)	
Test Case Number:	2
Test Case Name:	19-Digit Account Number
Objective:	To ensure acceptance of a card with a 19-digit account number. **Note:** *Visa Core Rules and Visa Product and Service Rules* and *Visa Europe Operating Regulations* require new and existing chip reading devices to be able to read Visa account numbers up to and including 19 digits. This includes ATMs accepting Plus cards.
Regional Requirement:	Mandatory All Regions ADVT Online Testing Required
Business Justification:	In addition to ensuring 19-digit account number acceptance by chip reading devices, the purpose of this card is also to gather information on general acceptance of 19-digit Visa PANs in the Visa acquiring environment. It is recommended that all acquiring host systems have the ability to accept 19-digit PANs.
Pre-requisite:	n/a
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	2
Test Evidence to be Submitted:	☒Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	Visa Core Rules and Visa Product and Service Rules Visa Europe Operating Regulations
Pass Criteria/User Validation:	**All Devices:** Ensure the device does not print the Primary Account Number (PAN) followed by an ‘F’ on the receipt. Because the PAN is 19 digits, the PAN field on the chip is padded with 1 F (per EMV). This ‘F’ must not be printed on the receipt. The device fails this test if it prints the ‘F’ as part of the PAN on the receipt.
	Offline-Only Devices: **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test.

Test Case 2/Test Card 2 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):** Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator and be approved. If the transaction is declined, it is not necessarily indicative of device failure. It could be that the acquiring host system is not capable of accepting 19-digit account numbers. If this is the case, include comments in the Test Results section within the Compliance Report via CCRT. For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

3.3 Test Case 3: T=1, DDA, OEP, and Issuer Authentication

Test Case 3/Test Card 3 (Mandatory; ADVT Online Testing)	
Test Case Number:	3
Test Case Name:	T=1, DDA, Offline Enciphered PIN, and Issuer Authentication
Objective:	To ensure acceptance of a card that supports the T=1 protocol and card is personalized to require successful Issuer Authentication on online transactions. Card supports DDA and Offline Enciphered PIN (OEP). **Note:** While cards can support either the T=0 or T=1 protocols, terminals must support both.
Regional Requirement:	Mandatory All Regions ADVT Online Testing Required
Business Justification:	There are millions of T=1 protocol cards in circulation. As such, Visa needs to ensure all terminals are capable of accepting cards using this protocol.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	3
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	EMV 4.3, Book 1, Section 9: Transmission Protocols
Pass Criteria/User Validation:	**Devices that Support Dynamic Data Authentication:** The device log must show: • Transaction Status Information (TSI), byte 1, bit 8 = 1 (Offline Data Authentication was performed) • TVR, byte 1, bit 8 = 0 (Offline Data Authentication was performed) • TVR, byte 1, bit 4 = 0 (DDA did not fail)
	Devices that Support Offline Enciphered PIN: The device log must show: • CVR, byte 2, bit 3 = 1 (Offline PIN Verification performed) • CVR, byte 2, bit 2 = 0 (Offline PIN Verification did not fail)

Test Case 3/Test Card 3 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**Offline-Only Devices:** **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test.
	ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs): Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator where VCMS/VMTS/approved host simulator will perform Online Card Authentication. Online Card Authentication must pass (Field 44.8 = 2). VCMS/VMTS/approved host simulator will respond with an Issuer Authentication cryptogram (Authorization Response Cryptogram—ARPC). The device must be able to receive the cryptogram in the response data and forward it to the card where the **transaction must be approved**. If the online transaction results in a decline, the user has failed the test (indicating that the device either did not forward the cryptogram to the card or incorrectly forwarded the cryptogram to the card). The device log must show: • CVR, byte 2, bit 4 = 0 (Issuer Authentication performed and not failed) For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

3.4 Test Case 4: Terminal Risk Management

Test Case 4/Test Card 4 (Mandatory)	
Test Case Number:	4
Test Case Name:	Terminal Risk Management
Objective:	To ensure the terminal correctly performs terminal risk management (specifically Floor Limit Checking) in accordance with Visa rules, even when the card is not personalized to support terminal risk management (AIP, Byte 1, Bit 4 = 0). **Note:** Card is personalized with 'Floor Limit Exceeded' bit set in the Issuer Action Code – Denial (Byte 4, Bit 8 = 1). **Note:** EMV only requires a terminal to perform Terminal Risk Management (TRM) if the "TRM is to be performed" bit is set in the card's Application Interchange Profile (AIP). However, Visa requires POS terminals to always perform TRM, even when this AIP bit is not set. Note that this requirement does not apply to online-only devices, such as ATMs, which are allowed to skip TRM processing.
Regional Requirement:	Mandatory All Regions
Business Justification:	Visa rules state that Terminal Risk Management should always be performed, irrespective of whether or not Terminal Risk Management is personalized on the card. This card is intended to test the terminal's compliance with this rule.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☐ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	4
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 10.6: Terminal Risk Management Terminal Acceptance Device Guidelines, Sections 5.5 & 5.9
Pass Criteria/User Validation:	**Online-Only Devices That Do Not Support Terminal Risk Management (TRM):** Not Applicable.
	All Other Devices: **The device must decline the transaction offline**. An error message, offline approval, or online approval is not acceptable and indicates failure of the test.

3.5 Test Case 5: Application Selection

Test Case 5/Test Card 5 (Mandatory)	
Test Case Number:	5
Test Case Name:	Application Selection
Objective:	This test has the following objectives: • Ensure acceptance of a card that contains multiple (five) applications, each distinguished by a unique suffix appended to the Visa AID • Ensure acceptance of a card containing a non-ASCII Application Preferred Name
Regional Requirement:	Mandatory All Regions
Business Justification:	As multi-application cards become more popular, it is important to ensure that terminals are able to correctly identify and select appropriate applications on the card and that the user interface is appropriate for the environment (i.e., the user interface must not confuse the merchant or the cardholder). According to the *Transaction Acceptance Device Requirements*, "Application Selection Indicators for Visa AIDs must indicate support for Partial selection." For cardholder convenience, issuers may choose to have the name of the application presented to the cardholder for selection in the cardholder's language (this is the Application Preferred Name). If the terminal supports the relevant alphabet ("Issuer Code Table Index"), it will display the Application Preferred Name rather than the Application Label. Otherwise, the terminal must ignore this feature and display the application name to the cardholder in the format specified in the Application Label.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	5
Test Evidence to be Submitted:	☒Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 1, Section 12.3.1: Matching Terminal Applications to ICC Applications EMV 4.3, Book 1, Section 12.4: Final Selection EMV 4.3, Book 4, Section 11.1: Language Selection EMV 4.3, Book 4, Section 11.3: Application Selection Transaction Acceptance Device Requirements

Test Case 5/Test Card 5 (Mandatory)	
Pass Criteria/User Validation:	Terminal must perform a complete VSDC transaction without error. A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test. Refer to Table 3-1: Test Case 5 Expected Results for details.
Specific Card Conditions:	Card contains five applications (3 x Visa Credit and 2 x Visa Debit) each with a unique suffix appended to the AID: • **Application #1**—Visa Credit is the first priority application. It contains an Application Preferred Name in Cyrillic code (i.e., Виса Кредит 1) and an Issuer Code Table Index of 05. This application is expired (i.e. its Application Expiration Date is personalized with 31 December 2005) and its IAC – Denial is set to decline transactions based on the expired application. • **Application #2**—Visa Debit is the second priority application. It contains an Application Preferred Name in Cyrillic code (i.e., Виса Дебет 1) and an Issuer Code Table Index of 05. This application is expired (i.e. its Application Expiration Date is personalized with 31 December 2005) and its IAC – Denial is set to decline transactions based on the expired application. • **Application #3**—Visa Credit is the third priority application. It contains an Application Preferred Name in Cyrillic code (i.e., Виса Кредит 2) and an Issuer Code Table Index of 05. This application is expired (i.e. its Application Expiration Date is personalized with 31 December 2005) and its IAC – Denial is set to decline transactions based on the expired application. • **Application #4**—Visa Debit is the fourth priority application. It contains an Application Preferred Name in Cyrillic code (i.e., Виса Дебет 2) and an Issuer Code Table Index of 05. The application has a unique PAN to allow easier identification of online transactions. • **Application #5**—Visa Credit is the fifth priority application. It contains an Application Preferred Name in Cyrillic code (i.e., Виса Кредит 3) and an Issuer Code Table Index of 05. The application has a unique PAN to allow easier identification of online transactions.

3.5.1 Test Case 5: Expected Results

This table outlines the expected results for Test Case 5. To determine which row to use for the expected results, identify the terminal's functionality including support for cardholder selection and Issuer Code Table Index of 05.

Table 3–1: Test Case 5: Expected Results

Terminal Scenario	Cardholder Selection Supported	Issuer Code Table Index 05 Supported	Expected Results
1	Yes	No	All five payment applications must be displayed to the cardholder in priority order using their Application Label. Since the first three applications are expired, either the fourth ("Visa Debit 2") or fifth ("Visa Credit 3") should be selected. The transaction must be approved offline or approved online. An offline decline is not acceptable and indicates failure of the test. The only situation where a decline is an acceptable response is when both the amount is above the floor limit and tests are being conducted in an offline mode (i.e., no connectivity to VCMS/VMTS/approved host simulator). In this scenario, the terminal must attempt to send the transaction online and then decline offline when online is not available (due to the IAC and TAC-Default for Floor Limit Exceeded). The Visa AID must be printed on the receipt and it is strongly recommended that the Application Label be printed as well.
2	Yes	Yes	All five payment applications must be displayed to the cardholder in priority order using their Application Preferred Name. Since the first three applications are expired, either the fourth ("Виса Дебет 2") or fifth ("Виса Кредит 3") should be selected. The transaction must be approved offline or approved online. An offline decline is not acceptable and indicates failure of the test. The only situation where a decline is an acceptable response is when both the amount is above the floor limit and tests are being conducted in an offline mode (i.e., no connectivity to VCMS/VMTS/approved host simulator). In this scenario, the terminal must attempt to send the transaction online and then decline offline when online is not available (due to the IAC and TAC-Default for Floor Limit Exceeded). The Visa AID must be printed on the receipt and it is strongly recommended that the Application Preferred Name (i.e. either "Виса Кредит" or "Виса Дебет") be printed as well.

Terminal Scenario	Cardholder Selection Supported	Issuer Code Table Index 05 Supported	Expected Results
3	No	N/A	In accordance with Visa rules, since the terminal does not support the displaying of mutually supported applications or Cardholder Selection, the highest priority application should be selected for the transaction. The transaction will be **declined offline** because the highest priority application is personalized with an expired application. If a receipt is printed, the Visa AID must be on the receipt and it is strongly recommended that the Application Label (Visa Credit) be printed as well.

3.6 Test Case 6: Dual Interface

Test Case 6/Test Card 6 (Mandatory)	
Test Case Number:	6
Test Case Name:	Dual Interface
Objective:	To ensure acceptance of a Dual Interface card (contact and contactless) containing the following within the contact payment application: • A long PDOL (45 bytes) • Language Preference field with Japanese, Korean, and Chinese language codes specified **Note:** The Language Preference field is an optional data element that issuers may include on their cards. If included on the card, the terminal must be able to handle this field. **Note:** The VSDC contact application supports DDA.
Regional Requirement:	Mandatory All Regions
Business Justification:	For cardholder convenience, issuers may use the Language Preference feature to allow cardholders to be presented with terminal messages in their language of choice. The terminal needs to ensure one of the following: • If it does **not** support any of the preferred languages identified on the card, it continues to execute the transaction using the language it supports. • If it does support one of the preferred languages, all terminal displays are presented in the highest priority language.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	6
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Pass Criteria/User Validation:	**Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test. In addition, if the device supports Japanese, Korean, or Chinese, the device must display any cardholder messages in that language (e.g., when prompting the cardholder to agree to the amount of the transaction, the device must display messages such as “Amount OK” to the cardholder in one of the above languages).

3.7 Test Case 7: Terminal Action Codes (TACs)

Test Case 7/Test Card 7 (Mandatory)	
Test Case Number:	7
Test Case Name:	Terminal Action Codes (TACs)
Objective:	To ensure Terminal Action Codes (TACs) are correctly configured (refer to Appendix B: Terminal Action Code (TAC) Settings for the TACs that must be loaded into the device). **Note:** In this test, the Application Usage Control on the card indicates that the card cannot be used for international transactions. This will cause the terminal to set the "Service Not Allowed For Card Product" bit in the TVR which must result in a declined transaction. This test is only for one bit in the TAC-Decline (Service Not Allowed For Card Product) but is intended to focus attention on the TAC values in general.
Regional Requirement:	Mandatory All Regions
Business Justification:	For risk management and acceptance purposes, Visa has defined and specified a set of values (referred to as Terminal Action Codes) that must be used on Chip Card Acceptance Devices accepting Visa cards. It is therefore important to ensure these values are being correctly applied. **Note:** TAC values are mandated by Visa for all devices. The values can be found in the *Transaction Acceptance Device Requirements* and Appendix B: Terminal Action Codes of this document.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	7
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**Device must decline the transaction offline**. The device fails the test if the transaction is terminated with an error message, approved offline, or sent online for authorization. The device log must show: • TVR, byte 2, bit 5 = 1 (Requested Service Not Allowed For Card Product) • Device requests an AAC in the FIRST GENERATE AC command

3.8 Test Case 8: Fallback

Test Case 8/Test Card 8 (Conditional)	
Test Case Number:	8
Test Case Name:	Fallback
Objective:	To ensure that the terminal properly allows fallback. **Note:** Card contains a faulty chip. **Note:** Because regional and/or domestic rules govern the policy on fallback, check with your Visa representative to determine if fallback is allowed.
Regional Requirement:	Conditional All Regions ADVT Online Testing Required
Business Justification:	Some Visa regional offices have defined rules around magnetic stripe fallback following failure of chip-based transactions. This card may be used to ensure correct rules are being applied and that the user interface is appropriate.
Pre-requisite:	Device supports magnetic-stripe fallback **Note:** Magnetic stripe fallback is **not** mandated at a Visa global level; Visa regional offices may apply regional or domestic policies on fallback. Contact your Visa representative to determine if regional or domestic policies apply.
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	8
Test Evidence to be Submitted:	☒Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	Visa Core Rules and Visa Product and Service Rules Visa Europe Operating Regulations Transaction Acceptance Device Guide
Pass Criteria/User Validation:	**General:** The device must attempt to read the chip, realize it is faulty, and allow the magnetic stripe to be read. This test should validate that the device allows for a magnetic stripe entry when the chip is faulty and then performs a magnetic stripe online transaction.
	Readers that Have Separate Insertion Areas for Chip and Magnetic Stripe Transactions: The device must clearly indicate during the attempt to read the chip that the "Chip Cannot Be Read" (or equivalent). To indicate that fallback is supported, the device must provide a message such as "Swipe Magnetic Stripe" (or equivalent).

Test Case 8/Test Card 8 (Conditional)	
Pass Criteria/User Validation (con't):	**Combined Readers (Readers, such as ATMs, where there is a single insertion point for both magnetic stripe and chip transactions):** In these devices, fallback to magnetic stripe is transparent to the user. However, the user must ensure that the device properly allows fallback (i.e., a magnetic-stripe transaction). The device fails this test when the device does not allow the magnetic stripe to be read and/or when the receipt contains the Visa AID (A0000000031010). **Note 1:** Any online response code is acceptable for the magnetic stripe fallback transaction including decline responses such as incorrect/missing PIN. **Note 2:** Some fallback procedures allow for more than one attempt to read the chip card.

3.9 Test Case 9: “Reserved for Future Use” CVM

Test Case 9/Test Card 9 (Mandatory)	
Test Case Number:	9
Test Case Name:	“Reserved for Future Use” CVM
Objective:	To ensure that the terminal correctly processes a card containing a CVM that the terminal does not recognize and the CVM is not on the list of CVMs that must be recognized by the terminal (i.e., the first CVM in the list is a “Reserved For Future Use CVM”, with instructions to apply the next CVM if CVM processing fails).
Regional Requirement:	Mandatory All Regions
Business Justification:	The CVM List of an EMV card may contain a method not recognizable by the terminal. If the terminal encounters such a method, it must follow the CVM rules and proceed with the transaction. This card is designed to ensure correct terminal behavior.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	9
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 10.5: Cardholder Verification Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**All Devices:** **The transaction must be approved offline or approved online.** An error message or an offline decline is not acceptable and indicates failure of the test.

Test Case 9/Test Card 9 (Mandatory)	
Pass Criteria/User Validation (con’t):	**<u>POS Devices:</u>** When encountering a new CVM (represented by a “Reserved For Future Use” CVM value in the CVM List), the device must set: • TVR, byte 3, bit 7 = 1 (Unrecognized CVM) Since this CVM list indicates that the “Reserved For Future Use” CVM must only be performed when supported by the device, the device must proceed to the remaining CVMs in the CVM list. For POS devices supporting signature, signature must be requested and the terminal must set: • TVR, byte 3, bit 8 to ‘0’ (Cardholder Verification Successful) **Note:** All online-capable unattended POS devices, including AFDs, must support the “No CVM” CVM. This means that they should process this card without requesting any CVM and send it online where it will be authorized.
	<u>ATMs:</u> ATMs must request the cardholder to enter their Online PIN, send the transaction online, and be approved.

3.10 Test Case 10: CDA

Test Case 10/Test Card 10 (Mandatory)	
Test Case Number:	10
Test Case Name:	CDA
Objective:	To ensure acceptance of a card that supports Combined DDA/Generate Application Cryptogram (CDA).
Regional Requirement:	Mandatory All Regions
Business Justification:	CDA combines DDA with the generation of a card's Application Cryptogram to assure card validity. It intended to protect offline transactions where there is significant opportunity for interception of chip-to-device communications. Support of CDA in devices may be needed in some countries, as this process has been implemented in specific markets. Check with your Visa representative on the requirements in your market.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	10
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV Terminal Acceptance Device Requirements
Pass Criteria/User Validation:	**Devices That Support CDA:** DDA is performed offline and is successful. If the transaction is sent online, Online Card Authentication must be successful (Field 44.8 = 2) and the transaction must be approved online. The device log must show: • Transaction Status Information (TSI), byte 1, bit 8 = 1 (Offline Data Authentication was performed) • TVR, byte 1, bit 8 = 0 (Offline Data Authentication was performed) • TVR, byte 1, bit 3 = 0 (CDA did not fail)

Test Case 10/Test Card 10 (Mandatory)	
Pass Criteria/User Validation (con't):	**Devices That Do Not Support CDA:** CDA is not applicable. Device must perform a complete transaction without any error messages. A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test. This test ensures that even though the device does not support CDA, a card supporting CDA does not cause acceptance problems.

3.11 Test Case 11: Multiple Applications

Test Case 11/Test Card 11 (Mandatory)	
Test Case Number:	11
Test Case Name:	Multiple Applications
Objective:	To ensure correct acceptance of a card containing multiple applications, but with only one application valid for use. Card contains three applications where the last one is the only usable application: • Application # 1 – Contains an unknown AID • Application # 2 – Blocked application (PAN = 47 61 73 90 01 01 00 10) • Application # 3 – Valid application (PAN = 47 61 73 90 01 01 01 19) **Note:** Application #3 supports DDA.
Regional Requirement:	Mandatory All Regions
Business Justification:	As multi-application cards become more popular, it is important to ensure that terminals are able to correctly identify and select appropriate applications on the card and that the user interface is appropriate for the environment (i.e., the user interface must not confuse the merchant or the cardholder).
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	11
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 1, Section 12.4: Final Selection
Pass Criteria/User Validation:	The transaction must be **approved offline or approved online**. An error message or an offline decline is not acceptable and indicates failure of the test. This test is applicable to all devices, irrespective of whether or not 'Cardholder Application Selection' is supported. Only one application is valid for use (Application #3) and therefore should be the one selected.

3.12 Test Case 12: Geographic Restrictions

Test Case 12/Test Card 12 (Mandatory)	
Test Case Number:	12
Test Case Name:	Geographic Restrictions
Objective:	To ensure the terminal correctly handles a “Conditions of Use Not Satisfied” (6985) response to the GET PROCESSING OPTIONS command. **Note:** Card supports the Geographic Restrictions check and is restricted to domestic transactions.
Regional Requirement:	Mandatory All Regions
Business Justification:	As part of their risk management requirements, an issuer may choose to restrict use of VSDC cards to domestic environments only. It is therefore important to ensure that if a terminal encounters such a card in an international situation, the appropriate terminal behavior is performed.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	12
Test Evidence to be Submitted:	☒Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	Device must send the GET PROCESSING OPTIONS command to the card. The card is personalized to perform the Geographic Restrictions check and respond with “Conditions of Use Not Satisfied” (6985). This must prompt the device to return to Application Selection and conclude that there are no applications to use for the transaction. At this time, the device must display a message such as “Not Accepted” or its equivalent (specific message content is based on best practice only and is not mandated). If the device accepts the card and completes the transaction, it fails this test. **Combined Readers (Readers, such as ATMs, where there is a single insertion point for both magnetic stripe and chip transactions):** For these devices, the user must verify that the transaction did not take place using the chip. The user can ensure this by either checking the logs to ensure that the transaction was magnetic stripe or ensuring that the AID (A0000000031010) does not appear on the receipt.

3.13 Test Case 13: Proprietary Data and 6-Digit PIN

Test Case 13/Test Card 13 (Mandatory; ADVT Online Testing)	
Test Case Number:	13
Test Case Name:	Proprietary Data and 6-Digit PIN
Objective:	To ensure acceptance of a card containing proprietary data. The test also ensures correct processing of a card with a 6-digit (Offline or Online) PIN. Card contains proprietary data. It contains the proprietary tags C2 with a value of "Sample" and tag 9F73 with a value of "80 80" in the PSE. It also contains a proprietary tag "C3" in a record in the application data. **Note:** The PIN value is 123412.
Regional Requirement:	Mandatory All Regions ADVT Online Testing Required
Business Justification:	An issuer may choose to include Discretionary Data on the card. It is important to ensure that terminals encountering cards that contain such data do not react negatively to its presence.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	13
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 7.0: Files for Financial Transaction Interchange
Pass Criteria/User Validation:	**Devices that Support Offline PIN:** The device log must show: • CVR, byte 2, bit 3 = 1 (Offline PIN Verification performed) • CVR, byte 2, bit 2 = 0 (Offline PIN Verification did not fail)
	Offline-Only Devices: **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test.

Test Case 13/Test Card 13 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):** Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator. Online Card Authentication must be successful (Field 44.8 = 2). **The transaction must be approved online.** For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

3.14 Test Case 14: Long PDOL and Unrecognized Tag

Test Case 14/Test Card 14 (Mandatory)	
Test Case Number:	14
Test Case Name:	Long PDOL and Unrecognized Tag
Objective:	To ensure acceptance of a card where the PDOL is requesting a long string of data, including an unrecognized tag.
Regional Requirement:	Mandatory All Regions
Business Justification:	Cases have been noted in the past where (often through personalization discrepancies) the length of a terminal-based data object requested by the card in a Data Object List (DOL) may differ from the actual length of the data object. EMV specifies that cards must not be rejected due to this situation. This card is intended to ensure that the specified rules are being correctly applied.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	14
Test Evidence to be Submitted:	☐Receipt ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 5.4: Rules for Using a Data Object List
Pass Criteria/User Validation:	**Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test. In addition, the device must send 97 zeroes followed by the Transaction Date in the GET PROCESSING OPTIONS command.

3.15 Test Case 15: Data Element with 2-Byte Length Field

Test Case 15/Test Card 15 (Mandatory)	
Test Case Number:	15
Test Case Name:	Data Element with 2-Byte Length Field
Objective:	To ensure acceptance of a card where: • A data element contains less than 128 bytes of data, yet its length field is configured as 2 bytes • A data element contains a length of zero **Note:** These are situations that could erroneously occur during card personalization. According to EMV, a data element can have a length field of 2 bytes even though the data value is less than 128 bytes in length. Usually, the length is 1 byte when the data value is less than 128 bytes in length, and it is 2 bytes when the data value is greater than 128 bytes in length. Issuers, however, can use a length of 2 bytes even when the data value is less than 128 bytes in length.
Regional Requirement:	Mandatory All Regions
Business Justification:	Cases have been noted in the past where (often through personalization discrepancies) the length field of a data record in the card is formatted as 2 bytes even though the actual record length may be less than 128 bytes (usually if a data record length is 2 bytes, the record contains at least 128 bytes). EMV specifies that cards must not be rejected due to this situation. This card is intended to ensure that the specified rules are being correctly applied.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	15
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Annex B
Pass Criteria/User Validation:	**Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test.

3.16 Test Case 16: Two Applications and Cardholder Confirmation

Test Case 16/Test Card 16 (Mandatory)	
Test Case Number:	16
Test Case Name:	Two Applications and Cardholder Confirmation
Objective:	This test has the following objectives: • Ensure acceptance of a card that contains two applications distinguishable by suffixes added to the Visa AID – Note: Visa Credit application is the first priority application and requires cardholder confirmation. It has an expired application and the IACs indicate to decline offline for expired application. – Note: Visa Debit application is the second priority application and does not require cardholder confirmation. • Ensure support of card requirements related to cardholder confirmation **Note:** This is a multi-access card.
Regional Requirement:	Mandatory All Regions
Business Justification:	As multi-application cards become more popular, it is important to ensure that terminals are able to correctly identify and select appropriate applications on the card and that the user interface is appropriate for the environment (i.e., the user interface must not confuse the merchant or the cardholder). According to the *Transaction Acceptance Device Requirements*, "Application Selection Indicators for Visa AIDs must indicate support for Partial selection." On this test card, the first application requires cardholder confirmation (which can be achieved through cardholder selection or cardholder confirmation). If the device does not support cardholder selection or cardholder confirmation, it must **not** proceed with a transaction using the first application (Visa Credit). It must stop processing the Visa Credit application and proceed to application selection for the second application (Visa Debit).
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	16
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log

Test Case 16/Test Card 16 (Mandatory)	
Document Reference:	EMV 4.3, Book 1, Section 12.3.1: Matching Terminal Applications to ICC Applications EMV 4.3, Book 1, Section 12.4: Final Selection EMV 4.3, Book 4, Section 11.3: Application Selection Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**All Devices:** **Transaction must be approved offline or approved online.** An error message or an offline decline indicates failure of this test.
	Devices That Do Not Support Cardholder Selection/Confirmation: First, the device attempts to select the Visa Credit application (this is the highest priority application). Upon recognizing that this application requires cardholder confirmation, the device terminates the transaction and begins processing the second application (Visa Debit, the second highest priority application). Since Visa Debit does not require cardholder confirmation, the transaction proceeds to completion using the Visa Debit application. **Note:** Devices that do not support cardholder confirmation must use the Visa Debit application for this test; they must not select and process the transaction using the Visa Credit application. In the event the device erroneously selects the Visa Credit application, the transaction will be declined offline because this application is expired. Use of the Visa Credit application for the transaction and/or an offline decline constitutes a failure of this test.
	Devices That Support Cardholder Selection/Confirmation: Both applications should be displayed to the cardholder in priority order (Visa Credit first, followed by Visa Debit). The tester should select the “Visa Debit” application (second) for the transaction, since the “Visa Credit” application has expired. **Note:** Since the objective of this test is to ensure that the desired application, as selected by the cardholder, is the one used for the transaction (not the one with the highest priority), an erroneous selection of the Visa Credit application by the device will result in a decline. A transaction using the “Visa Credit” application will be declined offline because this application has expired. Use of the “Visa Credit” application for this transaction and/or an offline decline constitutes a failure of this test. The Visa AID must be printed on the receipt and it is strongly recommended to print the Application Label (Visa Debit) as well.

3.17 Test Case 17: Magnetic Stripe Image

Test Case 17/Test Card 17 (Mandatory; ADVT Online Testing)	
Test Case Number:	17
Test Case Name:	Magnetic Stripe Image
Objective:	To ensure acceptance of a card containing the minimum set of VSDC data elements and functions (i.e., the Magnetic Stripe Image where neither SDA nor DDA is supported Cryptogram Version 12 is supported, and CDOLs contain the minimum set of data).
Regional Requirement:	Mandatory All Regions ADVT Online Testing Required
Business Justification:	Issuers may choose to support simple VSDC cards (i.e., cards that support minimum VSDC features and data). This test ensures that terminals accept and successfully process these cards.
Pre-requisite:	n/a
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	17
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	EMV 4.3 Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**Offline-Only Devices:** **Device must decline the transaction offline** (due to the TAC-Default setting for “Offline Data Authentication Not Performed”). The transaction must contain the TVR settings for: • TVR, byte 1, bit 6 = 0 (ICC Data is not Missing) • TVR, byte 1, bit 8 = 1 (Offline Data Authentication Not Performed)

Test Case 17/Test Card 17 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):** Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator. **The transaction must be declined online.** The transaction must contain the TVR settings for: • TVR, byte 1, bit 6 = 0 (ICC Data is not Missing) • TVR, byte 1, bit 8 = 1 (Offline Data Authentication Not Performed) For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

3.18 Test Case 18: T=1 and DDA with 1984 Certificate

Test Case 18/Test Card 18 (Mandatory)	
Test Case Number:	18
Test Case Name:	T=1 and DDA with 1984 Certificate
Objective:	To ensure acceptance of a T=1 card supporting DDA with a certificate signed with Visa CA’s key of 1984 bits.
Regional Requirement:	Mandatory All Regions
Business Justification:	Visa is currently providing Issuer Public Key Certificates to issuers based on a 1984-bit Visa Certificate Authority Public Key. Concerns were raised in the past regarding some terminals’ ability to support keys of this length, particularly terminals that were deployed in the earlier stages of chip migration. This card ensures that terminals are capable of supporting an Issuer Public Key of this length.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	18
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 10.3: Offline Data Authentication Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**Devices That Support Offline Data Authentication (ODA):** The device log must show: • Transaction Status Information (TSI), byte 1, bit 8 = 1 (Offline Data Authentication was performed) • TVR, byte 1, bit 8 = 0 (Offline Data Authentication was performed) • TVR, byte 1, bit 4 = 0 (DDA did not fail) **The transaction must be approved offline or approved online.** An error message or an offline decline is not acceptable and indicates failure of the test.
	Devices That Do Not Support ODA: For these devices, the primary objective of this test case is to ensure correct acceptance of a T=1 card. **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test.

3.19 Test Case 19: Plus and Visa Interlink

Test Case 19/Test Card 19 (Conditional; ADVT Online Testing)	
Test Case Number:	19
Test Case Name:	Plus and Visa Interlink
Objective:	This test has the following objectives: • **ATM—**Monitor acceptance of a card with the Plus AID in ATM environments; this card also contains a Suffix to ensure correct Partial Name Selection processing (A0 00 00 00 03 80 10 01) • **POS**—Monitor acceptance of a card with the Visa Interlink AID (no Suffix) at participating POS environments (A0 00 00 00 03 30 10) **Note:** Because regional and/or domestic rules govern the policy on Plus and Interlink, check with your Visa representative for current local rules and regulations.
Regional Requirement:	Conditional ADVT Online Testing Required
Business Justification:	This card is included to assess the general acceptance of: • **Visa RID with the Plus PIX at ATMs**—Plus is a deposit access product that offers worldwide cash access and other around-the-clock financial services through the Visa Global ATM Network. The Plus Program can be added to any banking card and complements the utility of other Visa products. • **Interlink AID at POS**—Interlink is part of Visa's Integrated Debit Solution which is a PIN-based POS Network that allows an account holder to use a stand-alone ATM card, Visa branded prepaid card, or Visa Check Card with the Interlink acceptance mark issued by their financial institution to make purchases at participating retail locations.
Pre-requisite:	• **ATM**—This test applies only to ATMs that support the Plus brand. • **POS**—This test applies only to POS environments that support Interlink.
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	19
Test Evidence to be Submitted:	☒Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	Visa Global ATM Member Guide, Appendix A: Acquirer Participation Requirements Transaction Acceptance Device Requirements

Test Case 19/Test Card 19 (Conditional; ADVT Online Testing)	
Pass Criteria/User Validation:	**ADVT Online Testing for ATMs Accepting Plus Cards[2]:** The transaction must be sent online to VCMS/VMTS/approved host simulator and be **approved**. The AID must be printed on the receipt. The receipt should also include the Suffix since it is part of the AID (A0 00 00 00 03 80 10 01). It is also strongly recommended that the Application Label (Plus) is printed on the receipt. For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.
	ADVT Online Testing for POS Devices Containing the Interlink AID: The transaction must be sent online to VCMS/VMTS/approved host simulator and be **approved**. The AID must be printed on the receipt. The receipt should also include the Suffix since it is part of the AID (A0 00 00 00 03 30 10). It is also strongly recommended that the Application Label (Interlink) is printed on the receipt. For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

[2] It is assumed that the ATM supports acceptance of Visa in addition to Plus.

3.20 Test Case 20: Visa Electron

Test Case 20/Test Card 20 (Conditional)	
Test Case Number:	20
Test Case Name:	Visa Electron
Objective:	To ensure acceptance of a Visa Electron card with an unusable magnetic stripe. **Note:** ATMs must support the Visa Electron AID (A0 00 00 00 03 20 10). Refer to the *Transaction Acceptance Device Guide* for more details. Merchants that agree to accept the Visa Electron product must support the Visa Electron AID in their terminals (A0 00 00 03 20 10). For other merchants, if the terminal supports the Visa AID, it is required to support the Visa Electron AID unless the merchant specifically chooses to exclude it because the merchant does not accept Visa Electron products by any interface including magnetic stripe. To accept Visa Electron cards, the only activity that is required is to add the Visa Electron AID to the terminal. No other activities (coding, adding keys, etc.) are required as terminals that support Visa Electron use the same code and keys as required for the Visa AID.
Regional Requirement:	Conditional
Business Justification:	This card ensures that the rules governing acceptance of the Visa Electron AID are being applied and that, where a combined reader is used, the terminal does not perform unnecessary processing on the magnetic-stripe data which may hinder chip acceptance. If the Visa AID is supported by the terminal, the Visa Electron AID must also be supported, unless the merchant has specifically chosen to exclude it, and ATMs must support the Visa Electron AID. When the magnetic stripe of a card is read and the service code begins with a 2 or a 6, indicating that a chip is present, the terminal must process the transaction using the chip and ignore any other features of the magnetic stripe data. Failure to apply these rules may lead to acceptance problems with chip-based Visa Electron cards and/or chip-only products which do not have meaningful magnetic stripe data.
Pre-requisite:	Device supports Visa Electron AID
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	20
Test Evidence to be Submitted:	☒Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log

Test Case 20/Test Card 20 (Conditional)	
Document Reference:	EMV 4.3, Book 4, 6.6 Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**The transaction must be approved offline or approved online.** An error message or an offline decline is not acceptable and indicates failure of the test. It is strongly recommended that the Application Label (VISA ELECTRON) or the Application Preferred Name (ELECTRON DE VISA) (where appropriate) be printed on the receipt. **Note:** To facilitate Visa Electron acceptance, all chip-reading devices that support the Visa Debit/Credit AID must also support the Visa Electron AID, unless specifically excluded by the merchant who has elected not to accept transactions from Visa Electron cards through any interface including magnetic stripe. Please consult with your Visa representative for further local rules and regulations related to Visa Electron acceptance.

3.21 Test Case 21: PIN Try Limit Exceeded (1)

Test Case 21/Test Card 21 (Mandatory)	
Test Case Number:	21
Test Case Name:	PIN Try Limit Exceeded (1)
Objective:	To ensure that the terminal correctly processes a card where the first CVM in the CVM List is Offline PIN and the PIN Try Limit is exceeded. The card is personalized to proceed to signature or Online PIN when Offline PIN processing fails or is not supported by the terminal.
Regional Requirement:	Mandatory All Regions
Business Justification:	Cards may have their "PIN Try Limit Exceeded" flag set and still be usable. Issuers may even issue cards with the PIN Try limit already exceeded. It is important that terminals appropriately handle this situation according to EMV and do not perform additional processing which contradicts EMV such as rejecting the card or displaying incorrect or misleading messages.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	21
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 10.5.1: Offline PIN Processing Transaction Acceptance Device Requirements

Test Case 21/Test Card 21 (Mandatory)	
Pass Criteria/User Validation:	**Devices That Support Offline PIN:** **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test. The device log must show: • TVR, byte 3, bit 6 = 1 (PIN Try Limit Exceeded) • TVR, byte 3, bit 8 = 0 (Cardholder Verification Successful) The device must proceed to the next CVM in the CVM list and validate the cardholder through signature or Online PIN depending on the methods it supports. **Note 1:** If the device supports Offline Plaintext PIN, but not Signature or Online PIN, then cardholder verification will fail and the transaction will be declined offline. The device must set the TVR, byte 3, bit 8 = 1 (Cardholder Verification Failed) and since the corresponding card IAC is set to decline offline, transaction must be declined offline. **Note 2:** When connected to VCMS/VMTS/approved host simulator, VCMS/VMTS/approved host simulator will decline the transaction due to the VCMS/VMTS/approved host simulator STIP response for PIN Try Limit Exceeded.
	Devices That Do Not Support Offline PIN: Not Applicable.

3.22 Test Case 22: PIN Try Limit Exceeded (2)

Test Case 22/Test Card 22 (Mandatory)	
Test Case Number:	22
Test Case Name:	PIN Try Limit Exceeded (2)
Objective:	To ensure that the terminal correctly processes a card where the first CVM in the CVM List is Offline PIN and the PIN Try Limit is exceeded. The card is personalized not to proceed when the first CVM fails. **Note:** The IAC indicates decline offline for PIN Try Limit exceeded.
Regional Requirement:	Mandatory All Regions
Business Justification:	Cards may have their PIN Try Limit exceeded and still be usable. Issuers may even issue cards with the PIN Try limit already exceeded. It is important that terminals appropriately handle this situation according to EMV and do not perform additional processing which contradicts EMV such as rejecting the card or displaying incorrect or misleading messages.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	22
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 10.5.1: Offline PIN Processing Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**<u>Devices That Support Offline PIN:</u>** The device must set: • TVR, byte 3, bit 6 = 1 (PIN Try Limit Exceeded) • TVR, byte 3, bit 8 = 1 (Cardholder Verification Failed) **The transaction must be declined offline** (the card is configured to decline offline when the PIN Try Limit is exceeded, so it will return an AAC irrespective of device type or capabilities).
	<u>Devices That Do Not Support Offline PIN:</u> Not Applicable.

3.23 Test Case 23: Combination CVM and Visa Fleet Chip

Test Case 23/Test Card 23 (Mandatory)	
Test Case Number:	23
Test Case Name:	Combination CVM and Visa Fleet Chip
Objective:	The objectives of this test case are to: • Ensure that the terminal correctly processes a card containing a CVM List that supports the combination CVM of Signature and Offline PIN • Ensure that a card that contains the Visa Fleet Chip (VFC) feature is accepted at standard EMV devices **Note:** The Offline PIN value is: “1234”. The Online PIN value is “1234”.
Regional Requirement:	Mandatory
Business Justification:	Although a combination CVM (i.e., Signature plus Offline PIN) is not commonly used by Visa issuers, it is important to ensure all terminals accept this CVM method. It is also important to ensure that, as additional payment features are introduced to the card (such as the Visa Fleet Chip feature), the card continues to be accepted at standard EMV acceptance devices.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	23
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 10.5: Cardholder Verification Transaction Acceptance Device Requirements

Test Case 23/Test Card 23 (Mandatory)	
Pass Criteria/User Validation:	**Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test. • If the device supports both Offline PIN and Signature then, by default, it supports the combination CVM of Offline PIN and Signature. If this is the case, the device must validate the cardholder's Offline PIN and print the signature line on the receipt: – CVR, byte 2, bit 3 = 1 (Offline PIN Verification performed) – CVR, byte 2, bit 2 = 0 (Offline PIN Verification did not fail) • For ATMs, Online PIN must be used: – TVR, byte 3, bit 3 = 1 (Online PIN Entered) • For devices supporting Online PIN and signature or Online PIN only, Online PIN must be used: – TVR, byte 3, bit 3 = 1 (Online PIN Entered) • For devices supporting Offline PIN but not Online PIN, Offline PIN must be used: – CVR, byte 2, bit 3 = 1 (Offline PIN Verification performed) – CVR, byte 2, bit 2 = 0 (Offline PIN Verification did not Fail) • For devices that only support signature, signature must be used

3.24 Test Case 24: Account Number with Padded Fs

Test Case 24/Test Card 24 (Mandatory; ADVT Online Testing)	
Test Case Number:	24
Test Case Name:	Account Number with Padded Fs
Objective:	To determine whether the terminal can handle transactions from a card that contains a 16-digit account number padded with hexadecimal "Fs" to maximize its field length.
Regional Requirement:	Mandatory ADVT Online Testing Required
Business Justification:	There have been cases where issuers have used the maximum length of the Primary Account Number field by padding the unused portion with 'F's'. It is important to ensure that all terminals accept any card configured in this way and that the padded 'F's' are not printed on the receipt.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	24
Test Evidence to be Submitted:	☒Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	EMV 4.3, Book 3, Section 4.3: Data Element Format Conventions
Pass Criteria/User Validation:	**Offline-Only Devices:** **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test. The device must not print the padded F's or the full Primary Account Number on the receipt.

Test Case 24/Test Card 24 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**<u>ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):</u>** Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator. Online Card Authentication must be successful (Field 44.8 = 2). **The transaction must be approved online.** For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT. The device must not print the padded F's or the full Primary Account Number on the receipt.

3.25 Test Case 25: No PAN Sequence Number

Test Case 25/Test Card 25 (Mandatory; ADVT Online Testing)	
Test Case Number:	25
Test Case Name:	No PAN Sequence Number
Objective:	To ensure acceptance of a card without a PAN Sequence Number.
Regional Requirement:	Mandatory ADVT Online Testing Required
Business Justification:	The PAN Sequence Number is an optional data element that issuers may use to differentiate card applications having the same Primary Account Number. If the issuer chooses not to include this data element, it is important to ensure that terminals and acquirer host systems recognize this omission and do **not** erroneously include this data element in the online message. **Note:** The PAN Sequence Number, if present, must come from the card; the terminal or acquirer must never populate the PAN Sequence Number field in the online or clearing message with a static value or a value from a terminal or acquirer-system table.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	25
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**Offline-Only Devices:** **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test.

Test Case 25/Test Card 25 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):** Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator. Online Card Authentication must be successful (Field 44.8 = 2). **The transaction must be approved online.** Since the Application PAN Sequence Number is not present on the card, the acquirer may either exclude the field entirely from the request message (Field 23) or include it with all zeroes. For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

3.26 Test Case 26: PAN Sequence Number of 11

Test Case 26/Test Card 26 (Mandatory; ADVT Online Testing)	
Test Case Number:	26
Test Case Name:	PAN Sequence Number of 11
Objective:	To ensure acceptance of a card with a PAN Sequence Number of 11.
Regional Requirement:	Mandatory ADVT Online Testing Required
Business Justification:	The PAN Sequence Number is an optional data element that issuers may use to differentiate card applications having the same Primary Account Number. In most cases, when this data element is used, its value is less then '10'. There have been interoperability problems, however, when the value is over 10 because acquirers have formatted this binary value as hex. The incorrect formatting of this field leads to erroneous Online Card Authentication failures which may lead to declines. This test ensures that a PAN Sequence Number greater than 10 is formatted correctly as a binary value.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	26
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	Transaction Acceptance Device Requirements
Pass Criteria/User Validation:	**Offline-Only Devices:** **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test.

Test Case 26/Test Card 26 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):** Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator. Online Card Authentication must be successful (Field 44.8 = 2). **The transaction must be approved online.** The online message must contain Field 23: PAN Sequence Number with a value of 11 (alphanumeric). For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

3.27 Test Case 27: 1144-Bit Issuer Public Key

Test Case 27/Test Card 27 (Mandatory)	
Test Case Number:	27
Test Case Name:	1144-Bit Issuer Public Key
Objective:	To ensure acceptance of a card with an Issuer Public Key Certificate based on an 1144-bit Issuer Public Key.
Regional Requirement:	Mandatory
Business Justification:	It has been discovered that there are some faulty RSA cryptographic engines that are unable to handle key lengths not evenly divisible by 16, 8 or 4. With this in mind, a card with an Issuer Public Key Certificate based on an 1144-bit (i.e., 143 bytes) Issuer Public Key was proposed. This test ensures that terminals can support cards with Issuer Public Keys that are not evenly divisible by 16, 8, or 4.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	27
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 2, Section 6.1: Keys and Certificates
Pass Criteria/User Validation:	**Devices That Support SDA:** **The transaction must be approved offline or approved online.** An error message or an offline decline is not acceptable and indicates failure of the test. The device log must show: • Transaction Status Information (TSI), byte 1, bit 8 = 1 (Offline Data Authentication was performed) • TVR, byte 1, bit 8 = 0 (Offline Data Authentication was performed) • TVR, byte 1, bit 7 = 0 (SDA did not fail)
	Devices That Do No Support SDA: Not Applicable.

3.28 Test Case 28: Multiple Features

Test Case 28/Test Card 28 (Mandatory; ADVT Online Testing)	
Test Case Number:	28
Test Case Name:	Multiple Features
Objective:	To ensure acceptance of a card with the following features: • Issuer URL in the FCI Issuer Discretionary Data • Extra Issuer Application Data • Application Expiration Date = December 31, 2025 • CVM List with no Signature • Specific IAC-Denial settings related to PIN activity • Cryptogram Version Number = 18 (hex '12')
Regional Requirement:	Mandatory ADVT Online Testing Required
Business Justification:	The Issuer URL was introduced to allow issuers to specify the location of their Library Servers for Internet service. There are a few known cases where terminals reacted negatively to cards containing an issuer URL. This test ensures that terminals can accept a card containing an issuer URL. A CVM List that does not contain "Signature" has been known to cause acceptance problems with some terminals. This test ensures that terminals can accept a card without this CVM. Since there is an expectation that a significant number of issuers will begin supporting CVN 18 card products over the coming years, acquirers need to prepare for support of this cryptogram version.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	28
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☒Host Simulator Log
Document Reference:	EMV
Pass Criteria/User Validation:	**Devices Supporting Offline PIN:** The device logs must show: • CVR byte 2 bit 3 = 1 (Offline PIN Verification performed) • CVR, byte 2, bit 2 = 0 (Offline PIN Verification did not fail)

Test Case 28/Test Card 28 (Mandatory; ADVT Online Testing)	
Pass Criteria/User Validation (con't):	**<u>Devices Supporting Online PIN:</u>** The device logs must show: • TVR, byte 3, bit 3 = 1 (Online PIN Entered)
	<u>Offline-Only Devices:</u> **Device must perform a complete transaction without any error messages.** A complete transaction is defined as the performance of all selected VSDC functions from Application Selection through to Completion. Error messages (such as Not Accepted or Card Error) are not acceptable and indicate failure of the test.
	<u>ADVT Online Testing (Online-Capable or Online-Only Devices including ATMs):</u> Device must perform an above floor limit transaction to send the transaction online to a VCMS/VMTS/approved test-host simulator. Online Card Authentication must be successful (Field 44.8 = 2). **The transaction must be approved online.** For ADVT Online Testing, additional requirements (such as providing a Retrieval Reference Number or submitting host logs) may apply and, if applicable, must be submitted in the compliance report via CCRT.

3.29 Test Case 29: Blocked Card

Test Case 29/Test Card 29 (Mandatory)	
Test Case Number:	29
Test Case Name:	Blocked Card
Objective:	To ensure correct terminal behavior for a card that is blocked from use. **Note:** The payment industry best practice recommends that a blocked card must not be accepted through fallback.
Regional Requirement:	Mandatory
Business Justification:	This card is intended to gather information on terminal behavior associated with a blocked card.
Pre-requisite:	
Applicable Terminal Device Type:	☒POS ☒ATM ☒MPOS
Applicable Terminal Interface:	☒Contact ☐Contactless
Test Card:	29
Test Evidence to be Submitted:	☐Receipt (where possible) ☐Card-to-Terminal Interaction Log ☐Host Simulator Log
Document Reference:	EMV 4.3, Book 1, Section 12.4: Final Selection
Pass Criteria/User Validation:	The card must be rejected immediately after insertion with a message such as “Card Blocked” (or equivalent). The device fails this test if it accepts the card via the chip.

A Visa CA Test Public Keys for VSDC

For devices that support offline functionality, these test keys need to be loaded into the terminal to support the tests associated with Offline Data Authentication and Offline Enciphered PIN.

Note: Expiration dates are not defined for test CA Public Keys, and it should not be assumed that a test key has the same expiry date as the live key of the same length. If your Terminal Management System requires expiry dates to be provided for CAPKs then please set the expiry date to 31 December 2025 for all test keys.

Important: Prior to deployment, these keys must be removed from the terminal and replaced with the Visa CA production keys.

A.1 1152 Bit VSDC TEST Key

This key is the Visa CA Public 1152 bit TEST key:

Table A–1: 1152 Bit VSDC Test Key

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	95
Modulus	BE 9E 1F A5 E9 A8 03 85 29 99 C4 AB 43 2D B2 86 00 DC D9 DA B7 6D FA AA 47 35 5A 0F E3 7B 15 08 AC 6B F3 88 60 D3 C6 C2 E5 B1 2A 3C AA F2 A7 00 5A 72 41 EB AA 77 71 11 2C 74 CF 9A 06 34 65 2F BC A0 E5 98 0C 54 A6 47 61 EA 10 1A 11 4E 0F 0B 55 72 AD D5 7D 01 0B 7C 9C 88 7E 10 4C A4 EE 12 72 DA 66 D9 97 B9 A9 0B 5A 6D 62 4A B6 C5 7E 73 C8 F9 19 00 0E B5 F6 84 89 8E F8 C3 DB EF B3 30 C6 26 60 BE D8 8E A7 8E 90 9A FF 05 F6 DA 62 7B
Exponent	03
Secure Hash Algorithm-1 Hash	EE 15 11 CE C7 10 20 A9 B9 04 43 B3 7B 1D 5F 6E 70 30 30 F6
Comments:	The production version of Visa’s 1152-bit CA public key is currently set to expire on December 31, 2015.

A.2 1408 Bit VSDC TEST Key

This key is the Visa CA Public 1408 bit TEST key:

Table A–2: 1408 Bit VSDC Test Key

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	92
Modulus	99 6A F5 6F 56 91 87 D0 92 93 C1 48 10 45 0E D8 EE 33 57 39 7B 18 A2 45 8E FA A9 2D A3 B6 DF 65 14 EC 06 01 95 31 8F D4 3B E9 B8 F0 CC 66 9E 3F 84 40 57 CB DD F8 BD A1 91 BB 64 47 3B C8 DC 9A 73 0D B8 F6 B4 ED E3 92 41 86 FF D9 B8 C7 73 57 89 C2 3A 36 BA 0B 8A F6 53 72 EB 57 EA 5D 89 E7 D1 4E 9C 7B 6B 55 74 60 F1 08 85 DA 16 AC 92 3F 15 AF 37 58 F0 F0 3E BD 3C 5C 2C 94 9C BA 30 6D B4 4E 6A 2C 07 6C 5F 67 E2 81 D7 EF 56 78 5D C4 D7 59 45 E4 91 F0 19 18 80 0A 9E 2D C6 6F 60 08 05 66 CE 0D AF 8D 17 EA D4 6A D8 E3 0A 24 7C 9F
Exponent	03
Secure Hash Algorithm-1 Hash	42 9C 95 4A 38 59 CE F9 12 95 F6 63 C9 63 E5 82 ED 6E B2 53
Comments:	The maximum expiration date for certificates issued using Visa's 1408-bit CA public key is December 31, 2016. Considered to have an anticipated lifetime to at least December 31, 2018.

A.3 1984 Bit VSDC TEST Key

This key is the Visa CA Public 1984 bit TEST key:

Table A–3: 1984 Bit VSDC Test Key

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	94
Modulus	AC D2 B1 23 02 EE 64 4F 3F 83 5A BD 1F C7 A6 F6 2C CE 48 FF EC 62 2A A8 EF 06 2B EF 6F B8 BA 8B C6 8B BF 6A B5 87 0E ED 57 9B C3 97 3E 12 13 03 D3 48 41 A7 96 D6 DC BC 41 DB F9 E5 2C 46 09 79 5C 0C CF 7E E8 6F A1 D5 CB 04 10 71 ED 2C 51 D2 20 2F 63 F1 15 6C 58 A9 2D 38 BC 60 BD F4 24 E1 77 6E 2B C9 64 80 78 A0 3B 36 FB 55 43 75 FC 53 D5 7C 73 F5 16 0E A5 9F 3A FC 53 98 EC 7B 67 75 8D 65 C9 BF F7 82 8B 6B 82 D4 BE 12 4A 41 6A B7 30 19 14 31 1E A4 62 C1 9F 77 1F 31 B3 B5 73 36 00 0D FF 73 2D 3B 83 DE 07 05 2D 73 03 54 D2 97 BE C7 28 71 DC CF 0E 19 3F 17 1A BA 27 EE 46 4C 6A 97 69 09 43 D5 9B DA BB 2A 27 EB 71 CE EB DA FA 11 76 04 64 78 FD 62 FE C4 52 D5 CA 39 32 96 53 0A A3 F4 19 27 AD FE 43 4A 2D F2 AE 30 54 F8 84 06 57 A2 6E 0F C6 17
Exponent	03
Secure Hash Algorithm-1 Hash	C4 A3 C4 3C CF 87 32 7D 13 6B 80 41 60 E4 7D 43 B6 0E 6E 0F
Comments:	This key length is currently considered to have an anticipated lifetime to at least December 31, 2018

B Terminal Action Codes (TACs)

This appendix provides the Terminal Action Codes for terminals. Please refer to Visa 1.4.1 or VIS 1.5, Section 10.2: Terminal Data for additional details.

Table B–1: Terminal Action Codes (TACs)

Terminal Action Code (TAC)	Value
TAC—Denial	0010000000 The TAC value causes a decline for the following condition: • Service not allowed for card product
TAC—Online	DC4004F800 This TAC value generates an online authorization when: • Offline data authentication is not performed or failed • The PAN is on the terminal exception file • The application is expired • An Online PIN is entered • The transaction exceeds the floor limit • The upper (9F23) or lower consecutive offline limit (9F14) is exceeded) • The transaction is randomly selected for online processing • The terminal forced the transaction online • CDA failure
TAC—Default	DC4000A800 This TAC value generates a decline if the transaction cannot be sent online for authorization when: • Offline data authentication is not performed or failed • The PAN is on the terminal exception file • The application is expired • The transaction exceeds the floor limit • The Upper Consecutive Offline Limit (9F23) is exceeded • The merchant forced the transaction online • CDA failure

Markets not supporting offline data authentication in cards may remove the TAC—Online and TAC—Default settings for Offline Data Authentication Not Performed resulting in a TAC—Online value of 584004F800 and a TAC—Default value of 584000A800.

C VSDC Stand-in Processing Conditions

This section provides the VSDC Stand-in Processing Conditions. When the Acquirer is connected to VCMS/VMTS and the transaction associated with one of the ADV Toolkit cards is sent online, VCMS/VMTS will use these conditions to make the online authorization decision.

Note: The Route to Issuer Default is not used as the transaction is processed in Stand-in. Only the Stand-in Authorization Response Defaults are used.

This information is valuable in determining the reason that VCMS/VMTS either approved or declined the online-initiated transaction.

For example, the VSDC Stand-in Authorization Response Default for expired application is “decline offline.” If the application is expired and the transaction is sent online to VCMS/VMTS, VCMS/VMTS will decline the transaction. VCMS/VMTS will indicate the decline in the Response Code (field 39) in the response message.

Note: Currently, there is no VSDC Stand-in Processing Condition for CDA.

Table C–1: VSDC Stand-In Processing Conditions

	Stand-In Condition	Source	Route-to-Issuer Default	Stand-in Author-ization Response Default
1	Transaction exceeds floor limit	TVR	No	Approve
2	Transaction selected randomly for online processing	TVR	No	Approve
3	Cardholder verification failed	TVR	Yes	Decline
4	Unrecognized cardholder verification method	TVR	Yes	Approve
5	Offline PIN verification failed	CVR	Yes	Decline
6	PIN entry required and PIN pad not present or not working	TVR	Yes	Decline
7	PIN entry required, PIN pad is present, but PIN not entered	TVR	Yes	Decline
8	Offline PIN try limit exceeded	CVR or TVR	Yes	Decline
9	Exceeded total, domestic, or international counters	CVR	Yes	Approve
10	Lower consecutive offline limit exceeded	TVR	Yes	Approve

	Stand-In Condition	Source	Route-to-Issuer Default	Stand-in Authorization Response Default
11	Upper consecutive offline limit exceeded	TVR	Yes	Approve
12	Expired application	TVR	Yes	Decline
13	Application not yet effective	TVR	Yes	Decline
14	Issuer Authentication failed on last transaction	CVR	Yes Issuer **cannot** modify	Approve
15	SDA failed	TVR	Yes Issuer **cannot** modify	Decline
16	Offline Data Authentication not performed Note: Not applicable to ATM transactions	TVR	Yes Issuer **cannot** modify	Approve
17	SDA failed on last transaction and was declined offline	CVR	Yes Issuer **cannot** modify	Approve
18	Script update succeeded on last transaction	CVR	Yes Issuer **cannot** modify	Approve Issuer **cannot** modify
19	Script update failed on last transaction	CVR	Yes Issuer **cannot** modify	Approve
20	Merchant forced transaction online	TVR	Yes	Decline
21	New card (first use)	CVR	Yes	Approve
22	Magnetic stripe read of VSDC card at VSDC terminal	*	Yes Issuer **cannot** modify	Approve
23	Last online transaction not completed	CVR	Yes	Approve
24	Card Authentication failure and Card Authentication reliable	**	Yes Issuer **cannot** modify	Decline

	Stand-In Condition	Source	Route-to-Issuer Default	Stand-in Author-ization Response Default
25	Card Authentication failure and Card Authentication unreliable	**	Yes Issuer **cannot** modify	Decline
26	Card Authentication not performed and Card Authentication unreliable	**	Yes Issuer **cannot** modify	Decline
27	DDA failed	TVR	Yes Issuer **cannot** modify	Decline
28	DDA failed on last transaction and was declined offline	CVR	Yes Issuer **cannot** modify	Approve

D Merchant Terminal Environments

This appendix outlines the following merchant terminal environments:

- Stand-Alone Terminals (SATs)
- Stand-Alone Terminals (SATs) with Semi-Integrated Functionality
- Fully Integrated Environments
  - Integrated: POS to Acquirer
  - Integrated: In-Store Controller to Acquirer
  - Integrated: Regional Network Controller to Acquirer

The EMV chip implementation process for POS environments and subsequently its testing requirements will vary according to merchant type, size, and complexity of the payment system infrastructure. Since merchant POS environments can be as simple as a stand-alone payment terminal at a small retailer, or as complex as a series of interconnected state-of-the-art large retailer systems, this section is intended to provide a general overview of the range of payment terminal environments. It gives users a sense of the impact of incorporating EMV functionality into these different environments and the testing implications.

D.1 Stand-Alone Terminals (SATs)

Separate from a merchant's electronic cash register, a stand-alone payment terminal serves the primary purpose of requesting authorizations and clearing payment card transactions. Typically merchant-facing, it may also include a customer-facing device (e.g., PIN Pad for customer PIN entry). Since the stand-alone terminal is usually supplied and managed by merchant acquirers, in many cases it contains acquirer-specific transaction functionality within its payment application.

For smaller merchants, a stand-alone payment terminal POS is usually not connected to their electronic cash register, but directly to an acquirer's host processor via a Public Switched Telephone Network (PSTN) or internet connection. Slightly larger merchants may, however, have their stand-alone payment terminal directly connected to their electronic cash register.

Figure D–1: Stand-Alone Terminal

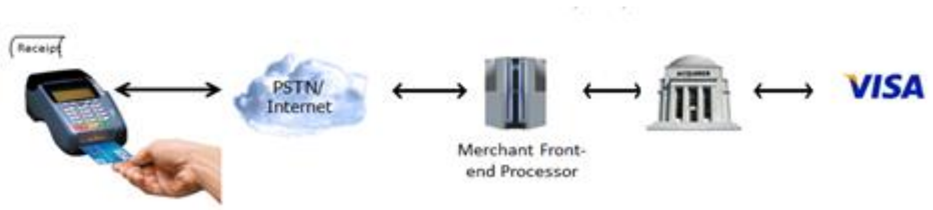
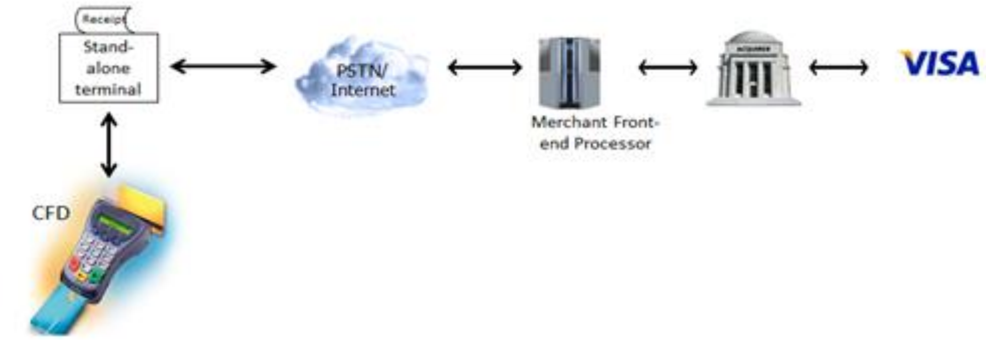


Figure D–2: Stand-Alone Terminal (SAT) with Cardholder-Facing Device



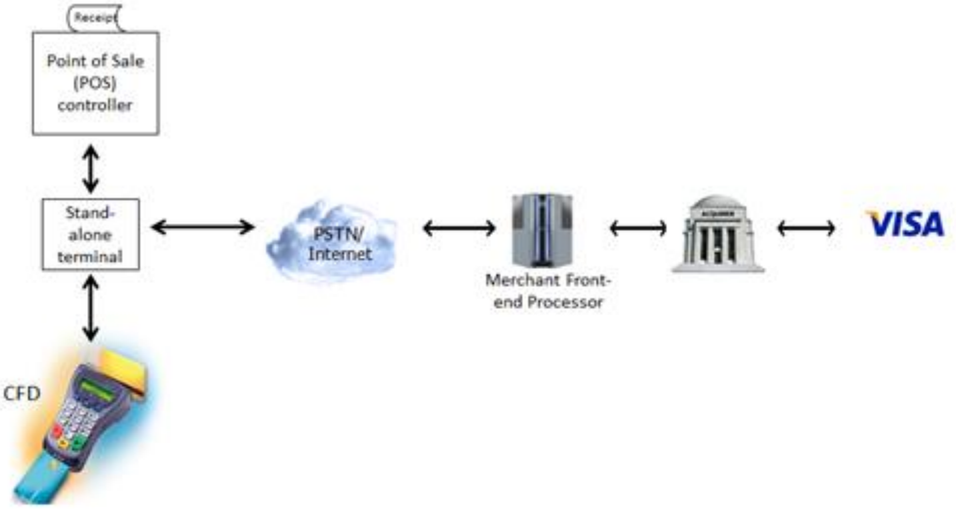
Characteristics of Stand-Alone Terminals:

- Mostly merchant facing, but may include a customer-facing device (PIN Pad); typically no signature capture
- If a PIN Pad is connected, it typically contains a chip card reader but not a magnetic stripe reader
- Typically connected directly to a host processor
- Used mostly by smaller merchants (US Tier 4-5)

D.2 Stand-Alone Terminals (SATs) with Semi-Integrated Functionality

Stand-alone terminals with semi-integrated functionality typically utilize a customer-facing device that interfaces with a POS system. The acquirer-specific transaction functionality generally resides either within the payment application of the customer-facing device or in other “middleware” that is physically and logically separated from the POS system.

Figure D–3: Stand-Alone Terminal (SAT) with Semi-Integrated Functionality



Characteristics of Stand-Alone Terminal with Semi-integrated Functionality:

- POS provides only the sale amount of the transaction but it is not involved in the processing of the payment transaction
- No payment card data is routed through the POS
- POS provides inventory management
- EMV code typically resides in the customer-facing device (PIN Pad)

D.3 Fully Integrated Environments

In the fully integrated merchant environments, the card acceptance device is usually customer-facing and is connected to and driven by logic that resides or co-resides in the POS system. All the acquirer-specific transaction logic is embedded within or behind the POS system and not within the customer-facing device.

This environment is typically implemented by the larger retailers and chain stores.

Figure D–4: Integrated—POS to Acquirer

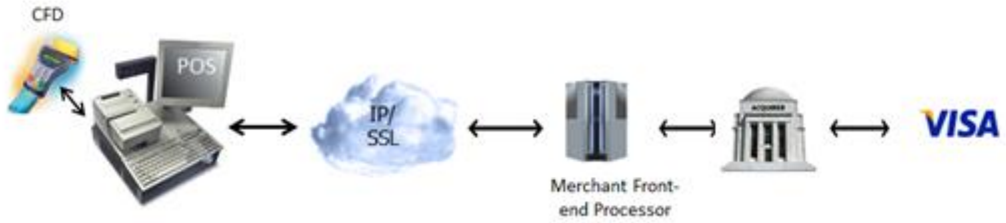


Figure D–5: Integrated—In-Store Controller (ISC) to Acquirer

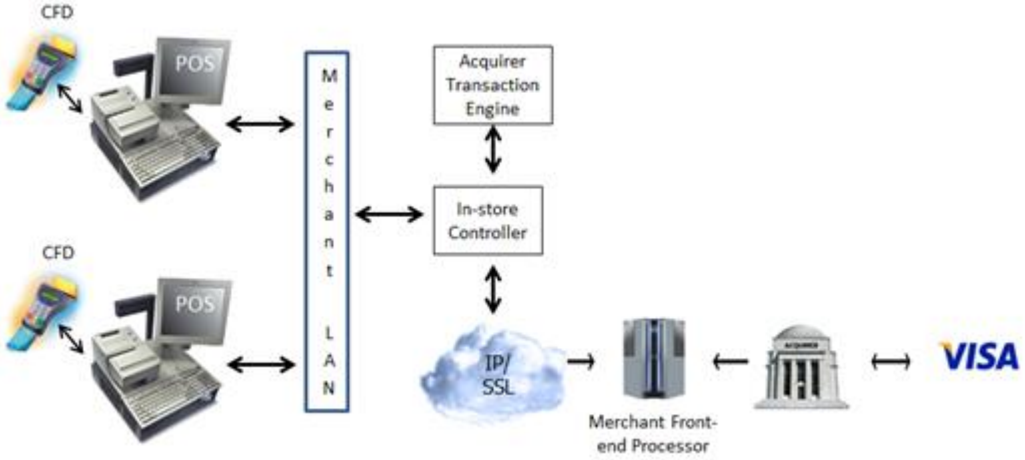
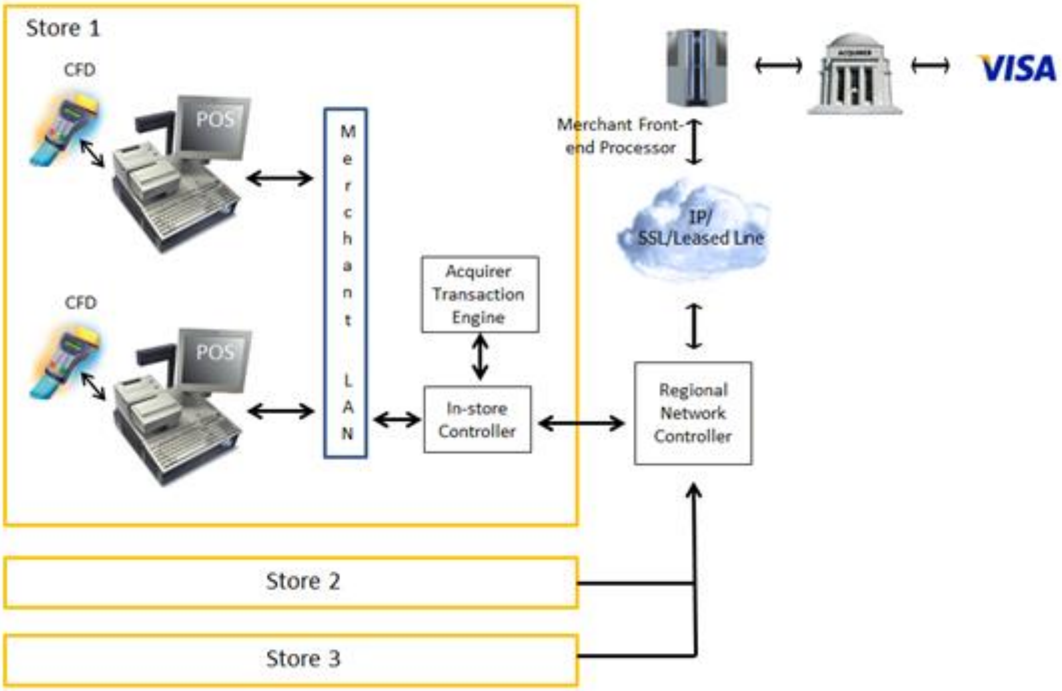


Figure D–6: Integrated—Regional Network Controller to Acquirer



Characteristics of Integrated Environments:

- Payment card data routes from customer-facing device to POS system, through other merchant systems (as needed), and to the acquirer
- The customer-facing device may be capable of signature capture
- The majority of devices are connected serially; some use Ethernet

E ADVT Testing Use Cases

This appendix provides frequently asked questions related to ADVT testing.

Note: All references to ADVT testing refer to completion of all the test cases in the toolkit.

Although the list of use cases provided in this appendix is not exhaustive, it includes real-world scenarios taken from user queries. Users should consult with their Visa representative for further clarifications on any remaining uncertainties or scenarios not specifically covered here.

For more information, refer to Section 1.5.1: ADVT Usage Guidelines. This section outlines the situations where ADVT testing is required, recommended, and not required.

E.1 Use Cases

This section provides use cases on the following:

- General Terminal Use Cases
- Acquirer/Processor Platform Use Cases
- System Integrator and Value-Added Reseller (VAR) Use Cases

A terminal can be any EMV chip capable terminal, peripheral card reader (such as a PIN pad, where the peripheral contains some or all of the Level 1 or Level 2 functionality), or an ATM unless noted otherwise. Terminals can also be other terminal types as defined in EMV, including POS terminals, bank branch terminals (BBTs), unattended terminals, and onboard devices (e.g., handheld terminals on airplanes).

E.1.1 General Terminal Use Cases

This section provides general terminal use cases.

Table E–1: General Terminal Use Cases

	General Terminal Use Cases
Q1	**Multiple Terminal Vendors** If I deploy terminals by multiple terminal vendors, do I need to test each terminal configuration by vendor?
	Yes. ADVT testing is required for each terminal configuration. Also, if there are any changes to the payment application affecting chip processing or the EMV kernel by terminal configuration, then retesting is required.
Q2	**Same Stand-Alone Terminal Deployed at Multiple Merchant Locations** I am an acquirer planning to deploy stand-alone terminals at multiple merchant locations, all with the same terminal type, payment application, EMV kernel, and payment transaction flow. Do I need to repeat ADVT testing at each merchant location?
	No. As long at the payment infrastructure remains the same across numerous merchants or merchant locations, then ADVT testing is only required once.
Q3	**Terminal Family** If I perform ADVT testing on a single terminal vendor product line, which has the same EMV kernel and payment application as other terminal models, do I need to test each one?
	No. If the payment application, EMV kernel, and chip transaction flow are the same in each individual POS model then this would be considered a "terminal family" and can be tested once. Please consult with the terminal vendor to ensure a group of terminals fall within the same family.
Q4	**New Communication Types** My terminal supports different communication types (e.g., Bluetooth, General Packet Radio Service (GPRS), internet, dial-up). Do I need to perform ADVT testing for each communication type?
	No. Only one set of ADVT testing per terminal family is required as long as the communication type is the only change. Consult with the terminal vendor for information on whether a group of terminals fall within the same terminal family.
Q5	**EMV Level 1 Hardware Changes** Do I need to perform ADVT retesting if there are changes to EMV Level 1 hardware on my device, which does not impact the EMV chip processing in the payment application or the EMV kernel?
	No. This constitutes a "minor change". Refer to the "Not Required" section in Section 1.5.1: ADVT Usage Guidelines.

	General Terminal Use Cases
Q6	**EMV Level 1 or Level 2 Approval Expiration** What happens when the Level 1 or Level 2 approval on my terminal expires?
	Visa does not require that deployed terminals with expired Level 1 or Level 2 approvals be replaced or updated. However, updates to software in existing terminals should be reviewed against Section 1.5.1: ADVT Usage Guidelines. Update of terminal software may require replacement or upgrading of expired Level 1 or 2 components. Alternatively, the vendor of the EMV kernel or chip reader (Level 1) may be able to renew the EMV Level 1 or Level 2 approval.
Q7	**Off-the-Shelf Terminal with EMV Approvals** I purchased an off-the-shelf chip terminal with EMV approvals. Do I still need to perform ADVT testing?
	Yes. ADVT testing will ensure overall system integration of the device. It will validate that the data from the card is correctly transmitted to the acquirer host, data from the acquirer host is correctly returned to the card, and the device meets Visa requirement.
Q8	**Upgraded Peripheral—New EMV Kernel** Does upgrading to a new version of a peripheral (such as a PIN pad with a new EMV kernel) require retesting?
	Yes. If the peripheral contains EMV Level 2 (kernel) functionality, ADVT retesting is required.
Q9	**Upgraded Peripheral—No EMV Kernel Changes** I am upgrading to a new version of a peripheral that does not involve changes to EMV chip processing but does involve other changes, such as changing prompts displayed to the customer. Do I need to retest with the new version of the peripheral?
	No. If EMV chip functionality is not impacted, ADVT retesting is not required.
Q10	**Upgraded Peripheral—New PIN Pad** Does upgrading to a new peripheral, such as a PIN pad require retesting?
	ADVT retesting is required when changes affect EMV chip processing. If the peripheral contains the chip reader (Level 1) or any part of the EMV kernel (Level 2), retesting is required. This would include a peripheral that supports Offline PIN. However, if the peripheral does not include any EMV functionality, such as a PIN pad that only supports Online PIN, retesting is not needed.
Q11	**Payment Application Changes—Magnetic Stripe Only** I will be making changes to the payment application which will impact magnetic stripe functionality only, do I need to retest?
	No. However, it is recommended that you perform the fallback related tests to ensure that chip and magnetic stripe functionality is invoked when required.
Q12	**Non-Payment Changes to Integrated POS** Do changes to an integrated POS that are not payment related require ADVT retesting (i.e., changes to the physical or logical interface between the cash register and the payment terminal)?
	No. ADVT retesting is not required in these cases.

	General Terminal Use Cases
Q13	**Portfolio Changes** Do I need to retest if the portfolio changes? For example, in the US market, my Independent Sales Organization (ISO) may sell or buy a portfolio and change where the device is pointing or change my merchant ID or terminal ID.
	If routing of the transaction is effected with a different gateway or acquirer processor, then ADVT testing **must** be performed. If the changes are only related to the terminal management system, ADVT testing is **not** required.
Q14	**Operating System Changes** If there are changes to my operating system (for example, Windows XP to Windows 7) do I need to repeat ADVT testing?
	If this is the only change and there are no changes to the payment application impacting EMV chip processing or the EMV kernel, then ADVT retesting is not required. However, if a new EMV kernel is required to support the new operating system, then ADVT retesting will be required.
Q15	**ADVT Scheduling** When performing ADVT testing, does an acquirer need to schedule testing with Visa?
	No. ADVT is considered self-service testing and does not require scheduling with Visa. You can perform the testing at your convenience. However, new acquirers need to ensure chip parameters are set up in Visa's test environment.
Q16	**ADVT Test Results Submission** Can I submit the test results without using the Chip Compliance Reporting Tool (CCRT)?
	No. CCRT must be used to submit test results.
Q17	**New Service (e.g., Dynamic Currency Conversion or Cash-Back)** If adding an additional service, such as dynamic currency conversion or cash-back, do I need to repeat required testing?
	Yes. Retesting ADVT will be required since there are impacts to the payment component of the terminal application for chip processing and the EMV kernel.
Q18	**Contactless Testing** Can the ADVT be used for testing contactless?
	No. ADVT is not used to test contactless terminal functionality. Contact your Visa representative for contactless testing requirements.
Q19	**New Non-Payment Application** Do changes to a non-payment related application (e.g., a loyalty program) on the device require ADVT retesting?
	No. Changes to non-payment applications are outside the scope of ADVT testing.

	General Terminal Use Cases
Q20	**Repaired/Replaced Terminals** When terminals break and are sent for repair and replacement, they are recycled back into stock, is ADVT testing required?
	No. As long as there were no software code changes impacting chip processing or the EMV kernel, ADVT testing is not required.

E.1.2 Acquirer/Processor Platform Use Cases

This section provides use cases for acquirer/processor platforms.

Table E–2: Acquirer/Processor Platform Use Cases

	Acquirer/Processor Platform Use Cases
Q1	**Visa Business Enhancements** When changes are applied to my platform as a result of Visa's bi-annual business release, do I need to perform any ADVT re-testing?
	No. In general, no ADVT retesting is required as a result of business release changes unless specified in the *Business Enhancement Technical and Implementation Guide*.
Q2	**Network Switch Upgrade** I am upgrading my network switch (i.e., the system which processes and routes data at the data link layer) to support changes from my supplier. Do I need to repeat ADVT testing?
	Retesting may be required, depending on the areas that are affected. Review Section 1.5.1: ADVT Usage Guidelines and consult with your Visa representative.
Q3	**New Platform** I am changing my payment platform to a different network switch vendor's platform using a different transaction message. Do I need to repeat ADVT testing?
	Yes. This is a major change and ADVT testing must be repeated.

E.1.3 System Integrator and Value-Added Reseller (VAR) Use Cases

This section provides use cases for System Integrators and Value-Added Resellers (VARs).

Table E–3: System Integrator and Value-Added Reseller (VAR) Use Cases

	System Integrator and Value-Added Reseller (VARs) Use Cases
Q1	**Inventory Management System Changes** In an integrated payment environment, if there are changes to an inventory management system within the payment application, would this require the terminal to be retested? For example, a retail and restaurant management systems' integrated payment application would include the inventory system. If a change is made to the inventory system, it will impact the payment application but not chip processing.
	Modularizing applications in these environments is recommended to protect the payment application and, provided this approach has been followed, no retesting would be required. Changes that affect the EMV kernel or chip processing, however, will necessitate ADVT retesting. Refer to Appendix D: Merchant Terminal Environments for examples.
Q2	**Application Programming Interface Changes** I am using a middleware application for EMV. If I update my Application Program Interface (API), do I need to repeat ADVT testing?
	No. Retesting is only required if the changes impact the payment application for chip processing or the EMV kernel. However, retesting is recommended as middleware changes often impact payment processing.
Q3	**New Peripheral Device** I've added a new payment peripheral device (for example, a printer or barcode reader) to my processing chain. Do I need to repeat ADVT testing?
	No. ADVT retesting is not required as long as the peripheral is not involved in EMV processing.
Q4	**Payment Application Change** The version of my payment application has changed but the device hardware version has not. Do I need to repeat ADVT testing?
	Yes. Whenever there is a change to the payment application impacting chip processing or the EMV kernel, retesting is required.

F Acronyms and Glossary

This appendix provides a list of acronyms used in this document and in EMV as well as a glossary of terms.

Table F–1: Acronyms

Acronym	Meaning
a	alpha
AAC	Application Authentication Cryptogram
AAR	Application Authentication Referral
ADA	Application Default Action
ADF	Application Definition File
ADVT	Acquirer Device Validation Toolkit
AEF	Application Elementary File
AFL	Application File Locator
AID	Application Identifier
AIP	Application Interchange Profile
an	alphanumeric
ans	alphanumeric special
APDU	Application Protocol Data Unit
API	Application Priority Identifier
ARPC	Application Response Cryptogram
ARQC	Application Request Cryptogram
ATC	Application Transaction Counter
ATM	Automated Teller Machine
AUC	Application Usage Control
b	binary
BIN	Bank Identification Number
CA	Certificate Authority
CAM	Card Authentication Method
CAT	Cardholder Activated Device
CDA	Combined Dynamic Data Authentication

Acronym	Meaning
CDOL	Card Risk Management Data Object List
CID	Cryptogram Information Data
cn	compressed numeric
CSV	Comma-Separated Values
CVK	Card Verification Key
CVM	Cardholder Verification Method
CVR	Card Verification Result
CVV	Card Verification Value
DDA	Dynamic Data Authentication
DDF	Directory Definition File
DDOL	Dynamic Data Authentication Data Object List
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DGI	Data Group Identifier (used by the Card Personalizer only)
DKI	Derivation Key Index
EMV	Europay, MasterCard & Visa
FCI	File Control Information
GPO	Get Processing Options
hex.	Hexadecimal
IAC	Issuer Action Code
ICVV	Alternate Card Verification Value
IFM	Interface Module
MCC	Merchant Category Code
MDK	Master Derivation Key
MPOS	Mobile Point of Sale Device
N/A	Not Applicable
n	numeric
PAN	Primary Account Number
PDOL	Processing Options Data Object List
PIN	Personal Identification Number

Acronym	Meaning
PIX	Proprietary Application Identifier Extension
PK	Public Key
PKI	Public Key Infrastructure
PKI	Public Key Index
POS	Point of Sale
PSE	Payment Systems Environment
PSTN	Public Switched Telephone Network
PVK	PIN Verification Key
PVV	PIN Verification Value
RFU	Reserved For Future Use
RID	Registered Application Provider Identifier
RSA	Rivest, Shamir, Adleman
RRN	Retrieval Reference Number
SAD	Signed Static Application Data
SAM	Secure Access Module
SDA	Static Data Authentication
STIP	Stand-In Processing
TAC	Terminal Action Code
TC	Transaction Certificate
TDOL	Transaction Certificate Data Object List
TITF	Terminal Integration Task Force
TLV	Tag-Length-Value
TSI	Transaction Status Information
TVR	Terminal Verification Result
UAT	Unattended Acceptance Device
UCAT	Unattended Cardholder Acceptance Device
UDK	Unique Derived Key
var.	variable
VCMS	Visa Certification Management Service
VIP	VisaNet Integrated Payment

Acronym	Meaning
VLP	Visa Low-value Payment
VMTS	Visa Member Test System
VSDC	Visa Smart Debit/Credit
VTS	VisaNet Test System
XML	Extensible Mark-up Language
XSD	XML Schema Definition

Table F–2: Glossary

Term	Definition
Application Protocol Data Unit (APDU	The communication format used between the chip card and the payment application on a card acceptance device. This format is defined in ISO specification 7816.
Automated Teller Machine (ATM)	An unattended device that has electronic capability to send transactions online for authorization, accepts PINs, and disburses currency.
Card Acceptor Terminal	See "Terminal."
Card/Terminal Log	A capture of the interaction between the card/card simulator and the device. Typically provided in Application Protocol Data Unit (APDU) format.
Card/Terminal Log Validation	A Test Plan-defined description of the requirements for elements and content of the card/terminal log to be validated during terminal integration testing.
Cardholder Activated Device	An unattended device, such as an automated dispensing machine, self-service device, or limited amount device that is not an ATM.
Certification	Validation that the format, function, and content of authorization messages executed from a defined test plan adheres to a provided specification and set of business rules.
Chip-Capable	A transaction acceptance device that is designed and constructed to facilitate the addition of a chip reader/writer.
Chip-Enabled	For chip cards, this describes the state in which the card has already been personalized with both cardholder and Brand-specific data in preparation for use. For terminals, this describes the state in which the terminal has already been equipped with a chip reader/writer and has been configured with Brand-specific data and is ready for use in accepting chip cards.

Term	Definition
Comma-Separated Values (CSV)	A format that stores tabular data (numbers and text) in plain-text form (i.e. a sequence of characters, with no data that has to be interpreted instead, as binary numbers). A CSV file consists of any number of records, separated by line breaks of some kind; each record consists of fields, separated by some other character or string, most commonly a literal comma or tab. Usually, all records have an identical sequence of fields.
Contact Transaction	An interaction between a chip application and a device using the physical electrical interface, as defined in [EMV Book 1].
Contactless Transaction	An interaction between a chip application and a device using the radio frequency wireless interface, as defined in [EMV CL].
Customer Activated Terminal (CAT)	See "Cardholder Activated Device."
EMVCo LLC (EMVCo)	Industry organization that manages, maintains, and enhances the EMV Specifications. Current Members are American Express, JCB International, MasterCard Worldwide, UnionPay, and Visa Inc.
EMV Specifications	Technical specifications developed and maintained by EMVCo to create standards and ensure global interoperability for use of chip technology in the payment industry. In order to support EMV, cards and terminals must also meet the requirements described in the bulletins available on the EMVCo website.
Host Authorization Message	A description of the transaction message initiated from the device and sent online via the acquirer and network to the issuer, processor, or Brand for transaction authorization.
Host Authorization Message Validation	A Test Plan-defined description of the requirements for elements and content of the Host Authorization Message to be validated during standalone or terminal integration testing.
Implement	To make a card, application, or device capable of performing a functionality. Functionality that is implemented may also need to be enabled (see *Chip-enabled*).
Interoperability	The ability of all card acceptance devices to accept and read all chip cards that are properly coded and personalized.
Kernel	EMV definition for the set of functions required to be present on every terminal implementing a specific interpreter. The kernel contains device drivers, interface routines, security and control functions, and the software for translating from the virtual machine language to the language used by the real machine. In other words, the kernel is the implementation of the virtual machine on the real machine.
Limited Amount Device	An unattended device that has data capture-only capability, and accepts payment for items such as parking garage fees, road tolls, etc.
Mobile Point of Sale (MPOS)	A smartphone, tablet, or dedicated wireless device that performs the functions of a cash register or electronic point of sale terminal (POS terminal).

Term	Definition
Offline-Capable	A transaction acceptance device that has the ability to process the transaction offline for card authentication and authorizations.
Offline-Only	A transaction acceptance device that is only able to process the transaction offline for card authentication and authorizations.
Online-Capable	A transaction acceptance device that is able to send transactions to the issuer or processor for authorizations.
Online-Only	A transaction acceptance device that requires that all transactions be sent online for authorization.
PAN Key Entry	A manual procedure in which the merchant uses a device key pad to enter the PAN embossed on a card in order to process a transaction.
Pass Criteria	A Test Plan-defined field that describes an expected result for a successful outcome or conclusion of a test case.
Pass Criteria File	The file (in CSV format) that embeds the Brand-defined pass criteria for each test case.
Personalization	For chip cards, the process of applying both cardholder and Brand-specific data to the card in preparation for its use.
Point of Sale	The physical location where a merchant or acquirer in a face-to-face environment or an unattended device completes a transaction.
Point-of-Sale Device	A device used at the POS to process transactions, including chip devices, automated dispensing machines, self-service devices, and ATMs.
Terminal	The device used in conjunction with the chip card at the point of transaction to perform a financial transaction. The terminal incorporates the interface device and may also include other components and interfaces such as host communications.
Terminal Configuration	A description of the features and parameters on the acceptance device under test. For example, it might include the EMV-defined terminal types, supported interfaces, etc.
Terminal Integration Testing	A process implemented and managed by the respective Brands, aimed at providing a level of assurance that Brand-specific requirements and recommendations are being implemented in contact or contactless chip acceptance devices that will accept a Brand’s products.
Terminal Integration Task Force (TITF)	Task Force established by EMVCo in 2013 with the purpose of examining each of the Brand’s terminal integration processes, in order to determine the possibilities of aligning key elements of these processes.
Test Card Image	An electronic representation of a physical card.
Test Case	A Test Plan-defined description of a test scenario, defined by a Payment Brand for execution of terminal integration or host message testing.
Test Case Name	A Test Plan-defined description of the name associated with a specific test case.
Test Case Number	A Test Plan-defined unique test case identifier.

Term	Definition
Test Case Objective	A Test Plan-defined description of the objective of performing a given test case.
Test Plan	A Brand-developed and managed set of test criteria that defines the requirement for terminal integration or host message testing. This may either take the form of a textual document or a machine-readable file.
Test Procedure	A Test Plan-defined description of the steps required in order to execute a specific test case.
Test Tool Confirmation	The process undertaken by each Brand to provide themselves, tool vendors, and clients will a level of assurance that the tools being used by clients to execute terminal integration testing will do so in compliance with Brand requirements. Process is also referred to as "Test Tool Qualification."
Test Tool Qualification	The process undertaken by each Brand to provide themselves, tool vendors, and clients will a level of assurance that the tools being used by clients to execute terminal integration testing will do so in compliance with Brand requirements. Process is also referred to as "Test Tool Confirmation."
Transaction Completion	An EMV definition for the successful closing of transaction processing. The completion function is always the last function in transaction processing and must occur unless the transaction is terminated prematurely by error processing.
Unattended Cardholder Activated Terminal (UCAT)	A cardholder-operated device that reads, captures, and transmits card information in an unattended environment. Also known as "Customer Activated Terminal (CAT)" or "Unattended Acceptance Device (UAT)."
User Validation	A Test Plan-defined description of the requirements for the user/tester to validate responses from the device under test.
Extensible Mark-up Language (XML)	A mark-up language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.