Visa Smart Debit/Credit and Visa payWave

U.S. Acquirer Implementation Guide

Version 2.2

November 2016

Visa Public

Important Information

This document is provided as a guide and tool to be used in conjunction with Visa's rules; it is proprietary to Visa.

THIS GUIDE IS PROVIDED ON AN "AS IS," "WHERE IS," BASIS, "WITH ALL FAULTS" KNOWN AND UNKNOWN. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VISA EXPLICITLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE LICENSED WORK AND TITLES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

Contents

Tables

Figures

About This Guide

This guide is designed to help U.S. acquirers prepare the terminal, host and back-office infrastructure to support a combined Visa Smart Debit/Credit (VSDC) and Visa payWave program. Because the U.S. is an always online or 'zero floor limit' environment, the cost and complexity of a traditional chip implementation is reduced. This guide includes:

- Best practices, suggestions, considerations and descriptions of step-by-step activities to assist with the implementation.
- Information to assist acquirers in supporting their merchants as they migrate to chip.
- A Section on implementation activities to highlight the support required in each section.

Given the nature of the U.S. payment environment, where all transactions are authorized online, this guide focuses solely on the implementation requirements relating to online-only terminals and does not discuss offline processing requirements in detail.

This guide also outlines requirements for supporting VSDC and Visa payWave using the qVSDC and MSD paths.

This guide references a number of other Visa and industry documents that are essential for implementing a chip program. Refer to Appendix C: Reference Materials.

Out of Scope

This guide is not intended to aid acquirers in making the decision to begin deployment of chip devices but instead to provide information on benefits and features of the service and in-depth educational background on chip cards, terminals or systems.

This guide will not address the capability of other networks to carry full chip data if the transaction is routed over a non-Visa network.

It does not address requirements relating to:

- Tasks related to implementing a new card acceptance program.
- Offline Processing: Acquirers considering offline processing support should review the global *VSDC Acquirer Implementation Guide* and the *Visa payWave Acquirer Implementation Guide*. Note: Offline chip approvals for transactions accepted in the U.S. do not provide protection against chargebacks, including No Authorization chargebacks.
- Support for Visa Contactless Payment Specification (VCPS) 1.4.2 readers.
- Chip processing at ATMs.

Assumptions

This document assumes that the:

- Acquirer currently accepts Visa cards at its terminals.
- Acquirer currently accepts Visa Interlink cards at its terminals.
- Acquirer is familiar with V.I.P. processing requirements.
- Acquirer is connected to VisaNet.
- Acquirer has an established mechanism for installing and configuring all devices.

Audience

The *Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide* is intended for acquirers, acquirer processors, and direct connect merchants in the U.S. responsible for the implementation, testing and activation of a dual-interface acceptance program combining support for VSDC and Visa payWave.

Document Organization

Section 1: Overview—This Section provides an overview of chip technology and the EMV global foundation for chip-based payment services.

Section 2: VSDC Transaction Flow—This Section describes the VSDC chip transaction steps at the terminal/card level and the host level.

Section 3: Visa payWave Transaction Flow—This Section describes the Visa payWave steps at the terminal/card level and the host level.

Section 4: Visa's Chip Terminal and Reader Requirements—This Section describes the requirements for deploying EMV-compliant VSDC terminals and VCPS compliant contactless readers.

Section 5: Additional Terminal Considerations—This Section discusses the additional consideration for the requirements outlined in Section 2.

Section 6: Terminal Selection and Approval—This Section is intended to assist acquirers in creating selection criteria for chip terminals and provides background information on the terminal approval process before deployment in the field.

Section 7: Terminal Testing and Maintenance—This Section outlines Visa's recommendations for acquirers to undertake post deployment testing to address and resolve acceptance and interoperability problems that may be inadvertently introduced during rollout.

Section 8: Terminal Management Systems—This Section provides the recommended functions to be supported by a Terminal Management System (TMS) in a chip environment.

Section 9: Acquirer System Changes—This Section outlines acquirer system changes to support EMV chip.

Section 10: Acquirer Host Testing—This Section addresses acquirer host testing to support VSDC and Visa payWave transactions. It assumes the acquirer is already a VisaNet endpoint.

Section 11: Acquirer Back-Office Changes—This Section addresses the technical changes to back-office functions that acquirers will need to support an EMV chip program.

Section 12: Merchant Support—This Section reviews the tasks related to supporting merchants as they make the transition to chip card acceptance. It focuses on the merchant support needs in areas such as system changes and training.

Appendix A: Planning Checklist—This Appendix is designed to help acquirers plan the implementation of their chip program and develop a detailed work plan.

Appendix B: V.I.P. System Message Requirements—This Appendix outlines the mandated tags that must be supported, and the related chip fields.

Appendix C: Reference Materials—This Appendix lists all the key guides referenced throughout the document.

Appendix D: Basic EMV Terminal Logic—This Appendix provides an overview of basic EMV terminal logic.

Appendix E: Special Terminal Logic—This Appendix includes the special terminal logic that is necessary for a merchant to determine the AID to be selected for an eligible transaction. Also this appendix illustrates the special contact terminal CVM logic that is necessary for a merchant participating in Visa's VEPS program or a merchant that supports cash-back.

Summary of Changes Since Version 2.1

This section highlights the major changes made to the document for this version:

Table 1: Summary of Changes

Changes	Sections
Sections updated to clarify implementation options related to the adoption of EMV chip technology in the U.S.	Section 2.2: Application Selection Section 2.2.1: Visa U.S. Common Debit AID and Customized Application Selection Section 3.5.1: Preliminary Processing Section 3.5.2: Application Selection Section 3.6.1: Application Selection Section 4.2.3.1: Implementation Activities Section 4.4.1: Contact EMV Application Selection Section 4.4.2: Application Initiation and Cardholder Selection/Confirmation and Section 4.4.2.1 Implementation Activities Section 4.4.5: Cardholder Verification Section 4.5.1: Application Selection Options Section 4.5.1.1: Contactless Reader Application Selection and Routing Option Logic Section 4.5.5: Reader Cardholder Verification Method – qVSDC Section 5.7: Transaction Routing Section 12.7.2: Cardholder Selection Section 12.7.3.2: PIN Appendix D: Basic EMV Terminal Logic Appendix E: Special Terminal Logic

Changes	Sections
Clarifications and updates to other sections	Section 3.2: U.S. Contactless Acceptance requirements (clarification on MSD and qVSDC requirements) Section 3.5.1: Preliminary Processing Section 3.6.5: MSD CVM Processing Section 4.3 Language Processing and 4.3.1 Implementation Activities Section 4.4.3: Contact Application Selection and Routing Options (DF Name requirements) Section 4.5.2: Transaction Speed (speed requirements apply to MSD) Section 4.5.8: Online Card Verification (cryptogram version numbers added and processing clarified) Section 5.1.2.2: Avoiding False Fallback Indication During Migration (new section) Section 5.1.2.3: Fallback Implementation Activities (two new VisaVue reports added) Section 5.2.3: DF Name (data element mandatory) Section 5.6: Cardholder Receipt Requirements Section 5.9: Deferred Authorization Section 5.10.5: Refunds Section 5.11: EMV Transactions in Specific Industries Section 6.1: Terminal and Reader Selection Criteria Section 6.6: Acquirer Device Validation Toolkit Section 6.6.2: ADVT and Expired EMV Approvals Section 6.6.3: ADVT and CDET Ordering Process Section 6.4: Contactless Device Evaluation Toolkit Section 6.6.5: Chip Compliance Reporting Tool Section 6.7: Additional Toolkit Requirements Section 6.8: Visa Chip Enabled Vendor Service (CVES) Section 6.9: Visa U.S. Chip Acquirer Self-Accreditation Service (new section) Section 6.9.1: Eligibility Requirements (new section) Section 6.9.2: Attestation Processing (new section) Section 6.10: Acquirer Host Testing Section 7.3: Chip Interoperability Compliance Program Section 8.2.4: Contactless CVM Limit Section 9.2.1: Data Requirements Section 12.2: Merchant Registration (section deleted) Section 12.3: Contactless Reader Migration Appendix B: V.I.P. System Message Requirements (DF Name added to table)

1. Overview

New technology is presenting Visa with exciting opportunities to provide enhanced payment services. Chip technology based on EMV can help prevent the compromise of sensitive cardholder data while providing consumers and merchants with fast and convenient ways to complete purchases across various form factors including mobile.

Because EMV provides a global foundation for chip-based payment services, adherence to its specifications ensures global interoperability and offers enhanced security and greater functionality to today's Visa products. Using the EMV foundation layer, Visa has developed additional specifications, for example, the Visa Integrated Circuit Card Specification (VIS), the Visa Contactless Payment Specification (VCPS) and payment service rules and implementation guidelines. Visa Smart Debit/Credit (VSDC) is a program specifically designed to aid Visa acquirers in migrating magnetic stripe Visa card programs and acceptance infrastructure to a chip-based payment service.

Additionally, Visa payWave provides a flexible and globally interoperable approach to contactless transactions. It offers several implementation options – all while ensuring the Visa payWave cards and other contactless form factors receive the same level of acceptance whether used at home or abroad.

To implement acceptance for VSDC and Visa payWave, as part of their migration to chip, acquirers will need to consider various changes to their existing terminals and host processing, including:

- New terminal applications and support for selectable EMV kernels
- Compliance with Visa and industry requirements for contact and contactless chip terminals
- Testing and approval processes for chip terminals
- Changes to terminal and host messaging
- Changes to host systems to process new or additional data
- Back office changes
- Impact to merchants and additional training

Note: The term "acquirer," as used in this Guide, will be defined as the acquirer or acquirer processor.

1.1 Compliance Documents and Reference Documentation

To facilitate requirements while ensuring global interoperability, terminals accepting Visa cards must comply with the following documents:

- *Visa Rules*
- *Visa Transaction Acceptance Device Requirements*

Note: Certain requirements related to Application Selection and routing logic do not apply to U.S. Covered Visa Debit Cards.

Note: Refer to Appendix C: Reference Materials for a more complete list of reference documents and for information on where to obtain the documents listed in this Section and throughout the Guide.

Contact chip terminals must comply with the EMV Integrated Circuit Card Specifications for Payment Systems, available from the EMVCo website (www.emvco.com) including any specification updates released by EMVCo.

Visa payWave readers must comply with the EMV Contactless Specifications, including Book C-3, and the Visa Contactless Payment Specification (VCPS), Version 2.1 or higher.

Devices accepting personal identification numbers (PINs) must comply with the Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements available from www.pcisecuritystandards.org and with the Visa PCI PIN Security Requirements.

A number of best practice documents are also available to assist acquirers in determining their terminal Requirements:

- Best practices relating to the deployment of acceptance terminals that support magnetic stripe, contact chip and contactless chip can be found in the *Visa Transaction Acceptance Device Guide* (TADG).
- Best practices relating to the Visa Easy Payment Service (VEPS) can be found on www.visa.com in the *Visa Easy Payment Service – Merchant Program Guide*.
- Best practices relating to payment acceptance for retail petroleum merchants can be found in the *Visa Payment Acceptance Best Practices for Retail Petroleum Merchants*.
- Risk management best practices for prepaid programs that will utilize a self-service kiosk can be found in *the Prepaid Product Risk Management Best Practices*.

In addition to following the recommendations outlined in the above-mentioned documents, acquirers can customize their programs through adoption of optional functionality and proprietary processing. Proprietary processing, however, must not interfere with global interoperability.

Note: Visa acquirers must download Visa chip documentation from the Visa Chip and Contactless webpage on Visa Online. Please see Appendix C for information on enrolling and gaining entitlement. Licensed vendors may download licensed Visa materials from the Visa Technology Partner site (https://technologypartner.visa.com).

1.2 Terminology

The following terms are used throughout this guide:

Table 1–1: Terminology

Term	Definition
Acquirer	A Member that signs a Merchant or disburses currency to a Cardholder in a Cash Disbursement, and directly or indirectly enters the resulting Transaction Receipt into Interchange. *Visa Rules* ID#: 010410-010410-0024219
AID	A data element that identifies the application in a card or terminal, such as Visa Debit/Credit or Visa Electron. It is composed of the Registered Application Provider Identifier (RID) and the Proprietary Application Identifier Extension (PIX).
Cardholder Selection	An EMV process whereby the Cardholder is presented with a list of mutually supported applications from which they choose the desired application.
Card (Visa Card)	A Magnetic Stripe and/or a Visa contactless card bearing the Visa Brand Mark, or a non-Card form Contactless Payment device bearing the Visa Brand Mark, that enables a Visa Cardholder to obtain goods, services, or cash from a Visa Merchant or an Acquirer. All Visa Cards must bear the Visa Brand Mark.
Chip Card	A Card embedded with a Chip that communicates information to a Transaction Acceptance Device (TAD).
Debit Pair	A set of the Visa U.S. Common Debit AID and the Visa ISO Debit AID which share the same funding source. A debit pair can be identified by the common BIN found in the File Control Information (FCI) associated with the respective AIDs.
Dual-interface Terminals	A terminal that supports both contact and contactless chip cards and complies with the EMV Specifications and VCPS. Support for contactless may be either as a reader separate from the POS device or via a reader integrated into a POS device

Term	Definition
EMV® Specifications	*EMV Integrated Circuit Card Specifications for Payment Systems* encompassing all 4 books which make the contact chip specifications and the EMV Contactless Specifications for Payment Systems encompassing 4 books which make up the contactless specification plus any updates published in specification bulletins on the EMVCo website
Merchant Routing Option	The option provided to U.S. merchants pursuant to the Dodd-Frank Act and Federal Reserve Board Regulation II to route covered debit transactions over one of at least two unaffiliated U.S. debit networks enabled on a card
Reader, Contactless Reader	The merchant device communicating with the card There are two scenarios in which typically a reader is used for a contactless transaction: • Either as a reader, also called a dongle or Proximity Coupling Device (PCD), separated from, but communicating with, a POS device. • Or as a reader integrated into a POS device. The word reader in this guide will cover both scenarios unless explicitly stated otherwise. It is not intended to imply in which physical component (the reader or the POS device) a specific action is performed.
Terminal	A transaction acceptance device
U.S. Common Debit AID	An AID that may be selected to enable merchant routing choice over multiple unaffiliated U.S. debit networks – see also Visa U.S. Common Debit Application Identifier
U.S. Covered Visa Debit Card	A Visa U.S. debit card as defined in the Visa Rules for debit and prepaid products covered by the unaffiliated network and routing requirements of the Dodd-Frank Act and Federal Reserve Board Regulation II.
Visa Contactless Payment Specification (VCPS	The *Visa Contactless Payment Specification*, which covers versions 2.1, and I.
Visa Rules	The *Visa Core Rules and Visa Product and Service Rules* (including any U.S.-specific rules), other Visa rules, and Visa Supplemental Requirements documents
Visa U.S. Common Debit Application Identifier	An EMV-compliant Application Identifier licensed for use with Visa's EMV and VIS-based applications for the purpose of processing a transaction for debit and prepaid products covered by the unaffiliated network and routing requirements of the Dodd-Frank Act and Federal Reserve Board Regulation II. In this document referred to as the Visa U.S. Common Debit AID

2. VSDC Transaction Flow

To better understand the impact of chip on an acquirer's systems and processes it is important to understand the various steps in a VSDC chip transaction. This Section describes the steps at the terminal/card level and the host level.

All activities, prior to the transaction going online for issuer approval, are transparent to the acquirer and occur between the card and the terminal. Some of these functions will not apply to terminals in the U.S. which operate as online-only terminals, and are so noted.

These functions are included in this Section to provide acquirers with an overall understanding of the processing that may occur in an EMV chip transaction. Their presence does not indicate the need to support them.

2.1 Initiating a Transaction

The chip card is inserted into the terminal or swiped through a magnetic stripe reader. If swiped, the terminal checks the service code in the magnetic stripe. If the first digit of the service code indicates a chip card, the terminal prompts the sales clerk or cardholder to insert the card into the terminal.

Note: To provide a faster transaction, merchants should be trained to insert the card into the chip reader when presented with a chip card rather than swiping the magnetic stripe.

2.2 Application Selection

The terminal determines the applications supported by the card and compares them to the applications supported by the terminal, in order to build the Candidate List. Once the list is built, the Application Selection phase is completed through selection of an application to initiate a transaction. The EMV Specifications allows for multiple processes for selecting the application to be used to initiate the transaction:

- Cardholder Selection, where the cardholder is prompted to select one of the applications in the Candidate List.
- Priority Selection, where the highest priority application (as assigned by the issuer) is selected to initiate the transaction.
- Special Application Selection Logic. In the U.S., U.S. Covered Visa Debit Cards can be routed exclusively using the Visa U.S. Common Debit AID. Implementation of Special Application Selection will require the deployment of custom logic.

The EMV Specifications also recognize that terminals may implement customized logic based on an industry agreement that affects the selection of the application:

> In the U.S., other options exist for Application Selection to support unaffiliated network and routing requirements of the Dodd-Frank Act and Federal Reserve Board Regulation II as outlined in Section 4.4.3: Contact Application Selection and Routing Options and Appendix E: Special Terminal Logic.

Application Selection logic may incorporate a mix of basic and customized processes.

2.2.1 Visa U.S. Common Debit AID and Customized Application Selection

All transactions initiated with a Visa owned Application Identifier (AID) other than the Visa U.S. Common Debit AID must be routed to VisaNet and be processed according to Visa or Visa Interlink (as applicable) network operating rules and technical standards. Some products may be personalized with more than one AID, where one or more AIDs may represent products with their own routing option(s), for instance the Visa U.S. Common Debit AID. To initiate a transaction using such an AID, certain terminal logic may need to be executed as part of the outlined VSDC transaction flow. This logic is described in Section 4.4.3.

2.3 Initiating Application Processing

The terminal signals to the card that the transaction is about to begin. The card response to the terminal includes data and risk management information for use during the transaction. Before responding, the card performs the following steps:

1. Restrictions Check (Optional)

   The card may determine if the transaction is taking place in an environment that the card does not allow. When the transaction is not allowed for this application, the card directs the terminal to a different application or alternatively terminates the transaction.

2. Card sends the Application Interchange Profile (AIP) and Application File Locator (AFL) to terminal (Mandatory).

   The card may send a different AIP or AFL depending on the transaction environment. For example, the card might send a different AIP and AFL for domestic versus international transactions.

   a. AIP specifies the application functions that are supported by the application in the chip card.

   b. AFL designates which records the terminal should read from the chip card.

2.4 Reading the Application Data

The terminal uses the AFL to determine the card data it should read to process the transaction. Once the terminal reads the data, it uses the AIP to determine what processing is needed for the transaction.

2.5 Risk Management Checks

Risk management checks are performed (if present on the card and supported by the terminal) to determine how the transaction should be processed.

In the U.S. all transactions require online processing, thus the terminal will send the transaction online.

2.5.1 Offline Data Authentication

Offline Data Authentication allows the terminal to confirm that the card data has not been tampered with after the card was issued by the issuer and in the case of Dynamic Data Authentication (DDA) and Combined DDA/Application Cryptogram Generation (CDA), protects against the re-use of copied chip data in an offline environment. This process is important for offline capable devices where there may be a possibility of an offline approved transaction.

For online-only devices, Offline Data Authentication is superfluous and devices are therefore **not** required to support Offline Data Authentication.

Note: Since all transactions in the U.S. will be sent online for issuer approval due to a zero floor limit, support for Offline Data Authentication is not required and not recommended. Acquirers or merchants that do not obtain an online approval do so at their own liability.

Depending on the card capabilities, one of the following Offline Data Authentication methods may be performed if the terminal supports Offline Data Authentication:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined DDA/Application Cryptogram Generation (CDA) (optionally supported)

SDA is performed by the terminal using static data read from the card. DDA and CDA are performed by the card and the terminal using dynamic data from the card and terminal. Offline capable devices need to support SDA and DDA.

U.S. acquirers that consider supporting Offline Data Authentication should review the global *VSDC Acquirer Implementation Guide* for further details, as Offline Data Authentication has specific support requirements.

2.5.2 Processing Restrictions

The processing restrictions function is used to determine the degree of compatibility between the application in the card and the terminal. These checks include determining whether there are any geographic or transaction-type limitations or whether the application on the card has expired.

The terminal performs the following checks using data read from the card:

- Effective/Expiration Date Checking
- Application Usage Control Checking
- Application Version Number Checking

Further information regarding Processing Restrictions can be found in the EMV Specifications and in Section 4.

2.5.3 Cardholder Verification

The terminal reads the Cardholder Verification Method (CVM) List on the card to determine the CVM to use for the transaction. It selects the CVM based on the CVMs mutually supported (between card and terminal) and the circumstances of the transaction.

CVM is used by the terminal and/or the merchant to verify that the cardholder is legitimate and that the card is not lost or stolen. The following CVM options are available in EMV:

- Online PIN
- Signature
- Offline Plaintext PIN
- Offline Enciphered PIN
- No CVM Required

More information regarding support by terminals for each of the CVMs can found in Section 4.4.5 Cardholder Verification, and in the *Visa Rules* and the *Visa Transaction Acceptance Device Requirements*.

Terminal request of specific CVMs for specific transaction types may be supported by selectable kernels as defined in contact EMV (see Section 4.4.6 and Section 8.4.2).

2.5.4 Terminal Risk Management

The terminal performs checks based on the acquirer risk control features and the capabilities of the terminal. For offline-capable terminals, some of the checks are mandatory whereas others are optional and at the discretion of the acquirer. The checks include:

- Floor limit check
- Random selection
- Transaction velocity checking
- Exception file check (optional)
- Offline transaction limit check (optional)

The results of these checks are used to determine how the terminal processes the transaction.

For online-only terminals in the U.S., these checks are not required as all transactions will be sent online. However, any acquirer considering use of offline-capable terminals needs to ensure that terminals support floor limit checks and the floor limits are set according to the *Visa Rules*.

2.6 Terminal Action Analysis

The results of the previous steps are used in Terminal Action Analysis to determine the disposition of the transaction. The results of the previous checks are stored in the Terminal Verification Results (TVR) data element, which is then compared to specific rules that are set by the issuer (in the card) and Visa (in the terminal).

Depending on the results, the terminal will request a cryptogram from the card. A cryptogram is a data element dynamically generated by the card using transaction specific data and a cryptographic key stored in the card. It allows the issuer to confirm data integrity and that the transaction was undertaken using a valid card. The result of Terminal Action Analysis determines which of the following cryptograms is generated:

- Authorization Request Cryptogram (ARQC)
- Transaction Certificate (TC)

Application Authentication Cryptogram (AAC)For online-only terminals in the U.S., other than in some exception situations, the terminals will always request an ARQC and go online.

The cryptogram is generated by the card and its generation is transparent to the terminal. Further information regarding the generation of the cryptograms and Terminal Action Analysis processing, including exceptions, can be found in the EMV Specifications and the Visa Integrated Circuit Card Specification (VIS).

2.7 Card Risk Management

Card Risk Management is transparent to the acquirer, merchant, and terminal. However its outcome confirms the disposition of the transaction. It allows the card to perform velocity checking and other risk management checks on behalf of the issuer to see if it agrees with the terminal's decision. The card may perform the following checks:

- New Card check
- Checking results from previous transactions (such as PIN Tries exceeded, Issuer Script results and result of Offline Data Authentication)
- Offline spending amounts and transaction counts (Velocity) checking

Once the card has completed the risk management checks, it responds to the terminal's request for a cryptogram with one of three cryptograms listed in Section 2.6 Terminal Action Analysis.

In the U.S., where the terminal will request to go online, the card will agree and respond with an ARQC.

2.8 Online Processing

Once the card generates an ARQC for online processing, the terminal captures the ARQC, the original data elements used by the chip card to generate the ARQC and information regarding the selected application and the interface used. This information, together with standard transaction data and the results of the risk management checks are forwarded online to the acquirer.

Acquirers format this data into the authorization message and forward the information to VisaNet. For authorization and full financial messages, acquirers send the chip data in Field 55 in TLV (Tag-Length-Value) format. It is critical that acquirers do not alter any of the data received from the card and terminal as these are used by the issuer, or Visa on its behalf, when authorizing the transaction. Altering data or data quality issues may have serious consequences that may result in a decline of the transaction by the issuer.

2.9 VisaNet Processes Acquirer Authorization Request

VisaNet may perform the following functions after it receives the authorization request:

- If the message format of the acquirer is different from the message format of the Full Data issuer (Field 55 acquirer to third bit map issuer), VisaNet converts the authorization to the issuer's message format.
- VisaNet uses the pre-processing chip indicators to help determine whether to route to the issuer. If the transaction is processed in Stand-In (STIP), these chip transaction indicators influence the approve/decline decision.
- VisaNet forwards the authorization request to the issuer if it has not been processed in STIP. If processed in STIP, the transaction proceeds as outlined in Section 2.11 VisaNet Processes the Issuer Response.

2.10 Issuer Receives Authorization Request

When the authorization request is received, the issuer or issuer processor will validate the cryptogram. In certain cases Visa may validate the cryptogram on the issuer's behalf.

The issuer may additionally review the chip data received in the authorization to determine whether to authorize or decline the transaction.

The issuer decides whether to approve or decline the transaction and sends the authorization response to VisaNet to transmit to the acquirer. The response may optionally include:

- An Authorization Response Cryptogram (ARPC), which is an similar to the ARQC but generated by the issuer, which the card will validate.
- An Issuer Script that is typically used to reset risk parameters on the card.

2.11 VisaNet Processes the Issuer Response

If the issuer is participating in the Visa Chip Authenticate service, VisaNet generates the ARPC on behalf of the issuer and includes it in the authorization response to the acquirer. Otherwise VisaNet forwards the issuer response to the acquirer.

2.12 Transaction Conclusion

The acquirer receives the authorization response and sends it to the terminal. The card and terminal perform final processing to complete the transaction including:

- If an ARPC is returned in the authorization response, the card validates the ARPC to ensure that the authorization response came from a valid issuer.
- Card authenticates and executes Issuer Script commands, if present.

The card generates the final cryptogram: a TC for approval or an AAC for decline. Once the transaction is completed, the terminal prompts the cashier or the customer to remove the card.

2.13 Clearing and Settlement

For approved transactions, the card generates a TC as the final cryptogram. The acquirer then submits the approved transaction to VisaNet for clearing and settlement. Acquirers and merchants in the U.S. deploying online-only terminals or terminals set with a Zero Floor Limit and that obtain an online authorization for all transactions are not required to support TCR 7 (chip data) in the clearing record.

- Acquirers send TCR 0 with POS Terminal Capability Code = 5 and POS Entry Mode = 05 or 95.
- Acquirers send TCR1 if cash-back is supported.
- Acquirers send TCR 5 as needed.
- Optionally, Acquirers may send TCR 7 with new chip data.

3. Visa payWave Transaction Flow

To better understand the impact of Visa payWave on an acquirer's systems and processes it is important to understand the various steps in a Visa payWave transaction. This Section describes the steps at the terminal/card level and the host level.

All activities, prior to the transaction going online for issuer approval, are transparent to the acquirer and occur between the card, the reader, and terminal.

Section 4: Visa's Chip Terminal and Reader Requirements provides further detail on some of the steps outlined in this Section and their implementation impacts. Section 9: Acquirer System Changes provides further information regarding host processing steps.

3.1 Acquirer Approaches

When adopting Visa payWave, Acquirers should support the latest versions of the *Visa Contactless Payment Specification* (as per Section 3.2). To provide support for the long-term development of the contactless platform, and its dependent propositions such as mobile proximity and transit, Visa has defined requirements relating to the support of qVSDC and MSD in the U.S.

The two approaches and Visa's requirements are outlined in more detail in the following sections.

3.1.1 Quick Visa Smart Debit/Credit (qVSDC)

qVSDC transactions follow an expedited EMV-processing model and chip-processing rules. These transactions can be sent online and validated using one of three dynamic authentication methods, Cryptogram Version Number 17 (CVN 17), CVN 10, or CVN 18.

The issuer decides whether to support CVN 17, CVN 10, or CVN 18, which is personalized on the card and carried during transaction processing. qVSDC is best suited for acceptance environments with EMV infrastructure, including support for chip data by the acquirer host.

3.1.2 Magnetic Stripe Data (MSD)

MSD contactless transactions follow magnetic stripe processing rules. MSD transactions are sent online and validated using CVN 17 (MSD CVN 17) or dynamic Card Verification Value (dCVV) (MSD Legacy). MSD is best suited for magnetic-stripe-only acceptance environments. MSD support is optional. Visa is currently evaluating time frames under which to establish a sunset date for the contactless MSD processing path.

3.2 U.S. Contactless Acceptance Requirements

Visa's rules regarding payWave acceptance initially read:

- Effective 1 April 2013, all new Visa payWave accepting contactless readers deployed in the U.S. must actively support both MSD and the qVSDC transaction path of VCPS 2.1 including all published updates. qVSDC may be supported on an online only basis (i.e., no support for offline authorizations).

To address challenges with legacy MSD acceptance and to prepare for the migration to qVSDC, Visa's rules regarding payWave acceptance have been updated to reflect the following:

- Effective 10 April 2015, contactless terminals deployed between 1 April 2013 and 31 December 2014 must comply with the VCPS 2.1.1 (or higher), and be capable of processing a transaction using both the MSD and qVSDC transaction paths (though the terminal may actively support only the MSD transaction path).
- Terminals deployed on or after 1 January 2015 must comply with the VCPS 2.1.1 (or higher), and be capable of processing a transaction using the qVSDC transaction path (though the terminal may actively support only the MSD transaction path).

Further details can be found in the *Visa Business News* article dated March 31, 2016 or from a Visa representative.

3.3 Contactless Processing Requirements

All transactions initiated with a Visa owned Application Identifier (AID – see Section 4.2) other than the Visa U.S. Common Debit AID must be routed to VisaNet and be processed according to Visa or Visa Interlink (as applicable) network operating rules and technical standards. Some products may be personalized with more than one AID, where one or more AIDs represent products with their own routing option(s). To initiate a transaction using an AID that is not the highest priority mutually supported AID (as specified by the card), certain terminal logic must be executed before the outlined qVSDC transaction flow. This logic is defined in Section 4.5.1.

Acquirers are responsible for their merchants' compliance with Visa rules governing Visa Contactless transactions, including ensuring proper transaction routing.

3.4 Initiating a Visa payWave Transaction

During a Visa payWave transaction, consumers briefly hold their Visa payWave card near the reader when prompted, instead of inserting their card in the reader as with VSDC transactions or swiping the magnetic stripe. The Visa payWave card is embedded with an antenna and a chip. The chip, through the antenna, communicates with the merchant's contactless reader to enable the transaction.

Acquirers should be aware that Visa payWave transactions may be initiated not only from a traditional plastic card but also from other form factors and devices such as *Near Field Communication* (NFC) enabled mobile devices and key fobs.

3.5 qVSDC Transactions

3.5.1 Preliminary Processing

Before the card and reader begin their interaction, the transaction amount is typically received by the reader before it performs its preliminary processing. Preliminary Processing expedites the transaction by allowing the reader to perform several risk management steps prior to interacting with the card.

During Preliminary Processing, the reader may use the transaction amount to perform the following checks:

- Reader Contactless Transaction Limit: Transactions for amounts above this limit are terminated and may be processed only by using a different interface.

Note: Contactless readers are required to either have the reader contactless transaction limit disabled or set to its maximum amount. This limit is not used in the U.S. region.

- Reader Cardholder Verification Method (CVM) Limit: Transaction amounts above this limit require cardholder verification for the contactless transaction. The supported CVMs for a qVSDC transaction are Signature, Online PIN, and Consumer Device CVM (e.g., Touch ID). When the transaction exceeds the Reader CVM Limit, the actual CVM performed is determined by the card and based in part on the configuration of the reader. If the transaction is below the Reader CVM Limit, no CVM is required.
  - A merchant or acquirer can promote their preferred CVM, including by steering towards PIN or auto-prompting for PIN, but they must minimally ensure that that the cardholder has the ability to opt-out of PIN and have an alternative method to complete the transaction, e.g., signature or no CVM.
  - Regardless of the verification method, merchants may use the Visa U.S. Common Debit AID for those networks enabled by the issuer on the card and route to the network of their choosing. This is true for any cardholder verification method, including PIN, signature, and "no CVM."
- Reader Contactless Floor Limit: Transactions above this limit require an online authorization by the card issuer. For the U.S. region this limit is set to zero or is not supported to ensure all transactions are sent online to be authorized by the issuer.

The reader sets the results of these checks in the Terminal Transaction Qualifiers (TTQ), a reader data element. The TTQ provides the card with the reader's capabilities and requirements. For U.S. readers the TTQ must reflect online-only transactions with no contact transaction limits.

3.5.2 Application Selection

Once the reader has completed Preliminary Processing, the reader signals to the consumer that the reader is ready for the contactless card. The cardholder briefly waves or holds the Visa payWave card close to the contactless reader to initiate the transaction. The reader determines whether it shares a contactless application with the card by selecting the card's list of contactless AIDs (called the Proximity Payment Systems Environment [PPSE]). If there are no AIDs in common, the reader terminates the transaction and the transaction may proceed via another interface such as magnetic stripe or contact chip.

If there is only one AID in common, that AID is automatically selected.

If there are two or more AIDs in common, the AID with the highest priority can be automatically selected as part of basic payWave processing. For example, a card may have both credit and debit AIDs, in which case the issuer or consumer will have defined one of those AIDs as a higher priority than the other. U.S. Covered Visa Debit Cards with multiple funding sources (e.g., credit and debit applications) would have a Visa AID connected to the credit function, and a debit pair consisting of a Visa AID and a Visa U.S. Common Debit AID both connected to a common source of debit funding. Removal of one of the AIDs of the debit pair from the Candidate List will result in two eligible AIDs (one for credit and one for debit). Either the highest priority AID (indicating the desired funding source) can be selected to initiate the transaction, or the merchant can implement custom logic to ask the cardholder which account they wish to use and select the appropriate AID that corresponds to the cardholder's account preference. The use of AID selection screens or labels to effectuate cardholder funding choice selection is optional, even for multi-account cards. Merchants that wish to maintain routing flexibility for debit transactions will need to deploy specific logic in their readers/terminals to ensure the Visa U.S. Common Debit AID is used for debit functionality, in addition to the non-paired Visa AID for credit functionality.

Note: For qVSDC readers supporting a flexible routing option, special logic may be used in selecting from the AIDs available on the card/consumer device and thereby the possible routing options that are available to the merchant. Section 4.5.1 provides further information on this approach.

3.5.3 Dynamic Reader Limits (Optional)

Once the application has been selected, readers that support Dynamic Reader Limits (DRL) examine the Application Program Identifier (Program ID) returned by the application to determine the applicable reader limits for the transaction.

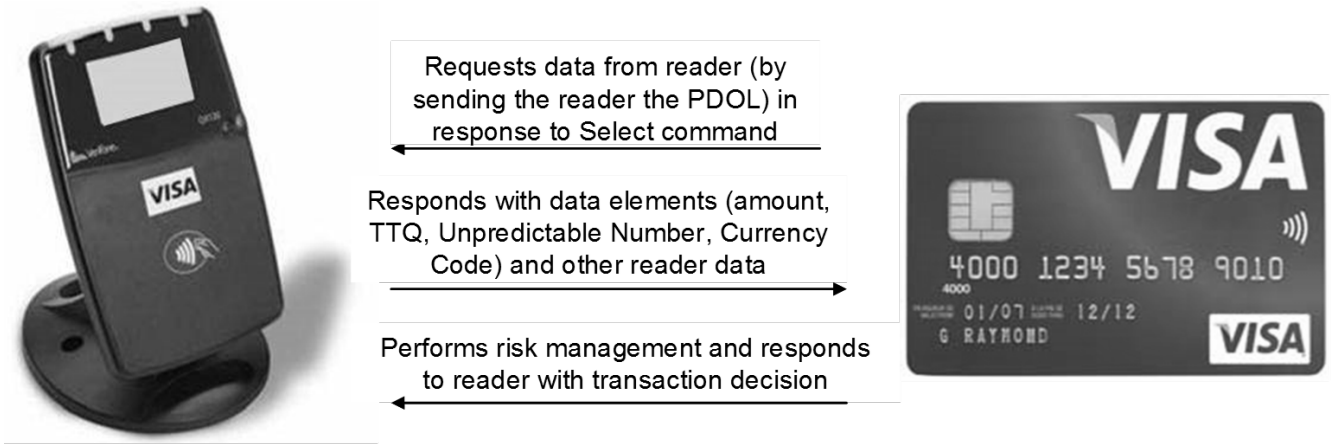
When the Program ID returned by the card does not match a reader Program ID (or the card does not return a Program ID), the reader processes the transaction using the reader limits and results determined during Preliminary Processing.

3.5.4 Card Requests Terminal and Transaction Data

Once the application is selected, the Visa payWave card responds by requesting information such as the transaction amount, TTQ, and the reader's currency code for use during the transaction. The reader responds with the requested information.

The Figure below provides a processing overview of the card requesting terminal and transaction data.

Figure 3–1: Card Requests Terminal and Transaction Data



The TTQ advises the Visa payWave card of the reader's requirements and capabilities for processing the specific transaction as follows:

- Whether it supports qVSDC or MSD as well as whether it supports contact VSDC
- Whether it supports Signature, Online PIN, Offline PIN through the Contact Interface, and/or Consumer Device CVM

Note: A Consumer Device CVM is a CVM that is performed on and validated by the consumer's payment device, independent of the reader.

- Whether cardholder verification is required for the transaction
- Whether the reader supports Issuer Update Processing

In qVSDC transactions, the card uses the information provided in the TTQ to make risk management decisions before responding to the reader.

3.5.5 Transaction Terminated

Rather than decline a transaction needlessly, if a Visa payWave transaction cannot be completed as a contactless transaction, the contactless transaction is terminated and may be processed as a physical contact chip or magnetic stripe transaction. If either the card or the reader decides to terminate the transaction, the transaction is terminated and the transaction may be completed using another interface (such as contact chip). In these instances, the reader should power down the contactless interface and direct the cardholder to use the alternate interface.

Terminated transactions differ from declined transactions because declined transactions may not be reinitiated. The acquirer's merchant environment may have specific best practices or requirements for situations where it is preferred to terminate the transaction and proceed with a contact interface.

3.5.6 Online Processing

The reader indicates to the cardholder that the card can be removed from the reader's field. The reader uses the information provided by the card and transmits the transaction to the acquirer.

The reader sends the data from the transaction including the cryptogram, information regarding the selected application and the interface used together with standard transaction data to the acquirer. The acquirer then formats the corresponding VisaNet authorization message including the relevant data fields. For qVSDC transactions the following V.I.P. Field values are included:

- Field 22 – POS Entry Mode with a value of 07
- Field 23 – Card sequence number that uniquely identifies the card used to initiate the transaction
- Field 55 – Including relevant Tags to support the Cryptogram, Form Factor Indicator (Tag 9F6E) and if present in the card the Customer Exclusive Data (Tag 9F7C)
- Field 60.2 – Terminal Entry Capability with a value of 5 (contact or contact and contactless chip capable terminal) or 8 (contactless chip capable terminal)

VisaNet performs processing on the authorization message to determine if the issuer participates in Visa Chip Authenticate. If not then authorization is sent directly to the issuer.

During a qVSDC transaction, the issuer validates the card using CVN 17, CVN 10, or CVN 18. Based on the results of online card verification, along with other standard risk management checks (such as ensuring that the card is not expired, and verifying that the account is in good standing and has available funds), the issuer either approves or declines the transaction in the authorization response.

The authorization response is sent to the acquirer which logs the response and forwards the response to the merchant terminal.

3.5.7 Transaction Outcome

The reader conveys the issuer's authorization response by displaying whether the transaction is approved or declined. If approved, depending on Visa rules, the transaction may not require a cardholder signature or a receipt.

3.6 MSD Transaction Flow

During an MSD transaction, the consumer briefly holds their Visa card near the contactless reader, instead of swiping or inserting it. The Visa payWave card is embedded with an antenna and a chip. The chip, via the antenna, communicates with the merchant's contactless reader to conduct the transaction. The card and reader exchange information in less than a half of a second and the transaction is processed and completed.

The transaction follows magnetic stripe processing and rules except that it includes enhanced online card authentication using CVN 17 or dCVV. Depending on requirements and rules, transactions below a certain defined value may not require cardholder verification (signature or online PIN) or a receipt. Regional rules and requirements define the Cardholder Verification Method for particular transactions. Acquirers should contact their Visa representative for specific information. The following sections outline the steps involved in a MSD transaction.

Note: payWave reader support for the MSD transaction path is now optional, see Section 3.2 for more information.

3.6.1 Application Selection

Unlike qVSDC, MSD readers do not support preliminary processing.

Typically, Application Selection for the MSD path follows the basic payWave process where the AID with the highest priority is automatically selected, as described in Section 3.5.2. Because MSD processing is functionally equivalent to magnetic-stripe processing (though with the enhanced security of dCVV or CVN 17) and does not rely on the AID selected for routing purposes, routing flexibility for MSD transactions can be accomplished through the use of BIN routing logic.

3.6.2 Card Requests Terminal and Transaction Data

Once the contactless application is selected, the Visa payWave card requests information from the reader to use during the transaction by sending the Processing Options Data Object List (PDOL) to the reader. The reader responds with the requested information.

The information includes the transaction amount, the reader's capabilities and requirements in the Terminal Transaction Qualifiers and other transaction data. The card uses the TTQ to ascertain the capabilities of the reader including whether the reader supports MSD CVN 17. After reviewing the TTQ, the card completes its part of the MSD transaction by sending data to the reader such as the Track 2 data and a CVN 17 cryptogram, if supported by the card. The reader then indicates to the cardholder that the card can be removed from the reader's field.

After the exchange, the reader prompts the cardholder to remove the card from the reader's field.

3.6.3 Online Processing

The reader sends the data from the transaction including the cryptogram to the acquirer. If the transaction is to be routed to VisaNet the acquirer then formats the corresponding VisaNet authorization message including the relevant data fields. For MSD transactions the following V.I.P. Field values are included:

- Field 22 – POS Entry Mode with a value of 91.
- Field 23 – Card sequence number that uniquely identifies the card used to initiate the transaction (If personalized on the card this field must be present in the authorization message)
- Field 55 – Including relevant Tags to support the Cryptogram, Form Factor Indicator (Tag 9F6E) and, if present in the card, the Customer Exclusive Data (Tag 9F7C)
- Field 60.2 – Terminal Entry Capability with a value of 8 (contactless chip capable terminal)

Note: For MSD transactions where a dCVV (MSD Legacy) card was used, Field 23 and Field 55 will not be sent in the authorization message.

VisaNet performs processing on the authorization message to determine if the issuer participates in Visa Chip Authenticate. If not then the authorization request message is sent directly to the issuer.

The issuer (or Visa, on the issuer's behalf) performs enhanced online card authentication using CVN 17 or validates the dCVV if a legacy transaction was used. The authorization response is determined by the cryptogram results along with other standard risk management checks such as checking the cardholder's Online PIN, if applicable, ensuring that the card is not expired, and making sure that the account is in good standing and has available funds. The issuer sends the authorization response to the reader.

3.6.4 Transaction Outcome

The acquirer formats the issuer response and forwards it to the terminal. The terminal or reader conveys the issuer's authorization response by displaying whether the transaction is approved or declined. If approved, depending on Visa rules, the transaction may not require a cardholder signature or a receipt.

If the transaction is approved, it is later submitted as part of clearing and settlement.

3.6.5 MSD CVM Processing

As the payWave MSD transaction replicates the physical magnetic stripe transaction, CVM rules for payWave MSD transactions are identical to physical magnetic stripe transactions. This means a signature or online PIN must be obtained, else the merchant could face a chargeback liability, except where no CVM is allowed such as for UCATs or under VEPS rules. Consumer Device CVM (e.g., Touch ID) is not supported for payWave MSD transactions. Because MSD processing is functionally equivalent to magnetic-stripe processing (though with the enhanced security of dCVV or CVN 17) routing for MSD transactions can be accomplished through the use of BIN routing logic.

3.7 Visa payWave for Mobile

Visa payWave for mobile brings the contactless payment experience to the mobile device through support of the Visa Mobile Contactless Payment Specification (VMCPS). The Visa payment application developed to VMCPS is called Visa Mobile Payment Application (VMPA).

From the acceptance perspective, mobile devices containing a VMPA can be accepted in any version of contactless readers that are developed to different versions of the Visa Contactless Payment Specification (VCPS); for instance, Version 2.1 including all published updates and EMV Contactless Kernel 3. Visa payWave transactions that originate from mobile devices have the same processing requirements as Visa payWave transactions that originate from cards. There is no difference between a card and a mobile Visa payWave transaction from the point of view of the transaction processing, authorization, and settlement data that is passed through V.I.P. and BASE II systems.

4. Visa's Chip Terminal and Reader Requirements

This Section describes the requirements for deploying EMV-compliant Visa Smart Debit/Credit (VSDC) terminals and Visa Contactless Payment Specification (VCPS)-compliant contactless readers. These are terminals and readers that meet the security, interoperability and functionality requirements outlined in the EMV Specifications, VCPS and comply with Visa's terminal requirements.

The focus is on requirements for online-only terminals. Some of the functions discussed in Section 2 and Section 3 relating to VSDC and Visa payWave processing are not covered in the following sections as they do not require action by acquirers and should be built into EMV-compliant terminals. Acquirers considering support for offline processing, for example, support for offline authorization, should review the global *VSDC Acquirer Implementation Guide*.

An overview of each function requiring action by acquirers is provided in the following sections. Further details can be found in the EMV Specifications, VCPS and in the *Visa Transaction Acceptance Device Requirements*. Acquirers should work with vendors to outline the support vendors will provide and the activities that should be handled internally by acquirers.

4.1 Terminal Types

A number of different terminal types are defined in the EMV Specifications as outlined in the table below. Depending on the nature of the merchant, its location and profile, acquirers can determine which type better supports the merchant's requirements. Selection of the type is also dependent on the nature of the domestic market.

The U.S. market is a zero floor-limit market, meaning all transactions need to be authorized online by the card issuer in order to protect the acquirer from liability. Therefore, it is expected that most U.S. acquirers and merchants will deploy online-only terminals and not offline capable terminals.

Acquirers may deploy terminals that are offline capable but any offline processing is at the acquirer's risk and accordingly may increase its liability. Acquirers considering this option should review the global *VSDC Acquirer Implementation Guide* requirements for offline capable terminals.

Table 4–1: EMV and VSDC Terminal Types

Type	Description
Offline/online terminals	Capable of processing both offline and online transaction authorization. For example, an online capable terminal with a floor limit above zero will execute both offline and online transactions.
Online-only terminals	Cannot approve transactions offline. For authorization processing, the transaction must be sent online to the issuer. These terminals may, however, decline transactions offline. For example, under EMV, ATMs are considered online-only terminals. It is expected that most U.S. acquirers will deploy online-only terminals since all transactions in the U.S. need to be authorized online.
Online-capable terminals	Includes online-only terminals, as well as offline/online terminals.

Note: Offline PIN processing is not directly related to online or offline authorization. For example, offline PIN processing may be performed for online authorized transactions.

4.2 Application Identifiers (AIDs)

The terminal must contain the Application Identifiers (AIDs) for all chip payment applications that it supports. If the terminal cannot match one of its AIDs with an AID from the card, a chip transaction cannot be completed. The AID consists of two components:

- Registered Application Provider Identifier (ISO RID) – indicates the payment system. Visa owned RIDs are:
  - The Visa ISO RID is A000000003
  - The Visa U.S. Common Debit RID for U.S. Covered Visa Debit Card is A000000098
- Proprietary Application Identifier Extension (PIX) – indicates the application.
  - The Visa globally interoperable PIXs are listed in Section 4.2.1.

The AIDs used for Visa globally interoperable cards use the Visa ISO RID and are outlined in the following:

- Table 4–2: Application Identifiers (AIDs) for Visa ISO RID by product type.
- The PIX used to define the Visa U.S. Common Debit AID is listed in Table 4–3: Application Identifier (AID) for Visa U.S. Common Debit AID.
- The AID used for U.S. Covered Visa Debit Card is defined in Table 4–3: Application Identifier (AID) for Visa U.S. Common Debit AID.

4.2.1 Visa AIDs

The AIDs used for Visa globally interoperable cards uses the Visa ISO RID and are outlined below.

Table 4–2: Application Identifiers (AIDs) for Visa ISO RID

Application	RID + PIX
Visa (e.g., Visa Credit or Visa Debit)	A000000003 1010
Visa Electron	A000000003 2010
Visa Interlink	A000000003 3010
PLU.S.	A000000003 8010

4.2.2 Visa U.S. Common Debit AID

The AID used for U.S. Covered Visa Debit Card is defined below.

Table 4–3: Application Identifier (AID) for Visa U.S. Common Debit AID

Application	RID + PIX
Visa U.S. Common Debit	A000000098 0840

4.2.3 Rules for Visa AIDs

An Application Selection Indicator associated with each terminal AID designates whether the terminal AID must exactly match the card AID or whether the terminal AID may match only the first portion of the card AID (partial selection). For Visa AIDs, this indicator must be set to allow partial selection.

All terminals accepting Visa must support the Visa AID.

All POS chip terminals that contain the Visa AID must also contain the Visa Electron AID.

All POS terminals accepting Visa Interlink must support the Visa AID, Visa Interlink AID, and the Visa U.S. Common Debit AID.

Acquirers should take care in using the AIDs listed above. Terminals should not use only the Visa ISO RID (i.e., without a PIX) with Partial AID Selection for Application Selection as some cards may contain ISO RID+PIX combinations for domestic applications that are not valid in other countries. For example, A000000003020201 is used for health care products in Canada only.

Note: In addition to the AIDs beginning with the Visa ISO RID, Visa cards may contain one or more non-Visa AIDs – some AIDs may represent specific routing options, others may be for non-payment functions or domestic applications from another country.

Note: ATMs have different rules for presence of AIDs. Interlink is not supported at ATMs, and ATMs must include the PLU.S. AID.

Note: Transactions initiated with an AID beginning with the Visa ISO RID must be routed to a Visa-affiliated network.

4.2.3.1 Implementation Activities

Acquirers should determine which AIDs to support in their terminals depending on the card programs accepted.

- If a merchant accepts Visa cards, they must support the Visa AID and the Visa Electron AID.
- If a merchant accepts Visa Interlink cards, they must support the Visa AID, the Visa Electron AID, the Visa Interlink AID, and the Visa U.S. Common Debit AID. Visa Interlink can only be accepted at terminals capable of processing online transactions with online PIN verification.
- To clarify, for U.S. Covered Visa Debit Cards merchants have flexibility to use either the Visa U.S. Common Debit AID or the Visa AID. Merchants are not required to use the Visa AID and may route U.S. Debit transactions using the Visa U.S. Common Debit AID exclusively if they so choose. A merchant or acquirer can promote their preferred CVM, including by steering towards PIN or auto-prompting for PIN, but they must minimally ensure that that the cardholder has the ability to opt-out of PIN and have an alternative method to complete the transaction, e.g., signature or "no CVM."
- Regardless of the verification method, merchants may use the Visa U.S. Common Debit AID for those networks enabled by the issuer on the card and route to the network of their choosing. This is true for any cardholder verification method, including PIN, signature, and "no CVM."

4.3 Language

Acquirers must decide the language(s) their terminals will offer to customers[1]. Language selection is an optional function that can be performed as an EMV function or as a separate process, such as cardholder selection at the beginning of the transaction (i.e., terminals already supporting a language selection process do not need to modify that process as part of EMV implementation).

EMV chip cards may contain a Language Preference data object (accessed as soon as the Application Selection process begins) which contains up to four (4) languages in order of preference. Use of EMV functionality for Language Selection provides a means for the terminal to shift to a language familiar to the cardholder.

[1] Language Selection, if present, is typically found at ATMs, but can be offered at the POS.

A terminal using EMV functionality to support multiple languages compares the card's Language Preference with the languages supported by the terminal at the beginning of the transaction. If a match is found, the language with the highest preference is used in the messages displayed to the cardholder. If no match is found, the terminal will use the default ("home") language.

Typically, EMV Language Preference processing does not offer any advantage over a menu-based language selection unless the terminal supports a very large number of languages. Further, because EMV language selection is based on the personalization by the issuer, rather than cardholder selection, it can result in selection of a language that is not optimal for the cardholder.

4.3.1.1 Implementation Activities

Acquirers should determine if they want terminals to support multiple languages. If their terminals already support additional languages, acquirers should determine if the current support is optimal, or if there are advantages to incorporating the EMV language functionality.

4.4 VSDC Requirements

The following sections outline the requirements relating to acceptance of contact chip VSDC cards. Requirements relating to acceptance of Visa payWave cards are outlined in Section 4.5: Visa payWave Reader Requirements.

4.4.1 Contact EMV Application Selection

EMV Application Selection consists of two phases:

- Building the list of applications mutually supported by the terminal and card
- Determining which application is to be used to initiate the transaction

When a VSDC card is presented to a terminal, the terminal determines which applications are supported by both the card and terminal by comparing the Application Identifiers (AIDs) on the card with the AIDs maintained by the terminal. The terminal builds an internal list of the applications jointly supported by the card and terminal (the "Candidate List") using either the **Directory Selection Method** or the **List of AIDs Method**. Support for the Directory Selection Method is optional for the card and terminal, while the List of AIDs Method is mandatory.

If both the card and terminal support the Directory Selection Method, the terminal reads a list of the payment applications maintained on the card from the Payment Systems Environment (PSE) file. The terminal compares the applications listed in the card PSE to the applications it supports and builds the Candidate List. Where the terminal supports many AIDs, the Directory Selection Method can provide more efficient processing.

If the card does not have a PSE or the terminal does not support the Directory Selection Method, the terminal uses the List of AIDs Method. With the List of AIDs Method, the terminal goes through its list of applications one-by-one and asks the card whether it also has the application. Common applications are put on the Candidate List created by the terminal.

Once the Candidate List is built, an application can be selected to initiate a transaction. This process is described in Section 4.4.2: Application Initiation and Cardholder Selection/Confirmation.

Further information regarding both methods can be found in the EMV Specifications. Additional information on application selection when the Visa U.S. Common Debit AID is present can be found in Section 4.4.3.

4.4.1.1 Implementation Activities

Support for the List of AIDs Method is mandatory and is supported by all terminals. All contact EMV-compliant terminals include this functionality.

Because the Directory Selection Method is optional, acquirers should evaluate its benefits for the domestic environment. If either or both of the following factors are true, acquirers may want to support the Directory Selection Method in addition to the List of AIDs Method:

- If domestic issuers are planning to support the Directory Selection Method on their cards; it will only be used when both the card and terminal support it. Otherwise, the List of AIDs Method will apply.
- If the acquirer's terminal supports many applications, increased efficiency may be realized when the Directory Selection Method is implemented.

Terminal vendors will cover development of application selection, so no internal technical resources are required. If the Directory Selection Method is controlled by a predefined parameter, acquirers should ensure that the Terminal Management System accommodates that parameter.

4.4.2 Application Initiation and Cardholder Selection/Confirmation

EMV Application Selection[2] allows for multiple processes for selecting the application to be used to initiate the transaction:

- Cardholder Selection of the desired application, where the cardholder is prompted to select one of the applications in the Candidate List.
- Priority Selection, where the highest priority application (as assigned by the issuer) is selected to initiate the transaction.

[2] The first two processes—Cardholder Selection and selection of the highest priority application—are referred to as "basic EMV Application Selection" in this document.

- Special Application Selection Logic. In the U.S., U.S. Covered Visa Debit Cards can be routed exclusively using the Visa U.S. Common Debit AID. Implementation of Special Application Selection will require the deployment of custom logic.

Note: Cardholder Selection or Priority Selection can be combined with aspects of any industry agreement so as to both meet specific processing requirements for U.S. cards and support non-U.S. issued international card configurations that may require cardholder confirmation for global interoperability. Cardholder confirmation does not apply to U.S. Covered Visa Debit Cards. Any application selection process that is not based on one or more of the above processes may not be compliant with the EMV specifications.

Once the Candidate List has been built, Application Selection is completed by selecting an application from the Candidate List to initiate the transaction:

- If the chip card and terminal have only one application in common and cardholder confirmation is not required, that application is used.
- If the chip card and terminal have only one application in common but cardholder confirmation is required on that application, Cardholder Selection (described below) can be used to meet that requirement.
- If the chip card and terminal have more than one application in common, the terminal can be configured to prompt the cardholder to make a selection (described below).
- For Cardholder Selection as defined within the EMV specifications:
  - The acceptance terminal displays a list of all of the commonly supported applications[3],[4] to the cardholder in the priority sequence specified by the issuer, or
  - The acceptance terminal displays each commonly supported application to the cardholder, one-by-one in the priority sequence specified by the issuer, and allows the cardholder to confirm the displayed application or to advance to the next application.

  By default, the terminal will display the Application Label description available on the card, but the merchant can override or enhance that descriptor, provided the descriptors are transparent to the consumer ("enhanced descriptor").

[3] Internally, the terminal performs Application Selection based on the Application Identifiers (AIDs) and associated data elements. When Cardholder Selection is used, the terminal displays the Application Labels associated with the AIDs, or an enhanced descriptor, as the Application Labels are more readily understandable to the cardholder. For convenience, this document will sometimes refer to displaying the "applications" to the cardholder, which should be understood as displaying the Application Labels to the cardholder.

[4] If Cardholder Selection is used to support Confirmation where there is only one application on the card, then only one application will be presented to the cardholder.

- The application selected is used to initiate the transaction.
- If the chip card and terminal have more than one application in common, but the terminal does not support any form of cardholder selection or specific application selection logic (see below), the application can be selected automatically based on the Application Priority Indicator set by the issuer. This approach (Priority Selection) may be appropriate where the terminal does not have any means for the cardholder to indicate selection, such as an unattended parking kiosk. Merchants that wish to maintain routing flexibility for debit transactions can deploy Specific Application Selection Logic as described in Appendix E: Special Terminal Logic to automatically select the Visa U.S. Common Debit AID for U.S. Covered Visa Debit Cards.
- If the chip card and terminal have more than one application in common, and the terminal supports Specific Application Selection Logic as in Appendix E: Special Terminal Logic, the terminal may identify cards that contain both the Visa AID and the Visa U.S. Common Debit AID and eliminate one of the AIDs from the Candidate List (when these AIDs share the same funding source ["debit pairs"]). The remaining AID can then be used for routing purposes. To clarify, merchants are not required to use the Visa AID, and may route debit transactions for U.S. Covered Visa Debit Cards using the Visa U.S. Common Debit AID exclusively if they so choose.
- A merchant or acquirer can promote their preferred CVM, including by steering towards PIN or auto-prompting for PIN, but they must minimally ensure that that the cardholder has the ability to opt-out of PIN and have an alternative method to complete the transaction, e.g., signature or "no CVM."
- Regardless of the verification method, merchants may use the Visa U.S. Common Debit AID for those networks enabled by the issuer on the card and route to the network of their choosing. This is true for any cardholder verification method, including PIN, signature, and "no CVM."
- If the chip card and terminal have no applications in common, and no application can be selected, the device should re-initiate the transaction using the magnetic stripe interface. If the terminal is chip-capable and supports all Visa required AIDs, the Terminal Entry Capability (TEC) should remain set to "5."

Application Selection logic that does not follow the above scenarios, including any customized terminal logic that does not properly support multi-function/multi-application cards (such as a card supporting both debit and credit), may not be compliant with EMV specifications.

A merchant or acquirer can promote their preferred CVM, including by steering or auto-prompting for PIN, but they must minimally ensure that the cardholder has the ability to opt-out of PIN and have an alternative method to complete the transaction, e.g., signature or "no CVM."

Recommended PIN opt-out options include:

- Displaying a 'signature' button on the PIN prompt screen
- Allowing the cardholder to use the 'cancel' button to opt out of PIN prompt, after clearly explaining to the cardholder how to opt out
- Using "credit" and "debit" buttons or labels with "credit" used to indicate cardholder preference to opt-out of entering a PIN and "debit" used to indicate cardholder preference to enter a PIN just as those terms were frequently used in the pre-EMV environment

Regardless of the verification method, merchants may use the Visa U.S. Common Debit AID for those networks enabled by the issuer on the card and route to the network of their choosing. This is true for any cardholder verification method, including PIN, signature, and "no CVM."

Further information regarding Application Selection can be found in Section 4.4.3, as well as the EMV Specifications and the *Visa Transaction Acceptance Device Guide*.

4.4.2.1 Implementation Activities

Because some cards may support more than one source of funds (i.e., credit and debit), cardholder selection allows the cardholder to select the appropriate funding source. For U.S. Covered Visa Debit Cards, Cardholder Selection can be combined with Special Terminal Logic to remove one AID of an AID pair from the Candidate List as described in Appendix E: Special Terminal Logic (e.g., for U.S. Covered Visa Debit Cards, merchants can remove the Visa AID and leave the Visa U.S. Common Debit AID).

To clarify, for U.S. Covered Visa Debit Cards merchants have flexibility to use either the Visa U.S. Common Debit AID or the Visa AID. Merchants are not required to use the Visa AID, and may route U.S. debit transactions using the Visa U.S. Common Debit AID exclusively if they so choose.

A merchant or acquirer can promote their preferred CVM, including by steering towards PIN or auto-prompting for PIN, but they must minimally ensure that that the cardholder has the ability to opt-out of PIN and have an alternative method to complete the transaction, e.g., signature or "no CVM."

Regardless of the verification method, merchants may use the Visa U.S. Common Debit AID for those networks enabled by the issuer on the card and route to the network of their choosing. This is true for any cardholder verification method, including PIN, signature, and "no CVM."

4.4.3 Contact Application Selection and Routing Options

To provide for transaction routing options (as required for a U.S. Covered Visa Debit Card), an additional AID (i.e., Visa U.S. Common Debit AID) will be present on a Visa debit or prepaid card.

A device that supports both a Visa ISO AID and the Visa U.S. Common Debit AID must ensure that transactions initiated with the Visa ISO AID route to a Visa affiliated network. To support this requirement, Visa requires that acquirers and any other routing entities receive the AID used to initiate the transaction. This AID is passed to the terminal in a card data element called the Dedicated File (DF) Name. The acquirer or other routing entities then use the DF Name to perform the appropriate routing process. Acquirers should review and implement this solution based on their routing needs. Effective October 1, 2015, Visa requires that DF Name be carried in Field 55 of the authorization request. For more information on the DF Name, refer to Table B–1: V.I.P. System Field 55 Mandated Data Tags.

Additional routing options may be supported by the presence of the Visa U.S. Common Debit AID or one or more non-Visa owned AIDs on the card, each representing a different product with their own routing options.

Note: Not all Visa cards will support multiple AIDs, as some products will not support multiple routing options. The presence of multiple AIDs in itself is not an indication that multiple routing options are supported by the card, as the non-Visa AIDs could be non-payment related or may relate to a non-U.S. domestic payment system.

Note: Visa cards that support multiple AIDs, of which one supports multiple routing option(s) for debit and prepaid, may also include a separate AID for a product that is not covered by the Dodd-Frank Act and Federal Reserve Board Regulation II – for instance a multi-application card with both credit and debit AIDs.

If a terminal does not offer Cardholder Selection (or an alternate form of cardholder selection) and does not use the Application Priority Indicator method, as described in Appendix D: Basic EMV Terminal Logic, the terminal must include specific logic to determine the AID. This logic and the process for determining the AID is as defined in Appendix E.1.

Certain functions may be associated with particular AIDs, such as cash-back. The logic to support cash-back is also discussed in Appendix E.1: Contact Terminal Application Selection.

Note: When Application Selection is used, it is important to communicate to the cardholder the Application Label selected, or an enhanced descriptor, so that the cardholder understands which account is being used for multi-account (credit/debit) cards.

4.4.3.1 Implementation Activities

If the terminal will not offer Cardholder Selection or apply Application Priority Indicator as described in Appendix D: Basic EMV Terminal Logic, the acquirer may need to request the terminal vendor to support the logic as described in Appendix E.1: Contact Terminal Application Selection. Also, the acquirer needs to ensure that terminals are equipped to determine whether a specific product allows the merchant to control the transaction routing. In order to make this determination, the acquirer (and other routing entities) will need to receive an indication of which AID was selected at the terminal.

4.4.4 Processing Restrictions

The terminal performs Processing Restrictions to see whether the transaction should be allowed. The terminal checks whether the effective date for the card has been reached, the card has not expired, the application versions of the card and terminal match, and if any Application Usage Control restrictions are in effect. An issuer may use Application Usage Controls to restrict a card's use for domestic or international transactions, as well as cash, goods and services or cash-back.

Processing Restrictions is a mandatory feature in EMV and must be performed by all terminals. Further information about processing restrictions may be found in the EMV Specifications.

4.4.4.1 Implementation Activities

Acquirers do not need to undertake any specific activities relating to Processing Restrictions. They should ensure that their terminal vendor has loaded the correct Application Version Number in the terminal.

4.4.5 Cardholder Verification

Cardholder verification is used to ensure that the cardholder is legitimate and the card has not been lost or stolen. The terminal uses a CVM List from the card to determine the type of verification to be performed, for example, signature or online PIN. The CVM List establishes a priority of CVMs to be used relative to the capabilities of the terminal and characteristics of the transaction.

Certain terminal types, as defined by Visa (e.g., ATMs), require an online PIN entry even when the card's CVM List does not include it. The table below lists the most common types of CVMs supported by terminals in the U.S. market. Acquirers may also determine whether support for other EMV provided CVMs, for example, offline PIN, would be advantageous.

Table 4–4: Types of Cardholder Verification Methods

Cardholder Verification Method	Description
Signature	Normally, operates in the same manner as in the magnetic stripe environment. The cardholder signs on the terminal or on the receipt and the merchant can compare this signature to the signature on the card. Signature support may be implemented by selecting the Visa AID (see Appendix D) or via special processing (see Appendix E)
Online PIN	Operates in the same manner as in the magnetic stripe environment. The cardholder-entered PIN is encrypted by the terminal and is sent online to the issuer for verification.
No CVM Required	Operates in the same manner as in the magnetic stripe environment where transaction authorization is independent of cardholder verification. No cardholder verification is necessary for low value transactions in some merchant environments, such as certain unattended terminals, quick service restaurants and qualifying VEPS transactions.
Fail CVM Processing	This is a catch-all option to ensure CVM processing is deemed to have failed. EMV requires that this CVM is always supported.

From a VSDC perspective, it is mandatory that terminals perform Cardholder Verification by reviewing the card's CVM List, if present, to determine the verification method for the transaction.

The specific CVMs supported by terminals are based on business needs, types of card programs accepted and Visa mandates. The following general guidelines are provided to assist acquirers to determine the types of CVMs to support at their POS terminals.[5]

Signature must continue to be supported for international Visa and Visa Electron card transactions, as well as domestic transactions (except for Visa Interlink and Unattended Cardholder Activated Terminals (UCATs)). Signature support may be implemented by selecting the Visa AID (see Appendix D) or via special processing (see Appendix E).

A merchant or acquirer can promote their preferred CVM, including by steering towards PIN or auto-prompting for PIN, but they must minimally ensure that the cardholder has the ability to opt-out of PIN and have an alternative method to complete the transaction, e.g., signature or "no CVM."

[5] Note that for ATMs, there are different requirements for CVM

Recommended PIN opt-out options include:

- Displaying a 'signature' button on the PIN prompt screen
- Allowing the cardholder to use the 'cancel' button to opt out of PIN prompt, after clearly explaining to the cardholder how to opt out
- Using "credit" and "debit" buttons or labels with "credit" used to indicate cardholder preference to opt-out of entering a PIN and "debit" used to indicate cardholder preference to enter a PIN just as those terms were frequently used in the pre-EMV environment

Note: There are many options for how to offer PIN opt-out in a way that is transparent and consumer friendly. Cardholders can be confused by opt-out processes that utilize unlabeled terminal buttons to effect the opt-out (e.g., pushing the red button or the green button with no label or explanation). Merchants customizing their terminals to implement PIN opt-out must minimally ensure that a cardholder presenting a Visa Debit card for payment can originate a transaction using a signature (or "no CVM") even if the cardholder is prompted or steered to enter a PIN.

Transactions that qualify under the VEPS program do not require cardholder verification. Acquirers should refer to the *Visa Rules* for requirements relating to VEPS including transaction value limits.

4.4.5.1 CVM List Processing Exceptions

Terminals need to support a minimum level of cardholder verification, as determined by Visa or by law, even when the card does not support CVM processing, "no CVM" List is present, or the last CVM processed in the CVM List is "no CVM required". If CVM processing does not result in the required CVM, the terminal may additionally perform the default CVM designated in the *Visa Rules* or in law for the terminal and transaction type. This may be accomplished through use of selectable kernels or, in some cases, code outside of the kernel.

Alternatively, if the terminal determines that CVM Processing has failed (for example, when the cardholder is unable to enter a PIN and the CVM list only supports PIN entry), the transaction is sent online and the issuer responds with an approval, Visa recommends that:

- The terminal prints a signature line on the receipt or shows a signature capture window on the display, and
- The terminal prompts the merchant to request a signature.

If a specific CVM is required for certain transactions (e.g., cash-back or low value transactions), the EMV concept of selectable kernels can be used to suppress certain CVMs for a specific transaction. See Section 4.4.6 for further details.

4.4.5.2 Implementation Activities

Acquirers need to determine the CVMs to implement at the terminal level, based on Visa applicable requirements. Some other factors acquirers should consider include:

- If an acquirer decides to implement signature and PIN, Visa recommends that the terminal omit printing of the signature line on those transactions that are PIN-based and instead print "Verified by PIN" or "PIN verified" in place of the signature line. In addition, acquirers should educate merchants to expect that the CVM will vary among transactions and the terminal will prompt some cardholders for a PIN and others for a signature.

PIN Entry Devices (PEDs) or PIN pads must conform to PCI PIN Transaction Security (PTS) requirements. If the PED has been integrated with the card-reading terminal, the entire terminal must meet the security requirements. Refer to Section 6.5: Payment Card Industry Requirements.

4.4.6 Cardholder Verification and Selectable Kernels

In order to support the use of Cardholder Verification methods that vary based on transaction characteristics, it is necessary for a terminal supporting cash-back or the VEPS program to support Selectable Kernel processing (see Section 8.4.2 Configurable and Selectable Kernels). This process ensures that the appropriate CVM is requested for the transaction, by invoking a terminal kernel that only supports the CVM appropriate to the transaction. The principle in using selectable kernels for Cardholder Verification is outlined in Appendix E Contact CVM Processing and Selectable Kernels Logic.

Usage of a Selectable Kernel is also recommended for terminals supporting PIN, when the cardholder selects to opt out of PIN entry.

4.4.6.1 Implementation Activities

Acquirers supporting cash-back or VEPS should ensure that their terminals support selectable kernels and that they can be configured to support the necessary CVM selection for a specific transaction.

4.4.7 Terminal Risk Management

Terminal Risk Management consists of a series of checks to protect the acquirer, issuer and system from potential fraud. The nature of online-only terminals means that all transactions have to be approved by the issuer and the functions in Terminal Risk Management are not necessary.

Acquirers may consider supporting Floor Limit checking although the U.S. is a Zero Floor Limit market, which results in all transactions going online. If Floor Limits are supported, to provide maximum flexibility, Visa suggests that acquirers set up devices to support the following limits, even if the values for magnetic stripe and chip transactions are currently the same:

- International Floor Limit for magnetic stripe transactions
- International Floor Limit for chip-initiated transactions
- Domestic Floor Limit for magnetic stripe transactions
- Domestic Floor Limit for chip-initiated transactions

4.4.8 Terminal Action Analysis

Terminal Action Analysis is mandatory and uses the results of Processing Restrictions, Terminal Risk Management, and Cardholder Verification, as well as rules set in the card and terminal, to determine whether the transaction should be approved offline, sent online for authorization, or declined offline.

After determining the disposition of the transaction, the terminal requests an Application Cryptogram from the card, corresponding to the transaction disposition:

- Authorization Request Cryptogram (ARQC) – Online authorization
- Application Authentication Cryptogram (AAC) – Offline decline

The card rules are set in Issuer Action Codes (IACs) fields, which are read by the terminal from the card. The Visa rules are stored in the terminal as Terminal Action Codes (TACs):

- Issuer Action Codes (IACs): Card-based rules the terminal uses during terminal action analysis. IAC values are defined by the issuer and stored in the card. There are three types of IACs: IAC – Denial, IAC – Online, and IAC – Default.
- Terminal Action Codes (TACs): Terminal-based rules for Terminal Action Analysis. TAC values are mandated by Visa and must be supported. There are three types of TACs: TAC – Denial, TAC – Online, and TAC – Default.

For the TAC values, refer to Table 4–5: Terminal Action Code (TAC) Values.

An online-only terminal always attempts to go online with the authorization request, unless declined offline due to IAC – Denial settings. During IAC – Denial and TAC – Denial processing, if a Terminal Verification Results (TVR) bit is set and the corresponding IAC – Denial or TAC – Denial bits are set (or it is set in both), the terminal declines the transaction. The only relevant Visa TAC setting for a transaction at an online-only terminal is "Service not allowed."

An online-only terminal may perform or omit IAC – Online and TAC – Online processing and IAC – Default and TAC – Default processing. For IAC – Online and TAC – Online processing, if performed, the only relevant TVR setting for an online-only terminal is "Transaction value exceeds the floor limit."

Because the floor limit is set to zero, the transaction always goes online and all other values in TAC – Online or IAC – Online are irrelevant. The IAC – Default and TAC – Default processing, if performed, will always cause a transaction to be declined if an online authorization could not be performed.

Visa recommends that online-only terminals do not perform IAC – Online and TAC – Online processing, as all transactions are sent online for approval. If the terminal is unable to go online, the terminal may either:

- Approve the transaction at the acquirer/merchant's risk and subsequently perform a deferred authorization.
- Request an AAC to decline the transaction and notify the cardholder that the service cannot be performed due to a communication failure.

If the terminal and card determine that the card was to be declined offline, the transaction is not sent online and the card generates an AAC.

4.4.8.1 Terminal Action Analysis for Visa U.S. Common Debit AID

For transactions initiated with the Visa U.S. Common Debit AID, the processing depends on whether the terminal supports TAC/IAC-Online and TAC/IAC-Default processing. TAC-Decline processing will always be performed.

Terminals that **do not** support TAC/IAC-Online and TAC/IAC-Default processing:

- Deploy the terminal with the TAC-Decline values set to x0000000000.
- Deploy the terminal without the TAC-Online and the TAC-Default values.
- Configure the terminal to always request to go online with an ARQC and always decline offline if unable to go online.

Terminals that **support** TAC/IAC-Online and TAC/IAC-Default processing:

- Deploy the terminal with all three sets of TACs using the following values:
  - TAC-Denial to x0000000000
  - TAC-Online to xFFFFFFFFFF
  - TAC-Default to xFFFFFFFFFF
- These TAC settings will configure the terminal to always request to go online with an ARQC and always decline offline if unable to go online.

Refer to Table 4–5: Terminal Action Code (TAC) Values for a summary of the values.

4.4.8.2 Terminal Action Code (TAC) Values

The following table outlines the TAC values that must be supported in the terminal by AID:

Table 4–5: Terminal Action Code (TAC) Values

AID	Online-only terminal does not support TAC/IAC-online and TAC/IAC-default processing	Online-only terminal supports TAC/IAC-online and TAC/IAC-default processing
Visa ISO AID	TAC Denial: x0010000000 TAC Online: n/a TAC Default: n/a	TAC Denial: x0010000000 TAC Online: x584004F800 TAC Default: x584000A800
Visa U.S. Common Debit AID	TAC Denial: x0000000000 TAC Online: n/a TAC Default: n/a	TAC Denial: x0000000000 TAC Online: xFFFFFFFFFF TAC Default: xFFFFFFFFFF

4.4.8.3 Implementation Activities

Acquirers should ensure that terminal vendors have loaded the Visa TACs correctly. Information regarding the TACs should also be provided to merchant service and technical areas to ensure they are used when troubleshooting or reviewing terminal problems.

4.4.9 Online Processing

The outcome of Terminal Action Analysis (and corresponding Card Action Analysis) will be for the transaction to be sent online or declined offline. If the transaction is to be sent online, the card returns a set of data including the Authentication Request Cryptogram (ARQC) which will be used by the issuer to determine whether the transaction is coming from a valid card.

4.4.9.1 Implementation Activities

Acquirers need to determine the requirements for sending transactions online. Further information regarding the authorization message requirements can found in Section 9: Acquirer System Changes.

4.4.10 Completion

The card and terminal perform final processing to complete the transaction.

When the online authorization is successfully completed, a final Application Cryptogram is generated by the card. The card uses the transaction disposition, Issuer Authentication results and issuer-encoded to determine whether to return a TC or an AAC.

Although terminals are not required to retain the cryptogram (TC or AAC) for online-approved transactions at single-message (SMS) or host-capture terminals, the terminal must request the final cryptogram to allow the chip card to complete Issuer Authentication to avoid unnecessary online requests during subsequent POS transactions.

A reversal must be generated for online approved transactions that are subsequently declined by the card.

For terminal-capture terminals, the terminal transmits the TC and the related cryptogram data in the clearing message. SMS and host-capture acquirers may transmit the ARQC and the related cryptogram data in the clearing message, if the authorization code returned by the issuer is included.

If during processing the terminal needs to terminate the transaction, the terminal must display a message to the cardholder and merchant indicating why the transaction cannot be completed and that the card should be removed.

4.4.10.1 Implementation Activities

Acquirers need to determine the requirements for transmitting or storing the final Application Cryptogram especially if they are considering supporting offline transactions.

Acquirers should also review changes required to reverse a transaction when the card declines the transaction after the issuer has approved it.

Note: For submitting offline clearing transactions, see Section 9.3: Host System Changes.

4.5 Visa payWave Reader Requirements

4.5.1 Application Selection Options

Contactless transactions do not support Cardholder Selection in the same way as contact chip transactions due to the minimal interaction between the contactless reader and the consumer device.

In basic Contactless Application Selection, the reader will always select the highest priority AID on the consumer device. The cardholder and terminal flow for this approach is:

- Cardholder taps the card/device against the payWave-enabled reader.
- Terminal selects the Visa AID based on highest priority.
- The cardholder performs the CVM negotiated by the terminal and card/device and the transaction is routed to Visa.

Merchants that prefer to offer options in regards to functions supported (e.g., cash-back) or wish to implement routing flexibility will need to deploy specific logic in their readers/terminals to ensure that the appropriate application is selected. Contactless transactions can ultimately be routed over the Visa U.S. Common Debit AID to the same extent as transactions initiated using other methods, but custom logic will be required. See Appendix E.2: Contactless Reader Application Selection/Special Logic for more information.

Note: For mobile-based payments using the Visa AID, the CVM may be entered and validated on the device (e.g., TouchID, biometrics). CVM confirmation is sent to the terminal and no additional CVM is requested.

Due to the short interaction time between reader and card, Contactless Application Selection does not allow cardholder access to the Candidate List for AIDs. Therefore, any special logic needs to take place *before* the basic Contactless Application Selection process begins. The special logic necessary to allow application selection does not impact the standard contactless kernel, but will take place in a separate reader application executed once the card/device enters the contactless field but before the normal contactless transaction flow begins. The logic for such a "pre-select" reader application is further described in Appendix E.2: Contactless Reader Application Selection/Special Logic.

Note: Because MSD processing is functionally equivalent to magnetic-stripe processing (though with the enhanced security of dCVV or CVN 17) and does not rely on the AID selected for routing purposes, routing flexibility for MSD transactions can be accomplished through the use of BIN routing logic.

4.5.1.1 Contactless Reader Application Selection and Routing Option Logic

Only readers that are *not* using the application selection process based on Application Priority Indicator need the special logic.

For such terminals, it is necessary to understand whether the card product represented by an AID is eligible for routing flexibility (e.g., U.S. Covered Visa Debit Card), in conjunction with a means of asking the cardholder for an indication of the chosen CVM.

Customized application selection logic is described in Appendix E.2: Contactless Reader Application Selection/Special Logic.

4.5.2 Transaction Speed

Visa payWave transactions are designed to be fast. Interaction between the card and the reader for both qVSDC and MSD must not exceed 500 milliseconds.

Note: The 500-millisecond requirement is for "card-in-field" time, and does not include qVSDC preliminary processing nor any processing after the reader has indicated that card read is complete.

4.5.3 Terminal Transaction Qualifiers

The Terminal Transaction Qualifiers (TTQ) is a data element provided by the terminal to the card during Preliminary Processing. The card uses this information to understand the terminal's capabilities and requirements in deciding how to process the transaction.

For qVSDC, the TTQ indicates:

- Whether the reader supports qVSDC.
- Whether the reader supports EMV contact chip.
- Whether the reader supports online processing.
- Whether the reader requests online processing.
- The Cardholder Verification Methods supported by the reader. This information can either be the same for all transactions or be dynamically set on a transaction-by-transaction basis.
- Whether a CVM is required for the specific transaction.
- Whether the reader supports Issuer Update Processing.

For the detailed layout of the TTQ, refer to VCPS.

For MSD, the TTQ should indicate support for MSD and CVN 17 if the acquirer has migrated and can support CVN 17 data. If the acquirer has not migrated and cannot support CVN 17 data, this data element should not be set. (CVN 17 support is indicated by setting the bit associated with "online cryptogram required.") The TTQ does not change based on the transaction. No other TTQ settings are required.

The TTQs are defined by VCPS as a 4-byte field and acquirers need to ensure their terminals are passing all 4 bytes to ensure issuers are able to process the transaction correctly. Failure to do this may lead to interoperability problems.

4.5.4 Reader Limits – qVSDC

The qVSDC reader performs preliminary processing to expedite the transaction. The reader compares the transaction amount against one or more of the following limits:

- **Reader Contactless Floor Limit**—For the U.S. region, this limit is set to zero to ensure all transactions are authorized by the issuer.
- **Reader Cardholder Verification Method (CVM) Limit**—Transactions for amounts above this limit require cardholder verification.

4.5.5 Reader Cardholder Verification Method – qVSDC

The card and terminal work together to determine the cardholder verification requirement for each transaction. On a qVSDC contactless transaction, the cardholder (or consumer using a mobile device) is either able to complete the transaction without cardholder verification or the cardholder provides a signature, enters an online PIN or enter a passcode on his or her mobile phone.

Step 1—The reader determines if cardholder verification is required and provides CVMs it supports to the card.

The reader determines whether it requires cardholder verification for the transaction by checking the transaction amount against the Reader CVM Limit. If the transaction amount is above this limit, the reader requires cardholder verification; if it is below the limit, the reader does not require cardholder verification. It also provides the card with the reader-supported CVMs (signature, online PIN, Consumer Device CVM) in the TTQ.

Note: Support for the Consumer Device CVM by the reader is required for readers supporting VCPS 2.1 including all published updates and higher.

The reader has two approaches for providing the Cardholder Verification Methods it supports to the card in the TTQ:

- The reader can provide the card with all the Cardholder Verification Methods it supports. This is the simplest approach.
- The reader can tailor the Cardholder Verification Methods to each transaction. For example, the device might accept "no CVM" for transactions below a specific amount while requiring an Online PIN for specific transaction types (e.g., cash-back).

Acquirers and merchants should be aware of these approaches when selecting a reader as this may require additional vendor development.

Note that signature support may be implemented by selecting the Visa AID see (Appendix D) or via special processing (see Appendix E).

Step 2—Card determines if cardholder verification is required.

The card reviews the TTQ. If the reader requires cardholder verification, the card cannot override this. If the device does not require cardholder verification, the card determines whether to require cardholder verification.

Step 3—If CVM is required, the card determines which CVM to use.

If cardholder verification is required, the card reviews the CVMs supported by the device and compares these methods to the ones it supports. If there is only one CVM in common, the card selects that CVM. If there is more than one common CVM, the card selects the first common CVM based on a predefined hierarchy/priority of contactless CVMs. The CVM hierarchy is shown in order below:

- Online PIN
- Consumer Device CVM (only for mobile phones)
- Signature

Step 4—Card communicates CVM selection to reader.

If a CVM is required, the card indicates the selected CVM to the reader in the Card Transaction Qualifiers (CTQ).

A merchant or acquirer can promote their preferred CVM, including by steering towards PIN or auto-prompting for PIN, but they must minimally ensure that that the cardholder has the ability to opt-out of PIN and have an alternative method to complete the transaction, e.g., signature or "no CVM."

Regardless of the verification method, merchants may use the Visa U.S. Common Debit AID for those networks enabled by the issuer on the card and route to the network of their choosing. This is true for any cardholder verification method, including PIN, signature, and "no CVM."

4.5.6 Reader Cardholder Verification Method – MSD

The terminal determines the cardholder verification requirement as per magnetic stripe processing rules. The cardholder may be validated using one of the following methods:

- No cardholder verification. The cardholder does not have to provide a PIN or signature. Some Visa environments allow transactions below a specific amount to take place without cardholder verification.
- Signature
- Online PIN

4.5.7 Expiration Date Check

During a contactless transaction, the reader checks the expiration date in the Track 2 Equivalent Data to ensure that the contactless application is not expired. If the card is expired, the reader declines the contactless transaction.

4.5.8 Online Card Verification

During a qVSDC transaction, the issuer, or Visa on the issuer's behalf, validates the card using the appropriate Cryptogram Version Number. Current Cryptogram Version Numbers include CVN 10 ('0A'), CVN 17 ('11'), CVN 18 ('12'), and CVN '43'. Acquirers are not required to perform any analysis related to the Cryptogram Version Number; they must pass the cryptogram and cryptogram data to VisaNet/issuer for processing.

For MSD transactions, acquirers must support the data associated with CVN 17 in authorization messages for online card verification of MSD transactions. Acquirers should continue to support dCVV as needed.

Note: MSD only supports CVN 17, which is also supported in qVSDC. CVN 10 and CVN 18 do not apply to MSD.

Note: Regardless of the cryptogram type supported, all chip data must be sent in Field 55 of the authorization message.

4.6 Additional Requirements for VCPS 2.1

In addition to the requirements listed in Section 4.5, Visa payWave Reader Requirements. VCPS 2.1 introduces additional functionality which acquirers need to consider. These additional items are listed in the sections below. For further details, acquirers should refer to VCPS.

4.6.1 Consumer Device CVM (CDCVM)

Contactless readers that support VCPS Version 2.1 or higher, must enable support for a Consumer Device CVM. The Consumer Device CVM is a CVM performed on the consumer's payment device (independent of the reader).

Reader support for the Consumer Device CVM is mandatory, as is indication of its support in the TTQ. In addition to supporting the Consumer Device CVM, the reader may support other CVMs such as signature and/or online PIN.

4.6.2 Support for Pre-Tap

As part of application processing, if a mobile device with Visa payWave capabilities is being used, the device may respond to the reader with an error when a CDCVM is required for the transaction and has not yet been performed. This is referred to as a Pre-Tap. Once the consumer performs the CDCVM, the mobile device is re-presented to complete the transaction.

5. Additional Terminal Considerations

In addition to the requirements outlined in Section 2, other considerations may apply to terminals, along with optional features. This Section discusses these additional considerations.

The items in this Section are covered in more detail in the *Visa Transaction Acceptance Device Guide*. Additionally, acquirers can discuss the requirements with their Visa representative.

5.1 Magnetic Stripe Transaction Terminal Requirements

Existing rules governing magnetic stripe transactions continue to govern transactions performed at magnetic stripe terminals. These rules also apply to magnetic stripe transactions performed at chip-reading terminals, including EMV-compliant terminals. Acquirers should implement fallback policies and procedures at the point of transaction, as well as support for new chip service code values. These policies and procedures are only applicable to contact-only or dual-interface cards.

5.1.1 Service Codes

The migration to chip has introduced new service code values. Visa chip cards must contain a service code beginning with **2**, indicating an international chip card, or **6**, indicating a domestic only usage chip card. Current Visa rules require all terminals to recognize and act on the service code.

Acquirers must ensure this new service code value will not cause a rejection at magnetic stripe-only terminals. This is not a new rule, although it may require magnetic stripe terminal software changes if terminals are not currently meeting this requirement.

For further details, acquirers should refer to the *Visa Rules*.

5.1.2 Fallback

Fallback transactions are non-chip transactions performed with chip cards at chip terminals. EMV-compliant terminals must accept both chip and magnetic stripe cards and have both a chip and magnetic stripe reader. When a chip card is accepted at these terminals, the card should be read via the chip reader and not the magnetic stripe reader.

There are situations when the chip terminal cannot accept a chip card (for example when the chip on the card is faulty or damaged or the terminal chip reader is malfunctioning). When a chip card is accepted via its magnetic stripe, the resulting transaction is referred to as a fallback transaction. These transactions are deemed less secure because magnetic stripe acceptance circumvents the control and risk management protection available with chip acceptance.

Unattended Cardholder Activated Terminals (UCATs) do not allow fallback beyond magnetic stripe transactions. In addition, fallback is not permitted for declined transactions.

The *Visa Rules* state that chip cards must be accepted by the chip reader unless the chip card or chip-accepting terminal is malfunctioning. In that case, the transaction can be processed using the magnetic stripe. This rule must be followed for international transactions and should be followed for domestic transactions.

The Global Fallback Monitoring Program was introduced to help reduce excessive international (and domestic) fallback transactions and to establish a global regulatory framework for these transactions. The intent is to motivate the timely repair or replacement of faulty equipment, and/or the correction of inaccurately flagged transactions.

The program identifies acquirer-country combinations with a ratio of international fallback to international chip-capable transactions that exceeds the global average international fallback ratio by one and one half times. Domestic fallback reporting can also use Global Fallback Monitoring Program thresholds. POS activity is reported separately from ATM activity. The program also identifies acquirer-country combinations that have fallback activity nearing program thresholds, which allows acquirers to take proactive measures to avoid exceeding thresholds.

Acquirers may incur a non-compliance assessment for each fallback transaction over their allowance. Acquirers should contact their Visa representative for more information regarding the Global Fallback Monitoring Program and its application in the U.S. market.

5.1.2.1 Fallback Prevention and Processing

Acquirers must have software in their terminals to request that the contact chip be used to prevent fallback transactions. A special chip service code (**2xx** or **6xx**) is encoded on the magnetic stripe of chip cards. When the magnetic stripe reader reads a chip service code, the terminal does not process the transaction but displays a message that the card should be read by the using contact chip. This check helps to ensure that chip cards are used for chip transactions at chip-reading terminals and minimizes the chance of inadvertent fallback transactions.

In a V.I.P. message, Terminal Entry Capability (Field 60.2), Service Code (Field 35 or 45), and POS Entry Mode (Field 22) are used in combination to determine whether it is a fallback transaction.

According to the *Visa Rules*, after a chip read failure, the terminal must send the next consecutive magnetic stripe read transaction online to the issuer, indicating a fallback transaction. The fallback transaction must be identified by populating the correct authorization message fields. If the transaction is not correctly identified, the issuer may have recourse via a chargeback. See Section 9.3.1: Host System Fallback Considerations and Section 11.4.2: Fallback Transactions for more information about fallback.

When online authorization is not available, the merchant may be given the option to perform voice authorization to complete the transaction. If the magnetic stripe cannot be read, or if an online authorization is not available, merchants can use existing card acceptance and transaction processing procedures.

5.1.2.2 Avoiding False Fallback Indication during Migration

Chip migration strategies may include piloting chip acceptance at a few stores prior to rolling out across terminal fleets. During these transitional periods, care should be taken to avoid indicating chip capability when processing components are not yet migrated to chip. This can occur when only a few of many stores are chip capable, and the central server updates the Terminal Entry Capability (TEC) to indicate chip acceptance. This would imply all transactions seem to be made at a chip capable terminal, and would therefore indicate fallback.

If a terminal has been updated to support chip for other card brands, but not yet for Visa, the Terminal Entry Capability (TEC) should remain set to 2 (or 8 for a payWave enabled terminal) for Visa transactions, until chip capability for Visa is fully implemented. This will avoid improper flagging of transactions as fallback during migration periods, providing correct information to both issuers and to Visa.

Once chip migration for Visa has been completed, including implementing support for the Visa and Visa Electron AIDs, the Terminal Entry Capability should remain set to 5 for all transactions.

Care should be taken when using any TEC manipulation logic to ensure the merchant is not exposed to counterfeit chargeback.

5.1.2.3 Fallback Implementation Activities

Fallback implementation activities include:

- Follow the *Visa Rules* recommendations for fallback transactions.
- The terminal should contain logic between the magnetic stripe reader and chip reader to invoke fallback if the chip cannot be read.
- Ensure that terminals do not indicate they are chip-capable until the terminal, merchant and acquirer are fully chip functional and can send all the required chip data. Terminals that indicate they are chip capable, while continuing to process only magnetic stripe transactions for chip-capable cards, are a common reason for acquirers to be selected for non-compliance assessments under the Global Fallback Monitoring Program.
- Monitor transaction activity for fallback. Excessive fallbacks can indicate failure of chip reading hardware. VisaVue Online has fallback chip reports available for acquirers to monitor their fallback through a subscription. The two reports include:
  - **Chip Fallback Quick Reports**—These two new quick reports—chip fallback summary and chip fallback detail—enable acquirers to analyze their portfolios' chip fallback transactions. VisaVue Online can generate a summary report of all fallback transactions or it can segment the information by defined merchants.
  - **Chip Summary Quick Report**—This report summarizes overall volume by "Chip," "Contactless" and "Other," all of which are sorted using POS Entry Mode.

There are also merchant education needs related to fallback. Refer to Section 12.6 Contactless Reader Branding and Placement for further details.

Note: A terminal's capability must take into account both hardware and software, and should only ever indicate a terminal's true ability to process a payment transaction. If a terminal has the hardware to read a chip but not the software to process the payment, it is not considered chip-enabled because it cannot read and transmit full chip data. Acquirers that are beginning to deploy hardware for chip terminals should continue to use the TEC value of "2" (or "8" for a payWave capable terminal) until the terminal application is enabled to accept chip technology. Once the application is enabled, the TEC should be updated to the value of "5."

5.2 Card Data in Online Messages

5.2.1 Use of Track 2 Equivalent Data

The terminal must always transmit the full, unmodified contents of the Track 2 Equivalent Data in the chip to the acquirer including the Issuer Discretionary data. The terminal should not construct the data in the magnetic stripe field in the online authorization message based on the individual data elements in the magnetic stripe or chip. The device should also ensure that if a transaction is processed as magnetic stripe, the track data used in the transaction is read from the magnetic stripe and correspondingly, if a transaction is processed as chip, the track data used should be read from the chip.

Note: For more information on Track Data, refer to the Visa Contactless Payment Specification.

The Track 2 Equivalent Data in the chip also contains critical information relating to the card being used, which an issuer may rely upon to authorize a transaction.

Because the data on the chip may differ from the data on the magnetic stripe, the POS Entry Mode Code field (V.I.P. Field 22) in the online authorization message that indicates the source of the track data (magnetic stripe or chip) must be accurate to avoid unnecessary declines.

Note: For either VSDC or qVSDC transactions Track 1 is not supported in the authorization message.

5.2.2 Form Factor Indicator

Dual-interface terminals will need to pass the Form Factor Indicator (Tag 9F6E) in V.I.P. Field 55 for a Visa payWave transaction, if present.

5.2.3 Dedicated File (DF) Name

A device that supports both the Visa ISO AID and the Visa U.S. Common Debit AID must ensure that debit transactions initiated with the Visa ISO AID route to a Visa affiliated network. To support this requirement, Visa currently requires that acquirers and any other routing entities receive the AID used to initiate the transaction. This AID is passed to the terminal in a card data element called the Dedicated File (DF) Name. The acquirer or other routing entities then use the DF Name to perform the appropriate routing process. Acquirers should review and implement this solution based on their needs to achieve appropriate routing. Effective October 1, 2015, Visa requires that the DF Name be carried in Field 55 of the authorization request. For more information on the DF Name, refer to Table B–1: V.I.P. System Field 55 Mandated Data Tags.

5.3 Support for up to 19 Digit PANs

Both the *Visa Rules* and the EMV Specifications require that all chip terminals that accept Visa and Visa Electron cards must support variable-length PANs up to and including 19 digits. The terminal is not required to transmit the 19-digit PAN to the acquirer and the acquirer is not required to transmit the 19-digit PAN to VisaNet, unless explicitly mandated, such as for Plus transactions. If the acquirer does not support 19-digit PANs and a 19-digit PAN is read from the chip, the terminal should indicate that the card type is not supported and end the transaction.

5.4 Terminal Display Messages

Terminal messages are displayed to let the merchant or cardholder know the status of a transaction and what action to take next. To ensure clear and effective transaction messages, acquirers and terminal vendors should follow a few basic principles, including:

- The message displayed must clearly instruct the merchant or cardholder on what action to take.
- Where the message is based on an issuer response, the message should clearly communicate the meaning of the response.
- The transaction amount can be displayed to the customer prior to PIN entry. The cardholder should be prompted to confirm the transaction amount; PIN entry is an acceptable method of confirmation. If PIN entry is requested before the transaction amount is known for throughput reasons, an explicit amount confirmation message can be displayed to the cardholder once the amount is known.

- The message displayed must clearly indicate the status of the transaction. Once the status of the transaction is determined, the terminal must be able to communicate the next action. Clear instructions are especially important when an error occurs and the transaction is terminated. In this case, the transaction message should not indicate a "decline" but rather that an error has occurred. Error messages for chip transactions should be closely aligned with messages for magnetic stripe transactions. Messages for magnetic stripe transactions should be upgraded if they do not already meet these principles.

For contactless transactions, the terminal or the reader should have visual and audible indicators to assist the cardholder. Visual indicators may take the form of LEDs or a display that allows a graphical representation of indicators.

For more information and recommendations regarding terminal messages refer to the *Visa Transaction Acceptance Device Guide* or alternatively the EMV Contactless Specifications, Book A, Architecture and General Requirements which is available from www.emvco.com. This guide includes a list of suggested terminal messages.

5.5 PIN Length and Character Set

The minimum PIN length is 4 digits. PEDs must be able to accept online PINs of 4, 5, and 6 digits.[6,7]

PEDs may visually indicate that a digit has been entered, such as with an asterisk (*). This visual indication should occur for each digit entered by the cardholder. For example, a PED should not display only four asterisks when six digits have been entered. Similarly, if audible tones are used, the tone should be generated each time that a digit is entered. The tone must be the same regardless of the digit entered.

The PIN character set is 0–9.

[6] Note that for ATMs, there may be different requirements for PINs.
[7] PCI PTS requires support for up to 12-digit PINs.

5.6 Cardholder Receipt Requirements

EMV requires that the terminal should always print the Application Identifier (AID), e.g., A0000000031010, on the receipt.

In addition, Visa requires that "VISA" be printed on any receipt where the transaction will be processed by Visa.

Receipts are optional for VEPS transactions. For transactions above the VEPS limit, terminals must generate a receipt.

Note: Cardholders can request a receipt on debit transactions above U.S.$15, even if that is below the VEPS limit.

Further information regarding receipts can be found in the *Visa Transaction Acceptance Device Guide*. Further information regarding VEPS can be found in the *Visa Easy Payment Service – Acquirer Program Guide*.

5.7 Transaction Routing

Final routing decision of a specific transaction is normally determined in the same manner as it is for magnetic stripe transactions, which is primarily through the use of BIN tables. However for chip transactions, the choice of routing possibilities at the acquirer level may be constrained by the AID used for the transaction as decided during application selection (see Section 4.4.3 or 4.5.1).[8]

Processing entities that deploy a device that supports both the Visa ISO AID and the Visa U.S. Common Debit AID must ensure that debit transactions initiated with the Visa ISO AID route to a Visa affiliated network. To support this requirement, Visa currently requires that acquirers and any other routing entities receive the AID used to initiate the transaction. This AID is passed to the terminal in a card data element called the Dedicated File (DF) Name. The acquirer or other routing entities then use the DF Name to perform the appropriate routing process. Acquirers should review and implement this solution based on their needs to achieve appropriate routing. Effective October 1, 2015, Visa requires that DF Name be carried in Field 55 of the authorization request. For more information on the DF Name, refer to Table B–1: V.I.P. System Field 55 Mandated Data Tags.

While the transaction must be routed to a Visa processing network, the actual Visa processing network utilized for the transaction will be defined by the acquirer typically via the use of BIN tables.

[8] Thus the acquirer must receive information about the selected AID used for a specific transaction.

This means that a transaction may be initiated from any Visa AID as defined in Section 4.2.1, but the transaction could be routed to a specific Visa affiliated network. Some examples of this behavior are:

- A transaction initiated using the Visa Global AID on a Visa/Interlink card can be routed to either the Visa network or the Visa Interlink network.
- A transaction initiated using the Visa Global AID on a Visa card can be routed to either the Visa network or the Visa Interlink network.
- A transaction initiated using the Visa Interlink AID on a Visa Interlink card must be routed to the Visa Interlink network.

These examples assume that all other eligibility criteria for the network in question have been met, such as the selected CVM.

It is very important to ensure routing decisions are not negatively affected by chip processing. Acquirers and terminal vendors must ensure that Visa, Visa Interlink, and Plus routing function normally for chip-initiated transactions. This includes transactions initiated for chip cards that contain only the Plus AID, such as non-Visa proprietary cards that are enrolled to use Plus or transactions initiated for chip cards that contain only the Visa Interlink AID, for example, non-Visa branded cards (proprietary debit cards), where Visa Interlink is used as an alternate network.

5.8 Acquirer Stand-In

The rules relating to acquirer stand-in for magnetic stripe continue to be applicable to chip transactions. Acquirers should refer to the *Visa Rules* for further details or contact a Visa representative.

5.9 Deferred Authorization

Deferred or delayed authorization occurs when an online authorization is performed after the card is no longer available. This occurs when the terminal requests an ARQC. The terminal then informs the card that it cannot go online and requests an AAC. Later, the terminal uploads a batch of authorization requests that include the ARQCs for those transactions that received AACs. The acquirer submits the authorization requests, some of which are approved online. The acquirer formats and submits a clearing record for each approved transaction (note: no chip data is required in clearing or settlement of chip transactions that were approved online). A deferred or delayed authorization may occur when a ferry is out of range of shore, for in-flight sales, or when the device does not have online capability (for example, unattended kiosks where the transactions are offloaded nightly to a server and submitted in batches). Merchants performing deferred or delayed authorizations should complete such authorizations within 24 hours of the transaction.

Beyond basic risk management used by the merchant to control risk, such as transaction amount ceiling or velocity checking, there should be no limitations or restrictions on when a deferred authorization is allowed by a merchant/acquirer. Specifically, deferred authorization in the U.S. shall not be restricted based on the performance of Offline Data Authentication as indicated in TVR, byte 1, bit 8 (Offline Data Authentication not performed). As U.S. issued chip cards generally do not support Offline Data Authentication restricting deferred authorization to performance of such a function has the effect of needlessly eliminating the vast majority of U.S. issued chip cards.

Finally, there are special considerations for debit acceptance and deferred authorizations, particularly associated with those transactions where a PIN has been captured. Rather than storing the PIN until the connection has been restored, the PIN Block shall be discarded in order to eliminate the potential for PIN compromise in the event of a breach. The transaction will then be authorized as PINless debit/ credit.

The best solution for PIN debit acceptance with connectivity issues is:

- Disable PIN pad during such outages (i.e., Selectable Kernel)
- Complete transaction as PINless
- Send Deferred Auth, 0100 (credit) without a PIN Block

5.10 Transaction Type Requirements

As with magnetic stripe transactions, chip terminals must support a variety of transaction types. For many of these transactions types, chip transactions should flow similarly to magnetic stripe transactions. In many cases, the Visa requirements and rules for chip transactions are no different from those for magnetic stripe transactions. In some cases, however, change is unavoidable.

Transactions where either the card or the terminal has not completed all required components of EMV processing, including generating an Application Cryptogram, are not EMV transactions. The same applies for contactless transactions and VCPS processing. This includes any transaction where data such as a PAN and expiration date are extracted and used to complete the transaction.

The following sections highlight some differences in transaction type processing that acquirers should be aware of and whether there are any differences between contact and contactless processing.

5.10.1 Pre-Authorizations

A pre-authorization is when an authorization takes place before the final amount is determined. It is usually employed for travel and entertainment transactions. Specific T&E environments have specific Visa rules and best practices regarding how estimated amounts are determined. Pre-authorizations are subject to Visa rules but normally will be EMV transactions (for contact chip) or VCPS transactions (for contactless).

5.10.2 Incremental Authorizations

Where the final amount will exceed or is likely to exceed the amount of the pre-authorization, a further incremental authorization may be obtained. The incremental authorization will be for the difference between the original pre-authorization and the actual or estimated final amount. A merchant may process as many incremental authorizations as are necessary to ensure the authorized amount is equal to or greater than the final transaction amount. Market practice or Visa rules may allow variances above the pre-authorized amount to be cleared for specific transaction scenarios.

Incremental authorizations are usually manual or key entered and are not chip transactions. The original chip data obtained during pre-authorization should not be resubmitted during incremental authorizations. No chip data (except the PAN and expiry date) nor the full Track 2 data should be stored or used for this purpose. Merchants can store the card's PAN and expiry date in order to perform incremental authorizations, as allowed by the Payment Card Industry Data Security Standard (PCI DSS) and Visa rules.

5.10.3 Sale Completion

A sale completion is the financial settlement of a previously pre-authorized transaction, often where the cardholder and card are no longer present. The final transaction amount may differ from the authorized amount, within a range defined by Visa. The sale completion typically does not carry any chip data, as is the case in fuel/AFD environments.

Note: Typically used for travel and entertainment where the final amount is not known.

The POS Entry Mode for a sale completion should be set to "chip read" only if the original online authorization contains a cryptogram and all of the chip data elements used to generate the cryptogram.

Transactions should not be identified as "chip read" unless all mandatory chip functions are performed, including reading all of the required chip data. Transactions identified as chip read, but with incomplete chip data, may be declined.

5.10.4 Status Check and Account Number Verification

A Status Check, sometimes referred to as "pre-authorization" or "pre-auth," is an online authorization for a single currency unit. Status Checks are used as authorizations limited to automated fuel dispensing, implicitly allowing up to a set amount to be used during completion. Status Checks must be sent online because the chip does not have any mechanism to recognize the implicit value of this special transaction.

Account Number Verification is an online message formatted as an authorization for a zero amount. It can be used to validate that the card used to pay for services in advance of delivery or to make a reservation is authentic. However, it is not an authorization and cannot be used to indicate that a clearing transaction was approved.

Except where specifically allowed, if an online validation is desired, an Account Number Verification transaction should be used rather than a Status Check.

5.10.5 Refunds

A refund occurs when the cardholder is credited with the value of returned goods or mis-performed services. Both full and partial refunds of the original transaction may be performed. A refund consists only of a clearing message.

Note: In some environments, the refund may be sent online. However, it is sent as an advice to the acquirer and the acquiring host does not forward the message.

Visa strongly recommends that refunds for contact chip cards be performed by following the normal EMV transaction flow to obtain the Track 2 Equivalent Data field from the chip. If this field is not present on the chip, the terminal should obtain the contents of the PAN and expiration date fields instead.

Once the required data (either Track 2 Equivalent Data or PAN and expiration date) is obtained, the terminal should then stop the transaction flow. The terminal must not request a TC and should request an AAC with the Amount Authorized field set to zero. The terminal completes refund processing normally using the PAN and expiration date.

For a contactless refund, a similar approach is taken by following a normal VCPS transaction flow to obtain the Track 2 Equivalent Data. The Cryptogram Amount for a qVSDC or MSD transaction should be set to zero and the transaction type set to "2x".

Once the terminal has read the Track 2 Equivalent Data information from the contactless chip, the subsequent decision of the contactless chip to approve or decline the transaction is not relevant. Therefore, merchant systems should be able to process the refund irrespective of the cryptogram produced by the card (ARQC or AAC). The decision to approve or decline the refund should be made by the acquirer or merchant in the same way as for magnetic stripe.

If an attempted chip refund fails (for example if the chip cannot be read or chip technology fails during the transaction), the merchant should re-initiate the refund transaction either by using the magnetic stripe or by using manual key entry.

Further information regarding processing of refunds can be found in the *Visa Transaction Acceptance Device Guide*.

Note: For SMS acquiring, as an alternative to the 0220 message, refunds can be processed via Interlink using the 0200 message format. When processing Interlink chip refunds via 0200, all message requirements apply including full chip data.

5.10.6 Reversals

Reversals are a function of the transaction network or of the device application and do not require interaction with the card for generation of the reversal message itself.

A reversal should be generated any time an approval is received for an online authorization request but where the transaction cannot be completed.

In certain circumstances, the issuer may have approved the transactions but the card may override this and decline the transaction. This is primarily due to an Issuer Authentication failure where the cryptogram sent by the issuer in the response message failed verification by the card. In this case, the terminal should initiate a reversal.

5.10.7 Referral

A referral is intended as a fraud control tool for issuers to use when more information is needed to verify the identity of the cardholder or the validity of the card prior to approving a transaction. A referral is not a “transaction”; it is an exception process for a purchase. Referrals are generally not recommended for Visa payWave transactions as they impede the convenience of a fast transaction which is associated with Visa payWave. When a referral authorization response is received from the card issuer, the terminal should request an AAC from the card. Generation of an AAC completes the EMV transaction flow so that the referral procedure can take place. The cryptogram produced by the card should be disregarded by the terminal as any subsequent approval of the transaction is dependent on the outcome of the referral process.

Depending on the implementation, the referral process will most likely result in a completely new transaction taking place generally when the card issuer has removed the referral block. Alternatively, the chip data can be used to create a clearing record to which the authorization code from the voice authorization is added. The clearing record can contain the ARQC and related data. However, because the chip data was not presented to the issuer at time of authorization, the POS Entry Mode must indicate manual entry.

5.10.8 Cancellation

A cancellation occurs when a purchase or sale completion transaction is aborted either during or after processing. In a dual-message environment cancellation should only occur before the transaction is “cleared” to the acquirer.

There are a number of reasons why a cancellation may occur, for example, an error in the amount entered by the merchant which the merchant may seek to correct by pressing a cancel button on the terminal. Cancellations also occur when a merchant does not approve the cardholder’s signature.

In all cases, initiation of a cancellation should result in the cessation of processing and clearing of any data elements.

If the transaction has not reached the point where an ARQC has been requested, the card can simply be powered off.

If an ARQC has been requested and the transaction has been routed online, then cancellation processing must also generate an authorization reversal. The transaction should be removed from the clearing batch or marked 'void'.

If the terminal has received a TC or AAC from the card, the transaction is completed and can be cancelled (removed from the batch or marked as void).

It is recommended that the terminal produce a receipt for the cardholder showing that the original transaction has been cancelled.

5.10.9 Cryptogram Generation in Multi-Currency Scenarios

Certain terminals have dynamic currency conversion capabilities and are able to handle multiple currencies. It is critical that the currency code used in the generation of the cryptogram (ARQC or TC) is the same as is included in the authorization and clearing messages (V.I.P. Field 55 Tag 5F2A) and is not altered by any intermediary networks. A change in the currency code could lead to the issuer declining the transaction as the cryptogram validation may fail.

In most scenarios, the transaction currency, V.I.P. Field 49, should contain the same value as the chip data related currency in V.I.P. Field 55 Tag 5F02. There may be instances where these differ. It is critical that the chip related field is not modified from the transaction currency that was sent from the terminal to the card and was used by the card to generate the cryptogram.

5.10.9.1 Implementation Activities

Acquirers should review the requirements for supporting transaction types in a chip environment and work with their terminal vendors to ensure terminals support the chip requirements. Further details are provided in the *Visa Transaction Acceptance Device Guide*.

5.11 EMV Transactions in Specific Industries

Certain industries have specific payment requirements besides the traditional purchase. For each scenario, the presence of a chip card may or may not have an impact on existing processing requirements. The following industries are affected by the introduction of chip, and have corresponding recommendations from Visa:

- Hotels and car rentals
  - Hotel Reservations—Handle reservations as you normally would. The reservation process usually does not involve the card being present or the chip being read.
  - Hotel Check-In / Vehicle Check-Out—Complete estimated authorization at Check-In/Vehicle Check-Out. Determine an appropriate estimated amount to be authorized, based on the guidelines outlined in the *Visa Acceptance Guide for the Lodging Industry* and *Visa Acceptance Guide for the Car Rental Industry* available at www.visa.com. Process the authorization as you do today.
  - Extended Rental/Higher Estimated Spend—If the estimated amount of the original authorization is no longer adequate to cover the estimated final bill, perform an incremental authorization. The card does not need to be present, and the authorization should not include chip data.
  - Hotel Check-Out / Vehicle Check-In—It is not necessary to perform a full EMV chip transaction once the final transaction amount is known. Generate a sale completion for the final billing amount and, if chip data is required for clearing, then include the chip data from the original authorization. The final amount should be displayed to the cardholder. Provide receipts as you do today.
- In-Flight transactions
  - Deferred Authorizations—See Section 5.9 for additional information.
- Restaurants
  - Gratuity—After authorization, add any gratuity or tip of up to 20 percent of the base transaction amount to the authorized amount submitted in the clearing record, just as you do today. In this instance, the authorized amount should always be equal to the amount of the bill prior to any added tip. See *Chip Payment Acceptance for Restaurant Merchants* for more information.

For more information regarding changes for specific industries, acquirers should refer to the following documents:

- *Visa Transaction Acceptance Device Guide*
- *Visa Payment Acceptance Best Practices for Retail Petroleum Merchants*

Recommendations for EMV Processing for Industry-Specific Transaction Types, available from www.emvco.com

5.12 Purchase with Cash-back

Visa allows cash-back with a purchase at the point of service for domestic transactions, under certain conditions. Cash-back is sometimes referred to as cash-back or cash-out. Current Visa rules do not allow cash-back to be provided on credit cards or when the cardholder has selected to use a credit facility. Cash-back is also not recommended for Visa payWave transactions as they diminish the speed and convenience factors that are key features of Visa payWave. However, issuers may elect to support cash-back with their Visa payWave cards and terminals should process the transactions according to cash-back rules.

Where permitted, a terminal must send the cash-back amount to the card when requested and then send the following cryptogram data to the acquirer for inclusion in the online message:

- Cryptogram Amount (V.I.P. Field 55 Tag 9F02) – The total of the purchase amount plus the cash-back amount
- Cryptogram Cash-back Amount (V.I.P. Field 55 Tag 9F03) – The cash-back amount

If the transaction involves cash-back, the Cryptogram Cash-back Amount must be present and included in the ARQC algorithm. If the transaction does not involve cash-back, the ARQC is calculated with a zero cash-back amount and the field is not present or is zero-filled.

5.13 Terminal PIN Requirements

When supporting PIN, acquirers must ensure their terminals adhere to the *Visa Rules* and PCI PIN Transaction Security (PTS) requirements. These PIN capable terminals may have either a PIN pad or a port capable of supporting a PIN pad.

If a PIN pad is present and active, it must comply with Visa's requirements. If the PIN pad is inactive or not present, the terminal may have the capability to support the required software to enable a PIN pad to be connected and to comply with Visa's requirements.

Acquirers should refer to the *Visa Rules* or contact their Visa representative for further information regarding PIN pad requirements.

5.14 Terminal Types and Configurations

Acquirers should consider all the possible terminal configurations and ensure that each terminal type is reviewed against the possible impact of migrating to chip acceptance. It is also important for acquirers to review the *Visa Rules* and other Visa documentation and ensure specific terminal type requirements are incorporated into their selection criteria and requirements.

5.14.1 Shared Display and Separate Display Terminals

Attended terminals may have a shared display or separate displays for the customer and the merchant to carry out the transaction. The terminal type used at a merchant is dependent on the terminal itself and the merchant environment.

Terminals may have a single display shared by the merchant and the customer during the transaction process.

Terminals with a separate display have a dedicated display for the merchant and one for the customer. These typically comprise a fixed enclosure for the merchant terminal and a tethered PIN pad with a dedicated display for the customer.

In general, and unless specifically stated, all requirements and best practices apply to both types of terminals. Support for application selection by cardholders may require special considerations where there are separate displays.

5.14.2 Unattended Cardholder Activated Terminals

An Unattended Cardholder Activated Terminal (UCAT) is an acceptance terminal managed by a merchant that dispenses goods or services without the assistance of an attendant to complete the transaction. Cardholder verification and authorization of such transactions occurs electronically, if required. These terminals include automated dispensing machines and self-service payment terminals in parking garages.

Note: The Visa Rules prohibit Visa card products from being used for scrip transactions. (Scrip is a receipt redeemable for goods, services or cash.)

UCATs fall into two categories:

- **Unattended Authorized**—Transactions are authorized and cardholder verification is not performed.
- **Unattended Authorized with PIN**—Transactions are authorized and online PIN entry is performed.

A UCAT must support "No CVM Required" to ensure CVM processing can be completed. Otherwise UCATs that support chip need to adhere to the general Visa requirements for chip terminals.

The following are not considered UCATs and are not required to meet UCAT Requirements

- ATMs, which must meet a different set of requirements.
- Attended cardholder activated terminals, for example, self-checkout terminals in supermarkets, where an attendant is available to help complete transactions.

5.14.3 Dual-Interface Terminal Configurations

The physical architecture of a terminal that supports both contact and contactless transactions can be any of the following:

- Fully integrated terminal: All elements included in a single device.
- Intelligent card reader: The reader handles most of the contactless transaction processing, passing the results for completion by the terminal.
- Combination of terminal and transparent card reader: The reader provides communication with the card, while kernels and other processes are in the terminal.

Acquirers need to determine which architecture best suits their needs and those of the merchants, including whether some of their existing infrastructure can be reused to support their migration to VSDC and Visa payWave acceptance.

Further information regarding contactless terminal configurations and requirements can be found in the EMV Contactless Specification for Payment Systems, Book A.

5.14.4 Automated Fuel Dispensers

An Automated Fuel Dispenser (AFD) is a self-service terminal or an automated dispensing machine that dispenses fuel such as gasoline, diesel fuel, or propane. The *Visa Rules* have specific requirements relating to the amount that an AFD can authorize before fuel is dispensed. These limits vary between chip and magnetic stripe and acquirers should review the *Visa Rules* for further information.

AFDs must do one of the following:

- Obtain an authorization for the exact amount of the transaction
- Use the Status Check / Pre-Auth Procedure, including use of an advice for final amount
- Process the transaction using Real Time Clearing

The above-mentioned processing requirements are not affected by support for chip. However the terminal needs to adhere to the general Visa requirements for chip terminals.

Acquirers should also note that the rules relating to AFDs and the liability shift for chip transactions are different to other device types. Further details are provided in Section 11.2 EMV Liability Shift.

5.14.5 Automated Teller Machines

Information regarding ATM requirements is not in scope of this document.

5.15 Terminal Requirements for CVM

Visa CVM requirements for terminals include:

- An attended POS terminal must support signature (for transactions that require a CVM) and it may support PIN. A terminal must not prompt international cardholders for PIN unless required by the chip card.
- A UCAT must support "No CVM Required."
- VCPS 2.1, including all published updates, and higher readers must enable support for a Consumer Device CVM. The Consumer Device CVM is a CVM performed on the consumer's payment device (independent of the reader).

Requirement

- If Visa Interlink is supported, online PIN must be supported for both contact chip and Visa payWave.
- In addition, some cardholders may be unable to enter a PIN at the POS terminal, or unwilling to do so due to security concerns or certain disabilities. Terminals need to support functionality that allows merchants to offer an alternative CVM than PIN for such cardholders.

6. Terminal Selection and Approval

This Section is intended to assist acquirers in creating selection criteria for chip terminals and provides background information on the terminal approval process before deployment in the field. It includes the following topics:

- Terminal and Reader Selection Criteria
- Terminal and Reader Approvals
- Considerations for EMV Approval for Contact And Contactless
- Payment Card Industry Requirements
- Acquirer Testing Toolkits and Host Testing
- Implementation Activities

The information included in Sections 4 and 5 should be considered when creating the selection criteria and as part of any requirements documentation provided to terminal vendors.

6.1 Terminal and Reader Selection Criteria

Prior to meeting with vendors and reviewing their available products, acquirers should develop their terminal requirements. Acquirers should begin the process by determining the minimum required, and recommended terminal requirements as outlined by Visa and the local environment.

This Section provides an overview of information acquirers could include in their terminal selection criteria. This is not meant to be an exhaustive list; it is intended to provide some guidelines to assist acquirers. Acquirers should:

- Ensure any terminals support and are in compliance with:
  - EMV requirements as outlined in the EMV Specifications and specification bulletins.
  - PCI requirements relating to PIN security (PCI-PTS) and Application Security (PCI PA-DSS)
  - Visa requirements as defined in the *Visa Rules*, *Visa Transaction Acceptance Device Requirements*, and other Visa documentation.
  - Ensure contactless readers comply with Visa's contactless reader requirements (refer to Section 3.2 U.S. Contactless Acceptance Requirements)
  - The reader has been tested and approved by Visa and is on the approved Visa Approved Product list.

- Ensure that the EMV-compliant chip-reading terminal:
  - Reads a magnetic stripe
  - Reads the chip, if an EMV-compliant chip is present, and does not allow for overriding the chip authorization controls by manually prompting the cardholder to use the magnetic stripe. The magnetic stripe may be read only if the chip is **not** EMV/VSDC-compliant, no AID(s) are in common, or if the chip or chip reader is inoperable (resulting in a fallback transaction).
  - Supports transaction type requirements; for example, pre-authorizations, reversals, referrals, and refunds.
  - Supports magnetic stripe terminal requirements, such as fallback processing and compliance with requirements for reading service codes.
  - Where Cardholder Selection is supported, provides selection to the cardholder from a list of both domestic and non-domestic payment applications as mutually supported by the card and terminal.
- Identify terminal types to be supported; for example, stand-alone point-of-transaction terminals, integrated POS terminals ("ECR"), mobile POS terminals, or UCATs.
- Identify requirements for a terminal-based exception file, if any.
- Identify cardholder verification requirements and how they are used for supported environments (online PIN and signature), including PIN length requirements.
- Ensure terminals respect cardholder CVM selection.
- Ensure terminals are equipped with ports that support peripherals capable of prompting, and accepting, a PIN based upon the CVM list on the card.
- Evaluate price versus functionality, hardware, and software peripherals, warranty conditions, and service and support agreements.
- Ensure that: the terminal is approved to EMV Level 1 and Level 2; EMVCo approval letters are available; the terminal is listed in the EMVCo website as having current approval and has an adequate approval period remaining to allow all testing to be completed.
- Ensure the terminal complies with Payment Card Industry (PCI) requirements and a PIN-accepting terminal is listed in the PCI published list of approved terminals.
- Ensure maintaining PCI compliance by properly installing payment applications securely.
  - Due to merchant breaches caused by payment applications improperly installed by integrators and resellers, the Payment Card Industry Security Standards Council (PCI SSC) updated Qualified Integrators and Resellers (QIR) Program to provide guidelines, training and certification.
  - Merchants should leverage the use of PCI QIRs when making changes to their POS environment.
- Confirm with the terminal vendor that the terminal was developed in compliance with the *Visa Rules*, *Transaction Acceptance Device Requirements*, and other applicable Visa documentation.

- Determine merchant requirements for terminal configuration, for example whether to require a separate chip acceptance terminal or a peripheral PIN pad unit, and that these terminals meet Visa's requirements.
- Verify product availability.
- Determine requirements for transaction speed and estimate the transaction volume to be supported.
- Identify which components of the complete merchant configuration are affected by chip, and identify:
  - Components that can be modified by software changes
  - Components that require new hardware
  - All of the involved vendors
- Conclude whether existing terminals can be upgraded or new terminals are required.
- Identify any additional technological features required, such as cell phone capability, or Internet connectivity.
- Determine if the terminal can be supported with the acquirer's existing Terminal Management System or if there is an impact to an existing one.
- Determine whether it is necessary for the terminal or reader to:
  - Have incorporated terminal logic to perform special application selection process to support merchant routing preferences.
  - Be able to transfer the result of special application selection process to the acquirer – in support of merchant routing preferences.
  - Support selectable kernels in support of specific CVM conditions (cash-back and VEPS).
- Complete ADVT and CDET terminal testing prior to deployment.

6.2 VSDC Terminal Approvals

Acquirers must select a product that meets all the various requirements related to EMV and VSDC and has been approved accordingly. At a minimum a terminal must meet EMV Level 1 and EMV Level 2 requirements and be noted as an approved product by EMVCo and listed in the EMVCo website. Information regarding the EMVCo approval process can be obtained from the EMVCo website at www.emvco.com.

All terminals that accept Visa cards must also comply with the *Visa Rules*. Many requirements specific to acceptance terminals, including for contact chip, are included in the *Visa Transaction Acceptance Device Requirements* document, a *Visa Rules* extension document. For additional information on the Visa-specific terminal requirements and best practices, refer to the *Visa Transaction Acceptance Device Guide*.

Terminals must comply with the PCI Data Security Standards (DSS), and often with the PCI Payment Application Data Security Standards (PA-DSS) relating to application security. Terminals accepting PINs must comply with the Payment Card Industry (PCI) PIN Transaction Security (PTS) Pin Security Requirements, Point of Interaction (POI) Modular Security Requirements and the Visa PCI PIN Security Requirements.

For more information on PCI PIN PTS testing including the Visa PIN Security requirements, refer to www.visa.com/pinsecurity and www.pcisecuritystandards.org/security_standards/ped.

The following sections provide further details on the various approvals required that acquirers need to consider as part of their VSDC migration project.

6.3 Considerations for EMV Approval

To accept Visa chip transactions, terminals must be approved for EMV Level 1 and Level 2 by an EMVCo-accredited laboratory. Compliance to the most current version of the specification will ensure that the terminal is able to more easily satisfy the testing requirements to gain approval.

6.3.1 EMV Level 1

EMV Level 1 approval is given for the interface modules (IFMs) – that is, the chip card reader – rather than for the terminal on which it is tested. An IFM consists of the hardware and software that powers the chip card and supports communication between the terminal and the card up to the transport layer. The three main functional components are the mechanical, electrical, and logical chip card interfaces.

An approved IFM can be used for any terminal, as long as the IFM is not modified and can be used with any approved EMV application kernel. It is important to identify the IFM component separately from the terminal, using a unique identifier.

6.3.2 EMV Level 2

EMV Level 2 Type Approval tests comply with the application requirements defined in the EMV Specifications. EMV Level 2 approval is not tied to a particular model of a particular type of hardware platform. The approval letter notes the hardware configuration to be used for testing. The portion of the application that performs EMV functions and is tested as part of the Level 2 Type Approval is commonly referred to as the "kernel."

An application kernel is approved to run on any terminal that has an approved IFM and supports the environment used during testing. If the kernel can be used on a terminal without recompilation, the kernel retains its EMV approval. EMV Level 2 test cases are performed only against EMV functions. Acquirer, payment scheme, and national specifications are not part of EMV testing.

An application provider may simulate any non-EMV functions necessary for the completion of the test cases, for example, message formats, communications protocols, terminal prompt sequences, or payment scheme settings. These other functionalities, however, do not necessarily represent the end product because some level of customization may be required for each acquirer, country, or payment scheme.

Rigorous testing needs to be performed to ensure that customizations and application changes have no adverse impact on the EMV kernel and functions.

A terminal must have an IFM that has been approved for EMV Level 1 before its EMV application kernel can be tested for Level 2.

6.3.3 EMVCo Approvals and Renewals

EMVCo has a renewal policy requiring all IFMs and kernels to be re-tested on a regular basis.

An IFM approval is valid for 4 years and an application kernel approval is for 3 years. This validity period applies to static and configurable kernels.

At expiration of the approval, EMVCo evaluates whether the product, either the IFM or the kernel, demonstrates sufficient conformance to the current EMV specification and may grant an extension. IFMs or kernels that do not pass the evaluation will not be granted an extension and their approval will be considered expired.

EMVCo may also revoke an approval of an IFM or kernel if a significant interoperability problem arises in the field.

Visa policy relating to terminal approvals requires that ADVT be performed only on terminals that are EMVCo approved. Acquirers should ensure that any new terminal installations contain IFMs or kernels that have a current EMVCo approval.

Further information on the EMVCo renewal policy can be found in the EMVCo website at www.emvco.com.

6.4 Contactless Reader Approvals and Renewals

Visa oversees testing of card acceptance devices that support Visa contactless payments. This process allows Visa to ensure that the devices are developed to Visa specifications and will support Visa applications.

Additionally, Visa recognizes the contactless Level 1 (analog and digital) testing offered by EMVCo for devices. Visa recommends that contactless devices have their contactless Level 1 tested and approved by EMVCo prior to submitting the device to Visa for application testing. The approval and renewal process for contactless devices is similar to that for contact chip as outlined in Section 6.3.3 EMVCo Approvals and Renewals.

Further information regarding EMVCo contactless approval can be obtained from the EMVCo website at www.emvco.com.

To facilitate the testing of devices, Visa has recognized a number of independent laboratories to functionally test devices containing Visa payment applications on behalf of Visa.

If the device is successfully tested, Visa issues a letter of approval to the device vendor that submitted the device for testing. The approval applies internationally, unless restrictions are specified in the letter of approval.

Note: Approval is not transferable from one vendor's product to another.

Upon successful completion of official testing, the card acceptance device will appear on one of the Approved Acceptance Device Products Lists located at Visa Technology Partner site (https://technologypartner.visa.com).

When a device product is approved by Visa, it is assigned a renewal date which is communicated to the device vendor in the letter of approval and also appears on the Visa Approved Products List.

Note: The renewal date is typically two years after the date of approval unless otherwise noted.

As a device approaches its renewal date, Visa reviews the product details to ensure that it complies with all current Visa policies and includes a payment application(s) that Visa continues to support. Further information regarding Visas current renewal policies is available from Visa Technology Partner site (https://technologypartner.visa.com).

6.5 Payment Card Industry Requirements

The Payment Card Industry (PCI) Security Standards Council (SSC) is an open global forum, launched in 2006, that is responsible for the development, management, education and awareness of the PCI Security Standards, including:

- Data Security Standards (PCI DSS)
- Payment Application Data Security Standards (PA-DSS)
- PIN Transaction Security (PTS) requirements

The Council's five founding global payment brands, (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.), have agreed to incorporate the PCI DSS technical requirements into their data security compliance programs.

6.5.1 PIN Entry Devices

A PIN Entry Device (PED) is any device used by a cardholder to enter a PIN. (It may also have other functions.) A PED that supports online PIN where the PED and chip reader are not integrated must contain an Encrypting PIN pad (EPP) used for entering a cardholder PIN.

The PED and EPP may be integrated, as in some standalone POS terminals, or the EPP may be just one component of a PED, as in a UCAT. Further information regarding requirements for PEDs can be found in the *Visa Transaction Acceptance Device Guide*.

6.5.2 PED Testing Requirements

Visa requires testing of PEDs against the PCI PIN Transaction Security (PTS) requirements if they are used in the acceptance of Visa card products with offline PIN or online PIN verification. PEDs and EPPs must undergo a physical and logical security evaluation performed at a PCI recognized test laboratory.

For information on PCI PIN entry device security requirements, see www.visa.com/PIN and www.pcisecuritystandards.org/security_standards/.

6.5.3 Payment Application Data Security

Visa has introduced compliance mandates requiring all new merchants to be PCI-DSS compliant, including using payment application software that uses Payment Application Data Security Standard (PA-DSS) compliant applications.

Acquirers must ensure that their merchants and agents use PA-DSS compliant payment applications. For purposes of the mandates, payment applications apply only to third-party payment application software that stores, processes, or transmits cardholder data as part of an authorization or settlement of a payment card transaction. POS terminals are an example of this.

PA-DSS does not apply to merchant or agent in-house developed applications, stand-alone hardware terminals or PEDs. Payment application vendors must validate the conformance of their products to the PA-DSS. Acquirers should insist that their merchants and agents use compliant applications and upgrade or patch applications to ensure the storage of sensitive cardholder data meets the Visa mandates.

More information can be found at www.visa.com and https://www.pcisecuritystandards.org/security_standards/.

6.6 Acquirer Device Validation Toolkit

Visa recognizes that acquirers and terminal vendors need a clear and easy way to validate that their contact chip terminals are configured to meet their domestic and regional market needs and that international chip cards entering their countries experience the same level of acceptance.

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

The *ADVT User Guide* and *U.S. Quick Chip and Minimum Terminal Configuration ADVT Use Cases* provide guidelines with details of the specific conditions that determine the use of ADVT.

If a terminal is configured for online-only functionality, the subset of ADVT can be used. If deploying online-only terminals that previously completed ADVT but are now intended to support Quick Chip, then regression testing is recommended using the ADVT subset of test cases (*U.S. Quick Chip and Minimum Terminal Configuration ADVT Use Cases*). Chip Compliance Reporting Tool (CCRT) submission is optional. If it is a new online-only terminal deployment with Quick Chip support, then the *U.S. Quick Chip and Minimum Terminal Configuration ADVT Use Cases* can be supported with test results submitted into CCRT.

6.6.1 ADVT and EMVCo Approval

Use of the ADVT does not preclude the requirement that contact chip terminal components be approved by an EMVCo-accredited laboratory. EMVCo approval is a prerequisite for a terminal to be validated by acquirers using the ADVT. Use of the ADVT is intended to ensure basic chip functionality is not compromised during application integration and that basic Visa requirements are met, as well as to uncover exposures to some common interoperability issues. Use of the ADVT does not imply or guarantee that a terminal is fully compliant with EMV specifications or Visa requirements.

6.6.2 ADVT and Expired EMV Approvals

To encourage the deployment of modern kernels and interface modules (IFMs) that are less susceptible to interoperability issues, Visa requires that an acquirer must not submit ADVT testing results to Visa for terminals containing kernels and IFMs that have expired.

This rule only applies where the results of ADVT testing are to be made available to Visa. Other uses of ADVT, such as for internal regression testing, are not affected. Acquirers participating in Visa U.S. Chip Acquirer Self-Accreditation Program will be granted a one-year blanket waiver from the kernel expiration date for acquirer end-to-end testing performed on an expired EMVCo-approved kernel supporting Quick Chip or Visa Minimum U.S. Online-Only Terminal Configuration. A waiver request will not be required.

This will not affect deployed terminals or the deployment of terminals already approved against ADVT. However, it will prevent the deployment of new and updated terminal configurations that use expired hardware or software. To reduce terminal testing requirements, as well as to minimize the impact when necessary updates/changes to existing terminals are deployed in the market, Visa recommends acquirers and merchants become familiar with the IFM revisions and kernel versions being supported in their terminals to assist in proper EMV kernel management. Kernel management promotes terminal vendor communication and standardizing solutions.

More information on the requirements and rules can be found in the ADVT User Guide.

6.6.3 ADVT and CDET Ordering Process

The ADVT and CDET toolkits can be obtained from Visa's third party fulfillment service. If you prefer to use a test tool, ADVT and CDET card profiles are available from confirmed third-party test tool vendors. For a list of Visa U.S. Confirmed Third-party Chip Acceptance Tool Suppliers, see U.S. Supporting Documentation at https://technologypartner.visa.com. For a list of global products, refer to Visa-confirmed tool vendors, see Products and Toolkits at https://technologypartner.visa.com.

6.6.4 Contactless Device Evaluation Toolkit

In addition to the use of ADVT, terminals that support Visa payWave must comply with Visa's Contactless Device Evaluation Toolkit (CDET). Similar to ADVT, CDET allows acquirers to validate the correct configuration of their contactless readers. The toolkit is also a self-administered solution. For new reader deployments, the acquirer executes each applicable CDET test to confirm that the expected outcome is achieved.

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

Visa rules regarding support for MSD and qVSDC have recently been modified so that:

- Effective 10 April 2015, contactless terminals deployed between 1 April 2013 and 31 December 2014 must comply with the VCPS 2.1.1 (or higher), and be capable of processing a transaction using both the MSD and qVSDC transaction paths (though the terminal may actively support only the MSD transaction path).
- Terminals deployed on or after 1 January 2015 must comply with the VCPS 2.1.1 (or higher), and be capable of processing a transaction using the qVSDC transaction path (though the terminal may actively support only the MSD transaction path).

Further information can be found in the *CDET Toolkit User Guide*.

6.6.5 Chip Compliance Reporting Tool

Visa developed the Chip Compliance Reporting Tool (CCRT) as a centralized, server-based solution for the systematic reporting of ADVT and CDET test results. The CCRT facilitates a more efficient submission and management process of compliance reporting by chip acquirers.

CCRT provides Visa acquiring clients with an appropriate level of security and confidentiality in managing their ADVT and CDET test results, and enables the CCRT service to be consolidated with other services currently provided. CCRT is available on Visa Online (Visa's online solution for providing secure access to Visa content and services for clients globally).

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

6.7 Additional Toolkit Requirements

Visa recommends that Acquirers use the ADVT and CDET toolkits prior to initial terminal deployment (including all variations of hardware, software, and parameter settings) to ensure that the terminal has been set up and configured correctly. It is expected that acquirers will run every applicable test to gain the full benefit of the toolkit. When the acquirer's test results do not match the expected outcome of the test, the acquirer should work with its terminal vendor (and Visa, if necessary) to correct the problem. The acquirer will continue to perform the test until the problem is resolved and the acquirer's test result matches the expected outcome. An acquirer that fails to use the ADVT and CDET toolkits on a device that causes interoperability issues may be subject to non-compliance assessments as defined in the Visa Chip Interoperability Compliance Program. Refer to Section 7.3 Chip Interoperability Compliance Program for more information.

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

Visa may ask the acquirer to undertake further ADVT or CDET testing if there is strong evidence that a terminal is causing acceptance or interoperability problems.

After an acquirer successfully completes the ADVT and CDET Toolkits testing, the test results are provided to Visa by submitting the results into the CCRT. U.S. clients should submit into CCRT using U.S. versions of ADVT and CDET which include U.S. debit test cases. Acquirers participating in Visa U.S. Chip Acquirer Self-Accreditation Program should refer to Section 6.9: Visa U.S. Chip Acquirer Self-Accreditation Program.

6.8 Visa Chip Vendor Enabled Service (CVES)

This service, launched in October 2013, will help streamline the testing and reporting requirements for the deployment of ATM and point-of-sale chip-acceptance devices in the U.S. CVES engages third-party chip tool vendors to execute mandatory Acquirer Device Validation Toolkit and Contactless Device Evaluation Toolkit testing on behalf of acquirers and processors, analyze the results and optionally submit reports to Visa using the Chip Compliance Reporting Tool.

Vendors choosing to participate in CVES must complete a confirmation process by which the vendors' eligibility is verified and the ability to effectively deliver the required services is demonstrated. For a list of Visa U.S. Confirmed Third-party Chip Acceptance Tool Suppliers, see U.S. Supporting Documentation at https://technologypartner.visa.com. For a list of global products, refer to Visa-confirmed tool vendors, see Products and Toolkits at https://technologypartner.visa.com.

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

Visa introduced the Visa U.S. Chip Acquirer Self-Accreditation Program, which enables U.S. acquirers to self-certify their chip point-of-sale (POS) devices. The new self-accreditation program for U.S. acquirers eliminates the need to use the CCRT to report ADVT and CDET terminal test results when they deploy chip POS solutions. The program streamlines acquirers' chip-testing process and removes redundant terminal test result reporting. It also allows acquirers to adjust their test plans based on the POS solution and merchant vertical where the terminal is deployed, enabling them to perform the Visa-recommended minimum set of test scripts for both contact and contactless solutions. Refer to the *U.S. Quick Chip and Minimum Terminal Configuration ADVT Use Cases* for more details.

6.9.1 Eligibility Requirements

To ensure all U.S. acquirers can take advantage of simplified terminal certification, acquirers will need to:

- Partner with an accredited CVES vendor that can execute, analyze, and validate terminal test results and has the capability to store test results, receipts, and logs for up to five years or has the equivalent chip tool capability available in-house.
- Have established testing processes and requirements (defined EMV terminal test cases).
- Complete the *Visa U.S. Chip Acquirer Self-Accreditation Program Acknowledgement Form*.
- Ensure all deployed terminals have all errors resolved and successfully "pass" testing.

6.9.2 Attestation Process

In exchange for simplified certification, acquirers must:

- Upon request from Visa, provide logs, receipts, and test results to resolve interoperability issues.
- Work with Visa to develop a remediation plan when interoperability issues are identified.
- Visa may ask the acquirer or merchant to undertake specific post-deployment testing if a terminal is causing acceptance issues in the field.
- An acquirer that fails to meet program requirements and causes interoperability issues will be managed through the Visa Chip Interoperability Compliance Program.

6.10 Acquirer Host Testing

One iteration of CDET and ADVT terminal testing needs to be completed prior to host testing. An acquirer will use a production ready terminal (EMVCo and Visa approved) which has completed terminal testing for host testing. An acquirer can also run the host test cards through a terminal prior to host testing. Further information regarding host testing can found in Section 10: Acquirer Host Testing.

6.11 Implementation Activities

To launch a program in the shortest timeframe, Visa recommends selecting a vendor that is already approved. A list of EMVCo-approved products and vendors may be found at www.emvco.com.

- Develop terminal requirements using the information in this Section as a guideline as well as the requirements and considerations outlined in Section 3 and Section 4.
- Review vendor products to determine which vendors meet the requirements. This may be accomplished through a Request For Proposal (RFP) process.
- Ensure that the vendor selected has obtained approval for EMV Level 1 and Level 2 or is in the approval process and EMV Level 1 contactless approval.
- Ensure that the contactless reader selected has obtained Visa approval and is listed on the Visa Approved Vendor List.
- Ensure that if PIN is a requirement in the selection criteria that terminal vendors have received PCI approval and the terminal is listed in the PCI website.
- Once terminals and reader have been selected, it is important to work with any preferred vendor to ensure they comply with Visa's requirements as well as any U.S. market requirements.
- The vendor should also integrate ADVT and CDET testing as part of their delivery schedule and ensure enough time is allowed to ensure adequate testing.

7. Terminal Testing and Maintenance

This Section outlines Visa's recommendations for acquirers to undertake post deployment testing to address and resolve acceptance and interoperability problems that may be inadvertently introduced during rollout. Visa has developed a number of toolkits that can assist acquirers.

The Section includes an approach and guidelines acquirers can follow to minimize the chance of terminals or contactless readers creating interoperability problems and the potential impacts, including Visa penalties, if interoperability issues are not addressed as defined in the Visa Chip Compliance Program.

7.1 Terminal Testing Process

Maintaining the reliable and efficient operation of acceptance terminals is critical to ensuring Visa cardholders continue to trust the payment system. The introduction of chip terminals may lead to unforeseen issues being introduced due to the complexity and possible lack of experience by acquirers or merchants. Problems could be created due to a lack of controls and processes around the deployment of production terminals in the field which could lead to:

- Incorrectly configured terminals or readers
- Deployment of untested or unapproved terminals or readers
- Deployment of outdated terminal applications
- Merchant training issues

To minimize the chance of these issues occurring, Visa has a set of testing toolkits designed to assist acquirers in detecting potential problems before they lead to interoperability or general acceptance problems. Refer to 6.6: Acquirer Device Validation Toolkit for more details.

Note: Visa recommends merchants with integrated systems complete the online test in CDET and ADVT into VCMS.

7.1.1 Production Testing Toolkit

Acquirers requesting production cards that can be used for testing in deployed production terminals should consult with their Visa Representative. Because testing is undertaken in production, the process is able to verify all the components that enable the transaction to occur, including the processing at the acquirer host. In some instances, an acceptance problem may not be caused by a terminal but by incorrect processing at the host level.

7.2 Interoperability Problems

The introduction of EMV chip has increased the complexity of the payment application in cards and terminals when compared to magnetic stripe. There are many parameters and options that must be set within both the chip card and the terminal to ensure that payment can occur and that the benefits provided by EMV are realized. Incorrect setting of these parameters can lead to interoperability problems. Interoperability is defined as the ability for all card acceptance terminals to accept and read all chip cards that are properly programmed. An interoperability problem may occur when parameters or settings on either the card or the terminal, or both, result in a condition where the payment cannot be completed. This can occur even when the terminal and the chip card are fully compliant with the EMV Specifications.

Principles acquirers should consider to reduce interoperability issues include:

- Acquirers must implement correct application of the EMV specifications, coupled with rigorous compliance and acceptance testing for both hardware and software for both chip card and terminal.
- Acquirers should regularly monitor interoperability bulletins published by EMVCo. These can be found at www.emvco.com. Visa also provides information on possible interoperability issues directly to its acquirers.
- Acquirers and merchants should ensure that their terminals use the features which EMVCo approved for their kernel. Terminals should not use features that were not tested during EMVCo Type Approval. Features that were included in Type Approval should not be turned off. If acquirers prefer to use multiple configurations in their terminals, the correct solution is to use a configurable kernel. Each configuration must be EMV approved before it is deployed. Terminal Management Systems should only load terminals with approved configurations. Kernels must be deployed only as a tested configuration.
- Terminals should be tested with ADVT and/or CDET for all new terminal models and new or altered configurations prior to deployment. ADVT and CDET are specifically designed to test for and help prevent known interoperability issues for the acceptance of Visa chip cards. Acquirers should have production support procedures to address and resolve issues that may arise with EMV type approved terminals already deployed in the field. If a problem is detected and diagnosed, any remedial plan should be enacted in a timely manner.
- If an acquirer suspects a problem with a deployed production terminal, they should use ADVT, CDET, and the production testing toolkit to assist in their analysis.
- Acquirers should ensure they test VCPS Version 2.1 or higher readers with a Version 1.4.2 card and a 2.0.2 (or higher if applicable) card to ensure the reader is correctly processing transactions using older cards.
- Terminals should support all 4 bytes of the Terminal Transaction Qualifiers as defined by VCPS. Failure to do so may result in issuer's declining transactions.

- Acquirers should have production support procedures to address and resolve issues that may arise with EMV type approved terminals already deployed in the field. If a problem is detected and diagnosed, any remedial plan should be enacted in a timely manner.
- Interoperability problems may not be immediately apparent, but could develop later in the lifecycle of a terminal. This may be due to an EMV feature for which the terminal had been approved, being introduced into the market sometime after the terminal had been initially deployed. The feature may cause an interoperability issue with the terminal model, which otherwise had exhibited no issues prior to the feature being deployed.
- If high levels of CVM failures or fallback are detected, acquirers should enact an action plan to investigate the reason.
- To ensure correct validation of the ARQC by the issuer, acquirers must ensure their terminals include in the online authorization the cryptogram and the same data that was used to generate the cryptogram.
- Terminals should support and correctly display the character sets of the language of the installed location and any other supported languages that are commonly used in a geographic area.
- Terminals must not, at any stage, cross check data in the chip against the magnetic stripe. There may be instances where specific data elements stored in both may actually differ due to personalization differences or other reasons. Alternatively there may be a secondary application in the chip that will not match the magnetic stripe.
- Acquirers should have access, either directly or via their vendors, to software and tools that allow analysis of transactions and generation of traces which will aid in detecting the source of any problem.
- No changes that may affect a terminal's operation should be made to terminals by vendors or merchants without the express knowledge of the acquirer.
- The use of a Terminal Management System is strongly recommended as it will result in a faster remediation process in many cases as it removes the need for site visits to enact changes to the terminal. Refer to Section 8: Terminal Management Systems for additional details.
- Acquirers should have regular communication with issuers regarding any negative experiences or possible problems to ensure issuers are able to assist if required.

The principles noted are not meant as an exhaustive list and acquirers may consider other possible actions to minimize the possibility of interoperability problems. If an interoperability problem is found, Visa will work with the acquirer to resolve the matter in a prompt manner.

7.3 Chip Interoperability Compliance Program

The Chip Interoperability Compliance Program provides the framework for a Visa client or a client's agent identified with high-severity chip interoperability problems to establish an agreed-upon resolution plan and effect a timely resolution. The program is applicable to both contact and contactless chip transactions.

When Visa determines that an acquirer or acquirer's agent has a high severity chip interoperability problem and that the progress toward an agreed-upon resolution plan is not acceptable, the acquirer or acquirer's agent is subject to the requirements of the Chip Interoperability Compliance Program.

Visa may impose non-compliance assessments unless an acquirer undertakes the following:

- Establish and commit to an agreed-upon chip interoperability resolution plan.
- Make satisfactory progress toward an agreed-upon chip interoperability resolution plan.

If it is determined that the terminal type causing the interoperability issue did not have ADVT and CDET test results submitted to Visa, the acquirer may lose the remediation period that is normally granted under the compliance program. Evidence of successful use of the ADVT and CDET is provided by the presence of a corresponding report in the Chip Compliance Reporting Tool as described in Section 6.6.5: Chip Compliance Reporting Tool. Refer to Section 6.9 for the Visa U.S. Chip Acquirer Self-Accreditation Program requirements which will eliminate the need to use the Chip Compliance Reporting Tool (CCRT) to report Acquirer Device Validation Toolkit (ADVT) and Contactless Device Evaluation Toolkit (CDET) terminal test results when they deploy chip POS solutions.

For dual-interface terminals, both ADVT and CDET are applicable and need to be completed to ensure acquirers minimize the opportunity for interoperability problems to occur.

Acquirers can obtain further information regarding the program from their Visa representative.

8. Terminal Management Systems

This Section provides recommended functions to be supported by a Terminal Management System (TMS) in a chip environment. TMS architecture should be sophisticated and flexible enough so that modifications can be made without requiring large terminal infrastructure changes. The more supportive and robust the management system is, the easier it is to respond to future environment needs, new requirements and the inevitable change requests. Terminal Management Systems are sometimes referred to as device management systems.

Acquirers who may be considering supporting offline capable terminals should also refer to the global *VSDC Acquirer Implementation Guide* for further information regarding TMS recommendations. One key component for offline capable terminals is the support for Visa Public Keys and its corresponding support by the TMS.

8.1 EMV Functions

Once a terminal is deployed, acquirers must not be able to change EMV functionality by setting or resetting parameters in non-EMV applications. Most EMV functions are mandatory, and any post-deployment change could affect a terminal's interoperability.

The TMS must not allow deletion of mandatory functions. The system may add or delete optional functions provided that the final configuration loaded into the terminal has been EMV-approved.

8.2 Data Elements

Although a complete TMS uses many data elements, only those that are new for contact chip terminals are discussed here. Data elements that may require post-deployment updates include Terminal Action Codes (TACs), Application Identifiers (AIDs), and floor limits.

8.2.1 Terminal Action Codes

Used in Terminal Action Analysis, TACs are terminal data elements with values defined by Visa. TACs must be loaded into the terminal for each RID (Visa has different sets of TACs for the Visa ISO AID and the Visa U.S. Common Debit AID). They indicate the action that the terminal should take based on the previous processing steps. While the TAC settings are very stable, they can be updated by Visa over time.

The TMS should be set up to track settings and update the settings through down-line loads. Merchants should not be able to change the TACs from their Visa specified values.

For the TAC values, refer to Table 4–5: Terminal Action Code (TAC) Values.

8.2.2 Application Identifiers

AIDs indicate the card applications that a terminal can support, such as Visa, Visa Electron, Plus, or a merchant loyalty program. All contact chip terminals that include the Visa AID must also include the Visa Electron AID. To support new Visa domestic programs, merchants may need to add the corresponding AID to their terminal.

8.2.3 Floor Limits

Currently the U.S. Floor Limits are zero for both magnetic stripe and chip transactions (including domestic and international).

8.2.4 Contactless CVM Limit

Acquirers should also have the capability to change limits for contactless transactions using the TMS. The limits for contactless transactions include:

- Reader CVM Limit
- Reader Contactless Floor Limit (for the U.S. this limit is set to zero)

The value of the above limits may change in the future and acquirers should consider supporting them in the TMS.

8.2.5 Application Version Number

The Application Version Number is the version of VIS supported by the card. It is the version, release and modification number in binary. It is recommended that the terminal Application Version Number match the most current VIS-specified card Application Version Number at the time the terminal received its EMVCo approval.

Version 1.5.0 of VIS would be coded in binary as '0096'.

8.2.6 Terminal Transaction Qualifiers (TTQ)

The TTQ advises the Visa payWave card of the reader's requirements and capabilities for processing the specific transaction including:

- Whether the reader supports qVSDC or MSD, as well as whether it supports contact VSDC
- What CVMs are supported
- Whether cardholder verification is required for the transaction
- Whether the reader supports Issuer Update Processing

The acquirer TMS should have the capability to update the TTQ in the instance that the reader capabilities change or if there is a Visa mandate or requirement to change the supported values.

8.3 Software Updates

Due to the complexity of EMV processing, and the wide range of options available to issuers globally, interoperability issues may arise after deployment. Acquirers and merchants should be prepared to apply software fixes as developed by the EMV kernel provider. The identifiers of kernels with interoperability issues are listed on the EMVCo website. Keeping track of which kernel is loaded into each terminal will allow acquirers to more quickly respond when an interoperability issue with a particular kernel is determined.

Similarly, updates to contactless reader software should also be supported to allow prompt upgrades where required.

8.4 EMV Functionality Considerations

The following sections outline some best practices recommendations for TMS.

8.4.1 Mandatory Functionality for EMV Terminals

The EMV Specifications include mandatory requirements for all terminals, classified by terminal type. These requirements may vary from terminal to terminal; any individual terminal must support the minimum requirements for its type.

To ensure EMV compliance, the terminal management software should include profiles or logic validating that all mandatory functions for a terminal type are active.

8.4.2 Configurable and Selectable Kernels

If an optional function is configurable – that is, if it can be turned on or off – it must work properly as configured. Software for the function should be identified as configurable, be tested and type approved in both on and off modes.

During vendor quality assurance testing, application kernels that are developed for multiple terminal types should be tested by using all EMV scripts for those terminals. Comprehensive quality assurance testing ensures proper support for mandatory and optional functions across terminal types.

A terminal may have one approved kernel that can be configured at installation to provide only needed functionality. EMV allows one kernel to be tested in multiple configurations. These kernels are referred to as configurable kernels.

Alternatively, a terminal may support selectable kernel configurations, that is, the kernel configurations used at a single terminal may vary based upon characteristics of the transaction rather than being set at the time of terminal installation. The selection criteria logic must be checked to ensure that it selects the correct configuration. All selectable configurations must be EMV type approved.

If an acquirer needs to support configurable functions in certain terminals, Visa recommends that acquirers consider the use of selectable kernels as a best practice.

Terminals supporting cash-back or VEPS may need to include selectable kernels to invoke correct CVM processing as per Section 4.4.6.

9. Acquirer System Changes

This Section outlines acquirer system changes to support EMV chip. Visa mandates that all acquirers must support the full set of changes required to support chip, previously termed "Full-Chip Data." If an acquirer is unable to support Full-Chip Data processing via its host system, it is prohibited from deploying or supporting chip terminals with the chip functionality enabled.

The following sections outline the changes required to support contact chip and their impact to the acquirer system along with a high level overview of the areas affected and associated changes required. Further information regarding specific changes to VisaNet messages to support VSDC and Visa payWave may be found in the *Visa Smart Debit/Credit (VSDC) System Technical Manual*

9.1 U.S. Acquirer Processor Mandate

Visa requires U.S. acquirer processors and sub-processors service providers to carry and process the additional data in EMV chip transactions, including the cryptographic data on all Visa networks. Visa requires support for V.I.P. Field 55 in authorization messages at the host level for both contact and contactless transactions. U.S. acquirers are required to confirm their ability to comply with this mandate. Acquirers need to ensure that connections from merchants and other partners are also ready and certified prior to the deadline.

9.2 Terminal-to-Acquirer Interface

VSDC introduces new data elements that must be carried in the terminal-to-acquirer interface. The terminal must be able to accept the card and transaction data used at the point of transaction and populate it into the terminal-to-acquirer message format.

Acquirers may also choose to support terminal-to-acquirer messaging requirements. However, the acquirer host-to-VisaNet interface must meet Visa requirements and have the flexibility to support future data requirements. The use of a TLV field, such as Field 55, provides the flexibility for including additional data or longer lengths of existing data, if required in the future.

9.2.1 Data Requirements

When supporting EMV, the terminal-to-acquirer messages must be upgraded to support the new data. The process of upgrading these links does not involve Visa and is the responsibility of each acquirer and/or their vendors. To aid acquirers in understanding the data required in these messages, a list of the minimum set of data elements required in the terminal-to-acquirer messages has been defined by EMV and Visa.

Information on the minimum set of data elements may be found in:

- EMV Specifications, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements located on the EMVCo website at www.emvco.com.
- *Visa Transaction Acceptance Device Guide*

VisaNet formats for the data elements are contained in the *VSDC System Technical Manual*.

Visa recommends that acquirers review the data required in the VisaNet messages to identify any necessary terminal-to-acquirer interface modifications.

In addition, to support the requirement to route debit transactions initiated with the Visa ISO AID to a Visa affiliated network, Visa currently requires that acquirers and any other routing entities receive the AID used to initiate the transaction. This AID is passed to the terminal in a card data element called the Dedicated File (DF) Name. The acquirer or other routing entities then use the DF Name to perform the appropriate routing process. Acquirers should review and implement this solution based on their needs to achieve appropriate routing. Effective October 1, 2015, Visa requires that the DF Name be carried in Field 55 of the authorization request. For more information on the DF Name, refer to Table B–1: V.I.P. System Field 55 Mandated Data Tags.

9.3 Host System Changes

Acquirer host systems must support new fields in the authorization, full financial, and clearing and settlement messages and systems.

The majority of this new data comes directly from either the card or terminal at the point of transaction and is protected by a cryptogram that must be authenticated by the issuer host or Visa. If any of the data that is part of the cryptogram is changed or manipulated, the cryptogram cannot be validated and authentication fails which can lead to declined transactions.

The terminal also transmits the full, unmodified contents of the Track 2 Equivalent Data in the chip which includes the Form Factor Indicator if personalized by the issuer for contactless transactions.

Upon receipt of this data at the host, acquirers must not manipulate or change any of the data element values as they are formatted into the VisaNet message and forwarded to the issuer. Visa recommends that acquirers integrate their host with a production-ready terminal to ensure that all components are working together correctly.

For authorization and full financial messages, the new data for both VSDC and Visa payWave transactions is formatted in Field 55 in TLV (tag-length-value) format. Appendix B contains a list of the mandatory tags included in Field 55. MSD Legacy transactions do not include the new data.

Additionally, the following existing V.I.P. fields will contain new values for chip transactions for VSDC transactions:

- Field 22 – POS Entry Mode – Value of 05 or 95 to indicate a chip card was read
- Field 60.2 – Terminal Entry Capability – Value of 5 to indicate that the device is capable of reading a chip card

For Visa payWave transactions the following existing V.I.P. fields will contain new values:

- Field 22 – POS Entry Mode – Value of 07 (for qVSDC) or 91 (for MSD)
- Field 60.2 – Terminal Entry Capability – Value of 5 to indicate that the device has contactless and contact chip capability or a value of 8 to indicate that it is a contactless-only capability

Other fields that carry new chip related data include:

- Field 23 – Card Sequence Number
- Field 44.8 – Card Authentication Results Code
- Field 60.3 – Chip Condition Code (optional)
- Field 60.6 – Chip Transaction Indicator
- Field 60.7 – Card Authentication Reliability Indicator

Acquirers should either support Field 44.5 or Field 39 – CVV/iCVV Results Code, sent in the authorization response to communicate the verification results for either dCVV or CVN 17.

For clearing and settlement, the majority of the new data elements are included in a new Transaction Component Record (TCR 7). TCR 0, TCR 1 and TCR 5 will also carry data relating to chip transactions. Acquirers and merchants in the U.S. who plan to deploy online-only terminals or terminals with a Zero Floor Limit and obtain online authorizations for all transactions are not required to support TCR 7.

Note: TCR7 is still required if a transaction is offline approved.

Acquirers should refer to the *VSDC System Technical Manual* for details of the additional data elements required and other host related changes relating to VSDC.

Acquirers will also need to make any host system changes needed to support back-office processes, such as merchant service and reporting. Refer to Section 11: Acquirer Back-Office Changes for more information.

In addition, to ensure that transactions initiated with the Visa ISO AID are routed to a Visa affiliated network, Visa requires that the terminal sends the AID to the acquirer (and any other downstream routing entities). The AID is contained in a card data element called the Dedicated File (DF) Name. For more information, refer to Table B–1: V.I.P. System Field 55 Mandated Data Tags.

9.3.1 Host System Fallback Considerations

Because issuers may treat fallback transactions differently than other transactions, acquirers need to identify fallback transactions in their acquirer-to-VisaNet messages, which can be accomplished through the population of the following fields:

- POS Entry Mode is 90 or 02 (V.I.P. Field 22), indicating that the transaction is magnetic-stripe read.
- Terminal Entry Capability (V.I.P. Field 60.2) and POS Terminal Capability (BASE II TCR 0, position 158) is 5, indicating that the terminal is a chip terminal.
- The service code value on the magnetic stripe contains a value of 2xx or 6xx identifying the presence of an EMV/VSDC-compliant chip on the card.

9.4 Implementation Activities

Implementation activities relating to authorization and clearing systems changes include:

- After the system changes have been made, Visa recommends that acquirers test the terminal-to-acquirer interface and interfaces to intermediate merchant host systems to ensure correct processing. For further details see Section 10.3 End-to-End Testing.
- System changes as outlined in the *VSDC System Technical Manual* and any changes required to support additional chip data between the acquirer host and VisaNet.
- Acquirers need to evaluate and undertake a gap analysis to determine how changes will affect their host system. The effort required will vary based on how the host system is configured.
- Acquirers must upgrade their host system to be able to receive chip data from the terminal in the terminal-to-acquirer message, format the data into the host system message (without changing any of the data element values), and forward the data to the issuer in the message. To help ensure they have properly upgraded their host system, acquirers should integrate a production-ready terminal (e.g., a terminal configured for deployment that has passed EMV Level 1 and Level 2 certification together with ADVT and CDET) into their testing efforts. This will help ensure that host and terminal are properly integrated and there is no altering of data elements received from the terminal.
- Acquirers should make host system changes to identify fallback transactions in the host system messages. For further information regarding testing refer to Section 10 Acquirer Host Testing. Acquirers should monitor levels of fallback to ensure that high levels of fallback are not a result of a faulty terminal, mishandling from the merchant, or even merchant collusion.
- Acquirers must ensure that debit transactions initiated using a Visa ISO AID are routed to a Visa affiliated network. To support this requirement, Visa requires that acquirers receive the AID (contained in card data element called the Dedicated File (DF) Name) from the terminal and use it to perform the appropriate routing. For more information, refer to Table B–1: V.I.P. System Field 55 Mandated Data Tags.

10. Acquirer Host Testing

This Section addresses acquirer host testing to support VSDC and Visa payWave transactions. It assumes that the acquirer is already a VisaNet endpoint. Host testing for VSDC and Visa payWave is mandatory.

This Section does not cover other testing considerations such as internal systems, back-office, and downstream processes. Due to the extent of changes involved in a VSDC program, it is imperative that testing takes place on all components. These areas should also be covered by the acquirer's test plan.

The main tool used in acquirer host testing is the Visa Test System – V.I.P. (VTS-VIP).

10.1 Testing Environment

Once internal testing of coding changes to support VSDC has been completed, acquirers will need to begin preparing for testing with VisaNet. The first step in the testing process is to ensure that all of the necessary components are in place. The following components are required for the VSDC testing environment:

- Connection to the VisaNet Certification Management Service (VCMS)
- Visa Test System – V.I.P. current release (VTS-VIP)
- VSDC testing scripts
- Visa payWave testing scripts
- Visa Host Test Kit – Personalized test chip cards (contact and contactless)
- Production ready/EMVCo approved terminal
- Production ready/EMVCo and Visa approved contactless reader

Acquirers should contact their Visa representative to obtain testing scripts and test cards.

Visa recommends that acquirers test connectivity to VCMS by performing magnetic stripe test transactions through the VCMS environment one to two weeks prior to scheduled online testing. This will allow time for trouble-shooting and correction should connectivity problems arise.

Further information regarding testing requirements can be found in the following documents:

- VCMS Testing Guide – V.I.P., Client Version
- VCMS Testing Guide – BASE II, Client Version
- Visa Test System – V.I.P. User's Guide
- *Visa Smart Debit/Credit System Technical Manual*

10.2 Testing Process

The acquirer must perform a series of transactions, referred to as test scripts, to demonstrate their host system is able to send and receive the new chip data and fields required in each message for both contact and contactless.

Acquirers will need to perform Field 55 host testing using the Visa Host Test kit along with a production-ready terminal (EMVCo and Visa approved) that has already successfully completed terminal testing using the required Acquirer Device Validation Toolkit (ADVT) and Contactless Device Evaluation Toolkit (CDET). ADVT and CDET test results must be submitted to Visa using the Chip Compliance Reporting Tool (CCRT). Before proceeding to host authorization testing, a minimum of one terminal must be successfully tested for use during host testing. This will ensure that components are correctly integrated and help to reduce interoperability problems.

Note: If an acquirer supports Network 2 (POS) and Network 3 (Interlink), the acquirer is required to process contact and contactless chip processing as of 1 April 2013 for POS transactions. U.S. Acquirers and acquirer processors are not required to support full chip data in Field 55 for ATM transactions as part of the April 2013 mandate. As a result, acquirers and processors that process ATM transactions are advised to factor support for chip data into their network and host development planning.

Note: Effective 17 April 2015 U.S. Third Party ATM acquirer processors and sub-processors must be able to support EMV chip data.

To support this process, Visa provides acquirers with host test chip cards. Acquirers need to use the card, indicated on the script, to generate transactions through VCMS. Your Visa representative will provide support through this process and will schedule attended testing.

The following table summarizes testing steps. In the table, V.I.P. System refers to tasks associated with both BASE I and SMS connected endpoints.

Table 10–1: Acquirer Host Testing Steps

Step	Action
1	Pre-requisite completed ADVT and CDET terminal testing, then submit results into CCRT.
2	Submit the Client Information Questionnaire (CIQ) and Global Testing Questionnaire to Visa. These forms are used to communicate the acquirer's details that will be used during testing. The forms may be obtained from a Visa representative.
3	Request host test cards and VSDC and payWave testing scripts from Visa.
4	Confirm online VCMS connectivity by performing test transactions using magnetic stripe data.
5	Perform pre-testing with VTS-VIP and VCMS.

Step	Action
	• If using a terminal emulator for terminal testing, completion is required before host testing can begin. • A production-ready terminal will be required to generate online authorization messages for host testing. • If using an EMV approved terminal a production ready terminal will be required to complete terminal testing requirements.
6	Submit V.I.P. system pre-testing VTS-VIP logs to Visa for approval.
7	Schedule online V.I.P. System testing with Visa.
8	Perform V.I.P. system testing through VCMS.
9	Verify SMS reports and raw data (if supported).
10	Schedule BASE II/settlement testing (if applicable).
11	Perform BASE II testing through VCMS (if supported).
12	If testing is successful, acquirers will receive confirmation from Visa of their successful testing. Acquirers whose testing was unsuccessful should work with a Visa representative to schedule a subsequent testing slot.
13	Submit the Client Information Questionnaire (CIQ) for BINs and PCR to request the activation of production participation flag in the VisaNet Systems Table for production.
14	Activate the production PCR participation flags in the VisaNet Systems Table on an implementation date selected by the acquirer. ***Note:*** *Acquirers must notify Visa immediately if the implementation date must be changed. Additionally, if the completion of testing is more than 90 days from the production date, Visa requires acquirers retest.*

10.2.1 BASE I and SMS Pre-testing

Acquirers who have completed the Client Information Questionnaire (CIQ) and the Global Testing Questionnaire will be provided with a database of test case transactions. Acquirers can conduct pre-testing using these test cases with VTS-VIP acting as an issuer. After testing internally with VTS-VIP, acquirers send the results to Global Client Testing team (GCT). GCT reviews the logs to ensure that acquirers are ready to begin testing and can confirm a testing date with Visa.

10.2.1.1 Test Cards

To support host testing, Visa provides test cards that are associated to a Visa Test BIN set up as a VSDC or Visa payWave issuer in the VisaNet and VCMS systems. These test cards must be used in host testing activities. Acquirers should contact their Visa representative to obtain the test cards.

10.2.1.2 Testing Scripts

Prior to online testing, acquirers must obtain testing scripts from Visa. These can also be downloaded from Visa Online. These testing scripts must be used along with test cards in the host testing activities.

10.2.1.3 Production Ready Terminal and Reader

The majority of the new data elements that need to be included in host system messages originate at the card or terminal level. These data elements are used to generate a cryptogram that is included in the message to the issuer. It is the acquirer's responsibility to receive these new data elements from the terminal in the terminal-to-acquirer message and forward them to the issuer unaltered so that the issuer or Visa can validate the cryptogram. If any of the data elements are corrupted or altered by the acquirer host system, the cryptogram may fail.

To ensure the acquirer host is able to receive the data from the terminal an approved production-ready terminal (including the contactless reader) must be included as part of the host testing activities.

The inclusion of a production-level terminal in testing activities helps ensure that all components are properly integrated and working together. It also helps to prevent interoperability problems and/or cryptogram failures that might be caused by data handling or data transmission errors.

Visa requires that that at least one CDET and ADVT terminal testing be completed prior to host testing. An acquirer will use a production ready terminal (EMVCo and Visa approved) which has completed terminal testing for host testing. An acquirer can also run the host test cards through a terminal prior to host testing.

Visa strongly recommends that acquirers perform test transactions with each type of terminal they plan to deploy.

10.2.1.4 V.I.P. System Testing Results

After online testing, Visa will review the results and advise of the status. Upon successful completion of all test cases, Visa will send a letter as evidence that testing has been completed.

10.2.2 BASE II Testing

Acquirers supporting BASE II are required to confirm their ability to send and receive new draft data values in existing fields and additional audit trail data for chip transactions. This new draft data will be present in TCRs 0, 1, 5, and 7 (TCR 7 is not applicable to acquirers deploying online-only terminals, see Section 9, Host System Changes for details).

Note: Acquirers that settle through SMS should review SMS reports and raw data to verify test results.

Visa defines the process of BASE II testing and acquirers may obtain this information from their Visa representative.

10.3 End-to-End Testing

Visa strongly recommends that acquirers perform tests from their production-ready terminal to their acquirer host and then to VCMS prior to going live. These tests ensure that components are correctly integrated and help to reduce interoperability problems. These tests can be performed as part of the host testing process and acquirers should perform end-to-end tests with each type of terminal acquirers plan to deploy.

10.4 Pilot Testing

Prior to a public launch, the acquirer may additionally elect to perform a pilot or soft launch, prior to a production launch. For pilot testing, acquirers can undertake transactions using production chip cards which may belong to the acquirer (if the acquirer is also an issuer) or may be obtained from an issuer through a direct agreement or obtained through Visa. These transactions are treated and processed as production transactions and not test transactions.

This process may provide the acquirer with an additional level of comfort that all its systems and its terminals have been configured and are working correctly.

11. Acquirer Back-Office Changes

This Section addresses the technical changes to back-office functions acquirers need to support an EMV chip program. The migration requires new procedures and processes to support the additional data and functionality provided by chip cards. Changes to general operations and dispute resolution processes need to be included in training materials for existing and new staff.

A suggested set of technical, operations, and training tasks is provided in the program planning checklist in Appendix A: Planning Checklist.

11.1 Dispute Resolution Management

Due to the new data provided by EMV transactions, acquirers will need to examine the potential impacts on back-office exception processing procedures that handle chargebacks, re-presentments and problem resolution. Exception processing allows an acquirer to respond to chargebacks from issuers by providing documentation and representing transactions. Changes affecting exception processing and dispute resolution should also be analyzed for impacts to host and customer service systems.

- Consider modifying systems to retain chip data for a period of time sufficient for use in responding to chargebacks; for example, up to 180 days. Access to chip information may be needed to provide supporting information on disputed items.
- Evaluate how the chip data may need to be displayed, for example on reports and screens.
- Determine the impacts of chip data used in dispute resolution on systems that capture, process, log, and backup transactions; then plan to make any needed changes. For example, it is highly recommended that a trouble-shooting system be in place for ongoing support or analysis of logged transactions such as offline-declined transactions.

For some transactions, the new chip-related information in the authorization request message provides evidence of the risk management steps executed by the card and terminal, and the authorization response is proof of the processing performed by the issuer.

For online authorized transactions processed in a host data capture environment, Visa recommends forwarding the Authorization Request Cryptogram (ARQC) and related data elements in a BASE II message.

Acquirers should review downstream processing for Visa Resolve Online for additional chip information.

The *Visa Rules* govern chargeback and re-presentment rights (which may be superseded by domestic or private agreements). Because the rules are periodically updated to reflect chip capabilities, it is important for acquirers to ensure they use the latest version.

11.2 EMV Liability Shift

EMV liability shift encourages the use of chip transactions because any chip-on-chip transaction (i.e., a chip card read by a chip terminal) provides dynamic authentication data, which helps to better protect all parties.

With EMV liability shift, the party that, due to their lack of chip technology, is the cause of a chip-on-chip transaction not occurring (either the issuer or the merchant's acquirer) will be financially liable for any resulting card-present counterfeit fraud losses. When a transaction occurs using chip technology, any liability for counterfeit fraud, though unlikely, would follow current *Visa Rules*.

The policy assigns liability for counterfeit fraud to the party that has not made the investment in EMV chip cards (issuers) or terminals (merchants' acquirers). The policy encourages wider deployment of EMV cards and terminals.

Effective 1 October 2015, the U.S. region is included in the global EMV liability shift, which will apply to all issuers and merchants' acquirers in the U.S. with the exception of transactions at Automated Fuel Dispensers (AFDs) and ATMs. Transactions made at AFDs and ATMs will be excluded from liability shift for a period of two (2) years due to the challenges faced by the petroleum and ATM industry in upgrading terminals to accept EMV chip cards. Effective 1 October 2017, transactions made at AFD and ATM terminals will be included in the global EMV liability shift. Acquirers requesting additional clarification or information can contact their Visa representative.

11.3 Chargebacks and Representments

The introduction of chip cards has resulted in changes to the chargeback and representment rules. Since chip gives the issuer increased protection regarding counterfeit fraud and the ability to control offline authorized transactions based on the issuer's chip settings, there will be less reason for the issuer to charge back transactions in general.

Many of the changes in the chargeback rules are the result of offline authorized transactions. For Zero Floor Limit markets, such as the U.S. where the transactions need to be authorized by the issuer, the impact will be minimal. Also many of the chargeback reason codes will still be ruled as they would be for magnetic stripe transactions since the chip does not provide any further evidence.

There is no chip data required in chargebacks and representments, that is, there are no new retain and return fields.

Further information regarding changes to chargebacks due to the migration to chip can be found in the *Visa Rules*.

11.4 Reporting

This Section gives an overview of the impact of chip acceptance on reporting. Reporting changes are outlined in the following sections:

- Chip Transaction Statistics
- Fallback Transactions
- Enhanced Reporting Opportunities

11.4.1 Chip Transaction Statistics

At a minimum, Visa recommends that acquirers differentiate chip transactions from magnetic stripe transactions. This will allow them to monitor the growth of their chip program, the success of merchant service activities, and the value of chip-enabled risk management features. It will also help acquirers to meet future reporting requirements.

For most reports, it will be helpful to maintain the existing format and provide the information for both chip and magnetic stripe transactions on the same report. Both sales volume and number of transactions should be tracked. These totals should be incorporated in settlement and reconciliation, fraud, customer service, and service assessment reports.

Acquirers can identify chip-initiated transactions through the following data elements:

- POS Entry Mode values of 05 or 95, indicating a contact chip-initiated transaction or POS Entry Mode values of 07 (qVSDC) or 91 (MSD) for contactless transaction
- Terminal Entry Capability (V.I.P. Field 60.2) and/or POS Terminal Capability (BASE II TCR 0, position 158) value of 5, indicating a chip-capable terminal and value of 8 indicating a contactless capable terminal.

11.4.2 Fallback Transactions

Acquirers should monitor and provide reporting for fallback transactions. Fallback transactions are those where a chip card is read as a magnetic stripe card at a chip terminal. Acquirers should track fallback transactions by merchant and terminal. A high incidence of fallback transactions indicates terminal problems (the chip terminal functionality is not working properly) or incorrect merchant procedures (merchants are incorrectly accepting chip cards via the magnetic stripe rather than the chip) and may result in a chargeback exposure.

Fallback transactions can be identified through the following data elements:

- POS Entry Mode (V.I.P. Field 22) is 90 or 02, indicating that the transaction is magnetic stripe read.
- Terminal Entry Capability (V.I.P. Field 60.2) and/or POS Terminal Capability (BASE II TCR 0, position 158) is 5; this indicates a chip-capable terminal.

- Service code value on the magnetic stripe contains a value of 2xx or 6xx either of which identifies the presence of a chip on the card.

When reports show a high incidence of fallback transactions, acquirers should investigate. To help merchants with this issue, acquirers may need to retrain them on chip card acceptance procedures. If problems persist, incentives or penalties could be considered.

Failure to take corrective action may result in the acquirer being identified by the Visa Global Fallback Monitoring Program and having to take corrective action.

11.4.3 Enhanced Reporting Opportunities

As acquirers migrate to chip, they can take advantage of the additional data provided in chip transactions. By offering a view of the interaction between the card and terminal, this data gives the opportunity to significantly enhance management reporting. Some reporting enhancements to consider include the following:

- Chip transaction reports
- Fraud reports that highlight differences between magnetic stripe and chip cards
- Suspect merchant activity
- Statistics comparing offline and online transactions (if offline transactions supported)
- Merchant service reports that monitor support levels for chip terminals

11.5 Visa Reporting

The Visa Quarterly Operating Certificate has been updated to include contact chip data. Acquirers will be required to provide the number of deployed chip enabled terminals and merchant locations at the end of each quarter.

11.6 Internal Staff Training

Each organizational unit involved in a merchant service function must be trained about the nuances of chip-based transaction processing. All areas that will be impacted by the implementation of chip terminals should also be trained on changes to internal operating procedures. The amount of training needed on changes to the merchant environment depends on how much a particular unit will be involved in providing merchant services. Units that have direct interaction with merchants will need more extensive training.

A comprehensive training plan helps ensure a smooth implementation process and minimizes the need for last-minute activities as the program launch approaches. The training plan development should include the following tasks:

- Develop objectives for chip training.
- Determine training requirements.
- Design training courses.
- Produce training materials, operational manuals, and help guides.
- Coordinate the training requirements of other departments that may be affected by the introduction of chip.
- Produce a training schedule.
- Provide training for staff, including operations, customer services, and branch staff.
- Staff should also be informed about how to get answers to questions that arise after the initial training is complete.

11.7 Implementation Activities

Implementation activities for back office in the areas of interchange, billing, dispute resolution, reporting, and training, include:

- Analyze pricing structure and determine if any changes are required.
- Assess the need for chip transaction data in reports and the need for new reports.
- Identify interchange rates; evaluate and notify merchants of any financial impact.
- Evaluate impact of rule changes to chargebacks and representments.
- Design and document procedures to accommodate chip-related changes.
- Notify merchants of any changes in procedures.
- Determine and make changes needed to customer service and exception processing systems.
- Develop and deliver chip training to all affected staff.

12. Merchant Support

This Section reviews the tasks related to supporting merchants as they make the transition to chip card acceptance. It focuses on the merchant support needs in areas such as system changes and training.

12.1 Merchant Agreement

Existing merchant agreements may need to be updated to reflect the migration to chip. It is important to review changes to the merchant relationship due to chip processing and then update the merchant agreement to include the following:

- Terminal costs and installation as well as any pricing changes
- Support for additional data for authorization and clearing messages
- Receipt of new information on reports
- Cost and competitive factors
- Procedural changes to card acceptance processes

Acquirers should obtain legal advice on regulatory and business requirements from their own counsel as they update merchant agreements.

12.2 Technology Innovation Program

To incent acquirers and merchants that upgrade their terminals to support EMV chip, effective 1 October 2012, Visa expanded the Technology Innovation Program (TIP) to the U.S. region. This program eliminates the requirement for eligible merchants to annually validate their compliance with the PCI DSS for any year in which at least 75 percent of the merchant's Visa transactions originate from dual-interface (contact and contactless) EMV chip enabled terminals, in addition to meeting other qualification criteria.

To qualify, terminals must be enabled to support both EMV contact and contactless chip acceptance, including mobile contactless based payments based on NFC technology. Contact chip-only or contactless-only terminals will not qualify for the U.S. program.

Visa developed TIP to recognize and acknowledge merchants that have taken action to prevent counterfeit fraud by investing in EMV technology and prepare for the use of emerging technologies.

Merchants that qualify for TIP can reap meaningful savings through the reduction of costs associated with annual PCI DSS validation.

Acquirers should contact their Visa representative for further details regarding the TIP program.

12.2.1 Minimum Merchant Qualification Standards for TIP

To qualify for the program, and receive its benefits, U.S. merchants must meet all of the following criteria:

1. The merchant must have validated PCI DSS compliance within the previous 12 months or have submitted to Visa (via their acquirer) a defined remediation plan for achieving compliance, based on a gap analysis.
2. The merchant must have confirmed that sensitive authentication data (i.e., full contents of magnetic stripe, CVV2 and/or PIN data) is not stored, as defined in the PCI DSS.
3. At least 75 percent of the merchant's total transaction count must originate from a secure acceptance channels, either: dual-interface (contact and contactless) enabled chip reading terminals **OR** a validated Point-to-Point Encryption service.[9]
4. The merchant must not be involved in a breach of cardholder data. A breached merchant may qualify for TIP if they have subsequently validated PCI DSS compliance.

Although Visa may waive the annual validation requirement for qualifying merchants, all merchants are required to maintain ongoing PCI DSS compliance and continue adhering to industry data security standards such as the PCI DSS, the PCI PIN Security Requirements, and the Payment Application Data Security Standards (PA-DSS).

12.2.2 Acquirer Requirements

Visa will work directly with acquirers to confirm eligible merchants and verify acquirer's reporting responsibilities. Participating in the program is contingent upon the acquirer's submission of and Visa's approval of a program application for each qualifying merchant. Visa will work closely with acquirers on the continued monitoring of merchants' PCI DSS compliance and dual-interface terminalization efforts.

Acquirers retain full responsibility for merchants' PCI DSS compliance, as well as responsibility for any fees, non-compliance assessments or penalties that may be applicable in the event of any data breach.

[9] Enabled chip reading devices must have current, valid EMV approval and pass Visa Acquirer Device Validation Toolkit (ADVT) and Contactless Device Evaluation Toolkit (CDET) implementation requirements as applicable, and must comply with the *Visa Transaction Acceptance Device Requirements (TADR)*. Acquirers should contact their Visa representative for further information.

12.3 Contactless Reader Migration

Many U.S. acquirers have already rolled out VCPS 1.4.2 contactless readers to begin acceptance of Visa payWave. Acquirers need to ensure that as part of their terminal renewal plan they consider Visa's contactless acceptance requirements.

Visa had rules which required that by 1 April 2013, all new Visa payWave accepting contactless readers deployed in the U.S. must actively support both MSD and the qVSDC transaction path of VCPS 2.1 including all published updates. These rules have recently been modified so that:

- Effective 10 April 2015, contactless terminals deployed between 1 April 2013 and 31 December 2014 must comply with the VCPS 2.1.1 (or higher), and be capable of processing a transaction using both the MSD and qVSDC transaction paths (though the terminal may actively support only the MSD transaction path).
- Terminals deployed on or after 1 January 2015 must comply with the VCPS 2.1.1 (or higher), and be capable of processing a transaction using the qVSDC transaction path (though the terminal may actively support only the MSD transaction path).

qVSDC may be supported on an online only basis (i.e., no support for offline authorizations). (Note that all transactions in the U.S. are subject to a zero floor limit.)

Effective 1 January 2015, Visa contactless readers connected to acquirer platforms that are certified for chip data no longer need to support the MSD transaction path.

12.4 Merchant Services

The installation of chip-capable terminals may increase the need for merchant service and support, both in implementing chip terminals and providing ongoing service. To provide the highest level of support when offering chip access to Visa credit and debit products, acquirers should plan to make some enhancements to their merchant service area.

12.4.1 Merchant Implementation Support

It is important for acquirers to plan how to support merchant conversions to EMV chip once the decision or agreement to place one or more chip-reading terminals has been completed. Because the number of problems experienced by merchants during the conversion can impact the success of the program launch, thorough preparation and merchant support and training are essential. Some of the activities that will need to be completed include:

- Determine how to provide hardware and software installation support.
- Anticipate merchant questions, areas of confusion, and problems; develop ways to handle them in advance.

- Develop train-the-trainer activities.
- Consider installing a telephone hotline for merchant questions.
- Evaluate potential physical changes to the merchant environment based on terminal specifications – especially the terminal footprint – including terminal stand modifications, electrical upgrades, PIN pad placement, and cabling changes.
- Address any impacts to merchant network interfaces to handle additional capacity for chip data.
- Evaluate and provide for terminal maintenance options, such as in-house or third-party support.
- Evaluate impact to terminal to host message format.

12.4.2 Terminal Installation

The final step in the terminal deployment process is to provide operational terminals to individual merchant locations. Acquirers should consider incorporating the following items into a terminal deployment schedule:

- Test all terminal components to make sure that they work together as planned. Perform basic functionality testing with individual terminals. Perform end-to-end testing to ensure terminal operability.
- Ensure that terminal data is properly loaded, including Application Identifiers (AIDs), Application Version Number, and Terminal Action Codes (TACs), and the terminal functionality is correct prior to shipping each terminal. Any test data, including test keys, must be removed from the terminal prior to installation.
- Decide on deployment methods to be utilized, for example, a site visit or shipment of terminals and training materials to merchant locations.
- Decide on deployment priorities, such as geographic area, existing high-fraud merchants, or merchants with suspect activity.
- Plan for delivery of supplies, for example, printer paper, ribbons, deposit slips, and terminal faceplates.
- Identify the need for accessories, for example, terminal stackers, pedestals, and cables.
- Develop service agreements, help desk support, and training.
- Develop terminal handling instructions for merchants.
- Determine if cardholder education materials should be available at the point of transaction and the appropriate contents.

Onsite installation and testing should include activities to make sure chip-related parameters are loaded successfully.

12.4.3 Ongoing Terminal Maintenance

Acquirers should directly, or via an agent, make use of a TMS to facilitate the remote ongoing maintenance of deployed terminals, which:

- Allows terminal data to be updated quickly and remotely and without the need for staff to visit the merchant location.
- Provides a readily accessible record of the configuration of any installed terminal which may assist the acquirer in future upgrade plans.

Further details are provided in Section 8 Terminal Management Systems.

12.4.4 Ongoing Merchant Service

Merchant service and support staff should be prepared to respond to customer inquiries related to the new capabilities introduced by the chip terminal. Some suggested activities to ensure an effective level of support include:

- Determine the likely sources and types of inquiries.
- Ascertain the expected level of terminal support.

Initially, acquirers should provide merchants with a special telephone hotline for inquiries. The hotline telephone number can be furnished in several ways, for example:

- Place a sticker on terminals.
- List on the merchant's deposit account statement.
- Include in merchant training materials or in a separate informational document.
- Include in a merchant brochure or newsletter.

12.5 Merchant Systems Changes

Impacts on merchant systems due to new chip data should be taken into consideration. Merchant systems that should be evaluated for possible modification include:

- Terminal-to-merchant host interface
- Terminal-to-retail workstation interface
- In-store terminal controllers
- Merchant-to-acquirer host interface
- Back-office systems for major merchants that support their own back-office systems
- Capacity planning for merchant networks that process, capture, log, and backup transactions
- Reporting systems

Adequate time should be allowed to test changes to the merchant configuration.

12.6 Contactless Reader Branding and Placement

Merchants are required to display the contactless symbol on all readers to let cardholders know how and where they can use Visa payWave cards. There are specific requirements relating to the branding of the terminals and further information can be found in the Visa Brand Mark and Contactless Symbol Guide for Payment Terminals. Visa can also provide appropriate artwork to be used for terminals and readers.

Merchants should also ensure they have placed contactless readers so as to ensure seamless usage by cardholders and to maintain the principle of a fast transaction. Some best practices include:

- In the case of the indicators that are intended to be visible to the cardholder, these should be located so they are clearly visible when the cardholder is looking at the reader landing zone. Ensure the reader is free from obstructions and easily accessible for cardholders to use the contactless payment feature.
- Merchants should place contactless card readers at least 12 inches away from each other. In retail locations where counter space is limited, the magnetic field of multiple readers in close proximity may overlap; thus disrupting the contactless transaction when a single contactless card is presented.

Further information regarding the placement of contactless readers can be found in the *Visa Transaction Acceptance Device Guide*.

12.7 Merchant Training

Chip introduces new functionality at the point of transaction through the deployment of EMV-compliant terminals. Merchants must be trained on the basic procedural differences between magnetic stripe and chip card acceptance:

- Chip cards are inserted into the chip reader and must remain inserted until the transaction is completed. This differs from the magnetic stripe method where the merchant swipes the card and immediately removes it in a single motion.
- Early removal of the chip card from the reader will terminate the transaction. As terminal messages vary, any message that signals when a transaction is completed should be clearly identified. Merchants and their customers should be educated to remove the card from the terminal only after seeing this message.
- Merchants need to educate cardholders about chip acceptance procedures in environments where customers insert their own cards in the chip reader. Unattended terminals, for example, ATMs, UCATs, or AFDs, should have instructional prompts and signage to support cardholders through each phase of the transaction.

Merchants should be trained to recognize a chip card and prompted to insert the card into the chip reader rather than swiping the magnetic stripe. This will make the transaction process faster and mitigate the potential problem where an issuer may have incorrectly personalized the card with a service code that does not correspond to a chip card.

Due to these changes, acquirers should evaluate making a cardholder pamphlet available to merchants to help ease the transition to chip.

12.7.1 Merchant Training Plan

Merchant training plan development typically includes the following tasks:

- Develop training objectives for chip
- Determine training requirements
- Design training courses
- Produce training materials
- Provide a train-the-trainer class

Training support materials will need to be developed to assist the merchant staff in the training process. Materials often provided for merchant training include:

- Training presentation
- Operations manual
- Quick reference guide
- Frequently asked questions from both the merchant and cardholder perspectives
- Contact information for the merchant service unit

Customer education materials can be given to merchants to help them answer common cardholder questions. Merchants should also be informed about how to get answers to questions that arise after the initial training is complete.

Follow-up training may be necessary, especially due to turnover, a high incidence of fallback transactions, or both.

Merchant training needs and materials should be evaluated regularly. Acquirers may also want to consider assisting merchants that provide their own help desk support with training and materials.

12.7.2 Cardholder Selection

With the introduction of multiple applications on a single card, cardholders can be prompted to select which application should be used for a given transaction. Cardholder Selection only takes place when both the card and terminal support more than one application in common or when required by the card.[10] Merchants should understand that depending on the merchant's EMV implementation, the cardholder could be prompted for application selection on some transactions and not others, based on the card's support for multiple products. See Appendix D Basic EMV Terminal Logic.

Cardholder Selection can be used to indicate a cardholder's preference of which funding source (e.g., credit and debit application) they may want for a given transaction. For U.S. Covered Visa Debit Cards, this will be represented by a Visa AID connected to the credit function, and a debit pair consisting of a Visa AID and a Visa U.S. Common Debit AID both connected to a common source of debit funding. Removal of one of the AIDs of the debit pair from the Candidate List will result in two eligible AIDs (one for credit and one for debit). Either the highest priority AID (indicating the desired funding source) can be selected to initiate the transaction or the merchant can implement custom logic to ask the cardholder which account they wish to use and select the appropriate AID that corresponds to the cardholder's account preference. The use of AID selection screens or labels to effectuate cardholder funding choice selection is optional, even for multi-account cards. Merchants that wish to maintain routing flexibility for debit transactions will need to deploy specific logic in their readers/terminals to ensure the Visa U.S. Common Debit AID is used for debit functionality, in addition to the non-paired Visa AID for credit functionality. See Appendix E: Special Terminal Logic.

Training should teach merchant front-line staff to understand and explain the application selection process where the merchant has chosen this implementation and how to guide their customers in selecting the application or account they prefer to use.

12.7.3 Cardholder Verification

Merchants and cardholders typically understand the methods of verifying a transaction in attended environments through cardholder signature or PIN entry. In unattended environments, the cardholder is also familiar with not having to sign and whether or not to enter a PIN.

In the chip environment, merchants and cardholders will rely on the chip-reading terminal and the chip card to agree on which CVM is required to complete the transaction.

The terminal and card interactive decision process and final selection is based on a mixture of elements that are specific to that particular transaction, such as amount, domestic or international transaction, whether the issuer's CVM preference can be met, and the other CVM options available.

[10] This does not apply to U.S. Covered Visa Debit Cards. Cardholder routing selection is not required for U.S. Covered Debit Cards and the U.S. Personalization Validation Requirements do not allow the Visa AID and the Visa U.S. Common Debit AID to be personalized to require cardholder confirmation.

Unlike magnetic stripe transactions where the card does not play a role in the selection of the CVM, in chip transactions the card plays a central role. The issuer determines its preference for the CVM used for a particular transaction, which is set in the card profile in the CVM list. The CVM list on a card will have a combination of CVMs and the rules for their use.

12.7.3.1 Signature

Visa card programs bearing a chip are required to also carry a magnetic stripe and a signature panel on the card.

Signature is supported by all Visa cards for cardholder verification. Requirements for checking signature verified transactions in the chip environment remain the same as they are in the magnetic stripe environment.

Signature is generally also used as the minimum level of cardholder verification when the card does not support CVM processing, "no CVM" was selected for processing, or if CVM processing failed. *Visa Rules* or local laws will determine the minimum level of CVM processing required.

12.7.3.2 PIN

Where PIN pads are deployed, training should include these points:

- The card, cardholder, and terminal interaction will determine the CVM and whether to prompt for a PIN.
- Because the card determines whether PIN entry is required on each transaction, lack of a terminal PIN prompt should not be considered an error. The merchant should not request PIN entry from the cardholder unless the terminal issues this prompt.
- Where a cardholder decides to enter a PIN, the secrecy of the PIN entry must be maintained.
- When a transaction is PIN-based, Visa's best practice is for a signature line not to be printed on the receipt. Merchants need to be aware that they should not request a signature from the cardholder when PIN is captured.
- Some cardholders might not enter the PIN at the POS terminal due to security concerns or certain disabilities. Merchants need to offer clear alternatives to these cardholders in accordance with merchant protection and local, state, or federal disability legislation.
    - A merchant or acquirer can promote their preferred CVM, including by steering towards PIN or auto-prompting for PIN, but they must minimally ensure that the cardholder has the ability to opt-out of PIN and to have an alternative method complete the transaction, e.g., signature or "no CVM."

- Recommended PIN opt-out options include:
    - Displaying a 'signature' button on the PIN prompt screen
    - Allowing the cardholder to use the 'cancel' button to opt out of PIN prompt, after clearly explaining to the cardholder how to opt out
    - Using "credit" and "debit" buttons or labels with "credit" used to indicate cardholder preference to opt-out of entering a PIN and "debit" used to indicate cardholder preference to enter a PIN just as those terms were frequently used in the pre-EMV environment

Regardless of the verification method, merchants may use the Visa U.S. Common Debit AID for those networks enabled by the issuer on the card and route to the network of their choosing. This is true for any cardholder verification method, including PIN, signature, and "no CVM."

Note: There are many options for how to offer PIN opt-out in a way that is transparent and consumer friendly. Cardholders can be confused by opt-out processes that utilize unlabeled terminal buttons to effect the opt-out (e.g., pushing the red button or the green button with no label or explanation). Merchants customizing their terminals to implement PIN opt-out must minimally ensure that a cardholder presenting a Visa Debit card for payment can originate a transaction using a signature (or "no CVM") even if the cardholder is prompted or steered to enter a PIN.

12.7.3.3 Consumer Device CVM (CDCVM)

VCPS 2.1 or higher readers must enable support for a Consumer Device CVM. The Consumer Device CVM is a CVM performed on the consumer's payment device (independent of the reader).

Reader support for the Consumer Device CVM is mandatory, as is indication of its support in the Terminal Transaction Qualifiers. In addition to supporting the Consumer Device CVM, the reader may support other CVMs such as signature and/or online PIN.

12.7.3.4 No Cardholder Verification Required (No CVM)

A chip card issuer has the ability to specify that a transaction may be completed, subject to other processing checks, without the need for the cardholder to provide a signature or enter a PIN. "No CVM Required" is a valid cardholder verification option where both the terminal and card agree on this CVM option.

This option would typically be used in unattended terminal environments. However, even when a card indicates "No CVM Required" for a particular type of terminal, the terminal may choose to default to the CVM specified for a magnetic stripe transaction to protect the transaction liability, e.g., signature at a POS or online PIN at an ATM.

Merchants participating in the Visa Easy Payment Service (VEPS) should be made aware that transactions below a certain limit will also not require any CVM and they should not request a CVM, if the terminal has not prompted for one.

12.7.4 Fallback Transactions

Visa policies state that chip cards must be read as chip cards at all times unless the chip card, chip reader, or terminal is malfunctioning. Chip cards may only be accepted via the magnetic stripe when the chip cannot be read.

In the event that a chip card or chip reader is not functioning and the physical magnetic stripe of the card is read, the terminal will read the service code and prompt the merchant to read the card as a chip card. Acquirers need to train merchants on the activities they should perform and the sequence of events they should follow when they are processing fallback transactions. Typically, the cashier will be given a number of chances to read the chip card using the terminal chip reader before the terminal prompts for fallback to be performed using the magnetic stripe, if permitted.

If the magnetic stripe functionality of the card or terminal is also not working or an online authorization is not available, merchants may then fallback to existing card acceptance procedures. Acquirers may need to revise their procedures on fallback related to PAN Key Entry and paper-based transactions.

Fallback requirements are governed by the *Visa Rules* relating to the Visa and Visa Electron programs. Fallback on Visa Electron cards beyond the magnetic stripe is not permitted and may not be possible (the full account number may not be printed on the face of the card). Acquirers can contact their Visa representative for further information.

Merchants must understand that a declined chip transaction is not a candidate for fallback and cannot be reinitiated using the magnetic stripe or any other means. If this does occur, the transaction can be charged back by the issuer.

Current procedures should then be followed for declines and failures, such as asking the customer for another form of payment.

Merchants should not force a fallback transaction as a way to circumvent the chip and potentially bypass the additional chip controls. Merchants may attempt to deliberately force a fallback by inserting the card incorrectly into the reader or by other means. Merchants should be made aware of the potential risk of accepting fraudulent cards by not making use of the additional controls included in the chip.

12.7.5 Other Transactions

Authorizations where the transaction is suspicious, refund or credit transactions, reversals, and voids are completed as they are performed today but via the chip, subject to individual acquirer requirements. Other card security features must be checked at the point of transaction.

12.7.6 Care of the Terminal

Training should include instructions on looking after terminals and keeping magnetic stripe and chip readers clean and free of obstructions.

Visa recommends that merchants regularly service their terminals, ensure that the battery is charged, and install them in protected places to prevent damage or loss of transactions due to a dead terminal.

12.7.7 International Transactions

Training should include instructions on supporting international transactions. Magnetic stripe cards are in frequent use throughout the world. Merchants should be aware that when accepting international cards, the Cardholder Verification Method may vary depending on the country of issuance.

12.7.8 Terminated Visa payWave Transactions

Acquirers may want their merchants to include information about terminated transactions in the merchant's communications and training plans. Ensuring that the merchant understands the difference between a terminated transaction (which means the transaction can continue over a different interface) and a declined transaction (which is a finished transaction with no possibility for another interface) will result in less confusion with the cardholder during the transaction.

Appendix A. Planning Checklist

Each acquirer implementation is different and the level of effort required will vary. An understanding of the features and benefits of chip and how they will address business needs, along with upfront preparation, can have a significant effect on the project duration.

Implementing chip will affect staff, merchants, terminal vendors, business processes and systems. It may require a cross-discipline team following project management best practices to manage several distinct, parallel tasks toward a common implementation date.

This appendix is designed to help acquirers plan the implementation of their chip program and develop a detailed work plan. It provides a checklist with policy, operation, and technical support activities that acquirers need to accomplish. Please note that the following contains suggestions and is not intended to be a complete list of all factors to consider.

Table A–1: Policy Related Tasks

#	Topic	Task	Description
1	General	Conduct situation analysis	Conduct market research, competitor analysis, business case, and liability shift impact
2	General	Develop launch strategy and plan	• Define launch objectives • Determine need for pilot • Determine broad launch plan • Create launch timetable
3	General	Define target merchant program	• Prioritize merchant segments including high risk merchant segments • Review pricing • Determine merchant benefits including liability shift and TIP • Consider implication of chip on merchant monitoring and management information systems
4	POS Related	Develop POS terminal strategy	• Define terminal replacement program to incorporate chip • Determine education and technical support
5	POS Related	Develop POS terminal requirements	• Cardholder Selection/confirmation • AIDs to support • Languages to support • CVM methods • Contactless support via integrated or separate readers
6	POS Related	Determine TMS support for chip	• Understand requirements to upgrade existing TMS • Determine need to procure new TMS to support chip

Table A–2: Operational Related Tasks

#	Topic	Task	Description
1	Terminal selection	Assess target merchant requirements	• Determine merchant environments (e.g., POS, UCAT, AFD) • Determine terminal characteristics
2	Terminal selection	Terminal Approval (EMV)	• Confirm terminal is in EMVCo approved list • If not approved, seek details for approval process
3	Terminal selection	Contactless reader Approval (VCPS and EMV Contactless)	• Confirm if reader is in Visa approved list and in EMVCo Level 1 approved list for contactless • If not approved, seek details for approval process
4	Terminal selection	PCI compliance	• Confirm if terminal is in PCI approved list • If not approved, seek details for approval process
5	Terminal selection	Determine terminal requirements	• Customize requirements to suit merchant and market needs • Determine CVM requirements • Processing restrictions
6	Merchant agreements	Update merchant agreements to account for new terminal functionality	• Evaluate need to change merchant agreements to include additional details relating to VSDC and Visa payWave support such as TIP and Liability Shift
7	Merchant migration	Merchant migration plan	• Develop a migration and rollout plan for key merchants and merchant segments • Account for lead times to source terminals and make system changes if any
8	Merchant migration	Merchant system changes	• Evaluate chip impact on terminal to merchant host interface and back office changes • Determine any changes to network and host capacity due to additional chip data
9	Merchant migration	Training program	• Determine training objectives and requirements • Incorporate new materials in existing training kits or develop new kits if required
10	Merchant migration	Terminal installation	• Order new terminals • Create testing plans • Develop installation timetable • Undertake end-to-end testing
11	Program launch	Develop launch program	• Confirm monitoring plans and prelaunch review • Conduct pilot to gather additional information • Undertake production launch
12	Program launch	Conduct post launch review	• Carry out implementation review • Identify and review issues arising from launch • Review internal process to address issues from launch

Table A–3: Technical Related Tasks

#	Topic	Task	Description
1	Terminal related	Determine terminal parameters and settings	Complete technical activities related to EMV and VCPS including supported CVMs, Processing Restrictions, and TACs
2	Terminal related	Transaction type requirements	• Determine transaction types to be supported (e.g., pre-authorization, refund, cash-back)
3	Terminal interface	Make necessary changes to terminal to acquirer interface	• Analyze changes to allow new chip data to be sent to host including support for fallback • Make changes to host interface and test
4	TMS	Ensure TMS supports chip related data elements	• Determine chip specific elements required to be supported by TMS • Determine whether existing TMS can support chip or an upgrade is required • Develop new processes to update and verify chip related changes made by TMS
5	Host changes	Evaluate necessary host changes	• Evaluate new data requirements for chip including for fallback transactions • Identify clearing and settlement processing • Consider changes required for back office activities and reporting
6	Host changes	Host testing	• Undertake systems testing prior to testing using VTS-VIP and Visa host test cards • Undertake online testing with Visa using VCMS • Undertake BASE II testing if applicable
7	Testing	ADVT	• Obtain latest version of ADVT • Perform testing and submit results to Visa
8	Testing	CDET	• Obtain latest version of CDET • Perform testing and submit results to Visa

Appendix B. V.I.P. System Message Requirements

Acquirers in the U.S. will be required to be able to carry and process chip data that is included in EMV chip transactions. All of the new data will be carried in Field 55 which is a TLV (Tag- Length-Value) format field. Table B–1: V.I.P. System Field 55 Mandated Data Tags outlines the mandated tags that must be supported and Table B–2: V.I.P. System Chip-related Fields outlines other chip fields that must be supported.

Table B–1: V.I.P. System Field 55 Mandated Data Tags

Data Element	Tag	Length	Description
Length of Field 55	n/a	1 byte	Total length of Field 55.
Dataset ID	n/a	1 byte	Contains an ID that identifies the type of data carried in this dataset. For Visa chip transactions, the value must be 01.
Dataset Length	n/a	2 bytes	Contains the length of the data that follows the dataset ID. The first byte is always zero. The second byte must equal the total length of Field 55 (specified in byte 1) minus 3.
Amount, Authorized	9F02	6 bytes	Originates from the acquiring POS device. Contains the amount of the transaction used by the cardholder's device when generating the application cryptogram.
Amount, Other	9F03	6 bytes	Originates from the acquiring POS device. Contains the amount of cash-back used by the cardholder's device when generating the cryptogram. Only applicable for cash-back transactions.
Application Cryptogram	9F26	8 bytes	Originates from the cardholder's device. Contains the online authentication cryptogram generated by the cardholder's device during the transaction. This cryptogram is validated by VisaNet (or the issuer) to ensure the cardholder's device is not counterfeit.
Application Interchange Profile	82	2 bytes	Originates from the cardholder's device. Contains information about the capabilities of the cardholder's device.
Application Transaction Counter (ATC)	9F36	2 bytes	Originates from the cardholder's device. Contains a counter that is incremented for each transaction and which, by inclusion in the application cryptogram, can prevent counterfeit cardholder devices.
Customer Exclusive Data	9F7C	Variable, up to a maximum of 32 bytes	Originates from the cardholder's device. Contains customer exclusive data. Must be sent by acquirer if present in the card. Only applicable for contactless transactions.

Data Element	Tag	Length	Description
Dedicated File (DF) Name	84	Variable, from 5 to 16 bytes	Contains the Application Identifier (AID) that was selected to initiate the transaction.
Form Factor Indicator	9F6E	4 bytes	Contains indicators about the attributes of the cardholder's device and the technology used for communication between the cardholder's device and the acquiring POS device. Must be sent by the acquirer if present in the card. Only applicable for contactless transactions.
Issuer Application Data	9F10	Variable, up to a maximum of 32 bytes	Originates from the cardholder's device. Contains various data from the cardholder's device depending on how its setup by the issuer.
Issuer Scripts Results	9F5B	Variable up to 21 bytes	Originates from the acquiring POS device. Indicates the results of issuer script template (1 or 2) processing. Only applicable to reversals.
Terminal Capabilities	9F33	3 bytes	Originates from the acquiring POS device. Indicates the cardholder's device data input, the cardholder verification method, and the security capabilities supported by the acquiring POS device.
Terminal Country Code	9F1A	2 bytes	Originates from the acquiring POS device. Identifies the country in which the acquiring POS device is located.
Terminal Verification Results (TVR)	95	5 bytes	Originates from the acquiring POS device. Generated during transaction processing; contains the results of risk management performed by the acquiring POS device.
Transaction Currency Code	5F2A	2 bytes	Originates from the acquiring POS device. Contains the currency code used for the transaction.
Transaction Date	9A	3 bytes	Originates from the acquiring POS device. Contains the local date on which the transaction was authorized.
Transaction Type	9C	1 byte	Originates from the acquiring POS device. Indicates they type of financial transaction (e.g., cash, purchase, etc.) as represented by the first two (2) digits of the processing code.
Unpredictable Number	9F37	4 bytes	Originates from the acquiring POS device. Contains an unpredictable number for the transaction to add variability to the application cryptogram. The acquiring POS device passes this unpredictable number to the cardholder's devices, which uses it to generate the application cryptogram along with other data elements.

Data Element	Tag	Length	Description
Issuer Authentication Data	91	Variable, from 8 to 16 bytes	Originates from VisaNet or the issuer. Contains authentication data sent in the authorization response used by the cardholder's device to authenticate the issuer.
Issuer Script Template 1	71	Variable, up to 256 bytes	Originates from the issuer. Contains any issuer script commands to update one or more parameters on the cardholder's advice. ***Note:*** *The acquirer may receive either Issuer Script Template 1 or Issuer Script Template 2 in the issuer's response, but not both.*
Issuer Script Template 2	72	Variable, up to 256 bytes	Originates from the issuer. Contains any issuer script commands to update one or more parameters on the cardholder's advice. ***Note:*** *The acquirer may receive either Issuer Script Template 1 or Issuer Script Template 2 in the issuer's response, but not both.*

Table B–2: V.I.P. System Chip-related Fields

Field	Description
22	POS Entry Mode
23	Card Sequence Number
44.8	Card Authentication Results Code
60.2	Terminal Entry Capability
60.3	Chip Condition Code
60.6	Chip Transaction Indicator
60.7	Card Authentication Reliability Indicator

Appendix C. Reference Materials

Key materials referenced throughout this Guide are listed in the table below. Please ensure you are using the latest versions of the Visa and other industry documents applicable to your implementation.

Note: There may be other requirements/specifications required to support and validate the cards for use in the Visa payments system.

Acquirers and non-client processors must have Visa Online (VOL) access to Visa Chip and Contactless Implementation page on VOL to download the Visa Implementation materials. All Visa materials are available on this site, unless noted otherwise. To request a VOL ID, clients must send an email to volamericas@visa.com.

For access to chip specifications, clients must already have a VOL ID must and request entitlement to the Visa Chip and Contactless Specs page by sending an email to volamericas@visa.com. When access is granted, the Chip and Contactless Specs link will appear on the VOL home page.

Please note that:

- VCMS materials are available on VOL VisaNet Testing pages (https://www.us.visaonline.com/us_sysoprs/testing/default.asp?src=home_sys_quicklink)
- For non-Visa materials, the sites are listed in the table, for example EMVCo.
- Licensed vendors may download licensed Visa materials from the Visa Technology Partner site (https://technologypartner.visa.com).

The table below lists key documents that may apply to your chip card program.

Table C–1: Reference Materials

Title and Description	Audience	User
Visa Transaction Acceptance Device Guide (TADG) Provides guidelines and best practices relating to implementation of Visa compliant acceptance devices including requirements for chip.	Acquirers, Terminal Vendors	Technical
Visa Transaction Acceptance Device Requirements (TADR) For ease of reference and to facilitate client access to device requirements not found in the *Visa Rules*, Visa consolidated most of these rules into TADR document.	Acquirers, Terminal Vendors	Technical
Visa Integrated Circuit Card Specification (VIS) Based on EMV, and provides the technical details of chip card functionality related to Visa Smart Debit and Visa Smart Credit transactions.	Issuers, Acquirers, Terminal Vendors	Technical

Title and Description	Audience	User
Visa Easy Payment Service (VEPS) Acquirer Program Provides acquirers an overview of VEPS along with acquirer implementation activities.	Acquirers	Technical
Visa Smart Debit/Credit (VSDC) System Technical Manual Provides detailed information for VisaNet chip-based debit/credit processing, including an overview of required host system changes. This document is designed to complement the payment service rules and VIS.	Acquirers, Issuers	Technical
Visa Smart Debit/Credit (VSDC) Acquirer Implementation Guide (global version) Provides guidelines and best practices relating to implementation of contact chip including support for offline-capable devices and offline processing options.	Acquirers	Business, Operations, Technical
Visa payWave Acquirer Implementation Guide (global version) Provides implementation guidelines for acquirers choosing to implement contactless devices that accept Visa payWave cards. Guides for *VCPS 2.0.2 and VCPS 2.*1 are available.	Acquirers	Business, Operations, Technical
Visa Contactless Payment Specification Version 2.0.2 – including additions and clarifications Defines the requirements for conducting Visa payWave transactions at point of sale devices and chip data messages.	Acquirers, Issuers, Terminal Vendors	Technical
Visa Contactless Payment Specification Version 2.1 – including published updates Defines the requirements for conducting Visa payWave transactions at point of sale devices and chip data messages.	Acquirers, Issuers, Terminal Vendors	Technical
Visa Product Brand Standards *(VPBS) site* *Your resource for* guidelines and artwork for use by acquirers, merchants and partners to accurately reproduce the Visa Brand mark and Contactless Symbol on payment terminals.	Acquirers, Merchants	Operations
Visa Global ATM Member Guide Designed to provide information necessary for Visa and Plus clients to successfully use the Visa Global ATM network and establish, manage or sponsor ATM cash access programs.	Acquirers	Operations, Technical
Visa Rules (Available at Visa.com)	Acquirers, Issuers	Business, Operations, Technical
Visa U.S. Chip and Contactless Definitions (Available at Visa Online)	Acquirers, Issuers, Merchants	Business, Operations

Title and Description	Audience	User
Visa Test Tools **Refer to Section 7 for process to obtain the test tools**		
Acquirer Device Validation Toolkit (ADVT) User's Guide Accompanies the ADVT, which is a deck of test cards, developed to provide a greater degree of service quality assurance to chip acquirers and device vendors developing and deploying chip reading devices. Its purpose is to validate the configuration of their EMV chip-reading devices. Available as part of the toolkit.	Acquirers, Terminal Vendors	Operations, Technical
U.S. Quick Chip and Minimum Terminal Configuration ADVT Use Cases	Acquirers, Terminal Vendors	Operations, Technical
Visa Contactless Device Evaluation Toolkit (CDET) User Guide Accompanies the CDET, which provides a means for contactless card reader suppliers and Visa acquirers (or agents) implementing a contactless chip program to test devices prior to deployment. Available as part of the toolkit.	Acquirers, Terminal Vendors	Technical
Chip Compliance Reporting Tool User's Guide for Chip Acquirers Provides guidelines and information on use of CCRT. Available from CCRT help menu. Access to CCRT is via VOL.	Acquirers	Operations, Technical
Visa U.S. EMV Chip Terminal Testing Document	Acquirers, Terminal Vendors, Merchants	Business Operations Technical
EMV Migration Forum Testing and Certification White Paper	Acquirers, Terminal Vendors, Merchants	Business Operations Technical
VisaNet Certification Management Service (VCMS) Available on VOL VisaNet Testing site (https://www.us.visaonline.com/us_sysoprs/testing)		
VisaNet Testing Best Practices for Issuers and Acquirers Outlines best practices and testing processes.	Acquirers, Issuers	Business, Technical
VCMS Testing Guide – V.I.P System, Client Version Explains requirements and procedures for testing with Visa's V.I.P. System.	Acquirers, Issuers	Technical
Visa Test System – V.I.P. User's Guide Provides procedures for installing and using VTS-VIP to run scripts for client pre-testing or host testing with VisaNet.	Acquirers, Issuers	Technical
VCMS Testing Guide – BASE II, Client Version Explains requirements and procedures for testing with Visa's BASE II System. Includes information on use of Visa Test System – Clearing and Settlement (VTS-CS).	Acquirers, Issuers	Technical

Title and Description	Audience	User
EMVCo Available at www.emvco.com		
EMV Integrated Circuit Card Specifications for Payment Systems Specifications consist of four books, available for view or download at www.emvco.com. ***Note:*** *Specification Bulletins are posted to the Specifications Section of EMVCo website. As the specification and the website are updated periodically, acquirers should ensure they have the latest version by checking the website.*	Acquirers, Issuers, Terminal Vendors	Technical
The EMV Contactless Specifications for Payment Systems consist of four books, available for view or download at www.emvco.com. ***Note:*** *Specification Bulletins are posted to the Specifications Section of EMVCo website. As the specification and the website are updated periodically, acquirers should ensure they have the latest version by checking the website.*	Acquirers, Issuers, Terminal Vendors	Technical
Recommendations for EMV Processing for Industry-Specific Transaction Types Describes a recommended approach to handling certain types of EMV-enabled transactions and environments including integrated POS and standalone terminals. It describes "best practice" implementations in certain environments and for certain types of transactions.	Acquirers, Terminal Vendors	Operations, Technical
PCI Materials Available at https://www.pcisecuritystandards.org/security_standards/documents.php		
Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements *PCI Payment Application Data Security Standards (PA-DSS)* Payment Card Industry requirements for Encrypting PIN pads and PIN acceptance devices used at the point of sale (POS) and for Application Data Security.	Acquirers, Terminal Vendors	Technical

Appendix D. Basic EMV Terminal Logic

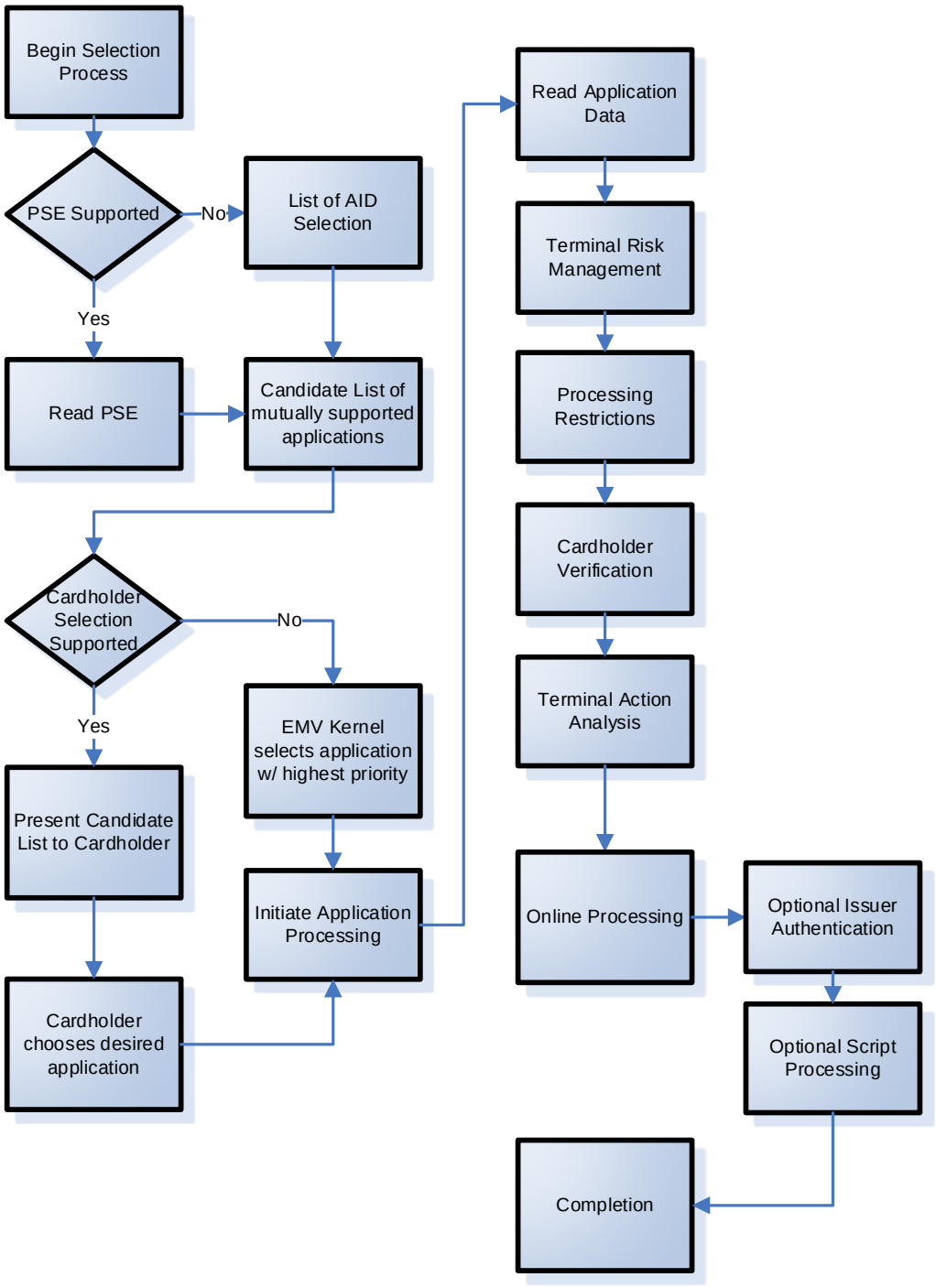
The following diagram provides an overview of the basic EMV terminal logic, with a specific focus on the selection process discussed in Section 4: Visa's Chip Terminal and Reader Requirements.

Visa cards may contain products associated with different funding sources. For example, some cards may contain two Visa AIDs, one Visa AID associated with a line of credit, and one Visa AID associated with a demand deposit account. Cardholder Selection ensures the account used for the transaction is appropriate and is what the cardholder expects.

The EMV architecture supports this same multiple AID concept for U.S. debit cards, where U.S. debit products carry two AIDs (a Visa AID and a Visa U.S. Common Debit AID), with both linked to the same funding source. U.S. cards may also contain a Visa AID that invokes a credit product, as well as the paired AIDs (the Visa AID and the Visa U.S. Common Debit AID) that invoke a debit product (only the debit product Visa AID will be paired with a Visa U.S. Common Debit AID). The employment of the EMV logic of Cardholder Selection ensures support is provided for both U.S. Debit cards with a single funding source and those with multiple funding sources (such as a card supporting both debit and credit), but is not required for single funding source cards.

Visa Easy Payment Service (VEPS) merchants may wish to deploy a selectable kernel structure in order to eliminate CVM requirements on VEPS-qualifying transactions. An example of selectable kernel processing is given in Figure E–4: Combined CVM Processing and Selectable Kernel in Section E.3.

Figure D–1: Basic EMV Terminal Logic



Appendix E. Special Terminal Logic

This appendix describes the special terminal logic that is necessary for a merchant to select the desired AID to effectuate routing options for U.S. Covered Visa Debit Cards, to select an AID eligible for the desired function (e.g., cash-back), and to support cardholder CVM selection.

The EMV architecture supports the multiple AID concept for U.S. debit cards, where U.S. debit products carry two AIDs with both linked to the same funding source ("paired AIDs"). U.S. cards may contain a Visa AID that invokes a credit product, as well as a Visa AID that invokes a debit product. (Only the debit product AID will be paired with a Visa U.S. Common Debit AID.) Implementation of special terminal logic should include support for all forms of multiple AID structures on the card.

Important: The Visa U.S. Common Debit AID must not be automatically selected without first correctly identifying the paired applications because this approach does not allow for the proper processing of true multi-application cards which may contain both debit and credit applications.

To support debit routing, U.S. Covered Visa Debit Cards will be issued with both the Visa AID and the Visa U.S. Common Debit AID and both AIDs may be present in U.S. terminals. When the Visa U.S. Common Debit AID is the AID selected for the transaction, U.S. merchants and acquirers can use BIN routing logic to route these transactions to the appropriate debit network. When the Visa AID is selected, the transaction must be routed to Visa.

To clarify, for U.S. Covered Visa Debit Cards, merchants have flexibility to use either the Visa U.S. Common Debit AID or the Visa AID. Merchants are not required to use the Visa AID, and may route U.S. Debit transactions using the Visa U.S. Common Debit AID exclusively if they so choose.

A merchant or acquirer can promote their preferred CVM, including by steering towards PIN or auto-prompting for PIN, but they must minimally ensure that that the cardholder has the ability to opt-out of PIN and have an alternative method to complete the transaction, e.g., signature or "no CVM."

Appendix E.1: Contact Terminal Application Selection defines the necessary special logic transaction flow for a contact EMV terminal, while Appendix E.2: Contactless Reader Application Selection/Special Logic defines the necessary flow for a Visa contactless reader.

This appendix also illustrates the special contact terminal CVM logic that is necessary for a merchant participating in Visa's VEPS program or a merchant that supports cash-back. Appendix E.3: Contact CVM Processing and Selectable Kernels Logic defines the necessary CVM processing for a contact EMV terminal to support VEPS processing.

The reference "Visa AID" is used to identify any AID that begins with the Visa ISO RID as defined in Section 4.2.1.

E.1 Contact Terminal Application Selection / Special Logic

E.1.1 Contact Terminal Application Selection Data Elements

As stated in Section 4.4.3, a contact chip terminal may need special logic in support of AID selection needed to support specific functional and routing requirements. This appendix describes how this special logic can be implemented.

The process utilizes the following data elements from the card (for data element descriptions, see EMV or VIS):

Table E–1: Contact AID Selection Data Elements

Data Element Name	Tag	Comment
Application Label	'50'	Issuer-defined text providing a meaningful identifier for the cardholder
Application Priority Indicator	'87'	The lower a value, the higher a priority (except for zero, which means "No priority")
Directory File (DF) Name	'84'	In this appendix, referred to as the (card) AID
Issuer Identification Number (IIN)	'42'	In this document called the BIN

E.1.2 Contact Terminal Application Selection Special Processing Logic

The process of selecting the appropriate AID for particular functions and routing options is discussed in this appendix.

If basic EMV Cardholder Selection is not used, special logic can be employed to select the appropriate AID as outlined below. Alternatively, other functionally equivalent methods may be implemented. The AID selected has implications on routing eligibility: routing flexibility may only be achieved via the Visa U.S. Common Debit AID.

After the terminal has built the Candidate List during Application Selection (as defined in Section 4.4.1 or – in detail – in Section 12.3 of EMV, Book 1), the terminal examines the Candidate List as follows:

1. If only one AID is present, that AID is used to initiate transaction processing.
2. If two AIDs are present and, besides the Visa AID, one is recognized as the Visa U.S. Common Debit AID, the terminal can examine the card response for both AIDs. Further processing depends on card response:

a. The terminal compares the BIN returned for the Visa U.S. Common Debit AID with the BIN of the Visa AID. If the BIN returned for the Visa AID is equal to the BIN returned for the Visa U.S. Common Debit AID, then the Visa U.S. Common Debit AID is associated with the corresponding Visa AID (i.e., is a debit pair), and represents access to the same source of funds.
If no BIN is returned for the Visa AID or the BIN returned is not equal to the BIN returned for the Visa U.S. Common Debit AID, continue with basic EMV Application Selection processing.

Note: In order to identify debit pairs, Visa rules require the issuer BIN to be present for debit AIDs on a U.S. Covered Visa Debit Card.

b. For a terminal implementation where the cardholder is able to indicate the desired CVM selection:[11]

   i. If the cardholder has indicated a preference for signature/no CVM, the terminal logic may choose to eliminate the Visa U.S. Common Debit AID, thereby selecting the Visa AID, or the merchant may invoke a dynamically selectable kernel to disable the PIN function, and then may select the Visa U.S. Common Debit AID (and capture the signature if required per network rules).

   ii. If the cardholder has indicated a desire for cash-back and/or a willingness to enter a PIN ("Debit", "Cash-back"), select the Visa U.S. Common Debit AID and continue with standard EMV processing.

c. For a terminal implementation where the cardholder indicates CVM selection after AID selection (e.g., EMV PIN Entry Bypass[12]):

   i. If a PIN prompt is forced (no prior cardholder selection), the consumer must be offered the ability of either proceeding by entering the PIN **OR** obtaining access to an alternate CVM through one of the three following options:

      1) Load a No CVM selectable kernel and restart with the Visa U.S. Common Debit AID. Complete the transaction with standard EMV processing, which will result in "No CVM," and capture signature if required by network rules. (Merchants could choose this implementation option to maintain routing flexibility and process transactions using the Visa U.S. Common Debit AID, while maintaining cardholder CVM choice.).

      2) Use EMV PIN Entry Bypass. (Merchants could choose this implementation option to maintain routing flexibility and process transactions using the Visa U.S. Common Debit AID, while maintaining cardholder CVM choice.)

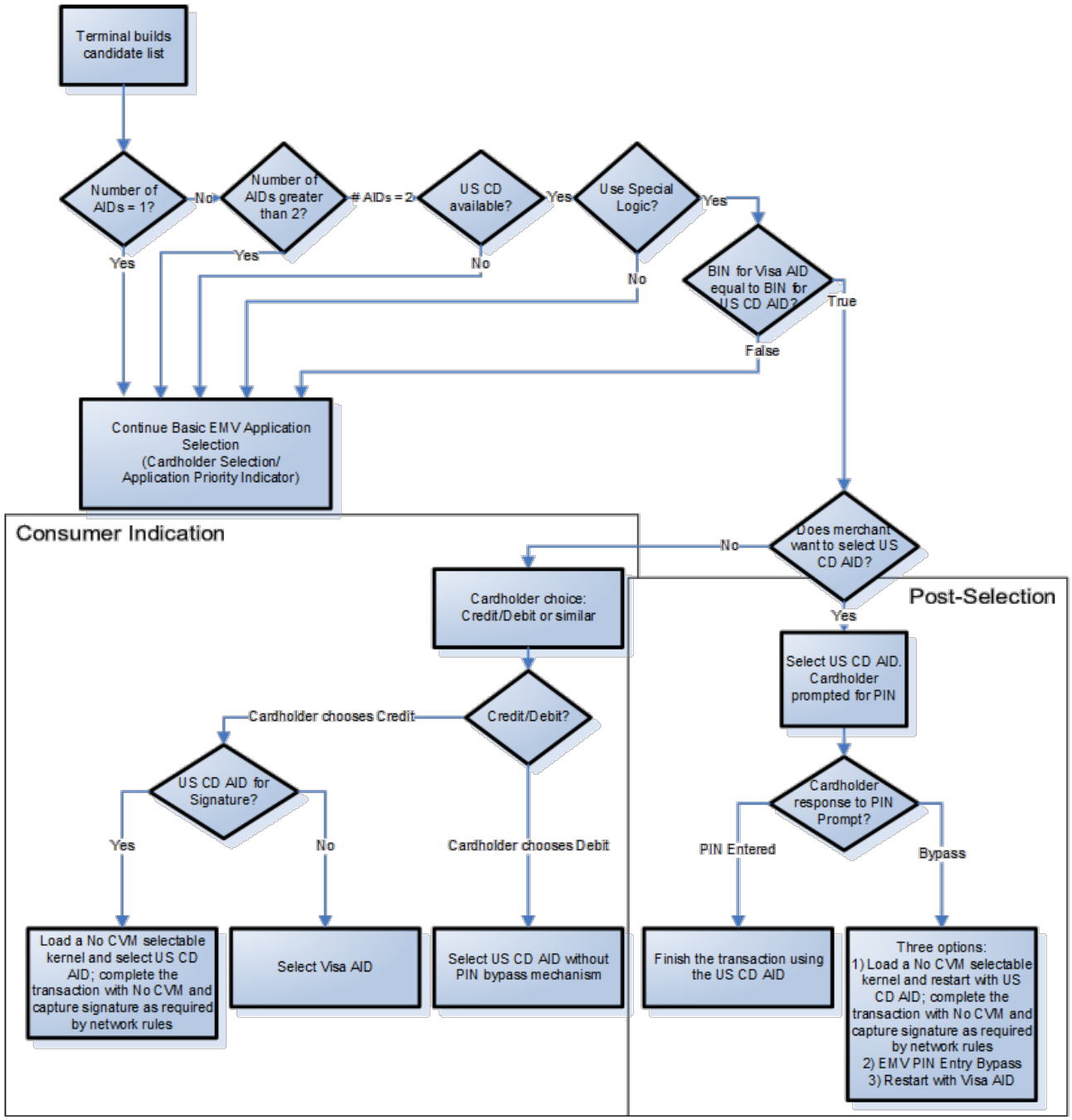
      3) Restart the transaction using the Visa AID.

3. If more than two AIDs are present, continue with basic EMV Application Selection processing as described in Appendix D by using Cardholder Selection.

[11] For example, via a Signature/PIN selection function on the terminal
[12] PIN Entry Bypass as defined in section 6 of EMV Book 4.

E.1.3 Contact Application Selection Special Logic Flow Chart

Figure E–1: Contact Application Selection Special Logic Flow Chart



E.1.4 Flow Example using Consumer Indication

The merchant has the option of offering the familiar Debit/Credit selection function, as shown in the "Consumer Indication" section in Figure E–1: Contact Application Selection Special Logic Flow Chart. By selecting "Debit," this will allow for selecting the Visa U.S. Common Debit AID. By selecting "Credit," the merchant has the option to select the Visa AID or to retain the Visa U.S. Common Debit AID in conjunction with a selectable kernel supporting "no CVM" (and signature by using a "capture signature" indicator as described in Appendix E.1.6: Flow Example for Visa U.S. Common Debit AID using Signature/No CVM).

The merchant may prefer to offer a PIN or Signature selection function. Examples of appropriate terminal prompts include:

- Visa Debit (Sign)/Debit (PIN)
- Visa Debit (Sign)/PIN Debit

Selection of the Visa U.S. Common Debit AID allows for routing across alternate unaffiliated networks in addition to the existing Visa networks.

E.1.5 Flow Example using Visa U.S. Common Debit AID and Post-Selection

The merchant has the option of selecting the Visa U.S. Common Debit AID without cardholder input, as shown in the "Post-Selection" section in Figure E–1: Contact Application Selection Special Logic Flow Chart. If logic exists that selects the Visa U.S. Common Debit AID without previous cardholder input, the consumer must be offered the option to select an alternate CVM than the prompted CVM.

Access to alternate CVMs can be obtained by one of three methods:

- Load a No CVM selectable kernel and restart with the Visa U.S. Common Debit AID. Complete the transaction with standard EMV processing, which will result in "no CVM." Signature can be captured as required by network rules and as shown in Appendix E.1.6: Flow Example for Visa U.S. Common Debit AID using Signature/No CVM.
- Allow EMV PIN Entry Bypass.
- Restart the transaction using the Visa AID.

Selection of the Visa U.S. Common Debit AID allows for routing across alternate unaffiliated networks in addition to the existing Visa networks.

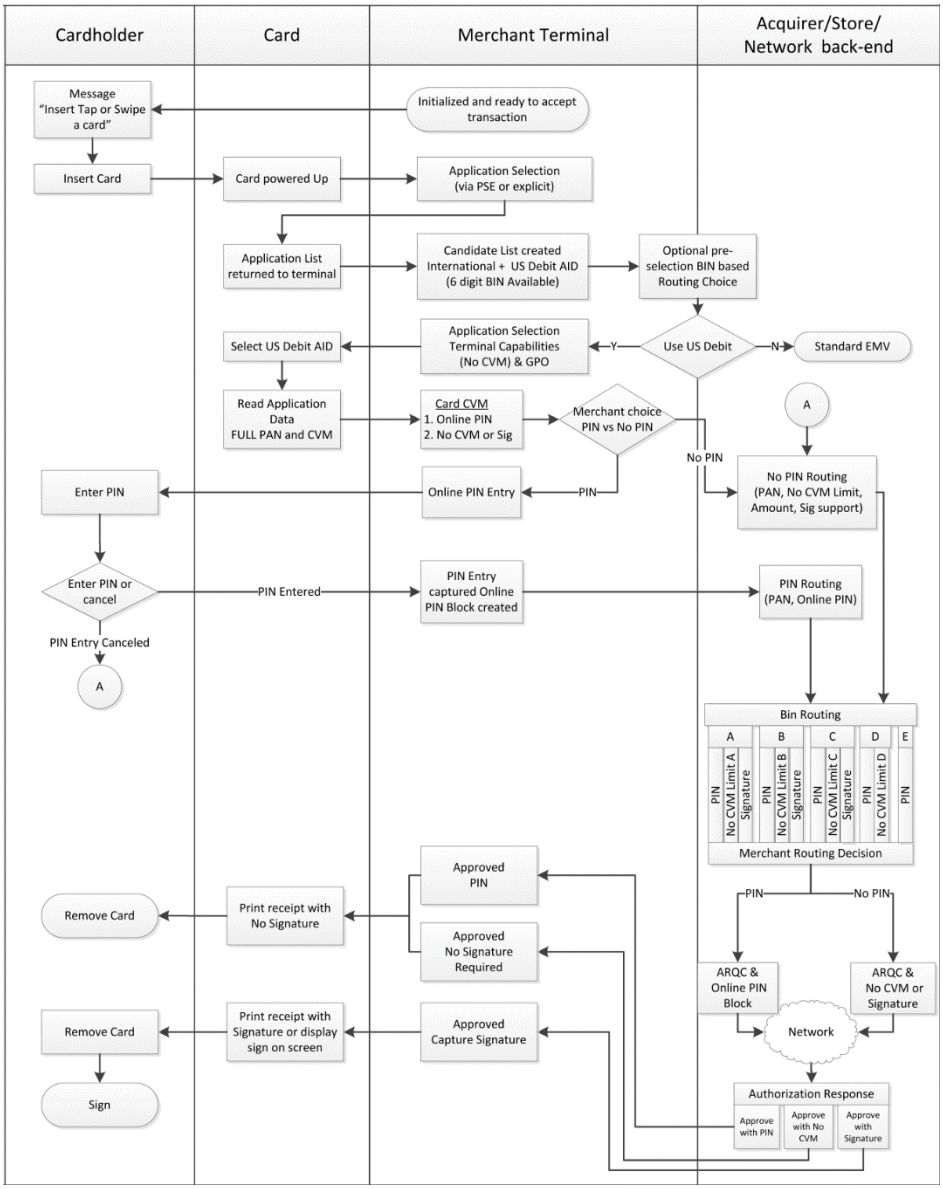
E.1.6 Flow Example for Visa U.S. Common Debit AID using Signature/No CVM

In this flow, the Visa U.S. Common Debit AID has been selected based on the flows described in Figure D–1: Basic EMV Terminal Logic. In order to process a Signature/No CVM transaction in this scenario, a selectable kernel is assumed whereby the terminal is dynamically configured based on a merchant or network determined transaction amount. While the Visa U.S. Common Debit AID is not personalized to support Signature, this approach can be used to obtain Signature where desired, by having the acquirer deliver a "capture signature" indicator to the terminal in conjunction with the approval response.

To accomplish this, configure Terminal Capabilities for No CVM Required and capture Signature if required by the host/network.

The following diagram was developed by the EMV Migration Forum, and illustrates an approach to U.S. common debit application acceptance for each of the supported CVMs.

Figure E–2: Visa U.S. Common Debit Application Acceptance Overview with PIN/Signature/No CVM



E.2 Contactless Reader Application Selection/Special Logic

As mentioned in Section 4.5.1, a contactless chip reader may need special logic to support custom AID selection, which must be executed before the basic contactless application selection. This appendix describes how this special logic can be implemented, if applicable.

For all contactless cards and mobile phones, the PPSE is a mandatory function, which can be utilized by a reader application to get a list of available applications on the card or mobile phone. For cards, the PPSE has been populated by the issuer through personalization, while for mobile phones, it is dynamically populated by the consumer on the mobile phone itself before the payment transaction takes place.

Note: While alternate routing for contactless cards can happen via contact chip or physical magnetic stripe interface, the same is not true for mobile phones or other non-card form factors.

The process utilizes the following data elements from the card:

Table E–2: Contactless AID Selection Data Elements

Data Element Name	Tag	Comment
Application Priority Indicator	'87'	The lower a value, the higher a priority (except for zero, which means "No priority")
Directory Entry	'61'	There is one directory entry per AID in the PPSE each defining a separate ADF Name, Application Priority Indicator and (optionally) Issuer Identification Number
Directory File (DF) Name	'84'	In this appendix, referred to as the (card) AID
Issuer Identification Number (IIN)	'42'	In this appendix referred to as the BIN

Note: Because MSD processing is functionally equivalent to magnetic-stripe processing (though with the enhanced security of dCVV or CVN 17) routing for MSD transactions can be accomplished through the use of BIN routing logic.

E.2.1 Processing

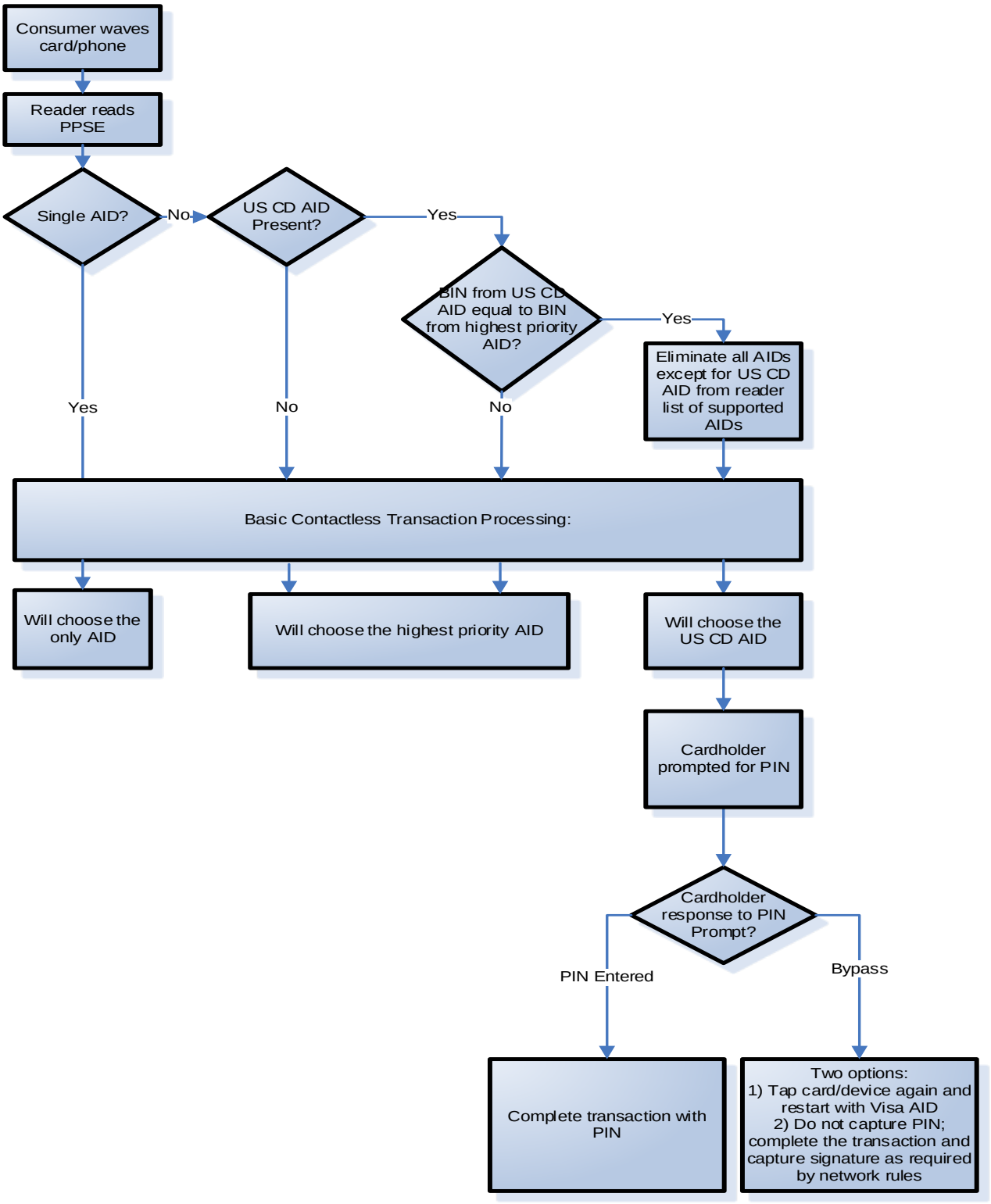
Because contactless does not support Cardholder Selection as in contact EMV, a contactless reader may need to execute a separate "pre-select" reader function once the card/device enters the contactless field but before the standard contactless transaction processing in order to examine the mutually supported AIDs. Since the contactless transaction processing will always select the highest-priority mutually-supported AID, the special logic “pre-selects” the desired AID needed to support merchant routing options. The “pre-selection” consists of removing all other AIDs from the reader’s list of supported AIDs. The AID used to initiate the transaction has implications on routing eligibility: routing may only be done via a U.S. Common Debit AID.

During this pre-select function, the reader selects the PPSE and receives a list of available AIDs on the card. With the list of AIDs on the card combined with the list of supported AIDs on the reader, the reader performs the following logic:

1. If the Directory Entry in the PPSE contains a single mutually supported AID, the reader continues with a standard contactless payment transaction flow without further special processing.
2. If the Directory Entry in the PPSE contains more than one mutually supported AIDs and the highest priority AID represents a functional or routing option that is consistent with the merchant desire for flexible routing, the reader continues with a standard contactless transaction flow without further special processing.
3. If the Directory Entry in the PPSE contains more than one mutually supported AIDs but the highest priority AID does **not** represent the desired functional or routing option, the reader interrogates the PPSE further. Further processing may take one of two paths as described in Appendix E.2.2.1: Direct Selection of the .
4. The outcome of the previous steps should be clearly understood by the cardholder, whether a basic contactless selection process or special logic selection process is used. This can be accomplished by notifying the cardholder via the display (Application Label or enhanced descriptor) and/or via the receipt (AID, as required by EMV).

E.2.2 Contactless Reader Application Selection Special Logic "Pre-Selection"

Figure E–3: Special Contactless Application "Pre-Selection" with Opt-out of PIN



E.2.2.1 Direct Selection of the Visa U.S. Common Debit AID

For a terminal implementation where the terminal programming will directly select the Visa U.S. Common Debit AID, and where the PPSE contains the Visa U.S. Common Debit AID, the terminal takes the following steps:

1. If there is only a single AID, that AID will be used.
2. If the Visa U.S. Common Debit AID is not present, the reader continues with a standard contactless transaction flow without further special processing.
3. If the BIN returned for the Visa U.S. Common Debit AID is equal to the BIN returned for the highest priority AID, eliminate all AIDs except the Visa U.S. Common Debit AID and continue Standard Contactless Transaction Processing.[13]
4. If the Cardholder requests to opt out of PIN entry, the transaction can be completed without PIN by completing the transaction as required by network rules.

See Figure E–3: Special Contactless Application "Pre-Selection" with Opt-out of PIN.

Note: Visa rules require the issuer BIN to be present for AIDs on U.S. Covered Visa Debit Card.

[13] Although not defined in contactless EMV, this proprietary mechanism is conceptually similar to Selectable Kernel in contact EMV. This will leave the Visa U.S. Common Debit AID as the only available AID in the terminal for that transaction.

E.3 Contact CVM Processing and Selectable Kernels Logic

Specific Cardholder Verification Method (CVM) processing may need to take place depending on transaction characteristics. Currently, there are three situations in which a special Cardholder Verification Method is necessary – if supported by the terminal:

- For terminals supporting VEPS. In this case, the terminal can offer the "no CVM" Method if the amount is less than as defined by Visa rules for VEPS.
- For terminals supporting cash-back.[14] In this case, the terminal will currently require a specific CVM – for instance Online PIN.
- For terminals supporting PIN, when the cardholder selects to opt out of PIN entry.

Normal terminal logic will indicate that certain cardholder verification methods are supported by the terminal in general, but with the selectable kernel approach, it is possible to offer only a specific Cardholder Verification Method for a specific transaction. The concept behind selectable kernel is defined in EMV and this Section will define the details necessary for VEPS and cash-back CVM processing.

Note: The selected AID can affect the ability to offer specific CVMs. Therefore, the processing described below takes place after the selected AID is known.

E.3.1 Processing

This section outlines special CVM processing used for terminals supporting cash-back or VEPS. The processing can take place as described in Figure E–4: Combined CVM Processing and Selectable Kernel or as described in Section E.3.1.1 and Section E.3.1.2 depending on terminal capabilities.

E.3.1.1 Cash-Back

The terminal will determine eligible CVMs for the current transaction. It is recommended that if a cardholder enters a PIN, and if cash-back eligibility has been determined, the cardholder then be prompted for cash-back choice. This will ensure that the cardholder can enter the necessary CVM for cash-back processing, avoiding the need to cancel cash-back processing if the cardholder is unable or not willing to enter a PIN.

For cash-back, there are two implementation scenarios: either the terminal can identify cash-back eligibility during chip processing or—before application selection—the terminal will have identified whether the cardholder requires cash-back as part of the transaction.

[14] This mechanism can also be used if for other reasons a specific CVM is required.

For the first cash-back scenario, the terminal first examines the response from the card for the selected AID:

- If the BIN in the FCI is not present or the Application Usage Controls do not allow cash-back, the terminal continues without a cash-back choice.
- If the BIN is present in the FCI, and the Application Usage Controls do allow cash-back[15], the BIN is eligible for cash-back, the terminal can offer a cash-back choice.
- If the cardholder is not presented with or does not accept a cash-back choice, the terminal continues with its standard CVM capability for the rest of the kernel processing (unless the transaction is VEPS eligible – see Appendix D: Basic EMV Terminal Logic)

Note: Following the PIN prompt with a cash-back choice may provide the simplest terminal logic.

For the second cash-back scenario, the terminal offers the cardholder a cash-back choice before the card is presented. If the choice is accepted, in commencing application selection:

- The terminal identifies debit pairs, and eliminates non-cash-back eligible AIDs (Application Usage Controls do not allow cash-back) from its candidate list.
- If there are no cash-back eligible AIDs, the terminal continues without cash-back processing.
- If there are AIDs in debit pairs which do support cash-back, and the Application Usage Controls do allow cash-back[16], the terminal continues with cash-back processing.
- If standard CVM processing does not result in the necessary CVM (online PIN) for cash-back, the terminal continues without cash-back processing.[17]

[15] Some merchants may choose to use a local file of cash-back eligible BINs; however, this must not override the AUC controls.
[16] Some merchants may choose to use a local file of cash-back eligible BINs; however, this must not override the AUC controls.
[17] Applications are typically personalized appropriately for supported functions, such as supporting online PIN if cash-back is supported. A merchant may choose to deploy selectable kernels as described in this appendix to invoke a "Cash-back/online PIN" configuration.

E.3.1.2 Visa Easy Payment Service (VEPS)

For VEPS, the terminal will have identified the amount for the transaction before application selection.

If the amount is less than or equal to the value defined by Visa rules for VEPS and otherwise qualifies for VEPS, the terminal either:

- Loads a selectable kernel configuration that only supports "no CVM" and continues with this CVM capability for the rest of the transaction

  OR

- When the CVM processed has been Signature, simply suppresses signature capture.

If the amount is greater than the value defined by Visa rules for VEPS or for other reasons the transaction does not qualify for VEPS (such as including cash-back), the terminal continues using its kernel configuration with its standard CVM capability for the rest of the transaction.

Note: The terminal must identify the AID to be selected in order to apply the correct VEPS limit to a Visa AID that begins with the Visa ISO RID as defined in Section 4.2 before processing the VEPS logic. Because other networks have different rules and transaction limits for No CVM transactions, there may be a different No CVM rule or limit for the Visa U.S. Common Debit AID or other non-Visa AIDs than the VEPS rule and limit for Visa AIDs. Accordingly, the AID to be selected has to be known before the correct rule and limit can be applied.

In addition, for AIDs supporting "no CVM" that are *not* exclusive to a single network (e.g., as is the case for Visa U.S. Common Debit AID), the terminal may need to have access to data that can determine the "no CVM" rules and limits for each network supporting the AID. Such functionality and how it is implemented is outside the scope of this guide and will be proprietary to each terminal/merchant implementation.

Figure E–4: Combined CVM Processing and Selectable Kernel