VSDC Contact & Contactless

U.S. Acquirer Implementation Guide

Version 3.0

Effective: June 2020

Visa Public

Important Information on Confidentiality and Copyright

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

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

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

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 document is designed to help acquirers prepare their device, host, and back-office infrastructure to support a VSDC contact- and/or contactless-chip program. It also provides information to assist acquirers in supporting their merchants as they migrate to chip.

It replaces the following documents:

- *VSDC and Visa payWave—U.S. Acquirer Implementation Guide*
- *VSDC ATM—U.S. Acquirer Implementation Guide*

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. Acquirers interested in offline functionality should refer to the global *VSDC Contact & Contactless Acquirer Implementation Guide*.

Note: In this document, what was formerly known as "Visa payWave" is now referred to as "contactless" or "qVSDC."

Audience

This document is intended for acquirers, acquirer processors, and merchants responsible for the implementation, testing, and activation of chip programs.

A separate guide (*VSDC Contact & Contactless Issuer Implementation Guide*) is available for issuers.

Document Purpose

This document is designed to serve as the acquirer's main handbook in implementing a chip program. It replicates high-level information from other documents, while also pointing to more detailed documents, where appropriate.

While it provides high-level information on terminals, the main resource for terminals is the *Transaction Acceptance Device Guide (TADG)*. See Section 9: References for more information.

Scope

In scope:

- Contact and contactless transactions
- POS and ATM transactions

Out of scope:

- Magnetic-stripe transactions
- Magnetic Stripe Data (MSD) contactless transactions
- Transit transactions (see Section 9.3: Visa Documents for references)
- Device-to-acquirer messaging (which is outside Visa's scope)
- Acquirer-to-VisaNet messaging (an overview of the changes is provided in Table 5–1: Chip Data Elements; see the *VSDC System Technical Manual* for details)
- Offline functionality (this document assumes that all transactions will be sent online for issuer processing)
- Detailed information on terminals and terminal-related functionality (including installing and configuring terminals, public key management, and Terminal Management Systems (TMS)) (For details on terminals, see the *TADG*)

Assumptions

This document assumes the following:

- The reader has basic knowledge of contact- and contactless-chip processing.
- The reader is familiar with VisaNet processing requirements.
- The acquirer involved in a chip program is an existing Visa acquirer. Tasks related to onboarding a new Visa acquirer are outside the scope of this document.

Key Terms

Key terms used in this document:

- **Chip** – General term for VSDC which can be used to represent contact-chip functionality, contactless-chip functionality, or both.
- **Contact** – The contact functionality of a chip terminal. Also referred to as "contact VSDC" or "contact chip."
- **Contactless** – The contactless functionality of a chip terminal. Also referred to as "contactless chip" or "qVSDC."
- **Device** – The hardware used to accept a chip card in order to conduct a transaction. Used interchangeably with the term "terminal." Also referred to as a "transaction acceptance device." In this document, this term refers to both POS devices and ATMs, unless explicitly noted otherwise.

- **qVSDC** – qVSDC is Visa's solution for contactless card acceptance. qVSDC is a minimized EMV® [1] transaction over the contactless interface where multiple EMV commands are compressed into fewer commands to streamline and expedite transaction processing. All newly issued Visa contactless cards and newly deployed contactless readers are required to support qVSDC.
- **Reader** – The component of the terminal that communicates with the card.
- **Terminal** – See the definition for "device."
- **VSDC** – See the definition for "chip."

For more information, see Appendix E: Glossary.

Device Compliance

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

- *Visa Core Rules and Visa Product and Service Rules ("Visa Rules")*
- *Payment Technology Standards Manual*
- *Transaction Acceptance Device Requirements (TADR)*

In addition to these requirements, devices need to comply with the following as applicable:

- **Contact** – Devices accepting Visa EMV-compliant contact-chip cards must comply with the *EMV Integrated Circuit Card Specifications for Payment Systems* ("*EMV Chip Specifications*")
- **Contactless** – Devices accepting Visa contactless cards must comply with one of the following:
  - *EMV Contactless Specifications for Payment Systems*, including Book C-3 ("*EMV Contactless Specifications*")
  - *Visa Contactless Payment Specification (VCPS)*
- **Payment Card Industry Security Standards Council (PCI SSC)** – Devices must comply with the following PCI SSC requirements (as applicable):
  - *PCI Data Security Standard (PCI-DSS)*
  - *Payment Application Data Security Standard (PA-DSS)*
  - *PCI PIN Security—Requirements and Testing Procedure*
  - *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*

See Section 9: References for a list of reference materials and where to obtain them.

[1] EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

Document Organization

This document contains the following sections:

About this Guide – Offers a general outline of the document, its purpose, and intended audience.

Section 1: VSDC Contact and Contactless Transaction Processing Overview – Provides high-level overviews of both contact and contactless transaction flows.

Section 2: Terminal Requirements – Provides a high-level overview of terminal requirements to support contact and contactless transactions.

Section 3: Terminal Selection and Approval – Aids merchants/acquirers in selecting their terminals and preparing them for production. It also provides an overview of the terminal approval process.

Section 4: Terminal Maintenance – Outlines merchant/acquirer requirements for maintaining their terminals and helping to address and prevent interoperability problems.

Section 5: Acquirer System Changes – Provides merchants/acquirers with information to help them update their systems to support contact and contactless transactions.

Section 6: Acquirer Host System Testing – Provides an overview of acquirer host system testing activities to support contact and contactless transactions.

Section 7: Acquirer Back-Office Changes – Addresses the technical changes to back-office functions that are required to support the acquirer's chip program.

Section 8: Merchant Support – Reviews the tasks related to supporting merchants as they make the transition to chip-card acceptance. It focuses on merchant support needs in areas such as system changes and training.

Section 9: References – Provides a reference to the documents listed throughout this document as well as other key documents.

Appendix A: Planning and Implementation – Provides acquirers with information to help them plan their chip program and includes an implementation checklist.

Appendix B: Basic EMV Terminal Logic – Outlines the basic EMV terminal logic to support Application Selection.

Appendix C: Special EMV Terminal Logic – Outlines special terminal logic to support Application Selection for the U.S. Common Debit AID.

Appendix D: Abbreviations – Provides a list of abbreviations used in this document.

Appendix E: Glossary – Provides a list of terms used in this document and their definitions.

Summary of Material Changes

The main purpose of updating this document is to:

- Create a single acquirer implementation guide that covers contact and contactless as well as all of the main acceptance environments (POS, ATM, and Unattended Cardholder Activated Terminals (UCATs)).
- Restructure it to remove duplication with other documents (mainly, the *Transaction Acceptance Device Guide (TADG)* and the *VSDC System Technical Manual*).

With the restructuring of the *VSDC Acquirer Implementation Guide* and the *Transaction Acceptance Device Guide (TADG)*, this document now focuses on acquirer activities while the *Transaction Acceptance Device Guide (TADG)* is the main handbook for terminals. Acquirers should refer to the *Transaction Acceptance Device Guide* (TADG) for information on terminals.

Appendix B: V.I.P. System Message Requirements has been deleted. This information is documented in the *VSDC System Technical Manual*. See the *VSDC System Technical Manual* for details.

In addition, a few material changes were made to this document to align it with rules and specifications:

Table 1: Summary of Material Changes

Item	Description	Section
Visa Easy Payment Service (VEPS)	VEPS is no longer applicable to the U.S. region.	References to VEPS have been removed from this document.
Signature	While the device kernel must continue to support signature to maintain processing interoperability, the merchant is no longer required to capture and verify the cardholder's signature.	Table 2–3: CVM Requirements by Terminal Type (Contact) Table 2–4: CVM Requirements by Terminal Type (Contactless)
Cardholder Device Cardholder Verification Method (CDCVM)	Contactless devices must support CDCVM.	Table 2–4: CVM Requirements by Terminal Type (Contactless)
Contactless Symbol	Contactless devices must display the EMV Contactless Symbol.	8.5: Contactless Reader Branding and Placement

1 VSDC Contact and Contactless Transaction Processing Overview

This section provides overviews of contact- and contactless-chip transactions.

1.1 VSDC Contact Transaction Processing Overview

This section provides a high-level overview of a contact-chip transaction. See *VIS* for details.

Table 1–1: VSDC Contact Transaction Processing Overview

Transaction Phase	Description
1. Initiate Transaction	The chip card is inserted into the chip-reading device or swiped through a magnetic-stripe reader. If swiped, the device checks the Service Code in the magnetic stripe to see if it is a chip card: • If the Service Code indicates that the card is not chip, the device continues to process the transaction as a magnetic-stripe transaction. • If the Service Code indicates a chip card, the device prompts the chip card to be used for the transaction.
2. Application Selection	The device determines the applications that are supported by both the card and device. The device then presents the cardholder with a list of applications to choose from or selects the application with the highest priority (as indicated on the card). Alternatively, terminals with special logic can automatically select the U.S. Common Debit AID for the transaction. See Section 2.2.2.3: Special Application Selection Logic and Appendix C: Special Terminal Logic for details. **Note:** If either there are no applications in common or if there are one or more applications in common but they require cardholder confirmation and the device does not support cardholder confirmation, the transaction is terminated.
3. Initiate Application Processing	The card sends the Application Interchange Profile (AIP) (a list of the functions the card supports) and the Application File Locator (AFL) (a list of the records the device obtains from the card) to the terminal. The card may send a different AIP or AFL based upon the transaction environment. For example, the card might send a different AIP and AFL for domestic versus international transactions. The device reads the card data designated in the AFL and determines the data to be used during Offline Data Authentication (if supported). **Note:** Offline Data Authentication is not applicable to ATMs or other online-only devices.

Transaction Phase	Description
4. Offline Risk Management	If supported by both the card and the device, offline transaction checks are performed. The results of these checks will later be used in the decision of whether the transaction should be processed online or offline. The offline processing checks may be performed in any order. Offline Data Authentication is also performed usually via Dynamic Data Authentication (DDA) although Combined DDA/Application Cryptogram Generation (CDA) may be supported. At the conclusion of offline risk management, the device records the results in the Terminal Verification Results (TVR) field. **Note:** If Offline Data Authentication is not performed, the transaction must be processed online.
5. Processing Restrictions	The device performs the following checks: • **Effective/Expiration Date Checking** – Checks to see if the current date is within the effective and expiration dates of the card, as applicable. • **Application Usage Control Checking** – Determines if the card can be used in the environment (e.g., domestic/international, for ATM transactions, etc.) • **Application Version Number Checking** – Checks the version of the card against the version of the device to see if the two match.
6. Cardholder Verification	The device reads the Cardholder Verification Method (CVM) List on the card to determine the CVM to use for the transaction. The cardholder is then verified by the card, merchant, or issuer depending on the CVM. Possible CVMs include: • Online PIN (the only CVM applicable to ATMs) • Offline Plaintext PIN • Offline Enciphered PIN • Signature • No CVM required If Offline Plaintext PIN is used, the device passes the PIN to the card in the clear. If Offline Enciphered PIN is used, the device uses public key technology to encrypt the PIN prior to sending it to the card. The card then decrypts the PIN prior to performing the validation. For ATM transactions, the only CVM used is Online PIN. No other CVM may be used. As long as the card can be used at an ATM, the ATM is allowed to prompt for Online PIN, even if the card's CVM List does not include Online PIN. Online PIN entry and processing are not defined by the *EMV Chip Specifications* and may occur at any point in the flow prior to Online Processing.

Transaction Phase	Description
7. Terminal Risk Management	The device performs checks based on the risk control features in place. The results feed into Terminal Action Analysis, which determines whether the device will approve offline, send online, or decline offline. These checks may include: • Floor limit check (mandatory for offline-capable devices) • Exception file check (if supported by the device) • Offline transaction limit check (if card is personalized to provide the associated data for this check to the device) • Random selection (mandatory for offline-capable devices) For online-only terminals, including ATMs, Terminal Risk Management is not required as all transactions will be sent online.
8. Terminal Action Analysis	The device applies the rules set by the issuer in the card (Issuer Action Codes – IACs) and the payment system in the device (Terminal Action Codes – TACs) to the results of offline processing. Based on the results, the device requests the card to generate one of the following Application Cryptograms: • Approve offline – Transaction Certificate (TC) • Send online – Authorization Request Cryptogram (ARQC) • Decline offline – Application Authentication Cryptogram (AAC)
9. Card Risk Management	The card may perform the following checks on behalf of the issuer to see if it agrees with the device's request to approve offline, send online, or decline offline: • Previous Transaction Checks • New Card Checks • Velocity Checks After the card has completed the risk management checks, it decides whether to approve offline, send online, or decline offline based on the type of cryptogram requested by the device and the results of Card Risk Management. It responds to the device's request for an Application Cryptogram with one of the following: • Approve offline – TC • Send online – ARQC • Decline offline – AAC **Note:** The card can only agree with the device's decision or make a more restrictive decision (e.g., if the device determines that the transaction should be processed online, the card can only conclude that the transaction must go online or be declined offline; it cannot approve offline).

Transaction Phase	Description
10. Online Processing	If requested, the device will attempt to send the transaction online. To support Online Card Authentication, the device sends the ARQC and the original data elements used by the chip to generate the cryptogram online to the acquirer. The acquirer sends the authorization message to VisaNet with the cryptogram and its associated data elements.
11. 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 Option issuer (e.g., Field 55 acquirer to third bit map issuer), VisaNet converts the authorization to the issuer's message format. • VisaNet may perform Online Card Authentication on the issuer's behalf. • VisaNet may process the transaction on the issuer's behalf in Stand-in, if the issuer is not available. VisaNet forwards the transaction to the issuer for processing (assuming the issuer is available).
12. Issuer Receives and Processes the Authorization Request	The issuer processes the authorization response to determine if the transaction should be approved or declined. In addition, the issuer may: • Perform Online Card Authentication to validate the card. • Generate the Authorization Response Cryptogram (ARPC) to send to the card in the response (to support Online Issuer Authentication). • Prepare Issuer Scripts (or Card Status Updates) to send to the card in the response. The issuer then sends the transaction response to VisaNet to transmit to the acquirer.
13. VisaNet Processes Issuer Response	If the message format of the Full Data Option issuer is different from the message format of the acquirer (e.g., Field 55 issuer to expanded third bit map acquirer), VisaNet converts the authorization response to the acquirer's message format. If the issuer is participating in the Visa Chip Authenticate service, VisaNet generates an ARPC and includes it in the authorization response for Online Issuer Authentication.
14. Acquirer and Device Process the Issuer Response	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. • Card authenticates and executes Issuer Script/Card Status Updates, 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 from the terminal. For approved ATM transactions, the ATM will dispense cash.

Transaction Phase	Description
15. Clearing and Settlement	The acquirer submits the approved transaction to VisaNet for clearing and settlement. It typically contains the chip data in TCR 5 and TCR 7. **Note:** TCR 7 is not required for transactions acquired in some online-only markets, such as the U.S. The details of offline declines are only sent to the issuer if the issuer and acquirer support Informational Advices (which are not recommended).

1.2 VSDC Contactless Transaction Processing Overview

This section provides a high-level overview of a contactless-chip transaction focusing on qVSDC. See *VCPS* for details.

Table 1–2: VSDC Contactless Transaction Processing Overview

Transaction Phase	Description
1. Processing Prior to Enabling the Contactless Interface	To minimize the duration in which the card must remain within the reader Radio Frequency (RF) field, the reader may obtain the transaction amount and perform some risk management checks prior to prompting for card presentment.
2. Discovery Processing	Discovery Processing is performed by the reader to poll for the presence of contactless cards that may have entered the reader's RF field.
3. Application Selection	Application Selection is performed immediately after activation of the contactless card and is the process of determining which of the applications that are supported by both the card and reader will be used to conduct the transaction. This process is performed in two steps: • The reader builds a candidate list of mutually supported applications. This process is modeled after the EMV Directory Selection Method, except that support for the Directory Selection Method is mandatory for readers (and cards), and the Proximity Payment System Environment (PPSE) is used in place of the Payment System Environment (PSE). • A single application from the candidate list is identified and selected to process the transaction. Alternatively, terminals with special logic can automatically select the U.S. Common Debit AID for the transaction. See Section 2.2.2.3: Special Application Selection Logic and Appendix C: Special Terminal Logic for details. The response message from the card includes the Processing Options Data Object List (PDOL) to identify the reader data needed to perform Initiate Application Processing.

Transaction Phase	Description
4. Initiate Application Processing	During Initiate Application Processing, the reader signals to the card that transaction processing is beginning by sending the GET PROCESSING OPTIONS command to the card. When issuing this command, the reader supplies the card with any data elements requested by the card in the PDOL. Initiate Application Processing is where the card performs Card Action Analysis, generates the Application Cryptogram, generates the signature for Offline Data Authentication (conditional), and returns card application data.
5. Read Application Data (Conditional)	Read Application Data is performed if the Application File Locator was returned by the card during Initiate Application Processing. During Read Application Data, the reader reads the records necessary to process the transaction. **Note:** In a contactless transaction, the card may return application data during Initiate Application Processing and Read Application Data.
6. Card Read Complete	During Card Read Complete, the reader indicates to the cardholder that the exchange of data between the reader and the card is complete, and the card may be removed from the reader field. The reader determines whether all mandatory data elements for the transaction were returned by the card and terminates the transaction if not.
7. Processing Restrictions (Conditional)	Processing Restrictions is implemented for readers supporting any of the Processing Restrictions checks. During Processing Restrictions, the reader checks the application expiration date, Application Usage Controls, and may check whether the card application is on the Terminal Exception File.
8. Offline Data Authentication (Conditional)	Readers supporting offline transactions validate the card using Fast Dynamic Data Authentication (fDDA) (a faster version of DDA that is suitable to the requirements of a contactless transaction). During fDDA, the device validates a cryptographic value generated by the card during the transaction. This validation ensures that the card data has not been copied (skimmed) and that the card is not counterfeit.
9. Cardholder Verification (Conditional)	During Cardholder Verification, the reader determines the Cardholder Verification Method (CVM) to be performed (if any). The CVM options for contactless transactions are Online PIN, signature, or Cardholder Device CVM (CDCVM).
10. Online Processing (Conditional)	When online processing is required for the transaction, the reader sends an online authorization request to the issuer host. Online Processing allows the issuer host to review and authorize or decline transactions using the issuer's host-based risk management parameters. In addition to performing traditional online fraud and credit checks, host authorization systems can perform Online Card Authentication using the card-generated cryptogram.
11. Completion	Completion is performed by the reader to conclude transaction processing. The reader indicates to the cardholder the outcome of the transaction.

2 Terminal Requirements

This section provides a high-level overview of terminal requirements to support contact- and contactless-chip transactions. It includes the following sections:

- **General Requirements** – Requirements for all terminals.
- **Contact-Chip Requirements** – Requirements for contact terminals.
- **Contactless-Chip Requirements** – Requirements for contactless terminals.

This section provides an overview. For details, see the following documents:

- *EMV Chip Specifications*
- *VCPS*
- *Transaction Acceptance Device Guide (TADG)*

2.1 General Requirements

This section outlines the general requirements that apply to any contact- and/or contactless-chip terminal.

2.1.1 Magnetic-Stripe Reader

The magnetic-stripe reader of the chip terminal needs to be able to:

- Accept magnetic stripes containing chip Service Codes (2xx and 6xx).
- Attempt to prevent fallback transactions. When the magnetic-stripe reader reads a card with a chip Service Code (**2xx** or **6xx**), the terminal must not process the transaction. Instead, it must display a message that the card should be read using the contact chip. This check helps to prevent chip cards from being processed as magnetic stripe. For more information on fallback, see Section 5.7: Fallback Transactions.

2.1.2 19-Digit Account Numbers

All chip devices (POS and ATM) that accept Visa, Visa Electron, Plus, and/or V PAY cards must support variable-length PANs up to and including 19 digits:

- The device/ATM 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 device should indicate that the card type is not supported and end the transaction. Support for 19-digit PANs is strongly recommended.

2.1.3 Language

Terminal messages can be displayed to the cardholder in their preferred language. Acquirers need to:

- Decide if they will offer messages in one language or multiple languages and, for multiple languages, which languages they will support.
- For multiple languages, work with their terminal vendor to decide how to offer language selection to their cardholders (e.g., using EMV functionality or through another means).

For most implementations, EMV functionality to support language selection does not offer a significant advantage over menu-based language selection unless the terminal supports a very large number of languages. If the acquirer's terminals already support multiple languages, the current functionality may be sufficient.

2.1.4 Application Identifiers (AIDs)

Acquirers must ensure that the appropriate AIDs are loaded into their terminals. The AIDs are listed in the following table.

Table 2–1: Application Identifiers (AIDs)

Application	RID + PIX
Visa (e.g., Visa Credit or Visa Debit)	A000000003 1010
Visa Electron	A000000003 2010
Visa Interlink	A000000003 3010
Plus	A000000003 8010
Visa U.S. Common Debit (U.S.)	A000000098 0840

2.1.4.1 Application Identifier (AID) Requirements

This section describes the AID requirements by device type:

Table 2–2: Application Identifier (AID) Requirements

Device Type	AID Requirements
POS Devices	POS devices must contain the Visa AID and Visa Electron AID. **Note:** All devices that accept the Visa AID must accept the Visa Electron AID. In countries where Visa Electron is not issued, Visa Electron cards are accepted and processed as Visa cards but the Visa Electron AID must still be present in the device to enable this.
	All POS terminals accepting Visa Interlink must support the Visa AID, Visa Interlink AID, and the Visa U.S. Common Debit AID. **Note:** Visa Interlink can only be accepted at POS devices capable of processing online transactions with Online PIN verification.
ATMs	ATMs must contain the Visa AID, Visa Electron AID, *and* the Plus AID. **Note:** ATMs that accept Plus chip cards but not Visa or Visa Electron chip cards must still support all three AIDs to ensure acceptance of Visa or Visa Electron cards that are registered with the Plus network but do not contain the Plus AID. Similarly, non-Visa Plus cards will only contain the Plus AID.

2.1.4.2 Application Identifier (AID) Support for Partial Name Selection

Visa AIDs must be configured in the terminal to support Partial Name Selection (where the terminal does not have to match on the entire AID in order select the application).

2.2 Contact-Chip Requirements

The section outlines terminal requirements for the acceptance of contact-chip cards.

Requirements for the acceptance of contactless-chip cards are outlined in Section 2.3: Contactless-Chip Requirements.

2.2.1 Application Selection Methods

Per the *EMV Chip Specifications*, there are two methods for performing Application Selection:

- List of AIDs Method (mandatory)
- Directory Selection Method (optional)

Merchants/acquirers need to determine if they will support the Directory Selection Method in addition to the mandatory List of AIDs Method in their terminals. They should work with their terminal vendor on this decision. There is a not a compelling benefit to support the Directory Selection Method unless the market supports a large number of AIDs.

Note: If the merchant/acquirer decides to support the Directory Selection method, it will only be invoked for cards that also support it; otherwise, the List of AIDs Method will be used.

2.2.2 Application Selection Processing (Contact)

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

- **Automatic Selection** – When there is only one application in common between the card and terminal, that application is automatically selected for the transaction.
- **Cardholder Selection** – When the card and terminal have multiple applications in common, the cardholder is prompted to select one of the mutually supported applications.
- **Priority Selection** – When the card and terminal have multiple applications in common, the highest priority application (as assigned by the issuer) is selected to initiate the transaction.
- **Special Application Selection Logic** – When the card and terminal contain the Visa U.S. Common Debit AID and the terminal supports special Application Selection logic (required for routing flexibility), it may result in the Visa U.S. Common Debit AID being selected for the transaction. This AID can then be used for routing to the acquirer's preferred issuer-enabled debit network (which may be a Visa-affiliated network or another debit network) and steer cardholder verification toward Online PIN (as long as the cardholder is provided with an option to opt out of PIN).

[2] The first three processes—Automatic Selection, Cardholder Selection, and Priority Selection—are referred to as "basic EMV Application Selection" in this document.

Each of these processes is described in the following sections.

Note: If the chip card and terminal have no applications in common, 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" (chip capable).

2.2.2.1 Cardholder Selection

Cardholder Selection as defined within the *EMV Chip Specifications*:

- The terminal displays a list of all the commonly supported applications[3] to the cardholder in the priority sequence specified by the issuer, or
- The 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 Preferred Name (if personalized on the card and the character set is supported by the terminal) or the Application Label, but the merchant can override or enhance that descriptor, provided the descriptor is transparent to the consumer (this is referred to as an "enhanced descriptor"). For convenience, this document will sometimes refer to displaying the "applications" to the cardholder, which should be understood as displaying the Application Preferred Name, Application Label, or an enhanced descriptor.

The application selected is used to initiate the transaction.

2.2.2.2 Priority Selection

Priority Selection allows the terminal to select the highest priority application supported by both the card and terminal as personalized in the Application Priority Indicator on the card. Priority Selection applies when the card and terminal have more than one application in common, but the terminal does **not** support:

- Cardholder selection (see previous section)
- Specific Application Selection logic (see next section)

This approach may be appropriate where the terminal does not have any means for the cardholder to indicate selection, such as an unattended parking kiosk.

[3] 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. For more information on cardholder confirmation, see the *TADG*.

2.2.2.3 Special Application Selection Logic

Terminals that support the Visa U.S. Common Debit AID may be customized to support special Application Selection logic which allows flexible routing options:

- Terminals with this special logic will identify that the card contains a "debit pair" (i.e., the Visa ISO AID[4] and the Visa U.S. Common Debit AID where the two AIDs are associated with the same funding source) and then eliminate the Visa ISO AID of the debit pair from the Candidate List. If the card supports multiple funding options (e.g., credit and debit applications on the same plastic), only the Visa ISO AID from the debit pair may be eliminated.
- Once the Visa ISO AID has been eliminated from the Candidate List, the terminal can select the Visa U.S. Common Debit AID for the transaction, or in the case of multiple funding options, provide cardholder choice between credit and debit.
- Once the Visa U.S. Common Debit AID has been selected, Online PIN will be prompted (although the cardholder must be provided with an option to opt out of PIN). This allows for flexible routing options.

Acquirers interested in this processing need to work with their terminal vendor to implement support for special Application Selection logic.

Important: Acquirers need to be aware that when a Visa ISO AID is selected for the transaction, the transaction must be routed to a Visa-affiliated network. See Section 5.1: Transaction Routing for details.

Important: Devices with special Application Selection logic must allow for basic Application Selection processing when the card does not contain the Visa U.S. Common Debit AID. See Section 2.2.2: Application Selection Processing (Contact) for details.

Note: During Application Selection, it is important to communicate the selected application to the cardholder so that the cardholder understands which account is being used for multi-account (credit/debit) cards.

Note: 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 its own routing options.

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).

[4] An AID that starts with the Visa ISO Registered Application Identifier (RID) 'A0 00 00 00 03'.

For more information:

- **Special Application Selection Logic** – For details on how to set up the terminal to support this special processing, see Appendix C: Special Terminal Logic.
- **Routing** – For details on how to use the Visa U.S. Common Debit AID for routing purposes, see Section 5.1: Transaction Routing.
- **Preferred CVM Processing** – For details on how to promote Online PIN, see Section 2.2.3.1: Preferred CVM Processing.

2.2.2.4 Summary for U.S. Common Debit AID

Because some cards may support more than one source of funds (e.g., credit and debit), cardholder selection allows the cardholder to select the appropriate funding source. For U.S. Covered Visa Debit Cards (i.e., not a card with multiple funding sources), Special Terminal Logic can be used to remove one AID of a debit pair from the Candidate List as described in Appendix C: Special Terminal Logic (e.g., for U.S. Covered Visa Debit Cards, merchants can remove the Visa ISO 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 a Visa ISO AID. Merchants are not required to use a Visa ISO AID and may perform 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").

2.2.3 Cardholder Verification (Contact)

This section outlines the terminal requirements for cardholder verification processing.

Cardholder verification is used to help 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 (e.g., 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. If the highest priority CVM is not applicable to this transaction, the next CVM is checked. This is done until an applicable CVM is found or the end of the CVM List is reached.

The following general guidelines are provided to assist acquirers in determining the CVMs to support at their terminals:

Key to the Table:

- M = Mandatory
- O = Optional
- – = Not Applicable

Table 2–3: CVM Requirements by Terminal Type (Contact)

Cardholder Verification Method (CVM)	Attended POS	UCAT	ATM
Signature	M (While the device kernel must support signature, the merchant is no longer required to capture and verify the cardholder's signature)	–	–
Online PIN	O (Mandatory if terminal supports Interlink)	O (Mandatory if terminal supports Interlink)	M (ATMs may prompt for Online PIN even if CVM List does not contain it)
Offline Plaintext PIN[5]	O	O	–
Offline Enciphered PIN[5]	O	O	–
No CVM Required	O (Recommended)	M	–

Offline PIN is not applicable to the U.S. market but it is included in the table for completeness.

[5] If device supports Offline Enciphered PIN, it must support Offline Plaintext PIN. In some markets, however, if the device supports Offline PIN, it must support both Offline Plaintext PIN and Offline Enciphered PIN. Check with your Visa representative for the requirements in your market.

Important: Devices that support PIN must comply with Visa and PCI SSC requirements. See the following for more information:

- *Payment Technology Standards Manual*
- PCI SSC documents (see Section 9: References for a list of PCI documents)

2.2.3.1 Preferred CVM Processing

Once a terminal supporting the Visa U.S. Common Debit AID has selected that AID for the transaction (see Section 2.2.2.3: Special Application Selection Logic for details), the terminal can steer the cardholder towards Online PIN as long as the terminal provides a mechanism to allow the cardholder to opt-out of Online PIN (and be validated via signature or "no CVM").

Recommended PIN opt-out options include:

- 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/labels (similar to pre-EMV environment):
  - "Credit" button/label is used to indicate cardholder preference to opt-out of entering a PIN.
  - "Debit" button/label is used to indicate cardholder preference to enter a PIN.

Regardless of the CVM, merchants may use the Visa U.S. Common Debit AID to route to their preferred issuer-enabled debit network. This is true for any CVM, including PIN, signature, and "no CVM."

2.2.4 Offline Data Authentication

Since the U.S. is a zero-floor limit market and all transactions will be sent online to the issuer for processing, terminals should not support Offline Data Authentication.

2.2.5 Terminal Risk Management

EMV Terminal Risk Management consists of a series of checks to protect the acquirer, issuer, and system from potential fraud and triggers the transaction to be sent online or declined offline. Offline-capable terminals must support Terminal Risk Management; Terminal Risk Management is not required in zero-floor limit POS environments or ATMs.

Since the U.S. is a zero-floor limit market and all transactions will be sent online to the issuer for processing, terminals do not need to support Terminal Risk Management.

2.2.6 Terminal Action Codes (TACs)

Terminal Action Analysis is the phase of the transaction where the terminal decides whether the transaction will be approved offline (not applicable to zero-floor limit environments), sent online, or declined offline—and what processing should take place if the decision is to send the transaction online but online processing is not available. The terminal uses data elements loaded into the terminal called Terminal Action Codes (TACs) and data elements personalized on the card called Issuer Action Codes (IACs) to support this process.

Terminals must be loaded with the Visa mandated TAC settings. For the TAC values, see the *TADG*.

Note: U.S. devices containing the Visa U.S. Common Debit AID must be loaded with the TACs for the Visa U.S. Common Debit AID and the TACs for the Visa ISO AIDs. See the *TADG* for details.

2.3 Contactless-Chip Requirements

This section outlines terminal requirements for the acceptance of contactless-chip cards focusing on qVSDC.

Requirements for the acceptance of contact-chip cards are outlined in Section 2.2: Contact-Chip Requirements.

qVSDC is Visa's solution for contactless card acceptance. qVSDC is a minimized EMV contact-chip transaction over the contactless interface where multiple EMV commands are compressed into as few commands as possible to streamline and expedite transaction processing. All newly issued Visa contactless cards and newly deployed contactless readers are required to support qVSDC.

Streamlined qVSDC is a simplified, online-only version of qVSDC which eliminates some of the internal card decision making steps. From the perspective of the device, however, a streamlined qVSDC transaction is similar to regular qVSDC, and there are no additional requirements.

2.3.1 Transaction Speed

Contactless transactions are designed to be fast. Interaction between the card and the reader 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.

2.3.2 Application Selection Processing (Contactless)

For most contactless transactions, due to the minimal interaction between the contactless terminal and the card/consumer device, the reader will automatically select the highest priority AID on the card/consumer device.

Merchants that wish to implement routing flexibility will need to deploy specific logic in their terminals to ensure that the appropriate application is selected. Contactless transactions can ultimately be routed using the Visa U.S. Common Debit AID to the same extent as transactions initiated using other methods, but special Application Selection logic will be required and this special logic needs to take place before the basic contactless Application Selection process begins.
See Appendix C: Special Terminal Logic for more information.

When the Visa U.S. Common Debit AID has been selected for the transaction, it may be used to route the transaction to the acquirer/merchant's preferred issuer-enabled debit network (which may be a Visa-affiliated network or another debit network).

Readers supporting flexible routing options need the special logic outlined in Appendix C. 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 cardholder means for opting out of Online PIN if Online PIN is automatically prompted.

2.3.3 Terminal Transaction Qualifiers (TTQ)

The reader must contain the Terminal Transaction Qualifiers (TTQ) data element. The reader provides the TTQ 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.

The TTQ advises the contactless card of the reader's requirements and capabilities for processing the specific transaction. This includes, but is not limited to:

- Whether cardholder verification is required for the transaction (based on the results of preliminary processing)
- What CVMs are supported (the reader must indicate support for Consumer Device CVM (CDCVM))
- Whether the reader requires online processing

2.3.4 Reader Contactless Floor Limit

The reader may contain a Reader Contactless Floor Limit. Contactless transactions above this limit require online authorization. For online-only countries, this limit is set to zero or is not supported by the reader.

For the U.S. region, this limit must be set to zero to ensure all transactions are authorized online by the issuer.

2.3.5 Reader Cardholder Verification Method (CVM) Required Limit

The reader may contain a Reader CVM Required Limit. Contactless transactions above this limit require cardholder verification. This limit is set based on business needs.

2.3.6 Fast Dynamic Data Authentication (fDDA)

fDDA is a form of Offline Data Authentication that is similar to DDA but performed on contactless transactions. fDDA is required for:

- Readers supporting offline contactless transactions.
- Environments, such as transit, where the card needs to be authenticated before the transaction is authorized online.

Otherwise, the reader should not support fDDA.

2.3.7 Cardholder Verification (Contactless)

This section outlines the contactless terminal requirements for cardholder verification processing.

Key to the Table:
- M = Mandatory
- O = Optional
- – = Not Applicable

Table 2–4: CVM Requirements by Terminal Type (Contactless)

Cardholder Verification Method (CVM	Attended POS	UCAT	ATM
Signature	M (While the device kernel must support signature, the merchant is no longer required to capture and verify the cardholder's signature)	–	M (While contactless ATMs must indicate support for signature, only Online PIN will apply to transactions)
Online PIN	O (Mandatory if terminal supports Interlink)	O (Mandatory if terminal supports Interlink)	M (ATMs may prompt for Online PIN regardless of CVM processing)
CDCVM	M	M	M (While contactless ATMs must indicate support for CDCVM, only Online PIN will apply to transactions)
Contact Chip with Offline PIN	O	O	– (Should not be supported at ATMs because it may cause unnecessary switch interface scenarios)

Additional information about contactless CVM processing:

- **"Contact Chip with Offline PIN"** – The terminal can be set to support "Contact Chip with Offline PIN." If this is a matching CVM, the interface will be switched to contact chip.
- **Contactless CVM Processing** – If the transaction requires a CVM, the card compares its supported CVMs to the ones supported by the device and the highest priority CVM supported between the two will be used for the transaction.
  - For cards compliant to VCPS 2.2.0 or earlier, Online PIN is always the highest priority CVM, followed by Contact Chip with Offline PIN, and then signature.
  - For cards compliant to VCPS 2.2.1 or later, the CVM hierarchy is configurable.
- **No CVM** – "No CVM Required" is not a CVM that is personalized on a contactless card but a contactless transaction may result in no CVM when neither the card nor device requires a CVM for the transaction (e.g., transaction is below the Reader CVM Required Limit).
- **Online PIN** – Dual-interface terminals that support Online PIN for contact chip should also support Online PIN for contactless transactions.
- **CDCVM** – CDCVM is performed by the cardholder's consumer device (e.g., mobile phone) and does not involve the terminal. It is generally the only CVM supported on a consumer device.

3 Terminal Selection and Approval

This section aids merchants/acquirers in selecting their terminals and preparing them for production. It also provides an overview of the terminal approval process. It includes the following sections:

- **Terminal Selection** – Information to assist merchants/acquirers in selecting their terminals.
- **Terminal Approval** – An overview of the EMV and Visa process for terminal approval.
- **Level 3 Testing** – Self-testing to help ensure terminals are ready for production.
- **Terminal Checklist** – A checklist for merchants/acquirers to help them ensure their terminals are ready for deployment.

3.1 Terminal Selection

Acquirers need to work with their merchants and/or staff to select the best terminals for their environments (POS, UCAT, and ATM). As part of these efforts, they should meet with a variety of vendors to review and compare available products.

Important: Since development of a new terminal is a lengthy process, it is recommended that acquirers select a product that has already been developed and approved. A list of EMVCo-approved (contact and contactless) and Visa-approved (contactless) products and vendors is available at www.emvco.com and www.technologypartner.visa.com, respectively.

3.1.1 Online-Only vs. Offline/Online

For POS terminals, acquirers need to determine whether their terminals need to support offline transactions or if all transactions will be sent online for issuer processing:[6]

- **Online-Only Terminals** – These terminals always send the transaction online for authorization; they cannot approve transactions offline. These terminals are appropriate for zero-floor limit environments.
- **Offline/Online Terminals** – These terminals are capable of processing both offline and online transactions.

Since the U.S. region is a zero-floor limit environment, this section focuses on the requirements for online-only terminals. Acquirers in the U.S. region considering offline options should review the global *VSDC Contact & Contactless Acquirer Implementation Guide* for the requirements for offline-capable terminals.

[6] Since ATMs are online-only devices, this is not a consideration for ATMs.

Note: Offline PIN processing may take place at either online-only terminals or offline/online terminals (e.g., Offline PIN can be used to validate the cardholder at an online-only terminal).

3.1.2 Terminal Types

Acquirers need to select the terminal type and functionality that meets their and/or their merchant's business needs:

Table 3–1: Terminal Types/Functionality

Terminal Type	Description
Attended POS	There are a wide variety of attended POS terminals available in the industry. They range from simple stand-alone devices to integrated devices that are part of a merchant's cash register. More sophisticated models support functions such as product scanning, product lookup, inventory management, and accounting. There are also multilane POS systems such as for large mass merchandise stores and grocery stores that are tied to one or more controllers.
Unattended Cardholder Activated Terminals (UCATs)	UCATs are acceptance devices that dispense goods or services, at which the card and cardholder are present, but the functions and services are provided without the assistance of an attendant to complete the transaction. These devices include Automated Fuel Dispensers (AFDs), self-service vending units, and self-service payment devices in parking garages or at parking meters. **Note:** UCATs and ATMs have separate rules. UCATs can also be used to dispense cash but when dispensing cash they are operating as an ATM and must follow all ATM rules.
Automated Teller Machines (ATMs)	ATMs are online-only, unattended devices that dispense cash and accept Online PINs. These devices may be simple, limited-capability cash dispensers or advanced-function ATMs with sophisticated applications and a range of business functions. Acquirers should evaluate whether they need to replace ATMs as the migrate to chip or if existing ATMs can be upgraded with chip functionality.
Contactless Functionality	Contactless functionality can be added to any of the above terminal types to give cardholders a faster payment option. Usually, the contactless functionality is built into the overall device. Some environments, however, may use a separate device referred to as a dongle or Proximity Coupling Device (PCD) that interfaces with the acceptance device to perform the contactless transaction.

3.2 Terminal Approval

Acquirers must select terminals that have been tested and approved by EMVCo (contact terminals) and tested and approved by EMVCo or Visa (contactless terminals).

Note: Contactless terminals may be developed to either the *EMV Contactless Specifications,* Book C-3 or *VCPS*:

- When the contactless terminal is developed to the *EMV Contactless Specifications*, Book C-3, it is tested and approved by EMVCo.
- When the contactless terminal is developed to *VCPS*, it is tested and approved by Visa.

Approved contact devices are listed on the EMVCo website at www.emvco.com.

Approved contactless devices are listed on the EMVCo website at www.emvco.com and on the Visa website at www.technologypartner.visa.com.

3.3 Level 3 Testing

Once the device has been approved (see the above section for details) and after it has been configured for deployment, it must be tested with the appropriate Level 3 testing tool(s) (currently, the Acquirer Device Validation Toolkit (ADVT) (for contact devices) and/or the Contactless Device Evaluation Toolkit (CDET) (for contactless devices)).

See the following documents for U.S. testing requirements:

- *U.S. EMV Terminal Testing Requirements*
- *Visa U.S. Quick Chip and Minimum Terminal Configuration ADVT 7/CDET 2.3 Use Cases*
- *U.S. Visa Contactless Transit Terminal Testing*

3.3.1 Visa Chip Vendor Enabled Service (CVES)

The Visa Chip Vendor Enabled Service (CVES) is a global service that supports acquirers in their Level 3 testing efforts. Through this program, acquirers have the option of engaging third-party chip tool vendors to execute Level 3 testing on their behalf. Acquirers can obtain a list of participating vendors on Visa Online (VOL) and the Visa Technology Partner website at www.technologypartner.visa.com.

Note: Vendors choosing to participate in CVES must complete a confirmation process to verify that they can effectively deliver the required services. Interested vendors should contact Visa for more information.

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

The Visa U.S. Chip Acquirer Self-Accreditation Program enables U.S. acquirers to self-certify their point-of-sale (POS) devices. The self-accreditation program for U.S. acquirers eliminates the need to use the Chip Compliance Reporting Tool (CCRT) to report ADVT and CDET terminal test results when they deploy chip POS solutions. The program streamlines acquirers' Level 3 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.

3.4 Terminal Checklist

The following table provides a checklist that acquirers can use to ensure their terminals are ready for deployment. For many of the items, see the *TADG* (the *TADG* is the main resource for information on terminals outside of the *EMV Chip Specifications* and *VCPS*).

Note: The information in this checklist is not meant to be an exhaustive list; it is intended to provide guidelines to assist merchants/acquirers.

Note: This checklist focuses on terminals. For a general checklist, see Table A–1: Implementation Checklist.

Table 3–2: Terminal Checklist

Item	Description	References
AIDs	Ensure terminals have been loaded with the appropriate AIDs.	2.1.4: Application Identifiers (AIDs)
Application Version Number	Ensure terminals have been loaded with the applicable Application Version Number. It is recommended that the device Application Version Number match the most current VIS-specified card Application Version Number at the time the device received its EMVCo approval: • VIS Version 1.6 (binary '00A0' which represents the decimal value of 160) • VIS Version 1.5 (binary '0096' which represents the decimal value of 150)	*TADG*

Item	Description	References
Cardholder Verification	Determine which CVMs to support: • Contact: Signature,[7] Offline Plaintext PIN, Offline Enciphered PIN, Online PIN, No CVM. • Contactless: Signature,[7] Online PIN, CDCVM.	2.2.3: Cardholder Verification (Contact) 2.3.7: Cardholder Verification (Contactless)
Contactless Limits	Set up contactless devices with the following limits (as applicable): • Reader Contactless Floor Limit • Reader Contactless CVM Required Limit **Note:** There is also a Reader Contactless Transaction Limit in the contactless device. Transactions for amounts above this limit are terminated and may only be processed using a different interface. All contactless readers should have this limit disabled or set to its maximum value.	2.3.4: Reader Contactless Floor Limit 2.3.5: Reader Cardholder Verification Method (CVM) Required Limit
Country Codes and Currency Codes	Set up terminals with the appropriate country code and currency code(s).	*EMV Chip Specifications*
DES Key Management	Ensure devices that support Online PIN or that use DES encryption to transport an Offline Plaintext PIN from the PIN pad to the card reader support DES key management. **Note:** PIN confidentiality depends on the implementation of adequate PIN security standards. To this end, ANSI, ISO, and Visa require the TDES algorithm using at least double-length keys.	*TADG* *Payment Technology Standards Manual*
Fallback	Ensure terminals properly perform fallback.	5.7: Fallback Transactions
Language(s)	Ensure terminals are able to display messages in supported languages.	2.1.3: Language
Level 3 Testing	Complete Level 3 terminal testing prior to deployment.	3.3: Level 3 Testing
Offline Data Authentication	Ensure offline-capable terminals support DDA (contact terminals) and fDDA (contactless terminals). fDDA is also required for transit terminals.	2.2.4: Offline Data Authentication 2.3.6: Fast Dynamic Data Authentication (fDDA)

[7] While the device kernel must support signature, the merchant is no longer required to capture and verify the cardholder's signature.

Item	Description	References
Payment Card Industry Security Standards Council (PCI SSC) Compliance	Ensure terminals are PCI SSC compliant.	*TADG*
Service Codes	Ensure the magnetic-stripe portion of terminals are able to read the chip-related Service Codes and prompt for chip cards to be read via the chip.	2.1.1: Magnetic-Stripe Reader *TADG*
Special Processing	Consider whether terminals need to support proprietary functionality (as applicable) such as domestic debit programs.	2.2.2.3: Special Application Selection Logic 2.3.2: Application Selection Processing (Contactless) Appendix C: Special Terminal Logic
Terminal Action Codes (TACs)	Ensure terminals have been loaded with the appropriate TAC values.	2.2.6: Terminal Action Codes (TACs) *TADG*
Terminal Capabilities	Set up terminals with the Terminal Capabilities data element.	*EMV Chip Specifications*
Terminal Compliance	Ensure terminals are compliant and have undergone the appropriate testing.	3.2: Terminal Approval *TADG*
Terminal Configuration	Ensure terminals only use the features which EMVCo approved for the kernel. Do not use features that have not been approved.	*TADG*
Terminal Exception File	Determine requirements for a terminal exception file, as applicable.	*TADG*
Terminal Management System (TMS)	Evaluate whether existing TMS can be updated for chip or if a new TMS needs to be procured/developed. Enhance TMS, as applicable.	*TADG*
Terminal Risk Management	Ensure offline-capable terminals support Terminal Risk Management (e.g., floor limits and random transaction selection).	*TADG*
Transaction Types	Ensure terminals support applicable transaction types. For example: • POS: Pre-authorizations, Incremental Authorizations, Referrals, Reversals, and Refunds. • ATM: Cash disbursements, Balance Inquiries, Account Transfers, and Deposits.	*TADG*

Item	Description	References
VSDC CA Public Keys and Public Key Management	Load the VSDC CA Public Keys into devices that support Offline Data Authentication or Offline Enciphered PIN. Ensure the test VSDC CA Public Keys have been removed from production devices. Ensure devices meet the Visa requirements associated with public key management.	*TADG* *TADR*

4 Terminal Maintenance

This section outlines merchant/acquirer requirements for maintaining terminals and helping to address and prevent interoperability problems.

Chip increases the complexity of the payment application in 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 of chip are realized. An interoperability problem may occur when parameters or settings on either the card or the terminal, or both, result in a condition where payment cannot be completed.

This section provides merchants/acquirers with guidelines for terminal maintenance activities. These guidelines will help to minimize the chance of terminals creating interoperability problems in the field. It contains the following sections:

- **Terminal Retesting with Level 3 Test Tools** – Mandatory and recommended scenarios that require terminal retesting with Level 3 test tools.
- **Monitoring and Production Support** – Information to aid merchants/acquirers in developing their monitoring and production support procedures.
- **Interoperability Problems** – The importance of addressing and resolving interoperability problems in a timely manner.
- **Merchant Outreach** – Working with merchants to investigate, research, and resolve problems.

4.1 Terminal Retesting with Level 3 Test Tools

Chip introduces additional complexity to the payment service. Even cards and terminals that are EMV/Visa approved can cause interoperability problems due to incorrect personalization/configuration settings. Because of this, it is important for merchants to test their devices upon initial deployment with Level 3 test tools. See Section 3.3: Level 3 Testing for details.

In addition to using Level 3 test tools when deploying a new terminal, there are specific situations where retesting the device with Level 3 test tools is required. As a general rule, acquirers are required to perform retesting when there are:

- Modifications to the terminal that involve a new EMV kernel (or significant modification of an existing one).
- Changes to the terminal's payment application which affect EMV processing or transaction flow.
- Changes to the CVMs supported.
- Updates to the terminal that include new functionality such as Dynamic Currency Conversion (DCC) or cash back.
- Changes to the terminal that affect the terminal-to-acquirer message format.

There are also scenarios where Level 3 re-testing is recommended (e.g., when minor modifications to the device take place that do not affect the kernel).

4.2 Monitoring and Production Support

Acquirers should have monitoring procedures in place to ensure that their terminals and transactions are working properly. Monitoring activities should include tracking and investigating high levels of:

- Declines
- Offline Data Authentication failures
- Cardholder verification failures
- Online Card and Issuer Authentication failures
- Fallback transactions

Acquirers should have access to software and tools (either directly or via their vendors) that allow analysis of transactions and generation of traces which will aid in detecting the source of any problem.

Acquirers should also review the EMV bulletins to keep abreast of any known terminal issues and updates to the specifications. Visa will also communicate known or suspected interoperability issues directly to acquirers.

4.3 Interoperability Problems

If the acquirer suspects a problem at a deployed production terminal, it is recommended that all applicable tests specified in Level 3 testing are carried out to assist with the analysis. Further, if Visa is aware of a potential interoperability problem, Visa may require the acquirer to run Level 3 testing on the device.

4.3.1 Visa Chip Interoperability Compliance Program

Acquirers are required to resolve interoperability problems in a timely manner. If an interoperability problem is not addressed and resolved in a timely manner, the acquirer may be subject to compliance action as defined in the Visa Chip Interoperability Compliance Program.

The Visa Chip Interoperability Compliance Program provides the framework for a Visa client or a client's agent identified with high-severity contact or contactless interoperability problems to:

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

4.4 Merchant Outreach

If a problem occurs, acquirers should work with their merchants to investigate, research, and resolve the problem. Some problems (such as excessive fallback transactions) could be due to merchant training issues (e.g., merchants are not ensuring that chip cards are read via the chip reader). For more information on initial and on-going merchant training, see Section 8.6: Merchant Training.

5 Acquirer System Changes

This section provides merchants/acquirers with information to help them update their systems to support contact and contactless transactions. It contains the following sections:

- **Transaction Routing** – Information to assist merchants/acquirers with transaction routing.
- **Terminal-to-Acquirer Messages** – An overview of the changes required to terminal-to-acquirer messages to support chip.
- **VisaNet Messages** – An overview of the changes required to VisaNet messages to support chip.
- **Reversals** – Information on reversals.
- **Transaction Types and Industry-Specific Transactions** – Changes required to transaction types and industry-specific transactions.
- **Fallback Transactions** – Information on processing and identifying fallback transactions.

5.1 Transaction Routing

In the U.S., U.S. Covered Visa Debit Cards can be routed exclusively using the Visa U.S. Common Debit AID. When the Visa U.S. Common Debit AID is selected for a given transaction (see Section 2.2.2.3: Special Application Selection Logic for details), the acquirer can route the transaction to an issuer-enabled debit network (such as determined by the BIN tables) or to a Visa network.

If a Visa ISO AID is selected for a given transaction, however, the transaction must be routed to a Visa-affiliated network. To ensure this rule is met, Visa requires that the terminal send the AID (which is contained in a data element called the Dedicated File (DF) Name) to the acquirer in the terminal-to-acquirer message along with the other chip data. When the acquirer (or other intermediary routing party) obtains the DF Name and it contains a Visa ISO AID, they can use this information to ensure the transaction is routed to a Visa-affiliated network.

While a transaction with a Visa ISO AID 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. For example, data from a card may be accessed using a Visa ISO AID, but the transaction could be routed to the Plus network. An example is a Visa/Plus card (containing only the Visa AID) presented at a Plus-only ATM.

Note: These examples assume that all other eligibility criteria for the network in question have been met, such as the selected CVM and BIN routing table.

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 (e.g., non-Visa proprietary cards that are enrolled to use Plus) or transactions initiated for chip cards that contain only the Visa Interlink AID (e.g., non-Visa branded cards, where Visa Interlink is used as an alternate network).

5.2 Terminal-to-Acquirer Messages

Terminals must pass the chip data to the acquirer in the terminal-to-acquirer message(s). This data includes the cryptogam and the data required to generate the cryptogram. It is important that the data is not manipulated from the POS/ATM to the acquirer. If the data is manipulated, the cryptogram will fail, resulting in declines.

5.3 VisaNet Messages

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).
- Forward the data to the issuer in the VisaNet message.

These new fields need to be provided in authorization, full financial, and clearing and settlement messages (although chip data is not required in the clearing messages of online-authorized chip transactions in the U.S. region). 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.

Important: If any of the data that is signed as part of the cryptogram has been changed or manipulated, cryptogram validation will fail which will lead to erroneous declines. Therefore, the acquirer must ensure the data is transported from the terminal to the acquirer unaltered and then from the acquirer to the issuer unaltered.

The following table provides an overview of the changes required to VisaNet message. For details, see the *VSDC System Technical Manual*.

Table 5–1: Chip Data Elements

Data	Description
Field 55	For authorization and full financial messages, acquirers must support Field 55 in TLV (tag-length-value) format to send chip data to the issuer.
New Values in Existing Fields	Field 22: POS Entry Mode: • 05 or 95 for a contact-chip transaction • 07 for a contactless-chip transaction
	Field 60.2: Terminal Entry Capability: • 5 to indicate that the device is capable of reading a chip card • 8 to indicate that the device has contactless capability but does not support contact chip
Track 2 Equivalent Data	The acquirer must forward the Track 2 Equivalent Data from the chip to the issuer unaltered.
Clearing and Settlement Data	TCR 0, TCR 1, and TCR 5 will carry a minimal amount of chip transaction-related data. **Note:** TCR 7 is not required in clearing and settlement messages for online-only or zero-floor limit terminals that always go online to obtain issuer authorization.
Visa ISO AID	Acquirers must ensure that transactions initiated using a Visa ISO AID are routed to a Visa-affiliated network. To support this requirement, Visa requires that the AID (contained in card data element called the Dedicated File (DF) Name) is received from the terminal and sent in Field 55 of the authorization message. For more information, see Section 2.2.2.3: Special Application Selection Logic.

5.4 Reversals

In most situations, the transaction will be sent online to the issuer for processing and the issuer's authorization response (approve or decline) will determine the outcome of the transaction. There may, however, be situations where the issuer approved the transaction but the outcome of Issuer Authentication (or other processing) requires the terminal to override the issuer's decision and decline the transaction. If this is the case, the terminal must send a reversal to the issuer and not submit the transaction for clearing and settlement.

5.5 Terminated Transactions

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

5.6 Transaction Types and Industry-Specific Transactions

POS terminals and ATMs must support a variety of transaction types. See the *TADG* for details on processing the following transaction types:

- **POS Transactions:** Pre-authorizations, incremental authorizations, sale completions, status checks, account number verifications, purchase with cashback, refunds, reversals, referrals, and cancellations.
- **ATM Transactions:** Cash Disbursements, non-cash transactions, mis-dispense transactions, cancellations, sales of good/services at ATMs, and dispensing/loading prepaid cards.

In addition, specific processing is required to support industry-specific transactions such as Deferred Authorizations, Acquirer Stand-in, Travel & Entertainment (T&E) transactions, and Automated Fuel Dispensers (AFDs). See the *TADG* for details.

5.6.1 Deferred Authorizations and Visa PIN Debit Gateway and Interlink

There are special considerations for debit acceptance and Deferred Authorizations, particularly associated with Store & Forward transactions routed to the Visa PIN Debit Gateway and Interlink. In 2010, Visa rules were updated to prevent Store & Forward transactions over the Visa PIN Debit Gateway and Interlink partly to address security concerns associated with the PIN Block and also to prevent complications associated with reversals and adjustments. The best solution for PIN debit acceptance with online connectivity issues is:

- Disable PIN pad during such outages (e.g., using a Selectable Kernel)
- Complete transaction without a PIN
- Send Deferred Authorizations 0100 (credit) or 0200 (debit) without PIN Block

Important: Effective with the April 2019 business release, Deferred Authorizations may include the deferred authorization indicator so that the issuer can identify them. Effective October 2019, acquirers must support sending the indicator. Effective April 2021, merchants must include the indicator in all Deferred Authorizations. For more information, see the *October 2019 and January 2020, VisaNet Business Enhancements, Global Technical Letter and Implementation Guide*, *Article 2.1: Mandate to Support the Message Reason Code for Deferred Authorizations*.

5.7 Fallback Transactions

Fallback transactions are non-chip transactions performed with chip cards at chip terminals. Chip cards must be accepted by the chip reader unless the chip card or terminal is malfunctioning.

There are specific situations (e.g., when the chip on the card is faulty or damaged or the chip reader in the terminal is malfunctioning) where the chip card can be accepted via the magnetic-stripe reader. In these situations, an online magnetic-stripe transaction to the issuer can take place (fallback to key-entry/manual procedures may be allowed in some environments). These transactions are less secure because magnetic-stripe acceptance circumvents the control and risk management protection available with a chip transaction.

Contact your Visa representative for information on local rules governing fallback.

For information on merchant training for fallback, see Section 8.6.4: Fallback Transactions.

5.7.1 Fallback Transaction Identification

Merchants/acquirers need to correctly identify magnetic-stripe fallback transactions as outlined in the following table and acquirers can use this information to locate fallback transactions for monitoring purposes.

Table 5–2: Magnetic-Stripe Fallback Data Elements

Field Location	Field Name	Value
V.I.P. Field 22	POS Entry Mode	02 or 90 (magnetic-stripe read)
V.I.P. Field 35	Track 2 Data	Service Code (Digit 1) is 2 or 6 (chip card)
V.I.P. Field 60.2	Terminal Entry Capability	5 (terminal is capable of reading a chip card)

Merchants/acquirers need to correctly identify key/manual-entry Fallback transactions as outlined in the following table.

Table 5–3: Key/Manual-Entry Fallback Data Elements

Field Location	Field Name	Value
V.I.P. Field 22	POS Entry Mode	01 (key/manual entry)
V.I.P. Field 60.2	Terminal Entry Capability	5 (terminal is capable of reading a chip card)

5.7.2 Fallback Transaction Monitoring

Acquirers should establish monitoring procedures to ensure fallback levels are kept to a minimum. They can use the fields outlined in the previous section to identify fallback transactions. High levels of fallback may indicate problems with a device or, alternatively, a need for further merchant education.

Visa has enacted a global monitoring program to identify acquirer/country combinations with high levels of international, and where applicable, domestic fallback (see next section for details). Acquirers identified will need to take corrective action.

5.7.3 Global Chip Fallback Monitoring Program

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.
- Acquirer-country combinations that have fallback activity nearing program thresholds, which allows acquirers to take proactive measures to avoid exceeding thresholds.

Domestic fallback reporting can also use Global Fallback Monitoring Program thresholds. POS activity is reported separately from ATM activity.

Acquirers may incur a non-compliance assessment for each fallback transaction over their allowance. Acquirers should contact their Visa representative for more information on this program.

6 Acquirer Host System Testing

Acquirers must perform host system testing with VCMS to ensure they can support the new chip data in their VisaNet messages. This testing is mandatory for new contact and/or contactless acquirers.

Important: Acquirers must perform Level 3 terminal testing prior to commencing with host system testing. See Section 3.3: Level 3 Testing for details.

This section provides an overview of the testing:

- Acquirers perform internal testing of both their terminal-to-acquirer messages and VisaNet messages to ensure all components are working properly.
- Acquirers ensure their test environment is set up by confirming their connection to the VisaNet Certification Management Service (VCMS) and obtaining test scripts and test cards from Visa.
- Acquirers perform host testing with VCMS. They will use the test cards and test scripts to initiate test transactions to VCMS.

For details on acquirer host system testing for chip, contact your Visa representative and see the following documents:

- *VisaNet Testing Guide*
- *VCMS Testing Guide – BASE II*
- *Visa Smart Debit/Credit System Technical Manual*

7 Acquirer Back-Office Changes

This section addresses the technical changes to back-office functions that are required to support the acquirer's 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. It contains the following sections:

- **Dispute Resolution Management** – Updating dispute resolution procedures for chip.
- **Reporting** – Enhancing reporting capabilities for chip.
- **Visa Quarterly Operating Certificate** – Providing chip information to Visa on the Quarterly Operating Certificate.
- **Internal Staff Training** – Training internal staff on all aspects of chip.

7.1 Dispute Resolution Management

Acquirers need to update their dispute resolution procedures for chip transactions. They should review the Dispute Resolution section of the *Visa Rules* to determine how chip transactions and chip data alter the dispute resolution process and then update their internal procedures as required to accommodate these changes. For example, the EMV Liability Shift protects the entity (acquirer or issuer) that has invested in EMV chip technology.

For more information on disputes, see the *Visa Rules*, Visa Resolve Online (VROL), and Visa Claims Resolution at: www.secure.visaonline.com/SitePages/Section.aspx?pageid=2.1.1.0.0.

7.2 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

7.2.1 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.

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 (POS)/Cash Disbursement volume (ATM) 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 transactions through the following data elements:

- POS Entry Mode (V.I.P. Field 22) values of 05 or 95 (contact transaction) or 07 (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 (terminal is capable of reading a chip card) or 8 (device has contactless capability but does not support contact chip).

7.2.2 Fallback Transactions

Acquirers should monitor and track fallback transactions. A high incidence of fallback transactions needs to be investigated as it indicates either device problems (the terminal is not working properly) or incorrect merchant procedures.

For more information on fallback transactions including information on the Visa Global Fallback Monitoring Program, see Section 5.7: Fallback Transactions.

For information on merchant training for fallback, see Section 8.6.4: Fallback Transactions.

7.2.3 Enhanced Reporting Opportunities

Acquirers can use the additional chip data in their reports. By offering a view of the interaction between the card and terminal, this data can 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
- Merchant service reports that monitor support levels for chip terminals

7.3 Visa Quarterly Operating Certificate

Acquirers must provide information on the Quarterly Operating Certificate to track the number of individual merchants and the number of merchant outlets accepting chip in the following categories:

- Magnetic stripe, contact chip, and contactless
- Magnetic stripe and contact chip (not contactless)
- Magnetic stripe and contactless (not contact chip)

7.4 Internal Staff Training

Each organizational unit involved in a merchant service function must be trained on the nuances of chip 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 development of the training plan should include the following tasks:

- Develop objectives for chip training.
- Determine audiences/departments that require 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 and customer services.

Staff should also be informed about how to get answers to questions that arise after the initial training is complete.

8 Merchant Support

This section reviews the tasks related to supporting merchants as they make the transition to chip card acceptance. It includes the following sections:

- **Merchant Agreement** – The merchant agreement may need to be updated to accommodate migration to chip.
- **Technology Innovation Program** – Information on the Technology Innovation Program.
- **Merchant Services** – The importance of providing merchants with support for their chip programs.
- **Merchant System Changes** – The system changes that may be required for merchants participating in chip.
- **Contactless Reader Branding and Placement** – Information on the branding and placement of contactless readers.
- **Merchant Training** – Guidelines for merchant training.

8.1 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.

8.2 Technology Innovation Program (TIP)

The Technology Innovation Program (TIP) recognizes and acknowledges merchants that have taken action to reduce the risk of compromise and fraud by investing in secure acceptance technologies.

With TIP, Visa eliminates the annual requirement for eligible merchants to validate PCI DSS compliance once 75% of the merchant's Visa transactions originate from enabled and operating chip-reading devices (devices must support both contact and contactless transactions for U.S. merchants) and/or through a PCI-validated point-to-point encryption solution. At the same time, Visa requires that merchants continue to protect any sensitive data that remains in their care and to adhere to PCI DSS as applicable.

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

8.2.1 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:

- 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.
- The merchant must have confirmed that sensitive authentication data (e.g., full contents of magnetic stripe, CVV2, and/or PIN data) is not stored, as defined in PCI DSS.
- At least 75 percent of the merchant's total transaction count must originate from dual-interface (contact and contactless) enabled chip-reading terminals.[8]
- 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 PCI DSS, the PCI PIN Security Requirements, and the Payment Application Data Security Standards (PA-DSS).

[8] Enabled chip reading devices must have current, valid EMV approval (Level 1 and Level 2), pass Visa Level 3 testing requirements, and must comply with the *Visa Transaction Acceptance Device Requirements (TADR)*. Acquirers should contact their Visa representative for further information.

8.2.2 Acquirer Requirements

Visa will work directly with acquirers to confirm eligible merchants and verify the 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 non-compliance assessments that may be applicable in the event of any data breach.

8.3 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 enhancements to their merchant service area.

8.3.1 Merchant Implementation Support

It is important for acquirers to plan how to support merchant conversions to 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 hotline for merchant questions. Ideas for communicating the hotline number include:
  - 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
- 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 the terminal-to-acquirer message format.

8.3.2 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. See Table 3–2: Terminal Checklist for details.
- Decide on deployment methods to be utilized (e.g., 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 (e.g., printer paper, ribbons, deposit slips, and terminal faceplates).
- Identify the need for accessories (e.g., 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.

8.3.3 Ongoing Terminal Maintenance

Acquirers should directly, or via an agent, make use of a Terminal Management System 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.

For more information on Terminal Management Systems, see the *TADG*.

8.3.4 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.
- Continue to support a telephone hotline for inquiries.

8.4 Merchant Systems Changes

Impacts on merchant systems due to 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.

8.5 Contactless Reader Branding and Placement

Merchants are required to display the EMV Contactless Symbol[9] on all readers to let cardholders know how and where they can use Visa contactless cards. These requirements are available from:

- Visa Merchant Signage website at www.merchantsignage.visa.com
- Visa Product Brand Standards website at www.productbrandstandards.com

Merchants should also ensure they have placed contactless readers so that they can be seamlessly used by cardholders and to maintain the principle of a fast transaction. Some best practices include:

- Reader indicators that are intended to be visible to the cardholder should be located so they are clearly visible when the cardholder is looking at the reader landing zone. Readers should be free from obstructions, and cardholders should be able to easily access 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.

For more information on the placement of contactless readers, see the *TADG*.

8.6 Merchant Training

Chip introduces new functionality at the POS. Merchants must be trained on the basic procedural differences between magnetic-stripe and chip-card acceptance:

- Contact-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 contact-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 especially in unattended environments such as ATMs, UCATs, and AFDs. These environments should have instructional prompts and signage to support cardholders through each phase of the transaction.

[9] The EMV Contactless Symbol is a trademark owned by and used with permission of EMVCo, LLC.

- Merchants should be trained to recognize a chip card and prompted to instruct the cardholder to insert the card into the chip reader (contact) or place the chip card on the landing pad (contactless) rather than swiping the magnetic stripe. This will speed and streamline the transaction.

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

8.6.1 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 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 (e.g., due to turnover or high incidents of fallback transactions).

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.

8.6.2 Cardholder Application Selection

If the terminal supports Cardholder Selection and the card contains multiple applications, cardholders may be prompted to select the application to be used for a given transaction. Cardholder application selection only takes place when the card and terminal have more than one application in common or when required by the card.[10] Merchants need to understand that cardholder application selection may occur on some transactions and not others and that this difference does not indicate a problem.

See Appendix B: Basic EMV Terminal Logic for details.

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 ISO AID connected to the credit function, and a debit pair consisting of a Visa ISO 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 ISO AID for credit functionality. See Appendix C: *Special Terminal Logic* for details.

Training should teach merchants to understand and explain the Application Selection process and how to guide their customers in pressing the correct button(s) to select the application or account they prefer to use.

8.6.3 Cardholder Verification

Merchants and cardholders typically understand the methods of verifying a transaction in attended environments such as 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.

[10] This does not apply to U.S. Covered Debit Cards. Cardholder 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.

The final CVM 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.

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:

- For contact transactions, the card contains a CVM List which is a prioritized list of CVMs along with the rules for their use. The terminal reviews the CVM List along with its CVM capabilities to determine the appropriate CVM for the transaction.
- For contactless transactions, when neither the card nor device requires a CVM for the transaction (e.g., transaction is below the Reader CVM Required Limit), the transaction takes place without a CVM. If the transaction requires a CVM, the card compares its supported CVMs to the ones supported by the device and the highest priority CVM supported between the two will be used for the transaction.

8.6.3.1 Signature

While the kernel in all attended POS devices must support signature, the merchant is no longer required to capture or validate the cardholder's signature. Contact your Visa representative for details.

Local laws and regulations supersede Visa's rules; if local regulatory requirements require a merchant to obtain a CVM (which may include a signature), then they should continue to do so.

8.6.3.2 PIN

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

- The card and terminal interaction will determine the CVM and whether to prompt for a PIN.
- Because the card and terminal determine whether PIN entry is required on each transaction, lack of a terminal PIN prompt should not be considered an error. The terminal will prompt for PIN only when a PIN is required. The merchant should not request PIN entry from the cardholder unless the terminal issues this prompt.
- Where a cardholder is required to enter a PIN, the secrecy of 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 a signature line is not present on the receipt.[11]
- Depending upon local requirements, a device may support both Online PIN and Offline PIN. From a merchant's perspective, there is no difference and PIN processing is the same.

[11] For devices that capture signature electronically, the device will not display the signature capture screen.

- Some cardholders might not enter the PIN at the POS terminal due to security concerns or certain disabilities. Merchants need to offer alternatives to these cardholders in accordance with merchant protection and local, state, or federal disability legislation.

8.6.3.3 Consumer Device CVM (CDCVM) (Contactless)

Contactless devices must support the Consumer Device CVM (CDCVM) and indicate support for it in the Terminal Transaction Qualifiers (TTQ). In addition to CDCVM, the reader may support other CVMs such as signature and/or Online PIN.

Note: On contactless transactions, to ensure acceptance, ATMs must indicate support for Online PIN, signature, and CDCVM in the TTQ, although Online PIN is the only CVM that will apply to ATM transactions.

8.6.3.4 No Cardholder Verification Required (No CVM)

There are situations where the chip card and terminal may decide that the transaction can take place without cardholder verification (i.e., no CVM); for example, a transaction taking place at a UCAT.

Merchants should be made aware that some transactions may not require any CVM, and they should not request a CVM if the terminal has not prompted for one.

8.6.4 Fallback Transactions

Visa policies state that chip cards must be read via the chip 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 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 (in some countries) may then fallback to existing card acceptance procedures. Acquirers may need to revise their procedures on fallback related to key-entry and paper-based transactions.

Fallback requirements are governed by the *Visa Rules* relating to 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 may 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 disputed 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 must not deliberately force 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 when not accepted by the chip.

8.6.5 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.

For details on transaction types such as refunds and reversals, see the *TADG*.

8.6.6 International Transactions

Merchants should be trained to accept international cards just as they would accept domestic cards with the difference that the CVM on an international transaction may differ from those associated with domestic transactions (e.g., signature on international transactions and PIN on domestic transactions).

8.6.7 Terminated Contactless 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 cardholder confusion during the transaction.

8.6.8 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.

9 References

This section outlines reference materials for this Guide. It includes the following sections:

- EMVCo Documents
- PCI SSC Documents
- Visa Documents

Note: Ensure you are using the latest versions of the Visa and other industry documents applicable to your implementation.

9.1 EMVCo Documents

The following documents are available on www.emvco.com:

- *EMV Acquirer and Terminal Security Guidelines*
- *EMV Contactless Specifications for Payment Systems* ("EMV Contactless Specifications")
- *EMV Integrated Circuit Card Specifications for Payment Systems* ("EMV Chip Specifications")
- *EMV Optimising Contact Chip Transaction Times Best Practices*
- *EMVCo Contactless Symbol Reproduction Requirements*
- *Recommendations for EMV Processing for Industry-Specific Transaction Types*

9.2 PCI SSC Documents

The following documents are available on www.pcisecuritystandards.org:

- *Payment Application Data Security Standard (PA-DSS)*
- *PCI Data Security Standard (PCI-DSS)*
- *PCI DSS Wireless Guidelines*
- *Skimming Prevention: Best Practices for Merchants*

The following documents are available on www.visaonline.com:

- *PCI PIN Security—Requirements and Testing Procedure*
- *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*

9.3 Visa Documents

This section provides references to Visa documents. Acquirers can obtain these documents from Visa Online (VOL) at www.visaonline.com or their Visa representative.

Table 9–1: Visa Reference Materials

Title and Description	Audience	User
Visa Specifications		
Visa Contactless Payment Specification (VCPS) Provides the Visa specification for contactless payments utilizing qVSDC. **Note:** Please ensure you have the latest published updates.	Issuers, Acquirers, Vendors	Policy, Operations, Technical
Visa Integrated Circuit Card Specification (VIS) Provides the Visa-companion specification to the *EMV Chip Specifications* that covers additional details about the chip card-to-device interfaces for Visa debit and credit programs. **Note:** Please ensure you have the latest published updates.	Issuers, Acquirers, Vendors	Policy, Operations, Technical
Visa Guides, Manuals, and Requirements		
Dynamic Currency Conversion (DCC) Guide – DCC Program Requirements Outlines the requirements and best practices for DCC for acquirers, merchants, and ATMs.	Acquirers, Merchants, and Vendors	Policy, Operations
Payment Technology Standards Manual Furnishes the standards applied to Online PINs, PIN-related security, and TDES key management, as well as the guidelines for encoding account and cardholder data on the magnetic stripe of a Visa card.	Issuers and Acquirers	Operations, Technical
Transaction Acceptance Device Guide (TADG) Provides vendors, merchants, acquirers, and device deployers with information to help them deploy transaction acceptance devices ("devices") that support the acceptance of Visa payment cards. Outside of the *EMV Chip Specifications* and *VCPS*, this is the main Visa resource for information on devices. The TADG is a public document available at www.visa.com/tadg.	Acquirers, Processors, Vendors	Operations, Technical
Transaction Acceptance Device Requirements (TADR) Outlines chip-device requirements that are not covered in the *Visa Rules*.	Acquirers, Vendors	Policy, Operations, Technical
VSDC Contact & Contactless Acquirer Implementation Guide Provides a handbook for acquirers or acquirer processors responsible for the implementation of a VSDC contact and/or contactless program. **Note:** A U.S.-specific version is available for acquirers in the U.S. region.	Acquirers, Processors	Operations, Technical

Title and Description	Audience	User
VSDC System Technical Manual Provides a processing overview document that provides details of VSDC-related host system changes for the authorization, full financial, and clearing and settlement messages, including new data elements.	Issuers, Acquirers, Processors, Host System Vendors	Technical
Merchandise Returns/Refunds		
Merchandise Return Authorization Messages October 2019 and January 2020, VisaNet Business Enhancements, Global Technical Letter and Implementation Guide, Article 2.8: Mandate for Credit Voucher and Merchandise Return Authorization Messages Describes the technical changes to support an authorization message for merchandise returns/refunds.	Acquirers, Merchants, and Vendors	Technical
Visa Branding		
Visa Merchant Signage Website Provides merchants with guidelines on using the Visa brand and the EMV Contactless Symbol. It also provides promotional and marketing materials that merchants can order. www.merchantsignage.visa.com	Acquirers, Merchants, and Vendors	Marketing Operations
Visa Public Keys		
Visa Smart Debit/Credit (VSDC) Certificate Authority (CA) Public Keys Provides the VSDC Certificate Authority (CA) Public Keys (includes both test and production keys). www.visa.com/pubkeys	Acquirers, Vendors	Technical
Device Testing		
Chip Card Acceptance Device – Testing and Approval Process Outlines the testing requirements for contact and contactless devices.	Acquirers, Vendors	Operations
Visa Level 3 Testing		
Acquirer Device Validation Toolkit (ADVT) User Guide Outlines test cases to validate new or upgraded EMV contact-chip devices.	Acquirers, Vendors	Operations
Contactless Device Evaluation Toolkit (CDET) User Guide Outlines test cases to validate new or upgraded contactless-chip devices.	Acquirers, Vendors	Operations
Visa Mobile Card Personalization (VMCP) App Usage Instructions Provides instructions for using VMCP for ADVT and CDET testing.	Acquirers, Vendors	Operations

Title and Description	Audience	User
Visa Rules		
Interlink Core Rules and Interlink Product and Service Rules Outlines the operating regulations for Interlink.	Issuers, Acquirers	Policy, Operations
Plus System, Inc. Operating Regulations Outlines the operating regulations for Plus.	Issuers, Acquirers	Policy, Operations
Visa Core Rules and Visa Product and Service Rules ("Visa Rules") Provides regulations for issuers and acquirers, including rules governing contact and contactless transactions, dispute processing, and interchange rates.	Issuers, Acquirers	Policy, Operations
Transit		
Visa Contactless Transit Implementation Guide Defines the general requirements and provides guidelines for stakeholders involved in the acceptance and processing of Visa contactless payments for automatic fare collection in mass transit systems.	Issuers, Acquirers, Processors, Merchants, Vendors	Technical
Visa Contactless Transit Kernel Specification Defines the technical differences between the kernel defined in *VCPS* and the *EMV Contactless Specifications* and the contactless kernel used in transit acceptance environments (i.e., the "transit kernel").	Acquirers, Processors, Merchants, Vendors	Technical
Visa Contactless Transit Terminal Requirements and Implementation Guide Defines the terminal requirements for acceptance of Visa contactless payments for automatic fare collection in mass transit systems.	Acquirers, Processors, Merchants, Vendors	Technical
VisaNet Business Enhancements Global Technical Letter and Implementation Guide, October 2018 and January 2019, Article 3.11: Support of Mass Transit Transactions **FAQs for Article 3.11, Changes to Support Mass Transit Transactions** Outlines the requirements to support transit using contactless cards and FAQ.	Issuers, Acquirers	Technical
U.S. Specific Chip Documentation		
Visa U.S. EMV Chip Terminal Testing Requirements Visa U.S. Quick Chip and Minimum Terminal Configuration ADVT 7/CDET 2.3 Use Cases Visa Minimum U.S. Online Only Terminal Configuration VSDC Contact & Contactless U.S. Acquirer Implementation Guide (this guide) U.S. Visa Contactless Transit Terminal Testing	Acquirers, Vendors	Operations, Technical

Appendix A. Planning and Implementation

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.

A.1 Planning

This section provides an overview of key considerations in planning for a chip program:

- Define project scope and success criteria
- Conduct situation analysis (market research, competitor analysis, business case, liability shift, etc.)
- Determine project team (team should include all relevant internal areas, acquirer processor, key vendors, and Visa)
- Define team member roles and responsibilities
- Determine project sponsor and project manager(s)
- Develop launch strategy, objectives, and plans including milestones and key dates
- Define target and priority merchants for deployment
- Develop a migration and rollout plan for key merchants, merchant segments, and ATM locations
- Determine whether you will support a pilot launch and if so, define the objectives, participants, and roles and responsibilities of the pilot

A.2 Implementation

This section provides a checklist for chip card implementations.

For a terminal-specific checklist, see Table 3–2: Terminal Checklist.

Table A–1: Implementation Checklist

	Topic	Task	Section Reference
1.	**Terminal Selection**	Create terminal requirements. Assess which terminal types are needed (attended POS, UCATs, AFDs, ATMs). For ATMs, determine if existing ATMs can be upgraded or if new ATMs are required. Determine whether terminals will include contactless functionality. Review available products with a range of vendors. Select terminals that best meet your requirements.	3.1: Terminal Selection
2.	**Terminal Approval**	Ensure terminals have been tested and approved by EMVCo (contact terminals) and tested and approved by EMVCo or Visa (contactless terminals). **Note:** It is recommended that acquirers select a product that has already been approved to expedite deployment timeframes.	3.2: Terminal Approval
3.	**Level 3 Testing**	Perform Level 3 self-testing on the terminal. **Note:** Acquirers in the U.S. region can utilize the Visa Chip Vendor Enabled Service (CVES) to engage third-party chip tool vendors to execute Level 3 testing on their behalf.	3.3: Level 3 Testing
4.	**Terminal Checklist**	Ensure terminals are properly set up with all applicable data elements and are ready for deployment.	Table 3–2: Terminal Checklist
5.	**Terminal Maintenance**	Develop a plan to maintain terminals and ensure they are not contributing to interoperability problems.	4: Terminal Maintenance
6.	**Terminal Retesting with Level 3 Test Tools**	Retest terminals with Level 3 test tools as required (e.g., when terminal changes affect the kernel, when adding new functionality such as cash back or Dynamic Currency Conversion (DCC), or when terminal-to-acquirer message format has changed).	4.1: Terminal Retesting with
7.	**Monitoring/ Production Support**	Have monitoring procedures in place to help ensure that terminals are working properly. Investigate high-levels of declines, cardholder verification failures, authentication failures, and fallback transactions.	4.2: Monitoring and Production Support

	Topic	Task	Section Reference
8.	**Interoperability Problems**	Assess, investigate, and research suspected interoperability problems. Level 3 test tools can be used to support these activities. Resolve any interoperability problems in a timely manner.	4.3: Interoperability Problems
9.	**Merchant Outreach**	Work with merchants to resolve interoperability problems as required.	4.4: Merchant Outreach
10.	**Transaction Routing**	Review any impacts to transaction routing for chip and make changes where required.	5.1: Transaction Routing
11.	**Terminal-to-Acquirer Messages**	Ensure terminal-to-acquirer messages support chip.	5.2: Terminal-to-Acquirer Messages
12.	**VisaNet Messages**	Upgrade host systems to support chip data in VisaNet messages.	5.3: VisaNet Messages
13.	**Reversals**	Be aware that there may be situations where the issuer approves the transaction in the authorization response but the terminal overrides the approval and declines the transaction. In these situations, the terminal must send a reversal.	5.4: Reversals
14.	**Terminated Transactions**	Ensure the terminal handles terminated transactions properly.	5.5: Terminated Transactions
15.	**Transaction Types**	Make terminal enhancements to support all applicable transaction types: • **POS Transactions:** Pre-authorizations, Incremental Authorizations, Sale Completions, Status Checks, Account Number Verifications, Purchase with Cashback, Refunds, Reversals, Referrals, and Cancellations. • **ATM Transactions:** Cash Disbursements, Non-Cash Transactions, Mis-dispense Transactions, Cancellations, Sales of Good/Services at ATMs, and Dispensing/Loading Prepaid Cards.	5.6: Transaction Types and Industry-Specific Transactions
16.	**Industry-Specific Transactions**	Support industry-specific transactions as applicable (e.g., deferred authorizations, hotel transactions, AFD transactions, etc.)	5.6: Transaction Types and Industry-Specific Transactions
17.	**Fallback Transactions**	Support fallback transactions.	5.7: Fallback Transactions
18.	**Acquirer Host System Testing**	Perform host system testing with Visa.	6: Acquirer Host System Testing

	Topic	Task	Section Reference
19.	**Dispute Resolution**	Review the Visa dispute rules for chip transactions and make changes to internal procedures as required.	7.1: Dispute Resolution Management
20.	**Reporting**	Enhance reporting to accommodate chip transactions.	7.2: Reporting
21.	**Visa Quarterly Operating Certificate**	Provide information about your chip project to Visa on the Quarterly Operating Certificate.	7.3: Visa Quarterly Operating Certificate
22.	**Internal Staff Training**	Develop training plans for internal staff and carry out training. Hold on-going training sessions as needed and for new and existing employees.	7.4: Internal Staff Training
23.	**Merchant Agreement**	Make changes to the merchant agreement for chip as applicable.	8.1: Merchant Agreement
24.	**Technology Innovation Program (TIP)**	Take advantage of the Technology Innovation Program (TIP) by deploying chip terminals.	8.2: Technology Innovation Program
25.	**Merchant Services**	Support merchants with their chip programs.	8.3: Merchant Services
26.	**Terminal Installation**	Develop terminal installation and deployment plans.	8.3.2: Terminal Installation
27.	**Terminal Maintenance**	Support the on-going maintenance of terminals.	8.3.3: Ongoing Terminal Maintenance
28.	**Merchant System Changes**	Work with merchants to help them determine their system changes for a chip program (e.g., impacts to terminal controllers and back-office systems).	8.4: Merchant Systems Changes
29.	**Contactless Reader Branding and Placement**	Ensure contactless terminals display the EMV Contactless Symbol. Ensure contactless readers are placed at least 12 inches away from each other.	8.5: Contactless Reader Branding and Placement
30.	**Merchant Training**	Develop and carry out merchant training plans highlighting the differences between accepting chip vs. magnetic-stripe cards.	8.6: Merchant Training
31.	**Proprietary Functionality**	Determine if your terminals need to support the Visa U.S. Common Debit AID and, if so, make changes to the terminal to support special Application Selection logic.	2.2.2.3: Special Application Selection Logic Appendix C: Special Terminal Logic

Appendix B. Basic EMV Terminal Logic

This appendix provides information on basic EMV terminal logic.

Note: "Visa AID" in this appendix refers to any AID that begins with the Visa ISO RID ('A0 00 00 00 03') as defined in Section 2.1.4: Application Identifiers (AIDs).

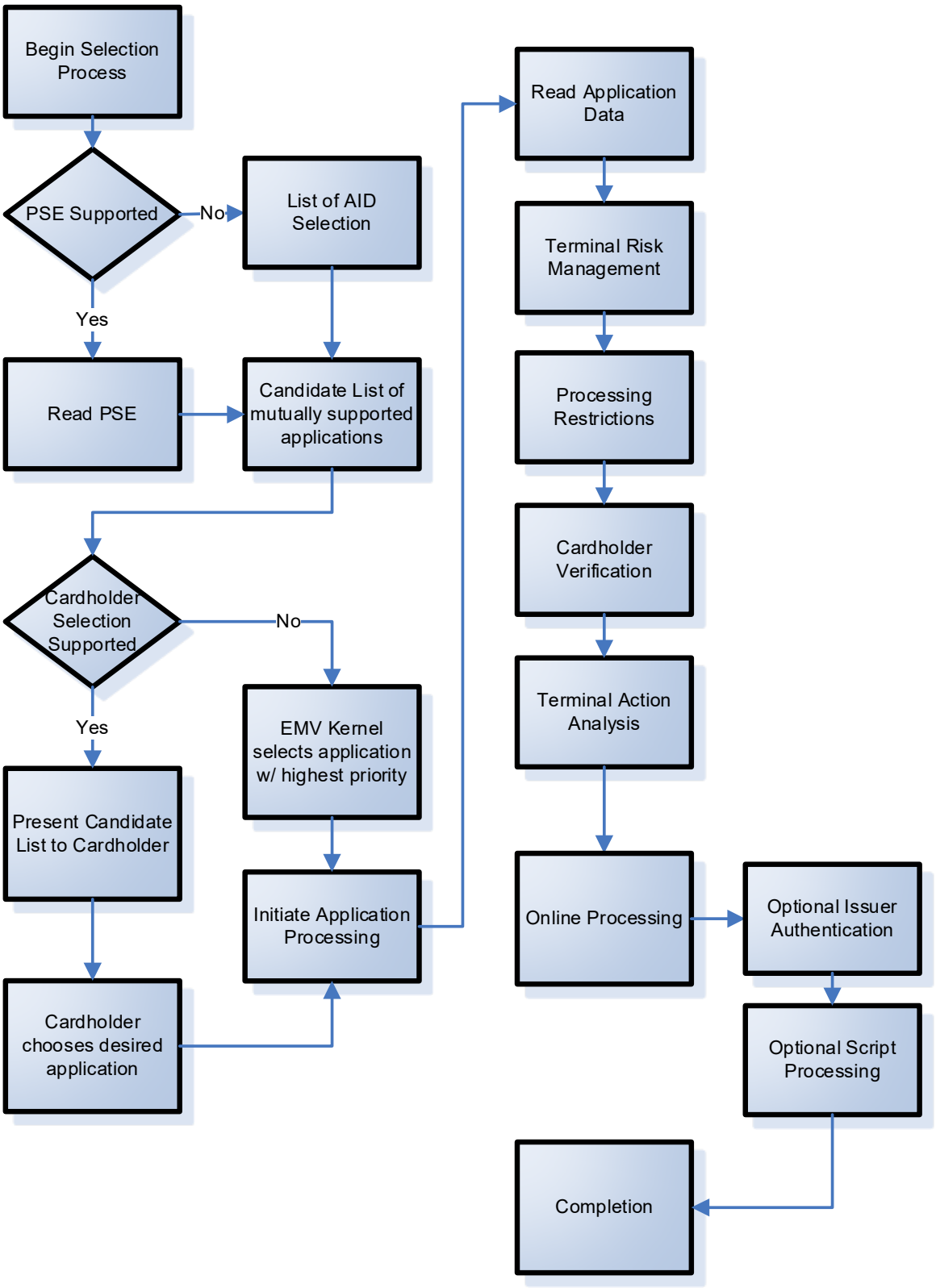
The diagram on the next page provides an overview of the basic EMV terminal logic, with a specific focus on the selection process discussed in Section 2.2.2: Application Selection Processing.

Visa cards may contain products associated with different funding sources. For example, some cards may contain two Visa ISO AIDs, one Visa ISO AID associated with a line of credit, and one Visa ISO 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 chip architecture supports this same multiple AID concept for U.S. debit cards, where U.S. debit products carry two AIDs (a Visa ISO 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 ISO AID that invokes a credit product, as well as the paired AIDs (the Visa ISO AID and the Visa U.S. Common Debit AID) that invoke a debit product (only the debit product Visa ISO 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.

Merchants may wish to deploy a selectable kernel structure in order to eliminate CVM requirements on some transactions. An example of selectable kernel processing is given in Figure C–4: Combined CVM Processing and Selectable Kernel in Appendix C.3: Contact CVM Processing and Selectable Kernels Logic.

Figure B–1: Basic EMV Terminal Logic



Appendix C. 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.

Note: "Visa AID" in this appendix refers to any AID that begins with the Visa ISO RID ('A0 00 00 00 03') as defined in Section 2.1.4: Application Identifiers (AIDs).

The EMV chip 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 ("debit pairs"). 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 contain both debit and credit applications.

To support debit routing, U.S. Covered Visa Debit Cards will be issued with both a 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 issuer-enabled 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 C.1: Contact Terminal Application Selection defines the necessary special logic transaction flow for a contact EMV terminal, while Appendix C.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 can enable CVM processing such as for cash back transactions. Appendix C.3: Contact CVM Processing and Selectable Kernels Logic illustrates the logic for a contact EMV transaction.

C.1 Contact Terminal Application Selection/Special Logic

C.1.1 Contact Terminal Application Selection Data Elements

As stated in Section 2.2.2.3: Special Application Selection Logic, 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 C–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

C.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 2.2.2: Application Selection Processing (Contact) 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:[12]

   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[13]):

   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.)

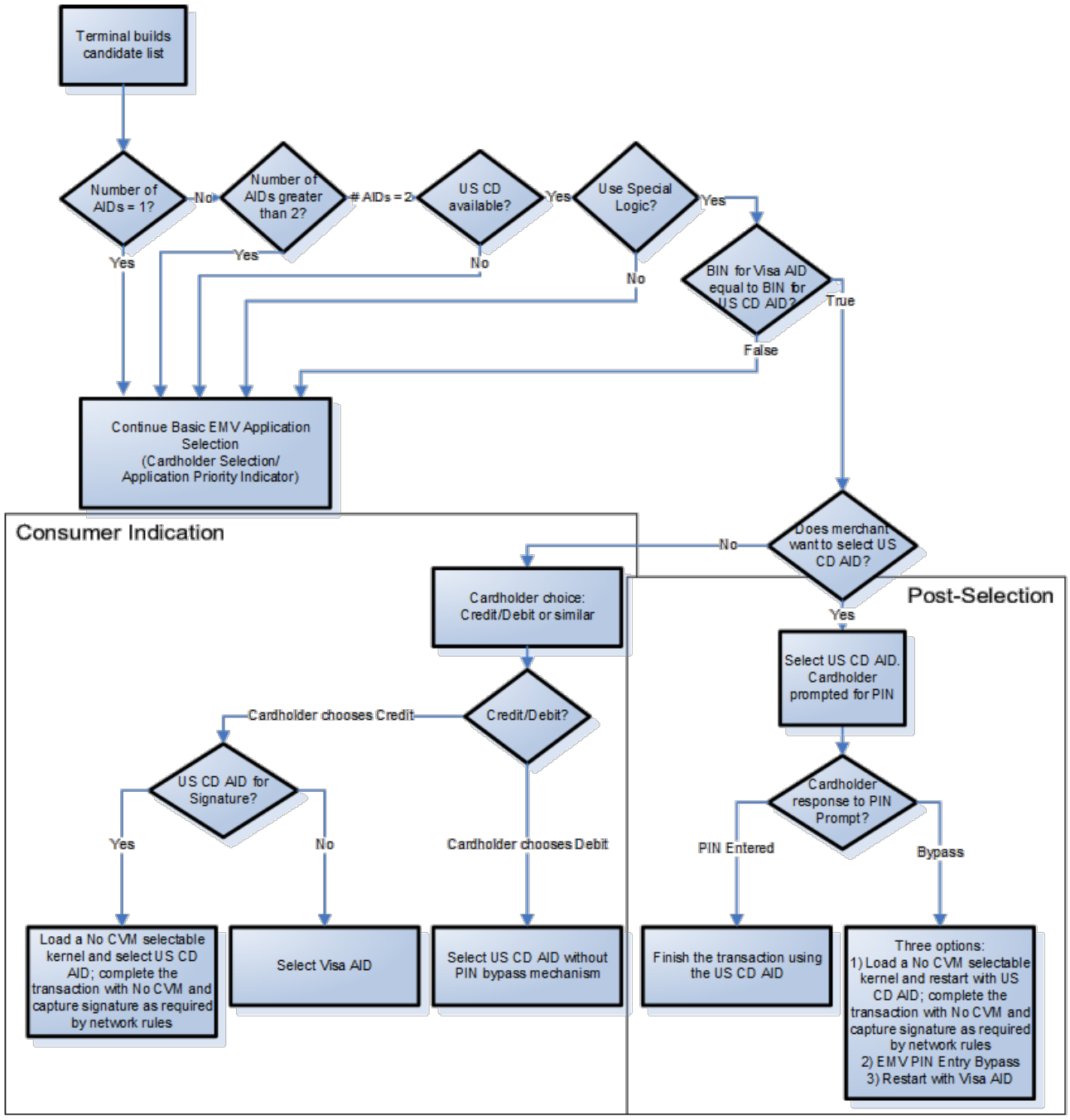
[12] For example, via a signature/PIN selection function on the terminal.
[13] PIN Entry Bypass as defined in EMV Book 4, Section 6.

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 B: Basic EMV Terminal Logic by using Cardholder Selection.

C.1.3 Contact Application Selection Special Logic Flow Chart

Figure C–1: Contact Application Selection Special Logic Flow Chart



C.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 C–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 C.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.

C.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 C–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 C.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.

C.1.6 Flow Example for Visa U.S. Common Debit AID using Signature/No CVM

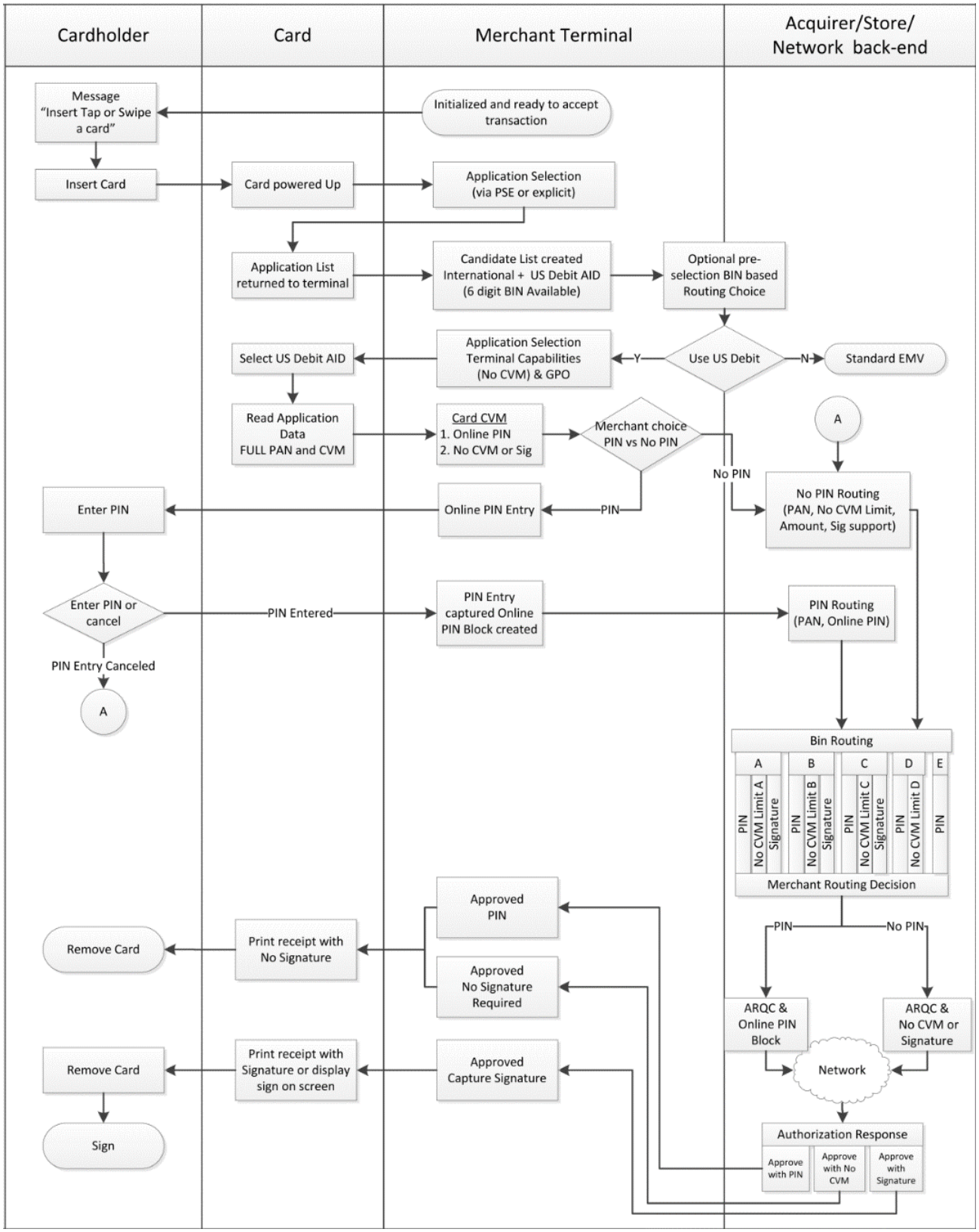
In this flow, the Visa U.S. Common Debit AID has been selected based on the flows described in Figure B–1: Basic EMV Terminal Logic. In order to process a signature/No CVM transaction in this scenario, a selectable kernel is assumed whereby the terminal is dynamically configured based on a merchant or 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.

Note: Where diagrams refer to the "US Debit AID," that is the same as the "Visa U.S. Common Debit AID" term used elsewhere in this document.

Figure C–2: Visa U.S. Common Debit Application Acceptance Overview with PIN/Signature/No CVM



C.2 Contactless Reader Application Selection/Special Logic

As mentioned in Section 2.3.2: Application Selection Processing (Contactless), 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 C–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 Issuer Identification Number (present on debit AIDs)
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.

C.2.1 Processing

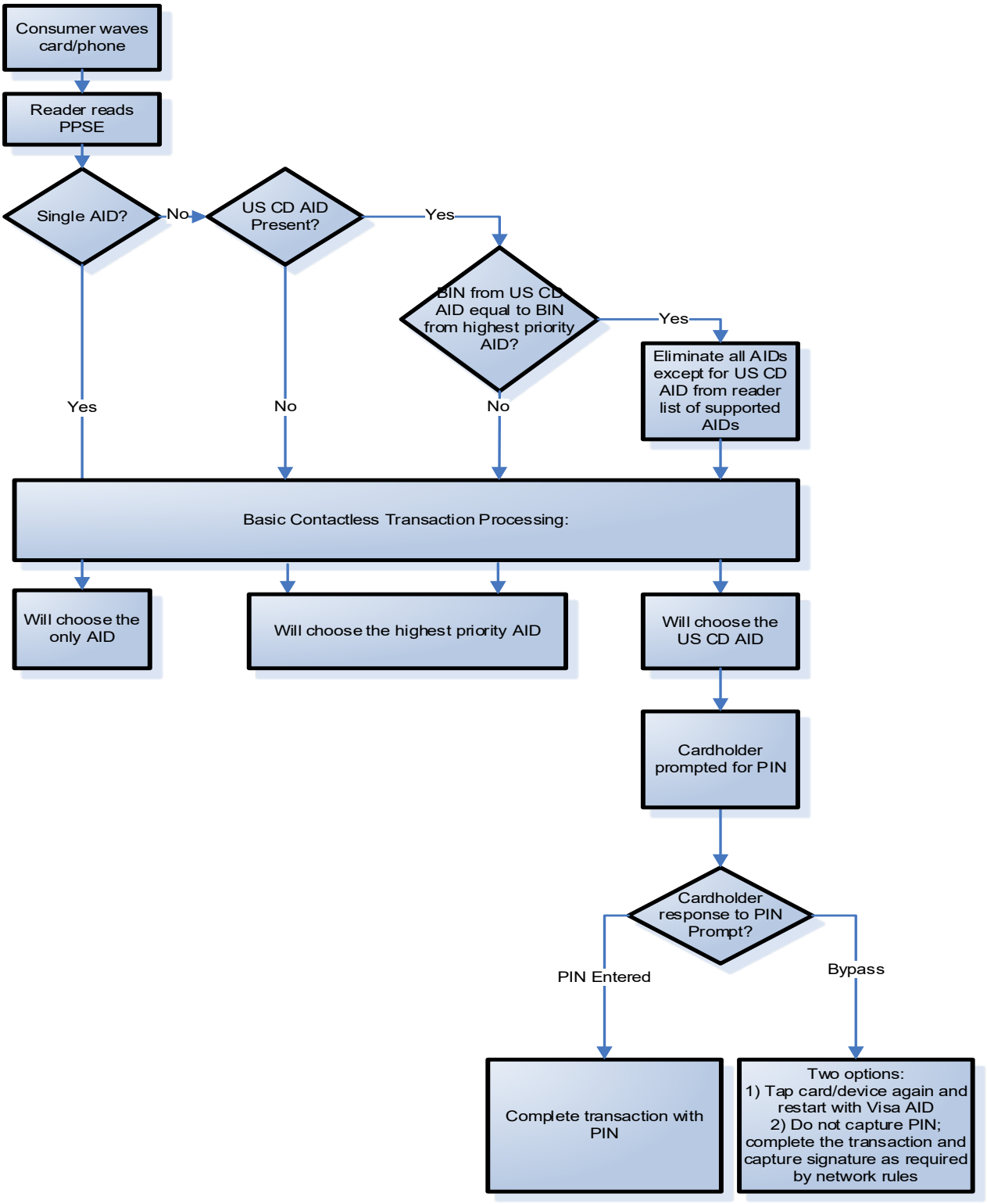
Because contactless does not support Cardholder Selection as in contact EMV, a contactless reader may need to execute a separate "pre-select" reader function once the card/device enters the contactless field but before the standard contactless transaction processing in order to examine the mutually supported 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 AID, 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 AID but the highest priority AID does **not** represent the desired functional or routing option, the reader interrogates the PPSE further. Further processing may take on one of two paths as described in the section on Direct Selection of the Visa U.S. Common Debit AID.
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).

C.2.2 Contactless Reader Application Selection Special Logic "Pre-Selection"

Figure C–3: Special Contactless Application "Pre-Selection" with Opt-out of PIN



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.[14]
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 C–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.

[14] 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.

C.3 Contact CVM Processing and Selectable Kernels Logic

Specific Cardholder Verification Method (CVM) processing may need to take place depending on transaction characteristics. There are situations in which a special Cardholder Verification Method is necessary – if supported by the terminal including:

- For terminals supporting cash back.[15] 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 CVMs are supported by the terminal in general, but with the selectable kernel approach, it is possible to offer only a specific CVM for a specific transaction. The concept behind selectable kernel is defined in the *EMV Chip Specifications* and this section will define the details necessary for 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.

C.3.1 Processing

This section outlines special CVM processing used for terminals supporting cash back. The processing can take place as described in Figure C–4: Combined CVM Processing and Selectable Kernel or as described in this section depending on terminal capabilities.

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.

[15] This mechanism can also be used if a specific CVM is required for other reasons.

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,[16] 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.

Note: Following the PIN prompt with a cash back choice may provide the simplest terminal logic.

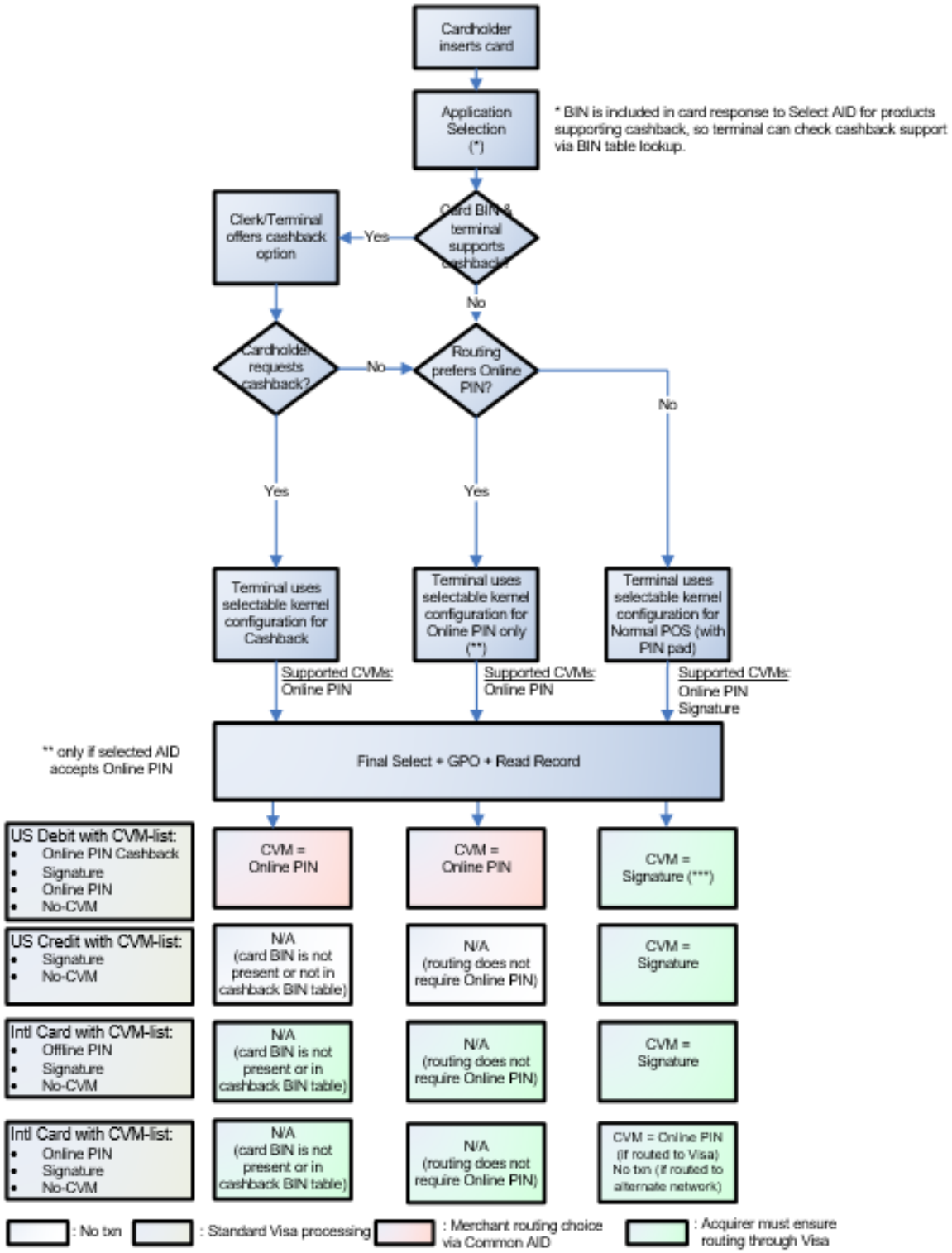
For the second cash back scenario, the terminal offers the cardholder a cash back choice before the card is presented. If the choice is accepted, in commencing Application Selection:

- 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]

[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.

Figure C–4: Combined CVM Processing and Selectable Kernel



*** These boxes represent the CVM Results (tag '9F34'). US Common Debit supports signature populated as No CVM in tag '9F34'. When the Visa AID is selected and CVM processing results in Signature, '9F34' will indicate Signature. When the Visa AID is selected, the transaction must be routed to Visa. Tag '9F34' will not be present in the authorization message for U.S. acquired transactions.

Appendix D. Abbreviations

Table D–1: Abbreviations

Abbreviations	Meaning
AAC	Application Authentication Cryptogram
AC	Application Cryptogram
ADVT	Acquirer Device Validation Toolkit
AFD	Automated Fuel Dispenser
AID	Application Identifier
AIP	Application Interchange Profile
ANSI	American National Standards Institute
ARPC	Authorization Response Cryptogram
ARQC	Authorization Request Cryptogram
ATC	Application Transaction Counter
ATM	Automated Teller Machine
AUC	Application Usage Control
BIN	Bank Identification Number
CA	Certificate Authority
CAM	Online Card Authentication (CAM is a previous acronym for Online Card Authentication)
CDET	Contactless Device Evaluation Toolkit
CDA	Combined DDA/Application Cryptogram (AC) Generation
CDCVM	Consumer Device Cardholder Verification Method
CTQ	Card Transaction Qualifiers
CVM	Cardholder Verification Method
CVR	Card Verification Results
CVV	Card Verification Value
DCC	Dynamic Currency Conversion
DDA	Dynamic Data Authentication
DDOL	Dynamic Data Authentication Data Object List
DES	Data Encryption Standard
EMV	EMV is a trademark dating back to 1999, and it refers to all of the specifications administered by EMVCo

Abbreviations	Meaning
fDDA	Fast Dynamic Data Authentication
FFI	Form Factor Indicator
IAC	Issuer Action Code
IAD	Issuer Application Data
ICC	Integrated Circuit Card
iCVV	ICC Card Verification Value
IEC	International Electrotechnical Commission
IFM	Interface Module
IPK	Issuer Public Key
ISO	International Organization for Standardization
L1	Level 1
L2	Level 2
L3	Level 3
ODA	Offline Data Authentication
PAN	Primary Account Number
PCD	Proximity Coupling Device
PCI SSC	Payment Card Industry Security Standards Council
PED	PIN Entry Device
PIN	Personal Identification Number
PIX	Proprietary Application Identifier Extension
POS	Point of Service/Point of Sale
PPSE	Proximity Payment Systems Environment
PSE	Payment Systems Environment
qVSDC	Quick Visa Smart Debit/Credit
RID	Registered Application Provider Identifier
RSA	Rivest, Shamir, Adleman (Public Key Technology)
SDA	Static Data Authentication
TAC	Terminal Action Code
TADG	Transaction Acceptance Device Guide
TADR	Transaction Acceptance Device Requirements
TC	Transaction Certificate

Abbreviations	Meaning
TCR	Transaction Component Record
TDES	Triple Data Encryption Standard (Triple-DES)
TVR	Terminal Verification Results
UCAT	Unattended Cardholder Activated Terminal
VCMS	VisaNet Certification Management Service
VCPS	Visa Contactless Payment Service
VIS	Visa Integrated Circuit Card Specification
VpTT	Visa payWave Test Tool
VSDC	Visa Smart Debit/Credit
VTS	Visa Test System

Appendix E. Glossary

Table E–1: Glossary

Term	Definition
Account Number Verification	Account Number Verification is an online authorization for a zero amount. It can be used to validate that the card used to make a reservation or to pay for services in advance of delivery is authentic.
Acquirer	A Visa client financial institution 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.
Acquirer Device Validation Toolkit (ADVT)	A set of test cards (or simulated test cards) and test cases used to validate new or upgraded EMV contact-chip devices.
American National Standards Institute (ANSI)	A U.S.A. standards accreditation organization.
Antenna	An antenna is embedded into a contactless card to allow the card to communicate with the contactless reader. The antenna may be placed around the border of the card, throughout the main area of the card, or within a small locale of the card.
Application Authentication Cryptogram (AAC)	A type of Application Cryptogram generated by the card at the end of offline and online declined transactions. The cryptogram is the result of card, device, and transaction data encrypted by a TDES key.
Application Cryptogram	A cryptogram generated by the card application.
Application Identifier (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) as described in ISO/IEC 7816-5.
Application Interchange Profile (AIP)	Information stored on the card that tells the terminal whether or not the card supports certain functions.
Application Label	An alphanumeric name used to identify each application associated with a VSDC account.
Application Preferred Name	An alphanumeric name associated with the VSDC application. It is displayed instead of the Application Label when the device supports the character set required by the Application Preferred Name.
Application Selection Indicator	A data element that indicates whether the associated AID in the device must match the AID in the card exactly, including the length of the AID, or only up to the length of the AID in the device.
Application Transaction Counter (ATC)	A counter on the chip card that provides a sequential reference to each transaction.

Term	Definition
Application Usage Control (AUC)	Controls similar to the Service Code that are placed on chip cards during card personalization to control where the card can be used, such as domestic vs. international, and the types of transactions the card can perform, such as a purchase or Cash Disbursement.
ATM Cash Disbursement	A Cash Disbursement obtained at a Visa or Plus ATM.
Authorization Request	An electronic request for an authorization sent to an issuer by a merchant or acquirer.
Authorization Request Cryptogram (ARQC)	A type of Application Cryptogram generated by the card for transactions requiring online authorization. The cryptogram is the result of card, device, and transaction data encrypted by a TDES key. The ARQC is used for a process called Online Card Authentication. The issuer validates the ARQC to help ensure that the card is authentic and card data and terminal data protected by the cryptogram has not been modified in transit.
Authorization Response	An issuer, authorizing processor, or stand-in processing reply to an authorization request or Account Number Verification generally resulting in an approval or a decline.
Authorization Response Cryptogram (ARPC)	A cryptogram used for a process called Online Issuer Authentication. This cryptogram is the result of the ARQC and the issuer's authorization response encrypted by a TDES key. It is sent to the card in the authorization response. The card validates the ARPC to ensure that it is communicating with the valid issuer and the issuer's authorization response has not been modified.
Automated Fuel Dispenser (AFD)	A self-service terminal or an automated dispensing machine that dispenses fuel such as gasoline, diesel fuel, or propane.
Automated Teller Machine (ATM)	An unattended device that has electronic capability, accepts PINs, and disburses currency or checks.
Candidate List	A list of applications mutually supported by both the card and the terminal. The Candidate List is built by the device during Application Selection.
Card	In general, the term "card" is used to describe the function performed by the VSDC or qVSDC application on the card.
Card Authentication	A means of validating whether a card used in a transaction is the genuine card issued by the issuer. See Online Card Authentication.
Card Authentication Method (CAM)	Previous terminology for the process now referred to as Online Card Authentication. See Online Card Authentication.
Card Verification Value (CVV)	An unpredictable check value encoded on the magnetic stripe or chip on a card. It is used to validate card information from the magnetic stripe during the authorization process and to detect counterfeit cards. The CVV is calculated from data encoded on the magnetic stripe using a secure cryptographic process. Also refer to iCVV.

Term	Definition
Cardholder Activated Device	See UCAT.
Cardholder Selection of the Application	Process by which the cardholder selects the application to be used for the transaction.
Cardholder Verification Method (CVM)	A method used to confirm the identity of a cardholder and, in some cases, also to signify cardholder acceptance of the transaction, such as signature, Offline PIN, and Online PIN.
Cardholder Verification Method List (CVM List)	An issuer-prioritized list of CVMs placed on the card during personalization that controls cardholder verification during transaction processing. The list on the card is used by the device to determine the appropriate CVM for each transaction.
Certificate Authority (CA)	In general, an entity responsible for establishing and vouching for the authenticity of public keys through issuance and management of public key certificates. For VSDC, Visa acts as a Certificate Authority (CA) for public key information related to Offline Data Authentication and Offline Enciphered PIN.
Chip Card	A plastic card embedded with an integrated circuit, or chip, that communicates information to a chip terminal. Chip cards offer increased functionality through the combination of significant computing power and substantial data storage.
Clearing	All of the functions necessary to collect a clearing record from an acquirer in the transaction currency and deliver it to the issuer in the billing currency, or to reverse this transaction.
Clearing Record	A record of a presentment or reversal in the format necessary to clear the transaction. Also referred to as a clearing transaction.
Combined DDA/Application Cryptogram Generation (CDA)	A type of Offline Data Authentication where the card combines generation of a cryptographic value (dynamic signature) for validation by the terminal with generation of the Application Cryptogram to ensure that the Application Cryptogram came from the valid card. (Note that CDA is not supported in qVSDC.)
Consumer Device CVM (CDCVM)	A Cardholder Verification Method performed on and verified by the consumer's device (e.g., mobile phone, watch, wearable), independent of the terminal.
Contactless	A chip transaction where the communication between the card and the device takes place over a contactless interface using Radio Frequency Identification (RFID) technology. In this document, a contactless transaction is based on quick Visa Smart Debit/Credit (qVSDC).
Contactless Device Evaluation Toolkit (CDET)	A set of simulated test cards and test cases used to validate new or upgraded contactless-chip devices.
Contactless Symbol	See EMV Contactless Symbol for details.

Term	Definition
Cryptogram	A value resulting from a combination of specific key data elements that are used to validate the source and integrity of data. Cryptograms used for VSDC are the Authorization Request Cryptogram (ARQC), Authorization Response Cryptogram (ARPC), Transaction Certificate (TC), and Application Authorization Cryptogram (AAC).
Cryptography	The study of mathematical techniques for providing aspects of information security, such as confidentiality, data integrity, authentication, and nonrepudiation.
Data Encryption Standard (DES)	The data encryption standard defined in ISO/IEC (16609 for DES, 18033-3 for TDES).
Default Dynamic Data Authentication Data Object List (Default DDOL)	The device value used when the card does not pass its own DDOL to the device.
Device	A device that accepts and processes Visa, Visa Electron, and/or Plus transactions. Also referred to as a "transaction acceptance device."
Device Management System	A system used by acquirers and merchants to track and update POS devices. Also referred to as a Terminal Management System (TMS).
Dual Interface Terminal	A terminal that supports both contact and contactless cards. The terminal may enable this support by having a contactless reader attached to it to facilitate contactless acceptance or alternatively have contact and contactless-chip capabilities integrated into the one device.
Dynamic Currency Conversion (DCC)	Dynamic Currency Conversion (DCC) is either: • The conversion of the purchase price of goods or services from the currency in which the purchase price is displayed to the cardholder's billing currency. That currency then becomes the transaction currency. • An ATM Transaction in which the Transaction Currency is different to the currency disbursed. DCC is not a Visa service, but merchants and ATMs may offer it through their acquiring bank.
Dynamic Data Authentication (DDA)	A type of Offline Data Authentication in which the device validates a cryptographic value generated by the card during the transaction. This validation helps to ensure that the card data has not been copied (skimmed) from a different card and that the card is not counterfeit.
Dynamic Data Authentication Data Object List (DDOL)	The card-originated data element that is used for constructing the INTERNAL AUTHENTICATE command.
EMV Contactless Specifications for Payment Systems ("EMV Contactless Specifications")	Technical specifications developed by EMVCo outlining the interaction between contactless-chip cards (and other form factors such as mobile phones) and devices to ensure interoperability for payment systems.

Term	Definition
EMV Contactless Symbol	A symbol that is placed on contactless devices to indicate contactless acceptance.
EMV Integrated Circuit Card Specifications for Payment Systems ("EMV Chip Specifications")	Technical specifications developed by EMVCo outlining the interaction between contact-chip cards and devices to ensure interoperability for payment systems.
EMVCo LLC (EMVCo)	Industry organization that manages, maintains, and enhances the *EMV Chip Specifications* and *EMV Contactless Specifications* (among other specifications). Members are American Express, Discover, JCB International, Mastercard Worldwide, UnionPay, and Visa Inc.
Fallback	A magnetic stripe transaction that takes place with a chip card in a chip device, typically due to an inoperative chip on the card or a malfunction of the chip reader.
Fast DDA (fDDA)	A faster version of DDA that is suitable to the requirements of a contactless transaction. During fDDA, the device validates a cryptographic value generated by the card during the transaction. This validation ensures that the card data has not been copied (skimmed) and that the card is not counterfeit.
Field 55 (F55)	The standard location identified by ISO as a more flexible message architecture to carry chip data in ISO authorized messages sent and received by acquirers and issuers.
Floor Limit	A currency amount that is established for single transactions at specific types of merchants, above which an authorization is required. These limits are defined in the *Visa Rules*.
Form Factor Indicator (FFI)	Indicates the form factor of the consumer device and the type of contactless interface over which the transaction was conducted. This information is made available to the issuer host. Examples include card, mobile phone, and key fob.
ICC Card Verification Value (iCVV)	An alternate CVV for chip-initiated transactions calculated using slightly different data than what is encoded in the magnetic stripe data portion of the chip. See Card Verification Value (CVV).
Incremental Authorization	Where the final amount will exceed or is likely to exceed the amount of the pre-authorization, one or more further incremental authorizations may be obtained. The incremental authorization(s) will be for the difference between the original pre-authorization and the actual or estimated final amount.
Integrated Circuit Card (ICC)	See Chip Card.
Interface Module (IFM)	The hardware or chip reader developed to the *EMV Chip Specifications* that provides physical communication with the chip card.
International Organization of Standardization (ISO)	The specialized international agency that establishes and publishes international technical standards.

Term	Definition
Issuer	A Visa client financial institution that issues cards and whose name appears on the card as the issuer (or, for cards that do not identify the issuer, the financial institution that enters into the contractual relationship with the cardholder).
Issuer Action Code (IAC)	A code placed on the card by the issuer during card personalization. IACs indicate the issuer's preferences for declining transactions offline, sending transactions online to the issuer, or declining transactions offline if they are unable to go online, based on the risk management performed. The terminal uses these settings when determining whether to request an offline approval, offline decline, or to go online for authorization.
Issuer Application Data	A data element that contains proprietary application data for transmission to the issuer in an online transaction.
Issuer Authentication	See Online Issuer Authentication.
Issuer Public Key (IPK)	The public key part of an issuer's public/private key pair, which is to be used with a specific Visa product or service. The IPK is contained in an IPK Certificate issued by the CA. See also Issuer Public Key Certificate.
Issuer Public Key Certificate	An IPK and associated data signed by the VSDC CA Private Key. The certificate is loaded on the card during personalization and used by the card and device during Offline Data Authentication to help validate that the card comes from a valid issuer.
Issuer Script	A process by which an issuer can update the electronically stored contents of chip cards without reissuing the cards. Issuer Script commands include blocking and unblocking an account, blocking the entire card, changing the cardholder's PIN, and changing the cardholder's Authorization Controls.
Kernel	A piece of software developed to the *EMV Chip Specifications* or *EMV Contactless Specifications* that interacts with the chip card and is integrated into the device application.
Key Management	The handling of cryptographic keys and other related security parameters during the entire lifecycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.
Key-Entered Transaction	A transaction where the account number is manually entered into the device to process the transaction. Also called a manual transaction.
Magnetic Stripe	The magnetic stripe on a card that is encoded with the necessary information to complete a transaction.
Magnetic Stripe Device	A device that reads the magnetic stripe on a card.
Merchandise Return/Refund	An online authorization message and associated clearing message to return goods/services for a refund. The transaction results in a credit to the cardholder's account for the amount of the returned goods/services. Both full and partial refunds of the original transaction may be performed.
N/A	Not applicable

Term	Definition
Offline Approval	A transaction that is positively completed (approved) at the point of transaction between the card and device without an online response from the issuer.
Offline Capable Device	A chip device that supports both offline and online processing.
Offline Data Authentication	A process whereby the card is validated at the point of transaction using RSA public key technology to protect against counterfeit or skimming.
Offline Decline	A transaction that is negatively completed (declined) at the point of transaction between the card and terminal without an online response from the issuer.
Offline Enciphered PIN	A CVM defined in EMV in which the cardholder PIN is entered at a POS device, encrypted with an ICC public key, and sent to the card where it is validated.
Offline PIN	A PIN stored on the card that is validated at the point of transaction between the card and device. Offline PIN is supported for contact-chip transactions but it is not supported for contactless-chip transactions.
Offline Plaintext PIN	Offline PIN processing in which the PIN entered by the cardholder is sent unencrypted (in plaintext) from the card reader PIN pad to the chip card for verification.
Offline Transaction	A transaction that takes place without an online authorization response.
Offline/Online Device	A device that is able to approve transactions offline but is also able to send transactions online for issuer processing.
Online Authorization	A method of requesting an authorization through a data communications network other than voice to an issuer, an authorizing processor, or stand-in processing.
Online Card Authentication	Validation of the card by the issuer to protect against data manipulation and data copying. See also Authorization Request Cryptogram (ARQC).
Online Issuer Authentication	Validation of the issuer by the card to ensure the integrity of the issuer. Also known as Issuer Authentication and Host Authentication. See also Authorization Response Cryptogram (ARPC).
Online PIN	A process used to verify the cardholder's identity by sending an encrypted PIN to the issuer or the issuer's agent for validation in an authorization request.
Online-Only Device	A device that requires that all transactions be sent online for authorization.
Partial Name Selection	The Application Selection process where the device AID uses only a partial name.
Payment Card Industry Security Standards Council (PCI SSC)	A consortium of payment card industry representatives, which became formalized as the PCI Security Standards Council.

Term	Definition
Payment Systems Environment (PSE)	The data element on a chip card that contains a list of applications supported on the card. The PSE is used during the Directory Selection Method of Application Selection.
PCI Data Security Standard (PCI DSS)	The PCI DSS is a widely accepted set of policies and procedures intended to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information.
PCI Payment Application Data Security Standard (PA-DSS)	PCI requirements relating to application security.
PCI PIN Transaction Security (PTS)	PCI requirements relating to PIN security formerly known as PCI-PED.
Personal Identification Number (PIN)	A numeric code of 4 to 12 characters that is used to verify cardholders at a customer-activated PIN pad. PINs can be verified online by the issuer or sent to the chip card for Offline PIN verification. See Online PIN and Offline PIN.
PIN Entry Device (PED)	A secure device that allows cardholders to enter their PINs.
Point of Sale (POS)	The physical location where a merchant or acquirer (in a face-to-face environment) or a UCAT (in an unattended environment) completes a transaction. Also called point of service or point of transaction.
Point of Service (POS)	See Point of Sale (POS).
Point of Transaction (POT)	See Point of Sale (POS).
Preliminary Processing	A phase during a qVSDC transaction that takes place prior to the contactless card interacting with the contactless reader. During this phase, the reader performs specific processing using the amount to expedite the transaction.
Primary Account Number (PAN)	An issuer-assigned number that identifies a cardholder's account. Also referred to as the Application Primary Account Number.
Private Key	The private (secret) component of an asymmetric key pair. The private key is always kept secret by its owner. It may be used to digitally sign messages for authentication purposes and to decrypt messages for confidentiality purposes (e.g., PIN).
Proximity Coupling Device (PCD)	The reader/writing device that uses inductive coupling to provide power to the consumer device, such as a contactless card or a cell phone, and also to control the data exchange with the consumer device.
Proximity Payments Systems Environment (PPSE)	A list of supported Application Identifiers (AIDs), Application Labels, and Application Priority Indicators for applications that are accessible over the contactless interface.
Public Key	The public component of an asymmetric key pair. The public key can be publicly exposed and available to users. In RSA, the public key consists of the public key exponent and the modulus.

Term	Definition
Public Key Algorithm	A cryptographic algorithm that allows the secure exchange of information and message authentication but that does not require a shared secret key, through the use of two related keys: a public key that may be distributed in the clear and a private key that is kept secret.
Public Key Certificate	A public key signed by the CA to prove origin/integrity.
Public Key Pair	The two mathematically related keys, a public key and a private key, which, when used with the appropriate public key algorithm, can allow the secure exchange of information and message authentication, without the secure exchange of a secret.
Quick Chip for Contact and Contactless	Quick Chip for EMV® Chip is a solution that speeds up checkout times on chip transactions at the POS and optimizes the consumer experience. Quick Chip allows customers to remove their card from the terminal before the transaction amount is finalized or before the authorization response has been received.
quick VSDC (qVSDC)	Visa's solution for contactless card acceptance. qVSDC is a minimized EMV transaction over the contactless interface where multiple EMV commands are compressed into fewer commands to streamline and expedite transaction processing.
RSA	A public key cryptosystem developed by Rivest, Shamir, and Adleman. It is used for data encryption and authentication. For VSDC, RSA is used for Offline Data Authentication and Offline Enciphered PIN.
Random Selection	A capability of an online-capable EMV-compliant device that allows for random selection of transactions for online processing.
Reader Cardholder Verification Method (CVM) Required Limit	A limit in the contactless device. When the transaction amount is above this limit, the contactless transaction requires cardholder verification.
Reader Contactless Floor Limit	A limit in the contactless device. When the transaction amount is above this limit, the transaction must be sent online.
Reader Contactless Transaction Limit	A limit in the contactless device. When the transaction amount is above this limit, a contactless transaction is not permitted (although, the transaction may proceed over another interface). All new contactless readers must have this limit disabled or set to its maximum value.
Reversal	An online message that is used to notify the issuer that the previous online authorization response was not received by the device. For chip, it is also used when the issuer approved an online authorization but the device declines the transaction (e.g., due to Issuer Authentication failure).
Sale Completion	The financial settlement of a previously authorized transaction (usually a pre-authorization and its associated incremental authorization(s) (as applicable), often where the cardholder and card are no longer present.

Term	Definition
Secure Hash Algorithm (SHA-1)	This algorithm is standardized as ISO/IEC 10118-3. SHA-1 takes as input messages of arbitrary length and produces a 20-byte hash value.
Selectable Kernel	A method defined in EMV where a terminal can change certain capabilities (e.g., supported CVMs) depending on transaction characteristics (e.g., amount or cash back transaction).
Service Code	Digits encoded on a magnetic stripe and replicated on the chip that identifies the circumstances under which the card is valid (e.g., international transactions, domestic transactions, restricted card use), and defines requirements for processing a transaction with the card (e.g., chip-enabled, cardholder verification, online authorization).
Skimming	A method of capturing the contents of a legitimate credit or debit card which are then copied onto another card to be used for counterfeit transactions.
Stand-In Processing (STIP)	A component of VisaNet that provides authorization services on behalf of an issuer when the issuer or its processor is unavailable or other STIP criteria are met.
Static Data Authentication (SDA)	A type of Offline Data Authentication where the device validates a cryptographic value placed on the card during personalization. The validation protects against altering data on the card after personalization but does not prevent skimming.
Status Check	An online authorization for a single unit of currency to verify the account. The use of a status check is limited to automated fuel dispensing.
Symmetric Algorithm	An algorithm in which the key used for encryption is identical to the key used for decryption. TDES is the best known symmetric encryption algorithm.
Terminal	See Device.
Terminal Action Code (TAC)	Visa-defined rules in the device which the device uses to determine whether a transaction should be declined offline, sent online for an authorization, or declined if online is not available.
Terminal Floor Limit	A data element that indicates the transaction amount equal to or greater than which the device will send the transaction online.
Terminal Risk Management	Offline checks, such as floor limit checks and exception file checks, that are performed by devices capable of supporting an offline transaction.
Terminal Verification Results (TVR)	A set of indicators from the VSDC device, recording the results of the transaction. These indicators are available to issuers in the online message and clearing transaction.
Track 2 Equivalent Data	A representation of the Track 2 data from the magnetic stripe which is encoded on the chip.
Transaction Acceptance Device (TAD)	See Device.

Term	Definition
Transaction Acceptance Device Guide (TADG)	A document that provides vendors, merchants, acquirers, and device deployers with information to help them deploy transaction acceptance devices ("devices") that support the acceptance of Visa payment cards. It focuses on contact-chip and contactless-chip card (and other form factor) acceptance but also provides information on magnetic-stripe and key-entered transactions for completeness.
Transaction Acceptance Device Guide (TADR)	A document that outlines the requirements for contact and contactless devices that are not covered in the *Visa Rules*.
Transaction Certificate (TC)	A type of Application Cryptogram generated by the card at the end of offline and online approved transactions. The cryptogram is the result of card, device, and transaction data encrypted by a TDES key.
Transaction Type	A data element that indicates the type of financial transaction, represented by the values of the first two digits of the Processing Code as defined by Visa.
Triple Data Encryption Standard (TDES)	TDES (also referred to as Triple Data Encryption Algorithm/TDEA) as defined in ISO/IEC 18033 Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers. It is the data standard used with single-, double-, or triple-length DES keys.
Unattended Cardholder Activated Terminal (UCAT)	A cardholder-operated device that reads, captures, and transmits card information in an unattended environment.
Unpredictable Number	A value used to provide variability and unpredictability to the generation of the Application Cryptogram.
Visa Contactless Payment Specification (VCPS)	The Visa specification for contactless payments utilizing qVSDC.
Visa Easy Payment Service (VEPS)	A service that permits qualified merchants to process small value transactions in a card-present environment without requiring cardholder verification or the issuance of a transaction receipt unless requested by the cardholder. This service no longer applies to the U.S. region.
Visa Electron	A Visa payment product offered exclusively outside of the U.S. region aimed at cardholders that are developing banking relationships. Visa Electron cards have greater usage restrictions and transactions are always processed online. Visa Electron cards are accepted in the U.S. region, though processed as a Visa transaction.
Visa Integrated Circuit Card Specification (VIS)	Chip card and application specifications developed by Visa for VSDC contact-chip programs. VIS serves as a companion guide to the *EMV Chip Specifications*.
Visa ISO AID	An AID that starts with the Visa ISO Registered Application Identifier (RID) 'A0 00 00 00 03'.
Visa payWave Test Tool (VpTT)	The mandated Europe region tool to test Visa payWave contactless acceptance devices against the Europe region's implementation requirements.

Term	Definition
Visa Rules	The short reference for the *Visa Core Rules and Visa Product and Service Rules*. These are the Visa rules that are designed to minimize risks and provide a common, convenient, secure, and reliable global payment experience while supporting geography-specific rules that allow for variations and unique marketplace needs.
Visa Smart Debit/Credit (VSDC)	The Visa service offerings for chip-based debit and credit programs. These services, based on the EMV and VIS specifications, are supported by VisaNet processing, as well as by the *Visa Rules*.
VisaNet Integrated Payment (V.I.P.) System	The systems and services through which Visa delivers online financial processing, authorization, clearing, and settlement services to clients.
VSDC Certificate Authority (CA)	An entity that issues and manages digital certificates for use on Visa chip cards in accordance with Visa specified requirements.
VSDC Certificate Authority (CA) Public Keys	The Visa Public Keys that reside in devices to support Offline Data Authentication and Offline Enciphered PIN.
Zero-Floor Limit	A floor limit with a currency amount of zero. Online authorization is required for all zero-floor limit transactions.