Transaction Acceptance Device Guide (TADG)

Version 3.2

Effective: January 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.

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 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[1] acceptance but also provides information on magnetic-stripe and key-entered transactions for completeness.

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

This is a public document available at www.visa.com/tadg.

Audience

This document is the main handbook for terminals and is intended for:

- Vendors who are developing, integrating, or testing devices to support acceptance of Visa cards
- Acquirers and merchants creating requirements for devices
- Acquirers, merchants, and device deployers creating, developing, testing, or deploying an infrastructure for acceptance

Acquirers should use this document in conjunction with one of the following documents available on Visa Access:

- **Non-U.S. Acquirers** – VSDC Contact and Contactless Global Acquirer Implementation Guide
- **U.S. Acquirers** – VSDC Contact and Contactless U.S. Acquirer Implementation Guide

Document Purpose

This document serves as a reference guide for vendors, merchants, acquirers, and device deployers. Users of this document can refer to it when needed to understand the best practices and requirements associated with a given topic. This document also points to more detailed documents, where appropriate.

[1] This includes cards and other form factors such as mobile phones and wearables.

Scope

In scope:

- Contact-chip transactions based on both of the following:
  - *EMV®*[2] *Integrated Circuit Card Specifications for Payment Systems* ("*EMV Chip Specifications*"), Version 4.3
  - *Visa ICC Specifications (VIS)*, Version 1.5 or later
- Contactless-chip transactions based on either of the following:
  - *EMV Contactless Specifications for Payment Systems*, including Book C-3 ("*EMV Contactless Specifications*"), Version 2.6
  - *Visa Contactless Payment Specification (VCPS)*, Version 2.1[3] or later
- Magnetic-stripe and key-entered transactions (covered at a high-level for completeness)

Out of scope:

- Magnetic Stripe Data (MSD) contactless transactions
- Transit transactions (see Section 10.3: Visa Documents for references)
- Device-to-acquirer messaging (which is outside Visa's scope)
- Acquirer-to-VisaNet messaging (except in a few instances for clarification) (see the *VSDC System Technical Manual* for details)

Note: Most region-specific requirements are not covered in 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."

[2] 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.

[3] Contact your Visa representative for the specific *VCPS* compliance requirements in your region.

- **Device** – The hardware used to accept a chip card in order to conduct a transaction. Used interchangeably with the term "terminal." 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 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."
- **Transaction Acceptance Device –** See the definition for "device."
- **VSDC** – See the definition for "chip."

For more information, see Appendix D: 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:

- **Contact** – Devices accepting Visa EMV-compliant contact chip cards must comply with the *EMV Chip Specifications*
- **Contactless** – Devices accepting Visa contactless cards must comply with the *EMV Contactless Specifications* including Book C–3 or the *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)*
  - *Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*
  - *PCI PIN Security Requirements*
- **Europe Region** – Device vendors servicing the Europe region should also refer to the *Visa Europe Contactless Terminal Requirements and Implementation Guide* which can be obtained by contacting the Europe region at chipven@visa.com

Note: See Section 10: References for a list of all reference materials and where to obtain them.

Document Organization

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

Section 1: Background – Provides background information on the transaction types, acceptance environments, and processing options covered in this guide.

Section 2: General Acceptance – Provides an overview of the general device requirements and best practices that apply to all devices (magnetic stripe, contact chip, and contactless) and all acceptance environments.

Section 3: Magnetic-Stripe Acceptance – Provides an overview of the requirements and recommendations for devices that accept magnetic-stripe cards.

Section 4: Contact-Chip Acceptance – Provides an overview of the EMV and VIS requirements and recommendations for contact-chip devices.

Section 5: Contactless-Chip Acceptance – Provides an overview of the *VCPS* and *EMV Contactless Specifications* requirements and recommendations for contactless devices focusing on quick Visa Smart Debit/Credit (qVSDC).

Section 6: Chip-Card Processing – Focuses on how to process specific transaction types initiated via a contact or contactless card.

Section 7: Security Characteristics – Outlines security requirements and characteristics for devices.

Section 8: Device Design, Deployment, and Management – Outlines recommendations for contact and contactless device design, deployment, and management.

Section 9: Device Testing – Provides information on the device testing activities required prior to device deployment.

Section 10: References – Provides a reference to the documents listed throughout this guide as well as other references.

Appendix A: Contactless Reader Placement – Outlines recommendations for the placement of contactless readers in a merchant retail environment where the contactless reader is a separate unit.

Appendix B: Visa U.S. Common Debit AID (U.S. Only) – Outlines Visa’s approach for supporting the Visa U.S. Common Debit AID at POS and ATMs.

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

Appendix D: 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 restructure it to remove duplication with other documents (mainly, the *VSDC Contact and Contactless Acquirer Implementation Guide*[4]). With the restructuring of these two documents, the *Transaction Acceptance Device Guide* now serves as the main handbook for information on terminals while the *VSDC Contact and Contactless Acquirer Implementation Guide*[4] provides an implementation guide for acquirers.

In addition, a few material changes were made to this document to align it with the *Visa Rules*, chip specifications, and VisaNet manuals and business enhancements:

Table 1: Summary of Material Changes for Version 3.2

Item	Description	Section
Signature	While attended POS device kernels (other than VEPS-only devices) must support signature, the merchant is no longer required to capture and verify the cardholder's signature at a chip device.	2.8.2: CVMs by Device Type
Cardholder Device Cardholder Verification Method (CDCVM)	Contactless devices must support CDCVM.	2.8.2: CVMs by Device Type
Dynamic Currency Conversion (DCC)	Service has been expanded to ATMs.	2.17: Dynamic Currency Conversion (DCC)
Contactless Symbol	Contactless devices must display the EMV Contactless Symbol.	2.16: Visa Branding of Payment Terminals 5.4: Device User Interface Recommendations
Terminal Action Codes (TACs)	TAC values have been updated.	4.10.1: Terminal Action Codes (TACs)
Account Number Verification	When initiated via a chip card, Account Number Verification messages must contain chip data.	6.4.5: Account Number Verifications
Merchandise Returns	Merchandise Returns must include an online authorization message (they can no longer be processed as a clearing transaction only).	6.4.6: Merchandise Returns/Refunds

[4] A U.S.-specific guide is available for U.S. acquirers (the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide*).

Item	Description	Section
Cash Back	Credit cards may be used for cash back transactions.	6.6.1: General Cash Back Requirements
Cash Back Cryptogram Transaction Type	The Cryptogram Transaction Type for cash back has been changed from 09 to 00.	6.6.2: Chip Cash Back Requirements
Appendices	The following appendices have been deleted: • Appendix A: Track 1 Data Specifications – Information covered in *Payment Technology Standards Manual* • Appendix B: Track 2 Data Specifications – Information covered in *Payment Technology Standards Manual* • Appendix C: Device Performance for EMV Transactions – Information outdated • Appendix D: EMV Tag to VisaNet Data Element Mapping – Information covered in the *VSDC System Technical Manual* • Appendix G: Contactless ATM Requirements • Appendix H: Region and Country Specific Requirements and Recommendations – Information not in scope **Note:** Appendix B: Visa U.S. Common Debit AID (U.S. Only) (previously Appendix F) remains intact from the previous version of this document and has not been changed.	

1. Background

This section provides background information on the transaction types, acceptance environments, and processing options covered in this guide.

1.1 Transaction Types

This guide covers three main types of transactions:

- **Magnetic-Stripe Transactions** – A magnetic stripe is used to initiate the transaction.
- **Contact-Chip Transactions** – A contact chip is used to initiate the transaction.
- **Contactless-Chip Transactions** – A contactless chip is used to initiate the transaction.

Each of these transactions is uniquely identified through the POS Entry Mode (Field 22) while the Terminal Entry Capability (Field 60.2) identifies the type of device.

In addition, this document also provides brief information on key-entered/manual transactions for completeness.

1.2 Acceptance Environments

This guide covers three types of acceptance environments:

- Attended POS Devices
- Unattended Cardholder Activated Terminals (UCATs)
- Automated Teller Machines (ATMs)

Where the information in this document applies to all devices, the term "device" is used. Where the information is specific to a certain type of device, the document refers to the device type.

1.2.1 Attended POS Devices

At an attended POS device, the card, cardholder, and clerk are present, and the cardholder makes a purchase (or related transaction) for goods/services. These devices can range from simple standalone devices used solely for the purpose of processing payment card transactions to more complex integrated POS systems or multilane devices such as those used in mass merchandise and grocery stores.

While the more complex solutions may support functionality beyond payment (e.g., product code scanning, inventory management, frequent shopper programs and coupon processing, accounting, and security/staff tracking), the information in this document focuses on payment processing.

1.2.2 Unattended Cardholder Activated Terminals (UCATs)

Unattended Cardholder Activated Terminals (UCATs) (also referred to as Unattended Acceptance Terminals) are devices managed by a merchant 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 cardholder activated fuel pumps (also called automated fuel dispensers, AFDs), self-service vending units, and self-service devices in parking garages or at parking meters.

UCATs may also dispense cash but when dispensing cash they function as an ATM and must adhere to the rules for ATMs. They may dispense either cash or goods/services in a single transaction but not both.

Note: Attended Cardholder Activated Terminals (also called Semi-Attended Cardholder Activated Terminals) such as self-checkout terminals in supermarkets, are not considered UCATs; therefore, they are not required to meet UCAT requirements.

Note: The *Visa Rules* prohibit Visa card products from being used for scrip transactions so information on UCATs that dispense scrip is not covered. (Scrip is a two-part paper receipt redeemable for goods, services, or cash.)

1.2.3 Automated Teller Machines (ATMs)

Automated Teller Machines (ATMs), also known as Automated Banking Machines (ABMs) or cash machines, are unattended devices that dispense cash and only 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.

In addition to Cash Disbursements, ATMs may support additional financial-related functions, such as Balance Inquiries and Funds Transfers. In certain countries, they may also provide PIN change facilities.

ATMs can provide goods or services (e.g., stamp purchases), but in these scenarios they operate according to the rules for UCATs rather than ATMs. See previous section for details.

ATMs always require Online PIN. In the majority of scenarios, the transaction is sent online for processing (although a chip transaction may be declined offline for the “Service Not Allowed” setting).

1.3 Processing Options

Merchants and acquirers process transactions using batch or real-time processing and device or host capture.

1.3.1 Dual- or Single-Message Processing

Transactions may be processed using dual message (one message for authorization and a second one for clearing) or single message (one message for both authorization and clearing). The method used depends on the acceptance environment, the acquirer capabilities, and local requirements. The transaction data may be captured either at the device or at the acquirer host (see next section for details).

The following provides an overview of dual- vs. single-message processing:

- **Dual Message** – This involves the exchange of data twice. The authorization occurs at the time of the purchase or Cash Disbursement transaction using one message and then the transaction is cleared later using another message. The clearing messages are usually gathered into a batch for POS devices. The batch is then sent to the acquirer as part of end-of-day (or end-of-cycle) processing. Non-batched systems may simply submit a series of clearing advices based on their transaction logs prior to end of day (or end of cycle). Device-capture and acquirer host-capture systems typically use dual-message processing.
- **Single Message** – Where the final amount is known at the time of authorization, a single message is used to authorize and clear the transaction (i.e., the online authorization message provides the issuer with all the information required to clear the transaction and post it to the cardholder’s account). Single message is also referred to as real-time processing.
    - Single-message merchants, particularly those in travel and entertainment segments, may use an authorization message (0100) followed by a sale completion (0220 or 0320) rather than a full financial message (0200). In these cases, the considerations are very similar to dual-message merchants.

Environments such as fuel retailing, where the final amount is generally not known at the time of authorization, may use a mix of dual- and single-message processing. For more information, see Section 6.5.2: Fuel/Petrol Dispensing.

1.3.2 Device-Capture vs. Host-Capture Systems

The following provides an overview of device vs. host-capture systems:

- **Device-Capture Systems** – The device creates the clearing message by combining the data from the authorization response with the data from the authorization request. The device then submits the clearing message to the acquirer.
- **Host-Capture Systems** – Before sending the authorization request to the issuer, the acquirer host retains a copy of the authorization and uses it along with data in the authorization response to create the clearing message. A device attached to a host-capture system may have a shadow (copy) of the clearing batch, but the shadow is only for informational or error recovery purposes. For devices using host capture, transactions appear to be single message because the acquirer is responsible for generating the clearing message.

Important: Regardless of device/host capture or single/dual messaging, offline-authorized chip transactions only consist of a clearing message.

For implications related to chip transactions, see Section 4.12.3: Online-Authorized Transaction Scenarios.

2. General Acceptance

This section provides an overview of the general device requirements and best practices that apply to all interfaces (magnetic stripe, contact chip, and contactless) and all acceptance environments, unless otherwise noted.

2.1 Primary Account Number (PAN) Recognition and Processing

This section outlines requirements for recognizing and processing PANs:

Table 2–1: PAN Requirements

Requirement	Description
General	A device accepting Visa and Visa Electron cards must accept all valid Primary Account Numbers (PANs).
19 Digit PANs	**ATMs** – ATMs accepting Plus cards must accept PANs up to 19 digits that contain a valid BIN registered with the Visa Plus program. The device must transmit the full PAN to the acquirer.
	Chip Devices – 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. • **Europe Region** – Acquirers must support transactions with 19-digit PANs in VisaNet messages. • **Outside of the Europe Region** – 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. **Note:** Support for 19-digit PANs is strongly recommended in those countries where it is not required.
Account-Number-Verifying POS Devices	In some countries, merchants may have installed account-number-verifying POS devices to aid in detecting counterfeit cards. These devices read the PAN from the track data and compare the last four digits to the key-entered last four digits of the embossed or printed PAN. This test is **not** recommended for devices that accept contact- or contactless-chip cards because chip cards may contain multiple payment applications (each with a unique PAN), of which only one PAN will appear on the front of the card; therefore, a valid multi-application card could erroneously fail this test.

2.2 Expiration Date

Requirements for expiration date processing:

- **Future Expiration Dates** – Because Visa does not impose a global upper limit for expiration dates on Visa cards, POS devices should not validate whether expiration dates are too far out in the future.[5] This type of validation can lead to erroneous declines.
- **ATMs** – ATMs must not return or decline a transaction based on the expiration date. They must accept the transaction, even if the card has expired, and route the transaction online for issuer authorization.
- **Contact-Chip Transactions** – During a contact-chip transaction, the expiration date will be checked and the device may take action on the expiration date based on normal EMV processing; however, the acquirer and the device should not interrogate the expiration date above and beyond normal EMV processing.
- **Expiration Date Testing** – Device vendors and deployers should ensure devices are tested with a wide variety of card expiration dates prior to production rollout to ensure that there are no rejections of valid date formats.

2.3 Account Selection

Account selection allows cardholders to select one of multiple sources of funds associated with the card or selected payment application at the time of the transaction.

Certain countries have defined rules for the selection of an account at the POS via the use of soft keys or dedicated keys on the device. The rules associated with the routing of these transactions and their use is defined according to local regulations and is not mandated by Visa.

Visa does not require that account selection be supported. If the merchant or acquirer offers account selection, Visa recommends that it offer a full range of options:

- Checking or current account
- Savings account
- Credit line account

Account selection at the POS or ATM is likely to be used only where multiple accounts are connected with a single credit or debit PAN. Account selection at the ATM may also extend to lines of credit associated with a Plus-only application.

[5] This does not preclude chip devices from performing expiration date checking per standard EMV chip processing.

Note: Account selection as described in this section is different from the EMV Application Selection process which is covered in Section 5.2.2: Application Selection.

2.4 Multiple Languages

Depending on the geographic location, devices may need to communicate in multiple languages to help merchants improve customer service. It is recommended that all devices support the display of multiple languages and characters for PIN entry prompts and/or cardholder selection of the application.

2.5 Device Messages

Device messages are displayed to let the merchant or cardholder know the status of a transaction and what action, if any, to take next. To ensure clear and effective messages, vendors should follow these basic principles:

Table 2–2: Device Messages Requirements

Requirement	Description
Instructive Messages	The message displayed should clearly instruct the merchant or cardholder on what action to take.
Clear Responses	Where the message is used to convey an issuer response, the message should clearly communicate the meaning of the response.
Amount/Currency and PIN Entry	Assuming the final amount and currency are known at the beginning of the transaction, they should be displayed to the customer prior to PIN entry (where PIN is applicable). The cardholder should be prompted to confirm the transaction currency and amount, and PIN entry is an acceptable method of confirmation. If PIN entry is requested before the transaction amount is known, an explicit amount confirmation message should be displayed to the cardholder once the amount is known.
Transaction Status	The message displayed should clearly indicate the status of the transaction. Transaction status is defined by one of four basic conditions or events: • Transaction is approved • Transaction is declined • Requested service is not available or not allowed • Error occurred on the transaction
Next Action/Instructions	Once the status of the transaction is determined, the device should communicate the next action. Clear instructions are especially important when an error occurs and the transaction is terminated.
Error Messages	Error messages for chip transactions should be closely aligned with messages for magnetic-stripe transactions. Messages for magnetic-stripe transactions should be upgraded if they do not already meet these principles.

For the specific device messages for contact and contactless devices, refer to the *EMV Chip Specifications* and the *EMV Contactless Specifications*.

Note: Certain Visa regions have specific requirements for the information that is displayed to the cardholder during a contactless transaction. Given the faster nature of a contactless transaction, other forms of messaging such as LED indicators and sound cues are used. Contact your Visa representative for details.

2.6 Accessibility Requirements

Device vendors and acquirers are responsible for ensuring that all customer-facing devices adhere to any and all accessibility requirements for the countries in which they operate and for the countries in which the devices are installed. In the absence of sufficient requirements, it is recommended that vendors, merchants, and acquirers support accessibility to persons with physical disabilities.

2.7 Transaction Receipts

This section outlines requirements for receipts.

The *Visa Rules* specify receipt requirements including those for manual receipts, electronic receipts (see Section 2.7.6: Electronic Receipts for details), travel and entertainment, Dynamic Currency Conversion (DCC), and aggregated transactions.

2.7.1 General Receipt Requirements

Except for certain transactions, such as qualifying VEPS transactions (see Section 2.14: Visa Easy Payment Service (VEPS) for details), merchants must be able to provide the cardholder with a written or printed receipt at the completion of the transaction.

2.7.2 ATM Receipt Requirements

ATM receipt requirements are the same as for POS receipts. There are no special receipt requirements for ATMs.

2.7.3 UCAT Receipt Requirements

If a receipt is not provided automatically, a UCAT must inform the cardholder that a receipt is available upon request.

2.7.4 Consumer Data on Receipts and Displays

The Payment Card Industry Data Security Standard (PCI DSS), Requirement 3.3 states: Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see the full PAN.

In light of this rule, Visa recommends that all but the last four digits are suppressed on receipts and displays.

Note (U.S.): Receipts in the U.S. must suppress all but the last four digits of the PAN and must not display/print the expiration date.

2.7.5 Authorization Code

Unlike online-authorized transactions where the Authorization Code is provided by the issuer in the authorization response, Authorization Codes for offline-approved chip transactions are left to the acquirer's discretion. Visa recommends that Authorization Codes for offline transactions be included on the receipt using the format "CHPxxx" where the acquirer or device can set "xxx" to any value.

2.7.6 Electronic Receipts

Merchants may optionally provide the cardholder with an electronic receipt. Electronic receipts must comply with existing requirements for cardholder transaction receipts. In addition, electronic receipts are subject to the following requirements:

- **Paper Receipt** – Merchants must be able to offer a paper receipt and must provide a paper receipt, if requested by the cardholder.
- **Account Number Truncation** – The account number on the electronic receipt must be truncated. See Section 2.7.4: Consumer Data on Receipts and Displays for details.
- **Electronic Receipt Delivery Options** – The electronic receipt may be contained in an email message, SMS text message, or available via a link provided in the message.
- **Receipt Title** – The title of the email message or first line of the SMS text message must contain the merchant name and an indication that a cardholder receipt or link to a cardholder receipt is included.
- **Static Format –** The electronic receipt must be delivered in static format that is not easily manipulated.
- **Timing** – The electronic receipt must be sent to the cardholder upon completion of the transaction.
- **Instructions for Receipt Retrieval** – Merchants must provide instructions to the cardholder for retrieval of the receipt in the event that the cardholder does not receive it.

The delivery of cardholder receipts via email or SMS text message does not affect existing requirements for cardholder verification.

2.7.7 Chip Transaction Receipts

In addition to the general information required on receipts per the *Visa Rules*, chip card receipts have the following additional requirements:

- **VISA** – The word "VISA" is required on the receipt where the transaction will be processed by Visa.[6]
- **Application Identifier (AID)** – The AID is required on the receipt per EMV. For more information on the AID, see Section 4.3.1: Application Identifiers.
- **Application Name** – It is strongly recommended to print the Application Preferred Name on the receipt (if provided by the card and the associated character set is supported by the device) or, if not, the Application Label.7 For more information on these data elements, see Section 4.3.7: Application Label and Application Preferred Name.

Also, when the PAN on a chip card is an odd number of digits (e.g., 19-digit PAN), an 'F' is appended to the tag that contains the Primary Account Number (Tag '5A') (e.g., for a 19-digit account number, Tag '5A' will contain 19 digits of the PAN followed by an 'F' to make it an even number of digits) but the 'F' must not be printed on the receipt when the device obtains the PAN from this tag.

[6] For U.S. Common Debit transactions, printing the Application Label on the receipt is sufficient.

[7] Most cards will be personalized with the Application Label (at a minimum).

2.8 Cardholder Verification Methods (CVMs)

Cardholder verification is used to evaluate whether the person presenting the card is the legitimate cardholder. The CVMs available on Visa transactions are outlined in the following table:

Table 2–3: Cardholder Verification Methods (CVMs)

Cardholder Verification Methods	Description
Signature	The cardholder signs the transaction receipt and the merchant compares this signature to the signature on the card. For the requirements associated with signature, see Section 2.8.3: Signature.
Online PIN	The cardholder-entered PIN is encrypted by the device using TDES key technology and sent online to the issuer for verification. For the security requirements associated with Online PIN, see Section 7.3: PIN and PIN Entry Device (PED) Security.
Offline Plaintext PIN	With this method of Offline PIN, the device prompts the cardholder for a PIN and transmits the cardholder-entered PIN to the card in the clear. The card then compares the cardholder-entered PIN to the Reference PIN stored in the chip. For the security requirements associated with Offline Plaintext PIN, see Section 7.3.4: Offline PIN Requirements.
Offline Enciphered PIN	With this method of Offline PIN, the device encrypts the cardholder-entered PIN with the card’s public key and sends the encrypted value to the card. The card decrypts the cardholder-entered PIN and compares it to the Reference PIN stored in the chip. This method protects the PIN in transit from the reader to the card. For the security requirements associated with Offline Enciphered PIN, see Section 7.3.4: Offline PIN Requirements.
No CVM Required	The transaction takes place without cardholder verification.
Consumer Device CVM (CDCVM)	The cardholder is verified on the consumer device itself. This typically involves a passcode or a biometric reading.

Note: Combination CVMs of Offline Plaintext PIN and Signature or Offline Enciphered PIN and Signature (where both methods must be performed to validate the cardholder) are also available on contact-chip transactions but are not recommended or widely used.

2.8.1 CVMs by Interface Type

The CVMs that may be supported by interface are outlined in the following table. See Section 2.8.2: CVMs by Device Type for CVM requirements by device type.

Table 2–4: Supported CVMs by Interface

CVM	Magnetic Stripe	Contact Chip	Contactless Chip
No CVM Required	✓	✓	✓
Signature	✓	✓	✓
Online PIN	✓	✓	✓
Offline Plaintext PIN		✓	
Offline Enciphered PIN		✓	
Offline Plaintext PIN and Signature*		✓	
Offline Enciphered PIN and Signature*		✓	
Consumer Device CVM (CDCVM)			✓

*Not widely used.

2.8.2 CVMs by Device Type

The following table outlines the minimum global requirements for CVMs that devices must support by device type. The items outlined as optional in the following table may be conditional or required in certain countries. Check with your Visa representative to understand the specific requirements for your market.

Key:

M = Mandatory
O = Optional
– = Not Applicable/Not Allowed

Table 2–5: Global Minimum CVM Requirements by Device Type

CVM	Attended POS			UCAT			ATM[8]	
	Magnetic Stripe Device	Contact Chip Device	Contactless Chip Device	Magnetic Stripe Device	Contact Chip Device	Contactless Chip Device	Contact ATM	Contactless ATM
Signature	M	M[9]	M[9]	–	–	–		M[10]
Online PIN	O	O	O	O	O	O	M	M[10]
Offline Plaintext PIN	–	O	–[11]	–	O	–[11]	–	–
Offline Enc PIN	–	O[12]	–[11]	–	O[12]	–[11]	–	–
No CVM	O	O	–[13]	O	M	–[13]	–	–
CDCVM	–	–	M	–	–	M		M[10]

Note: Individual countries may require at least one PIN option (e.g., Offline PIN or Online PIN) at chip-enabled devices. Contact your Visa representative to determine if there are any specific PIN requirements for your market.

[8] The CVM requirements listed in this table for ATMs are only applicable when dispensing cash. ATMs may also dispense goods/services; in which case, they would adhere to the CVM requirements for UCAT purchases.

[9] While the kernel in the device (other than VEPS-only devices) must support signature, the merchant is no longer required to capture and verify the cardholder's signature at a chip device.

[10] 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.

[11] While Offline PIN does not apply to a contactless transaction, 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.

[12] When Offline Enciphered PIN is supported, the device must also support Offline Plaintext PIN. In some markets, when the device supports Offline PIN, it must support both the plaintext and enciphered versions.

[13] "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).

Note: A device may need to support functionality that allows merchants to offer an alternative CVM to PIN for cardholders that may be unable or unwilling to enter a PIN at the POS due to security concerns or certain disabilities in accordance with merchant protection and local disability legislation.

Note: If the merchant is a VEPS merchant and the transaction qualifies for VEPS, the merchant may process the transaction without a CVM. For more information on VEPS, see Section 2.14: Visa Easy Payment Service (VEPS).

Note: Cards and devices may also agree on a higher level of CVM than the minimum. The *Visa Rules* concerning the level of cardholder verification required for certain types of transactions (e.g., manual cash or quasi-cash) apply regardless of whether the transaction is initiated from a chip or magnetic stripe.

2.8.3 Signature

This section outlines general requirements for signature:

- **Mandatory at Attended POS Devices** – The kernel of all attended POS devices (other than VEPS-only devices) must support signature; however, the merchant is no longer required to capture and verify the cardholder's signature at a chip device.
- **Signature Verification** – Where signature verification applies, the merchant is required to compare the signature on the receipt with the signature panel of the card. If the two signatures match, the cardholder's identity is deemed to have been correctly verified.
- **No Signature Line on Receipt** – If signature is to be captured on a printed receipt and there is no signature line on the receipt, the merchant may collect the signature anywhere on the receipt.
- **Signature Line –** If the cardholder is not required to be verified by signature, do not print the signature line on the receipt.
- **Combination CVM of Offline PIN and Signature** – In the instance where the selected CVM is a combination of Offline PIN and signature, the device may print (in addition to the PIN verification message) a signature line for the cardholder's signature or capture the cardholder's signature electronically.
- **Signature Capture** – The device may capture the cardholder's signature either by having the cardholder sign the receipt or capture it electronically using a touch screen and a pen-like device or stylus to write the signature.
- **Electronic Signature Capture Devices** – An electronic signature capture device enables a merchant to obtain a cardholder's signature for a transaction using a touch-sensitive electronic pad instead of a paper transaction receipt. These devices must:
  - Have proper controls in place to ensure the security of the stored signatures and other cardholder data in accordance with PCI DSS.
  - Store and reproduce a signature only on a transaction-specific basis, in relation to the transaction for which the signature was obtained.

  - Reproduce a signature only upon specific written request from the acquirer or in response to a retrieval request (where applicable).
  - Follow any country-specific rules for electronic signature capture.

2.9 Transaction Cancellation

Devices should enable a cardholder or merchant to cancel a transaction in progress at any time. The device may be required to generate a receipt for a canceled transaction, depending on local law.

2.10 Card Data in Online Messages

Requirements for card data in online messages:

- **Data Transmission** – The device must always transmit the full, unmodified contents of the magnetic-stripe data or the Track 2 Equivalent Data in the contact or contactless chip to the acquirer. The device should not construct the magnetic-stripe data field in the online authorization message based on the individual data elements in the magnetic stripe or chip.
- **No Data Mixing** – Where transaction data can be read from multiple interfaces, the transaction data must not be mixed (magnetic stripe data must be used on magnetic-stripe transactions, contact-chip data on contact transactions, and contactless-chip data on contactless transactions).
- **Track 2 Data** – Track 2 is the preferred data to be used for magnetic-stripe transactions and may be required in some countries. On chip-initiated transactions, the Track 2 data in the message must be populated using the Track 2 Equivalent Data on the chip. For more information on Track 2 Data, refer to the *Payment Technology Standards Manual*.
- **POS Entry Mode** – Because the data on the chip may differ from the data on the magnetic stripe, the POS Entry Mode Code field (Field 22) in the online authorization message that indicates the source of the track data (magnetic stripe or chip) must be accurate to avoid unnecessary declines.

2.11 Transaction Speed

Rapid authorization enhances the cardholder experience while providing reduced transaction and queue times for the merchant:

- **Faster Communications Technologies** – Online authorizations can be optimized through implementation of faster communication technologies (such as always-on or broadband). The benefits of customer satisfaction and higher throughput can offset additional communication costs in many cases.
- **Contactless Speed Requirements** – Speed requirements for contactless transactions are more stringent due to the convenience and speed factor associated with them. *VCPS* requires the contactless card read to be less than 500 milliseconds (ms). For more information, see Section 5: Contactless-Chip Acceptance.

2.12 Radio Frequency (RF) Interference

Device manufacturers should take care to shield contact-chip readers from sources of Radio Frequency (RF) radiation, such as contactless readers or wireless modems.

When processing via the contact-chip interface, the radio frequency (RF) field of the contactless interface should be powered down prior to initiating the contact-chip transaction. Simply disabling the logical function but leaving the field active may interfere with proper functioning of dual-interface cards.

For more information, see Appendix A: Contactless Reader Placement.

Note: Any time there is a device that supports more than one interface, the device must ensure that all of the data for a given transaction is from only one of the interfaces (i.e., if the device inadvertently obtains data from both the contact and the contactless chip, it must only use one set of data for the transaction rather than co-mingling the data).

2.13 Electrostatic Discharge Management

Device vendors and merchants need to ensure appropriate steps are taken to manage Electrostatic Discharge (ESD). ESD is the sudden and momentary electric current that flows between two objects at different electrical potentials when they are brought into close proximity to each other. ESD events are typically associated with the build-up of static electricity.

Merchants, particularly in dry environments, have reported disruptions of payment transactions by ESD events to EMVCo. Device vendors should take ESD into consideration during the device design, manufacturing, and testing process so as to avoid ESD events occurring in the field.

Additionally, EMVCo has outlined recommendations for reducing ESD at the POS. Some of these recommendations include:

- **Floor Mats/Carpets/Coatings** – Installation of static dissipative floor mats or carpets, or use of static dissipative or conductive floor coatings to reduce the build-up of static charge.
- **Table Mats** – Use of antistatic table mats that are connected to a ground point.
- **Cleaner/Treatment Cards** – Using ESD cleaner/treatment cards which assist in eliminating ESD and also cleaning the read head of the device.

EMVCo provides a device ESD evaluation process to evaluate the level of protection against ESD of devices. For more information, see www.emvco.com.

2.14 Visa Easy Payment Service (VEPS)

Visa Easy Payment Service (VEPS) streamlines merchant acceptance procedures by eliminating the need for cardholder verification and receipts (although a receipt must be provided if the cardholder requests one). VEPS is targeted at low-value POS transactions. Merchants that meet the qualification criteria may participate in the VEPS program.

For more information on VEPS including qualification criteria, refer to the *Visa Easy Payment Service – Acquirer Program Guide* or contact your Visa representative.

Note: Fallback transactions do not qualify for VEPS. For more information on fallback, see Section 4.2.2: Fallback Acceptance for Chip Read Failures.

2.14.1 General Requirements

General requirements for VEPS transactions are outlined in the following table:

Table 2–6: General VEPS Requirements

Requirement	Description
Authorized	• **Magnetic Stripe Transactions** – Online authorized with a valid Authorization Code. • **Contact/Contactless Transactions** – Offline or online authorized: – Offline authorized with an Authorization Response Code of Y1 or Y3. – Online authorized with a valid Authorization Code.
POS Entry Mode Value	• **Magnetic Stripe Transactions** – Value of 90. • **Contact Transactions** – Value of 05. • **Contactless Transactions** – Value of 07.

2.14.2 Contact Transactions

VEPS transactions do not require cardholder verification. Device vendors and acquirers may need to set up devices to only indicate support for the "No CVM Required" CVM on transactions equal to or below the VEPS country amount limit. One way to manage this type of processing is via an EMV selectable kernel:

- **Transaction Qualifies for VEPS** – The device invokes a specific kernel configuration that only supports the "No CVM Required" CVM. This will allow the transaction to take place without cardholder verification.
- **Transaction Does Not Qualify for VEPS** – The device uses its standard kernel configuration where it may support multiple CVMs such as signature, PIN, etc.

For more information on selectable kernels, see Section 6.9: Configurable/Selectable Kernels.

Note: Countries may also use the selectable kernel solution to facilitate PINless transactions that comply with local business requirements or regulations.

2.14.3 Contactless Transactions

For contactless transactions, the Reader CVM Required Limit controls whether the device requires a CVM on the transaction; transactions above this limit require a CVM while those below it do not. This limit should be set to the VEPS limit.[14]

Note: qVSDC readers may support a feature called Dynamic Reader Limits (DRL) allowing the reader to support multiple CVM limits according to the Application Program ID personalized on the card. For example, these qVSDC readers may be configured with a Reader CVM Required Limit for domestic transactions and a different Reader CVM Required Limit for international transactions. Device vendors and acquirers should consult with their Visa representative for the best approach in their region.

[14] Because the reader requires a CVM when the transaction amount is less than or equal to the Reader CVM Required Limit, the Reader CVM Required Limit should more accurately be set to the VEPS Limit plus one minor unity of currency. For example, with a VEPS limit of $25.00, the Reader CVM Required Limit should be set to $25.01.

2.15 Key-Entry Transactions

Where possible, transactions should be electronically read by inserting/tapping the chip card or swiping the magnetic stripe. Electronically-read data provides the issuer with valuable information for risk management.

When an electronic read is not possible and the transaction is key-entered, the key-entered transaction is identified in the authorization message through the following fields.

Note: Key-entered transactions are also referred to as "manual transactions."

Table 2–7: Key-Entered Transactions

Data Element	Values
POS Entry Mode (Field 22)	Set to "Manual Key Entry" (Value = 01).
POS Condition Code (Field 25)	Set to the appropriate value for the transaction: • **Normal Transaction of This Type** (Value = 00) – This value is used when the card, cardholder, and merchant are present. – This value should also be used when the PAN is read from the card by any means and is then used to initiate a key-entered or manually-processed transaction. For example, if Optical Character Recognition (OCR) is used to read the PAN, this value would apply. – This value should also be used when the card data is electronically read, but the PAN and expiration date are then extracted from the card data, and the magnetic-stripe or chip data is then discarded. – This is the best value to use for key-entered fallback transactions. • **Card Present, Magnetic Stripe Cannot Be Read (Key-Entered) (U.S. Only)** (Value = 71) – This value is used when the electronic reader has failed. • **Mail/Phone Order/Recurring Transaction** (Value = 08) – This value is used for transactions initiated by a cardholder using the telephone (whether interacting with a customer service representative or an interactive voice response (IVR) unit). For other values, see the VIP manuals.

Note: If an initial transaction is performed with the cardholder present, but then subsequent transactions are performed without the cardholder present, the subsequent transactions must be coded distinctly from the initial transaction using the above values.

2.16 Visa Branding of Payment Terminals

Visa has developed a set of guidelines and artwork to be used by acquirers, merchants, and other partners to accurately reproduce the Visa brand mark and the EMV Contactless Symbol[15] on devices and promotional materials.

These requirements are available from:

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

For more information on the EMV Contactless Symbol, see 5.4: Device User Interface Recommendations.

2.17 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. At checkout, the merchant or ATM may convert the advertised price to the currency agreed to by the cardholder. The cardholder must be offered a choice to accept or decline the DCC and must actively choose the DCC option prior to the merchant or ATM processing the transaction. The merchant or ATM must accept the cardholder's choice; if the cardholder refuses DCC, the merchant or ATM must process the transaction in their local currency.

- **General** – DCC is permitted on Visa transactions in all Visa regions, subject to the *Visa Rules* and the DCC Compliance Program requirements outlined in the *DCC Guide – DCC Program Requirements*.
- **DCC Compliance Program** – The global DCC Compliance Program comprises a global registration, certification, and POS audit program. The program seeks to ensure cardholders are provided with adequate disclosure and active choice when accepting DCC and that the transaction receipt complies with the *Visa Rules*.

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

- **Cardholder Billing Currency** – DCC registered merchants and ATM acquirers should confirm the correct cardholder billing currency before initiating a DCC transaction. As an optional service, DCC acquirers may receive a weekly electronic file (the Account Billing Currency file) from Visa to identify the billing currencies of account ranges that can be used to determine the appropriate currency for DCC. Use of this file is strongly recommended.
- **Chip Transactions** – The currency code used in the generation of the cryptogram (ARQC or TC) must be the same as is included in the authorization and clearing messages (Field 148, EMV Tag '5F2A'). A change in the currency code could lead to the issuer declining the transaction since cryptogram validation will fail.
  - In most scenarios, the transaction currency (Field 49) will contain the same value as the chip data related currency in Field 148, EMV Tag '5F2A'; however, there may be instances where these differ. The critical point is that the chip-related field is not changed from the currency provided to the card and then used by the card to generate the cryptogram.

3. Magnetic-Stripe Acceptance

This section provides an overview of the requirements and recommendations for devices that accept magnetic-stripe cards.

Important: Magnetic-stripe transactions are zero-floor limit; therefore, they must be sent online for authorization.

3.1 Card Acceptance Methods

A device accepts a magnetic-stripe card through one of the following methods:

- Swipe or slide
- Dip
- Insert (for motorized readers)

Note: A motorized reader with card retention capability may be needed to support requirements to capture cards.

The cardholder or merchant may be required to interact with the device before it can accept the card (e.g., the cardholder may be required to press a function key to select the card type).

When a card is presented at a magnetic-stripe-only device, the device should always attempt to read the magnetic stripe. If the magnetic stripe cannot be read, key-entry procedures may be used at the POS unless disallowed under the *Visa Rules* or prohibited by local law. For more information on key entry, see Section 2.15: Key-Entry Transactions.

3.2 Magnetic-Stripe Data Processing

A device that accepts magnetic-stripe transactions must:

- Read a magnetic stripe that conforms to the Track 1 or Track 2 data specifications.
- Not erase or alter any magnetic encoding on a card.
- Transmit all data encoded on either Track 2 or Track 1 of the magnetic stripe to the acquirer. It is strongly recommended that Track 2 is sent, with or without Track 1.
- Be able to distinguish the magnetic stripe containing Visa payment data from other proprietary magnetic-stripe data on a card (for devices with multiple reader heads).

Note: For both contact and contactless transactions, Track 1 is not supported in the authorization message.

For more information on Track 1 and Track 2, see the *Payment Technology Standards Manual*.

3.3 Service Codes

The Service Code on the magnetic stripe indicates the circumstances under which the card can be accepted (e.g., international transactions, domestic-only transactions, ATM-only transactions). The code also defines requirements for processing a transaction with the card (e.g., chip enabled or PIN required).

A device with online capability must either read and act upon the Service Code values on a card's magnetic stripe or send the transaction online to the issuer for authorization. Offline-only devices must both read and act upon the Service Code values.

3.3.1 Service Code Values

Information on Service Code values follows:

Table 3–1: Service Code Values

Service Code	Description
2xx and 6xx	Card is contact-chip enabled. When reading a card via the magnetic-stripe reader, contact-chip-capable devices must examine the Service Code on the magnetic stripe to determine if the card is contact-chip enabled. If the Service Code indicates that the card is contact-chip enabled, the device must prompt the cardholder or merchant to insert the card into the contact-chip reader, unless operating under fallback conditions. For more information on fallback, see Section 4.2.2: Fallback Acceptance for Chip Read Failures.
5xx and 6xx	Magnetic stripe is restricted to domestic-use only.
xx0, xx6, and x20	PIN required/may be required. A device that supports a PIN pad should use the Service Codes relating to PIN entry (xx0 and xx6) to determine if a PIN should be requested prior to initiating the online authorization. If an x06 (PIN, if PIN pad present) or x20 (PIN required) Service Code is read, the device should request PIN entry and transmit the transaction online. If the device is unable to process the transaction online, it should process the transaction as normal for an x06 Service Code or reject the transaction for an x20 Service Code. Note: When discussing Service Codes, references to PIN mean Online PIN. An offline-PIN-only PIN pad (which is to be used for contact-chip transactions) is considered "PIN pad not present" when evaluating the applicability of Service Codes. Also, if the acceptance device does not support PIN for Visa and Visa Electron, even if PIN is supported for other acceptance marks, the PIN pad is considered not present on Visa/Visa Electron transactions.

Service Code	Description
Xx3	Card is for ATM use only. POS devices processing transactions for amounts below the floor limit should ensure that the Service Code is not xx3 (ATM only).

3.3.2 Service Code Not Recognized

If the device does not recognize the Service Code, the transaction must be submitted for online authorization if the device has online capability. Offline-only devices or a device that temporarily cannot authorize a transaction should reject a transaction when the device does not recognize the Service Code.

4. Contact-Chip Acceptance

This section provides an overview of the EMV and VIS requirements and recommendations for contact-chip devices.

Note: Unless otherwise noted, all requirements in Section 2: General Acceptance apply to contact-chip devices. Device vendors and acquirers should ensure their chip devices meet those requirements as well as the requirements outlined in this section.

For more information on developing a device that accepts Visa contact-chip cards, see the *EMV Chip Specifications* and the *Visa ICC Specification (VIS)*.

4.1 Processing Overview

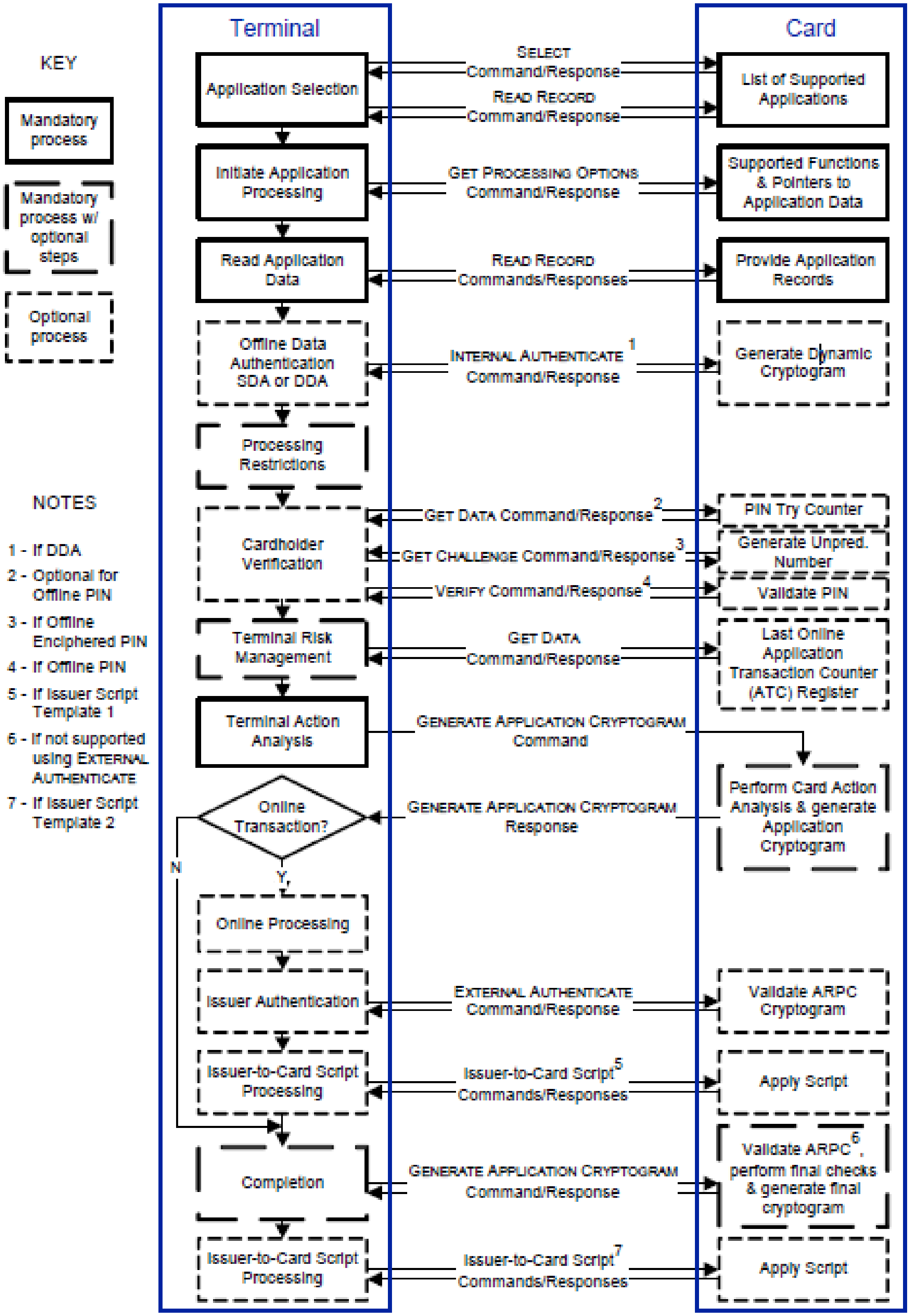
A contact-chip card and contact-chip device engage in a series of processing steps to complete an EMV transaction:

- Card Insertion
- Application Selection
- Initiate Application Processing
- Read Application Data
- Processing Restrictions
- Offline Data Authentication
- Cardholder Verification
- Terminal Risk Management
- Terminal Action Analysis
- Online Processing
- Completion
- Transaction Conclusion

This section outlines the device requirements associated with each step. All steps except the last one are documented in the *EMV Chip Specifications* and *VIS*. To fully understand each step, this section should be read in conjunction with these specifications.

The following figure illustrates a sample transaction flow including all the steps which are described in the subsequent sections.

Figure 4–1: Sample Transaction Flow Diagram


Terminal
Card
KEY
Mandatory process
Mandatory process w/ optional steps
Optional process
NOTES
1 - If DDA
2 - Optional for Offline PIN
3 - If Offline Enciphered PIN
4 - If Offline PIN
5 - If Issuer Script Template 1
6 - If not supported using EXTERNAL AUTHENTICATE
7 - If Issuer Script Template 2
Application Selection
SELECT Command/Response
READ RECORD Command/Response
List of Supported Applications
Initiate Application Processing
GET PROCESSING OPTIONS Command/Response
Supported Functions & Pointers to Application Data
Read Application Data
READ RECORD Commands/Responses
Provide Application Records
Offline Data Authentication SDA or DDA
INTERNAL AUTHENTICATE 1 Command/Response
Generate Dynamic Cryptogram
Processing Restrictions
Cardholder Verification
GET DATA Command/Response 2
PIN Try Counter
GET CHALLENGE Command/Response 3
Generate Unpred. Number
VERIFY Command/Response 4
Validate PIN
Terminal Risk Management
GET DATA Command/Response
Last Online Application Transaction Counter (ATC) Register
Terminal Action Analysis
GENERATE APPLICATION CRYPTOGRAM Command
Perform Card Action Analysis & generate Application Cryptogram
Online Transaction?
GENERATE APPLICATION CRYPTOGRAM Response
N
Y
Online Processing
Issuer Authentication
EXTERNAL AUTHENTICATE Command/Response
Validate ARPC Cryptogram
Issuer-to-Card Script Processing
Issuer-to-Card Script 5 Commands/Responses
Apply Script
Completion
GENERATE APPLICATION CRYPTOGRAM Command/Response
Validate ARPC 6, perform final checks & generate final cryptogram
Issuer-to-Card Script Processing
Issuer-to-Card Script 7 Commands/Responses
Apply Script

4.2 Card Insertion

A contact-chip device accepts a chip card through one of the following methods:

- Dip (and leave in)
- Insertion (for motorized readers)

The cardholder or merchant may be required to interact with the device before it can accept the card (e.g., the cardholder may be required to press a function key to select the application or the account type).

4.2.1 Chip Read

This section outlines information related to performing chip-read transactions.

Initiating a Chip Read

When a card is presented, the device should always check for the presence of a contact chip. This may be done by:

- Reading the chip directly.
- Reading the Service Code on the magnetic stripe to determine if the card is contact-chip enabled (2xx or 6xx).

If the Service Code indicates that the card is contact-chip enabled, the device must proceed to read the chip or prompt the cardholder or merchant to insert the card into the chip reader. The device must not perform any further magnetic-stripe processing unless the chip or chip reader are inoperative or the transaction is a non-EMV transaction.

Note: The controls associated with the Service Code are only applicable to magnetic-stripe transactions; they are not applicable to chip-initiated transactions. In lieu of the Service Code, chip transactions use other controls personalized on the card such as the Cardholder Verification Method (CVM) List and Application Usage Control (AUC).

Use of Chip Data on Chip Transactions

Devices must ensure they use the chip data appropriately on chip transactions:

- **Use Data Appropriate to the Transaction** – Devices with readers that support more than one interface, such as mechanized readers that support both contact chip and magnetic stripe (e.g., ATMs), must ensure that only data appropriate to the transaction is used. For contact-chip transactions, all data elements used must be read from the contact chip.
- **Do Not Compare Chip and Magnetic-Stripe Data** – Data from one interface may not match equivalent data from another interface and should not be compared. For example, the PAN read from the chip may be different from the PAN on the magnetic stripe, such as for multi-application cards where only one of the applications on the chip will match the magnetic stripe.

Important for ATMs: There have been situations during a chip transaction where ATM encryption PIN pads have used the PAN from the Track 2 data on the magnetic stripe to derive a session key to encrypt the Online PIN resulting in Online PIN errors. Developers must ensure that the PAN used to derive the session key is obtained from the Track 2 Equivalent Data (Tag '57') on the chip.

Chip Device Installed Before Chip Transaction Acceptance

An acquirer or merchant may install a contact-chip device before the acquirer or merchant is capable or ready to accept chip transactions. Country or regional rules may require that all new devices be capable of reading contact-chip cards, including merchant and acquirer processing support.

In such situations, the chip functionality in the device, including the requirement to examine and act upon the 2xx or 6xx Service Codes, **is not to be activated** until the acquirer and merchant are ready to accept chip transactions and have the ability to transmit the new chip data elements to the issuer.

Chip Cards with Non-Functioning Magnetic Stripes

Device vendors should be aware that some chip cards (e.g., V PAY cards) are intended for processing only via the chip and may not have fully functioning magnetic stripes (these cards only contain a magnetic stripe because it may be needed for certain motorized readers to operate properly). These magnetic stripes may be encoded with nonfunctional information, such as a PAN with all zeroes, but contain a valid Service Code (2xx or 6xx) and expiration date. If the device encounters a card with a magnetic stripe that appears to not be fully functioning, the device should continue to read the chip and, assuming the chip is functioning, perform a standard EMV chip transaction (ignoring the magnetic stripe).

4.2.2 Fallback Acceptance for Chip Read Failures

Contact-chip devices must contain logic that allows the transaction to be completed by reading the magnetic stripe (or key entered as a last resort[16]) when the transaction cannot be completed by reading the chip (i.e., the chip or chip reader is inoperable). This function is called "fallback." Device vendors should contact their Visa representative for information on local rules governing fallback.

The following table outlines the basic principles related to fallback:

Table 4–1: Fallback Principles

Fallback Topic	Description
Retry Reading Chip	Before falling back to magnetic stripe, devices should attempt to retry reading the chip three times. If feasible, devices with motorized readers (such as ATMs) should attempt to restage the card in the chip-reading station or retract and re-land the chip contacts to complete the transaction.
Online Authorization and Fallback Data Elements	Fallback transactions must be authorized online and contain the correct data elements. Acquirers should refer to the *VSDC Contact and Contactless Acquirer Implementation Guide*[17] for information on properly identifying fallback transactions in VisaNet messages.
Key-Entry/Manual Acceptance As Last Resort	For POS transactions, if the magnetic stripe cannot be read, key-entry or manual/paper voucher procedures may be used unless prohibited by local regulation or domestic operating rules.[16] These transactions must be authorized online or by voice (see Section 2.15: Key-Entry Transactions for details). Key-entry should only be used as a measure of last resort and only if fallback to magnetic stripe is not possible. **Note:** 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).
Fallback Not Permitted	If fallback is not permitted by local regulation or domestic operating rules, the transaction is terminated.
Device Supports Chip but Does Not Yet Support Visa	If the merchant or acquirer is adding support for chip processing to the device in stages (i.e., the migration to chip begins by upgrading devices to support a non-Visa payment scheme with plans to upgrade to Visa over time), it may read the Service Code on the magnetic stripe of a Visa chip card that it does not yet support, identify the card as a chip card through the 2xx or 6xx Service Code, and then read the chip. At this point, the transaction will fail because the terminal will be unable to find a matching application.

[16] In the Europe region, if a chip read is not possible, fallback to magnetic stripe is allowed but fallback to key entry is not.
[17] A U.S.-specific guide is available for U.S. acquirers (the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide*).

Fallback Topic	Description
Device Supports Chip but Does Not Yet Support Visa (continued)	In these situations, the device should process the transaction using the magnetic stripe. These transactions should not be identified as fallback; therefore, the Terminal Entry Capability (TEC) value needs to be changed from 5 (chip device) to 2 (magnetic-stripe device) at some point in the transaction lifecycle before the transaction reaches the issuer; however, once migration is completed and the device supports both chip and the required Visa AIDs, the TEC should not be manipulated. Once the device is migrated, there is a risk that the merchant can be exposed to disputes if the TEC is incorrect.

4.2.3 Merchant Override of Chip Read

Contact-chip devices that accept Visa chip cards must not allow the cardholder or merchant to override the requirement for a chip read by manually prompting the device to read data from the card's magnetic stripe. Data from the magnetic stripe may be used only to perform the transaction if the chip or chip reader is inoperable (i.e., for fallback transactions). See Section 4.2.2: Fallback Acceptance for Chip Read Failures for more information on fallback.

4.2.4 Historical Bytes

Some contact-chip cards have values in the historical bytes that are returned to the device in the Answer to Reset (ATR). Although the *EMV Chip Specifications* describe the format of these bytes, their use is outside the scope of the specifications and testing, and there is no cross-industry definition for their usage.

It is strongly recommended that devices do not use information from historical bytes in processing (e.g., attempting to use these bytes for access to legacy chip applications). Although such processing may be successful for domestic cards at domestic devices, non-domestic issuers (or card vendors) may define the same values in the historical bytes for different purposes. This could lead to cards being rejected or being processed incorrectly especially if usage of this information occurs before the device is able to determine if the card is domestic or non-domestic.

4.3 Application Selection

This section provides general information on Application Selection. For information on applications that require cardholder confirmation and device support for cardholder selection, see Section 4.3.6: Cardholder Selection.

In Application Selection, the device compares the applications it supports with those supported by the card:

- **No Applications in Common** – If no applications are mutually supported between the card and the device, the device should display a "CARD TYPE NOT SUPPORTED" message18 and invoke a magnetic-stripe read. See the EMV Chip Specifications and VIS for device display messages.
- **One Application in Common** – If the card and device only have one application in common (and the application does not require cardholder confirmation), the device automatically selects that application for the transaction.
- **Multiple Applications in Common** – If more than one application is mutually supported,19 the device should offer the cardholder an option to choose which application to use for the transaction (except for specific situations resulting from commercial agreements or local regulatory requirements).20 This is called cardholder selection. For more information, see Section 4.3.6: Cardholder Selection.
  - If the card and device have multiple applications in common but the device is unable to allow the cardholder to choose the application for the transaction, the device may automatically select the highest priority, mutually-supported application that does not require cardholder confirmation or may apply Visa-approved logic to select the appropriate application.[21]

[18] A device that captures the card for the transaction, such as an ATM, will recognize that there are no applications in common and automatically read the magnetic stripe without displaying a message to the cardholder.

[19] When building the list of mutually-supported applications (i.e., Candidate List), the device must include all applications common to both the card and device, except when allowed by certain conditions specified in the *Visa Rules*.

[20] In the U.S., certain requirements related to Application Selection and display do not apply to U.S. Covered Visa Debit Cards.

[21] For information on U.S. Covered Visa Debit Cards, see Appendix B: Visa U.S. Common Debit AID (U.S. Only) and the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide*.

If the device automatically selects the application, it is important for the device to display the application name[22] to the cardholder as an indication of what application is being used to conduct the transaction. The device can display the application name in one of the following ways:

- **PIN Entry** – If PIN entry is required, the device can display the application name along with the "ENTER PIN" message. The amount of the transaction can also be shown at this point.
- **Amount** – If PIN entry is not applicable, the device can display the application name before or at the time that the device displays the amount.

4.3.1 Application Identifiers (AIDs)

All chip-reading devices (contact and contactless) must contain the appropriate Visa Application Identifiers (AIDs). The AID consists of two components:

- **Registered Application Identifier (RID)** – The RID represents the payment scheme. Visa's RID is A000000003.
- **Proprietary Application Identifier Extension (PIX)** – The PIX represents the application.

The following table outlines the RID, PIX, and complete AID for each Visa product.

Table 4–2: Visa Application Identifiers (AIDs)

Product	RID	PIX	AID
Visa (i.e., Visa Debit or Visa Credit)	A000000003	1010	A0000000031010
Visa Electron	A000000003	2010	A0000000032010
Visa Interlink	A000000003	3010	A0000000033010
Plus	A000000003	8010	A0000000038010

AIDs may have a length of 5 to 16 bytes. As per the *EMV Chip Specifications*, devices must be able to select AIDs that are between 5 to 16 bytes in length.

[22] Either the Application Preferred Name (if provided by the card and the character set is supported by the device), the Application Label, or, in the U.S., an enhanced descriptor. Refer to Section 4.3.7: Application Label and Application Preferred Name for additional information.

Visa AIDs must be configured in the device to support Partial Name Selection (where the device does not have to match on the entire AID in order to select the application). The code in the device, however, needs to take into consideration that there may be one or more AIDs present on the card where the length of the card AID is greater than the length of the device AID because the card AID contains a PIX extension to identify two applications with the same AID (e.g., two Visa Credit applications or one Visa Credit and one Visa Debit application). The device should perform partial matching on the RID and PIX (first seven bytes of the AID) and ignore the PIX extension (one or more bytes appended to the end of the AID).

Note: Devices must not simply use the RID with Partial Name Selection to select applications because this can result in the selection of an application not supported by the device. A number of industry-only, region-only, or domestic-only Visa applications have been defined that use the Visa RID with a PIX defined for that application (e.g., AID A0000000032020 is used for V PAY applications).

4.3.2 Application Identifier (AID) Requirements

This section describes the AID requirements by device type:

Table 4–3: Application Identifier (AID) Requirements

Device Type	AID Requirements
POS Devices	Must contain the Visa AID and Visa Electron AID.[23] **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.
	In addition to the Visa AID and the Visa Electron AID, if the POS device supports Interlink, it must also contain the Visa Interlink AID.[24] **Note:** Visa Interlink can only be accepted at POS devices capable of processing online transactions with Online PIN verification.
ATMs	Must contain the Visa AID, Visa Electron AID, *and* 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.

Note: Depending on the country in which it is located, the device may also need to support Visa regional or domestic AIDs. Contact your Visa representative for details.

[23] The Visa Electron AID only needs to be loaded into online-capable terminals.
[24] U.S.: POS terminals that support Interlink must also support the U.S. Common Debit AID.

4.3.3 Transaction Routing

Requirements for transaction routing follow:

- **BIN Tables for Routing** – Chip transaction routing is normally determined in the same manner as it is for magnetic-stripe transactions, which is primarily through the use of BIN tables.
  - For example, at an ATM, data from a card may be accessed using a Visa AID, but the transaction could be routed to the Plus network such as when a Visa/Plus card (containing only the Visa Debit/Credit AID) is presented at a Plus-only ATM.
- **Chip Processing and Routing** – Acquirers and device vendors need to ensure that both Visa and Plus routing function normally for chip-initiated transactions. This includes transactions initiated for chip cards that contain only the Plus AID (i.e., non-Visa cards that are enrolled to use Plus such as proprietary ATM cards).
- **Routing Decision Timing** – The routing decision needs to take place after the application has been selected so that the BIN of the selected application can be used for routing (especially important for cards that contain more than one AID).
- **Visa AIDs Route to Visa Networks** – Transactions initiated via Visa ISO AIDs[25] must be routed to Visa affiliated networks.
- **Domestic Transaction Routing** – Certain countries have specific requirements relating to the routing of domestic transactions. Domestic arrangements, such as in the U.S., Canada, or the U.K., may allow for selection of other AIDs which in turn allows for routing of transactions initiated with these AIDs to alternate networks. Acquirers should ensure they comply with any domestic requirements relating to transaction routing.
- **Dedicated File (DF) Name** – In some markets, the device is required to send the AID to the acquirer (and other downstream routing entities). The AID is contained in a card data element called the Dedicated File (DF) Name (Tag '84'). Contact your Visa representative for details.

4.3.4 Application Selection Methods

There are two methods for performing Application Selection: List of AIDs Method and the Directory Selection Method. Support for the Directory Selection Method is optional for the card and device, while the List of AIDs Method is mandatory.

If both the card and device support the Directory Selection Method, the device reads a list of the payment applications maintained on the card from the Payment Systems Environment (PSE). The device compares the applications listed in the card’s PSE to the applications it supports and builds the Candidate List.

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

Acquirers/merchants need to determine if they will support the Directory Selection Method in addition to the mandatory List of AIDs Method in their devices. Where the device supports many AIDs, the Directory Selection Method can provide more efficient processing but is only available if the both the card and device support it. So, if the market is interested in this functionality, it needs to be a concerted effort between acquirers and issuers to enable support for it on cards and devices.

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

For more information on both methods, see the *EMV Chip Specifications*.

4.3.5 V PAY

V PAY is a chip-only, PIN-based debit card program for use at POS and ATMs in the Europe region. This section outlines requirements for V PAY:

- **V PAY AID**
  - V PAY has a unique AID. There are V PAY-only merchants whose terminals must be loaded with the V PAY AID only (they must not contain any other Visa AIDs). The terminals of general Visa merchants, who accept all Visa cards, must not be loaded with the V PAY AID.
  - Acceptance at general Visa merchants within the Europe region is provided at EMV-compliant chip devices through the inclusion of the Visa Electron AID on the cards and in devices. For this reason, in the Europe region, chip devices accepting Visa Electron also carry the V PAY brand mark.
  - V PAY cards carry the Visa Electron AID to allow for global acceptance and are processed as Visa Electron transactions outside of the Europe region.[26]
- **Chip-Only Solution** – V PAY cards are intended for processing only via the chip (unless co-badged with Plus or other payment brands). As a result, V PAY cards may contain minimally functional magnetic stripes (e.g., magnetic stripes with a PAN that contains all zeroes but with a valid Service Code and expiration date). The purpose of the magnetic stripe on these cards is to allow mechanized readers to read the magnetic stripe, recognize that the card is a chip card from the Service Code, and initiate the transaction using the chip. The device should not terminate processing due to the missing magnetic-stripe data.
- **Fallback Not Applicable** – Fallback transactions are not applicable to V PAY cards.

[26] EMV-compliant chip devices that accept Visa products and support PIN, but do not currently support Visa Electron products, will not accept V PAY cards.

4.3.6 Cardholder Selection

Issuers may issue cards with a setting that requires the application to obtain "cardholder confirmation" (as personalized in the Application Priority Indicator) prior to the application being used for the transaction. If the cardholder is not provided with an opportunity to confirm use of the application, the application cannot be used for the transaction.

As cards may be personalized with this setting, support for cardholder selection is strongly recommended for all devices that have the capacity (i.e., screens, menu functions) to support it.[27] Device support for cardholder selection also allows cardholders with multiple applications to select the one to use for a given transaction.

Devices should implement support for cardholder selection in one of the following ways:[28]

- **Menu** – Device displays a menu of all available applications to the cardholder in order of priority and prompts the cardholder to select one.
  - If the transaction cannot be performed with the selected application, the device should display the "TRY AGAIN" message and display the remaining mutually-supported applications.
  - If all applications have been displayed to the cardholder and the cardholder has not selected one, the transaction should be terminated and restarted, as necessary.
- **Single Name** – Device displays one mutually-supported application at a time in order of priority which the cardholder may accept or reject.
  - If rejected, the device then displays the next application, in priority order, continuing through the list of mutually-supported applications until the cardholder has selected one or rejected all of them.
  - If the cardholder rejects all of the applications, the device can re-start the process or terminate the transaction.

    Note: Single Name Application Selection should only be used where the terminal user interface is severely limited (e.g., only two lines of text can be displayed at a time).

If there is only one application in common between the device and card, or if a domestic arrangement is in place to use only a particular application for domestic cards,[27] cardholder selection is not necessary (assuming the card is not set up to require cardholder confirmation); however, the application name should be displayed to the cardholder (see Section 4.3.7: Application Label and Application Preferred Name) so that the cardholder knows which application is being used for the transaction and it should also be provided on the receipt (see Section 2.7: Transaction Receipts).

[27] For information on U.S. Covered Visa Debit Cards, see Appendix B: Visa U.S. Common Debit AID (U.S. Only) and the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide*.

[28] In the Menu and Single Name methods, the application name is displayed to the cardholder using the Application Preferred Name (if provided by the card and the character set is supported by the device) or the Application Label.

For devices where the cardholder and merchant have separate displays, the application names that appear for selection should be displayed only to the cardholder and not to the merchant (in some Visa regions, this is a requirement). The dual-display device should also not allow the merchant to choose the application on behalf of the cardholder. While the customer is choosing the application, the merchant display should inform the merchant that this is occurring. As soon as the cardholder has completed selection, the application should be identified to the merchant.

During the cardholder selection process, the cancel key should only be used to terminate the transaction, unless clear guidance is provided on the effect of using this key.

4.3.7 Application Label and Application Preferred Name

Contact-chip devices are required to support the character set used by the Application Label. Support for displaying/printing the Application Preferred Name depends on whether the device/printer supports the Issuer Code Table Index associated with the application:

- **Issuer Code Table Index Supported** – The device should display the Application Preferred Name and print it on the receipt.
- **Issuer Code Table Index Not Supported** – The device should display the Application Label and print it on the receipt.

Using the Application Preferred Name is preferred because it allows the name of the application to be displayed in the cardholder's local language (where this is possible using the ISO 8859 standard); however, some cards may only be personalized with the Application Label.

It is important that either the Application Preferred Name or Application Label is consistently used for both the display and the receipt.[29]

For multi-application cards, it is important to display and print the Application Preferred Name or Application Label so that the cardholder is aware which application is being used for the transaction.

If the Application Preferred Name or Application Label contains an invalid character, this character should be displayed, if the device is able to display it. If it cannot, it should display a space instead.

For the specific transaction receipt requirements associated with these data elements, see Section 2.7: Transaction Receipts.

[29] In the U.S., an enhanced descriptor may be used in place of the Application Label or Application Preferred Name for U.S. Covered Visa Debit Cards. These products are typically personalized only with the Application Label and not with the Application Preferred Name as further described in the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide.*

4.3.8 Multiple Languages

Devices may offer the cardholder a choice of languages to be used. This can be accomplished by using the EMV Language Selection function or through a proprietary process. If using the EMV function, the device will compare the card's Language Preference data element with the languages supported in the device:

- If matches are found, the matching language with the highest preference is used in the messages displayed to the cardholder.
- If no match is found and the device supports more than one language, the device allows the cardholder to select the preferred language at the beginning of the transaction (assuming it has the means to do so).

For most implementations, EMV functionality to support language selection does not offer a significant advantage over a proprietary process unless the terminal supports a very large number of languages.

4.4 Initiate Application Processing

Once an application is selected, the device sends the GET PROCESSING OPTIONS command to the card to request the card to indicate the data to be used for the transaction and its supported functions. The device also provides any data to the card as indicated by the Processing Options Data Object List (PDOL) sent by the card in the response to the SELECT command.

Account selection generally follows Application Selection for many ATMs and for those countries supporting account selection at the POS (see Section 2.3: Account Selection). Although the process for account selection is not part of the *EMV Chip Specifications*, EMV has defined an optional data element called Account Type. Using this data element, the device can send the cardholder's account selection to the card. A card may request this information in the PDOL.

4.5 Read Application Data

The device reads the data indicated by the card in the response to the GET PROCESSING OPTIONS command and uses the Application Interchange Profile (AIP) (a list of functions supported by the card) to determine whether to perform the following functions:

- Offline Data Authentication (optional in some cards)
- Cardholder Verification (required in all cards)
- Terminal Risk Management (see requirements in Section 4.9: Terminal Risk Management)
- Issuer Authentication using the EXTERNAL AUTHENTICATE command (optional in cards)

The data retrieved by the device during this step is identified by tags:

- The *EMV Chip Specifications* define the tags for the data elements
- There may also be payment system-specific tags, issuer-specific tags, and private tags agreed upon for use in a specific market

4.6 Processing Restrictions

The device must perform the processing restrictions checks based on data provided by the chip to determine whether the transaction should be allowed. These checks include:

- **Expiration and Effective Date Checking** – The device checks whether the expiration date and, if present, the effective date for the card has been reached. See Section 2.2: Expiration Date for more information.
- **Application Version Number Checking** – The device checks its version number against the card's version number.30 The Application Version Number is the VIS version, release, and modification number (in binary) supported by the card. 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)
- **Application Usage Control Checking** – The Application Usage Control field may be set by an issuer to limit or enable a card's use for certain transactions (e.g., domestic or international, cash, goods or services, or cash back). The device checks the Application Usage Control received from the card to see if the transaction type is allowed.
  - The two Application Usage Control settings "If Goods" and "If Services" should be treated as equivalent. A transaction for domestic goods or services is allowed if either a valid control for domestic goods or domestic services (or both) is set; the same is true for international goods and international services.

The device records the results of these checks in the TVR and uses them during Terminal Action Analysis (see Section 4.10: Terminal Action Analysis for details) to determine the decision to go online, decline offline, or approve offline.

[30] The Application Version Number generally does not impact card acceptance because the TVR bit corresponding to "ICC and terminal have different application versions" is rarely used to influence the outcome of transactions.

4.7 Offline Data Authentication

Offline Data Authentication enables authentication of a payment application for offline transactions. The three types of Offline Data Authentication are outlined in the following table along with their requirements for support.

Note: Offline Data Authentication is not required in ATMs or other online-only environments.

Table 4–4: Offline Data Authentication Methods and Requirements

Method	Definition	Requirement
Static Data Authentication (SDA)	A method that ensures a set of static data obtained from the valid issuer has not been modified since initial personalization onto the card.	Required for all contact-chip devices with offline capability.
Dynamic Data Authentication (DDA)	Offers a higher level of data authentication than SDA, providing protection against both counterfeiting and the replaying of copied data (comparable to magnetic-stripe-data skimming).	Same as above.
Combined DDA/Generate Application Cryptogram (CDA)	Combines DDA with the generation of a card's Application Cryptogram to assure card validity. CDA is intended to protect offline transactions where there is significant opportunity for interception of chip-to-device communications.	Required only in specific environments/markets. Contact your Visa representative for details.

All Visa cards that support DDA or CDA are required to support a DDA Data Object List (DDOL), which contains the list of device data elements that the device must send to the card in the command requesting a dynamic signature. If a DDOL is not received from the card, the device must use its Default DDOL. The Default DDOL must only contain the tag and length for the Unpredictable Number. No other data objects may be referenced in the Default DDOL.

4.8 Cardholder Verification

Cardholder verification is used to evaluate whether the person presenting the card is the legitimate cardholder. For contact-chip transactions, the device uses a CVM List from the card to determine the type of cardholder verification to be performed. The CVM List establishes a priority of CVMs to be used relative to the capabilities of the device and characteristics of the transaction. The CVMs that may be supported by a contact-chip device for a contact-chip transaction are:

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

For a description of each CVM, see Section 2.8: Cardholder Verification Methods (CVMs).

For the CVM requirements for a contact-chip device, see Section 2.8.2: CVMs by Device Type.

For information on signature, see Section 2.8.3: Signature.

For security requirements related to PIN, see Section 7.3: PIN and PIN Entry Device (PED) Security.

Note: Combination CVMs of Offline Plaintext PIN and Signature or Offline Enciphered PIN and Signature (where both methods must be performed to validate the cardholder) are also available but not recommended or widely used.

4.8.1 CVM List Processing Exceptions

The device should allow the CVM to be selected based on standard EMV CVM processing unless the *Visa Rules* or local laws for the environment/transaction require a particular CVM:

- **Minimum Level of Cardholder Verification** – If a situation occurs where the card does not support CVM processing (e.g., the card’s AIP does not indicate support for cardholder verification) or a CVM List is not present on the card, the device should perform a CVM designated in the *Visa Rules* or in local law for the device/transaction type to ensure a minimum level of cardholder verification takes place on the transaction.
- **ATMs and Online PIN** – Visa requires Online PIN for ATMs. ATMs will always request the cardholder to enter an Online PIN even if the CVM List does not contain Online PIN. No other CVMs are valid at ATMs.

- **Terminal Verification Results (TVR)** – The use of a CVM not required by the card, but required by the *Visa Rules*, should have no effect on the TVR:
  - If the result of CVM processing is "Cardholder verification was not successful", the corresponding bit should still be set in the TVR, even if a CVM is requested by the device in accordance with *Visa Rules*.
  - Similarly, when an Online PIN is requested as specified by *Visa Rules* (such as at an ATM), the "Online PIN entered" bit should be set if and only if Online PIN was requested as a result of CVM processing.
- **Cardholder Verification Failed But Issuer Approves Transaction** – If an attended device determines that CVM processing has failed (e.g., the CVM List only contains Online PIN but the cardholder is unable to enter a PIN) but the issuer approves the online transaction, it is recommended that the device captures a signature/prints a signature line on the receipt. Although the acquirer is not liable for the transaction since the issuer approved it, the collection of a signature will reduce the grounds for any potential disputes.

Note: PIN may only be requested when specified in the chip's CVM List or when explicitly allowed in the *Visa Rules* (e.g., at ATMs).

For information on cardholder verification for VEPS transactions, see Section 2.14: Visa Easy Payment Service (VEPS).

4.8.2 Last PIN Try Message

When the device determines that an Offline PIN is to be entered, the device must either:

- Prompt for PIN entry (without checking the PIN Try Counter).
- Check the PIN Try Counter and if it is greater than 1, prompt for PIN. If it is 1 (indicating one remaining PIN try), the device should display the message "LAST PIN TRY" or local language equivalent.

4.9 Terminal Risk Management

The device may be required to perform Terminal Risk Management:

- **Mandatory for Offline-Capable Devices** – Devices that are capable of both offline and online processing must perform terminal floor limit checking and random transaction selection as part of Terminal Risk Management, regardless of the settings in the card's Application Interchange Profile (AIP) related to Terminal Risk Management.
- **Not Applicable to Online-Only Devices** – Devices that have a zero-floor limit always send the transaction online to the issuer for processing and they do not need to perform Terminal Risk Management.

4.9.1 Terminal Floor Limits

Terminal floor limits are transaction amounts at or above which an online authorization should be performed. Acquirers use the *Visa Rules* for the country and merchant type to determine the appropriate floor limit. Offline-capable devices must perform floor-limit checking on all transactions:

- **Card Overrides Floor Limit** – If card parameters indicate that the transaction must be processed online, the device must attempt to send the transaction online regardless of the floor limit, and the transaction may be declined if the device cannot obtain an online authorization.
- **Different Magnetic Stripe and Chip Floor Limits** – Because countries may implement different floor limits for chip and magnetic-stripe transactions and for international and domestic transactions, devices and Terminal Management Systems should be capable of supporting the following floor limits:
  - International floor limit for non-chip transactions
  - International floor limit for chip-initiated transactions
  - Domestic floor limit for non-chip transactions
  - Domestic floor limit for chip-initiated transactions

  Note: Alternatively, where the magnetic-stripe floor limit is zero, the device could have a zero-floor limit for magnetic-stripe transactions by forcing all magnetic-stripe transactions online while using a floor limit for chip transactions.
- **Fallback** – Fallback transactions must be authorized online so floor limits are not applicable to these transactions. For more information on fallback, see Section 4.2.2: Fallback Acceptance for Chip Read Failures.

4.9.2 Random Transaction Selection

All online-capable devices must have the capability to randomly select below-floor-limit transactions for online processing. This functionality protects against fraudulent cards designed to operate exclusively offline.

Random Transaction Selection is not required in online-only devices.

Refer to the *EMV Chip Specifications* for information on how to set the random transaction selection parameters.

4.10 Terminal Action Analysis

During Terminal Action Analysis, the device uses the results of previous processing steps together with card rules called Issuer Action Codes (IACs) and device rules called Terminal Action Codes (TACs) (see next section for values) to determine whether a transaction should be approved offline, sent online for authorization, or declined offline. After determining the disposition of the transaction, the device requests an Application Cryptogram from the card using the GENERATE AC command, corresponding to the transaction disposition:

- Transaction Certificate (TC) – Offline approval
- Authorization Request Cryptogram (ARQC) – Online authorization
- Application Authentication Cryptogram (AAC) – Offline decline

Note: Currently, none of the cryptograms defined under *VIS* use the Transaction Certificate Data Object List (TDOL). As such, Visa does not have a defined value for the default TDOL. Vendors or acquirers may set the default TDOL to any value since it is not used for processing Visa transactions.

4.10.1 Terminal Action Codes (TACs)

The device must be loaded with the appropriate Terminal Action Codes (TACs). The TACs are defined and mandated by Visa. There are three types of TACs:

- TAC - Denial – Declines transactions offline.
- TAC - Online – Sends transactions online.
- TAC - Default – Declines transactions offline when online processing is not available.

The set of TACs differs based on whether the device is offline-capable or online-only; online-only devices only need to support TAC - Denial values and may opt to omit TAC - Online and TAC - Default values (since they always send transactions online and decline when online is not available).

Table 4–5: Terminal Action Codes (TACs)

		Online-Only Device	
AID	**Offline-Capable Device**	Device **Does Not** Support: TAC - Online and TAC - Default Processing	Device Supports: TAC - Online and TAC - Default Processing
Visa ISO AIDs[31]	TAC - Denial: x0010000000 TAC - Online: xDC4004F800 TAC - Default: xDC4000A800	TAC - Denial: x0010000000 TAC - Online: n/a TAC - Default: n/a	TAC - Denial: x0010000000 TAC - Online: xDC4004F800[32] TAC - Default: xDC4000A800[32]
Visa U.S. Common Debit AID[33]	n/a	TAC - Denial: x0000000000 TAC - Online: n/a TAC - Default: n/a	TAC - Denial: x0000000000 TAC - Online: xFFFFFFFFFF TAC - Default: xFFFFFFFFFF

The Visa TAC values are the hexadecimal representation of the minimum bit settings required by Visa. Acquirers may deploy TAC - Online and TAC - Default values in which additional bits are set but must not modify the TAC - Denial value as this could result in unnecessary declines.

4.11 Online Processing

Requirements for online messages:

Note: If the transaction is approved offline, an online message to the issuer does not take place and the transaction proceeds directly to completion (see the next section for details).

- **Online Message –** The acquirer formats the authorization message with the chip data in Field 55.[34] See the *VSDC System Technical Manual* for details on the data elements required in authorization and clearing/settlement messages.
- **ARQC and Associated Data** – When a transaction is sent online, the cryptogram and its associated data (which will be used by the issuer or VisaNet to perform Online Card Authentication) are provided in the online message. To prevent erroneous Online Card Authentication failures, the device must send the cryptogam and its associated data unaltered to the acquirer in the device-to-acquirer message and the acquirer must forward this data unaltered to VisaNet and the issuer.

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

[32] Alternatively, xFFFFFFFFFF may be used.

[33] U.S. only.

[34] Most countries require the acquirer to support the chip data in Field 55, although some allow support for the expanded third bit map. Check with your Visa representative for the rules in your country.

- **Merchant Forced Transaction Online** – Merchants/acquirers may optionally support device functionality to force transactions online to the issuer for processing which will set the "Merchant forced transaction online" bit in the Terminal Verification Results (TVR). This processing should be reserved for situations where the clerk explicitly forces a transaction online, such as for suspicious behavior. If a merchant needs to ensure that a particular category of transactions always goes online, they should not use this setting. Instead, they can achieve this by setting the "Transaction exceeds floor limit" bit in the TVR.
- **PAN on Exception File** – Merchants and acquirers should only indicate that a PAN was found in a terminal exception file when a formal arrangement with affected issuers is in place. This formal arrangement is the only time that the TVR condition "The PAN is on the terminal exception file" should be set. PANs extracted from the Visa Exception File for this use are considered compliant with this requirement.

4.12 Completion

Completion closes the processing of a chip transaction.

4.12.1 Offline Transactions

For offline approved transactions, the GENERATE APPLICATION CRYPTOGRAM (AC) command results in the card generating a TC. There is no online authorization for those transactions. The TC and its associated data are submitted into clearing.[35] These messages have unique requirements for the following data elements:

- **Authorization Response Code** – To indicate an offline approval, the device generates a Y1 or Y3 Authorization Response Code which is included in the clearing message. For a description of these codes, see the *VSDC System Technical Manual*.
- **Authorization Code** – See Section 2.7.5: Authorization Code for information on the Authorization Code for offline transactions.

For transactions that are declined offline after the first GENERATE AC command (card responds to first GENERATE AC command with an AAC), the device cannot force the transaction online in an attempt to get an approval. For more information on declined transactions, see Section 4.12.5: Declined Transactions.

[35] Offline approved transactions are not applicable in the U.S. or other zero-floor limit environments.

4.12.2 Online Transactions

After the transaction has been processed online, the device issues a second GENERATE AC command to the card to request additional card analysis and a final Application Cryptogram. To determine the type of cryptogram to request from the card, the device uses the Authorization Response Code received from the issuer in the online authorization response as follows:

- **TC (Approval)** – The device requests a TC when the Authorization Response Code is 00, 10, or 11 indicating that the issuer has approved the transaction.
- **AAC (Decline)** – The device requests an AAC when the Authorization Response Code is not an approval (i.e., not 00, 10, or 11).

Note: The Authorization Response Code received by the acquirer is coded in ASCII.

The card then uses the transaction disposition, Issuer Authentication results, and the Issuer Action Codes (IACs) to determine whether to return a TC or an AAC to the device:

- If a TC is returned, the TC and its associated data will be submitted into clearing.[36]
- If an AAC is returned, the transaction is declined and a decline message should be displayed to the cardholder. In addition, if the issuer approved the transaction online but it was declined by the card (e.g., due to Issuer Authentication failure), the device must generate a reversal. See Section 6.4.8: Reversals for details.

4.12.3 Online-Authorized Transaction Scenarios

This section provides a summary of information for online-authorized transactions.

For general information on device capture, host capture, and single-message processing, see Section 1.3: Processing Options.

Device Capture

These devices typically use dual-message processing. They exchange data with the acquirer once for online authorization (where applicable) at the time of the transaction and once later for clearing the transaction (typically via batches).

For chip transactions with an online authorization:

- ARQC and its associated data will be submitted in the authorization message.
- TC and its associated data will be submitted in the clearing transaction.[36]

[36] Assuming the acquirer provides chip data in the clearing transaction. For example, in the U.S., chip data is not required in clearing or settlement of chip transactions that were approved online.

The device should send the same data in the batch data capture message that was sent to the card in the GENERATE AC command immediately preceding the creation of the batch data capture message. For example, when a tip is added to the transaction amount at the end of the transaction, both the amount used in the GENERATE AC command and final amount should be sent in the clearing message.

Note: If the transaction is approved offline, there will only be a clearing message that contains the TC and its associated data (there will not be an online message).

Single Message/Host-Capture

These environments typically use a single message for authorization and clearing. For these environments, where the transaction is sent online, the ARQC and its associated data is considered sufficient. The device/acquirer does not need to submit the TC and its associated data for financial/clearing.

Important: Even though these devices will not submit the TC and its associated data, they should always finish the transaction by requesting a final cryptogram from the card.

Generally, the TC is discarded in single-message or host-capture environments; however, some countries may require retention of the TC and define the appropriate advice messages needed for transmission of it. Contact your Visa representative for details.

ATMs

For most ATM transactions, whether single- or dual-message, the clearing message contains the ARQC and not the TC. In most dual-message ATM implementations, the acquirer host captures the authorization response from the issuer to create the clearing message and does not have access to the final TC (similar to POS host-capture). If the ARQC is used in the clearing message, a valid Authorization Code is required.

Data Elements

Many data elements used in the generation of the Application Cryptogram are likely to be different between the authorization message and the clearing message. It is critical to use the data elements associated directly with the cryptogram provided in the message. Besides the cryptogram itself (ARQC or TC), the following data element values are also likely to differ between authorization and clearing:

- Card Verification Results (CVR) (the cryptogram type is updated as well as the Issuer Authentication results)
- Terminal Verification Results (TVR) (updated with Issuer Authentication results)
- Amount, Authorized (in some cases, such as partial approvals and travel and entertainment transactions, the amount in the authorization may differ from the final amount in clearing)

- Unpredictable Number (the Unpredictable Number in the clearing message must be the one used for the cryptogram included in the clearing message)

4.12.4 Authorization Response Cryptogram (ARPC) Considerations

Issuers may generate an Authorization Response Cryptogram (ARPC) as part of the response message to allow the card to validate that the response was provided by the legitimate issuer. This is known as Issuer Authentication. If the ARPC fails validation, the card may decline a transaction that was approved online. **In this situation, a reversal must be generated.** For more information on reversals, see Section 6.4.8: Reversals.

Issuer Authentication may fail for a variety of reasons including issuer host processing errors or acquirers modifying the data received from the issuer before it is passed to the device. The process of determining what happens if Issuer Authentication fails is determined solely by the settings in the card and the device should only follow the indications from the card.

4.12.5 Declined Transactions

Where the transaction results in an offline or online decline, the device should inform the merchant on the device display that the transaction has been declined. For the display to the cardholder, the message “NOT AUTHORIZED” may be preferred.

Authorization responses indicating a decline may contain an Issuer Script to be acted on by the card. If so, the Issuer Script must be processed.

In most countries, declines are deleted from the device; however, in a few countries, for auditing purposes, declined transactions are delivered along with the clearing batch to the acquirer (although the declines might not be forwarded to the issuer). Check with your Visa representative for the requirements in your market.

4.13 Transaction Conclusion

This section outlines considerations for finishing a transaction:

Note: This is not an official EMV step and should not be confused with “Completion” (which is an official EMV step and outlined in the previous section).

- **Transaction Finalization** – At the end of the transaction, assuming it was approved, the financial exchange is completed and the good/services or ATM cash along with a receipt (if applicable) are provided to the cardholder.
- **Card Remains in Reader During Transaction** – It is important to remember that, unlike magnetic-stripe transactions, the chip card remains in the chip-card reader until the last EMV chip transaction step which includes generating the final cryptogram. To support this, the device should display information to the cardholder to clearly communicate when to remove the card from the reader. If the card is removed before the transaction is finished, the transaction may fail.
- **Card Removed Before Device Receives TC/AAC From Card** – In this situation, the transaction is terminated and a new transaction should take place. If an online authorization occurred, a reversal message should be sent.
- **Card Removed After Second Cryptogram Generation but Before Issuer Script Processing** – In this situation, the transaction is considered complete and the transaction disposition is unchanged. To mitigate this, the device must not display a message indicating that the transaction has been approved or declined until after the completion of Issuer Script Processing; however, a script failure should not result in a declined or reversed transaction (except in the case of non-financial transactions requiring Issuer Script Processing, such as PIN Management at an ATM).

5. Contactless-Chip Acceptance

This section provides an overview of the *VCPS* and *EMV Contactless Specifications* requirements and recommendations for contactless devices focusing on quick Visa Smart Debit/Credit (qVSDC).

Note: Magnetic Stripe Data (MSD) was a Visa contactless solution that utilized the Track 2 Equivalent Data and magnetic-stripe rules to process contactless transactions. MSD is outside the scope of this document.

For more information on developing a device that accepts Visa contactless-chip cards, see the *VCPS* or the *EMV Contactless Specifications*, Book C-3. Vendors developing products that support Visa contactless-chip cards have the option of using either specification.

Important: *VCPS* and the *EMV Contactless Specifications* are collectively referred to as the “Contactless Specifications” in this section.

Note: Unless otherwise noted, all requirements in Section 2: General Acceptance apply to contactless-chip devices. Device vendors and acquirers should ensure their contactless devices meet those requirements as well as the requirements outlined in this section.

5.1 Quick Visa Smart Debit/Credit (qVSDC)

qVSDC is 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. 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.

Acceptance devices that support qVSDC usually have the contactless acceptance functionality integrated into the 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. The term “reader” in this section covers both scenarios unless explicitly stated otherwise.

5.2 Processing Overview

This section highlights contactless-reader requirements while outlining the different phases of a contactless transaction.

The phases of a contactless transaction are:

- Preliminary Processing
- Application Selection
- Dynamic Reader Limits (Optional)
- Card Requests Terminal and Transaction Data
- Fast Dynamic Data Authentication (fDDA) (Conditional)
- Cardholder Verification
- Transaction Terminated
- Online Processing
- Transaction Outcome

5.2.1 Preliminary Processing

Requirement: The reader must support Preliminary Processing and be loaded with the Reader Cardholder Verification Method (CVM) Limit and the Reader Contactless Floor Limit. Contact your Visa representative to obtain the limits for your market.

Background: Preliminary Processing expedites the transaction by allowing the reader to perform several risk management steps prior to interacting with the card.

During preliminary processing, the merchant typically provides the transaction amount to the reader and the reader uses it to perform the following checks:

- **Reader CVM Required Limit** – Contactless transactions above this limit require cardholder verification. This limit is normally set to the VEPS limit.
- **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.

Note: There is also a Reader Contactless Transaction Limit in the contactless device. Transactions for amounts above this limit are terminated and may be processed only by using a different interface. All new contactless readers should have this limit disabled or set to its maximum value.

The reader sets the results of these checks in the Terminal Transaction Qualifiers (TTQ), a reader data element. The reader provides the TTQ to the card later in the transaction and the card uses it to understand the reader's capabilities and requirements. See Section 5.2.4: Card Requests Terminal and Transaction Data for details.

5.2.2 Application Selection

Requirement: The reader must support Application Selection, must be loaded with the Application Identifiers (AIDs), and must support Partial Name Selection. See Section 4.3: Application Selection.

Note: Contactless transactions do not support Cardholder Selection in the same way as contact-chip transactions due to the minimal interaction between the contactless reader and the consumer device (e.g., card, mobile phone). In the most scenarios, the reader will select the highest priority AID on the consumer device.

Background: Once the reader has completed Preliminary Processing:

- The reader signals to the consumer that it is ready for the contactless card.
- Rather than inserting the card in the chip reader, the cardholder briefly waves or holds the card close to the contactless reader to initiate the transaction.

  Note: Merchants and acquirers should be aware that form factors other than cards, such as mobile phones, may be used to initiate the contactless transaction.
- The reader determines whether it shares a contactless application with the card by selecting the card's list of contactless applications called the Proximity Payment Systems Environment (PPSE).
- If there is one or more applications in common, identified by the Application Identifier (AID), the highest priority application is automatically selected.[37]
- Otherwise, the reader terminates the transaction and the transaction may proceed via another interface such as contact chip or magnetic stripe.

Note: AIDs may have a length of 5 to 16 bytes. As per the Contactless Specifications, devices must be able to select AIDs that are between 5 to 16 bytes in length.

[37] Special logic may allow selection of alternate AIDs as further described in the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide,* Chapter 2, section on "Special Application Selection Logic," Appendix on "Basic EMV Terminal Logic," and Appendix on "Special Application Selection Logic."

5.2.3 Dynamic Reader Limits (Optional)

Requirement: The reader may optionally need to be set up with Dynamic Reader Limits. These limits may be mandatory in some countries. Contact your Visa representative for details. Acquirers should also check to see if there is an applicable Application Program Identifier (Program ID) for their country and acceptance environment.

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

- **Program ID Does Not Match** – When the card returns a Program ID that does not match a reader Program ID (or the card does not return a Program ID), the reader processes the transaction using the default reader limits and results determined during Preliminary Processing. See Section 5.2.1: Preliminary Processing for details.
- **Program ID Matches** – When the card returns a Program ID that matches a reader Program ID (full or partial), the reader uses the reader limits associated with the matching Program ID to process the transaction.
  - For example, the default reader limits in Preliminary Processing may use a Global Reader CVM Required Limit of $25, and the reader may have a Reader CVM Required Limit of $100 for domestic cards (as identified by the matching Program ID). In this case, the Reader CVM Required Limit will be $100 for domestic cards and $25 for international cards.

5.2.4 Card Requests Terminal and Transaction Data

Requirement: The device must support the TTQ and the acquirer should have the capability to update the TTQ-associated values in the device when the reader capabilities change or if there is a Visa requirement to change the supported values.

Background: Once the application is selected, the contactless card responds by requesting information including the Transaction Amount, TTQ, and the reader's Unpredictable Number for use during the transaction. The reader responds with the requested information. The card uses the information provided in the TTQ to make risk management decisions before responding to the reader.

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 and/or the use of the dynamic reader limits, if applicable)
- What CVMs are supported (the reader must indicate support for CDCVM)
- Whether the reader supports Issuer Update Processing (optional)

For more information on the TTQ, see Section 5.5: Other Contactless Processing Considerations.

Note: The Contactless Specifications do not require the use of a Transaction Certificate Data Object List (TDOL). Vendors or acquirers may set the default TDOL to any value since it is not used for processing of Visa contactless transactions.

5.2.5 Fast Dynamic Data Authentication (Conditional)

Requirement: The reader may be required to support fDDA. 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 does not need to support fDDA.

Background: fDDA is similar to Dynamic Data Authentication (DDA) with the following differences:

- To optimize processing power and reduce transaction times, the fDDA dynamic signature is generated during the GET PROCESSING OPTIONS command rather than generating it at the end of the transaction using the INTERNAL AUTHENICATE command (when the card may be moving away from the reader Radio Frequency (RF) field). The DDOL is not used.
- The results of fDDA are not provided online to the issuer within the TVR or protected by the online authorization or clearing cryptograms.
- In addition to signing the Unpredictable Number (from the reader), which is signed in most EMV contact-chip applications, fDDA also signs additional dynamic transaction data including the Amount, Authorized, Transaction Currency Code, and the Unpredictable Number (from the card).

5.2.6 Cardholder Verification

Requirement: The reader must support cardholder verification and must support specific CVMs. For details, see Section 2.8.2: CVMs by Device Type.

For contactless, 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 a contact-chip transaction with Offline PIN, and then Signature.
- For cards compliant to VCPS 2.2.1 or later, the CVM hierarchy is configurable.

For consumer devices (e.g., mobile phones), CDCVM is generally the only CVM supported.

5.2.7 Transaction Terminated

Background: Rather than decline a transaction needlessly, if the transaction cannot be completed as a contactless transaction but may be completed via another interface, the contactless transaction may be terminated and may be processed as a contact-chip or magnetic-stripe transaction.

Important: Terminated transactions differ from declined transactions because declined transactions may not be reinitiated via another interface.

5.2.8 Online Processing

Requirement: For online transactions, the device needs to send the transaction online to the acquirer with all applicable data. The acquirer needs to forward the transaction to the issuer, receive the issuer's response, and send the issuer's response to the device.

Processing:

- The reader indicates to the cardholder that the card can be removed from the reader's field.
- The reader sends the transaction to the acquirer. The data identifies the transaction as a contactless transaction and includes the cryptogram and its associated data.
- The acquirer formats the authorization message with the chip data in Field 55.[38] See the *VSDC System Technical Manual* for details on the data elements required in authorization and clearing/settlement messages.
- Based on the results of Online Card Authentication, along with other standard risk management checks (such as ensuring that the card is not expired, verifying that the account is in good standing, and ensuring it has available funds), the issuer either approves or declines the transaction as part of the authorization response.
- The authorization response is sent to the acquirer which logs the response and forwards the response to the device.

[38] Most countries require the acquirer to support the chip data in Field 55, although some allow support for the expanded third bit map. Check with your Visa representative for the rules in your country.

5.2.9 Transaction Outcome

Background: During this phase of the transaction, the reader conveys the issuer's authorization response by displaying whether the transaction is approved or declined.

If the transaction is approved:

- The transaction may not require a cardholder signature or a receipt (depending on Visa and domestic rules).
- The device captures the cryptogram and the associated data and later submits it as part of clearing and settlement (as applicable).

5.3 Consumer Devices and Contactless

From an acceptance perspective, consumer devices (such as mobile phones) that contain a Visa contactless payment application can be accepted in any reader that accepts Visa for contactless payment.

Visa contactless transactions that originate from consumer devices have the same processing requirements as Visa contactless transactions that originate from cards. There are no processing differences between a transaction originating from a card and a transaction originating from a mobile phone from the point of view of the transaction processing, authorization, and clearing data that is passed through VisaNet systems.

5.3.1 CDCVM and Pre-Tap

When the consumer is using a consumer device capable of an on-device CVM (such as a mobile phone) to conduct the transaction and a CVM is required on the transaction, the cardholder removes their consumer device from the contactless reader, performs the CVM (such as biometrics) on the consumer device, and then re-presents the consumer device to the reader to complete the transaction. This process is referred to as pre-tap.

Note: Pre-tap and CDCVM as a recognized CVM are supported by readers compliant to *VCPS*, Version 2.1 and above.

The following is a description of the processing flow for CDCVM and pre-tap:

Table 5–1: CDCVM and Pre-Tap Process Flow

Step	Description
1.	The consumer device is presented to the contactless reader and a CDCVM is required to complete the transaction. A CDCVM may be required for many reasons, including, but not limited to, the following: • Consumer device is configured to require a CDCVM for every transaction. This may be the result of cardholder or issuer configuration settings. • A CVM is required for the transaction and CDCVM is the common CVM supported by both the consumer device and the contactless reader. CDCVM is performed and verified entirely on the consumer device. No additional action is required of the merchant or device to perform cardholder verification, unlike with Signature or Online PIN.
2.	The consumer device sends an indication to the contactless reader that some form of consumer interaction is required with the consumer device to complete the transaction. The consumer device accomplishes this by sending the GET PROCESSING OPTIONS (GPO) response with Status Word = '6986'.
3.	Upon receipt of this indication, the contactless reader displays a message instructing the cardholder to consult their consumer device for further instructions, and, after a short duration (usually a couple seconds), the contactless reader returns to Discovery Processing to await the re-presentment of the consumer device to reattempt the transaction.
4.	Once the cardholder has performed the necessary action on the consumer device (e.g., successfully performed a CDCVM), the cardholder re-presents the consumer device to the contactless reader and the transaction is completed. **Note:** An indication is sent to the reader and to the issuer that a CDCVM was performed for the transaction.

Similarly, the following is a description of the processing flow when a CDCVM is required and was performed by the cardholder prior to presenting the consumer device to the contactless reader (i.e., no pre-tap):

- Cardholder performs CDCVM before consumer device is presented to contactless reader.
- Cardholder presents the consumer device to the contactless reader.
- Consumer device determines that a CDCVM is required to complete the transaction and that a CDCVM has already been performed.
- The transaction is completed.

In this latter scenario, although a CDCVM was required for the transaction, a CDCVM had already been performed (no pre-tap), and the transaction was completed on the initial presentment of the consumer device.

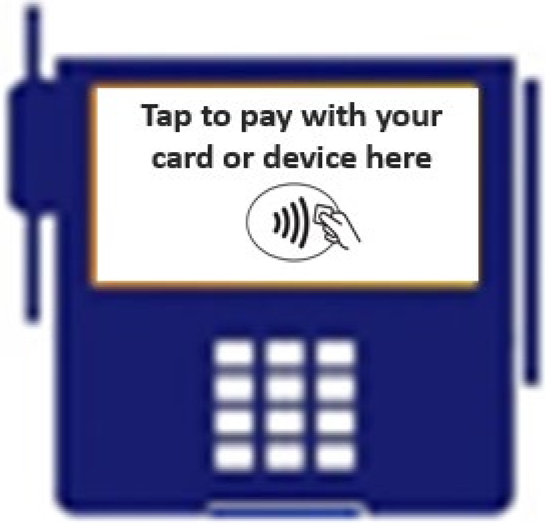
5.4 Device User Interface Recommendations

It is important that the cardholder's contactless payment process is as easy and intuitive as possible. To avoid confusion, it is important to have a consistent way to inform the cardholder about when and where to present their card/consumer device and when to remove it.

EMVCo has developed a set of user interface recommendations that provide best practices on how to design a device with a user interface that will provide a consistent consumer experience. Some of the recommendations include:

- The cardholder interface should provide a visual and audio indication of the appropriate status of a contactless transaction.
- The reader should support language selection as defined in the *EMV Chip Specifications*.
- The reader should support a standard set of display messages. The messages may also be complemented by corresponding visual and audio indications. See the *EMV Contactless Specifications*, Book C-3 for details.
- The POS environment should promote acceptance of contactless cards through marketing materials and signage.
- The reader must display the EMV Contactless Symbol on the device; it should be displayed in the appropriate location to indicate where the cardholder should tap their contactless card/consumer device (see Figure 5–1: Device Illustration with EMV Contactless Symbol).

Figure 5–1: Device Illustration with EMV Contactless Symbol



Certain regions have specific user interface requirements; contact your Visa representative to confirm local or regional requirements.

For details, see the *EMVCo Contactless Symbol Reproduction Requirements* and the Visa Merchant Signage website at www.merchantsignage.visa.com.

5.5 Other Contactless Processing Considerations

The section provides other processing considerations for contactless transactions:

- **Preventing "Switch Interface"** – To help ensure a positive cardholder experience over the contactless interface, the device needs to be set up so that the card does not unnecessarily reject the transaction. To accomplish this, the TTQ should have the following settings:
  - Signature and Online PIN supported (Byte 1, bits 2 and 3 set to 1b).
  - A CVM is NOT required (Byte 2, bit 7 set to 0b).
  - Consumer Device CVM (CDCVM) supported (Byte 3, bit 7 set to 1b).
- **Premature Card Removal** – If the card is removed before the transaction is complete (i.e., the transaction has not reached the Card Read Complete step), then the current transaction data is discarded and the reader returns to Discovery Processing.
- **Gratuities or Tips** – Gratuities/tips may be handled as described in Section 6.5.4: Gratuities/Tips.
- **Placement of Contactless Readers** – Visa has developed a set of recommendations for the placement of contactless readers/devices in a merchant retail environment. For more information, see Appendix A: Contactless Reader Placement.
- **Dynamic Currency Conversion (DCC)** – DCC is permitted on Visa contactless transactions. For more information on DCC, see Section 2.17: Dynamic Currency Conversion (DCC).

6. Chip-Card Processing

This section focuses on how to process specific transaction types initiated via a contact or contactless card. It includes the following sections:

- Quick Chip for Contact and Contactless
- Deferred Authorizations
- Acquirer Stand-in
- Other Transaction Types
- Industry-Specific Transactions
- Cash Back Transactions
- Online-Only POS Environments
- Non-EMV/VCPS Transactions Using EMV/VCPS Functionality
- Configurable/Selectable Kernels

Note: Fallback transaction processing is covered in Section 4.2.2: Fallback Acceptance for Chip Read Failures.

6.1 Quick Chip for Contact and Contactless

While it relies on standard EMV processing, Quick Chip allows for the removal of the contact-chip card from the device prior to receiving an online response to expedite the transaction. During the transaction, the card can be removed from the device before the processing of the final transaction amount, authorization response, and other post-authorization processing such as Issuer Authentication and Issuer Script.

Quick Chip:

- Significantly reduces the time of the card in the device.
- Provides an EMV level of security for online authorizations, including the cryptogram.
- Integrates with Visa Easy Payment Service (VEPS) processing.
- Supports all Cardholder Verification Methods (CVMs).

Quick Chip is a solution that is only applicable to online-only markets. Contact your Visa representative if you are interested in more information.

6.2 Deferred Authorizations

Deferred Authorization is where one of the following occurs:

- An online authorization is performed after the card is no longer available, typically because the device temporarily does not have a connection (e.g., communications failure or device is on a transit vehicle).
- Amount is over the floor limit and the device does not have online capability but the merchant elects to complete the transaction with the cardholder.

The merchant is at risk for those transactions that are subsequently declined, or, if cleared, the acquirer is liable in the event that the transaction is disputed for "No Authorization."[39]

Merchants performing Deferred Authorization should complete authorizations within 24 hours of the transaction (select MCCs have a longer timeframe). See the *Visa Rules* for details.

For chip transactions, a Deferred Authorization is processed as follows:

- In the case of contact chip, the device requests an ARQC and the card responds with one.[40] The device then informs the card that it cannot go online and requests an AAC.
- In the case of contactless, an ARQC is returned by the card.
- Later, the device uploads the deferred authorization requests that include the ARQCs.[41]
  Field 63.3: Message Reason Code must contain a value of **5206**.
- The acquirer submits the authorization requests, most of which are approved online.
  - Repeated attempts at authorization for declined transactions are permitted but declined transactions must eventually be discarded.
- The acquirer formats and submits a clearing record[42] for each approved transaction, using the ARQC and the Authorization Response Code returned in the authorization response.

Note: In countries with a non-zero-floor limit, the device may attempt to obtain an offline approval for under-floor limit transactions. For these offline-approved transactions, the TC is provided in the clearing record.

[39] For exceptions related to transit, see the *Visa Contactless Transit Terminal Implementation Guide*.
[40] Acquirers may want to consider checking the results of Offline Data Authentication and/or Offline PIN to manage their risk; however, if most cards in the country do not support offline functionality or if the merchant processes a high percentage of transactions from international issuers, the acquirer may decide to accept the risk in the interest of customer satisfaction.
[41] Use of the AAC rather than the ARQC in the authorization request may result in unnecessary declines by the issuer.
[42] Assuming the acquirer provides chip data in the clearing transaction. For example, in the U.S., chip data is not required in clearing or settlement of chip transactions that were approved online.

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*.

6.3 Acquirer Stand-In

Acquirer Stand-in (also called Authorization Truncation or Acquirer Forced Settlement) may take place when the acquirer or the device temporarily does not have a connection (communications failure) or the acquirer deems the risk of dispute to be less than the cost of authorization. The acquirer "stands in" for the issuer and returns a positive authorization response; however, because the acquirer does not have the issuer's authorization decision criteria, the acquirer is liable for these transactions in the event that they are disputed for "No Authorization."

Important: Deferred Authorization (see previous section) is the preferred approach for situations where the acquirer is unable to obtain issuer approval. Acquirer Stand-in is not allowed in some countries such as the U.S. In addition, it may have cost or fee considerations and/or may leave the merchant/acquirer open to compliance actions. Acquirers should also be aware that if the card approves offline, but the transaction amount is above the domestic floor limit for this merchant category, the merchant/acquirer is still liable for disputes associated with "No Authorization."

For chip transactions, an Acquirer Stand-in is processed as follows:

- The card generates an ARQC to indicate that the transaction must be sent online, but the acquirer is unable to communicate with the issuer.
- In the case of contact chip, the device indicates to the card that the transaction was unable to go online and the card may either approve the transaction (by sending the device a TC) or decline the transaction (by sending the device an AAC). [43]
- For approved transactions, the acquirer submits the TC along with its associated data following normal procedures.
- For declined transactions:
  - The decline is overridden (either by the device or by a message from the acquirer).

[43] Acquirers may want to consider checking the results of Offline Data Authentication and/or Offline PIN to manage their risk; however, if most cards in the country do not support offline functionality or if the merchant processes a high percentage of transactions from international issuers, the acquirer may decide to accept the risk in the interest of customer satisfaction.

- The acquirer clears the transaction at its own liability for disputes associated with “No Authorization.” For these transactions, the acquirer submits the AAC and its associated data.[44]
- The device displays a message to the cardholder (this message is determined by the acquirer but is not a decline message), the consumer receives the goods/services, and the transaction is cleared.

Important: The issuer may dispute these transactions if either they cannot collect from the cardholder or the cardholder disputes the transaction.

6.4 Other Transaction Types

The *EMV Chip Specifications* provide information on how to process basic purchase and Cash Disbursement transactions. This section provides high-level information on how chip impacts other transaction types. The information in this section applies to both contact and contactless transactions, unless otherwise noted.

Note: When the information in this section refers to “full chip data,” this means the message includes the cryptogram and all the data associated with the cryptogram.

Important:

- All transaction types in this section need to be identified correctly with Visa-specific values.
- All transaction types in this section are subject to the *Visa Rules*. For more information, see the *Visa Rules*. See also the *Recommendations for EMV Processing for Industry-Specific Transaction Types* available at www.emvco.com.

6.4.1 Pre-Authorizations

Definition: A pre-authorization is an online authorization that takes place before the final amount is known. This transaction is used in conjunction with incremental authorizations (if applicable) (see Section 6.4.2: Incremental Authorizations) and sale completions (see Section 6.4.3: Sale Completions).

Transaction: This transaction may be one of the following:

- Online chip authorization with full chip data (assuming a chip card is present and used to initiate the transaction).
- Key-entered transaction.

[44] Assuming the acquirer provides chip data in the clearing transaction. For example, in the U.S., chip data is not required in clearing or settlement of chip transactions that were approved online.

Notes:

- In certain environments, any estimated amount used for a pre-authorization is likely to be the maximum dispensable value of goods or services.
- Per PCI DSS, merchants may store the PAN and expiry date from the pre-authorization to use on subsequent incremental authorizations (if applicable) but they must not store the full chip data or the Track 2 Equivalent Data from the chip. See Section 6.4.2: Incremental Authorizations for more information.
- The amount presented to the card in the GET PROCESSING OPTIONS command of a pre-authorization should be an estimated amount and should be the same amount and currency that is sent to the issuer in the pre-authorization request message.

6.4.2 Incremental Authorizations

Definition: 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.

Transaction: These are usually key-entered transactions; however, if a chip card is present and read, the resulting transaction is an online chip authorization with full chip data.

Processing:

- Although not typical, if the chip card is present for the incremental authorization, an online chip authorization with full chip data may take place.
- Alternatively, merchants can use the card’s PAN and expiry date obtained from the pre-authorization to perform a key-entered incremental authorization.
- If the original pre-authorization was a chip transaction:
  - The chip data obtained during the pre-authorization must not be resubmitted during incremental authorizations.
  - As noted in Section 6.4.1: Pre-Authorizations, the merchant must not store the full chip data or the Track 2 Equivalent Data from the original pre-authorization.

6.4.3 Sale Completions

Definition: A sale completion is 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. The final transaction amount may differ from the authorized amount, usually within a range defined by the local environment.

Transaction: This transaction is the clearing component of a pre-authorization and any associated incremental authorizations.

Processing:

- If possible, merchants should use incremental authorizations to ensure the final authorization amount matches the sale completion amount. This ensures the cardholder's open-to-buy accurately reflects their transaction activity.
- If the original pre-authorization was a chip transaction, the full chip data from the pre-authorization should be included in the clearing message[45] or, in the case of multiple clearing messages (where multiple items are purchased but delivered separately), in each of the clearing messages. In the event of multiple clearing messages, the total of the sale completions should add up to the amount of the pre-authorization plus any associated incremental authorizations, if applicable.
- The POS Entry Mode Code for a sale completion should be set to "chip read" only if it contains the full chip data from an original chip-based pre-authorization.
- It is recommended that the Authorization Code from the original pre-authorization response message (as opposed to those obtained from incremental authorizations) be used in the sale completion as this code will generally be associated with the highest value transaction.

6.4.4 Status Checks

Definition: A status check is 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 and is not allowed in some markets.

Transaction: This transaction is an online authorized chip transaction for a single unit of currency with full chip data.

[45] Assuming the acquirer provides chip data in the clearing transaction. For example, in the U.S., chip data is not required in clearing or settlement of chip transactions that were approved online.

6.4.5 Account Number Verifications

Definition: An account number verification is an online authorization for a zero amount. It can be used to validate that the card used to pay for services in advance of delivery or to make a reservation is authentic.

Transaction: This transaction may be one of the following:

- Online chip authorization for a zero amount with full chip data (assuming a chip card is present and used to initiate the transaction).[46]
- Key-entered transaction for a zero amount.

6.4.6 Merchandise Returns/Refunds

Definition: A Merchandise Return/Refund is 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.

Important: Effective October 2019 (Canada, LAC, and U.S.) and effective April 2020 (AP, CEMEA, and Europe), all merchants must send an online authorization message to the issuer for merchandise returns/refunds. See the *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*.

Transaction: This transaction may be one of the following:

- An online chip authorization where full chip data is strongly recommended followed by a clearing transaction where full chip data is strongly recommended.[47]
- Key-entered authorization transaction following by a clearing transaction.

Processing: The processing depends on merchant procedures. Possible solutions follow:

- **Chip Transaction** – The cardholder's chip card is used to initiate the return/refund (to the extent possible, this should be the card used to perform the original purchase transaction).
  - The transaction is a chip-card transaction with a POS Entry Mode indicating "chip read" and it is strongly recommended that the transaction contains full chip data.
  - The transaction is properly identified as a return/refund. See the VIP manuals for details.
  - The chip data from the original purchase transaction must **not** be resubmitted/replayed on the return/refund.

[46] A tokenized transaction must include chip data.

[47] Assuming the acquirer provides chip data in the clearing transaction. For example, in the U.S., chip data is not required in clearing or settlement of chip transactions that were approved online.

  - If the PDOL indicates that the Transaction Amount and the Transaction Type are to be included in the GET PROCESSING OPTIONS command, it is recommended that the device send the refunded amount as the Transaction Amount and the Transaction Type (Tag '9C') as 20. If the PDOL indicates the Transaction Amount is to be included, but not the Transaction Type, the Transaction Amount should be set to zero.
  - If an attempted chip refund fails (e.g., if the chip cannot be read, chip technology fails during the transaction, or the transaction is declined), the merchant should re-initiate the refund transaction either by using the magnetic stripe or by key entry.
- **Key-Entered Transaction** – The merchant looks up the original transaction in their system and uses the stored PAN and expiry date from the original transaction to perform a key-entered return/refund authorization followed by a clearing transaction. Another option is to read the chip to obtain the PAN and expiry date but then submit the authorization as key entered (and without chip data) followed by a clearing transaction.

6.4.7 Partial Authorizations

Definition: A partial authorization occurs when the issuer provides an authorization response for an amount which is less than the transaction amount requested by the merchant (this may happen if the cardholder balance is not sufficient to allow the transaction for the full amount).

Transaction: A chip transaction with full chip data.

Processing:

- **Clearing Amount** – The device or acquirer must submit the amount from the partial authorization response as the Source Amount in the clearing transaction.
- **Reversals** – Following standard procedures, if the goods/services provided to the cardholder end up being less than the authorized amount in the partial authorization, the acquirer must submit a reversal for the difference. See Section 6.4.8: Reversals for information on reversals.
- **Disputes** – Following standard procedures, if the transaction is cleared for an amount that is greater than the authorized amount in the Partial Authorization, the issuer may have the right to dispute the difference as a “No Authorization” dispute.

6.4.8 Reversals

Definition:

- A reversal is a function of the transaction network or of the device application; it does not require interaction with the card.
- A reversal is an online message that is used to notify the issuer that the previous online authorization response was not able to be completed. This could occur due to a systems timeout/communications problem or because the transaction has been annulled or voided by the device for whatever reason.

- A reversal should be generated any time an approval is received for an online authorization request but where the authorization cannot be completed.
- For chip, a reversal must be generated when the issuer approves the transaction but the card overrides the approval and declines the transaction (e.g., due to Issuer Authentication failure where the ARPC sent by the issuer in the authorization response message was verified by the card but failed).

Transaction: This is an exception transaction associated with an original online chip transaction (assuming a chip card was used to initiate the original transaction).

Processing:

- An online chip authorization took place but was not successful per one of the situations outlined in the Definition section above.
- The device or the network sends the reversal to the issuer. Interaction with the card is not required.
- If the device generates a reversal for a transaction containing an ARQC, then, in the case of contact chip, the device should request an AAC from the card to avoid unnecessary requests for online authorizations on subsequent transactions.
- If the contact-chip situation where the issuer approved the transaction but the card declined it (usually due to Issuer Authentication failure), the following data elements may optionally be included in the reversal:
  - TVR (updated with the Issuer Authentication results)
  - CVR (updated with the Issuer Authentication results)
  - Issuer Script results (if the original authorization response message from the issuer contained an Issuer Script, the Issuer Script results are provided in this field)
  - **Note:** Other than these data elements, chip data does not need to be included in a reversal.

Partial Reversal: A partial reversal reverses a portion of the original transaction amount. Acquirers and merchants submit a partial reversal when an estimated amount exceeds the final value of the completed transaction. For instance, if the estimated amount is USD$200 but the final amount is USD$100, then a partial reversal can be submitted for the USD$100 difference between the estimated and final amounts. The chip-related requirements for partial reversals are the same as those for full reversals.

6.4.9 Cancellations

Definition:

- A cancellation occurs when a purchase or sale completion transaction is aborted either during or after processing. In a dual-message environment, a cancellation should only occur before the transaction is cleared to the acquirer.
- There are a number of reasons why a cancellation may occur, such as an error in the amount entered by the merchant which the merchant may seek to correct by pressing a cancel button on the device. Cancellations also occur when a merchant does not approve the cardholder's signature.
- Initiation of a cancellation should result in the cessation of processing and clearing of any data elements.

Transaction: This is an exception transaction associated with an original chip transaction.

Processing:

- If the cancellation occurs before the first cryptogram generation, the card can simply be powered off.
- If the cancellation occurs after going online but before the second cryptogram generation, then the device/merchant should complete the transaction with an AAC and generate a reversal. The transaction should be removed from the clearing batch or marked as void.
- If the cancellation occurs after going online and after second cryptogram generation, then the device/merchant should generate a reversal. The transaction should be removed from the clearing batch or marked as void.
- If the transaction has completed and the final cryptogram is an AAC, there is no need to cancel the transaction since it has been declined.
- If the transaction has completed and the final cryptogram is a TC, the merchant should cancel the transaction and send a reversal to the issuer. The transaction should be removed from the clearing batch or marked as void.
- It is recommended that the device produce a receipt for the cardholder showing that the original transaction has been cancelled.

6.5 Industry-Specific Transactions

Certain industries have specific payment requirements besides the traditional purchase. For each scenario, the presence of a chip card may or may not have an impact on existing processing requirements. The following sections outline possible changes to processing when a chip card is used.

If the transaction is completed by extracting data from the chip (but not following the entire EMV payment transaction flow), the transaction is considered key entered. For information on key-entered transactions, see Section 2.15: Key-Entry Transactions.

6.5.1 Hotels and Tourism Industries

The various activities relating to payments in the hotel industry should be treated as follows:

Table 6–1: Hotels and Tourism Industry Transactions

Topic	Description
Reservations	This process does not normally involve the card being present or the chip being read so normal procedures should be followed.
No-Shows	Same as reservations.
Check-In with Pre-Authorization	A pre-authorization is completed at check-in to ensure the card and cardholder are genuine and to guarantee the funds before the final transaction amount is known. Local requirements will determine the estimated amount to be used. To avoid confusion, the estimated amount should not be displayed to the cardholder. The estimated amount is the amount presented to the chip card. Depending on merchant procedures, the transaction will be a chip transaction (assuming chip card present) or a key-entered transaction for the estimated amount. For more information on pre-authorizations, see Section 6.4.1: Pre-Authorizations.
Extended Stay or Higher Than Estimated Spending	If the estimated amount used for the pre-authorization is no longer sufficient to cover the estimated final bill, incremental authorizations should be performed. In most situations, the card is not present. For more information on incremental authorizations, see Section 6.4.2: Incremental Authorizations.
Express Check-Out	It is not necessary to perform a complete card-present chip transaction once the final transaction amount is known. A sale completion (which is a clearing transaction) is generated for the final billing amount and, if the original pre-authorization was chip-based, then the chip data from the original pre-authorization is included. For more information on sale completions, see Section 6.4.3: Sale Completions.
Additional Charge After Check-Out	Any additional charges identified after check-out should be processed as a new/separate card-absent transaction. The chip data from the pre-authorization should not be submitted in the clearing record.

Similar processes to those described above may be used for the car rental or other tourism and travel industries. Acquirers and merchants should review the *Visa Rules* or contact their Visa representative for more information.

6.5.2 Fuel/Petrol Dispensing

The various activities relating to payments in the fuel/petrol industry should be treated as follows:

Note: In some AFD environments, due to the custom authorization process, it may not make sense to display the amount before PIN entry (because the final amount is not known).

Table 6–2: Fuel/Petrol Dispensing Transactions

Topic	Description
Pre-Authorization	For chip transactions, complete either of the following before fuel is dispensed: • **Status Check** – The status check provides authorization protection up to the domestic rule limit. • **Estimated Amount Transaction** – The estimated amount provides authorization protection up to the approved estimated amount. If approved, the merchant must: – In some countries, send a real-time sale completion for the actual amount within 2 hours (if operating under the Real Time Clearing program), or – Submit a reversal for the unused portion of the authorization and submit a sale completion for the actual amount. For more information on status check transactions, see Section 6.4.4: Status Checks. For more information on pre-authorizations, see Section 6.4.1: Pre-Authorizations. For more information on sale completions, see the row in this table and Section 6.4.3: Sale Completions.
Enhanced Automated Fuel Dispenser (AFD) Non-Financial Advice	In countries where Enhanced AFD is supported, merchants must follow a status check with an authorization advice within two hours of the status check for the actual amount. This advice must equal the sale completion amount.
Sale Completion	When fuel dispensing is completed and the final transaction amount is known, a sale completion (which is a clearing transaction) for the final amount should be submitted containing the chip data from the status check or pre-authorization. Single-message environments may require an adjustment to the pre-authorization amount, particularly if an estimated amount was used rather than a status check. For more information on sale completions, see Section 6.4.3: Sale Completions.

Offline chip approvals are not appropriate for fuel dispensing as it is not possible to readily adjust for the actual amount dispensed.

The process outlined above may vary in different countries and acquirers and vendors should consult with their Visa representative to confirm local requirements.

6.5.3 Mobile Top-Up

Mobile Top-Ups consist of a standard purchase transaction, sometimes followed by an advice to the service operator indicating that additional service has been purchased. An example would be the purchase of additional minutes for a mobile phone at a UCAT. Unless specifically requested by the service operator, the format of the advice message should be unaffected by use of a chip card to complete the purchase.

For the Merchant Category Code (MCC):

- **MCC 4814** – If the main function of the merchant environment is to provide top-up services (i.e., purchasing additional mobile minutes), use the MCC of 4814 (Telecommunication Services, including Local and Long Distance Calls, Credit Card Calls, Calls Through Use of Cellular Telephone Service).
- **Merchant MCC** – Otherwise, use the MCC associated with the merchant environment where the transaction is taking place.

If a top-up transaction is completed:

- With card-on-file data, the transaction is considered to be a card-absent transaction.
- Using the chip, the full chip data should be provided in the message.
- By extracting data from the chip (but not following the entire EMV chip transaction flow), the transaction is considered key entered.

Note: Only the PAN and expiry date should be stored, never full Track 2 data or the full chip data. When the PAN and expiry date are stored, they must be protected according to PCI DSS.

6.5.4 Gratuities/Tips

Gratuities/tips may be handled using one of the two options outlined in the following table; however, vendors should consult with their Visa representative, as:

- Local rules and regulations in some countries require the use of a specific option (and prohibit the other option), and
- Some countries may restrict the handling of gratuities/tips in these manners to specific MCCs.

Generally, countries outside of Europe will use option 1, while countries in Europe will use option 2.

Table 6–3: Gratuities/Tips Options

Options	Description	Authorization	Clearing
		Amount/Cryptogram Amount	**Amount/ Cryptogram Amount**[48]
Option 1	After authorization, a gratuity/tip is added of up to 20% of the base transaction amount to the authorized amount submitted in the clearing record	Amount *without* gratuity	Amount plus gratuity
Option 2	Gratuity/tip is added to the transaction amount before authorization	Amount plus gratuity	Amount plus gratuity

Note: Other Amounts/Cryptogram Cash Back Amount fields should not be used for processing tips.

6.5.5 Discounts

Some merchants may use the Primary Account Number (PAN) to determine if a discount applies to the transaction. To support this, the device should:

- Begin a chip transaction to obtain the PAN.
- Reach out to the other system(s) with the PAN to see if a discount applies prior to cryptogram generation.

[48] In the U.S., chip data is not required in clearing or settlement of chip transactions that were approved online. Where the ARQC is used in clearing, such as for single-message and host-capture systems, the ARQC should not be modified and thus may contain only the original amount.

6.6 Cash Back Transactions

This section outlines general and chip-specific requirements for cash back.

6.6.1 General Cash Back Requirements

General cash back requirements are outlined in the following table:

Table 6–4: General Cash Back Requirements

Topic	Description
Visa Rules and Local Requirements	Devices supporting cash back must be configured to meet all of Visa's cash back rules including any local requirements.
Domestic Transactions Only	Visa allows cash back to be provided with a purchase at the point of sale for domestic transactions, under certain conditions.
Online Authorization with Cardholder Verification	All cash back transactions must be online authorized and include appropriate cardholder verification (i.e., cash back transactions with Signature or "No CVM" are not permitted).
Separate Entry of Purchase and Cash Back Amounts	The device must be able to give the merchant the capability to enter purchase and cash back amounts separately.
Amount and Cash Back Amount in Transaction	The cash back amount must be uniquely identified in the authorization and clearing messages from the total transaction amount: • Total transaction amount (purchase plus cash back) in Amount, Transaction (Field 4). • Cash back amount in Other Amounts (Field 61.1).
Reconciliation	An end-of-day batch from devices must identify cash back amounts so merchants can reconcile with their cash drawers.
Cash Back Responses	The device must be able to handle responses relating to cash back such as: • A response from the issuer that the cash back service is not available to the cardholder. • A response that the cash back amount is more than the maximum cash back amount agreed for the country. (In this case, the merchant could retry the transaction for a smaller cash back amount or for the purchase amount only.) • A response that the cash back amount is equal to the total transaction amount (this is not allowed).

Note: Certain special conditions will require different actions by the merchant. Merchants may need to work with their acquirers to determine appropriate POS procedures.

For specific cash-back requirements for chip transactions, see the next section for details.

6.6.2 Chip Cash Back Requirements

This section outlines cash back requirements for chip transactions.

Note: Acquirers/merchants may need to enable cash back functionality in their chip devices by switching on the cash back setting in the EMV kernel.

For chip transactions, the sequence of cash back activities should be executed as follows:

1. **Cash Back Inquiry** – The device asks the cardholder if they would like cash back and, if so, obtains the cash back amount from the cardholder. It may be useful to inquire about cash back prior to Application Selection if the choice of cash back may affect the Application Selection process or other EMV processing.
2. **Amount Display** – The device displays the total amount of the transaction (the amount of the purchase plus cash back) to the cardholder. If the device supports amount confirmation, it requests the cardholder to confirm the amount.
3. **PIN Entry** – If PIN is applicable to the transaction, the device should provide the cardholder with the PIN prompt. PIN entry should be requested after amount display.

The device must send the amount and cash back amount to the card when requested and then send the following cryptogram data to the acquirer for inclusion in the online message:

- **Cryptogram Amount (Field 147, EMV Tag '9F02')** – This field contains the purchase amount plus the cash back amount.
- **Cryptogram Cash Back Amount (Field 149, EMV Tag '9F03')** – This field contains the cash back amount.
- **Cryptogram Transaction Type (Field 144, EMV Tag '9C')** – This field contains the value '00'.

Note: The requirements for Field 147 and Field 149 are in addition to the current requirements for Amount (Field 4) and Other Amounts (Field 61.1). Chip processing does not impact these existing requirements. See Section 6.6.1: General Cash Back Requirements for details.

The values in the Cryptogram Amount and Cryptogram Cash Back Amount must always be the values passed from the device to the card. The values should never be converted to other currencies or altered in any other way.

Important: Gratuities/tips should not be placed in the Cryptogram Cash Back Amount field. For more information on gratuities/tips, see Section 6.5.4: Gratuities/Tips.

6.7 Online-Only POS Environments

This section provides a summary of the requirements for online-only POS devices.

Online-only POS devices are not required to support EMV functions associated with offline transactions. These devices will always attempt to send the transaction online by requesting an ARQC during the first cryptogram generation.[49] If online processing is not available, the device will request an AAC in the second cryptogram generation.

Note: Devices may achieve being online only by setting the floor limit to zero (in conjunction with the Visa TAC settings) or through other means. Devices configured in such a way can be considered functionally equivalent to online-only devices.

The following EMV functions are eliminated or modified for online-only devices; otherwise, all other EMV functions apply:

- **Offline Data Authentication** – Online-only devices are not required to support Offline Data Authentication; therefore, they do not need to be loaded with the VSDC CA Public Keys (unless the device supports Offline Enciphered PIN).
- **CVM Support** – The kernel in attended POS online-only devices must minimally support signature (although the merchant is no longer required to capture and verify the cardholder's signature at a chip device).50 These devices may optionally support Offline PIN and/or Online PIN based on market needs. Support for particular types of PINs may be necessary to meet domestic requirements. Acquirers should check with their Visa representative on local CVM requirements. For the global minimum CVM requirements, see Section 2.8.2: CVMs by Device Type.
- **Terminal Risk Management** – Terminal Risk Management consists of a series of checks to protect the acquirer, issuer, and system from potential fraud by forcing some transactions online. Since online-only devices will always send the transaction online, Terminal Risk Management does not need to be supported.
- **Terminal Action Analysis** – Since online-only devices will attempt to go online and decline if online is not available, they may eliminate TAC - Online and TAC - Default processing and only support TAC - Denial processing (to decline offline if the service is not allowed for the card product). See Section 4.10: Terminal Action Analysis for details.

[49] These devices may decline the transaction offline if they check the card settings in the Application Usage Control and see that the card cannot be used in the environment.

[50] If the device is VEPS-only, the kernel does not have to support signature. For devices that support VEPS and non-VEPS transactions, a kernel may be invoked on VEPS transactions that supports "no CVM" only. For more information on VEPS, see Section 2.14: Visa Easy Payment Service (VEPS).

6.8 Non-Financial Transactions Using EMV or VCPS Functionality

It is possible to use EMV or VCPS functionality to undertake non-financial transactions. These transactions can use EMV or VCPS functionality to obtain information from the card (such as the PAN), to verify the validity of the card for identification purposes, and/or to validate the cardholder:

- The transaction amount for these transactions should be set to zero and there should be no clearing records.
- Contact-chip transactions should be completed with an AAC. In this instance, an AAC indicates completion and is not a decline.
- The processing for these transactions should follow the respective (i.e., EMV or VCPS) transaction flow.

6.9 Configurable/Selectable Kernels

Devices can be configured to support different functionality depending on the environment they operate in or to support a function or process under certain circumstances. There are two ways to support configurable functions:

- Configurable Kernels
- Selectable Kernels

6.9.1 Configurable Kernels

A configurable kernel is a kernel that has been tested for multiple configurations during EMV testing. Then, during deployment, the kernel can be set up to provide only the needed functionality:

- If an optional function is configurable (i.e., it can be turned on or off), it must be able to work properly as configured. Software for the function should be identified as configurable and should be tested and EMV type approved in both on and off modes.
- During vendor quality assurance testing, application kernels that are developed for multiple device types should be tested using all EMV scripts for those devices. Comprehensive quality assurance testing ensures proper support for mandatory and optional functions across device types.

6.9.2 Selectable Kernels

A selectable kernel is one where the kernel configuration used at a single device may vary based upon characteristics of the transaction rather than being set at the time of device installation:

- The logic in the device should be checked to ensure that it selects the correct configuration.
- All selectable configurations must be EMV type approved.
- The configuration should be selected prior to the issuance of the GET PROCESSING OPTIONS command so that the correct device information can be sent to the card, if requested in the PDOL.

Note: Terminal testing should be carried out for all possible kernel configurations.

For selectable kernel examples, see Section 2.14.2: Contact Transactions.

7. Security Characteristics

This section outlines security requirements and characteristics for devices and includes the following sections:

- Public Key Management
- Triple Data Encryption Standard (TDES) Key Management
- PIN Security and PIN Entry Device (PED) Security
- Data Security
- Unpredictable Number Generation
- Device Security and Risk Policy

For more information on device security, see the following resources:

- *EMV Acquirer and Terminal Security Guidelines* available from www.emvco.com
- PCI SSC documentation available from www.pcisecuritystandards.org

7.1 Public Key Management

Devices that support one or both of the following must be loaded with the VSDC CA Public Keys:

- Offline Data Authentication (e.g., DDA, fDDA)
- Offline Enciphered PIN

Important Information:

- **ATMs** – Since ATMs do not support Offline Data Authentication or Offline Enciphered PIN, the VSDC CA Public Keys are not applicable to these devices. ATM acquirers and vendors can skip this section.
- **Online-Only POS** – These devices do not need to support Offline Data Authentication so they only need to be loaded with the VSDC CA Public Keys if they support Offline Enciphered PIN.
- **Transit** – Transit devices generally support Offline Data Authentication; therefore, they must contain the relevant public keys (including the transit-specific key). See the Transit resources in Section 10.3: Visa Documents for more information.

7.1.1 VSDC CA Public Keys – General Requirements

General requirements for VSDC CA Public Keys:

Table 7–1: VSDC CA Public Keys – General Requirements

Topic	Description
Acquirer Responsibility	Acquirers are responsible for ensuring that the VSDC CA Public Keys are loaded/removed from their devices according to annually published Visa schedules; they are also responsible for removing keys if an accelerated key revocation is required.
Device Requirements	Devices must enable the secure loading, updating, and maintenance of the VSDC CA Public Keys.
Protection from Unauthorized Changes	Unauthorized changes to the keys or algorithms, or insertion of an unauthorized key should not be possible.
EMV/VIS Compliance	Devices must comply with the Visa and EMV chip requirements for withdrawal and introduction of the VSDC CA Public Keys.
Six Key Slots	To ensure sufficient levels of support for public key backup, key recovery, and key migration, the device must be capable of securely storing at least six VSDC CA Public Keys and their associated data elements.
1984 Key Length	Devices must be able to support key lengths up to 1984 bits. The current implemented lengths can be found on www.emvco.com and at the Visa Technology Partner website at www.technologypartner.visa.com.
Key Selection via RID and Public Key Index (PKI)	A device must be able to select the corresponding key and algorithm in conjunction with the RID and PKI of the selected application.
Test Keys	Acquirers and device vendors must ensure that any test keys that may have been loaded into the device to support testing are removed from production devices.

7.1.2 VSDC CA Public Keys – Downloading

Device deployers can obtain the VSDC CA Public Keys from the *Visa Smart Debit/Credit Certificate Authority Public Keys* which is available for public download on www.visa.com/pubkeys.

7.1.3 VSDC CA Public Keys – Validation

Before acquirers load the keys into their devices, they should check the information with a secondary source. For a secondary source, they can obtain the *Visa Smart Debit/Credit Certificate Authority Technical Requirements* from Visa Access. This document contains the current VSDC CA Public Keys, including a SHA-1 hash digest of each key, and explains how to validate the VSDC CA Public Keys against a secondary source.

Validating the VSDC CA Public Keys against a secondary source is essential to counter the risk of the Visa website (or the particular page on the website with the VSDC CA Public Keys) being compromised (hacked) while an acquirer is downloading the keys.

Acquirers can also use the key validation checks to verify the continued integrity of the VSDC CA Public Keys while they are stored with the acquirer.

7.1.4 VSDC CA Public Keys – Loading

While Visa does not mandate specific loading processes for the VSDC CA Public Keys and their associated data, EMVCo provides guidelines on this process (see *EMV Chip Specifications,* Book 2*).* Acquirers and device vendors should follow these guidelines. Acquirers should also periodically ensure the integrity of each key component (e.g., the Public Key Exponent, the CA Public Key Index, etc.).

Once loaded, EMVCo suggests that devices include a mechanism to allow acquirers to determine which keys are present at any given time to assist in the ongoing management, including removal, of keys through the lifetime of the device. Visa suggests that this functionality is built into a Terminal Management System. See Section 8.7: Terminal Management Systems for details.

7.1.5 VSDC CA Public Keys – Expiration

Based on EMVCo assessments, Visa periodically reviews and determines the expiration dates of the VSDC CA Public Keys. Visa publishes this information to acquirers in an annual *Visa Business News* article and the information is also reflected in the *Visa Smart Debit/Credit Certificate Authority Public Keys*. Acquirers must support removal of expired keys from their devices based on the expiration and removal dates. Generally, a 6-month grace period is provided to assist acquirers in these efforts.

For the EMVCo annual key length assessment report, see www.emvco.com.

7.1.6 VSDC CA Public Keys – Planned Revocation

Once a Certificate Authority Public Key pair has reached its planned expiration date, it must be removed from service. Visa has a planned revocation process to remove older keys. At an appropriate time prior to the planned revocation/expiration date, Visa will stop signing Issuer Public Keys with the corresponding Certificate Authority (CA) Private Key (i.e., VSDC CA Private Key).

Important: Planned and accelerated key revocations (see next section) require that keys be updated in all devices. Consequently, these data elements should be treated as variable parameters, not as components of the kernel. Post-deployment data integrity must also be verified. Failure to load the correct production VSDC CA Public Keys or a newly introduced key will result in Offline Data Authentication or Offline Enciphered PIN failures which may lead to declined transactions.

7.1.7 VSDC CA Public Keys – Accelerated Revocation

Visa analyzes and determines if an accelerated or emergency key revocation is required due to public key attacks. Should this occur, clients will be advised of Visa's findings and associated procedures.

7.1.8 VSDC CA Public Keys – Distribution and Management

This section provides a summary of the Visa principles to support the distribution and management of the VSDC CA Public Keys:

Table 7–2: VSDC CA Public Keys – Distribution and Management

Topic	Description
Authentication	Prior to loading a key into the device, the device should authenticate the entity sending the key.
Secondary Source	Recipients should always double check the key against a secondary source. See Section 7.1.3: VSDC CA Public Keys – Validation for details.
Integrity	The secure distribution of keys to devices is critical to ensure that the keys are not corrupted or modified during delivery. Valid keys should be delivered to the device in a manner that protects their integrity.
New Keys	Acquirers need to have a manual or automated procedure to ensure that new keys are loaded into their devices prior to the keys' effective dates.
Key Expiration/ Revocation	Expired or revoked keys must be removed from devices or disabled. As with new keys, a manual or automated procedure should be in place to ensure this.
Key Download Notification	Managing keys manually across a large device base can pose significant difficulties. The Terminal Management System should automatically notify all affected devices when a key is to be downloaded or removed. Notification may be done during an authorization response, a batch upload acknowledgement, an end-of-day response, or an explicit call by the Terminal Management System. Alternatively, devices may regularly contact the Terminal Management System for outstanding updates. Once notification is received, the device should automatically implement a scheduled process that results in a timely update of the keys.
Tracking	Within a reasonable timeframe, acquirers should be able to determine which VSDC CA Public Keys are active in each of their devices.

Topic	Description
Reporting	Acquirers should be able to report on the status of their installed device base to assure issuers that cards with new keys can be accepted and to protect against attacks based on devices whose expired or revoked keys have not been removed. Visa strongly recommends that the process be automated.

7.1.9 Issuer and ICC Public Keys

Issuer and ICC public keys, extracted during Offline Data Authentication and Offline Enciphered PIN processing, may have lengths up to 1976 bits. Devices must be able to support issuer and ICC keys that are not based on 8-byte boundaries (e.g., a key may be 127-bytes long).

7.2 TDES Key Management

Triple Data Encryption Standard (TDES)[51] key management is required for:

- Any device supporting Online PIN.
- A device that needs to securely transport the Offline PIN (whether plaintext or enciphered) from the PIN pad to the card reader.

Note: PIN confidentiality depends on the implementation of adequate PIN security standards. To this end, ANSI, ISO, and Visa require migration from the DES algorithm using single-length keys to the TDES algorithm using at least double-length keys.

7.3 PIN and PIN Entry Device (PED) Security

This section outlines requirements for Online PIN and Offline PIN.

The *Visa Rules* and the *Payment Technology Standards Manual* contain Visa's requirements for PIN entry. For additional information on security requirements associated with PIN entry and PIN processing, see the following resources:

- Visa PIN Security website at www.visa.com/pinsecurity
- PCI PIN Security Requirements and Testing Procedures at www.pcisecuritystandards.org

[51] Advanced Encryption Standard (AES) may also apply.

7.3.1 PIN Length and Character Set

This section outlines PIN length and character set requirements:

- **Minimum PIN Length** – The minimum PIN length is 4 digits.
- **Online PIN Length** – Per Visa Rules, ATMs and POS PEDs must be able to accept Online PINs of 4, 5, and 6 digits (and can accept up to 12 digits). U.S. ATM acquirers must be able to accept and transmit Online PINs that are 4 to 12 digits long.
- **Offline PIN Length** – Per EMV, chip devices must be able to handle Offline PINs between 4 and 12 digits.
- **PIN Character Set** – The PIN character set is 0 to 9.

7.3.2 PIN Storage

Any device with a PIN Pad, including a POS device or an ATM system, must not retain any PIN-related data after an authorization response. Retention of an Online PIN block is allowed for Deferred Authorizations but only for the minimum time necessary to complete the transaction.

7.3.3 Online PIN Requirements

For Online PIN, the PIN is entered, encrypted, transmitted, translated, and verified against the reference PIN data available in the issuer's processing center or, for instance, by using the PIN Verification Value (PVV) method (where the cardholder-entered PIN is compared to a cryptographic transformation of the PIN). If the PINs match, the cardholder's identity is deemed to have been correctly verified. Requirements are outlined in the following table:

Table 7–3: Online PIN Requirements

Topic	Description
Online PIN Encryption	For ATMs and POS devices that support Online PIN, the PIN must be protected: • Immediately upon entry by encryption in accordance to ISO 9564. • As specified in the *PCI PIN Security Requirements.* • As specified in the *PCI Transaction Security POI Modular Security Requirements*.
Online PIN Processing	The process of entering an Online PIN for chip-initiated transactions is outside the scope of EMV chip processing. Online PIN processing should take place on chip transactions as it takes place on magnetic-stripe transactions and may occur at any point in the user interface flow prior to online processing. **Note:** The encrypted PIN may remain in the Encrypting PIN Pad (EPP) until needed for online processing.

Topic	Description
Online PIN Retries	Certain transactions, such as ATM Cash Disbursements or Balance Inquiries, may include the cardholder re-entering their PIN after an incorrect PIN entry. Acquirers may use the same chip data with the PIN retry or they may start a new chip transaction for each PIN retry using the AID selected in the initial Application Selection process.
PIN Entry Capability Field	An acquirer must only use PIN Entry Capability (Field 22, Position 3) to identify support for Online PIN. If a device only supports Offline PIN and/or only supports Online PIN associated with a domestic payment scheme, this field must be set to indicate that the device cannot accept and forward a PIN.
Service Code	For transactions initiated via the magnetic stripe, the PIN settings in the Service Code only refer to Online PIN capability. For more information on Service Codes, see Section 3.3: Service Codes. **Note:** The Service Code value is not used during a chip transaction except to identify the card as a chip card via 2xx/6xx.
PIN Block Construction	During a chip transaction, devices must use the PAN received from the chip application and not the one encoded on the magnetic stripe when building PIN blocks.

7.3.4 Offline PIN Requirements

For Offline PIN, the device compares a cardholder-entered PIN to a reference PIN stored in a secure location on the card's chip, which then returns a pass or fail indicator to the device. This indicator is one of many used to determine whether the transaction is sent online or declined offline.

There are two types of Offline PIN verification:

- **Offline Plaintext PIN** – The chip reader sends the PIN to the chip as plaintext.
- **Offline Enciphered PIN** – Either the secure component in the device (e.g., the chip reader) or the PIN pad itself enciphers the PIN, using an authenticated public key from the chip. The enciphered PIN is sent to the chip where the chip uses its private key to decipher and validate the PIN.

Requirements for Offline PIN:

- **Optional** – Offline PIN is optional and only applicable to contact-chip devices.
- **Not Applicable to Contactless or ATMs** – Offline PIN is not applicable to ATMS (which must support Online PIN only) or contactless transactions.
- **Offline Plaintext and Offline Enciphered PIN** – It is strongly recommended that devices supporting Offline PIN support both plaintext and enciphered. If a contact-chip device supports Offline Enciphered PIN, it must also support Offline Plaintext PIN.

Offline PIN must be processed as specified in the following documents:

- EMV Chip Specifications
- PCI PIN Security Requirements
- PCI PTS POI Modular Security Requirements

7.3.5 EMV Terminal Capabilities

When a device has a PIN pad that is not used for chip transactions (e.g., if it processes only magnetic-stripe-based domestic debit transactions), the EMV Terminal Capabilities data element should indicate that the device does not support Offline PIN or Online PIN.

7.3.6 EMV PIN Entry Bypass

EMV PIN Entry Bypass is a mechanism that is available to environments that are transitioning from signature to PIN at the POS:

- During the transition period, if cardholders forget their PIN, they can cancel out of PIN entry.
- The device will set the "PIN entry required, PIN pad working, but PIN not entered" bit in the TVR and this bit setting will be provided in the online authorization message to the issuer.

For more information, see the *EMV Chip Specifications*, Version 4.3, Book 4, Section 6.3.4.3.

Note: The card needs to be personalized correctly to allow PIN Entry Bypass. Acquirers should check with their Visa representative to determine if this mechanism applies to their market.

Note: Some countries do not allow PIN Entry Bypass.

7.3.7 PIN Exceptions

Support for PIN may not be required in situations where interaction between a device and cardholder is inherently impractical (e.g., road tolls and transit applications). Some countries may have other specific exceptions. For information on the exceptions in your market, contact your Visa representative.

7.3.8 PIN Entry Device (PED) General Security

A PIN Entry Device (PED) is any device used by a cardholder to enter a PIN. It may have other functions (e.g., to enter a loyalty program number). For a contact-chip device, it may contain an EMV kernel. This section provides an overview of PED security requirements. See *PCI PIN Security Requirements and Testing Procedures* for details:

- **PED Connectivity** – If a device is configured with an external PED, the application needs to ensure that the PED is always connected to the device and is functional.

- **PED Security** – The PED must be protected against unauthorized removal.
- **PED Tampering Prevention** – Devices that support Online PIN entry should be constructed so that any tampering with the device stops it from working.
- **PIN Entry Indication** – PEDs may visually indicate that a digit has been entered, such as with an asterisk (*). This visual indication should occur for each digit entered by the cardholder. For example, a PED should not display only four asterisks when six digits have been entered. Similarly, if audible tones are used, the same tone should be generated each time that a digit is entered.
- **Encrypting PIN PAD (EPP)** – A PED that supports Online PIN, Offline Plaintext PIN, or both, where the PED and chip reader are not integrated, must contain an EPP for cardholder PIN entry. The EPP may be integrated, as in some standalone POS devices, or the EPP may be one component of a PED, as in an ATM.
- **PED Security** – If the design of the device requires that parts of the device be physically separated (e.g., the PED is not integrated into the device) and any cardholder instructions or processing data pass between the separate parts, there must be equal levels of protection between the different parts that make up the device.

7.3.9 PED Testing Requirements

PEDs used in the acceptance of Visa card products must be evaluated against the PCI PIN PTS Requirements and listed as approved on the PCI PTS Approved Device List.

For more information, see the following website:

- www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

7.4 Data Security

This section describes the industry security standards for cardholder and payment application data.

7.4.1 Cardholder Data Security

When customers use their cards at the point of sale, they want assurance that their account information is safe. Cardholder data must be protected in accordance to the PCI DSS standard.

Acquirers must ensure their merchants and service providers comply with the PCI DSS standard where they may store, process, or transmit Visa account numbers.

For more information, see the following websites:

- www.visa.com/cisp
- www.visa.co.uk/pay-with-visa/security/risk (Europe region)
- www.pcisecuritystandards.org/document_library (filter by “PCI DSS”)

7.4.2 Payment Application Data Security

Requirements for payment application data security:

- **Data Storage Requirements** – Subsequent to an authorization, storage of sensitive authentication data (e.g., Track 2 Equivalent Data from the chip, Card Verification Value (CVV), PIN data) is prohibited.
- **PA-DSS Requirements** – Per Visa mandates, all agents and merchants that use payment applications must comply with Payment Application Data Security Standard (PA-DSS).
- **PA-DSS Eligibility** – Payment applications are eligible for review and listing as part of the PA-DSS program if the application stores, processes, or transmits cardholder data as part of authorization or settlement, and is sold, distributed, or licensed to third parties; however, all payment applications and devices remain subject to the requirements of PCI DSS.

For more information, see the following PCI SSC documents:

- www.pcisecuritystandards.org/document_library (filter by "PA DSS")

7.4.3 Data Processing and Transmission Security and Integrity

Any data that passes through the acquirer to VisaNet or the issuer must not be altered, especially chip data related to the cryptogram and its generation. This applies to online authorization requests and responses which may include additional data such as Issuer Scripts. If present, devices must forward Issuer Scripts to the card.

Similarly, acquirers will collate transaction data for clearing and settlement purposes. Typically, the data is collated and then batched for processing on a regular basis (generally daily). All data should be protected against unauthorized alteration and deletion.

Any processing and storage of data must comply with PCI SSC requirements as outlined in previous sections.

7.4.4 Wireless Security

The PCI SSC has developed guidance and recommendations for the deployment of wireless networks, including 802.11 Wi-Fi and 802.15 Bluetooth technologies to ensure protection of cardholder data. The *PCI DSS Wireless Guidelines* are designed to help organizations understand and interpret how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless, and to provide practical methods and concepts for deployment of secure wireless in payment card transaction environments.

Merchants and device vendors that use or develop devices that transmit payment card information over wireless technology should have these controls in place to protect those systems and reduce the risk of data compromises.

The PCI SSC guidelines recommend the use of technologies such WPA2 or secure pairing for Bluetooth devices for encrypting and authenticating wireless LANs. Wireless networks are also considered to be public networks meaning all cardholder data must be encrypted as required in PCI DSS if it is to be transmitted over a wireless network.

For more information, see the *PCI DSS Wireless Guidelines* supplement.

7.5 Unpredictable Number Generation

EMV devices are required to provide unpredictable values as part of several steps in the EMV process, such as the generation of the cryptogram. EMVCo has specific recommendations on the effective generation of unpredictable numbers.

For more information, device vendors and acquirers should review the *EMV Acquirer and Terminal Security Guidelines* available from www.emvco.com.

7.6 Device Security and Risk Policy

Acquirers should develop a device security and risk policy that considers the various issues associated with the deployment of devices, threats to their operation, and the policies required for their secure operation. This policy should then be socialized with the acquirer’s device vendors and payment system providers as well as internal risk and operations teams.

Parts of the policy may then also be included as part of the commercial agreement between acquirers and merchants to ensure merchants comply with any requirements that are their responsibility.

The policy should, wherever possible, reference Visa and industry guidelines and recommendations such as those from the PCI SSC.

8. Device Design, Deployment, and Management

This section outlines recommendations for contact and contactless device design, deployment, and management. It includes the following sections:

- Device Design
- Device Deployment
- Device Management
- Device Performance Considerations
- Device Clock
- Device Maintenance
- Terminal Management Systems

8.1 Device Design

Device vendors should adopt a modular approach to design so that minor changes can be made without the need for major modifications. It is recommended that non-EMV functionality reside outside the kernel so that these functions may be updated without requiring a kernel update and subsequent re-approval.

Recommended modules include:

- Table-driven currency codes
- Drivers for peripherals, such as printers
- Communications and message drivers
- Cardholder and merchant interface, including table-driven prompts and responses
- Functions that are outside the scope of the EMV Chip Specifications, such as the device display (e.g., the EMV module looks up display messages without impacting the kernel)

8.2 Device Deployment

To reduce acceptance problems, device deployers should follow some basic practices:

Table 8–1: Device Deployment Activities

Topic	Description
Latest Specifications for Kernels/Software	When selecting software for devices, determine the EMV kernel identifier and review the listing of approved kernels at www.emvco.com. The later the version of specifications and test plan, the less likely that any in-the-field interoperability problems will arise.
	Because software associated with earlier specification versions is more likely to have problems in the field, only implement software that incorporates kernels based on: • Contact: – *EMV Chip Specifications*, Version 4.3 or later • Contactless: – *VCPS,* Version 2.1.3 or later – *EMV Contactless Specifications*, Book C-3, Version 2.5 or later
Software Updates	As interoperability problems are uncovered globally, new testing is put in place at EMVCo-accredited laboratories. Deployers should plan to refresh the software in their devices every few years to ensure that they have the latest fixes and functionality.
Updated Kernel as Part of Device/ Software Contract	Deployers should consider including language in purchase or lease contracts so that the device or software vendor will supply updated kernels at no charge, as they become available, for at least 3 to 5 years.
Only Use EMV Approved Features	Acquirers and merchants should ensure that their devices use the features which EMVCo approved for their kernel. Devices should not use features that were not tested during EMV Level 1 and Level 2 testing. Features that were included in EMV testing should not be turned off. If acquirers prefer to use multiple configurations in their devices, the correct solution is to use a configurable kernel. Each configuration must be EMV approved before it is deployed. Terminal Management Systems should only load devices with approved configurations. Kernels must be deployed only as a tested configuration.
Device Changes	Changes that may affect a device's operation should not be made without the express knowledge of the acquirer.
Language Display	Devices should support and correctly display the character set of the language of the installed location and any other supported languages that are commonly used in the geographic area.
Public Key	Deployers will need to have a means of updating public keys in their devices. See Section 7.1: Public Key Management for details.

Topic	Description
Device-to-Acquirer Message Format	With the emergence of new functionality such as authentication methods, deployers who do not use a flexible format for their device-to-acquirer messaging should plan to migrate to a format based on XML, TLV, or a similar flexible system. The length of variable length data elements may change over time (as new requirements are introduced), and so the flexible format should allow for the length of data elements sent in device-to-acquirer messages to change/grow over time.

8.3 Device Management

Acquirers should develop a device management process to protect devices and minimize any potential misuse which may lead to interoperability problems or possible fraud. This will ensure that any potential problems can be pinpointed and resolved in an expedited manner. This will also aid in replacing or upgrading devices once their EMV kernels expire or require renewal.

EMVCo has outlined a set of guidelines for the deployment and management of devices which includes the following:

- **Device Inventory** – Acquirers should maintain an inventory of all deployed devices and should be able to identify each device uniquely, know where it is located, and which software versions it is running.
- **Device Management Policy** – Acquirers should establish a device management policy with merchants, such that device replacement and maintenance procedures are clearly defined.
- **Physical Security** – For devices in exposed environments or environments with a high level of staff turnover (e.g., garages and fast food outlets), acquirers should recommend merchants to physically secure the devices, using a lock under control of site management. For more information, see the PCI SCC document *Skimming Prevention Best Practices for Merchants* available from the PCI SCC website at www.pcisecuritystandards.org/security_standards.

For more information, acquirers should review the *EMV Acquirer and Terminal Security Guidelines* document which is available from www.emvco.com.

8.4 Device Performance Considerations

A contact-chip device must provide fast, efficient processing of chip-card transactions. Device processing should be optimized to help ensure the fastest transaction possible. Much of the communication between the device and chip card can take place while waiting for a manual action from either the cardholder or the merchant. Examples include:

- Initiating a transaction immediately after the card is inserted in the device.
- De-energizing the chip after completion of the transaction, instead of waiting for the receipt to be printed (if applicable), so that the cardholder can remove the card while the receipt is being printed.
- Processing some or all of the steps concurrently instead of sequentially (e.g., Offline Data Authentication, Processing Restrictions, Cardholder Verification, and Terminal Risk Management).

To further streamline transactions and provide cardholders with payment options, devices should support contactless transactions. See Section 2.11: Transaction Speed for information on the speed requirements for these transactions.

8.5 Device Clock

EMVCo requires that devices have a clock with date and time which is either autonomous or updated based on online messages:

- **Clock Synchronization** – The clock should be synchronized regularly to ensure it is accurate and any seasonal time shifts have been taken into account.
- **Clock Resetting** – The clock should be reset with each host response or when polled for the collection of transactions for clearing and settlement. (Integrated systems may have a central date and time that is distributed to a network of devices.)
- **Clock Adjustment** – Any manual adjustment of the clock by a merchant should only be possible with authorization via methods such as key switch or a password.
- **Battery Backup** – In the case where the device may lose power without resynchronization of the clock when the power is restored, the device clock should have a battery backup.

8.6 Device Maintenance

Device maintenance:

- **Regular Maintenance** – As a best practice, acquirers should ensure that POS devices receive regular maintenance including battery replacement.
- **Power Failures** – If a power failure occurs and the battery in the device is dead, the merchant may need to manually re-enter information from the receipts of captured transactions. The merchant is at risk of losing payment for those transactions because the full magnetic stripe or chip information is not included on the merchant's copy of the receipt.
- **Transactions Cleared Daily** – To reduce the impact of losing captured transactions, acquirers should ensure their devices are cleared every day and merchants are educated accordingly. Use of nonvolatile journaling (in accordance with PCI DSS requirements) is also recommended.

8.7 Terminal Management Systems

Terminal Management System architecture should be sophisticated and flexible enough so that modifications can be made without requiring large device infrastructure changes. The more supportive and robust a Terminal Management System is, the easier it is to respond to future market needs, new requirements, and change requests.

8.7.1 EMV Functionality

Terminal Management System functionality for EMV:

- **EMV Mandatory Functionality** – Devices must support all mandatory requirements for their device type as outlined in the *EMV Chip Specifications*. To ensure EMV compliance, the Terminal Management System should include profiles or logic validating that all mandatory functions for a device type are active.
- **No Deletion of Mandatory EMV Functionality** – The Terminal Management System should ensure the mandatory functions cannot be deleted. The system may add or delete optional functions provided that the final configuration loaded into the device has been EMV-approved.
- **No Manipulation of EMV Functionality by Non-EMV Applications** – Once a device is deployed, the Terminal Management System should not be able to change EMV functionality by setting or resetting parameters in non-EMV applications. Most EMV functions are mandatory and any post-deployment change could affect a device's interoperability.

8.7.2 Data Element Tracking

The Terminal Management System should track certain data elements in their devices along with their specific values. Where applicable and if necessary, the Terminal Management System should be able to update these data elements post-device deployment.

Table 8–2: Terminal Management System (TMS) Data Element Tracking

Data Element	Reference
Application Identifiers (AIDs)	Section 4.3.1: Application Identifiers (AIDs)
Application Version Number	Section 4.6: Processing Restrictions
Contactless Limits (If device supports contactless transactions) • Reader CVM Required Limit • Reader Contactless Floor Limit	Section 5.2.1: Preliminary Processing
Floor Limits	Section 4.9.1: Terminal Floor Limits
Random Transaction Selection Parameters (If device supports offline transactions)	Section 4.9.2: Random Transaction Selection
Terminal Action Codes (TACs)	Section 4.10.1: Terminal Action Codes (TACs)
Terminal Capabilities	See *EMV Chip Specifications* for details
Terminal Transaction Qualifiers (TTQs) (If device supports contactless transactions)	Section 5.2.4: Card Requests Terminal and Transaction Data Section 5.5: Other Contactless Processing Considerations
Terminal Type	See *EMV Chip Specifications* for details
VSDC CA Public Keys (If device supports Offline Data Authentication or Offline Enciphered PIN)	Section 7.1: Public Key Management

9. Device Testing

This section provides information on the device testing activities required prior to device deployment:

- **Contact-Chip Transactions** – Devices must comply with the current version of the *EMV Chip Specifications* and complete Level 1, Level 2, and Level 3 testing.
- **Contactless-Chip Transactions** – Devices must comply with the current version of *VCPS* or the *EMV Contactless Chip Specifications,* Book C-3 and complete Level 1, Level 2, and Level 3 testing.

9.1 Device Testing Overview

Contact and contactless devices each have the following testing requirements:

- Level 1 (L1)
  - Contact (Interface Module): Testing managed by EMVCo
  - Contactless (Proximity Coupling Device): Testing managed by EMVCo
- Level 2 (L2)
  - Contact (Kernel): Testing managed by EMVCo
  - Contactless (Kernel):
    - Devices developed to *VCPS*: Testing managed by Visa
    - Device developed to *EMV Contactless Specifications*, Book C-3: Testing managed by EMVCo
- Level 3 (L3) (Terminal Integration Testing)
  - Contact: Self testing with Acquirer Device Validation Toolkit (ADVT)
  - Contactless: Self testing with Contactless Device Evaluation Toolkit (CDET) or Visa payWave Test Tool (VpTT) (Europe only)

9.2 Contact Devices

Device testing for contact devices is outlined in this section.

9.2.1 Level 1 (Interface Module)

Level 1 addresses conformance of interface modules (IFM) to the EMV defined set of electrical, mechanical, and communication protocol characteristics. This testing is managed by EMVCo:

- The approval is given to the interface module (IFM) (i.e., the chip-card reader) rather than for the device on which it is tested. An IFM consists of the hardware and software that powers the chip card and supports communication between the device and the card up to the transport layer.
- An approved IFM can be used (as long as the IFM is not modified) with any approved application kernel provided criteria defined in the EMV administrative process document is met.
- It is important to identify the IFM component separately from the device, using a unique identifier.

For more information on the EMV Level 1 contact device approval process, see www.emvco.com.

9.2.2 Level 2 (Kernel)

Level 2 addresses conformance of the application software to the required and optional *EMV Chip Specifications* functionality. This testing is managed by EMVCo:

- The approval is given to the portion of the application that performs EMV functions (which is referred to as the “application kernel” or “kernel”).
- The approval is not tied to a particular model or a particular type of hardware platform; however, the approval letter notes the hardware configuration that was used for testing.
- The kernel can be ported into a device as long as conditions stated in the EMV administrative process document are met.
- Approved, unmodified kernels may be used across a family of devices.

Note: Although the term “EMV-approved device” is commonly used, an approved device is one that contains both an approved interface module (Level 1) and an approved software kernel (Level 2).

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

For more information on the EMV Level 2 contact device approval process, see www.emvco.com.

9.2.3 Level 3 (Terminal Integration Testing for Contact)

Acquirers (or their agents) must perform Level 3 (L3) testing using the ADVT prior to device deployment. The ADVT is a self-administered set of test cards (possibly generated by a card simulator) and test scripts that acquirers or vendors can use on devices that have already received Level 1 and Level 2 approval and are configured for deployment (i.e., after the country code, floor limits, and other processing parameters are set up in the device).

Acquirers outside of the U.S. must submit ADVT results to Visa using the Chip Compliance Reporting Tool (CCRT) available on Visa Access.

There are two options for obtaining the ADVT:

1. Contact a third-party L3 test tool supplier from Visa’s list of “Confirmed” L3 test tool suppliers (www.technologypartner.visa.com/Toolkits/#publiclist).

2. Download the Visa Mobile Card Personalization (VMCP) App from the Google Play Store, then order the VMCP Utility Card packet from XpressDocs (Visa’s Fulfillment Service). The VMCP App includes all the current ADVT card profiles. For more information on the app and utility card, see the *Visa Mobile Card Personalization App Usage* Instructions.

For more information on the ADVT, see the *ADVT User Guide*.

In the U.S. region, see *Visa U.S. Quick Chip and Minimum Terminal Configuration ADVT/CDET Use Cases* for testing requirements.

9.3 Contactless Devices

Device testing for contactless devices is outlined in this section.

Important: In addition to the information in this section, acquirers should also ensure compliance with any additional regional requirements for contactless testing.

9.3.1 Level 1 (Proximity Coupling Device)

Similar to contact devices, contactless devices must be tested to support Level 1 at an EMVCo-accredited laboratory.

For more information on the EMV Level 1 contactless device approval process, see www.emvco.com.

9.3.2 Level 2 (Kernel)

For Level 2 testing, the device can either be tested at an EMVCo-accredited laboratory or by Visa (depending on whether it was developed to the *EMV Contactless Specifications* or *VCPS*). The device must be tested for Level 1 before it is submitted for Level 2 testing.

This testing may include cross testing/interoperability testing based on the scope of testing required for the specific device.

For more information on the EMV Level 2 contactless device approval process, see www.emvco.com.

For more information on the Visa approval process for contactless devices, see the *Chip Card Acceptance Device Testing and Approval Requirements*.

9.3.3 Level 3 (Terminal Integration Testing for Contactless)

Acquirers outside of Europe must perform L3 testing using CDET prior to device deployment. CDET is a self-administered set of test cases delivered via a mobile app called the Visa Mobile Card Personalization app. Acquirers or vendors can use the app (loaded on a consumer device such as a mobile phone) to perform testing on devices that have already received Level 1 and Level 2 approval and are configured for deployment (i.e., after the country code, floor limits, and other processing parameters are set up in the device).

The VMCP app is available from the Google Play Store. For more information on the app, see the *Visa Mobile Card Personalization App Usage Instructions*.

Europe Only: Instead of using CDET, acquirers/vendors in Europe must use the Visa payWave Test Tool (VpTT). For more information, contact your Visa representative in the Europe region.

Acquirers outside of the U.S. must submit CDET or VpTT results to Visa using the Chip Compliance Reporting Tool (CCRT) available on Visa Access.

For more information on CDET, see the *CDET User Guide*.

For the U.S., see the *U.S. EMV Chip Terminal Testing Requirements*.

9.4 Level 1 and 2 Approvals, Renewals, and Revocations

Once the device has been successfully tested, Visa/EMVCo issues a letter of approval[52] to the device vendor. The approval applies internationally, unless restrictions are specified in the letter of approval. Approval is not transferable from one vendor's product to another:

- **EMV** – For products completed through the EMV testing process:
  - The device will appear on one of the Approved Products Lists located on www.emvco.com.
  - The device is assigned an expiration date. At expiration of the approval, EMVCo evaluates whether the IFM/Proximity Coupling Device or kernel demonstrates sufficient conformance to the current *EMV Chip Specifications/EMV Contactless Specifications* and may grant an extension. IFMs or kernels that do not pass the evaluation will not be granted an extension and their approval will be considered expired.
  - EMVCo may revoke an approval of an IFM/Proximity Coupling Device or kernel if a significant interoperability problem arises in the field.
  - For more information on the EMVCo approval and renewal policy, see www.emvco.com.
- **Visa** – For products completed through the Visa testing process:
  - The device will appear on the Approved Acceptance Device Products Lists located at the Visa Technology Partner website at www.technologypartner.visa.com.
  - The device is assigned a renewal date which is communicated to the device vendor in the letter of approval and also appears on the Visa Approved Products List. The renewal date is typically four years after the date of approval, unless otherwise noted.
  - As a device approaches its renewal date, Visa reviews the product details to ensure that it complies with all current Visa policies and includes a payment application(s) that Visa continues to support.
  - For more information on the Visa approval and renewal policies, see the Visa Technology Partner website at www.technologypartner.visa.com.

[52] The interface module (Level 1) and application kernel (Level 2) receive separate letters of approval. As discussed above, the reader and application kernel may be used unmodified in other terminal models, generally in the same family.

9.5 Post-Deployment Testing

Acquirers should have production support procedures in place to address and resolve issues that may arise with devices already deployed in the field. If a problem is detected and diagnosed, any associated action plan should be enacted in a timely manner. Visa will support acquirers with these activities. Acquirers should be aware that Visa has a Chip Interoperability Program in place in the event that problems are not being resolved in a timely manner. See the *Visa Rules* for details.

In addition, acquirers should be aware that device testing according to Visa’s Level 3 terminal integration testing process may be required if the device undergoes a significant upgrade.

10. 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.

10.1 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

10.2 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
- PCI PIN Security Requirements
- PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements
- Skimming Prevention: Best Practices for Merchants

10.3 Visa Documents

The TADG is available at www.visa.com/tadg.

While the TADG and the Visa Rules are public documents:

- Acquirers can obtain other documents from Visa Access at www.VisaAccess.com.
- Vendors can obtain other documents from the Visa Technology Partner (VTP) website at www.technologypartner.visa.com after they register and obtain a license (vendors can use the VTP website to initiate the license registration process).

For a list of U.S. specific documents, see Section B.4: Visa U.S. Specific References.

Table 10–1: Visa Reference Materials

Title and Description	Audience	User
Visa Specifications		
Visa Contactless Payment Specification (VCPS) Provides the Visa specification for contactless payment 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) (this guide) 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

Title and Description	Audience	User
Transaction Acceptance Device Requirements (TADR) Outlines chip-device requirements that are not covered in the *Visa Rules*.	Acquirers, Vendors	Policy, Operations, Technical
Visa Easy Payment Service (VEPS) Acquirer Program Guide Provides a program guide for the Visa Easy Payment Service.	Issuers and Acquirers	Operations, Technical
Visa Europe Contactless Terminal Requirements and Implementation Guide (Europe Region Only) Outlines Europe region requirements for contactless devices. This document is available from the Europe region.	Vendors	Technical
V PAY Card and Acceptance Device Technical Specifications Provides card and device technical specifications for V PAY.	Issuers, Acquirers, and Vendors	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
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

Title and Description	Audience	User
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 Europe - payWave Terminal Test Procedures **Visa Europe – payWave ATM Test Procedures** **Visa Europe - payWave Transit Gate Test Procedures** Provide a description of the VpTT test cases for different terminal types.	Acquirers, Vendors	Operations
Visa Mobile Card Personalization (VMCP) App Usage Instructions Provides instructions for using VMCP for ADVT and CDET testing.	Acquirers, Vendors	Operations
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”) (Public Document) Provides regulations for issuers and acquirers, including rules governing contact and contactless transactions, dispute processing, and interchange rates.	Issuers, Acquirers	Policy, Operations
V PAY Operating Regulations (Europe Region Only) Outlines the operating regulations for V PAY.	Issuers, Acquirers	Policy, Operations

Title and Description	Audience	User
Visa 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

Appendix A. Contactless Reader Placement

This appendix outlines recommendations for the placement of contactless readers in a merchant retail environment where the contactless reader is a separate unit (i.e., not an integrated reader that supports contact, contactless, and magnetic stripe).

These recommendations are based on laboratory tests conducted on behalf of Visa and industry best practices. They are intended to provide guidance to expedite contactless-card reader integration into a merchant POS environment and ensure efficient operation.

Recommendations for contactless reader physical placement are also applicable to unattended devices such as ATMs and kiosks. Where available, Visa has provided specific guidelines and placement recommendations. Merchants should consult with their acquirers, Visa representatives, contactless-card reader manufacturers, and installation technicians to determine the optimal implementation in their retail environments. There may be additional specific domestic and regional placement recommendations and requirements. For more information, contact your Visa representative.

A.1 Local Regulatory Compliance

The contactless-card reader must comply with all local legal regulations ranging from electromagnetic emissions to consumer privacy.

A.2 Proximity to RFID and Antitheft Devices

The contactless-card reader should be placed so that it is not affected by Radio Frequency Identification (RFID) readers or antitheft devices. Many factors influence RF interference, so that testing under a variety of conditions during deployment is advised. If feasible, placing the reader at least 200 centimeters (80 inches) away from an antitheft RFID device is recommended.

A.3 Proximity to Transmitting Devices

Active transmitting devices (e.g., mobile phones) can disrupt a contactless transaction if it is very close to a contactless card while the card is attempting to communicate with a contactless-card reader.

If the cardholder presents the contactless card while holding an active transmitting device in the same hand, the transaction may be adversely impacted. The remediation is for the cardholder to move the active transmitting device away from the contactless card and reader and re-present the contactless card. A label or placard may be placed near a contactless-card reader to advise cardholders not to place an active transmitting device close to a contactless card while it is communicating with a contactless-card reader.

A.4 Susceptibility to Electromagnetic Interference

The contactless-card reader should not be placed in close proximity to electrically powered equipment that can generate electromagnetic interference or static electricity (e.g., personal computers, lighted displays, cooking appliances, or refrigeration equipment).

To protect contactless cards from problems at the POS, Visa recommends that:

- The POS device and contactless-card reader power supplies are fitted with transient arrestor devices for protection from power surges.
- As protection against interference, contactless-card readers should not be placed near equipment that switches inductive loads such as electrical distribution junctions.
- All electrically powered devices in use near a contactless-card reader (e.g., cash registers) should be regularly tested to ensure proper electrical grounding and that there are no loose electrical connections or unshielded cables.
- Equipment that is improperly grounded or has exposed wiring could generate electromagnetic interference, which could adversely impact the operation of a contactless payment transaction.

A.5 Contactless-Card Readers Mounted on Motor Vehicles

A contactless-card reader that is mounted on a motor vehicle should be positioned away from high voltage vehicle components such as ignition coils, ignition wires, and lamp relays. The card reader power supply should be from an auxiliary source with voltage filtering/smoothing. This protects the contactless-card reader from potential interference and ensures the efficient performance of the contactless payment transaction.

This recommendation applies to any deployment scenarios involving motor vehicles, including buses or trains. Close proximity to a vehicle's electrical systems or unshielded internal electrical wiring (e.g., direct placement over the electrical system), could have a negative impact on a contactless-card reader's operation. Merchants should consult with their acquirers, Visa representatives, contactless-card reader manufacturers, and installation technicians to determine possible sources of transaction interference.

A.6 Proximity to Metallic Material

Metallic material positioned between a contactless card and a contactless-card reader may prevent the card and reader from communicating. Visa recommends that the space in between the card and reader should be clear of metallic material.

A.7 Proximity of Multiple Readers

Merchants should place contactless-card readers at least 30 centimeters (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.

A.8 Proximity to EMV-Compliant Contact-Chip Devices

Merchants should place the contactless-card reader at least 15 centimeters (6 inches) away from the EMV-compliant contact-chip device (primarily for nonintegrated devices).

Note: Device and reader manufacturers should shield the part of the device that contains the contactless-card reader from the part of the device that reads the contact-chip card (for devices where the contactless reader is integrated in the EMV-compliant contact-chip device).

Appendix B. Visa U.S. Common Debit AID (U.S. Only)

This appendix is specific to the U.S. It outlines Visa's approach for supporting the Visa U.S. Common Debit AID at POS and ATMs. The Visa U.S. Common Debit AID is intended for U.S. domestic use only including all 50 states, the District of Columbia, and the territories that comprise the United States of America.

Note: The information in this appendix is based, in part, on the *U.S. Debit EMV Technical Proposal* white paper developed by the U.S. Payments Forum.

Note: While each payment scheme has its own U.S. Common Debit AID, all references to this term in this appendix refer to the Visa U.S. Common Debit AID ('A0 00 00 00 98 08 40').

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 4.3.1: Application Identifiers (AIDs).

U.S. Visa cards are typically personalized with the Application Label and not with the Application Preferred Name. The following discussion assumes that only the Application Label is available, but the Application Preferred Name may be used as an alternative to the Application Label as described in Section 4.3.7: Application Label and Application Preferred Name. Note also that merchants may choose to offer enhanced descriptors for debit applications as further described in the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide,* Chapter 2, section on "Cardholder Selection."

B.1 Background

To support debit routing, U.S. Covered Visa Debit Cards[53] 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 debit network. When the Visa AID is selected, the transaction must be routed to Visa.

[53] **U.S. Covered Visa Debit Card** – A Visa U.S. debit card as defined in the *Visa Rules* for debit and prepaid products covered by the unaffiliated network and routing requirements of the Dodd-Frank Act and Federal Reserve Board Regulation II.

B.2 Options for Application Selection, Funding Selection, and CVM Selection

Per Basic EMV Application Selection processing, terminals may provide cardholders with the ability to select which application they want to use on a given transaction by building a Candidate List of all mutually supported applications and then displaying them to the cardholder for selection. This terminal selection can be customized to meet merchant preferences in the U.S.

For U.S. Covered Visa Debit Cards, merchants have flexibility to use either the Visa U.S. Common Debit AID or the Visa AID. Application Selection (including the display of an Application Selection screen) is not required by Visa for debit functionality on U.S. Covered Visa Debit Cards. 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 by deploying specific logic in their readers/terminals to ensure the Visa U.S. Common Debit AID is used. See Section B.3.2: Special Application Selection Logic. If a customer presents a U.S. Covered Visa Debit Card with multiple funding sources (e.g., credit and debit applications), merchants may present screens to enable the cardholder to select a funding source. Any such screens should clearly identify the source of funds to avoid cardholder confusion, but merchants are not required to display debit AID selection screens or labels as part of that cardholder funding selection process.

In some implementations, unless modified by the merchant, the terminal will apply U.S.-specific Application Selection logic, which may result in auto-selection of the application.

Merchants can promote their preferred Cardholder Verification Method, including discouraging the use of signature. Where merchants automatically prompt for PIN on card present transactions, they must minimally ensure that a cardholder presenting a Visa Debit card for payment can originate a transaction using a signature (or “no CVM”), even if the cardholder is steered to enter a PIN.

Recommended PIN opt-out options include:

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

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

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

B.3 Other Approaches

This section outlines other possible approaches that are part of EMV processing.

Implementation of any of these alternative approaches is optional. Merchants may route all debit transactions from U.S. Covered Visa Debit Cards using the Visa U.S. Common Debit AID by applying special terminal logic, if they so desire. See Section B.3.2: Special Application Selection Logic.

B.3.1 Selecting Application with Highest Priority

Cardholder Selection may be inherently impractical in environments such as road tolls or transit. In these environments, the terminal can follow basic EMV processing to build the Candidate List and then automatically select the application with the highest priority (as defined by the issuer in the card's Application Priority Indicator). If the Visa AID is selected as the highest priority application, the transaction will be routed to Visa (transactions initiated with a Visa AID must be routed to a Visa network).

B.3.2 Special Application Selection Logic

Another approach is for the terminal to identify cards that contain both a Visa AID and the Visa U.S. Common Debit AID and eliminate one of the AIDs from the Candidate List (when these AIDs share the same funding source ["debit pairs"]). The remaining AID can then be used for routing purposes. This approach, and other options, are discussed in more detail in the following sections of the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide*:

- Chapter 2, section on "Special Application Selection Logic"
- Appendix on "Basic EMV Terminal Logic"
- Appendix on "Special Application Selection Logic"

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 Common AID exclusively if they so choose. If a customer presents a U.S. Covered Visa Debit Card with multiple funding sources (e.g., credit and debit applications), merchants may present screens to enable the cardholder to select a funding source. Any such screens should clearly identify the source of funds to avoid cardholder confusion, but merchants are not required to display debit AID selection screens or labels as part of that cardholder funding selection process.

B.3.3 Application Selection for Contactless Transactions and the Visa U.S. Common Debit AID

Contactless transactions do not support Cardholder Selection in the same way as contact-chip transactions due to the minimal interaction between the contactless reader and the consumer device. The default AID to be selected will normally be the highest priority AID (as identified by the issuer or consumer) on the consumer device. So, if merchants wish to preserve their routing choice for debit functionality or offer additional options (e.g., cash back), they must override the default selection, preselect the AID, and should preselect the Visa U.S. Common Debit AID. In other words, contactless transactions can ultimately be routed over the Visa U.S. Common Debit AID to the same extent as transactions initiated using other methods, but custom logic will be required.

This approach is discussed in more detail in the following sections of the *VSDC Contact and Contactless U.S. Acquirer Implementation Guide*:

- Chapter 2, section on "Special Application Selection Logic"
- Appendix on "Basic EMV Terminal Logic"
- Appendix on "Special Application Selection Logic"

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

Assumptions for EMV Processing Approaches

1. U.S. Covered Visa Debit Cards will contain a Visa U.S. Common Debit AID in addition to a Visa AID. Technically, this assumption is per BIN/PAN. This assumption is likely to remain true for some time (i.e., a given card will only have one source of debit funding).
2. A card may contain both credit and debit functionality. This will be represented by a Visa AID connected to the credit function, and a debit pair consisting of a Visa AID and a Visa U.S. Common Debit AID both connected to a common source of debit funding. Removal of one of the AIDs of the debit pair from the Candidate List during Application Selection will result in two eligible AIDs. Either the highest priority AID can be selected to initiate the transaction or the two AIDs can be presented to the cardholder for selection. Merchants that wish to maintain routing flexibility will need to deploy specific logic in their readers/terminals to ensure the Visa U.S. Common Debit AID is used for debit functionality, in addition to the non-paired Visa AID for credit functionality.
3. The terminal must pass the AID (contained in the DF Name, Tag '84') used to initiate the transaction to the acquirer or other routing entity in the transaction message to enable the acquirer or other routing entities to perform appropriate routing.

U.S. Territories and Protectorates

If there is a business need in a U.S. Territory to support the Visa U.S. Common Debit AID, the terminal should set the Terminal Country Code (Tag '9F1A') to '08 40' **for the Visa U.S. Common Debit AID only**. This will allow acceptance of the Visa U.S. Common Debit AID.

B.4 Visa U.S. Specific References

- Visa U.S. EMV Chip Terminal Testing Requirements
- Visa U.S. Quick Chip and Minimum Terminal Configuration ADVT/CDET Use Cases
- Visa Minimum U.S. Online Only Terminal Configuration
- VSDC Contact and Contactless U.S. Acquirer Implementation Guide

Appendix C. Abbreviations

Table C–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
CDET	Contactless Device Evaluation Toolkit
CDA	Combined DDA/Application Cryptogram (AC) Generation
CDCVM	Consumer Device CVM
CED	Customer Exclusive Data
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

Abbreviations	Meaning
EMV	EMV is a trademark dating back to 1999, and it refers to all of the specifications administered by EMVCo
EPP	Encrypting PIN Pad
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
MSD	Magnetic Stripe Data
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
PKI	Public Key Infrastructure
POS	Point of Service/Point of Sale
PPSE	Proximity Payment Systems Environment
PSE	Payment Systems Environment
PVV	PIN Verification Value
qVSDC	Quick Visa Smart Debit/Credit
RID	Registered Application Provider Identifier

Abbreviations	Meaning
RSA	Rivest, Shamir, Adleman (Public Key Technology)
SDA	Static Data Authentication
TAC	Terminal Action Code
TAD	Transaction Acceptance Device
TADG	Transaction Acceptance Device Guide
TADR	Transaction Acceptance Device Requirements
TC	Transaction Certificate
TCR	Transaction Component Record
TDES	Triple Data Encryption Standard (Triple-DES)
TMS	Terminal Management System
TVR	Terminal Verification Results
UCAT	Unattended Cardholder Activated Terminal
VCMS	VisaNet Certification Management Service
VCPS	Visa Contactless Payment Specification
VEPS	Visa Easy Payment Service
VIS	Visa Integrated Circuit Card Specification
VpTT	Visa payWave Test Tool
VSDC	Visa Smart Debit/Credit
VTS	Visa Test System

Appendix D. Glossary

Table D–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 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. See also 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).
Cryptographic Key	The numeric value entered into a cryptographic algorithm that allows the algorithm to encrypt or decrypt a message.
Cryptography	The study of mathematical techniques for providing aspects of information security, such as confidentiality, data integrity, authentication, and nonrepudiation.
Customer Exclusive Data (CED)	A contactless data element on the card that contains issuer proprietary information and is provided in authorization messages (for U.S. transactions).
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.”
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.

Term	Definition
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.
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.
Encrypting PIN PAD (EPP)	Device used to enter the cardholder's PIN in a secure manner and form part of a PIN Entry Device (PED).
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.

Term	Definition
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.
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 manual transaction.
Magnetic Stripe	The magnetic stripe on a card that is encoded with the necessary information to complete a transaction.

Term	Definition
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
Offline Approval	A transaction that is positively completed (approved) at the POS 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 cardholder verification methodology 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 Capable Chip Device	A contact-chip device that supports both offline and online 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.

Term	Definition
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.
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.

Term	Definition
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.
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 Contact and Contactless 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.
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).

Term	Definition
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.
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.
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 Management System (TMS)	A system used by acquirers and merchants to track and update POS devices.

Term	Definition
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.
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 Requirements (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.

Term	Definition
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.
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*.
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.