Transaction Acceptance Device Guide (TADG)

Version 3.3

Effective: August 2025

Visa Public

Important Information on Confidentiality and Copyright

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

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

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

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

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN: THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. VISA MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

Contents

Tables

Figures

About This Guide

The *Transaction Acceptance Device Guide (TADG)* provides vendors, merchants, acquirers, and device deployers with information to help them deploy transaction acceptance devices ("devices") that support the acceptance of Visa payment cards. It focuses on contact chip and contactless chip card[1] acceptance but also provides information on magnetic-stripe and key-entered transactions for completeness.

This is a public document available at digitalpartnerservices.visaonline.com.

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 seeking information about terminals. 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 or later*
  - *Visa ICC Specifications (VIS)*
- Contactless chip transactions based on either of the following:
  - *EMV Contactless Specifications for Payment Systems, including Book C-3 ("EMV Contactless Specifications")*
  - *Visa Contactless Payment Specification (VCPS)*
- 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 10.4: 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)
- Tap to Phone
- Tap to Consumer Device

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."

[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.

- **Contactless** – The contactless functionality of a chip terminal. Also referred to as "contactless chip" or "qVSDC".
- **Device** – The hardware used to accept a chip card in order to conduct a transaction. Used interchangeably with the term "terminal." In this document, this term refers to both POS devices and ATMs, unless explicitly noted otherwise.
- **qVSDC** –Visa's solution for contactless card acceptance. 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 E: Glossary.

Device Compliance

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

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

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

- **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 applicable PCI SSC standards

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: Contact Chip Transaction Flow – Describes the interaction between terminal and card shown in Figure 4–1: Sample Contact Chip Transaction Flow Diagram

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

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

Summary of Material Changes

This document serves as an update to the previous TADG, version 3.2, published in January 2020. The material changes made to this update are shown in the table below.

Table 1: Summary of Material Changes for Version 3.3

Item	Description	Section
Cardholder Verification Method Requirements	Global Minimum CVM Requirements by Device Type (Table 2–5) has been updated.	2.8.2: CVMs by Device Type
Electrostatic Discharge Management	Electrostatic Discharge Management section has been removed.	Section 2
Dynamic Reader Limits	Dynamic Reader Limits have been removed.	2.13.3: Contactless Transactions
Magnetic Stripe Data (MSD)	MSD has been removed.	5: Contactless Chip Acceptance
Streamlined qVSDC	Streamlined qVSDC has been removed.	5.1: Quick Visa Smart Debit/Credit (qVSDC)
Acquirer Stand-in	Acquirer Stand-in section has been removed	Section 6
Contact Chip Online OCT Transactions	A new section that describes the best practice process for performing OCTs as online chip transactions has been added.	Section 6.3.6
Mobile Top-up	Mobile Top-up section has been removed	Section 6
Kernel Configurations	The description of configurable kernels has been fully refreshed and updated for accuracy	6.8: Kernel Configurations
Level 3 Testing	Level 3 Testing process, tools, and reference documentation has been updated	9.1: Device Testing Overview 9.4: Level 3 Testing
AES Cryptography	References to cryptographic algorithms have been updated to includes AES	Throughout
PCI DSS	References to PCI Standards and all relevant text has been updated or refreshed	Throughout
ISO Standards	ISO references have been updated	10.3: ISO Documents

Item	Description	Section
Visa Document References	The set of Visa documents relevant to this Guide has been updated	10.4: Visa Documents
Visa Common Debit AID	Appendix B has been updated to the latest requirements	Appendix B
Contact Transaction Flow	A new Appendix C has been added to describe contact transaction flow for Accessibility readers	Appendix C
Errata and other corrections	Various corrections to grammar, spelling etc. have been made	Throughout

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 merchant's representative 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 PIN as a CVM. 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, cash/check deposits), 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 to be performed. 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 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 6.4.2: 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 4.12.4: 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, UCAT 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.

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.[3] 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.

[3] 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 5.2.3: 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 to be used for the transaction.

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, merchants and acquirers are responsible for ensuring that all customer-facing devices adhere to 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 Visa Easy Payment Service (VEPS) transactions (see Section 2.13: 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 3.4.1 states: *PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN*.

In light of this requirement, Visa requires that all but the last four digits of the PAN are suppressed on cardholder receipts and displays visible to the cardholder. Other details embossed on the card (e.g., expiration date, BIN) can only be printed on the merchant copy of the receipt.

Last 4 Digits of the PAN

For mobile payment applications, in which the card has been tokenized, the issuer personalizes the Last 4 Digits of PAN data object to enable merchants to print or display the last four digits of the number the cardholder would recognize as their account number (instead of the last four digits of the tokenized PAN, which is usually visible in the mobile payment application but meaningless to the cardholder).

In such transactions, the value of the Last 4 Digits of PAN data object should be printed or displayed by the merchant in place of the last four digits of the value read for the Application PAN from the card.

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.

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.
- I**nstructions 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:

- **Card network/scheme name** – The word "Visa" is required on the receipt where the transaction will be processed as a Visa transaction.[4,5]
- **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.[6] 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.

[4] For U.S. Common Debit transactions, printing the selected Application Label (e.g., Visa Debit or US Debit) or another enhanced descriptor on the receipt is required.
[5] In the Europe Region: For a card that supports more than one payment scheme, the card network/scheme name must only contain "Visa" if Visa is the payment scheme selected by the cardholder or, if the cardholder does not select a payment scheme, the merchant elects to accept the transaction as a Visa scheme transaction.
[6] 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 TDEA or AES cryptography 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[7]	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. Examples include mobile payment devices or cards enabled with biometric elements (for example: requiring a fingerprint).

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 compliant to versions of VIS up to 1.6 but are not recommended or widely used. They are not supported from VIS 3.0 onwards.

[7] Offline Plaintext PIN is no longer supported at UCATs. By 1st January 2030, all chip cards that support Offline PIN must support Offline Enciphered PIN.

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	Y	Y	Y
Signature	Y	Y	Y
Online PIN	Y	Y	Y
Offline Plaintext PIN[8]	N	Y	N
Offline Enciphered PIN	N	Y	N
Offline Plaintext PIN and Signature[9]	N	Y	N
Offline Enciphered PIN and Signature[9]	N	Y	N
Consumer Device CVM (CDCVM)	N	N	Y

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
C = Conditional
O = Optional
– = Not Permitted

[8] Offline Plaintext PIN is no longer supported at UCATs. By 1st January 2030, all chip cards that support Offline PIN must support Offline Enciphered PIN.
[9] Combination CVMs of Offline Plaintext PIN and Signature or Offline Enciphered PIN and Signature are also available on contact chip transactions compliant to versions of VIS up to 1.6 but are not recommended or widely used. They are not supported from VIS 3.0 onwards.

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

CVM	Attended POS Contact Chip Device	Attended POS Contactless Chip Device	Unattended Cardholder Activated Terminal Contact Chip Device	Unattended Cardholder Activated Terminal Contactless Chip Device	Contact ATM	Contactless ATM
Signature	M[10]	M[10]	–	M[11]	–	M[12]
Online PIN	C[13]	C[13]	C[13]	C[13]	M[14]	M[12]
Offline Enciphered PIN	O[15]	–[16]	O[15]	–[16]	–	–
Offline Plaintext PIN	O [15]	–[16]	–	–[16]	–	–
No CVM Required	C[17]	–[18]	M	–[18]	–	–
CDCVM	–	M	–	M	–	M[12]

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.

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.

[10] While the kernel in the device must support signature, the merchant is no longer required to capture and verify the cardholder's signature.
[11] For qVSDC, TTQ Byte 1, bit 2 in the kernel must indicate support for signature to prevent some cards from being unnecessarily rejected, even though signature must not be captured at UCATs.
[12] For qVSDC, to ensure acceptance, ATMs must indicate support for Online PIN, Signature, and CDCVM in the TTQ, even though Online PIN is the only CVM that will apply to ATM transactions. ATMs may prompt for Online PIN regardless of CVM processing.
[13] Mandatory, if Interlink supported.
[14] ATMs shall prompt for Online PIN even if CVM List does not contain it.
[15] Please refer to the *Visa Rules* for specific rules on Offline PIN.
[16] 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.
[17] If the terminal supports VEPS transactions, then "No CVM Required" must be supported. Otherwise, support for "No CVM Required" is optional but strongly recommended.
[18] For qVSDC, "No CVM Required" is not a CVM that is personalized on a qVSDC card but a qVSDC transaction may result in no CVM when neither the card nor device requires a CVM for the transaction (e.g., the transaction is below the Reader CVM Required Limit).

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 2.13: 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.
- **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 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.

2.13.1 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.

Requirement	Description
POS Entry Mode Value	• **Magnetic Stripe Transactions** – Value of 90 or 91[19]. • **Contact Transactions** – Value of 05. • **Contactless Transactions** – Value of 07.

2.13.2 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. This may be configured on a per-transaction basis as described in the *EMV Chip Specifications* Book 4 Section 10.1.2:

- **Transaction Qualifies for VEPS** – The device invokes the specific data object 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 invokes the specific data object configuration where it may support multiple CVMs such as Signature, PIN, etc.

Note: Support for transaction-related data functionality is optional for the terminal. The implementation of this functionality is left to the discretion of the terminal manufacturer and is outside the scope of EMV.

2.13.3 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 country amount limit as defined in the *Visa Rules*.[20]

[19] MSD is out of scope of this document but is listed here for completeness. While a POS Entry Mode value of 91 is supported for VEPS in some regions, it is dependent on local market regulations. See the *Visa Rules* for the specific requirements regarding MSD support in a market/region.

[20] Because the reader requires a CVM when the transaction amount is greater than or equal to the Reader CVM Required Limit, and VEPS does not require a CVM when the transaction amount is less than or equal to the VEPS 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.

2.14 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.

2.15 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[21] 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 Section 5.4: Device User Interface Recommendations.

2.16 Dynamic Currency Conversion (DCC)

Dynamic Currency Conversion (DCC) is one of:

- 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 or the currency inserted.
- A Manual Cash transaction in which the transaction currency is different to the currency disbursed.

DCC is not a Visa service. It is a merchant, ATM or branch-offered currency conversion service that is provided by acquirers or DCC agents. 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* available on Visa Access.
- **DCC Compliance Program** – The global DCC Compliance Program comprises registration, certification, and annual audits. 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*.

[21] 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.

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 2.14: Key-Entry Transactions.

3.2 Magnetic-Stripe Data Processing

A device that accepts magnetic-stripe transactions:

- Reads a magnetic stripe that conforms to the Track 1 or Track 2 data specifications.
- Does not erase or alter any magnetic encoding on a card.
- Transmits 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.
- Is 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 that is processing a transaction using the magnetic stripe either reads and acts upon the Service Code values on a card's magnetic stripe or sends the transaction online to the issuer for authorization. Offline-only devices 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 for a magnetic stripe transaction. 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 magnetic stripe 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 is processing a magnetic stripe transaction and 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

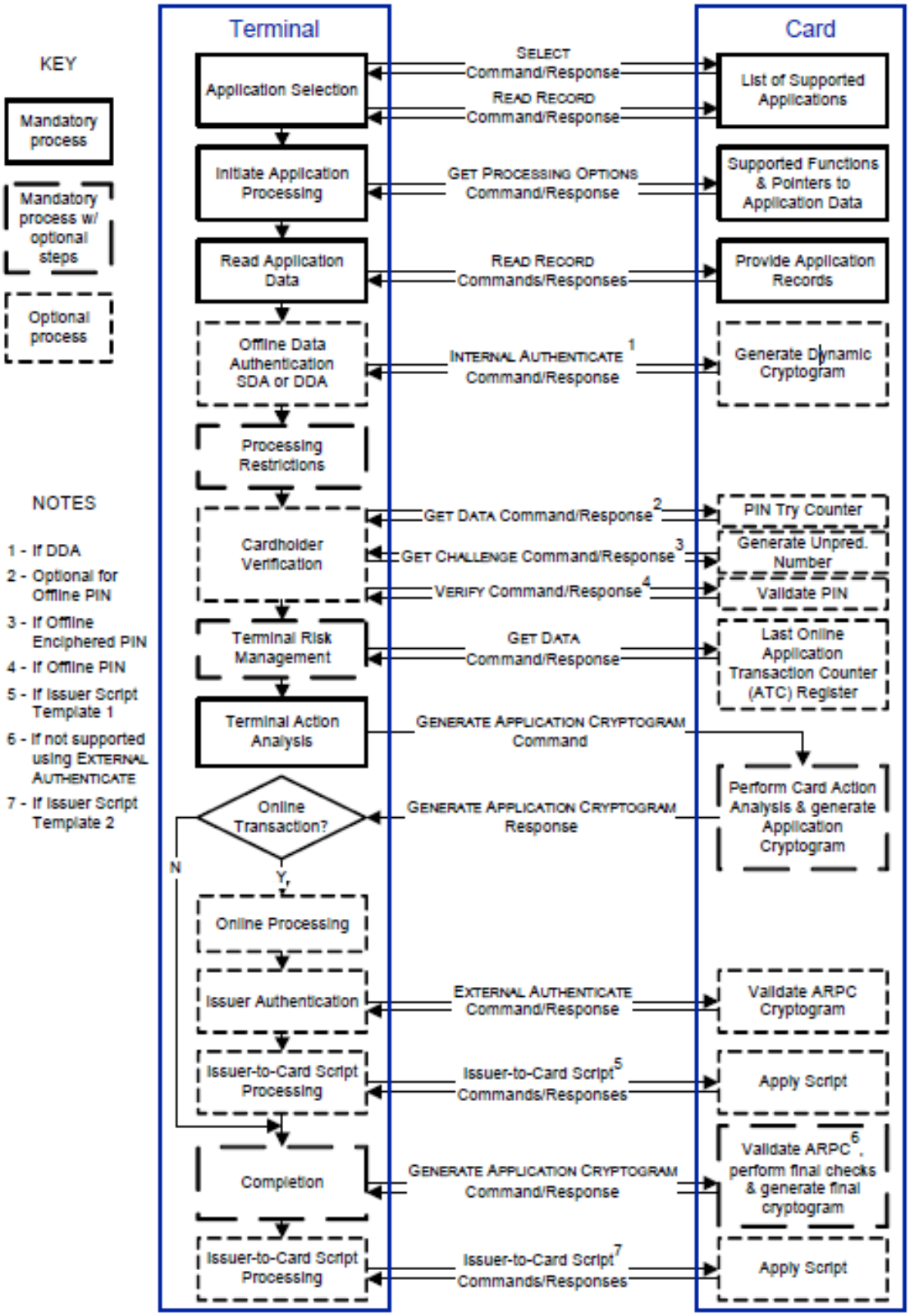
A contact chip card and contact chip device engage in a series of processing steps to complete an EMV transaction:

- 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 (based on VIS 1.6) including all the steps which are described in the subsequent sections. For accessibility, see Appendix C: Contact Chip Transaction Flow Description for a full description of the figure.

Figure 4–1: Sample Contact Chip Transaction Flow Diagram



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[23]) 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 Global Acquirer Implementation Guide*[22] 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[23]. **Error! Bookmark not defined.** These transactions must be authorized online or by voice (see Section 2.14: 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. 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.

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

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 "NOT ACCEPTED" message[24], terminate the chip transaction and (if possible) invoke a magnetic-stripe read. See the *EMV Chip Specifications* Book 4 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. If the application requires Cardholder Confirmation, the cardholder must be given the opportunity to confirm or select the application before it can be used (or the terminal will behave as if there is no application in common).
- **Multiple Applications in Common** – If more than one application is mutually supported,[25] 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).[26] 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.[27]

If the device automatically selects the application, it is important for the device to display the application name[28] 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:

[24] 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.
[25] 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*.
[26] In the U.S., certain requirements related to Application Selection and display do not apply to U.S. Covered Visa Debit Cards.
[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] 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.

- **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 global 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
V PAY	A000000003	2020	A00000000320202[29]

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.

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).

[29] V PAY is only available in Europe. Refer to the *V PAY Card and Acceptance Device Technical Specifications* for the conditions on using this 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	POS devices must contain the Visa AID and Visa Electron AID.[30] **Note:** All devices that accept the Visa Debit/Credit AID must accept the Visa Electron AID (unless the Merchant does not accept Visa Electron Cards by any method, including Magnetic Stripe). 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.[31] **Note:** Visa Interlink can only be accepted at POS devices capable of processing online transactions with Online PIN verification. V PAY-only terminals must be loaded with the V PAY AID only (they must not contain any other Visa AIDs). Terminals that are not V PAY-only must not contain the V PAY AID. 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. See Section 4.3.5.
ATMs	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. V PAY transactions at ATM are performed using the Electron 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.

[30] The Visa Electron AID only needs to be loaded into online-capable terminals.
[31] 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[32] 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 some European countries, 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.

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

Acquirers/merchants choose whether they 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 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. Most terminals support the Directory Selection Method.

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 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.[33]
- **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.

[33] 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.

See the V PAY documents referenced in Table 10–2: Visa Guides, Manuals, and Requirements and Table 10–7: *Visa Rules* for additional information.

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.[34] Device support for Cardholder Selection also allows cardholders with multiple applications to select the one to use for a given transaction.

Note: Device support for Cardholder Selection and Cardholder Confirmation both require the device to have a way to display choices to the cardholder (e.g., a screen) and for the cardholder to provide input (e.g., buttons to press). Thus, a device either supports both Cardholder Selection and Cardholder Confirmation, or it supports neither Cardholder Selection nor Cardholder Confirmation.

Devices should implement support for Cardholder Selection in one of the following ways:[35]

- **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).

[34] 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*.
[35] 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.

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,[34] 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).

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.[36]

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.

[36] 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*.

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

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 that was requested using 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 (enablement in cards is always optional, implementation is mandatory from VIS 3.0)
- 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, not used for newer 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 performs 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.[37] 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 3.0 (hexadecimal '012C' which represents the decimal value of 300)
  - VIS Version 1.6 (hexadecimal '00A0' which represents the decimal value of 160)
  - VIS Version 1.5 (hexadecimal '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 cashback). 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 ("goods" and "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.

[37] When updates to VIS are published in the future, an issuer may choose to indicate which update version is supported by incrementing the Application Version Number value personalized into cards accordingly. 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, but acquirers should be aware of this potential difference in Application Version Number.

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.

4.7 Offline Data Authentication

Offline Data Authentication enables authentication of a payment application for offline transactions. The types of Offline Data Authentication supported by Visa 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
Dynamic Data Authentication (DDA)	Provides protection against both counterfeiting and the replaying of copied data (comparable to magnetic-stripe-data skimming).	Required for all contact-chip devices with offline capability.
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[38]
- 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 on contact chip transactions compliant to versions of VIS up to 1.6 but are not recommended or widely used. They are not supported from VIS 3.0 onwards.

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.

[38] Offline Plaintext PIN is no longer supported at UCATs. By 1st January 2030, all chip cards that support Offline PIN must support Offline Enciphered PIN.

- **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.

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 2.13: 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 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 Online vs Offline Authorized Transactions

The *Visa Rules* require that all transactions are authorized online when the amount exceeds the Floor Limit. The Floor Limit is zero for all transactions and markets, except for specific exceptions in a few markets and for specific MCC codes (see *Visa Rules ID# 0008901*).

For POS terminals, acquirers need to determine whether their terminals need to support offline transactions or if all transactions will be sent online for issuer processing. In the majority of chip programs, support for offline capable devices will not be required.

Note: Environments such as transit or wherever offline data authentication is desired for deferred online authorizations do *not* require terminals that support offline authorization.

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

Note: For more information on floor limits, see *Visa Rules ID# 0008901*.

4.10.2 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) for Contact Chip

AID	Offline-Capable Device	Online-Only Device **Does Not** Support: TAC - Online and TAC - Default Processing	Online-Only Device Supports: TAC - Online and TAC - Default Processing
Visa ISO AIDs[39]	TAC - Denial: '0010000000'[40] TAC - Online: 'DC4004F800' TAC - Default: 'DC4000A800'	TAC - Denial: '0010000000'[40] TAC - Online: n/a TAC - Default: n/a	TAC - Denial: '0010000000'[40] TAC - Online: 'DC4004F800'[41] TAC - Default: 'DC4000A800'[41]
Visa U.S. Common Debit AID[42]	n/a	TAC - Denial: '0000000000' TAC - Online: n/a TAC - Default: n/a	TAC - Denial: '0000000000' TAC - Online: 'FFFFFFFFFF' TAC - Default: 'FFFFFFFFFF'

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.[43] See the *VSDC System Technical Manual* for details on the data elements required in authorization and clearing/settlement messages.

[39] An AID that starts with the Visa ISO Registered Application Identifier (RID) 'A0 00 00 00 03'.
[40] Alternatively, '0000000000' may be used.
[41] Alternatively, 'FFFFFFFFFF' may be used.
[42] U.S. only.
[43] 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.

- **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 cryptogram and its associated data unaltered to the acquirer in the device-to-acquirer message and the acquirer must forward this data unaltered to VisaNet.
- **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 "Card appears on 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 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.[44] 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 4.12.7: Declined Transactions.

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:

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

- **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.[45]
- 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 6.3.9: 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.[45]

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.

[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.

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 6.3.9: 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.

Note: Newer cards perform Issuer Authentication during processing of the second GENERATE AC command, instead of using the dedicated EXTERNAL AUTHENTICATE command. For these cards, the terminal will not know whether Issuer Authentication was performed by the card, or whether it passed.

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 goods/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.

qVSDC is Visa's globally deployed solution for contactless card acceptance. All Visa contactless cards and contactless readers are required to support qVSDC.

For more information on Visa contactless chip card acceptance device requirements, see *VCPS* or the *EMV Contactless Specifications*, Book C-3. Vendors have the option of using either of these specifications.

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.

Note: See the *Transaction Acceptance Device Requirements (TADR)* for configuration requirements for Visa contactless acceptance devices.

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.

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 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 for qVSDC

This section highlights contactless reader requirements for terminals that support qVSDC, and outlines the phases of a qVSDC contactless transaction.

The phases of a qVSDC contactless transaction are:

- Processing Prior to Enabling the Contactless Interface
- Discovery Processing
- Application Selection
- Card Requests Terminal and Transaction Data
- Fast Dynamic Data Authentication (fDDA) (Conditional)

- Cardholder Verification
- Transaction Terminated
- Online Processing
- Transaction Outcome

5.2.1 Processing Prior to Enabling the Contactless Interface

Requirement: All contactless readers are required to support qVSDC.

Requirement: The reader must support Processing Prior to Enabling the Contactless Interface 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: Processing Prior to Enabling the Contactless Interface expedites the transaction by allowing the reader to perform several risk management steps prior to interacting with the card.

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

- **Reader Contactless CVM Required Limit** – Contactless transactions above this limit require cardholder verification. This limit is normally set to the VEPS limit (see the *Visa Rules* for VEPS Maximum Transaction Amounts by market). In markets where VEPS does not apply, the Reader CVM Required Limit may be either disabled or set to the highest possible value.
- **Reader Contactless Floor Limit** – Contactless transactions above this limit require online authorization. For online-only countries, this limit is set to zero.

Note: The contactless device might have a Reader Contactless Transaction Limit. The *Visa Rules* require that a contactless acceptance device must not limit the transaction amount of a contactless transaction. Therefore, if the contactless device has a Reader Contactless Transaction Limit, it must be 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. If the transaction is subsequently processed as a qVSDC transaction, then 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 Discovery Processing

Requirement: The reader must support Discovery Processing.

Background: Discovery Processing is performed by the reader to poll for the presence of contactless cards that may have entered the reader's RF field.

5.2.3 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 most scenarios, the reader will select the highest priority AID on the consumer device.

Note: Local market regulations may require different behavior. Contact your Visa representative for information regarding your market.

Background: Once the reader has completed Processing Prior to Enabling the Contactless Interface:

- The reader signals to the consumer that it is ready for the contactless card to be presented.
- 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 through a secondary application called the Proximity Payment Systems Environment (PPSE).
- If the reader has one or more applications in common with the card, as identified by the Application Identifier (AID), the highest priority application is automatically selected.[46]
- 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 *VCPS* and the *EMV Contactless Specifications*, devices must be able to select AIDs that are between 5 to 16 bytes in length.

5.2.4 Card Requests Terminal and Transaction Data

Requirement: The device must support the TTQ data object 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.

[46] 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."

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 Processing Prior to Enabling the Contactless Interface, if applicable)
- What CVMs are supported (the reader must indicate support for CDCVM)

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

Note: The *VCPS* and *EMV 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 (fDDA) (Conditional)

Requirement: The reader may be required to support fDDA. fDDA is required for:

- Readers supporting offline authorized contactless qVSDC transactions.
- Environments such as transit[47] where the card needs to be authenticated before the transaction is authorized online.

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 (GPO) command rather than generating it at the end of the transaction using the INTERNAL AUTHENTICATE command (when the card may be moving away from the reader's 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 reader-generated Unpredictable Number, 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 card-generated Unpredictable Number.

[47] Throughout this document, "transit" refers to transit network access devices (e.g., transit fare gates), where speed of transaction is the priority. It does not include other retail devices that are deployed in a transit station.

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 qVSDC, if the transaction requires a CVM, the card compares its supported CVMs to the CVMs 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 can be terminated and instead 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 via VisaNet, 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.[48] See the *VSDC System Technical Manual* for details on the data elements required in authorization and clearing/settlement messages.

[48] 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.

- The acquirer submits the authorization message to VisaNet for processing and onward transmission to the issuer (if not processed by Visa as a STIP transaction).
- Based on the results of Online Card Authentication (which may be performed by Visa or the issuer), 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 (or Visa if processed in STIP) 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.

5.2.9 Transaction Outcome

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

If the transaction is approved:

- The transaction may not require a cardholder signature or generation of 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

Consumer devices (such as mobile phones) that contain a Visa contactless payment application can be accepted by 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 consumer device from the point of view of the transaction processing, authorization, and clearing data that is passed through VisaNet systems.

Note: Mobile contactless acceptance devices (e.g., Visa Tap to Phone devices) are out of scope of this document.

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, but a CVM has not yet been performed, 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:

- 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.
- 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.
- 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 of seconds), the contactless reader returns to Discovery Processing to await the re-presentment of the consumer device to reattempt the transaction.
- 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 has already been 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 A 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). More information about the EMV Contactless Symbol can be found on the EMVCo website at www.emvco.com/trademark-centre.

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:

- **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 6.4.3: 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 2.16: 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[49] for Contact
- Deferred Authorizations
- Acquirer Stand-in
- Other Transaction Types
- Industry-Specific Transactions
- Cashback Transactions
- Online-Only POS Environments
- Non-Financial Transactions Using EMV or 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

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 from the host. This is done to remove the complexity around transaction completion processing as well as to expedite the transaction. In addition, to further streamline checkout, Quick Chip optionally allows the application cryptogram to be generated before the final transaction amount is known. These features are also commonly used in Visa contactless transactions. 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 Processing.

Quick Chip:

- Significantly reduces the time that the card remains 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)

[49] Typically deployed only in the U.S.

Quick Chip is a solution that is only applicable to online-only markets (and is typically deployed only in the U.S). Contact your Visa representative for more information.

6.2 Deferred Authorizations

Deferred Authorization may occur when an online authorization is performed after the card is no longer available for presentment/re-presentment, typically because the device temporarily does not have a connection (e.g., communications failure or device is in a transit environment).

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."[50]

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.[51] 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. In some acceptance environments (e.g., transit), the card may also return data that permits Offline Data Authentication (ODA) to be performed by the reader[51].
- Later, the device uploads the deferred authorization requests that include the ARQCs.[52] Field 63.3: Message Reason Code must contain a value of **5206**. This value acts as the deferred authorization indicator.
- The acquirer submits the authorization requests, seeking online approval. Some requests may be declined.
  - Repeated attempts at authorization for declined transactions are permitted but declined transactions must eventually be discarded.
- The acquirer formats and submits a clearing record[53] for each approved transaction, using the ARQC and the Authorization Response Code returned in the authorization response.

[50] For exceptions related to transit, see the *Visa Urban Mobility Implementation Guide* and *Visa Urban Mobility Terminal Requirements and Implementation Guide*.
[51] 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.
[52] Use of the AAC rather than the ARQC in the authorization request may result in unnecessary declines by the issuer.
[53] 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.

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.

6.3 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 processing 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.

6.3.1 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 6.3.2: Incremental Authorizations) and sale completions (see Section 6.3.3: Sale Completions). A pre-authorization may be performed as an Initial Authorization or an Estimated Authorization, depending on the acceptance environment and/or the region/country. See the *Visa Rules* for full details.

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

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 6.3.2: Incremental Authorizations for more information.

- The amount presented to the card in the GET PROCESSING OPTIONS (GPO) command of a pre-authorization should be either a genuine estimation of what the cardholder will spend or an initial authorization amount up to the limit specified in the *Visa Rules* (if applicable to the acceptance environment). In both cases, it should be the same amount and currency that is sent to the issuer in the pre-authorization request message.

6.3.2 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 6.3.1: Pre-Authorizations, the merchant must not store the full chip data or the Track 2 Equivalent Data from the original pre-authorization.

6.3.3 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[54] or, in the case of multiple clearing messages (e.g., 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 for a sale completion should be set to "chip read" (05 for contact, 07 for contactless) 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.

6.3.4 Status Checks

Definition: A Status Check is an online authorization for a single unit of currency to verify the account and to pre-authorize a transaction amount up to the regional or country permitted value as defined in the *Visa Rules*. The use of a Status Check is limited to automated fuel dispensing (AFD) 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.

[54] 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.

6.3.5 Account Verifications

Definition: An account 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).[55]
- Key-entered transaction for a zero amount.

6.3.6 Contact Chip OCT Transactions

Definition: An Original Credit Transaction (OCT) performed as an online chip transaction, used to credit a card account with funds e.g., for the disbursement of gambling winnings.

Transaction: This transaction is an online chip transaction that uses a similar process to Quick Chip (Section 6.1) and Deferred Authorizations (Section 6.2) in that a final cryptogram is requested from the card before online processing has completed. In the case of OCTs, this ensures that the card account is not credited twice due to an incomplete chip transaction, noting that OCT Reversals are not permitted by the *Visa Rules*.

Processing:

- The device requests an ARQC cryptogram, and the card responds with one (if no other reason to decline).
- The device then informs the card that it cannot go online and requests an AAC cryptogram.
- The card responds with an AAC.
- The device passes the authorization request including the initial ARQC to the acquirer.
- The acquirer submits the authorization request to the issuer and returns the issuer response to the device.
- The device completes the transaction based on the issuer response.
- For approved dual-messaging authorizations:
  - The acquirer formats and submits a clearing record for the approved transaction, using the initial ARQC and the Authorization Response Code returned in the authorization message.

[55] A tokenized transaction must include chip data.

6.3.7 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.

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.[56]
- 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" (05 for contact, 07 for contactless) 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.
  - If the PDOL sent by the card to the reader indicates that the Transaction Amount and the Transaction Type are to be included in the GET PROCESSING OPTIONS (GPO) 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[57]), 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.

[56] 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.
[57] Card-requested declines as part of refund transaction processing are no longer performed from *VIS 1.5.3* and *VCPS 3.0* onwards.

6.3.8 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 6.3.9: 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.

6.3.9 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 some 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 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.
- For contact chip, if 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[58])
  - 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$150, then a partial reversal can be submitted for the USD$50 difference between the estimated and final amounts. The chip-related requirements for partial reversals are the same as those for full reversals.

Note: See the Visa Direct Original Credit Transaction (OCT) - Global Implementation Guide for additional guidance about reversals of OCTs.

6.3.10 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 card data elements held in the device.

[58] The terminal may not be aware of Issuer Authentication results. If the card performs Issuer Authentication during the GENERATE AC command processing, the CVR will inform the issuer of Issuer Authentication results.

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.

6.4 Industry-Specific Transactions

Certain industries have specific payment requirements beyond the basic purchase transaction`. For each scenario, the presence of a chip card may or may not have an impact on non-chip processing requirements. The following sections outline the typical 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 2.14: Key-Entry Transactions.

6.4.1 Hotels and Tourism Industries

The common payment scenarios used in the hotel and tourism industry should be handled as follows:

Table 6–1: Hotel 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. 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 6.3.1: 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 6.3.2: 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 6.3.3: 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.

Processes similar 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.

6.4.2 Fuel/Petrol Dispensing

The common payment scenarios used in the fuel/petrol industry should be handled 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[59]	For chip transactions, the merchant must complete either of the following before fuel is dispensed: • **Status Check** – The Status Check provides authorization protection up to the regional or country permitted value as defined in the *Visa Rules*. • **Initial Authorization Request** – The Initial Authorization provides authorization protection up to the approved transaction 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 6.3.4: Status Checks. For more information on pre-authorizations, see Section 6.3.1: Pre-Authorizations. For more information on sale completions, see the row in this table and Section 6.3.3: 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 Acquirer Confirmation Advice within two hours of the Status Check for the actual amount. This advice must confirm the final transaction amount.
Sale Completion	When fuel dispensing is completed and the final transaction amount is known, in some countries a sale completion (which is a clearing transaction) for the final amount must be submitted containing the chip data from the Status Check or Initial Authorization Request. Single-message environments may require an adjustment to the pre-authorization amount, particularly if an Initial Authorization Request was used rather than a Status Check. For more information on sale completions, see Section 6.3.3: Sale Completions.

[59] The Visa rules for AFD pre-authorization request types changed from April 2025. See the latest *Visa Rules* for details.

Offline chip approvals are not appropriate for fuel dispensing as it is not possible to adjust the final transaction amount to 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.

6.4.3 Gratuities/Tips

Gratuities/tips may be handled using one of the two options outlined in the following table; however, acquirers 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.

Table 6–3: Gratuities/Tips Options

Options	Description	Authorization Amount / Cryptogram Amount	Clearing Amount / Cryptogram Amount[60]
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 Cashback Amount fields should not be used for processing tips.

6.4.4 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 obtain the PAN and reach out to the other merchant system(s) with the PAN to see if a discount applies prior to initiating the chip transaction.

[60] 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 cryptogram was generated using the original amount.

6.5 Cashback Transactions

This section outlines general and chip-specific requirements for cashback.

6.5.1 General Cashback Requirements

General cashback requirements are outlined in the following table:

Table 6–4: General Cashback Requirements

Topic	Description
***Visa Rules* and Local Requirements**	Devices supporting cashback must be configured to meet all of Visa's cashback rules including any local requirements.
Domestic Transactions Only	Visa allows cashback to be provided with a purchase at the point of sale for domestic transactions, under certain conditions. **Note:** Cashback will be expanded to support International Transactions from 2026
Online Authorization with Cardholder Verification	All cashback transactions must be online authorized and include appropriate cardholder verification (i.e., cashback transactions with Signature or "No CVM" are not permitted[61]).
Separate Entry of Purchase and Cashback Amounts	The device must be able to give the merchant the capability to enter purchase and cashback amounts separately.
Amount and Cashback Amount in Transaction	The cashback amount must be uniquely identified in the authorization and clearing messages from the total transaction amount: • Total transaction amount (purchase plus cashback) in Amount, Transaction (Field 4). • Cashback amount in Other Amounts (Field 61.1).
Reconciliation	An end-of-day batch from devices must identify cashback amounts so merchants can reconcile with their cash drawers.

[61] The *Visa Rules* permit cashback without a CVM in Argentina, instead allowing use of a valid cardholder identification document.

Topic	Description
Cashback Responses	The device must be able to handle responses relating to cashback such as: • A response from the issuer that the cashback service is not available to the cardholder. • A response that the cashback amount is more than the maximum cashback amount agreed for the country. (In this case, the merchant could retry the transaction for a smaller cashback amount or for the purchase amount only.) • A response that the cashback amount is equal to the total transaction amount (this is not allowed in most markets. See *Visa Rules* for local market regulations).

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 cashback requirements for chip transactions, see the next section for details.

6.5.2 Chip Cashback Requirements

This section outlines cashback requirements for chip transactions.

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

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

1. **Cashback Inquiry** – The device asks the cardholder if they would like cashback and, if so, obtains the cashback amount from the cardholder. It may be useful to inquire about cashback prior to Application Selection if the choice of cashback 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 cashback) 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 cashback 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 cashback amount.
- **Cryptogram Cashback Amount (Field 149, EMV Tag '9F03')** – This field contains the cashback amount.

- **Cryptogram Transaction Type (Field 144, EMV Tag '9C')** – This field should contain the value '00' (although '09' may apply in certain markets).

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 6.5.1: General Cashback Requirements for details.

The values in the Cryptogram Amount and Cryptogram Cashback Amount must always be the values passed from the device to the card.

Important: Gratuities/tips should not be placed in the Cryptogram Cashback Amount field. For more information on gratuities/tips, see Section 6.4.3: Gratuities/Tips.

6.6 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.[62] If online processing is not available, the device will request an AAC in the second cryptogram generation.

Note: Devices may effectively be 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).[63] 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.

[62] 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.
[63] 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 Required" only. For more information on VEPS, see Section 2.13: Visa Easy Payment Service (VEPS).

- **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.

6.7 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.

These types of transactions are further described in the *Recommendations for EMV Processing for Industry-Specific Transaction Types* available at www.emvco.com.

6.8 Kernel Configurations

Device kernels can be configured to support different functionality depending on the environment they operate in or to support a function or process under certain circumstances. The approach to configurable application kernels is different for a contact kernel vs a contactless kernel.

6.8.1 Contact Kernel Configurations

A Multiple Configuration Kernel (MCK) is a kernel that has been tested for multiple configurations during EMV type approval. Then, during deployment, the kernel must be set up in one of the approved configurations.

If optional functions are configurable (i.e., they can be turned on or off), then all required configurations must be individually EMV type approved. The scope of testing for each possible configuration is reduced for functions of configurations that have already been tested.

6.8.2 Contactless Kernel Configurations

The following description applies to EMVCo testing of kernels compliant to *EMV Contactless Specifications* Book C–3, and Visa testing of kernels compliant to the *Visa Contactless Payment Specification (VCPS)*.

A contactless kernel that supports optional configurable features must indicate all the supported features to be tested in the submission to EMV type approval.

All configurable features will then be tested in on and off modes. Once approved, the vendor may deploy the kernel with any of the approved options set on or off. Any option not originally identified in the submission as supported must remain off.

7. Security Characteristics

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

- Public Key Management
- Triple Data Encryption Algorithm (TDEA) and Advanced Encryption Standard (AES) 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 RSA Public Key Management

Devices that support one or both of the following must be loaded with the currently active VSDC CA RSA Public Keys[64]:

- 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 RSA 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 RSA Public Keys if they support Offline Enciphered PIN.
- **Transit** – Transit devices generally support Offline Data Authentication; therefore, they must contain the relevant RSA public keys (including the transit-specific key[64]). See the Transit documentation resources in Section 10.4: Visa Documents for more information.

[64] Available here: digitalpartnerservices.visaonline.com/Document/Download/579

7.1.1 VSDC CA RSA Public Keys – General Requirements

General requirements for VSDC CA RSA Public Keys:

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

Topic	Description
Acquirer Responsibility	Acquirers are responsible for ensuring that the VSDC CA RSA 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 RSA 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 RSA 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 RSA Public Keys and their associated data elements.
1984 Key Length	Devices must be able to support RSA key lengths up to 1984 bits. The current recommended lengths can be found on www.emvco.com and the Visa key length requirements at digitalpartnerservices.visaonline.com/Document/Download/579.
Key Selection via RID and Certification Authority Public Key Index (CA PKI)	A device must be able to select the corresponding key and algorithm in conjunction with the RID and CA PKI of the selected application.
Test Keys	Acquirers and device vendors must ensure that any RSA test keys that may have been loaded into the device to support testing are removed from production devices before deployment.

7.1.2 VSDC CA RSA Public Keys – Downloading

Device deployers can obtain the VSDC CA RSA Public Keys from the *Visa Smart Debit/Credit Certificate Authority Public Keys* document which is available for public download at digitalpartnerservices.visaonline.com/Document/Download/579.

7.1.3 VSDC CA RSA 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 RSA Public Keys, including a SHA-1 hash digest of each key, and explains how to validate the VSDC CA RSA Public Keys against a secondary source.

Validating the VSDC CA RSA 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 RSA Public Keys) being compromised (hacked) while an acquirer is downloading the keys, or if the Visa website is being locally or globally spoofed.

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

7.1.4 VSDC CA RSA Public Keys – Loading

While Visa does not mandate specific loading processes for the VSDC CA RSA 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 CA 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 RSA Public Keys – Expiration

Based on EMVCo assessments and recommendations, Visa periodically reviews and determines the expiration dates of the VSDC CA RSA 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* (which can be downloaded as described in Section 7.1.2). Acquirers must support removal of expired keys from their devices based on the expiration and removal dates. Generally, a 6-month grace period starting from the planned expiration date is provided to assist acquirers in these efforts.

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

7.1.6 VSDC CA RSA 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) RSA Private Key (i.e., the VSDC CA RSA 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 RSA 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 RSA 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 RSA Public Keys – Distribution and Management

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

Table 7–2: VSDC CA RSA 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 RSA 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.

Topic	Description
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 RSA Public Keys are active in each of their devices.
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 RSA Keys

Issuer and ICC public RSA 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 RSA keys that are not based on 8-byte boundaries (e.g., a key may be 127 bytes long).

7.2 TDEA and AES Key Management

Triple Data Encryption Algorithm (TDEA) or Advanced Encryption Standard (AES) 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 security controls outlined in the *PCI PIN Security Requirements and Testing Procedures* and *PCI PIN Transaction Security (PTS) Point of Interaction (POI)* standards.

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:

- *PCI PIN Security Requirements and Testing Procedures*
- *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*
- Visa PIN Security website at usa.visa.com/partner-with-us/info-for-partners/pin-security.html

7.3.1 PIN Length and Character Set

This section outlines PIN length and character set requirements:

- **PIN Character Set** – The permitted PIN character set is 0 to 9 (as specified in *ISO 9564-1*).
- **Minimum PIN Length** – The minimum PIN length is 4 digits (as specified in *ISO 9564-1*).
- **Online PIN Length** – Per *Visa Rules*, ATMs must be able to accept Online PINs of 4-6 digits in all regions except the U.S., and be able to accept Online PINs of 4-12 digits in the U.S.
- **Offline PIN Length** – Per *EMV Chip Specifications*, Book 3 Table 25, chip devices must be able to handle Offline PINs between 4 and 12 digits.

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 and Testing Procedures*. • As specified in the *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*.

Topic	Description
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.
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**[65] – 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:

[65] Offline Plaintext PIN is no longer supported at UCATs. By 1st January 2030, all chip cards that support Offline PIN must support Offline Enciphered 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 enciphered PIN. Please refer to the *Visa Rules* for specific rules on Offline PIN.

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

- *EMV Chip Specifications*
- *PCI PIN Security Requirements and Testing Procedures*
- *PCI PIN Transaction Security (PTS) Point of Interaction (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 4.4, 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 Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements* 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 Transaction Security (PTS) Point of Interaction (POI) Security Requirements* and listed as approved on the PCI Approved PTS Devices 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 security.

7.4.1 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 with the *Payment Card Industry Security Standards Council (PCI SSC)* standards (as applicable):

- *Payment Card Industry Data Security Standard (PCI DSS)*
- *PCI PIN Security Requirements and Testing Procedures*
- *PCI Software Security Framework (SSF)*
- *Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*

Acquirers must ensure their merchants and service providers comply with all applicable Visa Rules and programs related to cardholder data security. For more information, see the following:

- corporate.visa.com/en/resources/security-compliance.html
- corporate.visa.com/en/resources/pin-security.html
- Section 10.2 PCI SSC Documents for a list of reference materials and where to find them.

7.4.2 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.

7.5 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 and interoperability 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 identifiers that will be supported in the device and review the listing of approved kernels at www.emvco.com for those kernel identifiers. The later the version of specifications and test plan, the less likely that any in-the-field interoperability problems will arise.
Software Updates	When global interoperability problems are discovered, 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: RSA Public Key Management for details.

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/document_library/.

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 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 the steps concurrently instead of sequentially (e.g., Offline Data Authentication, Processing Restrictions, Cardholder Verification, and Terminal Risk Management).

See Section 2.11: Transaction Speed for information on the speed requirements for contactless 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[66]:

[66] See *EMV Acquirer and Terminal Security Guidelines* and *EMV Chip Specifications, Book 4*.

- **Clock Synchronization** – The clock should be synchronized regularly to ensure it is accurate and that any seasonal time shifts are taken into account. The synchronization may typically be during a terminal management session or when polled for the collection of transactions for clearing and settlement.
- **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

Devices should be well maintained:

- **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.

  Note: PCI DSS does not permit sensitive authorization data to be stored in persistent memory.
- **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. When the terminal supports batch data capture, the captured transactions and advices stored in the terminal should not be erased or altered until the next reconciliation with the acquiring system.

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

The following describes some basic principles regarding 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: 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 4.10.2: 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 RSA Public Keys (If device supports Offline Data Authentication or Offline Enciphered PIN)	Section 7.1: RSA 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 and Contactless: Performed using a third-party vendor-provided Visa-confirmed L3 test tool that contains the Visa EMV-compliant L3 Test Set Files. Once L3 testing is completed, acquirers submit L3 testing results to Visa using the Chip Compliance Reporting Tool (CCRT) available on Visa Access.

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 Contact Level 2 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.

9.3 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*.

9.4 Level 3 Testing

Once the contact and/or contactless device has been approved at L1 and L2 (see the above sections for details), it must undergo Level 3 (L3) testing. L3 testing helps ensure that chip terminals that have been configured for deployment by acquirers are correctly integrated into the Visa payment acceptance environment and do not contribute to interoperability problems. This improves acceptance of Visa-branded products.

Note: L3 testing applies to both contact and contactless devices.

L3 testing is performed using a third-party vendor-provided L3 test tool that contains the Visa EMV-compliant L3 Test Set Files. Acquirers need to obtain an L3 test tool from an L3 test tool vendor and use it to perform L3 testing on their chip device. During testing, the device must be connected to their acquirer host environment and through to either the VisaNet Certification Management Service (VCMS) or a Visa-confirmed host simulator.

Once L3 testing is completed, acquirers must submit L3 testing results to Visa using the Chip Compliance Reporting Tool (CCRT) available on Visa Access at digitalpartnerservices.visaaccess.com/ (unless the acquirer is the U.S. or LAC region and participates in the Visa Global Acquirer Self-Accreditation Program).

For more information, refer to the following documents:

- *Visa Global L3 Testing Guidelines and Frequently Asked Questions*
- *EMV Qualified and Visa Confirmed L3 Test Tools*

9.4.1 Visa Chip Vendor Enabled Service (CVES)

The Visa Chip Vendor Enabled Service (CVES) is a global service that supports acquirers in their Level 3 testing efforts for both contact and contactless chip implementations. Through this program, acquirers have the option of engaging third-party L3 test tool vendors to execute Level 3 testing on their behalf. Acquirers can obtain a list of participating vendors on Visa Access at digitalpartnerservices.visaaccess.com/.

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

9.5 Level 1 and Level 2 Approvals, Renewals, and Revocations

Once the device has been successfully tested, Visa/EMVCo (as relevant) issues a letter of approval[67] (LoA) 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.

[67] 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.

- **Visa** – For products completed through the Visa testing process:
  - The device will appear on the Visa Approved Products – Chip Card Acceptance Devices list located on the Visa Digital Partner Services (VDPS) website at digitalpartnerservices.visaaccess.com/Product/ChipCardAcceptanceDevices.
  - 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 any payment applications that Visa continues to support.
  - For more information on the Visa approval and renewal policies, see the Visa Digital Partner Services (VDPS) website at digitalpartnerservices.visaaccess.com/Document.

9.6 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 if required. Acquirers should be aware that Visa has a Chip Interoperability Compliance 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. For L3 re-testing requirements, refer to the *Visa Global L3 Testing Guidelines and Frequently Asked Questions*.

10. References

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

- EMVCo Documents
- PCI SSC Documents
- ISO 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")*
- *EMVCo Contactless Symbol Reproduction Requirements and EMVCo Contactless Indicator Reproduction Requirements (both available in the EMVCo Trademark Centre at emvco.com/trademark-centre)*
- *Recommendations for EMV Processing for Industry-Specific Transaction Types*

10.2 PCI SSC Documents

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

- *PCI Data Security Standard (PCI DSS)*
- *PCI Security Software Framework (PCI SSF)* which consists of:
  - *PCI Secure Software Standard*
  - *PCI Secure Software Lifecycle (Secure SLC) Standard*
- *PCI PIN Security Requirements and Testing Procedures* (also known as the PCI PIN Security Standard)
- *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*
- *Skimming Prevention: Best Practices for Merchants*

Note: Please ensure that the most current versions of PCI documents are used.

10.3 ISO Documents

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

- *International Standards Organization (ISO) 3166-1: Codes for the Representation of Names of Countries.*
- *International Standards Organization (ISO) 4217: Codes for the Representation of Currencies and Funds.*
- *International Standards Organization (ISO) 7816-5: Identification Cards—Integrated Circuit Cards with Contacts—Part 5: Numbering System and Registration Procedure for Application Identifiers.*
- *International Standards Organization (ISO) 8859: Information Processing—8-bit Single-Byte Coded Graphic Character Sets.*
- *International Standards Organization (ISO) 9564-1: Banking—Personal Identification Number Management and Security.*
- *International Standards Organization (ISO) 10118-3: IT Security techniques — Hash-functions – Part 3: Dedicated hash-functions*.
- *International Standards Organization (ISO) 18033-3: Information technology — Security techniques — Encryption algorithms – Part 3: Block ciphers.*

10.4 Visa Documents

Unless otherwise indicated below:

- Acquirers can obtain Visa documents from Visa Access at visaaccess.com.
- Vendors can obtain Visa documents from the Visa Digital Partner Services (VDPS) Library at digitalpartnerservices.visaaccess.com/Document. Vendors will need to register and obtain a license to access most documents (vendors can use the VDPS 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 Chip Specifications

Title and Description	Audience	User
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
Quick Chip for EMV and qVSDC - Specification Describes modifications to the use of standard processes for EMV contact chip transactions that is compatible with EMV kernels and optimizes processing time by removing or reducing dependencies for chip insertion time in the reader. It also provides guidance to achieve a similar experience for qVSDC contactless chip transactions. **Note:** Please see Section 6.1 for more guidance about the use of Quick Chip.	Issuers, Acquirers, Vendors	Policy, Operations, Technical

Table 10–2: Visa Guides, Manuals, and Requirements

Title and Description	Audience	User
Dynamic Currency Conversion (DCC) Guide – DCC Program Requirements Outlines the requirements and best practices for DCC for acquirers, merchants, and ATMs.	Acquirers, Merchants, Vendors	Policy, Operations
Payment Technology Standards Manual Furnishes the standards applied to Online PINs, PIN-related security, and TDEA/AES 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
T*ransaction 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 digitalpartnerservices.visaonline.com.	Acquirers, Processors, Vendors	Operations, Technical
Transaction Acceptance Device Requirements (TADR) Outlines chip-device requirements that are not covered in the *Visa Rules*.	Acquirers, Vendors	Policy, Operations, Technical

Title and Description	Audience	User
Visa Direct Original Credit Transaction (OCT) – Global Implementation Guide Provides the requirements and best practices for Original Credit Transactions for acquirers, service providers, merchants, and issuers.	Acquirers, Merchants, Processors, Issuers	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
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 Global 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
Visa Contactless ATM Acquiring Guide Provides requirements and guidelines for supporting contactless at ATMs.	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

Table 10–3: Merchandise Returns/Refunds

Title and Description	Audience	User
Credit Voucher and Merchandise Return Authorization Messages – Global Implementation Guide A Guide for Acquirers with respect to their implementation of purchase return authorization messages.	Acquirers, Merchants, and Vendors	Technical

Table 10–4: Visa Branding

Title and Description	Audience	User
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. Available at www.merchantsignage.visa.com	Acquirers, Merchants, and Vendors	Marketing Operations

Table 10–5: Visa Public Keys

Title and Description	Audience	User
Visa Smart Debit/Credit (VSDC) Certificate Authority (CA) Public Keys Provides the VSDC Certificate Authority (CA) Public Keys (includes both test and production keys). Available at digitalpartnerservices.visaonline.com/Document/Download/579	Acquirers, Vendors	Technical

Table 10–6: Visa Level 3 Testing

Title and Description	Audience	User
Visa Chip Vendor Enabled Service (CVES) Provides an overview of the Chip Vendor Enabled Service (a service that acquirers in some regions can use for L3 testing where third-party vendors perform L3 testing on their behalf enabling a faster time-to-market for chip contact and contactless terminal deployment).	Acquirers, Vendors	Policy
EMV Qualified and Visa Confirmed L3 Test Tools Provides a list of vendor test tools available for L3 testing.	Acquirers	Operations
Visa Global Chip Acquirer Self-Accreditation Program Provides acquirers with information on the Self-Accreditation Program (a program to streamline L3 testing for acquirers).	Acquirers	Policy
Visa Global Level 3 (L3) Testing Guidelines and Frequently Asked Questions Provides Visa's guidelines for Visa Global L3 Testing along with answers to frequently asked questions.	Acquirers, Vendors	Policy, Operations

Table 10–7: *Visa Rules*

Title and Description	Audience	User
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

Title and Description	Audience	User
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 Core Rules and V PAY Product and Service Rules ("V PAY Rules") (Europe Region Only) Provides regulations for issuers and acquirers, including rules governing contact and contactless transactions, dispute processing, and interchange rates for V PAY system participants.	Issuers, Acquirers	Policy, Operations

Table. 10-8 Visa Transit

Title and Description	Audience	User
Visa Business News AI12430 - Reminder: Clients Must Ensure Proper Handling of Mobility and Transport Transactions - published 13th October 2022. To support increasing demand for tap-to-ride urban mobility payments, this VBN reminds clients of the requirements for handling mobility and transport transactions.	Acquirers and Processors in AP, Canada, CEMEA, LAC, Europe regions	Technical, Policy, Operations
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 Urban Mobility 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 Urban Mobility 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

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 and contactless (and possibly 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

An active transmitting device (e.g., mobile phone) 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[68] 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 both Visa networks and the appropriate debit unaffiliated network. When the Visa AID is selected, the transaction must only be routed to a Visa network.

[68] A U.S. Covered Visa Debit Card is 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. U.S. 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 for more details. If a customer presents a U.S. Covered Visa Debit Card with multiple funding sources (e.g., credit and debit applications), merchants shall 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, often referred to as "AID filtering", which may result in auto-selection of the application.

Merchants can promote their preferred Cardholder Verification Method, including encouraging the use of PIN. 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 without a PIN (e.g., "No CVM"), even if the cardholder is steered to enter a PIN.

Recommended PIN opt-out options include:

- If the US Common AID is selected, allowing the cardholder to use the "cancel" button to opt out of PIN prompt after clearly explaining to the cardholder how to opt out. For contact chip transactions the PIN Entry Bypass bit is set in the Terminal Verification Result. This bit should **not** be set in contactless transactions
- 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
- Using standard application selection that allows the cardholder to select the Visa Debit application. Any circumstances that result in the selection of the Visa AID, a PIN Entry Bypass feature is not required
- For contactless transactions, a high value Cardholder Verification Method (CVM) limit may also be set eliminating the need for any additional logic

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, including applicable Visa networks, such as Interlink and VisaNet. 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 the Signature CVM method (or "No CVM" method) 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 the 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 (AID Filtering)

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 B, section on "Basic EMV Terminal Logic"
- Appendix C, section on "Special Terminal Logic"

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., cashback), they must override the default selection, 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 B, section on "Basic EMV Terminal Logic"
- Appendix C, section on "Special Terminal 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 who 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 '0840' **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

Please refer to the following U.S.-specific reference documents for U.S. implementations:

- *Visa U.S. EMV Chip Terminal Testing Requirements*
- *Visa Minimum U.S. Online Only Terminal Configuration*
- *VSDC Contact and Contactless U.S. Acquirer Implementation Guide*

Appendix C. Contact Chip Transaction Flow Description

For accessibility tools that have difficulty describing flow diagrams, this appendix provides a verbal description of the interaction between terminal and card that was shown in Figure 4–1: Sample Contact Chip Transaction Flow Diagram.

Step 1. The transaction process begins when the card is inserted into the terminal. The terminal conducts Application Selection through the SELECT Command/Response and (if required) a number of READ RECORD Command/Response interactions in order to get the list of supported applications from the card. The terminal then selects the final application to be used for the transaction and sends another SELECT Command to the card to select the chosen application. The card responds with a list of data objects that it requires from the terminal in order to process the transaction. Application Selection is mandatory as it sets the foundation for the transaction by identifying and selecting the appropriate application on the card.

Step 2. Next, the terminal performs Initiate Application Processing. The terminal sends a GET PROCESSING OPTIONS command to the card and receives a response that contains information about the functions supported by the card and some pointers to application data. This step is mandatory.

Step 3. The terminal then performs Read Application Data to read the application data from the card via a series of READ RECORD Commands/Responses. This step is mandatory.

Step 4. Next, if Offline Data Authentication (ODA) is supported, the terminal sends an INTERNAL AUTHENTICATE Command to the card which generates a dynamic cryptogram and supplies Signed Dynamic Application Data. The terminal then performs Offline Data Authentication to verify that the card is genuine. Support for ODA processing is optional in cards.

Step 5. Processing Restrictions are checked next. The terminal checks if the card has any restrictions of usage (for example, whether the card is limited to domestic use, or is not permitted at ATMs). This step ensures adherence to processing restrictions set by the card issuer, noting that some types of check are optional in the card and may not be supported.

Step 6. Cardholder Verification follows, in which the card provides a Cardholder Verification Method (CVM) List that identifies the supported CVMs. If the terminal chooses Offline PIN (if supported by the card), it then sends the GET DATA Command to the card to get the PIN Try Counter (if supported by the card), which then sends the PIN Try Counter to the terminal. If the PIN Try Counter equals zero, then Offline PIN is not permitted. Else, the terminal sends a GET CHALLENGE Command to the card which generates an Unpredictable Number and returns this to the terminal. Finally, the terminal sends the VERIFY Command to the card which verifies the submitted PIN value and then sends a response to the terminal. All other CVM methods do not interact with the card and are managed via the terminal.

Step 7. Terminal Risk Management is then performed using data provided by the card. This involves executing risk management checks that are mandatory but may include additional optional checks based on the terminal's configuration and the card's data.

Step 8. In the Terminal Action Analysis step, the terminal uses the Issuer Action Codes (IACs) returned by the card and its own Terminal Action Codes (TACs and analyzes the previously performed offline processing to identify the transaction disposition and determine what type of cryptogram to request from the card. The terminal then sends a GENERATE AC command to the card. This step is mandatory and helps determine whether to proceed with online processing or offline approval/decline.

Step 9. In the Card Action Analysis step, the card may perform velocity checking and other risk management checks, sets the results of those checks into the Card Verification Results (CVR), and generates the cryptogram. The card may downgrade the cryptogram type from that requested by the terminal (for example, request an offline decline. The resulting cryptogram options for *VIS 1.6* and *VIS 3.0* are different. At this step, a *VIS 3.0* card cannot return a TC (offline approval) cryptogram type.

Step 10. If Online Processing is selected (the card returned an ARQC cryptogram type), the terminal sends an authorization request to the acquirer. The acquirer then submits the request via VisaNet to the issuer (unless Visa Stand-in Processing occurs) for authorization and receives an authorization response via the same route. This step is mandatory if online processing is required.

Step 11. The transaction then moves to the Completion stage, in which the terminal requests a final cryptogram from the card (using the GENERATE AC Command) and the card makes a decision about the final transaction disposition. This step is not performed if the card approved the transaction with a TC cryptogram type at Step 9.

Step 12. Finally, the terminal (or the acquirer) records the transaction data and may print a receipt if applicable. This final step is mandatory to ensure the transaction is properly recorded and concluded.

Note: There is an optional processing step called Issuer-to-Card Script Processing that may occur either between Steps 10 and 11, or between steps 11 and 12. This is not described in the above to reduce complexity.

Appendix D. Abbreviations

Table D–1: Abbreviations

Abbreviations	Meaning
AAC	Application Authentication Cryptogram
AC	Application Cryptogram
AES	Advanced Encryption Standard
AFD	Automated Fuel Dispenser
AID	Application Identifier
AIP	Application Interchange Profile
ANSI	American National Standards Institute
ARPC	Authorization Response Cryptogram
ARQC	Authorization Request Cryptogram
ATM	Automated Teller Machine
AUC	Application Usage Control
BIN	Bank Identification Number
CA	Certificate Authority
CAM	Online Card Authentication
CDA	Combined DDA/Application Cryptogram (AC) Generation
CDCVM	Consumer Device CVM
CED	Customer Exclusive Data
CVM	Cardholder Verification Method
CVR	Card Verification Results
DCC	Dynamic Currency Conversion
DDA	Dynamic Data Authentication
DDOL	Dynamic Data Authentication Data Object List
DES	Data Encryption Standard
EMV	EMV is a trademark dating back to 1999, and it refers to all of the specifications administered by EMVCo
EPP	Encrypting PIN Pad
fDDA	Fast Dynamic Data Authentication
FFI	Form Factor Indicator

Abbreviations	Meaning
IAC	Issuer Action Code
IAD	Issuer Application Data
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
IFM	Interface Module
IPK	Issuer Public Key
ISO	International Organization for Standardization
L1	Level 1
L2	Level 2
L3	Level 3
ODA	Offline Data Authentication
PAN	Primary Account Number
PCD	Proximity Coupling Device
PCI SSC	Payment Card Industry Security Standards Council
PED	PIN Entry Device
PIN	Personal Identification Number
PIX	Proprietary Application Identifier Extension
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
RSA	Rivest, Shamir, Adleman (Public Key Technology)
TAC	Terminal Action Code
TADG	Transaction Acceptance Device Guide
TADR	Transaction Acceptance Device Requirements
TC	Transaction Certificate
TCR	Transaction Component Record
TDEA	Triple Data Encryption Algorithm (Triple-DES)

Abbreviations	Meaning
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
VSDC	Visa Smart Debit/Credit

Appendix E. Glossary

Table E–1: Glossary

Term	Definition
Account Number Verification	Account Number Verification is an online authorization for a zero amount. It can be used to validate that the card used to make a reservation or to pay for services in advance of delivery is authentic.
Acquirer	A Visa client financial institution that signs a merchant or disburses currency to a cardholder in a Cash Disbursement and, directly or indirectly, enters the resulting transaction receipt into interchange.
Advanced Encryption Standard (AES)	The advanced encryption standard defined in ISO/IEC 18033-3.
American National Standards Institute (ANSI)	A U.S.A. standards accreditation organization.
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 TDEA or AES key.
Application Cryptogram	A cryptogram generated by the card application.
Application Identifier (AID)	A data object 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 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.
Asymmetric Algorithm	An algorithm in which the key used for encryption is different from the key used for decryption (see the definitions for Public Key and Private Key). RSA is an example of an asymmetric encryption algorithm.
ATM Cash Disbursement	A Cash Disbursement obtained at a Visa or PLUS ATM.

Term	Definition
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 TDEA or AES 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 TDEA or AES 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 Contactless application on the card.
Card Authentication	A means of validating whether a card used in a transaction is a genuine card issued by an 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.
Cardholder Activated Device	See UCAT.
Cardholder Selection	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.

Term	Definition
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	The functions and processing 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 Message	A record of a presentment or reversal in the format necessary to clear the transaction. Also referred to as a clearing transaction or clearing record.
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 a 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 Symbol	See EMV Contactless Symbol for details.
Cryptogram	A value resulting from a combination of specific key data objects 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.

Term	Definition
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 18033-3 as a component of TDEA).
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."
Dynamic Currency Conversion (DCC)	Dynamic Currency Conversion (DCC) is one of: • 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. • A Manual Cash transaction in which the transaction currency is different to the currency disbursed. DCC is not a Visa service, but merchants and ATMs may offer it through their acquiring bank.
Dynamic Data Authentication (DDA)	A type of Offline Data Authentication in which the device validates a cryptographic value generated by the card during the transaction. This validation helps to ensure that the card data has not been copied (skimmed) from a different card and that the card is not counterfeit.
Dynamic Data Authentication Data Object List (DDOL)	The card-originated data element that is used for constructing the INTERNAL AUTHENTICATE command.
EMV Contactless Specifications for Payment Systems ("*EMV Contactless Specifications*")	Technical specifications developed by EMVCo outlining the interaction between contactless chip cards (and other form factors such as mobile phones) and devices to ensure interoperability for payment systems.
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)	The organization of payment systems that manages, maintains and enhances the *EMV Chip Specifications*, *EMV Contactless Specifications* and others. For more information, see www.emvco.com

Term	Definition
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.
Incremental Authorization	Where the final amount will exceed or is likely to exceed the amount of the pre-authorization, one or more further incremental authorizations may be obtained. The incremental authorization(s) will be for the difference between the original pre-authorization and the actual or estimated final amount.
Integrated Circuit Card (ICC)	See Chip Card.
Interface Module (IFM)	The hardware or chip reader developed to the *EMV Chip Specifications* that provides physical communication with the chip card.
International Organization of Standardization (ISO)	The specialized international agency that establishes and publishes international technical standards.
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.

Term	Definition
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.
Level 3 Testing	A mandatory phase of terminal testing that helps ensure that chip terminals (POS, mobile Point of Sale, ATM, Transit, Tap to Phone, Fleet, etc.) are correctly integrated into the Visa payment acceptance environment and do not unduly contribute to interoperability problems.
Magnetic Stripe	The magnetic stripe on a card that is encoded with the necessary information to complete a transaction.
Magnetic Stripe Device	A device that reads the magnetic stripe on a card.
Merchandise Return/Refund	An online authorization message and associated clearing message to return goods/services for a refund. The transaction results in a credit to the cardholder's account for the amount of the returned goods/services. Both full and partial refunds of the original transaction may be performed.
N/A	Not applicable
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.

Term	Definition
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.
Online Authorization	A method of requesting an authorization through a data communications network other than voice to an issuer, an authorizing processor, or stand-in processing.
Online Card Authentication	Validation of the card by the issuer to protect against data manipulation and data copying. See also Authorization Request Cryptogram (ARQC).
Online Issuer Authentication	Validation of the issuer by the card to ensure the integrity of the issuer. Also known as Issuer Authentication and Host Authentication. See also Authorization Response Cryptogram (ARPC).
Online PIN	A process used to verify the cardholder's identity by sending an encrypted PIN to the issuer or the issuer's agent for validation in an authorization request.
Online-Only Device	A device that requires that all transactions be sent online for authorization.
Partial Name Selection	The Application Selection process where the device AID uses only a partial name.
Payment Card Industry Security Standards Council (PCI SSC)	A consortium of payment card industry representatives, which became formalized as the PCI Security Standards Council.
Payment Systems Environment (PSE)	The data object 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 for contact transactions.
PCI Data Security Standard (PCI DSS)	The PCI DSS is a widely accepted set of policies and procedures intended to optimize the security of payment card transactions and protect cardholders against misuse of their personal information.
PCI Software Security Framework (PCI-SSF)	Provides vendors with security standards for developing and maintaining payment software so that it protects payment transactions and data, minimizes vulnerabilities, and defends against attacks..

Term	Definition
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).
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).
Processing Prior to Enabling the Contactless Interface	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.
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 mobile phone, and also to control the data exchange with the consumer device.
Proximity Payments Systems Environment (PPSE)	A card application that provides a list of supported Application Identifiers (AIDs), Application Labels, Application Priority Indicators and other information for payment applications on the card 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 made available to users.
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.

Term	Definition
Quick Chip for Contact	Quick Chip for Contact 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 globally deployed solution for contactless card acceptance. qVSDC is a contactless EMV transaction which optimizes commands where possible to save time and allow cryptographic operations to be performed up front as opposed to later when the card is more likely to be leaving the field.
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). The *Visa Rules* require that a contactless acceptance device must not limit the transaction amount of a contactless transaction. Therefore, if the contactless reader has this limit, it must be 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).
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 cashback 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).

Term	Definition
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.
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. TDEA and AES are two of the best known symmetric encryption algorithms.
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.
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 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 TDEA or AES 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.

Term	Definition
Triple Data Encryption Algorithm (TDEA)	TDEA (also referred to as Triple Data Encryption Standard/TDES) as defined in *ISO/IEC 18033 Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers*. It is the data encryption 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.
Visa Electron	A Visa payment product aimed at cardholders that are developing banking relationships. Visa Electron cards have greater usage restrictions and transactions are always processed online.
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 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 (qVSDC) 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.