Transaction Acceptance Device Guide (TADG)

Version 3.1
November 2016

Visa Public

Important Information

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

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

Contents

Tables

Figures

Transaction Acceptance Device Guide Overview

The increasingly global nature of the payment card industry is creating new requirements to ensure the interoperability of cards and devices. Interoperability is the cornerstone of Visa brand acceptance and a driving force behind Visa's long-standing commitment to work with financial institutions, merchants, vendors, and third-party organizations to create the global infrastructure needed to meet these challenges.

The *Transaction Acceptance Device Guide* (TADG) is intended to provide vendors, merchants, acceptance device deployers, and acquirers or their agents with an overview of the requirements for devices that accept Visa magnetic stripe, contact chip, and contactless transactions. Transaction acceptance devices can be operated directly by an acquirer or under the terms of a merchant or acquirer agent agreement.

This document assists vendors in designing devices that meet industry and Visa specific standards.

Audience

This guide is intended for:

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

This document is available to the public on the Visa website (www.visa.com/tadg).

Scope

The focus throughout this document is on device requirements for vendors, merchants, and acquirers to help ensure compliance with the Visa requirements for card-present transactions, along with best practices for implementation. This document assumes a basic knowledge of magnetic-stripe processing, the EMV contact chip specifications, the EMV contactless chip specification, and the *Visa Contactless Payment Specification*. The recommendations for contact chip and contactless chip processing should be read in conjunction with the appropriate specifications.

This document refers to requirements that apply in most countries. Specific countries, however, may have local laws or Visa requirements that apply to their environment. Devices deployed must adhere to all applicable global and local requirements.

This document contains references to the *Visa Core Rules and Visa Product and Service Rules*. It does not, however, replicate all the device requirements from the *Visa Core Rules and Visa Product and Service Rules*.

This document does not address:

- Card-not-present transactions
- Acquirer roles and responsibilities
- Acquirer-to-VisaNet messaging (except in a few instances for clarification)
- Device-to-acquirer messaging (which is outside Visa's scope)
- Functionality of handheld electronic devices used in mobile payment acceptance solutions (the card reader/PIN pad device is in scope but the phone or tablet it is connected to or embedded within is not in scope)

This document applies to devices operating under a merchant agreement, such as point-of-service (POS) equipment, or under an acquiring contract, such as an Automated Teller Machine (ATM). Portions of this document may also be useful to developers of issuer-operated or cardholder-owned devices.

Compliance Documents and Devices

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

- The Visa rules and regulations consisting of:
  - *Visa Core Rules and Visa Product and Service Rules* (available at www.visa.com)
  - *V PAY Operating Regulations* (for countries in the Europe Region)
- *Payment Technology Standards Manual* (see Appendix A and Appendix B for the Visa standards for Tracks 1 and 2, respectively)
- *Transaction Acceptance Device Requirements (TADR)*
- *Global ATM Member Guide*

Note: Additional reference documentation is provided in Appendix I: Reference Materials.

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

- **EMV**—Devices accepting Visa EMV-compliant contact chip cards must comply with the *EMV Integrated Circuit Card Specifications for Payment Systems* (the EMV specifications), including any specification updates released by EMVCo, which are maintained by EMVCo at www.emvco.com.
- **PIN**—Devices accepting Personal Identification Numbers (PINs) must comply with the *Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements* and the PCI PIN Security Requirements on www.pcisecuritystandards.org.
- **Visa payWave**—Visa payWave readers must comply with the *EMV Contactless Specifications* including Book C–3 or the *Visa Contactless Payment Specification* (VCPS) including all published updates.
- **Europe Region**—Device vendors servicing the Europe Region should also refer to the *Visa Europe Contactless Terminal Requirements and Implementation Guide* which can be obtained by contacting the Europe Region at chipven@visa.com.

Acquirers may download Visa chip documentation from the Chip and Contactless Specifications site on Visa Online. Acquirers should contact their local representative for information on enrolling and gaining access. Licensed vendors may download licensed Visa materials from the Visa Technology Partner site at https://technologypartner.visa.com.

Best Practice Reference Materials

The following documents provide best practices for various acceptance environments:

- **Visa Easy Payment Service (VEPS)**—Best practices relating to VEPS can be found in the *Visa Easy Payment Service—Acquirer Program Guide* which can be obtained from a Visa representative.
- **Retail Petroleum Merchants**—Best practices relating to payment acceptance for retail petroleum merchants can be found in the *Visa Payment Acceptance Best Practices for Retail Petroleum Merchants* which can be obtained from a Visa representative.
- **User Interface for Contactless Devices**—Best practices relating to the user interface for contactless acceptance devices can be found in the *EMV Contactless Specifications, Book A: Architecture and General Requirements*, which can be obtained from the EMV website at www.emvco.com.
- **Contactless Indicator and Contactless Symbol—**Guidelines for using the indicator and symbol can be obtained from the EMV website at www.emvco.com.
- **Prepaid Programs Using Self-Service Kiosks**—Risk management best practices for prepaid programs that utilize a self-service kiosk can be found in the *Prepaid Product Risk Management Best Practices* which can be obtained from a Visa representative.

In addition to complying with these documents, countries can customize their programs beyond these minimum requirements through adoption of the optional functions or through proprietary processing. Proprietary processing, however, must not interfere with global interoperability.

Terminology

The following terms are used in this guide:

Table 1: Terminology

Term	Definition
Acquirer	Includes acquirers and their agents, such as an acquirer processor.
Card	Any Visa-approved card (magnetic stripe, chip, and/or contactless) that can be used to initiate a Visa transaction. The term may apply to other form factors (such as mobile devices) which are compliant with Visa's rules and requirements and which may be used to initiate Visa transactions.
Cardholder	An individual who is issued and authorized to use either or both a: • Card • Virtual Account
Device	A transaction acceptance device.
EMV Specifications	*EMV Integrated Circuit Card Specifications for Payment Systems* encompassing all four books which make the contact chip specifications and the *EMV Contactless Specifications for Payment Systems* encompassing all seven books which make up the contactless specification, plus any updates published in specification bulletins on the EMVCo website.
Reader, Contactless Reader	The merchant device communicating with the card. There are two scenarios where a reader could typically be used for a contactless transaction: • Reader (also called a dongle or Proximity Coupling Device, PCD) separated from, but communicating with, a POS device. • Reader integrated into a POS device. The word *reader* in this guide covers both scenarios unless explicitly stated otherwise. It is not intended to imply in which physical component (the reader or the POS device) a specific action is performed.
Terminal	See Device.
Visa Contactless Payment Specification (VCPS)	Visa's specification for contactless payment.
Visa rules and regulations	*Visa Core Rules and Visa Product and Service Rules* (formerly referred to as the *Visa International Operating Regulations*)

Additional terms and definitions are provided in Appendix J: Acronyms and Glossary at the end of this guide.

Summary of Changes Since Version 3.0

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

Table 2: Summary of Changes

Chapter/ Appendix	Summary of Changes
General	References to 'Visa Europe' changed to 'Europe Region.'
Section 3.2.2: Fallback Acceptance of Chip Read Failures, bullet #5	Information related to the Terminal Entry Capability clarified.
Section 4.1: MSD Section 4.7: MSD Transaction Flow	Information clarified that MSD routing flexibility for U.S. Covered Visa Debit cards can be achieved using BIN routing logic.
Section 6.6.1: Keyboard Layout	Section deleted; information out-of-date.
Section 9.7: ADVT Section 9.7.2 ADVT and Expired EMV Approvals	Information related to ADVT usage requirements/recommendations updated.
Section 9.8: qVSDC Device Module	Section deleted; qVSDC Device Module (DM) is no longer applicable.
Appendix F: Visa U.S. Common Debit AID	Appendix F updated to clarify implementation options related to the adoption of EMV chip technology in the U.S. Minor changes to other areas of the document to align with the Appendix F updates: • Section 3.3: Application Selection • Section 3.3.1: Application Identifiers • Section 3.3.5: Cardholder Selection • Section 3.3.7: Application Label and Application Preferred Name • Section 4.6.2: Application Selection

1. Transaction Acceptance Environments

This chapter describes the three types of transaction acceptance devices referred to in this document:

- Attended POS Devices
- Unattended Cardholder Activated Terminals (UCATs)[1]
- Automated Teller Machines (ATMs)

This chapter also references other device reader peripherals and describes various authorization processing methods used in different environments.

1.1 Attended POS Devices

Attended POS devices can be described in three categories:

- Integrated POS Systems
- Standalone POS Devices
- Multi-lane POS Devices

Note: While these devices may support a variety of functions, the requirements in this document focus on payment functionality.

1.1.1 Integrated POS Systems

An integrated POS is a system that processes payment card transactions in addition to a wide array of other functions. Other functionality may include:

- Product code scanning, product lookup, and sales tax calculation
- Inventory management and item tracking
- Customer preference, coupon, and frequent shopping programs
- Security and staff tracking
- Accounting

Integrated POS systems can be as complicated as a state-of-the-art retail workstation or as simple as a basic till with an integrated-card reader.

[1] These devices are referred to as Unattended Acceptance Terminals (UATs) in the Europe Region.

1.1.2 Standalone POS Devices

Compared to integrated POS systems, a standalone POS device serves the primary purpose of authorizing and clearing payment card transactions. Other names for standalone devices include electronic POS devices (although this also refers to integrated systems) or electronic data capture devices.

A standalone POS device is usually not connected to a merchant's electronic cash register; rather, it connects directly to a host processor. For slightly larger merchants, the standalone device may be added to a cash register as a plug-in or stand-beside device.

1.1.3 Multi-lane POS Devices

The term multi-lane is often used to describe the multiple checkout lanes found in large mass merchandise or grocery stores. A multi-lane configuration consists of multiple payment devices tied to one or more controllers. The controller provides messaging between the store and the host processor for services (for example: authorization, reporting, or inventory management). Each checkout location generally supports all the functions required for transacting business, including card acceptance.

The three most common types of multi-lane configurations are:

- **Stand-Beside or Physically-Separated Systems**—For these systems, the card payment function is separate from in-store operations.
- **Semi-Integrated or Logically-Integrated Systems**—For the most common semi-integrated configuration, the transaction acceptance device connects directly to the integrated POS device and runs on a local area network linked to the payment controller.
- **Fully-Integrated or Physically-Integrated Systems**—For this configuration, the store's system controls all the components, and the integrated POS platform physically incorporates the transaction acceptance device.

1.1.4 Shared Display and Separate Display Devices

Attended devices may have a shared display or a separate display:

- **Shared**—Devices with a shared display only have a single display that is shared by the merchant and the customer during the transaction process.
- **Separate**—Devices with a separate display have a dedicated display for the merchant and one for the customer. These typically comprise a fixed enclosure for the merchant terminal and a tethered PIN pad with a dedicated display for the customer.

Which device is used at a merchant is dependent on the device itself and the merchant environment.

In general and unless specifically stated, all requirements and best practices apply to both types of devices. There are specific requirements related to Application Selection which vary depending on whether the device has a shared or a separate display. These are covered in more details in Chapter 3: Contact Chip Acceptance.

1.2 Unattended Cardholder Activated Terminals

In this document, the term Unattended Cardholder Activated Terminal (UCAT)[2] refers to an acceptance device managed by a merchant that dispenses 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, self-service vending units, and self-service payment devices in parking garages or at parking meters.

Devices that support cash dispensing and provide goods and services must comply with the Visa rules and regulations appropriate to the transaction:

- When dispensing cash, the device is considered an ATM and, therefore, must adhere to the Visa rules and regulations for ATMs.
- When dispensing goods or services, the device is considered a UCAT and must adhere to the Visa rules and regulations for unattended purchases.

Although unattended devices (e.g., ATMs, UCATs) may dispense goods and services as well as cash, transactions involving a purchase with cash back are not allowed. In other words, an unattended device may dispense either cash or goods and services in a single transaction but not both.

Attended Cardholder Activated Terminals,[3] such as self-checkout terminals in supermarkets, are not considered UCATs and therefore are not required to meet UCAT requirements.

Note: Information on UCATs that dispense scrip is not addressed because the Visa rules and regulations prohibit Visa card products from being used for scrip transactions. (Scrip is a two-part paper receipt redeemable for goods, services, or cash.)

1.3 Automated Teller Machines

Automated Teller Machines (ATMs), also known as Automated Banking Machines (ABMs) or cash machines, are unattended devices that dispense cash and accept Online PINs. These devices may be simple, limited-capability cash dispensers or advanced-function ATMs with color screen graphics, sophisticated applications, and a range of business functions.

[2] Referred to as Unattended Acceptance Terminals (UATs) in the Europe Region.
[3] Referred to as Semi-Attended Cardholder Activated Terminals in the Europe Region.

ATMs may support additional financial-related functions, such as balance inquiries, account transfers, and activating or topping up prepaid cards. In certain countries, they may also provide customer PIN change facilities.

ATMs can also be used to provide goods or services (such as mobile top-up), but in these scenarios they operate according to the rules for UCATs rather than ATMs.

1.4 Self-Service Card Dispensing Kiosks

Self-service card dispensing kiosks allow consumers the convenience to purchase and/or reload a Visa prepaid card. Cards dispensed via kiosks are restricted to limited use, non-personalized cards (for example, gift cards or temporary general purpose cards). Other functions of a kiosk could include the ability to check a card balance or pay bills. The purchase of Visa cards at a kiosk may be completed with various forms of tender: cash, credit, or debit cards. Visa prepaid cards sold at a kiosk will be expected to meet all existing Visa requirements including the following:

- Visa rules and regulations including but not limited to Agent Registration, Risk Management, General Card Acceptance, and Unattended Acceptance Terminal requirements
- Visa Prepaid Products Program Guidelines
- PCI PIN Security Requirements*
- PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*
- Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support, and Fulfillment Card Vendors
- Payment Card Industry Data Security Standards (PCI DSS) including the Payment Application Data Security Standard (PA—DSS)

* Required for PIN accepting kiosks—for more information go to www.pcisecuritystandards.org.

All kiosk implementations must be supported by a comprehensive maintenance plan for upkeep of the devices. The plan must include, at a minimum, the following:

- Inventory management and restocking of the machine to ensure adequate stock
- Troubleshooting of the device if not operating properly (i.e., machine is out of order, not dispensing cards, not taking bills or payment, not issuing a receipt, etc.)
- Available contact information for consumer inquiries
- Retailer training for consumer inquiries

For additional risk management best practices for prepaid programs that will utilize a self-service kiosk, refer to the *Prepaid Product Risk Management Best Practices*.

1.5 Card Readers

Card readers are available in a number of form factors. A reader may support multiple technologies (for example, magnetic stripe, contact, and contactless), be dedicated to one technology, and/or be extended to support a new acceptance technology. The basic configurations are:

- **Fully Integrated Reader**—Delivered by vendors as part of a POS system.
- **Fully Integrated Reader Module**—Module plugged into an existing reader to extend functionality (often to support new technology).
- **Peripheral Reader**—Plugs into POS system; usually contains all functionality needed to support an acceptance technology.

In some cases, reader functionality may be integrated into the PIN pad.

1.5.1 Contactless Readers

There are specific requirements for contactless readers. Refer to Chapter 4 for more information. There are two scenarios in which a reader is typically used for a contactless transaction:

- Reader (also called a dongle or Proximity Coupling Device (PCD)) separated from, but communicating with, an acceptance device.
- Reader integrated into an acceptance device.

The term contactless reader covers both scenarios unless explicitly stated otherwise. It is not intended to imply in which physical component (the reader or the POS device) a specific action is performed.

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

1.6 Mobile Payment Acceptance Solutions

Mobile Payment Acceptance solutions (also referred to as "mobile POS" or "mPOS") make use of an electronic handheld device (e.g., smart or feature phone, tablet, or PDA) that is not solely dedicated to payment acceptance and that has the ability to communicate via wireless across open networks.

The solution may include a hardware attachment for the purpose of reading card data from a card and/or PIN entry. Solutions that do not electronically read account data may not be acceptable in all countries or may be subject to restrictions. Solution providers and vendors must review local Visa rules and regulations prior to providing mobile payment acceptance solutions to merchants.

Vendors, merchants, and acquirers involved in the development or deployment of these solutions must follow all Visa rules and requirements for magnetic stripe, chip, and contactless acceptance (where supported). Visa also recommends that solution providers maintain an EMV roadmap.

There may be additional PCI documentation that defines best practices, guidelines, and/or security standards for mobile payment acceptance solutions. For more information, refer to PCI website at www.pcisecuritystandards.org. Acquirers should also review the security best practices related to mobile payment acceptance solutions in Chapter 5.

1.7 Processing Options and Host or Device Capture

Transactions may be processed using batch clearing or real-time processing. The method used is dependent 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.

Note: Visa documentation often refers to batch clearing and real-time processing as VIP Authorization and VIP Full Service, respectively.

The following provides an overview of batch clearing and real-time processing:

- **Batch Clearing**—Batch clearing (sometimes referred to as batch processing or dual-message processing) involves the exchange of data twice. In dual-message processing, the authorization occurs at the time of the purchase or cash disbursement transaction using one message, and the transaction is cleared later using another message. These 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.
- **Real-Time Processing**—Real-time processing involves all transaction data flowing online. Where the final amount is known at the time of authorization, the same online message also provides the issuer with all the information required to clear the transaction and post it to the cardholder's account. Real-time processing is often referred to as single-message processing. Real-time processing merchants, particularly those in travel and entertainment segments, may use an authorization message (0100) followed by a sales 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 batch clearing and real-time processing. For more information, refer to Section 3.15.2: Fuel/Petrol Dispensing.

With device-capture systems, the device combines the authorization response with the data from the authorization request to create the clearing message. In an acquirer host-capture system, the host retains a copy of the authorization coming from the device before sending the request for authorization and uses the data along with 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, all transactions appear to be single message because the acquirer is responsible for generating the clearing message.

Although single-message systems typically use full financial messages, they may also use an authorization followed by a clearing advice.

For chip transactions that are authorized offline or magnetic-stripe transactions that are under the device floor limit, only a clearing message—whether single- or dual-message, device- or host-capture—is transmitted.

1.8 Deferred Authorization

Deferred Authorization occurs when an online authorization is performed after the card is no longer available. The time delay may be brief, such as for a temporary communications failure or where the merchant simply wishes to speed processing. The time delay may be extended, as when a ferry is out of range of shore, for in-flight sales, or when the device does not have online capability (for example, unattended kiosks where the transactions are offloaded nightly to a server and submitted in batches). Merchants performing Deferred Authorization should complete authorizations within 24 hours of the transaction.

This type of transaction may be referred to as "store-and-forward", but that term can extend to situations where third parties retain and later relay transactions. The term "Deferred Authorization," therefore, is used in this document to describe this type of transaction.

Note: The processing of Deferred Authorizations originating from contact chip cards has some different considerations from that of magnetic stripe. Section 3.12.2: Deferred Authorization outlines the requirements relating to contact chip cards.

1.9 Acquirer Stand-In

Transactions above the Visa floor limit or chip transactions where the chip card requests an online authorization (by returning an ARQC) are normally sent online to the issuer for authorization. In some environments, however, acquirers may choose to stand in for authorizations in their host system or in the device. The device displays an appropriate message to indicate that the transaction is being completed and that the goods or services are being provided to the cardholder.

Acquirer stand-in (also called authorization truncation) may be done for various business reasons. However, the acquirer is liable for these transactions in the event that they are charged back for no authorization. Acquirer stand-in is not allowed in some countries, such as the U.S. Deferred Authorization is a preferred approach to these situations, particularly in a chip environment.

Refer to Section 3.12.3: Acquirer Stand-In for further details regarding Acquirer Stand-In in a chip environment.

1.10 Partial Authorization

Partial Authorizations occur when the issuer returns an authorization approval 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.

Where devices support Partial Authorizations, the device must be able to reset the amount of the purchase to the amount approved by the issuer.

The device or acquirer must submit the authorized amount from the Partial Authorization response as the Authorized Amount in the clearing transaction. The actual amount for the goods or services dispensed after receiving the Partial Authorization is submitted as the settlement amount in the Source Amount field in the clearing transaction.

If the approved amount is not fully dispensed as goods or services, an authorization reversal must be issued for the remaining amount. Alternatively, if the transaction is cleared for an amount that is greater than the authorized amount in the Partial Authorization, the issuer has a right to chargeback for the amount exceeding the Partial Authorization amount.

2. General Acceptance

This section provides an overview of the general transaction acceptance device requirements and best practices that apply to magnetic stripe, contact chip, and contactless devices.

2.1 Primary Account Number Recognition and Processing

A device accepting Visa and Visa Electron cards must accept all valid Primary Account Numbers (PANs). An ATM 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.

Modulus-10 checking is only recommended for below floor limit, magnetic-stripe transactions.[4]

In some countries, merchants may have installed account-number-verifying POS devices to aid in detecting counterfeit cards. These devices read the PAN from the magnetic stripe and compare the last four digits of the PAN to the key-entered last four digits of the embossed or printed PAN. This test is **not** recommended for devices that accept contact or contactless chip cards because chip cards may contain multiple payment applications (each with a unique PAN), of which only one PAN will appear on the front of the card and therefore, a valid multi-application card could erroneously fail this test.

2.2 Expiration Date

Because Visa does not impose a global upper limit for expiration dates on Visa cards, POS devices should not validate whether expiration dates are too far out in the future.[5] This type of validation can lead to erroneous declines.

ATMs 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.

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.

[4] Acquirers and merchants should be aware that 19-digit debit cards may not pass Modulus-10 checking.
[5] This does not preclude chip devices from performing expiration date checking per standard EMV/VIS processing.

2.3 Account Selection

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

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.

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.

Note: Account selection as described in this section is different to the EMV Application Selection process which is covered in more detail in Chapter 3: Contact Chip Acceptance.

2.4 Multiple Languages

Depending on the geographic location, devices may need to communicate in multiple languages to help merchants improve customer service and profitability. Support for multiple languages and characters on the device's display for PIN entry or cardholder selection of the application is recommended for all devices.

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 transaction messages, vendors should follow a few basic principles. These principles help guide networks and vendors to maintain clarity in their device messages through both language translation and message-length constraints.

Basic principles related to device messages include:

- **Instructive Messages**—The message displayed must clearly instruct the merchant or cardholder on what action to take.
- **Clear Responses**—Where the message is based on an issuer response, the message should clearly communicate the meaning of the response.
- **Amount/Currency and PIN Entry**—The transaction currency as well as the amount should be displayed to the customer prior to PIN entry (if applicable). The cardholder should be prompted to confirm the transaction currency and amount; PIN entry is an acceptable method of confirmation. If PIN entry is requested before the transaction amount is known for throughput reasons, an explicit amount confirmation message should be displayed to the cardholder once the amount is known.
- **Transaction Status**—The message displayed must clearly indicate the status of the transaction. Transaction status is defined by one of five basic conditions or events:
  - The transaction is approved
  - The transaction is declined
  - The transaction is referred
  - The requested service is not available
  - The transaction experienced an error

Once the status of the transaction is determined, the device must be able to communicate the next action. Clear instructions are especially important when an error occurs and the transaction is terminated. 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.

The following table describes the recommended terminal display prompts in English. These, or the local language equivalents, may be used.

Table 2–1: Transaction Scenarios and Device Messages

Scenario	Transaction Scenarios and Device Messages
Device prompts for merchant or cardholder to enter amount	ENTER AMOUNT
Device prompts for cardholder to enter PIN	ENTER PIN
Device prompts for cardholder to enter PIN or cancel PIN entry **Note:** *EMV PIN Entry Bypass is not supported in all environments. Refer to Section 6.3.4: EMV PIN Entry Bypass for more information.*	ENTER PIN OR CANCEL
Incorrect PIN entered	INCORRECT PIN, RE-ENTER PIN

Scenario	Transaction Scenarios and Device Messages
PIN try limit exceeded during current transaction	INCORRECT PIN (Transaction proceeds to conclusion)
Inoperable PIN pad	ERROR; PIN PAD INOPERATIVE
Modulus-10 check fails for key-entered transaction **Note:** *Should only be performed on below-floor limit magnetic-stripe transactions.*	ENTER AGAIN
Merchant or cardholder removes card before the transaction is completed	CARD REMOVED TOO SOON; TRY AGAIN
Chip transaction is complete and card may be safely removed	TRANSACTION COMPLETE; REMOVE CARD
Transaction is declined	DECLINED
Transaction is approved	APPROVED
Transaction is referred	CALL BANK FOR AUTHORIZATION
Device temporarily unable to go online (zero floor limit environment or offline chip approval not supported)	UNABLE TO AUTHORIZE. PLEASE TRY LATER/CONTACT YOUR CALL CENTER
Network unavailable to authorize a transaction above the floor limit (for example, if issuer is unavailable and Visa stand-in processing is not available)	SERVICE NOT SUPPORTED
Chip read problem at a device that supports Fallback	CHIP ERROR; USE MAG STRIPE
EMV chip card inserted into non-EMV chip device (such as a domestic purse application reader)	UNABLE TO PROCESS; USE MAG STRIPE
Non-EMV chip card inserted into EMV chip device	USE MAG STRIPE
Device with chip functionality not activated and with separate readers for chip and magnetic stripe	CHIP ERROR; USE MAG STRIPE
Device not able to accept chip card because of no match on the Application Identifier (AID)	CARD TYPE NOT SUPPORTED; USE MAG STRIPE
Device supports cardholder selection but transaction cannot be performed with selected application	TRY AGAIN (Application should be removed from selection process before new list presented to cardholder)
Device prompts cardholder to select application	SELECT APPLICATION TO BE USED, or USE xxxxxxxx? YES/NO? (where xxxxxxxx is the Application Preferred Name or Application Label)
Device does not support cardholder confirmation but all mutually supported chip applications require cardholder confirmation	CARD TYPE NOT SUPPORTED; USE MAG STRIPE

Note: These recommendations assume a small display. Developers for devices with larger displays should take advantage of the ability to provide more information, using these recommendations as a guideline.

There are also specific requirements relating to the user interface of devices for use with multi-application chip cards. These are outlined in more detail in Chapter 4: Contactless Acceptance and are in addition to the messages noted in Table 2–1.

For further information regarding the messaging and best practices relating to the user interface for devices accepting contactless transactions, acquirers and vendors should refer to the *EMV Contactless Specifications for Payment Systems, Book A* which can be obtained from the EMVCo website.

Certain Visa regions also have specific requirements relating to what is displayed to the cardholder for a contactless transaction and specific requirements for terminal displays. Given the faster nature of a contactless transaction, other forms of messaging such as LED indicators and sound cues are used.

2.6 Accessibility Requirements

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

2.7 Transaction Receipts

Except for certain transactions, such as qualifying VEPS transactions, merchants must be able to provide the cardholder with a written or printed receipt at the completion of the transaction. For more information on electronic receipts, refer to the next section.

The Visa rules and regulations specify receipt requirements including those for manual receipts, electronic receipts, travel and entertainment, dynamic currency conversion, and aggregated transactions. There are also specific requirements relating to transactions that qualify under VEPS. Refer to the Visa rules and regulations for more information.

In addition to the general information required on receipts per the Visa rules and regulations, chip card receipts have the following requirements:

- **Application Name**—It is strongly recommended to print the Application Preferred Name (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, refer to Section 3.3.7: Application Label and Application Preferred Name.

[6] Some cards will be personalized with the Application Label only.

- **Application Identifier (AID)**—The AID is required on the receipt per EMV. For more information on the AID, refer to Section 3.3.1: Application Identifiers.

On chip cards, when the PAN 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.

Although most authorizations occur electronically, occasionally merchants need to authorize transactions over the telephone as a result of issuer referrals, network problems, or system outages. Devices that print cardholder transaction receipts should also provide the capability to enter an authorization code (for example, via a keypad). These devices should also include the authorization code in the electronic transaction capture file for later batch clearing.

2.8 Electronic Receipts

Merchants have the option to 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:

- Merchants must be able to offer a paper receipt and must provide a paper receipt, if requested by the cardholder.
- The account number on the electronic receipt must be truncated to the last 4 digits.
- The electronic receipt may be contained in an email message, SMS text message, or available via a link provided in the message.
- The electronic receipt must be delivered in static format that is not easily manipulated.
- The electronic receipt must be sent to the cardholder upon completion of the transaction.
- 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.
- 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 messages does not affect existing requirements for cardholder verification such as the need for signature.

For more information on electronic receipts, refer to the Visa rules and regulations.

2.9 Consumer Data on Receipts and Displays

The Visa rules and regulations require that at least four digits of the PAN on the cardholder transaction receipt must be disguised or suppressed. To support this requirement, it is strongly recommended that all but the last four digits of the PAN on the cardholder transaction receipt be suppressed on receipts and displays.

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

Certain countries, such as the U.S., may also have legal restrictions on PAN and expiration date printing on cardholder transaction receipts and displays. For U.S.-based merchants, POS devices must only provide the last four digits of the PAN and must not provide the expiration date on cardholder transaction receipts.

2.10 Transaction Cancellation

Devices should enable a cardholder or merchant to cancel a transaction in progress at any time. The device generates a receipt for a canceled transaction when required by local law.

2.11 Card Data in Online Message

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 data in the magnetic-stripe field in the online authorization message based on the individual data elements in the magnetic stripe or chip. The device should also ensure that if a transaction is processed as magnetic stripe, the track data used in the transaction is read from the magnetic stripe and correspondingly, if a transaction is processed as chip, the track data used must be read from the chip.

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.

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

2.12 Cash Back Identification and Processing

Where the Visa rules and regulations and local laws in a country allow cash back[7] with a purchase, the cash back amount must be uniquely identified in the authorization and clearing messages from the total transaction amount.

Authorization messages contain:

- Total transaction amount (purchase plus cash back) in Amount, Transaction (V.I.P. Field 4).
- Cash back amount in Other Amounts (V.I.P. Field 61.1).

All cash back transactions must be online authorized.

Devices supporting cash back must be configured to meet all of Visa's cash back requirements including local requirements (where applicable).

Devices must be able to:

- Enable cash back functionality (for chip devices, this includes switching on the cash back functionality setting in the EMV kernel)
- Capture cash back amount and populate it in the authorization message

The device must be able to give the merchant the capability to key in purchase and cash back amounts separately (the authorization amount is for the total amount which is the purchase amount plus the cash back amount). An end-of-day batch from terminals must identify cash back amounts so merchants can reconcile with their cash drawers.

Devices must be able to handle special conditions relating to cash back such as:

- A response from the issuer that the cash back service is not available to the cardholder.
- A response that the cash back amount is more than the maximum cash back amount agreed for the country. (In this case, the merchant could retry the transaction for a smaller cash back amount or for the purchase amount only.)
- A response that the cash back amount is equal to the total transaction amount. (This is not allowed.)

Certain special conditions will require different actions by the merchant. Merchants may need to work with their acquirers to determine appropriate point-of-service procedures.

There are specific requirements relating to how a chip transaction which includes a cash back component is processed. Refer to Section 3.11.4: Cash Back for details.

[7] In certain countries, the term "cashback," "cash-back," or "cash-out" may be used.

2.13 Transaction Speed

Rapid authorization enhances the cardholder experience while providing reduced transaction and queue times for the merchant. Online authorizations can be optimized through implementation of fast communication technologies (such as always-on or broadband). The benefits of customer satisfaction and higher throughput can offset additional communication costs in many cases. For more information, refer to Appendix C: Device Performance for EMV Transactions.

Speed requirements for contactless transactions are more stringent due to the convenience and speed factor associated with them. The Visa requirement is for the transaction time not to exceed 500 milliseconds based upon the interaction between the card and the reader, beginning at the first card response during Discovery Processing and concluding at Card Read Complete. This excludes any additional time required for an online authorization or processing for Offline Data Authentication. For more information, refer to Chapter 4: Contactless Acceptance.

2.14 Unattended Cardholder Activated Transactions

Unattended Cardholder Activated Terminals (UCATs)[8] must be able to read the card data electronically and provide a transaction receipt. A UCAT must inform the cardholder that a receipt is available upon request, if it is not provided automatically.

The Visa rules and regulations define a transaction performed at a UCAT as falling into one of three categories:

- **Below-Floor Limit With No CVM (Magnetic-Stripe Only)**—Transactions are below the floor limit, the transaction is not authorized, and cardholder verification is not performed.

  Note: These transactions must not be initiated as magnetic-stripe transactions from either Visa or Visa Electron cards with a Service Code containing a 2 in the second position (indicating that online authorization is required). This type of transaction is allowed only in some countries and only for a very limited number of merchant categories.
- **Authorized With No CVM**—Transactions are authorized (offline or online) and cardholder verification is not performed.
- **Authorized With CVM**—Transactions are authorized (offline or online) and PIN entry[9] is performed.

[8] Referred to as Unattended Acceptance Terminals (UATs) in the Europe Region.
[9] Visa is currently defining additional CVM methodologies.

A UCAT may support all three categories provided that the device adheres to the cardholder verification requirements appropriate to each transaction type.

Note: At a minimum, a UCAT must support "Authorized with no CVM" at all online-capable chip contact and contactless terminals.

For more information, refer to the Visa rules and regulations for the location of the merchant.

2.15 Automated Teller Machines

This section provides an overview of ATM transactions:

- **Online Authorizations**—All ATM transactions must be transmitted electronically to the issuer or issuer's agent. Transactions must not be approved offline but may be declined offline based on processing restrictions from a contact chip card.
- **Online PIN**—The cardholder must be verified via an Online PIN at the ATM (this is the only Cardholder Verification Method allowed in this environment).
- **Multiple Languages**—ATMs should be able to display messages in multiple languages. The messages should indicate the type of currency dispensed.
- **Cash Disbursements**—An ATM cash disbursement must be processed as a Visa transaction when either a Visa or Visa Electron card is used or as a Plus transaction when either a Plus, Visa, or Visa Electron card is used at a Plus-only (non-Visa) ATM.
- **Canceled Transactions**—A transaction must be canceled if network problems or system outages occur.
- **Reversals**—If an authorization request has been sent and cash was not disbursed, a reversal must be sent.

2.16 Dynamic Currency Conversion

Dynamic Currency Conversion (DCC) is a merchant-offered currency conversion service that is provided by acquirers or DCC service providers (agents) and is not a Visa service. It is the conversion of the purchase price of goods or services from the currency of the country in which the transaction is taking place to another currency as agreed to by the cardholder and merchant. That currency becomes the transaction currency, regardless of the merchant's local currency.

DCC is permitted on Visa transactions in all Visa Inc. regions, subject to the DCC rules in the *Visa Core Rules and Visa Product and Service Rules* and the DCC Compliance Program requirements included in the *International Transactions Guide*. DCC is permitted for POS transactions in both card present and card absent environments, and is not allowed at ATMs in Visa regions (except the Europe Region) in accordance with the *Visa Core Rules and Visa Product and Service Rules*. The Europe Region has separate rules for DCC.

The global DCC Compliance Program was developed in 2010 and comprises a global registration, certification, and Point of Sale audit program. Specifically, the program seeks to ensure cardholders are provided with adequate disclosure and active choice when accepting DCC and that transaction receipt requirements comply with the requirements set out in the *Visa Core Rules and Visa Product and Service Rules*.

DCC registered merchants should confirm the correct cardholder billing currency before initiating a DCC transaction. As an optional service, DCC acquirers may receive a file from Visa that helps identify the actual billing currencies of BINs that can be used in DCC processing to assist with accurate currency selection.

For more information on DCC, refer to the *International Transactions Guide*.

2.17 Visa Easy Payment Service (VEPS)

Visa Easy Payment Service (VEPS) streamlines the merchant acceptance procedures by removing certain requirements such as the need for cardholder verification and generation of receipts, unless requested by the cardholder.

VEPS is targeted at low-value transactions under certain limits. These limits vary in different countries and regions. It is important for device vendors to check with their local Visa representative on specific requirements and qualifying criteria that may apply. To qualify for VEPS, a merchant must be a Visa payWave merchant or in one of the eligible Merchant Category Codes (MCCs).

For further details on how VEPS affects contact, contactless, and magnetic-stripe acceptance, refer to the following section:

- Contact: Section 3.19: Visa Easy Payment Service (VEPS) Transactions
- Contactless: Section 4.12.5: Visa Easy Payment Service (VEPS) Transactions
- Magnetic Stripe: Section 5.4: Visa Easy Payment Service (VEPS) Transactions

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

2.18 Radio Frequency (RF) Interference

A reader that supports multiple interfaces, such as contact chip and contactless, shall ensure that the operation of one interface does not interfere with the operation of another. In particular, 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.

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 together).

2.19 Management of Electrostatic Discharge

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

Disruptions of payment transactions by ESD events, particularly in dry environments, have been reported to EMVCo and have resulted in the disruption of the transaction process. Device vendors should take ESD into consideration during the terminal design, manufacturing, and testing process so as to avoid ESD events occurring in the field.

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

- Installation of static dissipative floor mats or carpets, or use of static dissipative or conductive floor coatings to reduce the build-up of static charge.
- Use of antistatic table mats that are connected to a ground point.
- Using ESD Cleaner/Treatment cards which assist in eliminating ESD and also cleaning the read head of the terminal.

EMVCo also provides a Terminal ESD Evaluation process to evaluate the level of protection against ESD of devices. Refer to www.emvco.com for more information.

Acquirers and device vendors should review the full list of EMVCo recommendations in the Interoperability Advisories section of the EMVCo website.

2.20 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 contactless symbol on payment terminals. The guidelines and artwork are available from Visa and acquirers and vendors should contact their Visa representative to obtain a copy.

2.21 Cardholder Present PAN Key Entry Transactions

Visa strongly recommends that all cardholder-present transactions be initiated with an electronic read. Electronically-read data provides the issuer with valuable information for risk management, while providing appropriate protection to the merchant.

If PAN Key Entry transactions are submitted for authorization, it is important to clearly identify the acceptance environment.

For transactions where the cardholder, card, and merchant are all present, but the transaction is initiated through manual entry of the PAN:

- POS Entry Mode should be set to "Manual Key Entry"
- POS Condition Code should be set to "Normal transaction of this type"

These same values should also be set 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, these values would apply. Also, if 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, these values apply.

It is recommended that devices support the POS Condition Code value for "Card present, magnetic stripe cannot be read (key-entered)" for those events where the electronic reader has failed.

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. For example:

- **Telephone**—If subsequent transactions are initiated by a cardholder using the telephone (whether interacting with a customer service representative or an interactive voice response (IVR) unit), the POS Entry Mode is still set to "Manual Key Entry," but the POS Condition Code is set to "Mail/phone order/recurring transaction."
- **Internet**—If subsequent transactions are initiated by a cardholder over the internet, the POS Entry Mode is set to "Manual Key Entry," and the POS Condition Code is set to "E-commerce request through public network."

3. Contact Chip Acceptance

This section provides an overview of the requirements and recommendations for an EMV compliant contact-chip transaction acceptance device that accepts Visa contact-chip cards. This section describes the processing steps for simple retail transactions and cash disbursements for EMV contact-chip transactions. It also contains Visa recommendations for industry-specific transaction types.

Important: Many environments have adopted a zero-floor limit for chip transactions. In these environments, offline risk controls, such as Offline Data Authentication, are not required and should not be implemented.

3.1 Contact Chip Card Processing

To complete a contact-chip transaction, a contact-chip card and contact-chip device engage in a series of processing steps:

1. Card Insertion
2. Application Selection
3. Initiate Application Processing
4. Read Application Data
5. Processing Restrictions
6. Offline Data Authentication
7. Cardholder Verification
8. Terminal Risk Management
9. Terminal Action Analysis
10. Online Processing
11. Completion
12. Transaction Conclusion

All steps except the last one are documented in the EMV and VIS specifications. To fully understand each of the steps, this section should be read in conjunction with these specifications.

3.2 Card Insertion

A contact chip device must be able to accept 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. For example, the cardholder may be required to press a function key to select the application or the account type. The device must then be able to establish contact by activating the chip and reading the available applications.

3.2.1 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 (for example, in some environments, refunds are not implemented using EMV functionality).

A device that reads both the magnetic stripe and chip when the card is inserted, such as an ATM, must either process the transaction using the chip data or check the Service Code to determine if a chip is present and then use the chip data accordingly.

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 with readers that support more than one interface, such as mechanized readers that support both contact chip and magnetic stripe, must ensure that only data appropriate to the transaction is used. For contact-chip transactions, all data elements used must be read from the chip.

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 (especially for multi-application cards where only one of the applications on the chip will match the magnetic stripe).

Important: 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, including the requirement to examine and act upon the 2xx or 6xx Service Codes, must not 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 also 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 since it may be needed for some types of 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/VIS chip transaction (ignoring the magnetic stripe). For more information, refer to Section 3.3.5: V PAY.

3.2.2 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[10]) when the transaction cannot be completed by reading the chip (i.e., the chip or chip reader is inoperable). This function is called Fallback and must be supported unless Fallback is disallowed by local regulation or domestic operating rules. Device vendors should contact their local Visa representative for further information regarding local rules governing Fallback.

The following outlines the basic principles related to Fallback:

- **Retry Reading Chip**—Before falling back to reading the magnetic stripe, devices should attempt to retry reading the chip three times. If feasible, devices with motorized readers 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 are processed as described in Chapter 5: Magnetic Stripe Acceptance for magnetic-stripe transactions, with the exception that all Fallback transactions must be authorized online. Fallback transactions must also contain the correct VisaNet data elements, indicating a magnetic-stripe read transaction using a chip card at a chip terminal, so issuers are able to correctly identify and process them accordingly. Details on the data elements required in a Fallback transaction are provided in Section 8.4: Fallback Processing.
- **Key-Entry/Manual Acceptance As Last Resort**—If the magnetic stripe cannot be read, key-entry or manual/paper voucher procedures may be used at the point of service unless prohibited by local regulation or domestic operating rules.[11] These transactions must be authorized online or by voice and contain the correct data elements (refer to Section 8.4: Fallback Processing for details). Key entry should only be used as a measure of last resort and only if Fallback to magnetic stripe is not possible.
- **Fallback Not Permitted**—If Fallback is not permitted by local regulation or domestic operating rules, the transaction is terminated.

[10] In the Europe Region, if a chip read is not possible, fallback to magnetic stripe is allowed but fallback to key/manual entry is not.
[11] See previous footnote.

- **Device Supports Chip but Does Not Yet Support Visa**—If the device is adding support for chip processing 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. Upon reading the chip, it will determine that Visa is not supported since the Visa AID has not yet been loaded into the device. 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 chargeback if the TEC is incorrect.
- **Liability**—Issuers are liable for Fallback transactions that have been online approved and correctly identified by the merchant.[12] Because performing a Fallback transaction circumvents the improved security offered by chip, issuers may choose to decline these transactions based on their individual risk policies.

3.2.3 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 must be used only to perform the transaction if the chip or chip reader is inoperable.

3.2.4 Support for 19-Digit PANs

Both Visa rules and regulations and the EMV specifications require that all contact-chip devices (POS and ATM) that accept Visa, Visa Electron, Plus, and/or V PAY cards must support variable-length PANs up to and including 19 digits.

In the Europe Region, acquirers must support transactions associated 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 and V PAY 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.

Important: Even in those countries where acquirer support for 19-digit PANs is not required, it is strongly recommended.

[12] The merchant/acquirer must clearly identify these transactions as Fallback and, if not, the merchant is liable. Refer to Section 8.4: Fallback Processing for information on properly identifying fallback transactions.

3.2.5 Device Messages

The EMV specifications require messages to be displayed on the screen of the device. The messages or their equivalent meaning are intended to ensure consistency in what is displayed by the device and the PIN entry device. Chip display messages are included in Table 2–1: Transaction Scenarios and Device Messages.

3.2.6 Historical Bytes

Some contact chip cards have values in the historical bytes that are returned to the device in the Answer to Reset. Although the EMV 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; for example, attempting to use these bytes for access to legacy chip applications. Although such processing may be successful for domestically issued 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.

3.3 Application Selection

This section provides general information on Application Selection. For information on applications that require cardholder confirmation and device support for cardholder selection, refer to Section 3.3.6: Cardholder Selection.

When a card only contains one application (and the application does not require cardholder confirmation) and the device supports the application, the device automatically selects that application for the transaction.

When a multi-application card is presented, the device determines which payment applications are supported by both the card and the device:

- **No Applications in Common**—If no applications are mutually supported, the device should display a CARD TYPE NOT SUPPORTED message[13] and invoke a magnetic-stripe read. See Table 2–1: Transaction Scenarios and Device Messages for chip-display messages.
- **One Application in Common**—If only one application is mutually supported (and the application does not require cardholder confirmation), the device automatically selects that application for the transaction.

[13] 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.

- **Multiple Applications in Common**—If more than one application is mutually supported,[14] the device should offer the cardholder an option to choose which application to use for the transaction (except for U.S. Covered Visa Debit Cards).[15] This is called cardholder selection. For more information, refer to Section 3.3.6: 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. In the U.S., the terminal may be configured to utilize the Visa U.S. Common Debit AID.[16] When the device automatically selects the application, it is important for the device to display the application name[17] to the cardholder as an indication of what application is being used to conduct the transaction.

The device can display the application name in one of the following ways:

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

The receipt should include the application name as per the recommendations in Section 2.7: Transaction Receipts.

Note: The EMV Application Selection Indicators supported in the device must indicate support for partial name selection for all Visa Application Identifiers (AIDs).

Important: There may be arrangements in place in a local environment to support specific Application Selection processing. Special Application Selection processing is allowed under EMV and may be the result of local law, a commercial agreement with Visa, or by Visa's acceptance of local industry standards. These solutions may allow for the suppression of a Visa AID in favor of another AID linked to the same account (such as one belonging to a domestic scheme). To determine if there are any special local arrangements in place in your environment for Application Selection, contact your Visa representative. See also Appendix F: Visa U.S. Common Debit AID for a discussion of Application Selection considerations in the U.S.

[14] 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 and regulations.
[15] In the U.S., certain requirements related to application selection and display do not apply for U.S. Covered Visa Debit Cards.
[16] Alternatively, for U.S. Covered Debit Card transactions, the terminal may be configured to utilize the Visa U.S. Common Debit AID or other customized Application Selection logic. See also Appendix F: Visa U.S. Common Debit AID.
[17] Either the Application Preferred Name (if provided by the card and the character set is supported by the device), the Application Label, or enhanced descriptor in the U.S. Refer to Section 3.3.7: Application Label and Application Preferred Name for additional information.

3.3.1 Application Identifiers

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)**—Represents the payment scheme. Visa's RID is A000000003.
- **Proprietary Application Identifier Extension (PIX)**—Represents the application.

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

Table 3–1: Visa Application Identifiers (AIDs)

Product	RID	PIX	AID
Visa Debit or Credit	A000000003	1010	A0000000031010
Visa Electron	A000000003	2010	A0000000032010
Plus	A000000003	8010	A0000000038010

Additional digits may be appended to the end of a card's AID if the card has multiple applications with the same AID (for example, the card supports both Visa Debit and Visa Credit). Because the Application Selection Indicators for AIDs must indicate support for partial name selection, the device is able to select all applications with the same AID.

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

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. For example, AID A0000000034010 is used for Visa Fleet applications, while AID A0000000032020 is used for V PAY applications (Europe-only).

Visa chip-reading devices must contain the Visa Debit/Credit AID and the Visa Electron AID.

Note: 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 to enable this.

All ATMs accepting Visa, Visa Electron, and/or Plus, must support the Visa Debit/Credit, Visa Electron, and Plus AIDs. ATMs that accept Plus chip cards but not Visa or Visa Electron chip cards must still support all three AIDs, as a Visa or Visa Electron card registered with the Plus network will likely not contain the Plus AID.

3.3.2 Transaction Routing

Routing or processing of transactions 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. An example is a Visa/Plus card (containing only the Visa Debit/Credit AID) presented at a Plus-only ATM. For multi-application cards, the device should ensure that the routing is undertaken using the BIN of the application selected; this means that the routing decision must be made only after the application has been selected.

Transactions initiated via Visa AIDs are routed to Visa affiliated networks. Domestic arrangements, such as in the U.S. and Canada, may allow for selection of other AIDs which in turn allows for routing of transactions initiated with these AIDs to alternate networks.

Chip processing should not affect decisions related to routing and, conversely, routing decisions should not affect chip processing. Acquirers and device vendors must 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 (non-Visa cards that are enrolled to use Plus such as proprietary cards).

There are no EMV or Visa chip-card processing requirements that assume the transaction is routed over a particular network. All information needed to process the transaction is carried in the message.

Certain countries have specific requirements relating to the routing of domestic transactions. Acquirers should ensure they comply with any domestic requirements relating to transaction routing.

3.3.3 Regional and Domestic Applications

Depending on the country in which it is located, the device may also need to support Visa regional or domestic AIDs.

To support regional and domestic routing, the device may need to send the acquirer (and other downstream routing entities) the AID. The AID is contained in a card data element called the Dedicated File (DF) Name (Tag '84'). Refer to Table D–2: EMV/VisaNet Data Elements and Tags.

3.3.4 Visa Electron

Visa Electron is a Visa product where transactions are always authorized (either offline or online).

In countries where Visa Electron is not issued, and assuming the merchant/acquirer agreement does not contain any specific provisions for Visa Electron, Visa Electron cards are accepted and processed identically to Visa cards. Visa Electron cards may not contain the Visa AID so the Visa Electron AID needs to be loaded into all Visa-accepting devices.

3.3.5 V PAY

The Europe Region has a chip-only, PIN-based debit card program called V PAY, which has a unique AID. The V PAY card program was created by the Europe Region for use within the European territories. V PAY cards are being issued by banks and accepted by merchants and ATMs throughout the Europe Region. Acceptance 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.

The V PAY AID is only present on acceptance devices which do not accept Visa or Visa Electron cards.

VPAY cards typically carry the Visa Electron AID to allow for global acceptance and are processed as Visa Electron transactions outside of the Europe Region territories.[18]

Devices accepting V PAY must accept PANs up to 19 digits that contain a valid BIN registered with the V PAY program. These devices must be capable of transmitting 19-digit PANs to the acquirer and, in turn, the acquirer must be capable of transmitting the full PAN to VisaNet in the authorization and clearing messages.

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 transactions are not applicable to these cards.

Note: V PAY cards typically carry the Visa Electron AID to allow for global acceptance and are processed as Visa Electron transactions outside of the Europe Region territories.

[18] 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.

3.3.6 Cardholder Selection

Issuers may deploy cards supporting "cardholder confirmation" (as personalized in the Application Priority Indicator) except for U.S. Covered Visa Debit Cards.[19] This setting indicates the cardholder *must* be provided an opportunity to select the application in order for the application to be used for transaction processing. If the cardholder is not provided such an opportunity, the related application requiring cardholder confirmation is not eligible for transaction processing. As cards may be personalized with this setting, it is important for devices to support cardholder selection. In addition, cardholder selection allows cardholders with multiple applications to select the one to use for a given transaction. Support for cardholder selection is strongly recommended for all devices that have the capacity (i.e., screens, menu functions) to support it.

Devices should implement support for cardholder selection in one of the following ways:[20]

- **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, in order of priority, one mutually-supported application 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 start the process over or terminate the transaction; the transaction can be restarted, as necessary.

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, cardholder selection is not necessary (unless the card requires cardholder confirmation) but the application name should be displayed to the cardholder (refer to Section 3.3: Application Selection for details) and should be provided on the receipt (refer to Section 2.7: Transaction Receipts).

For devices with separate cardholder and merchant 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.

[19] Cardholder confirmation does not apply to U.S. Covered Visa Debit Cards. The U.S. Personalization Validation Requirements do not allow the Visa AID and U.S. Common Debit AID to be personalized to require cardholder confirmation.
[20] 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.

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 the cancel key.

Note: Cardholder selection may be used in conjunction with domestic application selection processes. For example, domestic application selection processes may be used to remove one or more AIDs that point to a common source of funds. Cardholder selection may then be offered if more than one AID remains, such as when the remaining AIDs point to different sources of funds (i.e., credit and debit). Cardholder selection is not required for debit functionality on U.S. Covered Visa Debit Cards.[21]

3.3.7 Application Label and Application Preferred Name

Contact chip devices are required to support the character set used by the Application Label, i.e., ISO/IEC 8859. Support for displaying/printing the Application Preferred Name depends on whether the device/printer supports the Issuer Code Table Index associated with the application:

- **Device Supports Issuer Code Table Index**—The device should display and print the Application Preferred Name on the receipt.
- **Device Does Not Support Issuer Code Table Index**—The device should display and print the Application Label on the receipt.

Displaying the Application Preferred Name is preferred because it allows the name of the application to be displayed in the cardholder's local language. However, some cards may be only 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.[22]

Note: Although the wording may be slightly different, this recommendation is consistent with the known recommendations and requirements of the other payment schemes.

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. The Application Preferred Name or Application Label can be displayed at any appropriate time in transaction processing; Account Selection or PIN entry are often useful points to display the Application Preferred Name/Application Label.

---

[21] Cardholder selection is not required for debit functionality on U.S. Covered Visa Debit Cards. If a cardholder presents a multi-funding source (e.g. credit and debit applications) U.S. Covered Visa Debit Card, merchants that wish to maintain routing flexibility will need to deploy specific logic in their readers/terminals to ensure the Common AID is presented to the cardholder for debit functionality, in addition to the non-paired Visa AID for credit functionality. See Appendix F: Visa U.S. Common Debit AID.

[22] 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 Section 4.4.2 of the *Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide*.

It can be helpful to have both the Application Preferred Name and Application Label presented to the cardholder. This reinforces to the cardholder that either application name is applicable to this application and prepares the traveling cardholder for times when only the Application Label is displayed due to language constraints.

The formats of the Application Preferred Name and Application Label allow spaces in these data elements. The device must display all characters of the Application Preferred Name or Application Label. If the Application Preferred Name or Application Label contains an invalid character, this character must be displayed if the device is able to display it. If the device is unable to display the invalid character, it must display a space instead. Devices must not reject cards with spaces or invalid characters in these data elements.

For the specific transaction receipt requirements associated with these data elements, refer to Section 2.7: Transaction Receipts for details.

3.3.8 Multiple Languages

Devices may offer the cardholder a choice of languages to be used. Devices have traditionally offered a menu of all languages supported by the device and have allowed the cardholder to select the language to be used for subsequent messages.

A chip card may contain a Language Preference data object (accessed when the Application Selection process begins), which contains up to four languages in order of preference. Use of EMV functionality for language selection allows the device to shift quickly to a language most familiar to the cardholder.

At the beginning of the transaction, a device using EMV functionality to support multiple languages must compare the card's Language Preference with the languages supported in the device:

- If matches are found, the matching language with the highest preference must be used in the messages displayed to the cardholder.
- If no match is found and the device supports more than one language, the device must allow the cardholder to select the preferred language at the beginning of the transaction if it has the means for allowing such selection.

A chip card may contain more than one cardholder language option. Depending on the geographic location, devices may need to be capable of recognizing and communicating in multiple languages. Support for multiple languages and character sets is recommended for all devices. Local requirements may affect the display of languages.

3.4 Initiate Application Processing

Once an application is selected, the device sends the GET PROCESSING OPTIONS command to the card to request that the card indicates the data to be used for that application and its supported functions. The device also provides any information requested by the card as indicated by the Processing Data Object List (PDOL) sent in the Application Selection response. If the PDOL indicated that the transaction amount is to be included in the GET PROCESSING OPTIONS command, obtaining the transaction amount must precede the Initiate Application Processing for attended POS devices. UCATs and ATMs may either obtain the transaction amount or put zeroes in that field.

Account selection generally follows Application Selection for many ATMs and for those countries supporting account selection at the point of service (see Section 2.3: Account Selection). Although the process for account selection is not part of the EMV 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 typically requests this information in the PDOL.

3.5 Read Application Data

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

- Offline Data Authentication (optional in certain cards).
- Cardholder Verification (Visa cards are required to support this function).
- Terminal Risk Management (devices must always perform this function regardless of the application's AIP settings unless they are online-only devices. Random transaction selection need not be performed by offline-only devices. See 3.9: Terminal Risk Management for more information).
- Issuer Authentication using the EXTERNAL AUTHENTICATE command (optional in cards).

3.5.1 Tags

The data retrieved by the device during this step are identified by tags. The EMV specifications define the tags for the data elements.

There may also be payment system-specific tags, issuer-specific tags, and private tags agreed upon by multiple issuers. To process private tags, a device must have the data required to identify the scope of a private tag (i.e., whether it has meaning for the transaction). If the device message format supports a generic EMV data field, such as Field 55 in an ISO message, the private-data tag should be included in that field so that it may be sent to the issuer. If the data element and logic required to identify the scope of the private tag are not correct or available, the device ignores the private tag.

3.6 Processing Restrictions

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

The device must check whether the expiration date and, if present, the effective date for the card has been reached. These conditions are later evaluated based on card and device settings to determine the transaction outcome.

ATMs must not return or decline a transaction based on expiration date. They must accept the transaction even if the card has expired and must route the transaction for issuer authorization unless the card is set to decline offline (as configured in the card Issuer Action Codes).

Note: If the ATM is performing Terminal Action Analysis, a setting in the Issuer Action Codes may cause an offline decline.

The Application Usage Control field may be set by an issuer to limit or enable a card's use for certain transactions (for example, domestic or international, cash, goods or services, or cash back). The device checks the Application Usage Control received from the card to see if the transaction type is allowed.

The two Application Usage Controls "If goods" and "If services" should be treated as equivalent. A transaction for domestic goods or services is allowed if either a valid control for domestic goods or domestic services (or both) is set; the same is true for international goods and international services.

3.7 Offline Data Authentication

Offline Data Authentication enables authentication of a payment application for offline transactions. The three types of offline authentication are:

- **Static Data Authentication (SDA)**—A counterfeit protection method that ensures a set of static data obtained from the valid issuer has not been modified since initial personalization onto the card. SDA support is required for all contact-chip devices with offline capability.
- **Dynamic Data Authentication (DDA)**—Offers a higher level of data authentication than SDA, providing protection against both counterfeiting and the replaying of copied data (comparable to magnetic-stripe-data skimming). DDA support is 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. Support of CDA in devices may be needed in some countries, as this process has been implemented in specific environments.

Note: Many Visa countries have adopted a zero floor limit for chip transactions. At devices in these environments, the use of the Authorization Request Cryptogram (ARQC) in the online authorization message provides protection equivalent to the dynamic forms of Offline Data Authentication. Therefore, Offline Data Authentication and the other offline risk controls do not need to be implemented.

All Visa cards that support DDA or CDA are required to support the Dynamic Data Authentication 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 contain only the tag and length for the Unpredictable Number. No other data objects may be referenced in the Default DDOL.

Note: The Europe Region mandates that contact cards with offline capability must support DDA. Other regional variations requiring migration from SDA to DDA may exist.

3.8 Cardholder Verification

Cardholder verification is used to evaluate whether the person presenting the card is the legitimate cardholder. The CVMs that may be supported by a contact-chip device for a chip transaction are:

- Offline Plaintext PIN
- Offline Enciphered PIN
- Online PIN
- Offline Plaintext PIN and Signature
- Offline Enciphered PIN and Signature
- Signature
- No CVM Required
- Fail CVM Processing

Note: All contact-chip devices that support Offline Enciphered PIN must also support Offline Plaintext PIN.

For the minimum global requirements for CVM support by device type, refer to Section 6.5: Cardholder Verification Method Requirements.

The device uses a CVM List from the card to determine the type of 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 CVM List may contain a CVM called Fail CVM Processing.

Sections 3.8.1 and 3.8.2 discuss processing exceptions for the CVM List and the LAST PIN TRY display message. (See Table 2–1: Transaction Scenarios and Device Messages for display message information.) Additional CVM considerations are discussed in Chapter 6: Security Characteristics.

3.8.1 CVM List Processing Exceptions

Devices need to support an appropriate minimum level of cardholder verification, as determined by Visa or by local law, even when the card does not support CVM processing, no CVM List is present, or the last CVM processed in the CVM List is No CVM Required. If CVM processing does not result in the required CVM, the device may additionally perform the CVM designated in the Visa rules and regulations or in local law for the device and transaction type.

If the terminal determines that CVM Processing has failed (for example, where the cardholder is unable to enter a PIN but the CVM list only supports PIN entry) and the transaction is sent online and the issuer responds with an approval, it is recommended that the device captures a signature/prints a signature line on the receipt. Although the acquirer has no liability for the transaction, given the issuer has approved it, the collection of a signature will reduce the grounds for any potential future disputes.

Visa requires Online PIN for ATMs. ATMs will always request the cardholder to enter his/her Online PIN.

If the Visa rules and regulations or local laws do not require a particular CVM, merchants should allow CVM processing to determine the CVM to be used. The Visa rules and regulations prohibit requesting PIN unless specified in the chip's CVM List or as noted above.

For information related to cardholder verification and VEPS transactions, refer to Section 3.19: Visa Easy Payment Service (VEPS) Transactions.

3.8.2 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) or check the PIN Try Counter. If the PIN Try Counter is checked and it contains a value of 1 indicating one remaining PIN try, the device should display the Visa proprietary message of LAST PIN TRY or local language equivalent.

3.9 Terminal Risk Management

Prior to sending an authorization decision to the card, the device determines whether Terminal Risk Management must be performed.

Online-capable devices (i.e., devices capable of both offline and online processing) must support terminal risk management and perform terminal risk management for Visa chip cards, regardless of the parameters in the card. (The EMV specifications allow for cards that do not require terminal risk management.) The two mandatory risk management checks for online-capable devices are: terminal floor limits and random transaction selection.

Online-only devices (i.e., devices that always send the transaction online to the issuer for processing) will have a zero floor limit and do not need to perform terminal risk management or random transaction selection.

3.9.1 Terminal Floor Limits

Terminal floor limits are transaction amounts at or above which an online authorization should be performed. Acquirers use the Visa rules and regulations for the country and merchant type to determine the appropriate floor limit.

Online-capable devices must perform floor-limit checking on all transactions. 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.

Because countries may implement different floor limits for chip and magnetic-stripe transactions, devices should be capable of supporting both. Alternatively, devices could have an effective zero floor limit for magnetic-stripe transactions by forcing all magnetic-stripe transactions online (only where the magnetic stripe floor limit is zero) and use a floor limit for chip transactions.

Floor limits for magnetic-stripe transactions are not applicable for Fallback transactions, since all Fallback transactions should be authorized online. Refer to Section 3.2.2: Fallback Acceptance for Chip Read Failures.

An acquirer or merchant may have business reasons for setting a different floor limit value from that published by Visa. Setting the device's floor limit value higher than that published by Visa creates a liability for the merchant and acquirer. In this document, floor limit values are assumed to be set to the values published by Visa in its rules and regulations.

3.9.2 Random Transaction Selection

Random selection of transactions for online processing must be supported by terminals with both online and offline capability. This functionality protects against fraudulent cards designed to operate exclusively offline.

All online-capable devices must randomly select below-floor-limit transactions for online processing. The values used in this selection are determined per country, balancing two goals:

- Preventing fraudsters from predicting a device's online behavior and exploiting the floor limit
- Providing appropriate opportunities for transactions to be approved offline, depending on issuer-determined card controls

Random Transaction Selection is primarily useful in environments where offline transactions are prevalent. In environments where the chip floor limit is set to zero, there is no need to randomly select transactions since online processing is always attempted. Visa does not require the use of Random Transaction Selection.

There are two types of random selection:

- **Random Selection**—A certain percentage, between 0 and 99 percent, of below-floor-limit transactions is sent online.
- **Biased Random Selection**—A formula is used to determine whether the transaction goes online. This formula increases the probability of online authorization the closer the transaction amount is to the floor limit.

Visa does not have any mandates or recommendations related to the values of these parameters.

Selection Factors

Random transaction selection is based on three factors:

- **Target Percentage for Random Selection**—(a value between 0 and 99). This value determines the approximate percentage of transactions below the threshold value that the device sends online for authorization. It also determines the minimum percentage of above-threshold transactions to be sent online. Setting the target percentage to zero turns off random transaction selection (that is, no transactions will be randomly selected to go online).
- **Threshold Value for Biased Random Selection—**(a value between 0 and the value of the floor limit). Below this threshold, transactions are subject to random selection; above it, to biased random selection. If this value is zero, all transactions would be evaluated by biased random selection; if set to the floor limit, biased random selection would not be used (only random selection).
- **Maximum Target For Biased Random Selection**—(a value between 0 and 99, equal to or greater than target percentage for random selection). This value is used to weight the above-threshold selection criteria to increase the percentage of selected transactions as the transaction value approaches the floor limit. The higher a value, the more likely that the transaction will go online.

Random Transaction Selection Process

If the transaction amount is less than the threshold value for biased random selection, then random selection is performed as follows:

1. The device generates a random number between 1 and 99.
2. If the device-generated number is higher than the target percentage for random selection value, the transaction may be approved offline if card controls permit. (The card, using its own parameters, may require that the transaction be sent online for authorization.)

3. If the device-generated number is lower than or equal to the target percentage for random selection value, the device sends the transaction online for authorization. If online processing is unavailable, the transaction may be approved offline by the card if the card controls permit.

If the transaction amount is greater than or equal to the threshold value for biased random selection, the transaction is subject to biased random selection:

- Here the nearer the transaction amount is to the floor limit, the greater the likelihood that the device will select the transaction for online authorization. The target percentage for random selection sets the minimum percentage selected by this method, and the maximum target percentage for biased random selection determines the maximum percentage of transactions selected for online authorization by biased selection.

To summarize, assuming a random distribution of transaction amounts:

- All above-floor-limit transactions will go online for authorization.
- Below the floor limit and below the threshold, the target percentage (for random selection) of transactions will be sent online.
- Below the floor limit and above the threshold for biased random selection, transactions will be increasingly likely to go online the closer they are to the floor limit. This probability will be capped by the maximum target percentage.

The examples below are based on an environment using the values shown in Table 3–2.

Table 3–2: Random Transaction Selection Values

	International	Domestic
Chip floor limit	€0	€100
Threshold value for biased random selection	N/A	€40
Target percentage for random selection	N/A	20%
Maximum target percentage for biased random selection	N/A	50%

Assuming that the device has generated a random number of 25 for this transaction, the following points provide examples of the result:

- **International Transaction Amount = 15**—Because there is a zero floor limit for international transactions, the transaction is selected for online processing.
- **Domestic Transaction Amount = 15**—Because the transaction amount (15) is below both the floor limit (100) and the threshold value for biased random selection, random selection is performed. The terminal random number (25) is compared to the target percentage for random selection (20) and, because the random number is higher, the transaction is not selected for online processing.
- **Domestic Transaction Amount = 60**—Because the transaction amount (60) is below the floor limit but above the threshold value for biased random selection (40), biased random selection is performed. The following calculations are performed:

1. A ratio, or bias, is determined: (transaction amount—threshold value)/(floor limit—threshold value) =(60—40)/(100—40) = 20/60 = 1/3
2. The incremental percentage to be biased is determined: (maximum target % for biased random selection—target % for random selection) = (50—20) = 30
3. The biased incremental percentage is calculated: (incremental percentage * ratio) = (30 * 1/3) = 10
4. A weighted target is created: (target % for random selection + biased incremental percentage) = (20 + 10) = 30. This weighted target (30) is greater than the device's random number of 25, so the transaction is selected for online processing.

- **Domestic Transaction Amount = 150**—Because this is above the floor limit, the transaction is not subjected to random selection. It is selected for online processing by the device's floor-limit checking function.

3.10 Terminal Action Analysis

Terminal Action Analysis determines the type of cryptogram the terminal should request from the card. This decision is based on rules from the card called Issuer Action Codes and rules set in the terminal called Terminal Action Codes. The device uses the results of previous processing steps together with the device and card rules 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, corresponding to the transaction disposition:

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

In this step, the device issues the card a GENERATE APPLICATION CRYPTOGRAM (GEN AC) command. The device indicates if CDA is to be performed.

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 of Visa transactions.

Section 3.10.1: Terminal Action Codes and Issuer Action Codes discusses the details of Terminal Action Analysis processing.

Section 3.18: EMV in Online-Only Environments discusses the unique requirements for online-only devices.

3.10.1 Terminal Action Codes and Issuer Action Codes

Terminal Action Codes (TACs) are the device-based rules for Terminal Action Analysis. TAC values are mandated by Visa and must be supported by offline-capable devices. There are three types of TACs: TAC-Denial, TAC-Online, and TAC-Default.

Issuer Action Codes (IACs) are the card-based rules that the device uses during Terminal Action Analysis. IAC values are set by the issuer. There are three types of IACs:
IAC-Denial, IAC-Online, and IAC-Default.

For more information on the TACs including TAC values, refer to Section 7.2.2: Terminal Action Codes.

3.11 Online Processing

This section outlines the requirements for online messages.

3.11.1 ARQC and Associated Data

The ARQC and its associated data must be included in the authorization message. The issuer validates the ARQC to help ensure that the card is valid and can use the results in its authorization decision. Visa can also validate the ARQC on behalf of the issuer in the instance where the issuer host is unavailable or the issuer does not have the internal capability to undertake the validation.

The ARQC uses dynamic transaction data to provide high protection levels against counterfeit and skimming. To facilitate validation of the ARQC, the device must send the same data in the online authorization that was sent to the card in the first GENERATE AC command. Failure to comply could lead to failures in the Card Authentication process and unnecessary declines.

3.11.2 Merchant Forced Transaction Online

Setting the “Merchant forced transaction online” bit is reserved for situations where the clerk explicitly forces a transaction online, such as for suspicious behavior. Support for a facility to force the transaction online, as described in the EMV specifications, is optional and not mandatory and may be determined by acquirer or local requirements.

Setting this bit should not be used to make a transaction go online; the issuer may interpret this as evidence of suspicious behavior and decline the transaction. If a merchant needs to ensure that a particular category of transactions always goes online, they can achieve this by setting the “Transaction exceeds floor limit” bit in the TVR.

3.11.3 PAN on Exception File

Merchants and acquirers should not indicate that a PAN was found in a terminal exception file except when a formal arrangement with affected issuers is in place. Specifically, the TAC condition "The PAN is on the terminal exception file" should be evaluated as true only if the PAN was placed in the terminal exception file under the formal arrangement. PANs extracted from the Visa Exception File for this use are considered compliant with this requirement.

3.11.4 Cash Back

This section provides information on cash back related to chip transactions. For general information on cash back, refer to Section 2.12: Cash Back Identification and Processing.

Visa allows cash back to be provided with a purchase at the point of service for domestic transactions, under certain conditions. Current Visa rules do not allow cash back to be provided on credit cards or when the cardholder has selected to use a credit facility.

A cash back transaction must always be sent online and there must always be cardholder verification (i.e., a No CVM Cash Back transaction is not permitted).

In situations where cash back is supported, the sequence of events is important and should be executed as follows:

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

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

- Cryptogram Amount (V.I.P. Field 147, EMV Tag '9F02')—Purchase amount plus the cash back amount
- Cryptogram Cash Back Amount (V.I.P. Field 149, EMV Tag '9F03')—Cash back amount
- Cryptogram Transaction Type (V.I.P. Field 144, EMV Tag '9C')—Equal to '09'
  Note: This field contains a different value from the first two digits of the Processing Code, which will be '00' (Purchase).

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. Refer to Section 2.12: Cash Back Identification and Processing.

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

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

Important: Gratuities/tips should not be placed in the Cryptogram Cash Back Amount field. For more information on gratuities/tips, refer to Section 3.15.5: Gratuities or Tips.

3.11.5 Online Transaction Data Requirements

Appendix D: EMV Tag to VisaNet Data Element Mapping provides information to help vendors and acquirers understand the chip data required in messages sent between devices and acquirers and between acquirers and VisaNet.

3.12 Completion

Completion closes the processing of a chip transaction. The card and device perform final processing to complete the transaction. When the online authorization is successfully completed, the device issues a final 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:

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

- TC (Approval)
  - If the Authorization Response Code is 00, 10, or 11 indicating that the issuer has approved the transaction, the device requests the approval cryptogram (TC).
- AAC (Decline)
  - If the Authorization Response Code is 01 or 02 indicating that the issuer has requested a referral, the device should request the decline cryptogram (AAC).
  - If the Authorization Response Code does not contain the above-mentioned values indicating approval or referral, the device requests the decline cryptogram (AAC).

The card uses the transaction disposition, Issuer Authentication results, and issuer-encoded rules to determine whether to return a TC or an AAC.

Although devices are not required to retain the cryptogram (TC or AAC) for online-approved transactions at single-message or host-capture devices, the device must request the final cryptogram to allow the chip card to complete Issuer Authentication to avoid unnecessary online requests in environments that support offline approvals. A reversal must be generated for approved transactions that are subsequently declined by the card.

Note: After generating an ARQC, generating a TC causes the offline counters in the card to be reset (if Issuer Authentication is successfully completed). Not requesting a TC could cause a subsequent online request to be generated prematurely.

For terminal-capture devices, if the transaction was approved either online or offline, the device transmits the TC and the related cryptogram data in the clearing message.[23]

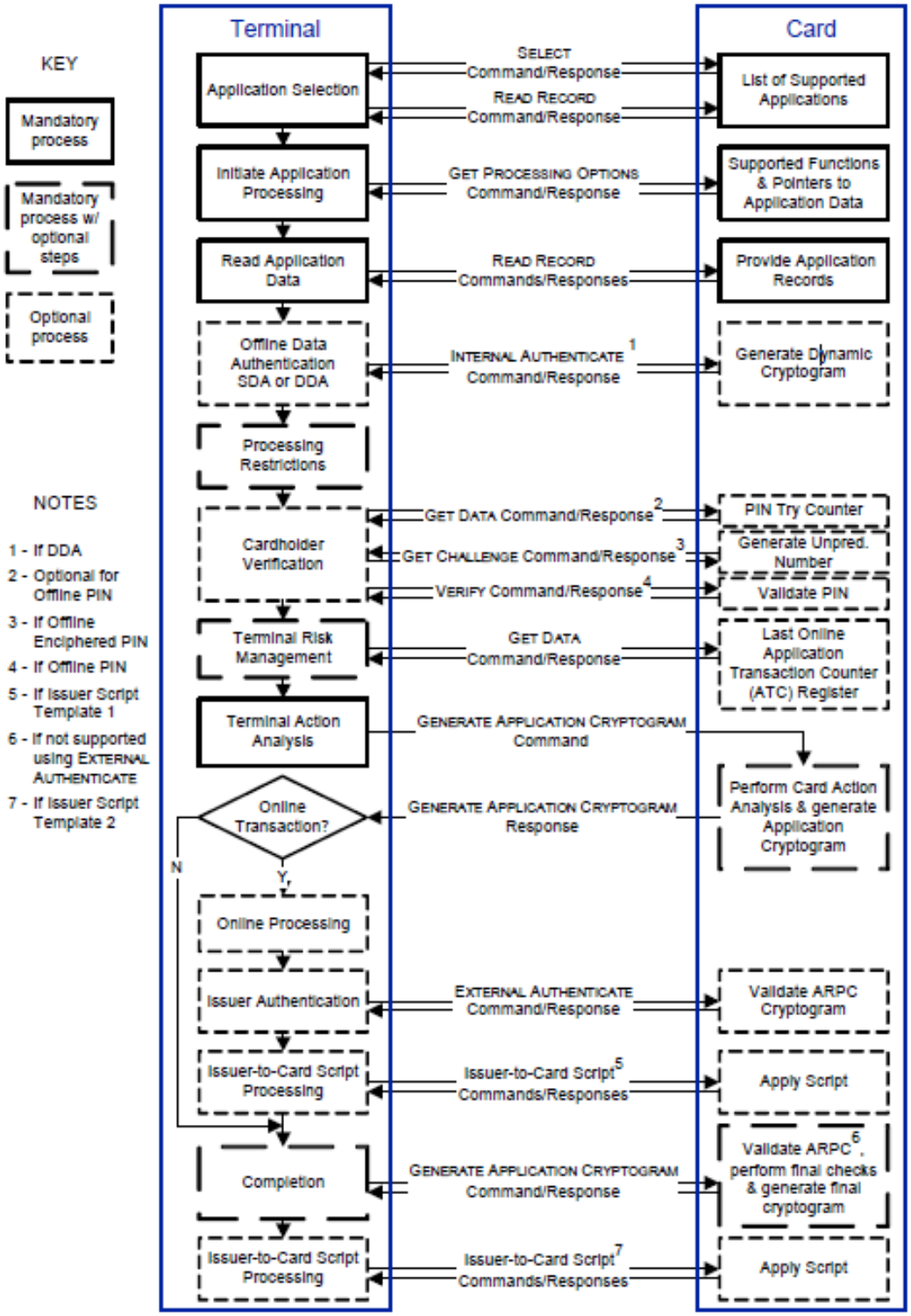
If during processing, the EMV specifications require the device to terminate the transaction, the device needs to display a message to the cardholder and merchant indicating why the transaction cannot be completed and that the card should be removed.

If the transaction is declined offline, the device cannot force the transaction online in an attempt to get an approval. Declined transactions are further discussed in Section 3.12.7: Declined Transactions.

Figure 3–1 illustrates a sample transaction flow including all the various steps described in the previous sections.

[23] In the U.S., chip data (including the TC) is not required in the clearing message.

Figure 3–1: Sample Transaction Flow Diagram



3.12.1 Online-Authorized Transactions

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

Single Message/Host-Capture

Single-message full financial and host-capture transactions contain the ARQC in the financial/clearing message.[24] These devices should ensure a TC is generated for approved transactions. Although not needed for clearing, generating a TC ensures that cards do not request unnecessary online approvals on subsequent transactions and also provides liability protection for acquirers.

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.

Device Capture

Device-capture acquirers use the ARQC for the authorization and the TC for the clearing message.[25]

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 host-capture point of service). If the ARQC is used in the clearing message, a valid authorization code is required.

Data Elements

Many data elements used for Application Cryptogram generation 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 included in the message. Besides the cryptogram itself (ARQC or TC), the following elements are also likely to differ:

- Card Verification Results (CVR) (the cryptogram type is updated as well as the Issuer Authentication 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)

[24] In the U.S., chip data is not required in the clearing message.
[25] In the U.S., chip data (including the TC) is not required in the clearing message.

- Unpredictable Number (devices must use a new Unpredictable Number for each cryptogram generation; the Unpredictable Number sent in the clearing message must be the one used for the cryptogram sent in the clearing message)

3.12.2 Deferred Authorization

Deferred Authorization is where an online authorization is performed after the card is no longer available as discussed in Section 1.8: Deferred Authorization.

This is accomplished by the device requesting an ARQC. The device then informs the card that it cannot go online and requests an AAC. Later, the device uploads a batch of authorization requests that include the ARQCs.[26] The acquirer submits the authorization requests, most of which are approved online. Repeated attempts at authorization for declined transactions are permitted but declined transactions must eventually be discarded.

The acquirer then formats and submits a clearing record[27] for each approved transaction, using the ARQC for online approved transactions and the authorization response code returned in the authorization response.

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 used in the clearing record.

Merchants may elect to implement additional risk management controls in these situations, such as imposing a ceiling on transaction size, or even implementing velocity checking. If most cards in the country support Offline Data Authentication, the device should check the results of Offline Data Authentication prior to dispensing goods or services and before flagging the transaction for Deferred Authorization.

3.12.3 Acquirer Stand-In

If the card generates an ARQC to indicate that the transaction must be sent online, but the acquirer is unable to communicate to the issuer and wants the disposition of the transaction to be decided by the card and the device, the acquirer causes the device to indicate that the transaction was unable to go online:

- If the second Application Cryptogram is a TC, the transaction is approved.
- If the second Application Cryptogram is an AAC, the transaction is declined.

[26] Use of the AAC rather than the ARQC in the authorization request may result in unnecessary declines by the issuer.
[27] Chip data is not needed in clearing for online-approved transactions in the U.S.

An acquirer may decide to override the decline decision and clear the transaction at its own liability for chargebacks associated with no authorization.[28]

To accomplish this, the acquirer may either set up the device to override a decline under certain conditions or send an indication to the device to override if a particular transaction is declined. When this occurs, the device does not display a decline message but displays another message determined by the acquirer, the consumer receives the goods or services, and the transaction is cleared.

The device should request a TC, and the card will respond with either a TC (indicating that the transaction is approved offline) or an AAC (indicating that the transaction is declined offline):

- **TC**—If the card generates a TC, the acquirer should use this TC and its associated data elements for the clearing message. (The transaction is approved, and the acquirer retains protection.)
- **AAC**—If the card generates an AAC, and the acquirer elects to clear the transaction, the transaction must be cleared with the AAC and its associated data elements. (The transaction is not approved, and the acquirer submits the transaction into clearing at its own liability. The issuer may charge back these transactions if either they cannot collect from the cardholder or the cardholder disputes the transaction.)

If most cards in the country support Offline Data Authentication, it is recommended that the device checks the results of Offline Data Authentication prior dispensing goods or services.

Note: A preferable approach is to use the ARQC to perform a Deferred Authorization (refer to Section 3.12.2: Deferred Authorization). Submission of transactions without authorization may not be allowed in some countries, may have cost or fee considerations, and/or may leave the acquirer/merchant open to compliance actions. Note also that if the card approves offline, but the transaction amount is above the country floor limit for this merchant category, the acquirer/merchant is still liable for chargebacks associated with no authorization.

3.12.4 Acquirer Forced Settlement

In certain circumstances such as when the transaction is above floor limit but the terminal is unable to go online, the acquirer may elect to clear a transaction even if Terminal Action Analysis indicates that an AAC is requested in the second GENERATE AC. In this case, the card will return an AAC and the transaction is cleared with the AAC and its associated data elements. The transaction is cleared at the acquirer's liability.[29]

Note: A preferable approach is to use the ARQC to perform a Deferred Authorization (refer to Section 3.12.2: Deferred Authorization). Some countries may not allow forced settlement.

[28] 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 whose cards do not support offline functionality), the merchant may decide to accept the risk in the interest of customer satisfaction.

[29] Refer to the footnote in Section 3.12.3: Acquirer Stand-In.

3.12.5 Authorization Response Cryptogram Considerations

Issuers may generate an Authorization Response Cryptogram (ARPC) as part of the response message to allow the card to validate that it was generated 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, EMV requires that online data-capture devices generate a reversal.

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.

3.12.6 Offline-Authorized Transactions

Offline chip authorization may occur when a transaction amount is under the floor limit or the device is offline only. In these cases, the card generates a TC, which is included in the clearing message along with its associated data. The device generates a Y1 or Y3 Authorization Response Code indicating an approval for inclusion in the clearing message (see Appendix D: EMV Tag to VisaNet Data Element Mapping for a description of these codes).

For online authorized transactions, an Authorization Code is included in the authorization response, which is provided on the transaction receipt and sent in the clearing message. Authorization Codes for offline-authorized chip transactions are left to the acquirer's discretion. Visa recommends that Authorization Codes for offline transactions be included on the receipt in the CHPxxx format where xxx can be set to any value by the acquirer or device.

3.12.7 Declined Transactions

Where the authorization response received by a device indicates a decline, the merchant should be informed on the device display that the transaction has been declined. For the display to the cardholder, the term 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 a few countries, for auditing purposes, declined transactions are delivered along with the clearing batch to the acquirer (though the declines might not be forwarded to the issuer). In other countries, declines may simply be deleted from the device.

3.13 Transaction Conclusion

Transaction conclusion, as described here, is not part of the EMV or VIS specifications for the processing of contact-chip transactions. It should not be confused with transaction completion, which is a required EMV/VIS step.

Transaction conclusion may be viewed as the point in the process where the device has gathered all the data necessary to process the transaction. It may also be viewed as the point in the dialogue between cardholder and device where goods or services are either exchanged for payment or the transaction is terminated. Evidence of transaction conclusion is usually the generation of a receipt—a record (paper or electronic) that confirms the exchange of goods or services for payment. For device-capture systems, the device adds the transaction data to the current batch.

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.

The chip card must remain in the chip card reader until the last EMV transaction step, including Issuer Script processing, is completed. The cardholder and merchant experience here is different compared to a magnetic-stripe transaction, where the merchant may swipe the card and immediately return it to the cardholder. To reinforce this behavior, once the EMV transaction has ended and is approved, the device should display a message instructing the cardholder or merchant to remove the card. Merchant staff should ensure that they do not remove the card before the message is displayed; otherwise, the transaction may fail.

If the card is removed before the transaction is complete (i.e., the TC or AAC has not been received from the card), the transaction must always be terminated. If an online authorization has taken place, a reversal message should be sent. (If a decline response has been received, it is not necessary to send a reversal.)

If a card is removed after the second cryptogram generation but before Issuer Script processing, the transaction is considered complete and 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.

3.14 Considerations for Industry-Specific Transaction Types

The EMV specifications address the use of EMV functions for simple retail transactions and cash disbursements, which are described in sections 3.10 through 0. EMV functionality for other financial and nonfinancial transactions is discussed further in *Recommendations for EMV Processing for Industry-Specific Transaction Types*, available at www.emvco.com. This section contains additional Visa recommendations for these transaction types.

Generally, chip transactions should flow similarly to magnetic-stripe transactions. In many cases, the Visa rules and regulations for chip transactions are no different from those for magnetic-stripe transactions. In some cases, change is unavoidable, such as the display of a cardholder application selection menu when the chip supports more than one application or the introduction of a new CVM.

Transactions where either the card or the device has not completed all required components of EMV processing, including generating an Application Cryptogram, are not EMV transactions. This includes any transaction that begins as an EMV transaction to extract data such as a PAN and expiration date but then the EMV transaction is terminated and a non-EMV transaction using the extracted data takes place.

3.14.1 Pre-Authorizations

A pre-authorization is when an authorization takes place before the final amount is determined. Pre-authorizations are subject to Visa rules and regulations but normally follow standard EMV transaction processing.

Note: In certain environments, any estimated amount is likely to be the maximum dispensable value of goods or services.

3.14.2 Incremental Authorizations

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

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

If the card is present, the incremental authorization can be chip-read, and should be conducted as described in Section 3.14.1: Pre-Authorizations.

3.14.3 Sale Completion

A sale completion is the financial settlement of a previously authorized transaction, 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.

Note: Typically, an online authorization for an estimated amount is used for travel and entertainment where the final amount is not known. Check the Visa rules for the specific country and T&E category.

It is recommended that, if available, the merchant uses 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.

The chip data obtained in the pre-authorization should be included in the clearing message or, in the case of multiple clearing messages (where multiple items are purchased but delivered separately), in each of the clearing messages. In the event of multiple clearing messages, the total of the sales completions should add up to the amount of the pre-authorization.

The POS Entry Mode Code for a sale completion should be set to "chip read" only if either of the following conditions occurs:

- The original online authorization contains a cryptogram and all of the chip data elements used to create the cryptogram.
- The cryptogram and all of the chip data elements used to create the cryptogram from the offline authorization are included with the sale completion. The original offline authorization is not submitted into clearing.

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

3.14.4 Status Check

A status check is an online authorization for a single unit of currency. The use of status checks is limited to automated fuel dispensing.

In some countries, status checks are used as pre-authorizations for automated fuel dispensing, implicitly allowing up to a set amount to be used in the sale completion. Status checks must be sent online because the chip does not have any mechanism to recognize the implicit value of this special transaction. For more information on Automated Fuel Dispensers, refer to Section 3.15.2: Fuel/Petrol Dispensing.

3.14.5 Account Number Verification

Account number verification is a Card Not Present 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.

3.14.6 Refunds

A refund occurs when the cardholder is credited with the value of returned goods or mis-performed services. Both full and partial refunds of the original transaction may be performed. In most environments, a refund consists only of a clearing message and does not require an online message to the acquirer or issuer. In single-message environments, clearing-only messages may be sent online. Some environments do require that the acquirer approves a refund and device vendors should check with their local acquirer or processor.

It is strongly recommended that refunds for chip cards be performed by following the normal EMV transaction flow to obtain the Track 2 Equivalent Data from the chip. If this tag is not present on the chip, the device should obtain the contents of the PAN and expiration date fields instead. Performing Offline Data Authentication (if supported by the card) and cardholder verification, as performed for purchases, will help protect the merchant and acquirer against fraudulent refunds. There is no requirement to perform Terminal Risk Management.

If the PDOL indicates that the Transaction Amount and the Transaction Type are to be included in the GET PROCESSING OPTIONS command, it is recommended that the device send the refunded amount as the Transaction Amount and the Transaction Type (Tag '9C') as 20. If the PDOL indicates the Transaction Amount is to be included, but not the Transaction Type, the Transaction Amount should be set to zero.

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

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

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

3.14.7 Reversals

Reversals are a function of the transaction network or of the device and do not require interaction with the card for generation of the reversal message. No chip card data needs to be included in the authorization reversal. The acceptance device sends a reversal to the acquirer which in turn sends it to the issuer to notify that the previous authorization response was not delivered to the device (known as a system reversal) or has been annulled or voided by the device.

If the device generates a reversal (e.g., because it detects the connection to the acquirer host has been lost, or has timed out because no authorization response has been received) and an ARQC has been requested, then an AAC should be requested of the card to avoid unnecessary requests for online authorizations on subsequent transactions.

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

In certain circumstances, the issuer may have approved the transaction but the card may override the approval and decline the transaction. This is primarily due to an Issuer Authentication failure where the ARPC sent by the issuer in the response message was verified by the card but failed.

Acceptance devices must initiate a reversal message if the card declines a transaction that the issuer approved online.

If a reversal is required, the card is present, and the following fields are available, they should be included in the reversal:

- TVR (updated with the Issuer Authentication results)
- CVR (updated with the Issuer Authentication results)
- Issuer Script results (if the original response message from the issuer contained an Issuer Script, the Issuer Script results are provided in this field)

Otherwise, chip data does not need to be included in a 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$80, then a partial reversal can be submitted for the USD$120 difference between the estimated and final amount. The chip-related requirements for partial reversals are the same as for full reversals.

3.14.8 Referral

A referral is intended as a fraud control tool for issuers. Issuers may respond to an online authorization with a referral response when the issuer needs more information before approving a transaction. A referral is not a transaction; it is an exception process for a purchase.

In many cases, a referral response from an issuer will be converted to a decline by retailers in which speed of transactions is considered important (e.g., supermarkets).

In most cases, when a referral response reaches the device, the terminal will terminate the transaction by requesting an AAC from the card in the second GENERATE AC request. The referral process may then take place using normal procedures (i.e., the merchant calls the issuer to obtain a manual authorization or to have the referral block cleared so a new transaction can take place).

3.14.9 Cancellation

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

There are a number of reasons why 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.

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

If the transaction has not reached the point where an ARQC has been requested, the card can simply be powered off. If an ARQC has been requested and the transaction has been routed online, then cancellation processing should also generate an authorization reversal. The transaction should simply be removed from the clearing batch or marked as void.

If the device has received a TC or AAC from the card, the transaction is completed and can now be cancelled (removed from the 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.

3.14.10 Cryptogram Generation in Multi-Currency Scenarios

Certain devices have Dynamic Currency Conversion capabilities and as such are able to handle multiple currencies. It is critical that the currency code used in the generation of the cryptogram (ARQC or TC) is the same as is included in the authorization and clearing messages (V.I.P. Field 148, EMV Tag '5F2A') and is not altered by any intermediary networks. A change in the currency code could lead to the issuer declining the transaction since the cryptogram validation will fail.

In most scenarios, the transaction currency (V.I.P. Field 49) will contain the same value as the chip data related currency in V.I.P. Field 148, EMV Tag '5F02'. However, there may be instances where these differ. The critical point is that the chip-related field is not changed from the currency used to generate the cryptogram.

3.15 EMV Transactions in Specific Industries

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

Transactions using EMV functions must follow all relevant EMV requirements. If the transaction is completed by extracting data from the chip (but not following the entire EMV payment transaction flow), the transaction is considered manually entered.

3.15.1 Hotels and Tourism Industries

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

- **Reservations**—This process does not normally involve the card being present or the chip being read so normal procedures should be followed.
- **No-Shows**—Charges for guaranteed reservations (no shows) should not be processed as chip transactions unless an EMV transaction has been performed at the time of the reservation.
- **Check-In**—A pre-authorization is completed at check-in to ensure the card and cardholder are genuine and to guarantee the funds before the final transaction amount is known. Local requirements will determine the estimated amount to be used. To avoid confusion, the estimated amount should not be displayed to the cardholder. The estimated amount is the amount presented to the chip card. If online authorization is required, it is also the amount used to generate the ARQC and sent online in the authorization message.
- **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. The card does not need to be present and the authorizations should not include any chip data.
- **Express Check-Out**—It is not necessary to perform a full EMV transaction once the final transaction amount is known. A sale completion is generated for the final billing amount and, if chip data is required for clearing, then the chip data from the original pre-authorization should be included.
- **Additional Charge After Check-Out**—Any additional charges identified after check-out should be processed as a separate Card Not Present transaction. The chip data from the pre-authorization should not be submitted in the clearing record.

Similar processes to those described above may be used for the car rental or other tourism and travel industries. Acquirers and merchants should review the Visa rules and regulations or contact their local Visa representative for further details.

3.15.2 Fuel/Petrol Dispensing

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

- **Unattended Petrol Environment**—For chip transactions, complete an online status check transaction before fuel is dispensed. The status check provides authorization protection up to the domestic rule limit.
- **Enhanced AFD Non-Financial Advice**—In countries where Enhanced AFD is supported, merchants must follow a status check with an authorization advice within two hours of the status check for the actual amount. This advice must equal the sale completion amount.
- **Pre-Authorization**—Where estimated authorizations are allowed, the merchant estimates the amount (usually more than cardholders typically incur at the pump) and submits a pre-authorization for that 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 an authorization reversal for the unused portion of the authorization and submit a sale completion for the actual amount.
- **Sale Completion**—When the transaction is completed (i.e., when the fuel dispensing is completed) and the final transaction amount is known, a clearing record for the final amount should be submitted containing the chip data from the status check or pre-authorization. Single-message environments may require an adjustment to the pre-authorization amount, particularly if an estimate was used rather than a status check.

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

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

3.15.3 Mobile Top-Up

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

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

If a top-up transaction is completed with card-on-file data, the transaction is considered Card Not Present. If the transaction is completed by extracting data from the chip (but not following the entire EMV payment transaction flow), the transaction is considered manually entered.

Note: Only PAN and expiry date should be stored, never full Track 2 data. Stored PAN and expiry date must be protected according to PCI DSS.

3.15.4 Forced Acceptance for On-Board Transactions

In some environments where online authorizations are not normally available, such as aircrafts and ferries, merchants may need to obtain an authorization before submitting an item for clearing (a Deferred Authorization). In this case, the ARQC may be used later to request an online authorization (for example, after the plane lands or the ferry docks), and the approval code along with the ARQC may be put into the subsequent clearing message.

Some countries may allow an attended terminal to have functionality allowing an attendant to override the decline (AAC) returned by the chip card if the terminal requests for an approval (TC) during the second GENERATE AC command. If this occurs, the merchant may put the AAC into the clearing message to indicate that the transaction was declined by the chip (most likely due to the card's risk management settings). This process is also known as Acquirer Stand-In as discussed in Section 3.12.2: Deferred Authorization.

Note: Deferred Authorization and Acquirer Stand-In may not be supported in all regions. Acquirers should contact their Visa representative to determine the applicability of Deferred Authorization and Acquirer Stand-In in their country.

3.15.5 Gratuities or Tips

Gratuities/tips may be handled using one of the two options outlined in the table below.

However, vendors should consult with their local Visa representative, as:

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

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

Table 3–3: Gratuities/Tips Options

Options	Description	Authorization: Amount/ Cryptogram Amount	Clearing: Amount/ Cryptogram Amount[30]
Option 1	After authorization, a gratuity/tip is added of up to 20% of the base transaction amount to the authorized amount submitted in the clearing record	Amount *without* gratuity	Amount plus gratuity
Option 2	Gratuity/tip is added to the transaction amount before authorization	Amount plus gratuity	Amount plus gratuity

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

3.15.6 Discounts

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

- Begin an EMV transaction to obtain the PAN.
- Reach out to the other system(s) with the PAN to see if a discount applies.
- Apply the discount to the amount before sending the amount to the card for cryptogram generation.

3.16 Non-EMV Transactions using EMV Functionality

Non-EMV transactions using EMV functionality are commonly employed in the retail or cash disbursement environment but do not directly result in the purchase of goods or services or in the disbursement of cash. EMV functions that extract information or request identification or authentication can be readily used to complete these transactions.

Important: Merchants should not rely on being able to access the cardholder name (either for payment or non-EMV transactions) as more and more payment instruments will not be carrying this sensitive data element.

[30] The U.S. does not require any chip data, including the cryptogram, in clearing. Where the ARQC is used in clearing, such as for single-message and host-capture systems, the ARQC should not be modified and thus may contain only the original amount.

EMV functions can be used for the following purposes:

- **Information**—To obtain information, such as how many applications are in a card. To support this, a device can use the Application Selection, the Initiate Application Processing, and the Read Application Data functions.
- **Verification**—To verify the identity of the cardholder, the device can use any of the CVMs as defined in the CVM List.
- **Authentication**—To check the authenticity of the payment application, the device can use the Offline Data Authentication function as part of offline processing or allow the issuer to validate the payment application using the ARQC as part of online processing. (For example, by using Account Number Verification.)
- **Card Management**—Issuer Script processing may be used for card management, such as updating PINs.

Non-EMV transactions should be completed by an AAC.

Note: An AAC generated for a non-EMV transaction simply indicates completion and is not a decline.

Note: Transactions where either the card or the terminal has not completed EMV processing, by generating an Application Cryptogram, are also not considered EMV transactions.

Transactions using EMV functions must follow all relevant EMV requirements. EMV functions should be executed in the same order as for standard EMV transactions (i.e., non-EMV transactions using EMV functionality should follow the EMV transaction flow). If the transaction is completed by extracting data from the chip (but not following the entire EMV payment transaction flow), the transaction is considered manually entered.

Refunds and on-us ATM transactions are examples of non-EMV transactions using EMV functionality.

3.17 EMV at ATMs

ATMs have some unique characteristics that need to be considered for EMV. ATMs will always go online for cash disbursement and balance inquiry authorizations. Many of the offline functions that are supported under EMV are not required since transactions will always be authorized by the card issuer.

In this document, ATM transactions are assumed to be cash disbursements, as defined under EMV. Other ATM transaction types (such as balance inquiries, deposits, and funds transfers) are not considered EMV transactions. These transaction types can use EMV functions and can be initiated using the EMV chip. However, they will not go through all stages of EMV processing.

Sales of goods and services and related transaction types, if performed at an ATM, fall under the rules and procedures for UCATs and are not considered ATM transactions. The Processing Code will be 00 and an appropriate MCC other than 6011 should be used.

If a purchase is made via an ATM, where the ATM acquirer is the owner of the goods sold or the services provided, the Processing Code is set to 00 for a purchase and an MCC of 6012 should be used. The MCC of 6011, which is normally used for ATMs, should not be used.

The following sections outline some of the key requirements and considerations for acquirers and ATM vendors when migrating to EMV. Device-specific requirements for ATMs are included in Chapter 6: ATM, of the *Visa Core Rules and Visa Product and Service Rules*. Acquirers should review these rules to ensure they comply with all of Visa's ATM requirements.

3.17.1 Basic EMV Requirements for ATMs

This section outlines basic EMV requirements for ATMs:

- **Zero Floor Limit**—The terminal floor limit for ATM transactions must be set to zero.
- **No Offline Functionality**—Because ATMs will always go online, they are not required to perform Offline Data Authentication (SDA/DDA/CDA), and it is recommended that they do not perform these functions.
- **CVM Processing**—The CVM is Online PIN and no other CVMs are currently supported for ATM transactions. The ATM must always request Online PIN regardless of the card's CVM list.
- **Online Card Authentication**—Enhanced security is achieved by performing Online Card Authentication where an ARQC is generated by the chip and validated by the issuer as part of online authorization processing.
- **Issuer Authentication and Reversals**—The issuer may optionally send an ARPC in the response which is validated by the chip card. The issuer may personalize the card to issue a subsequent decline, if Issuer Authentication fails. ATMs must be capable of supporting ARPC validation by passing the required data to the card and must generate a reversal if a decline is returned in response to the final cryptogram generation request after an online approval by the issuer.
- **Issuer Script**—The ATM must also pass script commands to the card if the issuer has sent them.

Other than what is described above, the ATM should only perform the minimum and mandatory EMV functions required to send the transaction online using Online PIN.

3.17.2 ATM Card Read Order

Chip cards need to stay in the reader for the duration of the transaction similar to POS transactions. Because the chip card and reader make actual contact, acquirers will need to ensure they implement a process to regularly clean the card readers and perform other preventative measures.

When a chip card is inserted into a chip-reading ATM, the order of read is outside the EMV flow, as long as the actual processing is initiated using the chip data. For example, any of the following is acceptable when using a motorized reader:

- The card is passed through to the chip card reading station. If communications are established with the chip, EMV processing continues using the chip. For Fallback, the card is returned to the magnetic-stripe reading station.
- The card is passed through the magnetic-stripe reading station and the magnetic-stripe data is read into a buffer. The card is then passed to the chip card reading station. If communications are established with the chip, EMV processing continues using the chip. The data in the buffer is not used for EMV transaction processing. If Fallback occurs, the data in the buffer can be used to re-initiate the transaction as a magnetic-stripe transaction.
- The card is passed through the magnetic-stripe reading station, the magnetic-stripe data is read, and the Service Code is examined. If the Service Code is 2xx/6xx, then the card is passed to the chip reading station. If communication is established with the chip, EMV processing continues using the chip. For Fallback, the magnetic-stripe buffer can be used, or the card can be read again.

Important: Transaction data must not be mixed. If the POS Entry Mode indicates "chip-read," only data from the chip should be used in the transaction. If the terminal entry mode indicates "magnetic-stripe read," only data from the magnetic stripe should be used (not data from the Track 2 Equivalent Data on the chip).

3.17.3 Fallback to Magnetic Stripe at ATMs

The ATM shall always process the transaction using the chip if the chip is present and readable. The ATM should attempt to retry accessing the chip a number of times (minimum three) prior to falling back. If feasible, the ATM should attempt to restage the card in the chip reading station, or retract and re-land the chip contacts in order to complete the transaction.

Fallback to magnetic stripe circumvents the improved security offered by chip. Therefore, it is the issuers' discretion whether to approve or decline a chip card that has fallen back to magnetic stripe.

Note: Fallback may be optional in some countries. In these countries, if the chip is inoperable, the transaction is terminated. For details, contact your Visa representative.

Note: If an ATM has been upgraded to support EMV for some payment schemes but not for Visa, it should not identify the transaction as a fallback transaction. For these transactions, the value in the Terminal Entry Capability should be changed from '5' to '2' before the transaction reaches VisaNet.

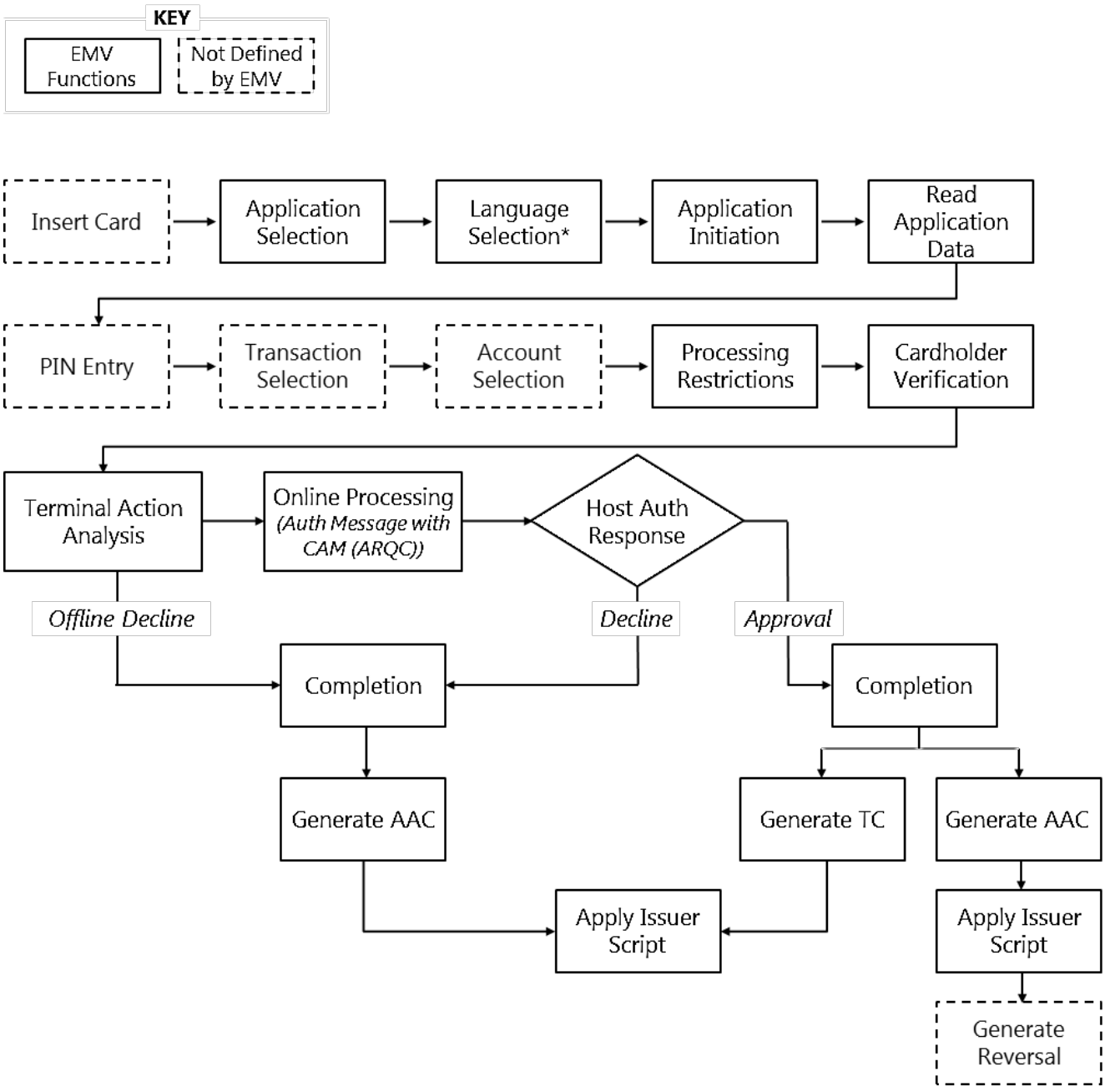
For additional information including the fields that must be populated to identify the transaction as Fallback, refer to Section 8.4: Fallback Processing.

3.17.4 EMV Transaction Flow at ATMs

The EMV flow at an ATM follows a similar path to that of a POS transaction, and as outlined in Section 3.7 and Section 3.8.1, with the key difference that ATMs are not required to perform Offline Data Authentication and the only applicable CVM is Online PIN.

There are, however, some subtle differences in some of the other supported functions such as Terminal Action Analysis and some additional non-EMV processes that are required to ensure a successful transaction. The following sections outline the functions that are different to POS processing. Otherwise, all other functions are performed similarly to online-only POS devices.

Figure 3–2: Sample EMV Flow at ATMs



* Language Selection can be performed as an EMV function.

3.17.5 Language Selection

ATMs may offer the cardholder a choice of languages to be used. Traditionally, ATMs have offered a menu of all languages supported by the ATM and have allowed the cardholder to select the language to be used for subsequent messages.

EMV chip cards may contain a Language Preference data object (accessed as soon as the Application Selection process begins) which contains up to four (4) languages in order of preference. Use of EMV functionality for Language Selection allows the ATM to quickly shift to a language most familiar to the cardholder. If the ATM, however, allows for the cardholder to select the language prior to reading the language preference from the chip, then that language should be used for the remainder of the transaction (as opposed to performing language selection again when the language data is read from the chip).

An ATM using EMV functionality to support multiple languages shall compare the card's Language Preference with the languages supported by the ATM. If a match is found, the language with the highest preference shall be used in the messages displayed to the cardholder. If no match is found and the ATM supports more than one language, the ATM shall allow the cardholder to select the preferred language at the beginning of the transaction.

Local requirements and laws may affect the display of multiple languages.

3.17.6 Cardholder Verification

For all ATM transactions, the CVM must be Online PIN. No other CVM is allowed even though the card's CVM list may contain other entries. If ATM transactions are allowed by the EMV Processing Restrictions check, but the CVM list on the card does not contain Online PIN, the ATM is allowed to prompt for Online PIN. In this case, the relevant TVR bits will not be set.

3.17.7 Terminal Action Analysis

If a Terminal Verification Results (TVR) bit is set (as a result of processing) and the corresponding IAC/TAC—Denial bit is set, the ATM will decline the transaction. The only relevant setting for ATM transactions is "Service Not Allowed". If the card does not allow usage at an ATM, the ATM should display an appropriate error message, such as "This card does not permit ATM usage."

As an online-only device, the ATM should process Terminal Action Analysis as outlined in Section 3.18.4: Terminal Action Analysis.

3.17.8 Offline Declined ATM Transactions

In certain instances, an ATM may decline a transaction offline rather than send it online. This may happen if the issuer has set the IAC-Denial bit corresponding to "Service Not Allowed" and the Application Usage Control (AUC) in the card is set to not allow the card to be used at an ATM. In this case, the ATM will request an AAC in the first GENERATE AC command resulting in a declined transaction.

3.17.9 Non-EMV Processes

Processes that are not defined by EMV such as Transaction Selection or Account Selection may be executed at any appropriate time.

Transaction Selection allows the cardholder to select the type of transaction that is to be performed. Choices typically include cash disbursement, balance inquiry, and funds transfer or other functions provided by the acquirer. As noted previously, Cash Disbursement is the transaction type currently covered by the EMV specifications.

Account Selection must be supported for chip just as it is for magnetic stripe. Although not part of the EMV processing flow, Account Selection will generally follow Application Selection (and Transaction Selection). Account Selection allows the cardholder to select one of the multiple sources of funds associated with the primary account. For example, these accounts might include:

- Checking Account
- Savings Account
- Credit Card Account

Some domestic implementations may base account selection on domestic/proprietary information read from the chip.

Online PIN entry is also not defined in the EMV specifications. Online PIN entry may occur at any point in the user interface flow prior to Online Processing.

3.17.10 Transaction Chaining

ATMs often support Transaction Chaining, where a transaction is completed by offering another service. In this way, cardholders can complete several transactions without retrieving and re-inserting their cards.

The important considerations for Transaction Chaining are:

- Although the card does not need to be retrieved and reinserted, the cardholder must be requested to re-enter his/her Online PIN and the PIN must be successfully validated before the chained service can be carried out. This helps to ensure that the rightful owner of the card is conducting the subsequent transaction.

- During an EMV session (Cash Disbursement), following contact activation (energizing the contacts), Application Selection to build the candidate list is the first step.
- If an EMV transaction follows a proprietary transaction that has used non-EMV commands to communicate with the chip, the contacts shall be deactivated/reactivated and Application Selection will then follow. If a proprietary application follows the EMV transaction, this can be performed without contact deactivation.
- The AID selected for the first transaction can be retained and used to select the application for subsequent transactions. However, the cardholder should be prompted to ensure they wish to continue using the same application.

3.17.11 Non-Cash ATM Transactions

ATMs generally support other financial management transactions such as balance inquiries and transfers, as well as customer-specific transactions offered by the acquirer. Visa EMV functions that extract information, request identification, or perform authentication can be used to complete these transactions. Transaction types supported on the Visa/Plus ATM network should follow the full EMV processing flow. Currently, the Visa/Plus ATM network supports Cash Disbursements, Funds Transfers, Balance Inquiries, and Shared Deposits (Plus only). Transactions not supported by the Visa/Plus ATM network are not considered Visa EMV transactions.

Transactions using EMV functions must follow all relevant EMV requirements. EMV functions should be executed in the same order as for Visa transactions (i.e., non-Visa transactions using EMV functionality should follow the EMV transaction flow).

Important: Non-cash transaction types at ATMs, such as Balance Inquiries, Deposits, and Funds Transfers can use EMV functions and will normally be initiated using the EMV chip. However, they will normally complete with an AAC, rather than a TC.

The basic features of non-cash disbursement transactions follow:

- **Amount**—Non-cash disbursement ATM transactions will have the Cryptogram Amount (as well as the transaction amount) set to zero.
- **CVM**—CVM processing will proceed identically to cash disbursement transactions with Online PIN used as the CVM.
- **Application Usage Controls (AUC)**—AUC controls will be evaluated in the same manner as an ATM cash disbursement (unattended cash).
- **Online Processing**—The device will always request an ARQC and will always go online. If the issuer responds with an approval, the associated function can be executed (balance displayed, funds transferred, etc.).

- **AAC as Final Cryptogram**—Unlike cash transactions, the final cryptogram requested will be an AAC regardless of the issuer approval or non-approval. Therefore, non-cash ATM transactions cannot be used to reset offline counters, unless specific PIN and card management transactions have been implemented. At this time, Visa does not provide global support for PIN and card management transactions, but does allow implementations in some countries.
- **Issuer Authentication**—Issuer Authentication may be performed, but the results cannot be considered in regards to execution of the related function. For example, if Issuer Authentication fails, an approved balance inquiry transaction will still result in display of the balance returned by the issuer.

Sales of goods and services, as well as related transaction types that support purchases, if performed at an ATM, fall under the rules and procedures for UCATs and are not considered ATM transactions.

Dispensing, or reloading, prepaid cards should be treated in an appropriate manner. If the prepaid card supports cash access, this is considered quasi-cash and should be managed as a cash disbursement. If the prepaid card does not support cash access, it can be treated as a purchase and UCAT rules will apply.

Misdispense

For a misdispense, the ATM acquirer must advise the issuer as follows:

- **Single-Message ATM Acquirers**—They must use an adjustment transaction with a message reason code to indicate that a misdispense has occurred.
- **Dual-Message ATM Acquirers**—They must process an ATM partial reversal for the actual amount dispensed if the misdispense is detected prior to the submission of the BASE II clearing record. If the error is identified after submission of the clearing record, the acquirer must reverse the original TC 07 and resubmit a new TC 07 with the actual dispensed amount.

Important: The adjustment transaction does not need to contain any chip data.

3.18 EMV in Online-Only Environments

Many merchants operate in a zero floor limit environment where, in most cases, transactions are sent online to be authorized by the issuer. Online-only devices are not required to support many of the EMV functions which are used for offline approvals, such as Offline Data Authentication.

Online-only devices follow a more streamlined EMV flow, using EMV mandatory functions as required. These devices will always attempt to send the transaction online by requesting an ARQC in the first GENERATE AC command. If online is not available, the device will request an AAC in the second GENERATE AC command.

Also, transactions may always be sent online 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 sections outline the EMV functions and processes which are different for online-only environments. Otherwise, other EMV functions are the same as outlined in previous sections.

3.18.1 Offline Data Authentication

Online-only devices are not required to support Offline Data Authentication. Since all transactions are sent online for authorization by the issuer, the ARQC will confirm to the issuer the authenticity of the card.

3.18.2 CVM Support

Online-only devices must support signature at a minimum. Optionally, these devices can support offline and/or Online PIN. Support for particular types of PINs may be may be necessary to meet domestic requirements. Acquirers should check with their Visa representative on local CVM requirements.

For the global minimum CVM requirements, refer to 6.5: Cardholder Verification Method Requirements.

3.18.3 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. The nature of online-only devices means that all transactions have to be approved by the issuer and the functions in Terminal Risk Management are not necessary.

3.18.4 Terminal Action Analysis

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

Note: "Service not allowed" is the only TAC-Denial setting for an online-only device because most of the other TAC settings focus on offline results, such as the outcome of Offline Data Authentication and Offline PIN processing which are not applicable to an online-only device.

An online-only device may perform or omit IAC-Online and TAC-Online processing and IAC-Default and TAC-Default processing. For IAC-Online and TAC-Online processing, if performed, the only relevant TVR setting for an online-only device is "Transaction value exceeds the floor limit". Because the floor limit is set to zero, the transaction always goes online and all other values in TAC-Online or IAC-Online are irrelevant.

The IAC-Default and TAC-Default processing, if performed, always causes a transaction to be declined if an online authorization could not be performed.

Visa strongly recommends that online-only devices omit the IAC-Online and TAC-Online processing and request an ARQC after IAC-Denial and TAC-Denial processing. If unable to go online, the device should request an AAC and notify the cardholder that the service cannot be performed due to communications failure. The device should not perform the IAC-Default and TAC-Default processing. The TAC values do not need to be present if the associated processing is omitted.

For the TAC values, refer to Section 7.2.2: Terminal Action Codes.

3.18.5 VSDC CA Public Key Support

Since online-only devices are not required to support Offline Data Authentication or Offline Enciphered PIN,[31] support for asymmetric keys is not required. The processes for loading and removal of VSDC CA Public keys as outlined in Section 6.9: Key Management are not applicable.

3.19 Visa Easy Payment Service (VEPS) Transactions

Transactions that qualify under the Visa Easy Payment Service (VEPS) program have specific requirements that device vendors need to ensure they meet:

- **Offline or Online Authorization**—VEPS transactions must be offline or online authorized:
  - Online transactions must contain a valid authorization code.
  - Offline approved transactions must indicate offline approval with an authorization response code of Y1 or Y3.
- **Chip Data and POS Entry Mode**—Chip data must be provided unaltered in the authorization message or in the clearing message for offline approved transactions and identified by a POS Entry Mode of 05.
- **No Cardholder Verification**—VEPS transactions do not require cardholder verification. Device vendors and acquirers 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.

[31] Offline Enciphered PIN is required in some countries.

- One way to manage this type of processing is via an EMV selectable kernel. When the device determines that the transaction qualifies for VEPS, it can invoke a different kernel configuration that only supports the "No CVM Required" CVM. This will allow the transaction to take place without cardholder verification (assuming the card supports the "No CVM Required" CVM in its CVM List). When the transaction does not qualify for VEPS, the device can use its standard kernel configuration where it may support signature, PIN, etc.
- Countries may also use the selectable kernel solution to facilitate PINless transactions that comply with local business requirements or regulations.

VEPS transactions may not be permitted in all countries or may not be permitted for some merchant categories. Check with your Visa representative.

3.20 Lower Voltage Card Migration

The release of low-voltage and multi-voltage payment cards will have minimal impact on the design of devices in the short term. The voltage of a device determines the voltage at which a card must be able to operate.

At present, all transaction acceptance devices must support 5V operation.

For further information, visit the EMVCo website.

4. Contactless Acceptance

This section provides an overview of the requirements and recommendations for devices that are compliant to VCPS and process Visa payWave transactions.

Visa offers two ways to conduct payment over the contactless interface:

- Magnetic stripe contactless payment (Magnetic Stripe Data, MSD)
- quick Visa Smart Debit/Credit (qVSDC)

Important: Global interoperability is achieved by requiring newly issued cards and newly deployed devices to support qVSDC.

The two approaches to contactless payment are briefly introduced in the following sections. This chapter also describes the processing steps for a contactless transaction and Visa recommendations relating to contactless readers (dongle, card reader, or other terminal device).

While MSD acceptance may currently be supported in some countries, Visa payWave acceptance is transitioning to qVSDC as the global standard. Acquirers and vendors should refer to their local Visa representatives for guidance on the Visa payWave acceptance requirements for specific regions.

Additionally, vendors developing products that support Visa payWave have the option of using the VCPS documents or alternatively the *EMV Contactless Specifications*, Book C-3. Acquirers and vendors can discuss their approach in more detail with their local Visa representative.

4.1 MSD

The MSD contactless transaction operates under magnetic stripe payment service rules according to Visa rules and regulations. As for magnetic stripe processing, routing for MSD transactions can be accomplished through the use of BIN routing logic.

MSD offers a magnetic stripe payment service using Track 2 Equivalent Data acquired from the chip (or Track 1 constructed from data acquired from the chip) over the contactless interface.

MSD operates under magnetic stripe payment rules and offers the following additional risk management features:

- MSD Legacy offers Dynamic Card Verification Value (dCVV), as defined by VCPS. MSD Legacy is defined in VCPS to support backwards compatibility with VCPS 1.4.2 cards and readers.
- MSD CVN17 offers an EMV strength application cryptogram.

While not EMV-compliant, MSD uses EMV methodology for selecting applications, initializing transaction processing, and reading records to obtain the application data. MSD uses a subset of EMV commands and requirements. MSD does not require all mandatory EMV data elements to be present in the card.

Note: Magnetic Stripe Image (MSI) is sometimes confused with MSD. MSI is EMV-compliant, and is the minimum implementation of VIS. MSI is not allowed as a contactless magnetic stripe solution.

4.2 qVSDC

qVSDC is based on EMV concepts and uses the existing Visa chip systems and rules of operation.

qVSDC reduces the reader to card processing time by minimizing the number of commands and responses that must be exchanged between the reader and the card. It offers an offline quick low value (LV) payment feature, Offline Data Authentication, and Online Card Authentication using the current Cryptogram Version Number 10, the minimized Cryptogram Version Number 17, or Cryptogram Version Number 18.

qVSDC uses the EMV methodology for selecting applications, initializing transaction processing, and reading records to obtain the application data. qVSDC uses a subset of EMV commands and requirements. The GET PROCESSING OPTIONS command response uses EMV Format 2, but is not fully EMV-compliant because it does not always contain the Application File Locator (AFL).

qVSDC does not require that all mandatory contact EMV data elements be present in the card or if present, that they be included in the card data that is read.

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

4.2.1 Fast Dynamic Data Authentication (fDDA)

qVSDC offers support for Offline Data Authentication using fDDA, which is similar to Dynamic Data Authentication (DDA), with the following differences:

- Generation of the dynamic signature is initiated by the GET PROCESSING OPTIONS command. The INTERNAL AUTHENTICATE command is not used and no DDOL is used.
- The results of fDDA are not provided online to the issuer within the TVR or protected by the online authorization or clearing cryptograms.

Using card and reader dynamic data, fDDA validates that card data has not been fraudulently altered and that the card is genuine and has not been created from skimmed data. In addition to signing the (reader) Unpredictable Number, which is signed in most EMV contact chip applications, fDDA also signs additional transaction dynamic data. The Amount, Authorized, Transaction Currency Code, and (card) Unpredictable Number are all signed using fDDA.

To optimize processing power and reduce transaction times, the fDDA dynamic signature is generated during the GET PROCESSING OPTIONS command, rather than generating the dynamic signature at the end of the transaction when the card may be moving away from the reader Radio Frequency (RF) field.

4.3 Global Interoperability

All newly issued Visa payWave cards and newly deployed readers are required to support qVSDC. While MSD support may be allowed for legacy programs in some countries, support for MSD is not recommended as its use is prohibited in some countries and may be in a sunset phase in others.

As part of our efforts to improve interoperability and payment security, Visa is committed to the eventual migration of all contactless payments away from MSD processing to more reliable and secure EMV-based qVSDC processing. Visa is currently evaluating time frames under which to establish a global sunset date for the contactless MSD processing path.

Table 4–1 describes the possible interactions between contactless cards and readers.

Table 4–1: Summary of Possible Reader and Card Interactions

Reader Configuration	Card (supports qVSDC and MSD) Method Selected
qVSDC-only	qVSDC
qVSDC and MSD	qVSDC
MSD-only[32]	MSD

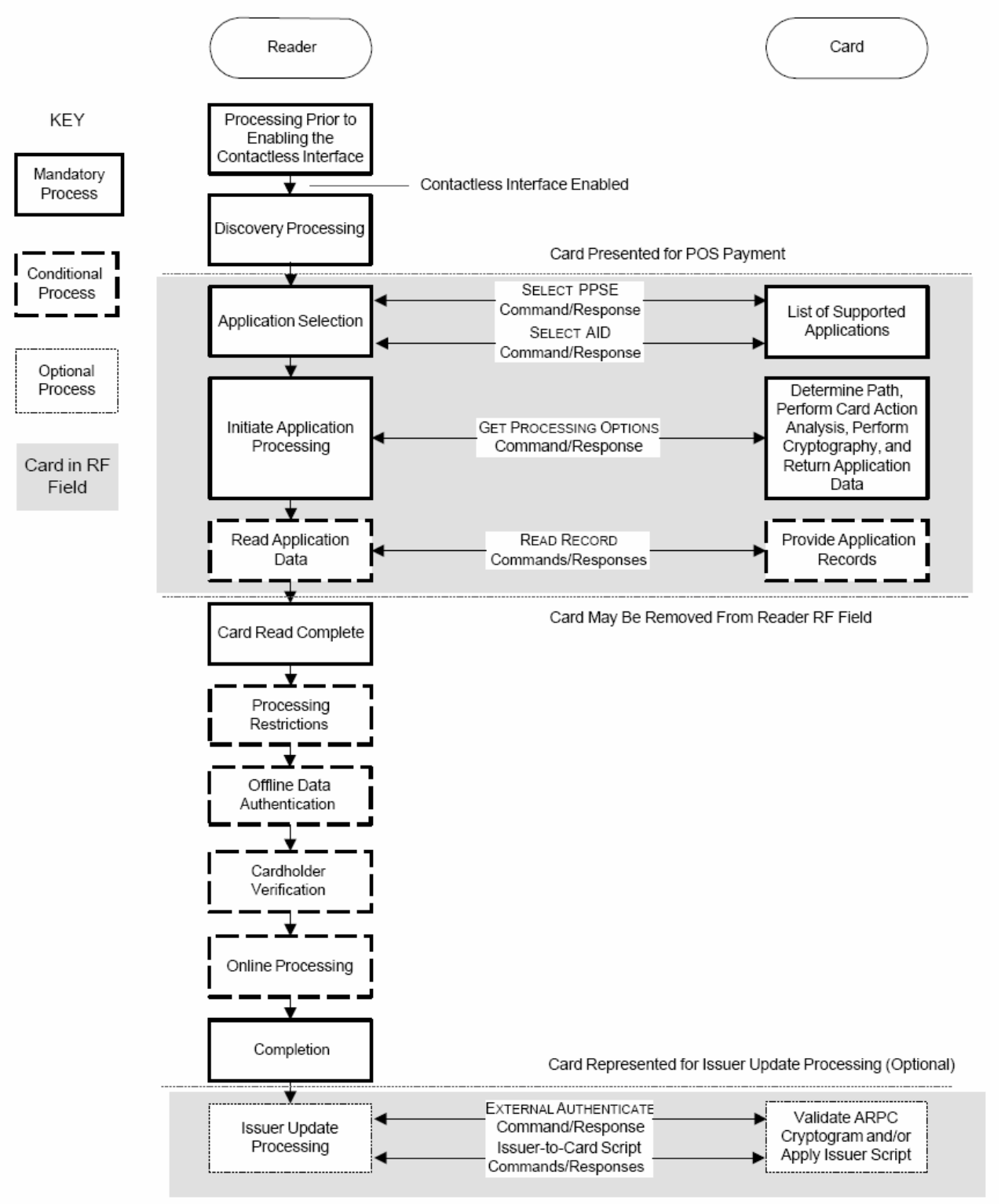
Visa requires that newly deployed devices comply with VCPS 2.1.x. or the *EMV Contactless Specification for Payment Systems,* Book C-3.

4.4 Processing Overview

This section provides an overview of a VCPS transaction. Functions are mandatory unless otherwise specified. Refer to VCPS for further details. Figure 4–1 is a diagram of a typical contactless transaction noting both MSD and qVSDC steps. Functions noted as Conditional are functions that are followed if the various conditions relating to the function are met. Functions that are noted as Optional are those which may be enabled at the discretion of the acquirer or due to local requirements.

[32] For legacy reasons and to accommodate special arrangements, some MSD form factors may exist in select countries. These form factors can be supported by readers that support qVSDC and MSD but not those that only support qVSDC. All newly deployed Visa payWave devices must support qVSDC.

Figure 4–1: Sample Contactless Transaction Flow Diagram



4.5 Initiating a Visa payWave Transaction

During a Visa payWave transaction, consumers briefly hold their Visa payWave card near the reader, when prompted, instead of inserting their card in the reader as with contact chip transactions or swiping the magnetic stripe. The Visa payWave card is embedded with an antenna and a chip. The chip, through the antenna, communicates with the merchant's contactless reader to enable the transaction. Acquirers should be aware that Visa payWave transactions may be initiated not only from a traditional plastic card but also from other contactless form factors and devices (e.g., NFC-enabled mobile devices and key fobs).

The transaction processing will then differ depending on whether it is a qVSDC or MSD transaction. The following sections outline the processing for each scenario.

4.6 qVSDC Transaction Flow

4.6.1 Preliminary Processing

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

During preliminary processing, the reader may use the transaction amount to perform the following checks:

- **Reader Contactless Transaction Limit**—Transactions for amounts above this limit are terminated and may be processed only by using a different interface. All new contactless readers must have this limit disabled or set to its maximum value[33] and this will become a requirement for all contactless devices at a later date.
- **Reader Cardholder Verification Method (CVM) Limit**—Transaction amounts above this limit require cardholder verification for the contactless transaction. This limit is normally set to the VEPS limit.
- **Reader Contactless Floor Limit**—Transactions above this limit require an online authorization by the card issuer. This limit is generally the same as the magnetic stripe and contact chip floor limits. For online-only countries, this limit is set to zero or is not supported by the reader.

The reader sets the results of these checks in the Terminal Transaction Qualifiers (TTQ), a reader data element. The TTQ provides the card with the reader's capabilities and requirements.

[33] This is a requirement in Visa AP and CEMEA.

4.6.2 Application Selection

Once the reader has completed Preliminary Processing, the reader signals to the consumer that the reader is ready for the contactless card. The cardholder briefly waves or holds the Visa payWave card close to the contactless reader to initiate the transaction. The reader determines whether it shares a contactless application with the card by selecting the card's list of contactless applications called the Proximity Payment Systems Environment (PPSE). If there is an application in common, that application is automatically selected; otherwise, the reader terminates the transaction and the transaction may proceed via another interface such as contact chip or magnetic stripe.

An Application Identifier (AID) is an identifier of the application. The reader compares the AIDs that it supports to the ADF Names in the PPSE on the card to determine which application to use for the transaction. The reader must contain the applicable Visa AIDs. Refer to Section 7.2.3: Application Identifiers for details.

Note: If there are two or more applications in common, the application with the highest priority can be automatically selected.[34] For example, a card may have both credit and debit applications, in which case the issuer or consumer will have defined one of those applications as a higher priority than the other.

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

4.6.3 Dynamic Reader Limits (Optional)

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

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

If a Program ID is returned by the card and it matches a reader Program ID (full or partial), the reader uses the reader limits associated with the matching Program ID to process the transaction.

[34] Special logic may allow selection of alternate AIDs as further described in the Sections 4.4.3, 4.5.1. and Appendices D and E of the *Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide* and the *Visa Reference on Application Selection for the U.S.*

For example, the default reader limits in Preliminary Processing may use a global reader CVM limit of $25, and the reader may have a Reader CVM Limit of $100 for domestic cards (as identified by the matching Program ID). In this case, the Reader CVM limit will be $100 for domestic cards and $25 for international cards.

DRLs may be mandatory in some regions and acquirers should confirm this with their local Visa representative. Acquirers should also confirm if there is an applicable Program ID for their country and acceptance environment.

4.6.4 Card Requests Terminal and Transaction Data

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

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

- Whether it supports qVSDC or MSD as well as whether it supports contact VSDC
- Whether it supports Signature, Online PIN, (Contact Chip) Offline PIN, and/or Consumer Device CVM

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

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

In qVSDC transactions, the card uses the information provided in the TTQ to make risk management decisions before responding to the reader. Visa does not require the use of a Transaction Certificate Data Object List (TDOL). As such Visa does not have a defined value for the default TDOL and vendors or acquirers may set the default TDOL to any value since it is not used for processing of Visa contactless transactions.

4.6.5 Fast Dynamic Data Authentication (Conditional)

fDDA is required for readers supporting offline transactions or for environments such as transit where the card needs to be authenticated before the transaction is authorized online. During fDDA, the reader verifies the dynamic signature returned by the card and authenticates data from the card.

Refer to Section 4.2.1: Fast Dynamic Data Authentication (fDDA) for more information.

4.6.6 Cardholder Verification (Conditional)

Cardholder Verification is required for readers implementing qVSDC. During Cardholder Verification, the reader determines the Cardholder Verification Method to be performed (if any).

The cardholder may be validated using one of the following methods:

- No cardholder verification. The cardholder does not have to provide a signature or PIN. For example, transactions that qualify for VEPS may take place without cardholder verification.
- Signature
- Online PIN
- Consumer Device CVM (CDCVM)

Note: A CDCVM is a CVM performed on the consumer's payment device independent of the reader. For further information see Section 6.4: Consumer Device CVM (CDCVM).

4.6.7 Transaction Terminated

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

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

4.6.8 Online Processing

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

The reader sends the data from the transaction including the cryptogram, information regarding the selected application, and the interface used together with standard transaction data to the acquirer. The acquirer then formats the corresponding VisaNet authorization message including the relevant data fields with the additional chip data sent in V.I.P. Field 55.[35]

[35] 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.

During a qVSDC transaction, the issuer, or Visa on the issuer's behalf, validates the card using the appropriate Cryptogram Version Number.[36] Based on the results of Online Card Authentication, along with other standard risk management checks (such as ensuring that the card is not expired, and verifying that the account is in good standing and has available funds), the issuer either approves or declines the transaction in the authorization response.

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

4.6.9 Transaction Outcome

The reader conveys the issuer's authorization response by displaying whether the transaction is approved or declined. If approved, depending on Visa and domestic rules, the transaction may not require a cardholder signature or a receipt. If the transaction is approved, this includes capturing the cryptogram and the associated data are captured and later submitted as part of clearing and settlement.

4.7 MSD Transaction Flow

MSD support may be allowed for legacy programs in some countries, but it is not recommended. Its use is prohibited in some countries and may be in a sunset phase in others. If support for contact chip is already present, restricting support to the qVSDC path for contactless will simplify the contactless implementation.

MSD transactions follow magnetic-stripe processing and rules, with routing accomplished through the use of BIN routing logic, except that they may include enhanced Online Card Authentication using CVN 17. Depending on local requirements and rules, transactions below a certain defined value may not require cardholder verification (signature or Online PIN) or a receipt. Regional rules and requirements define the cardholder verification method for particular transactions. Acquirers should contact their Visa representative for specific information.

The following sections outline the steps involved in a MSD transaction.

[36] Current Cryptogram Version Numbers include CVN 10 ('0A'), CVN 17 ('11), CVN 18 ('12'), and CVN '43'. Acquirers are not required to perform any analysis related to the Cryptogram Version Number; they should simply pass the cryptogram to VisaNet/issuer for processing.

4.7.1 Application Selection

Unlike qVSDC, MSD readers do not support preliminary processing but otherwise Application Selection is very similar.

First, the reader determines whether it shares a contactless application with the card by selecting the card's list of contactless applications (the PPSE). If there is an application in common, that application is automatically selected. If there are no applications in common, the contactless transaction is terminated and the transaction may proceed via another interface (magnetic stripe or contact chip).

In the event that there are two or more applications in common, the application with the highest priority is automatically selected. For example, if a card contains both a credit and debit application, the issuer defines one of those applications with a higher priority and the higher priority application is automatically selected.

The reader compares the AIDs that it supports to the AIDs in the PPSE on the card to determine which application to use for the transaction. The reader must contain the applicable Visa AIDs.

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

4.7.2 Card Requests Terminal and Transaction Data

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

The information includes the transaction amount, the reader's capabilities and requirements in the Terminal Transaction Qualifiers and other transaction data. The card uses the TTQ to ascertain the capabilities of the reader including whether the reader supports MSD CVN17. After reviewing the TTQ, the card completes its part of the MSD transaction by sending data to the reader such as the Track 2 data. The reader then indicates to the cardholder that the card can be removed from the reader's field.

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

4.7.3 Cardholder Verification (Conditional)

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

- No cardholder verification. The cardholder does not have to provide a signature or a PIN. For example, transactions that qualify for VEPS take place without cardholder verification.
- Signature
- Online PIN

4.7.4 Online Processing

The reader sends the data from the transaction including the cryptogram to the acquirer. If the transaction is to be routed to VisaNet, the acquirer then formats the corresponding VisaNet authorization message including the relevant data fields such as the PAN Sequence Number in V.I.P Field 23 (when returned by the card) and the additional chip data in V.I.P Field 55.

Note: For MSD transactions where a MSD legacy card was used, Field 23 and Field 55 are not sent.

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

4.7.5 Transaction Outcome

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

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

4.8 Visa payWave for Mobile

From an acceptance perspective, mobile devices containing a Visa contactless payment application can be accepted in any version of contactless readers that are developed to different versions of the *Visa Contactless Payment Specification* (VCPS) such as VCPS 1.4.2, VCPS 2.0.2, and VCPS 2.1.x. However, only readers developed to the VCPS 2.1.x are able to accept the Consumer Device CVM (CDCVM) as a recognized Cardholder Verification Method (CVM). CDCVM is a CVM type performed and verified on the consumer's payment device (usually a mobile handset), requiring no additional action by the reader.

Visa payWave transactions that originate from mobile devices have the same processing requirements as Visa payWave transactions that originate from cards. There is no difference between a card and a mobile Visa payWave transaction from the point of view of the transaction processing, authorization, and settlement data that is passed through V.I.P. and BASE II systems.

Acquirers can obtain more information from their Visa representative.

4.8.1 Pre-tap and CDCVM

Although a contactless transaction is normally completed with a single presentment of the contactless payment card, when the consumer's payment device is a mobile handset, the initial presentment of the mobile handset may result in what is referred to as a "pre-tap." A pre-tap is defined as the first presentment of the mobile handset to the reader wherein the mobile handset requires some consumer interaction to complete the transaction. For example, this may occur when a CDCVM is required for the transaction and one has not yet been performed. After the consumer interaction has been completed, the mobile handset is re-presented to the contactless payment reader to conduct the payment transaction.

Note: Pre-tap and CDCVM as a recognized Cardholder Verification Method are supported by readers compliant to VCPS 2.1 and above.

The following is a description of the processing flow when a CDCVM is required and was not performed by the cardholder prior to presenting the mobile handset to the contactless reader:

1. The mobile handset 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:
    - Mobile handset is configured to require a CDCVM for every transaction. This may be the result of cardholder or issuer configuration settings.
    - CVM was required for the transaction and CDCVM is the common CVM supported by both the mobile handset and the contactless reader. Note that the CDCVM is performed and verified entirely on the mobile handset. No additional action is required of the merchant to capture CVM, unlike with Signature and Online PIN.
2. The mobile handset sends an indication to the contactless reader that some form of consumer interaction is required to complete the transaction (that is, a pre-tap has occurred). This indication is conveyed by the mobile handset by sending a GET PROCESSING OPTIONS (GPO) response with Status Word = '6986'.
3. Upon receipt of this indication, the contactless reader displays a message instructing the cardholder to consult their mobile handset for further instructions, and after a short duration (usually a couple seconds), the contactless reader returns to Discovery Processing to await the re-presentment of the mobile handset to reattempt the transaction.
4. Once the cardholder has performed the necessary action on the mobile handset (e.g., successfully performed a CDCVM), the cardholder re-presents the mobile handset 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, following is a description of the processing flow when a CDCVM is required and was performed by the cardholder prior to presenting the mobile handset to the contactless reader:

- The mobile handset is presented to the contactless reader, the mobile handset determines that a CDCVM is required to complete the transaction and that a CDCVM has already been performed, and the transaction is completed.

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

4.9 Reader User Interface Recommendations

Since contactless cards are generally new to the market, it is important that the process of the cardholder presenting their card for use at the merchant is made as easy and intuitive as possible. To avoid confusion, it is also important to have a consistent way to inform the cardholder about when and where to present their card and when to remove it.

EMVCo has developed a set of user interface recommendations that provide best practices on how to design a reader 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 Specifications.
- The reader should support a standard set of display messages. The EMV specifications provide a suggested set. The messages may also be complemented by corresponding visual and audio indications.

Certain regions will also have specific user interface requirements and it is important to contact the local Visa representatives to confirm local or regional requirements in this regard.

The best practices outlined in this section are noted in greater detail in the *EMV Contactless Specifications for Payment Systems—Book A*, which can be obtained from EMVCo.

4.10 Contactless Processing for Industry Specific Transactions

The following sections provide some guidelines and best practices on how to handle specific industry transaction scenarios where a contactless card is used at a contactless device. Appendix D: EMV Tag to VisaNet Data Element Mapping provides information on how to map EMV data elements mentioned in these sections to the VisaNet (V.I.P. and BASE II) messages.

4.10.1 Pre-Authorizations

If an authorization takes place before the final amount is determined, then it is known as a pre-authorization; pre-authorizations are subject to payment system rules. The amount presented to the card in the GET PROCESSING OPTIONS command of a pre-authorization should be an estimated amount and should be the same amount and currency that is sent to the issuer in the authorization request message (if required). MSD merchants may present a zero for the Cryptogram Amount, while using the estimated amount in the authorization message itself. Note that in unattended environments, this estimated amount is likely to be the maximum dispensable value of goods or services.

The Pre-Authorization process will perform all the VCPS functions and the online request message (if generated) should contain all the appropriate contactless chip data elements. The card and device interact in an identical fashion to the purchase process, including CVM processing. The appropriate contactless chip data elements from both the Pre-Authorization request and response should be retained for the Sale Completion transaction. These elements include the TC or ARQC. The full Track 2 data should not be retained (in line with Payment Card Industry Data Security Standard (PCI DSS)) but the PAN and expiry date will be required. If a pre-authorization is performed without the card being present, the introduction of VCPS has no impact and existing practices should continue.

4.10.2 Sale Completion

A Sale Completion is the financial settlement of a previously pre-authorized transaction, often where the cardholder and card are no longer present.

The final transaction amount may differ from the pre-authorized amount, within a range defined in the Visa rules by country. Where a cryptogram and its associated data are provided in clearing,[37] the retained contactless chip data elements from the associated Pre-Authorization transaction, including all fields needed to validate the cryptogram, should be populated into the clearing message. It is recommended that the authorization approval code from the original pre-authorization response message (as opposed to those obtained from incremental authorizations) be used in this message as this code will generally be for the highest value.

The Sale Completion will contain an ARQC for online approved transactions or a TC for offline approved transactions.

[37] In some instances, the cryptogram data is not required in clearing.

4.10.3 Deferred Authorizations

Deferred Authorization is where an online authorization is performed after the card is no longer available, typically because the device temporarily does not have a connection (i.e., communications failure or device is on a transit vehicle) or the amount is over the floor-limit and the device has no online capability. The acquirer is at risk for those transactions that are subsequently declined, or if cleared, is liable for these transactions in the event that they are charged back for no authorization. Note that submission of unauthorized transactions into clearing may not be allowed in some countries, such as in the U.S.

Deferred Authorization is the recommended process for dealing with temporary outage situations. Where the environment supports offline authorization, Deferred Authorization can be supplemented with offline approvals for transactions under the floor limit. (Note that offline approvals for a transaction over the floor will still leave the acquirer liable for chargebacks for no authorization.)

In a zero-floor limit (always online) country, an ARQC is requested and retained for the subsequent authorization request. In a country supporting offline approvals, a TC may be requested for under-floor-limit transactions.

Deferred Authorization requests that receive an approval may be cleared. Those that do not must be discarded. Transactions in a non-zero-floor-limit environment that received a TC may be cleared.

4.10.4 Acquirer Stand-in

Acquirer stand-in (also called authorization truncation) may be done because the acquirer or the device temporarily does not have a connection (communications failure) or the acquirer deems the risk of chargeback to be less than the cost of authorization. The acquirer “stands in” for the issuer and returns a positive authorization response. However, because the acquirer does not have the issuer’s authorization decision criteria, the acquirer is liable for these transactions in the event that they are charged back for no authorization

4.10.5 Status Check and Account Number Verification

In a card present environment, VCPS functions such as Offline Data Authentication (fDDA, if supported by the card application) can be used to validate a card against the possibility of counterfeit. However, offline validation will not protect against lost and stolen, nor can it ensure that funds are available.

Status Checks (an authorization request for a single unit of currency was traditionally invoked to validate that the card used to make a reservation, or to pay for goods in advance of delivery is authentic. In a card present environment, VCPS functions such as Offline Data Authentication (fDDA, if supported by the card application) should be sufficient to ensure a card is not counterfeit (i.e., a non-VCPS transaction should be used and a status check may no longer be necessary). Except for a few specific merchant categories, if an online validation is desired, use of a Status Check has been replaced by an Account Number Verification (an authorization request for a zero amount).

4.10.6 Refunds

The recommended method for performing a contactless refund is to start a contactless transaction and follow the normal VCPS transaction flow in order to obtain the Track 2 Equivalent Data field from the contactless chip. An ARQC should be requested.

MSD merchants may present a zero for the Cryptogram Amount. For qVSDC merchants, if the PDOL indicates that the transaction type is to be included in the GET PROCESSING OPTIONS command, the terminal should send the transaction type as '20' and should use the refund amount. If the transaction type is not requested, the Cryptogram Amount should be set to zero.

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

If an attempted contactless refund fails (for example, if the contactless chip cannot be read or contactless technology fails at some point in the transaction), the merchant should re-initiate the refund transaction either by using the magnetic stripe or by using Key Entry procedures (if available).

4.10.7 Reversals

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

The authorization reversal is an online message indicating the amount (the difference between the authorized amount and the dispensed amount) that is to be credited back to the cardholder’s account. No contactless chip data needs to be included in the authorization reversal.

In the settlement message, the Cryptogram Amount should contain the original estimated authorization amount, while the transaction amount should reflect the dispensed goods amount. In a single-message system, the original transaction will contain the estimated amount and the contactless chip data (including ARQC).

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

4.10.8 Cancellations

Cancellations may occur when a purchase or sale completion is aborted during processing or after processing and may occur due to a number of reasons. In all cases, initiation of a cancellation should result in the cessation of processing and clearing of any data elements.

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

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

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

Visa recommends that the device produce a receipt for the cardholder showing that the original transaction has been cancelled.

4.10.9 Referrals

A referral is intended as a fraud control tool for issuers to use when more information is needed to verify the identity of the cardholder prior to approving a transaction. A referral is not a transaction; it is an exception process for a purchase.

In most cases, the referral process involves a discussion between the cardholder and the issuer, and will result in a completely new transaction taking place once the issuer has lifted the authorization block.

4.10.10 VCPS Transactions using Magnetic Stripe Data

Visa payWave transactions performed as defined in the VCPS 1.4.2 specifications are referred to as MSD Legacy transactions. MSD Legacy transactions are processed identically to magnetic-stripe-read transactions, with the exception that the POS Entry Mode is set to 91.[38] All other data and processing is identical to a magnetic-stripe read (except that dCVV is used instead of CVV).

Note: VCPS 2.x products may perform MSD Legacy transactions to be backwards compatible with VCPS 1.4.2 products that are already deployed or issued.

[38] The Terminal Entry Capability for all transactions from these devices will be set to either 5 (contact support; may support contactless) or 8 (contactless support; does not support contact) depending on the capabilities of the device.

4.10.11 Non-VCPS Transactions Using VCPS Functionality

Similar to contact chip and EMV, it is possible to use VCPS functionality to undertake non-VCPS transactions. These transactions will use the VCPS functionality to obtain information from the card (such as the card number) and to also verify the validity of the card for identification purposes.

Various VCPS functions can be used in this case including Application Selection, Initiate Application Processing, Read Application Data, Online Processing, and Issuer Update Processing.

Transaction Amounts for these transactions should be set to zero and there are no clearing records. Non-VCPS transactions using VCPS functionality should follow the VCPS transaction flow and follow all relevant VCPS requirements.

POS balance inquiries and POS deposits are examples of non-VCPS transactions using VCPS functionality.

4.11 Contactless Transactions at ATMs

This section provides an overview of considerations for contactless ATM transactions. For details, refer to Appendix G: Contactless ATM Requirements.

4.11.1 Contactless ATM Transaction Processing

ATMs have some unique characteristics that need to be considered when performing contactless transactions. This section provides a summary of these items:

- **ATM Card Read**—Unlike contact-chip initiated and magnetic-stripe initiated transactions, contactless chip-initiated transactions do not require the card be inserted into the reader. Contactless cards may simply be presented to the contactless landing pad to initiate a contactless-chip transaction.[39]
- **Online Authorization**—ATMs are online-only devices; they will always go online for Cash Disbursement and Balance Inquiry authorizations.
- **No Offline Data Authentication**—Because transactions are always sent online, ATMs do not perform Offline Data Authentication.
- **No Pre-Processing**—Unlike typical POS contactless transactions, ATMs do not perform any Pre-Processing.

[39] This does not preclude implementations where the contactless card can be inserted into the ATM, with a contactless chip read occurring while the card is within the body of the ATM. However, requiring that the contactless chip card be inserted into the ATM may physically preclude the ATM from being able to accept contactless capable consumer payment devices that have other form factors (for example, mobile handsets, key fobs, wearables). For this reason, such an implementation is not recommended.

- **Online PIN**—The CVM is Online PIN and no other CVMs are currently supported for ATM transactions. Online PIN will **always** be requested regardless of the CVMs supported by the card. The Terminal Transaction Qualifiers (TTQ, Tag '9F66') data element on the ATM, however, must be configured to indicate that the ATM does not require a CVM for the transaction and that the ATM supports Signature, CDCVM, and Online PIN. This is done to ensure that the contactless card does not unnecessarily terminate the transaction.
- **Online Card Authentication**—Enhanced security is achieved by performing Online Card Authentication Method where an ARQC is generated by the chip and validated by the issuer as part of online authorization processing.
- **Processing Restrictions**—ATMs supporting contactless transactions may implement the ATM Offline Check to determine whether contactless ATM transactions are supported by the card, and if not supported, whether the issuer prefers ATM transactions for their cards to be switched to contact chip or declined offline.

  Note: The ATM Offline Check is strongly recommended in the Europe Region and optional in other countries. Check with your Visa representative.

- **Amount, Authorized**—The Amount, Authorized, also referred to as the Cryptogram Amount, is the amount sent from the ATM to the card for generation of the ARQC. In most instances, during a contactless ATM transaction, the amount of the transaction is not known at the time that the ATM sends the cryptogram data to the issuer so the Cryptogram Amount is usually zero. (If the amount is known, e.g., when performing a subsequent transaction using Transaction Chaining, the actual amount of the transaction, rather than a zero, is used.
- **Transaction Chaining**—ATMs often support Transaction Chaining, where a transaction is completed by offering another service. Re-tapping the card on the contactless landing pad is recommended for financial transactions and optional for non-financial transactions. For both financial and non-financial transactions, cardholders must re-enter their PIN.
- **No Data Mixing**—For implementations where transaction data can be read from multiple interfaces, the transaction data should not be mixed (e.g., when the data is read from the contactless interface, only data from that interface should be used on the transaction).

Other than what is described above, the ATM should only perform the minimum and mandatory Visa payWave functions required to send the transaction online using Online PIN.

Note: Sales of goods and services and related transaction types, if performed at an ATM, fall under the rules and procedures for UCATs and are not considered ATM transactions. The Processing Code will be 00 and an appropriate MCC other than 6011 (such as 6012, if the transaction is a purchase) should be used.

For details, refer to Appendix G: Contactless ATM Requirements.

4.11.2 Contactless ATM Processes Not Defined by VCPS

Processes that are not defined by VCPS such as Transaction Selection or Account Selection may be executed at any appropriate time:

- **Transaction Selection**—Transaction Selection allows the cardholder to select the type of transaction that is to be performed. Choices typically include cash disbursement, balance inquiry, and funds transfer or other functions provided by the Acquirer.
- **Account Selection**—If Account Selection is supported, Account Selection must be supported for contactless chip just as it is for magnetic-stripe. Although not part of the Visa payWave processing flow, Account Selection will generally follow Application Selection (and Transaction Selection). Account Selection allows the cardholder to select one of the multiple sources of funds associated with the primary account (such as checking, savings, or credit card account).

Online PIN entry is also not defined in the Visa payWave specifications. Online PIN entry may occur at any point in the user interface flow prior to Online Processing.

4.11.3 Additional Contactless ATM Transaction Types

ATMs generally support other financial management transactions such as Balance Inquiries and Funds Transfers, as well as customer-specific transactions offered by the acquirer. Visa payWave functions that extract information or request identification or authentication can be used to complete these transactions. Transaction types supported on the Visa network should follow the full Visa payWave processing flow. Currently, the Visa network supports Cash Disbursements, Funds Transfers, Balance Inquiries, and Shared Deposits (Plus only). Transactions not supported by the Visa network are not considered Visa payWave transactions.

Transactions using Visa payWave functions must follow all relevant Visa payWave requirements. Non-Visa payWave transactions using Visa payWave functionality should follow the Visa payWave transaction flow.

4.12 Other Processing Considerations for VCPS

The following sections address other processing considerations for VCPS.

4.12.1 Forcing a CVM

Where a POS device is allowed to bypass CVM processing (i.e., merchant participates in VEPS) or where the ATM always forces Online PIN, the device will need to ensure the card does not unnecessarily reject the transaction.

This can be accomplished by indicating in byte 1 of the Terminal Transaction Qualifiers (TTQ) that both Online PIN and Signature are supported, and in byte 2 that CVM is not required. A new setting in byte 3 of the TTQ should also indicate that the contactless reader can accept a Consumer Device CVM (CDCVM).

The VCPS specifications provide more detail on the use of the TTQ.

4.12.2 Premature Card Removal

If the card is removed before the transaction is complete (i.e., the transaction has not reached Card Read Complete step), then the current transaction data is discarded and the reader returns to Discovery Processing.

4.12.3 Gratuities or Tips

Gratuities/tips may be handled as described in Section 3.15.5.

4.12.4 Placement of Contactless Readers

Visa has developed a set of recommendations as general guidance for the placement of contactless card reading devices in a merchant retail environment. They are intended to provide guidance to expedite contactless card reader integration into a merchant POS environment and ensure efficient operation. Refer to Appendix E: Placement of Contactless Readers, for more details.

4.12.5 Visa Easy Payment Service (VEPS) Transactions

Transactions that qualify under the VEPS program have specific requirements that device vendors need to ensure they follow.

- **Authorization**—VEPS transactions must be authorized (either online or offline):
  - Online transactions must contain a valid Authorization Code.
  - Offline approved transactions must indicate offline approval with an Authorization Response Code of Y1 or Y3.
- **POS Entry Mode**—Chip data must be provided unaltered in the authorization message or in the clearing message for offline approved transactions and identified by:
  - POS Entry Mode 07 (for qVSDC).
  - POS Entry Mode 91 (for MSD).
- **qVSDC Reader CVM Required Limit**—The Reader CVM Required Limit should be set to the VEPS limit.[40] With this configuration, the reader will require a CVM for transactions above the VEPS limit, and will not require a CVM for transactions below the VEPS limit.

  Note: qVSDC readers may support a feature called Dynamic Reader Limits (DRL), allowing the reader to support multiple CVM limits. These qVSDC readers may be configured with a Reader CVM Required Limit for domestic transactions and a different Reader CVM Required Limit for international transactions. In this scenario, the Reader CVM Required Limit for domestic cards should be set to the VEPS country limit[41] and the Reader CVM Required Limit for international cards should be set to the VEPS international limit.[42]
- **MSD**—For MSD transactions, handling of VEPS is performed in exactly the same manner as for physical magnetic stripe transactions (i.e., when the amount is equal to or below the VEPS limit, the transaction may take place without cardholder verification or a receipt).

Device vendors and acquirers should consult with their local Visa representative for the best approach in their region.

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

4.12.6 Dynamic Currency Conversion (DCC)

Dynamic Currency Conversion (DCC) is described in Section 2.16: DCC may be performed for Visa payWave transactions, subject to the rules and recommendations outlined in that section.

Note: DCC is permitted for POS transactions in both card present and card absent environments, and is not allowed at ATMs in Visa Inc. regions in accordance with the *Visa Core Rules and Visa Product and Service Rules*. The Europe Region has separate rules for DCC.

If and when DCC is performed for Visa payWave, this section describes the procedures to be performed, in order to minimize the number of the times the card is presented to the acceptance device:

1. The cardholder presents the Visa payWave card to the acceptance device, transaction data is exchanged between card and acceptance device (including any amount and local currency information requested by the card), and the cardholder removes the card.
2. The acceptance device determines whether the transaction is eligible for DCC and offers DCC to the cardholder.
3. If the cardholder accepts DCC, the acceptance device performs an online authorization and the online authorization message (and any subsequent clearing records) contains:
    - Converted amount in V.I.P. Field 4 and the cardholder's billing currency in V.I.P. Field 49.
    - Unconverted amount and the local currency, as used in the card-and-acceptance device interaction, in V.I.P. Field 55.

5. Magnetic Stripe Acceptance

This section provides an overview of the requirements for a transaction acceptance device that accepts magnetic-stripe cards.

5.1 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. For example, the cardholder may be required to press a function key to select the application or 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 point of service unless disallowed under the Visa rules and regulations or prohibited by local law.

5.2 Magnetic Stripe Data Processing

A device that accepts magnetic-stripe transactions must:

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

5.3 Service Codes

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

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

5.3.1 Service Code Values

For a description of the Service Code, refer to Appendix A: Track 1 Data Specifications and Appendix B: Track 2 Data Specifications.

The following outlines specific information for Service Code values:

- **2xx and 6xx**—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 chip enabled (2xx or 6xx). If the Service Code indicates that the card is 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, refer to Section 3.2.2: Fallback Acceptance for Chip Read Failures.
- **5xx and 6xx**—Service Codes 5xx and 6xx indicate that the magnetic stripe is restricted to domestic-use only. The device, however, does not necessarily know in which country the card was issued and is not required to do so.
- **x2x**—For transactions processed using data read from the magnetic stripe, Service Codes requiring online authorization (x2x) must be respected regardless of floor limit. Offline-only devices, or a device that is temporarily unable to send a transaction online, cannot authorize the transaction when the card's magnetic stripe is encoded with an x2x Service Code. A merchant could, however, complete the transaction by obtaining a voice authorization.
- **xx0, xx6, and x20**—A device that supports a PIN pad should use the Service Codes relating to PIN entry (xx0 and xx6) to determine if a PIN should be requested prior to initiating the online authorization. If an x06 (PIN, if PIN pad present) or x20 (PIN required) Service Code is read, the device should request PIN entry and transmit the transaction online. If the device is unable to process the transaction online, it should process the transaction as normal for an x06 Service Code or reject the transaction for an x20 Service Code.

Note: When discussing Service Codes, references to PIN mean Online PIN. An offline-PIN-only PIN pad (which is to be used for contact-chip transactions) is considered "PIN Pad Not Present" when evaluating the applicability of Service Codes. Also, if the acceptance device does not support PIN for Visa and Visa Electron, even if PIN is supported for other acceptance marks, the PIN pad is considered not present.

- **xx3**—POS devices processing transactions for amounts below the floor limit should ensure that the Service Code is not xx3, ATM only.

5.3.2 Service Code Not Recognized

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

5.3.3 Magnetic-Stripe Service Code Chargebacks

Magnetic-stripe transactions submitted into clearing without online authorization are subject to chargebacks for Service Code violation if the Service Code was ignored.

5.4 Visa Easy Payment Service (VEPS) Transactions

Merchants that meet specific qualification criteria may participate in the VEPS programs. On qualifying VEPS transactions, merchants are not required to perform cardholder verification and a receipt is optional, unless requested by the cardholder.

VEPS transactions that are completed with a magnetic-stripe card must be authorized online and contain a valid authorization code. The data transmitted in the authorization message must be full and unaltered with a POS Entry Mode of 90.

6. Security Characteristics

This chapter provides an overview of security requirements and characteristics relating to acceptance devices, such as PIN Entry Devices (PEDs), key management, and security best practices for mobile payment acceptance solutions.

Devices must be able to ensure the security of sensitive data, such as cardholder PINs and secret keys for symmetric algorithms, and to ensure the integrity of public keys for asymmetric algorithms. Similarly devices must ensure data security when cardholder data is transmitted over wireless networks or when used in mobile payment acceptance solutions.

EMVCo has produced the *EMV Acquirer and Terminal Security Guidelines* to assist acquirers with terminal security and acceptance processing. The document can be downloaded from the EMVCo website at www.emvco.com.

Additionally, acquirers and device vendors are required to comply with various requirements of the PCI Security Standards Council (PCI SSC) which owns, maintains, and distributes the PCI Data Security Standard (DSS), PCI PIN Transaction Security (PTS), and all their supporting documents. Various PCI requirements are outlined in this section and relevant PCI documentation is available from the PCI website at www.pcisecuritystandards.org.

6.1 Cardholder Verification Methods

The CVMs that may be supported by a transaction acceptance device are outlined in the following table:

Table 6–1: Allowable CVMs by Environment

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

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

The Visa rules and regulations allow some transactions to be performed without cardholder verification under certain conditions, such as VEPS transactions. Merchants that participate in VEPS need to take steps to ensure their terminals do not request a Cardholder Verification Method (i.e., signature or PIN) for qualifying transactions.

6.2 Signature

All attended devices must support signature. At attended devices, where a PIN has not been entered, the device must capture the cardholder's signature (either by having the cardholder sign the receipt or capturing it electronically using a touch screen and a pen-like device or stylus to write the signature) where CVM List processing requires it, unless the Visa rules and regulations allow an exception, such as for VEPS transactions. The merchant is required to compare the signature on the receipt with that on the signature panel of the card. If the two signatures match, the cardholder's identity is deemed to have been correctly verified.

Note: A contact chip card may require both PIN and signature for a given transaction.

If the transaction is verified and approved via a PIN, the terminal should state "Verified by PIN" or "PIN Verified" on the receipt in place of the signature line. However, 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. If signature is to be captured on a printed receipt and there is no signature line on the receipt, the merchant may collect the signature anywhere on the receipt.

6.3 Personal Identification Number (PIN)

PIN verification is performed by verifying the PIN entered at the point of transaction, either online by the issuer or offline using a chip card.

- **Online PIN**—When the PIN is to be verified online, the PIN is entered, encrypted, transmitted, translated, and verified against the reference PIN data available in the issuer's processing center or verified using the PVV method of verification (in which the cardholder's PIN entry is compared against a cryptographic transformation of the PIN). If the PINs match, the cardholder's identity is deemed to have been correctly verified.
- **Offline PIN**—When the PIN is to be verified offline, the PIN is entered and verified against the reference PIN stored on the card's chip. If the PINs match, the cardholder's identity is deemed to have been correctly verified.

The PIN requirements in this section apply only to VisaNet interchange transactions. Client financial institutions may develop and comply with their own standards for PINs used in on-us transactions.

Note: During a chip transaction, devices must use the PAN received from the chip application and not that encoded on the magnetic stripe when building PIN blocks.

The Visa *Transaction Acceptance Device Requirements* document and the Visa rules and regulations contain Visa's requirements for PIN entry. For more information on security characteristics and requirements, see www.visa.com/pinsecurity and www.pcisecuritystandards.org.

6.3.1 PIN Length and Character Set

The minimum PIN length is 4 digits. Visa specifies that ATMs and POS PEDs must be able to accept Online PINs of 4, 5, and 6 digits (and can accept up to 12 digits).

An ATM acquirer conducting business in the U.S. must be able to accept and transmit Online PINs that are 4 to 12 digits long.

Offline PINs may be between 4 and 12 digits long and are validated offline between the card and the device. Per EMV and VIS, chip devices must be able to handle Offline PINs with these lengths.

PEDs may visually indicate that a digit has been entered, such as with an asterisk (*). This visual indication should occur for each digit entered by the cardholder. For example, a PED should not display only four asterisks when six digits have been entered. Similarly, if audible tones are used, the tone should be generated each time that a digit is entered. The PIN character set is 0 to 9. For more information, refer to *PCI PTS*.

6.3.2 Online PIN

For devices such as ATMs and POS devices where Online PIN is supported, the PIN must be protected immediately upon entry by encryption in accordance to ISO 9564 and must be processed as specified in the *PCI PIN Security Requirements* and protected as specified in the *PCI PTS POI Modular Security Requirements*.

Online PIN entry may occur at any point in the user interface flow prior to online processing; the encrypted PIN may remain in the encrypting PIN pad (EPP) until needed for online processing.

Devices that support Online PIN entry should be constructed so that any tampering with the device stops it from working. See *PCI PTS* for additional details.

The process of entering an Online PIN for chip-initiated transactions is outside the scope of EMV processing. The use of a CVM that is not required by the card but is required by the Visa rules and regulations should have no effect on the TVR. If the result of CVM List processing is "cardholder verification was not successful", the corresponding bit should still be set in the TVR. Similarly, the "Online PIN entered" bit should not be set even when Visa rules and regulations require that an Online PIN be requested. For example, an ATM always requests an Online PIN regardless of CVM List preferences.

There are two situations where PIN capability specifically refers to Online PIN for Visa products:

1. **PIN Entry Capability**—An acquirer must only use PIN Entry Capability (V.I.P. 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.
2. **Service Code**—For transactions initiated via the magnetic stripe, the PIN settings in the Service Code only refer to Online PIN capability. **Note:** The Service Code value is not used during a chip transaction except to identify the card as a chip card via 2xx/6xx.

6.3.3 Offline PIN

When a device supports Offline PIN verification, a cardholder-entered PIN is compared 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 can be approved or declined offline or must be sent online for authorization.

The Offline PIN must be processed as specified in the EMV specifications and the *PCI PIN Security Requirements* and protected as specified in the *PCI PTS POI Modular Security Requirements*.

Offline PIN verification may occur in one of two ways:

- **Offline Plaintext PIN**—The chip reader sends the PIN to the chip as plaintext.
- **Offline Enciphered PIN—**Either the secure component in the device (for example, the chip reader) or the PIN pad itself enciphers the PIN, using an authenticated encryption public key from the chip. The enciphered PIN is sent to the chip, where the PIN is deciphered using the private key on the chip.

The encrypting PIN pad (EPP) and the chip reader are either integrated into a single device or configured as two separate devices (for example, using an external EPP). In addition, depending on device design, the PIN entered may either travel directly from the EPP to the chip reader within a secure environment or travel indirectly (via a tethered cable if some distance is involved) to the chip reader.

When the EPP and the chip reader are integrated and the PIN travels directly from the EPP to the reader within a protected environment as defined in ISO 9564-1, the PIN does not need to be encrypted at the point of entry.

When the environment from the PIN pad to the chip reader is unprotected (for example, via a tethered cable or a lengthy travel path), the EPP must immediately either encrypt the PIN at the point of entry using a Triple Data Encryption Standard (TDES) key or encipher the PIN using an appropriate RSA public key from the chip, before sending the PIN to the chip reader. This allows protection of the PIN during transport. For more information, refer to the *PCI PTS*.

For Offline Plaintext PIN, the EPP encrypts the entered PIN using TDES, sends the encrypted PIN to the chip reader, which decrypts the encrypted PIN, and sends the PIN to the chip as plaintext.

For Offline Enciphered PIN, one of two situations may occur:

- **Public Key**—The chip reader extracts the chip card public key and sends it to the EPP. The EPP enciphers the entered PIN using the RSA public key and sends the enciphered PIN to the chip reader. The chip reader sends the RSA-enciphered PIN to the chip.
- **TDES**—The EPP encrypts the entered PIN using TDES and sends the encrypted PIN to the chip reader. The chip reader decrypts the encrypted PIN using TDES and then enciphers it using the appropriate RSA public key from the chip.

All contact-chip devices placed in service that support Offline Enciphered PIN must also support Offline Plaintext PIN. It is strongly recommended that devices supporting Offline PIN support both plaintext and enciphered.

Offline PIN is not allowed for ATMs, which must support and transmit only Online PINs.

6.3.4 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 point of sale. 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. Refer to EMV v4.3, Book 4, Section 6.3.4.3 for more information on PIN Entry Bypass.

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 and device vendors should ensure their devices comply with local requirements.

6.3.5 Online PIN Retries

Certain transactions, such as ATM withdrawals or balance inquiries, may involve Online PIN retries by the cardholder following entry of an incorrect PIN. Acquirers may accompany the PIN retry with the same chip data as was sent during the first attempt, or they may restart the chip transaction for each PIN retry using the AID selected in the initial Application Selection process.

6.4 Consumer Device CVM (CDCVM)

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

Reader support for the CDCVM is mandatory for VCPS 2.1.x readers, as is indication of its support in the Terminal Transaction Qualifiers. In addition to supporting the CDCVM, the reader may then support other CVMs such as signature and/or Online PIN.

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

6.5 Cardholder Verification Method Requirements

The following table outlines the minimum global requirements for CVMs that devices must support by device type (M = Mandatory, O = Optional, – = Not Applicable or Not Allowed). 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 country.

Table 6–2: Global Minimum CVM Requirements by Device Type

	Attended POS			UCAT			ATM [43]
CVM	**Magnetic Stripe Device**	**Contact Chip Device**	**Contactless Chip Device**	**Magnetic Stripe Device**	**Contact Chip Device**	**Contactless Chip Device**	
No CVM	O	O	O	O	M (all new devices must support; all existing must support as of July 1, 2015)	M (all new devices must support; all existing must support as of July 1, 2015)	–
Signature	M	M	M	–	–	–	–
Online PIN	O	O	O	O	O	O	M
Offline Plaintext PIN	–	O	–	–	O	–	–
Offline Enciphered PIN	–	O (Must also support Offline Plaintext PIN)	–	–	O (Must also support Offline Plaintext PIN)	–	–
CDCVM	–	–	M (only applicable to VCPS 2.1.x devices)	–	–	M (only applicable to VCPS 2.1.x devices)	–

Note: If the merchant is a VEPS merchant and the transaction qualifies for VEPS, the merchant may optionally process the transaction without a CVM.

[43] The CVM requirements listed in this table for ATMs are only applicable when dispensing cash. ATMs may also dispense goods and services; in which case, they would adhere to the CVM requirements for UCAT purchases. In addition, an ATM may be configured to indicate support for other CVMs in addition to Online PIN to ensure acceptance of chip cards although these other CVMs will never be used for transaction processing; only Online PIN will be used.

6.6 PIN Entry Devices (PED)

A PED is any device at which a cardholder enters their PIN. It may have other functions. For example, to enter a loyalty program number. For a contact-chip device, it may contain an EMV kernel.

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. The PED must be protected against unauthorized removal as defined in *PCI PTS*.

A PED that supports Online PIN, Offline Plaintext PIN, or Offline PIN (both Offline Plaintext PIN and Offline Enciphered PIN) where the PED and chip reader are not integrated must contain an encrypting PIN pad (EPP) used for entering a cardholder PIN. The PED and EPP may be integrated, as in some standalone POS devices, or the EPP may be just one component of a PED, as in an ATM.

The following sections discuss the chip-reading device requirements for PEDs and PED testing requirements.

6.6.1 Chip-Reading Device Requirements for PEDs

Contact-chip devices should be capable of accepting a PIN for verification of Visa transactions. At a minimum, chip devices must be equipped with a port that can support a PED if the devices do not have a PED present.

If a PED is present and active, the chip device must use a PIN pad that meets Visa requirements. It must also act on the CVM List, except as specified in the Visa rules and regulations.

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

If the design of the device requires that parts of the device be physically separated (for example, 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.

When a device has a PIN pad that is not used for chip transactions (for example, 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 or Online PIN.

6.6.2 PED Testing Requirements

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

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

6.7 Terminal Security and Risk Policy

Acquirers should develop a terminal security and risk policy that considers the various issues associated with the deployment of terminals, 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 PCI.

6.8 Terminal Deployment and Management

Acquirers should develop a terminal deployment process which safeguards the use of the terminals and minimizes any potential misuse which may lead to interoperability problems or possible fraud. Acquirers should maintain an inventory of all their terminals and be able to identify each terminal uniquely, including its location and software version. This will ensure that any potential problems can be pinpointed and resolved in an expedited manner. This will also aid in replacing or upgrading terminals once their EMV kernels expire or require renewal.

EMVCo has outlined a set of guidelines in relation to deployment and management of terminals. Some of these guidelines are noted below:

- Acquirers should maintain an inventory of all the terminals from which they process transactions and should be able to identify each terminal uniquely, know where it is located, and which software versions it is running.
- Acquirers should establish a terminal management policy with merchants, such that terminal replacement and maintenance procedures are clearly defined.

- For terminals in exposed environments and especially those with a high level of staff turnover, such as garages and fast food outlets, acquirers should recommend to merchants to physically secure the terminals, using a lock under control of the site management. Information can be found in the PCI SCC document *Skimming Prevention Best Practices for Merchants* available from the PCI SCC website at www.pcisecuritystandards.org/security_standards/.
- Acquirers should review the *EMV Acquirer and Terminal Security Guidelines* document which is available from the EMVCo website for further details.

6.9 Key Management

Key management plays an essential role in integrating the components of a working security architecture. It provides critical security support to ensure the integrity of all cryptographic processes involved in card life cycle and transaction processing. The security of data is dependent upon the prevention of disclosure and unauthorized modification, substitution, insertion, or deletion of keys.

Key management requirements are described in the *PCI PIN Security Requirements* and in the EMV Specifications including EMV's security guidelines.

Sections 6.9.1 through 6.9.9 describe the symmetric and asymmetric key management requirements, the management of Visa Smart Debit/Credit (VSDC) Certification Authority (CA) Public Keys, and Issuer and ICC keys.

Important: Acquirers are responsible for ensuring that test keys are removed from terminals prior to production deployment.

6.9.1 Symmetric Key Management

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

TDES support is required for any device supporting Online PIN as well as for any device that uses DES encryption to transport an Offline PIN (both Offline Plaintext PIN and Offline Encrypted PIN) from the PIN pad to the card reader. Visa requires that all Online PINs (and Offline PINs where applicable) be protected with TDES.

6.9.2 Asymmetric Key Management

It is the acquirer's responsibility to ensure that VSDC CA Public Keys are loaded or deleted from devices that support SDA, DDA, CDA, fDDA, or Offline Enciphered PIN according to annually published Visa schedules.

To ensure sufficient levels of support for RSA key backup, key recovery, and key migration, offline-capable devices must be capable of securely storing six VSDC CA Public Keys and their associated data elements. A device should enable the secure loading, updating, and maintenance of the VSDC CA Public Keys. In this context, secure means that the keys should be protected from unauthorized modification.

Terminals supporting offline cryptography must be able to support key lengths up to 1984 bits. The current implemented lengths can be found on the EMVCo website at www.emvco.com and at the Visa technology partner site at https://technologypartner.visa.com. The 1984-bit key has been published, meaning that if all keys are installed at the time of deployment, the acquirer might not require any further key installation. However, acquirers should retain the ability to do so if required. Acquirers whose terminal base does not currently include all the keys must add the missing keys.

A device must be able to select the corresponding key and algorithm in conjunction with the RID and the Public Key Index (PKI) of the selected application. Planned updates and accelerated key revocations require that keys be updated in all devices. Unauthorized changes to the algorithms, keys, and insertion of an unauthorized key should not be possible. Devices must comply with the Visa and EMV requirements for withdrawal and introduction of the VSDC CA Public Keys.

6.9.3 Obtaining VSDC CA Public Keys

The VSDC CA Public Keys are available for public download from Visa's website, www.visa.com/pubkeys or at the *Visa technology partner site* at https://technologypartner.visa.com/Library/Specifications.aspx.
The websites contain the VSDC CA Public Keys via a link to an Adobe format (PDF) document.

Before an acquirer relies on the downloaded information (for example, by loading it onto the device population), it should check the information with a secondary source. Acquirers may check the *Visa Smart Debit/Credit Certification Authority Technical Requirements*. This document contains the current VSDC CA Public Keys, including a SHA-1 hash digest of each key, and explains how to validate the VSDC CA Public Keys against a secondary source.

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

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

6.9.4 Loading VSDC CA Public Keys

Visa does not mandate specific loading processes for the VSDC CA Public Keys and their associated data. EMVCo, however, provides some guidelines on this process (see *EMV ICC Specifications for Payment Specifications Book 2*) and acquirers and device vendors should ensure their processes comply with these guidelines. Acquirers should also periodically ensure the integrity of each key component, including the public exponent, the CA Public Key Index, and others.

Once loaded, EMVCo suggests that terminals should 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 terminal.

Since Offline Data Authentication and Offline Enciphered PIN are not supported at ATMs, there is no need to set up a public key management system to support ATM acquiring.

6.9.5 Planned Revocation of VSDC CA Public Keys

Once a Certification 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 Certification Authority Private Key.

Acquirers and device vendors must also ensure that any test keys that may have been loaded to undertake testing prior to production rollout are removed from the device.

6.9.6 Expired VSDC CA Public Keys

Based on developments at EMVCo, Visa periodically reviews and determines the expiration dates of the VSDC CA Public Keys. Acquirers' key management must support removal of expired keys from their devices based on the expiration and removal dates.

A Visa International Member Letter or Visa Business Review is sent to acquirers advising them of the planned expiration and removal dates. Generally, an 18-month grace period is provided to assist acquirers in these efforts.

6.9.7 Accelerated Revocation of VSDC CA Public Keys

Visa analyzes and determines if an accelerated or emergency key revocation is required due to public key attacks. Should this occur, clients are advised of Visa's findings and associated procedures. For more information, refer to the EMV specifications.

6.9.8 Managing VSDC CA Public Keys Distribution

To ensure the integrity of the VSDC CA Public Keys as acquirers are distributing them to their deployed device base, Visa has established the following principles:

- If the keys are being distributed across a communication channel that is not under the control of an acquirer, the receiving device should be able to authenticate the communication originating from the acquirer.

  Devices not on a private network should perform some kind of authentication. For example, manually updated devices require log in; remotely managed devices need to validate the device management system. This could be done with a cryptographic challenge or any reasonable validation method. The proprietary nature of device management systems and devices will likely result in the use of proprietary validation systems.

  Any time that a key is distributed across an uncontrolled channel when it is not possible to authenticate the acquirer or authorized agent, it should be validated against an alternate channel.

  Recipients should always double check the key against a secondary source.

- Valid keys should be delivered to the device in a manner that protects their integrity.

  Note: The primary purpose of this principle is to ensure that keys are not corrupted or modified during delivery and to ensure that their integrity is maintained. For example, the device could validate the key by checking a hash generated from the key such as SHA-1. Alternatively, the device management system could do the integrity validation using its own validation technique such as check sum as long as the device management system completely controls the software updates to the device.

- Ensure that new keys are loaded prior to the effective date.

  Note: All deployed devices should have new keys prior to cards being circulated. A manual or automated procedure should be in place to begin deployment of keys in sufficient time to ensure that all deployed devices accept cards with the new keys as they are issued.

- Ensure that expired or revoked keys are removed or disabled within 18 months of expiration or revocation.

  Note: As above, a manual or automated procedure should be in place to ensure that all keys are removed or disabled within 18 months of the expiration date.

- Within a reasonable timeframe, acquirers should be able to determine which VSDC CA Public Keys are active in each of their devices.

  Note: Acquirers should be able to report on the status of their installed device base to assure issuers that cards with new keys are 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.

6.9.9 Issuer and ICC Keys

Issuer and ICC keys, extracted during Offline Data Authentication and Offline Enciphered PIN processing, may have lengths up to 1984 bits. Devices must be able to support issuer and ICC keys that are not based on 8-byte boundaries. For example, a key may be 127-bytes long.

6.10 Data Security

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

6.10.1 Cardholder Data Security

When customers offer their cards at the point of service, they want assurance that their account information is safe. Cardholder data must be protected wherever it resides.

The Payment Card Industry Data Security Standard (PCI DSS) resulted from a cooperative effort among Visa, MasterCard, American Express, Discover, and JCB to offer a single approach to safeguarding sensitive data for all card brands. The PCI Security Standards Council (PCI SSC) owns, maintains, and distributes the PCI Data Security Standard (DSS) and all its supporting documents. Compliance with the PCI DSS is validated under two programs within Visa:

- Cardholder Information Security Program (CISP) for U.S.-based entities (www.visa.com/cisp)
- Account Information Security (AIS) for non-U.S.-based entities

Europe Region entities can find more information at: http://www.visaeurope.com/en/businesses_retailers/payment_security.aspx, while other non-U.S.-based entities can access http://corporate.visa.com/st/.

It is a requirement of Visa acquirers that they must ensure the compliance of their merchants and service providers to the PCI standards where they may store, process, or transmit Visa account numbers.

More information can be found at www.pcisecuritystandards.org/security_standards/.

6.10.2 Payment Application Data Security

Payment applications must not retain full magnetic-stripe data, Card Verification Value (CVV), Card Verification Value 2 (CVV2), or PIN data and must support a merchant's and agent's ability to comply with the PCI DSS.

Note: Payment Application-Data Security Standard (PA-DSS) compliant payment applications never handle unencrypted PIN data.

Merchants and agents using vulnerable payment applications are at heightened risk of compromise attacks. The PCI SSC adopted Visa's PCI Payment Application Best Practices and released the standard in April 2008 as the Payment Application Data Security Standard (PA-DSS).

Per Visa mandates, all new merchants must use payment application software that uses PA-DSS compliant applications or be PCI-DSS compliant. Acquirers must ensure that their merchants and agents use PA-DSS compliant payment applications. For purposes of the mandates, payment applications apply only to third-party payment application software that stores, processes, or transmits cardholder data as part of an authorization or settlement of a payment card transaction. POS devices are an example of this. PA-DSS does not apply to merchant or agent in-house developed applications, standalone hardware terminals, or PEDs. Payment application vendors must validate the conformance of their products to the PA-DSS. Acquirers should insist that their merchants and agents use compliant applications and upgrade or patch applications that cause the storage of sensitive cardholder data to meet the Visa mandates.

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

6.10.3 Data Processing and Transmission Security and Integrity

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

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 also comply with PCI requirements as outlined in previous sections.

6.10.4 Wireless Security

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

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

The PCI guidelines recommend the use of technologies such WPA2 or secure pairing for Bluetooth devices for encrypting and authenticating wireless LANs. Wireless networks are also considered to be public networks meaning all cardholder data must be encrypted as required in PCI DSS if it is to be transmitted over a wireless network. Encryption methods can include, but are not limited to, SSL/TLS, IPSEC, and WPA2-AES.

Further information can be found in the *PCI DSS Wireless Guidelines* supplement available at https://www.pcisecuritystandards.org/security_standards/documents.php.

6.11 Card Verification Value 2

The CVV2 is a card verification tool designed to reduce fraud losses on transactions. It consists of three digits printed either on the signature panel or on the card to the right of the signature panel.

Although CVV2 is primarily used for Card Not Present transactions (for example, mail order, telephone order, electronic commerce), in some countries, the CVV2 is also used in card-present transactions.

6.12 Random Number Generation

EMV devices are required to provide random 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 random numbers. Device vendors and acquirers should review the *EMV Acquirer and Terminal Security Guidelines* available from the EMVCo website for further information.

6.13 Security Best Practices for Mobile Payment Acceptance Solutions

Visa has developed a set of security best practices for vendors, merchants, acquirers, and service providers of mobile payment acceptance solutions. The goal of the recommendations is for vendors and service providers to design and implement secure solutions and limit exposure of account data that could be used to commit fraud.

Some of the best practices that vendors, merchants, acquirers, and service providers of mobile payment acceptance solution vendors should follow are outlined below. The *Visa Security Best Practices for Mobile Payment Acceptance Solutions* provides a full list and explanation of Visa's recommended best practices. These guidelines may be requirements in certain Visa regions. Acquirers should contact their Visa representative to determine whether these guidelines are requirements in their region.

Solution Vendors:

- Provide payment acceptance applications and any associated updates in a secure manner, with a known chain of trust.
- Develop mobile payment acceptance applications based on secure coding guidelines.
- Protect encryption keys that secure account data against disclosure and misuse, in accordance with industry-accepted standards.
- Provide the ability to disable the Mobile Payment Acceptance Solution.
- Provide functionality to track use and key activities within the Mobile Payment Acceptance Solution.
- Provide the ability to encrypt all public transmission of account data.
- Ensure that account data electronically read from a payment card is protected against fraudulent capture and use by unauthorized applications in a Consumer Mobile Device.
- Ensure chip acceptance devices are implemented correctly.
- Provide the ability to truncate or tokenize the Primary Account Number (PAN) after authorization, to facilitate cardholder identification by the merchant.
- Protect stored PAN data and/or sensitive authentication data.
- Provide security for Account on File Systems.

Merchants:

- Only use Mobile Payment Acceptance Solutions as originally intended by an acquiring bank and solution provider.
- Limit access to the Mobile Payment Acceptance Solution.
- Immediately report the loss or theft of a Consumer Mobile Device and/or hardware accessory.
- Install software only from trusted sources.
- Protect the Consumer Mobile Device from malware.

Acquirers and Payment Service Providers (PSPs):

- Provide the ability to uniquely identify a transaction coming from a merchant.
- Restrict manual PAN key-entered transactions on a Consumer Mobile Device to a minimum.
- Ensure appropriate due-diligence when on-boarding and monitoring merchants, including adequate Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures.
- Where network connectivity is available, ensure that all authorizations are processed online.
- Develop fraud-monitoring capability specifically for mobile payment acceptance.

Vendors, merchants, acquirers, and service providers should contact their Visa representative to obtain a copy of the best practices document. Best practice information can also be found at the following locations:

- http://usa.visa.com/merchants/risk_management/cisp_overview.html
- http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html
- http://usa.visa.com/download/merchants/bulletin-updates-pin-framework-111809.pdf

6.13.1 Security for Account on File Systems

Some solutions involve account data being captured and retained in a central system where this retained data can subsequently be used to authorize new transactions. With some services, a cardholder can make payments using the data stored on a central system through the use of credentials, such as passwords or tokens, to pay at the point of sale. A Quick Response (QR) code would be an example of a token. Such solutions must also comply with PCI DSS principles, if storing any card information.

In registering new card details, the solution should take steps to establish the legitimacy of the enrolling card/cardholder. If available, Verified by Visa and address verification checks should be performed as part of the registration process. The registration process should not occur on the merchant's mobile device.

When accepting payments, the solution should clearly provide a means to capture the cardholder's intent to make a payment.

Where tokens are used, tokens should be time-bounded and be revocable. Where possible, the solution vendor should take steps to limit the value of the stolen tokens for fraudulent users. For example, in a parking garage, the token could be bound to the cardholder's registered vehicle license plate. The registration of additional benefactors should follow a similar process to that of registering new card details with the solution.

For Account on File solutions, CVV2 must never be retained after initial authorization.

To avoid disruption in customer relationships due to Visa account information changes, when making Account on File based payments, solutions vendors should consider subscribing to Visa Account Updater (VAU), if the vendor's operating environment supports the solution. Acquirers and vendors should contact their local Visa representative to discuss possible use of the VAU service.

7. Device Management Systems

This section provides recommended functions to be supported by a device management system (also known as Terminal Management Systems or TMS) in a chip environment (contact and contactless). Device 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 device management system is, the easier it is to respond to future market needs, new requirements, and change requests.

7.1 EMV Functions

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

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

7.2 Data Elements

Although a complete device management system uses many data elements, only those that apply to contact and contactless chip devices are discussed here.

7.2.1 VSDC CA Public Keys

VSDC CA Public Keys are used to support SDA, DDA, CDA, fDDA, and Offline Enciphered PIN transactions. Device management systems should allow for six VSDC CA Public Keys.

Planned changes and accelerated key revocations require that keys be updated in all devices. Consequently, these data elements should be treated as variable parameters, not as components of the kernel. Post-deployment data integrity must also be verified. Failure to load the correct production VSDC CA Public Keys or a newly introduced key will result in failure to correctly process SDA, DDA or CDA which may lead to a declined transaction depending on the risk parameters setup in the card or the issuer host.

To ensure effective management of VSDC CA Public Keys, the device management system should:

- Download keys to devices prior to and after deployment
- Download new keys prior to their effective date
- Remove expired or revoked keys by the Visa published date

- Notify all deployed devices when a key is to be downloaded or removed
- Distribute keys to deployed devices in a manner that protects their integrity
- Maintain status of keys in deployed devices

Managing keys manually across a large device base can pose significant difficulties. The device management system should, therefore, 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 device management system. Alternatively, devices may regularly contact the device 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.

The secure distribution of keys to devices is critical to ensure that the keys are not corrupted during delivery. For example, a device could validate the keys by checking the SHA-1 hash. Alternatively, the device management system could validate key integrity by using its own validation technique as a check sum. Acquirers should ensure that the terminals detect and report unexpected modification of the key set.

For more information on updates and management of public keys, refer to Section 6.9: Key Management.

7.2.2 Terminal Action Codes

Used in Terminal Action Analysis, TACs are mandatory device data elements with values defined by Visa. They indicate the action that the device should take based on the TVR.

Note: For online-only devices (devices that process all transactions online), there are different TAC settings depending on whether the device supports TAC/IAC-Online and TAC/IAC-Default processing.

Table 7–1: Terminal Action Codes

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)[44]
Visa ISO AID	TAC Denial: x0010000000 TAC Online: xDC4004F800 TAC Default: xDC4000A800	TAC Denial: x0010000000 TAC Online: n/a TAC Default: n/a	TAC Denial: x0010000000 TAC Online: x584004F800 TAC Default: x584000A800
Visa U.S. Common Debit AID	n/a	TAC Denial: x0000000000 TAC Online: n/a TAC Default: n/a	TAC Denial: x0000000000 TAC Online: xFFFFFFFFFF TAC Default: xFFFFFFFFFF

[44] The TAC values in this column are defined for Visa Inc. countries; they are not applicable to the Europe Region.

The Visa TAC-Online and TAC-Default values are the hexadecimal representation of the minimum bit settings required by Visa. Acquirers may deploy TAC-Online and Default values in which additional bits are set. (This logic does not apply to the TAC-Denial value as this could result in unnecessary declines.)

The device management system should be set up to track and update the settings in the TACs through downline loads, when appropriate. Merchants must not be able to update the TACs. If the device does not have the correct TACs, the acquirer may be subject to compliance requirements as with any violation of the Visa rules and regulations, and may be subject to penalties as outlined in the Visa rules and regulations.

7.2.3 Application Identifiers

AIDs indicate the card applications that a device can support, such as Visa, Visa Electron, Plus, or a merchant loyalty program. All contact and contactless chip devices that include the Visa Debit/Credit AID must also include the Visa Electron AID, unless specifically excluded by the merchant.

For the list of Visa AIDs, refer to Section 3.3.1: Application Identifiers.

7.2.4 Random Transaction Selection Parameters

The parameters for random transaction selection define the percentage and threshold values used by devices that support both offline and online transactions. They are used specifically in the random selection of transactions to be sent online for authorization, independent of transaction characteristics.

For more information on random selection, see Section 3.9.2: Random Transaction Selection.

7.2.5 Floor Limits

In conjunction with the Visa-published floor limits for specific country and MCC combinations, the acquirer may set floor limits for chip and magnetic-stripe transactions. The chip card can request, however, that a transaction to be transmitted online for a transaction that is under the acquirer-established floor limit.

To provide maximum flexibility, devices and device management systems should support 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

For more information on floor limits, see Section 3.9.1.

Additionally, terminals supporting Visa payWave need to support the following contactless limits:

- Reader CVM limit
- Reader Contactless Floor Limit

For more information on contactless limits, refer to Section 4.6.1: Preliminary Processing.

7.2.6 Terminal Transaction Qualifiers (TTQ)

For devices supporting contactless transactions, the TTQ advises the Visa payWave card of the reader's requirements and capabilities for processing the specific transaction, including:

- Whether the qVSDC and/or MSD is supported
- Whether contact VSDC is supported
- What CVMs are supported
- Whether cardholder verification is required for the transaction
- Whether the reader supports Issuer Update Processing

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

7.2.7 Application Version Number

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

The current version of VIS is 1.5.0 which would be coded in binary as '0096'. Previous versions, 1.4.1 (binary '008D') and 1.4.0 (binary '008C') would also be acceptable. Version 1.3.2 (binary '0084') remains valid for older devices.

7.3 EMV Functionality Considerations

Visa recommends the best practices in the following sections for device management systems.

7.3.1 Mandatory Functionality for EMV Devices

The EMV specifications include mandatory requirements for all devices, classified by device type. These requirements may vary from device to device, but any individual device must support the minimum requirements for its type.

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

7.3.2 Configurable Functions

Devices can be configured to support different functionality depending on the environment they operate in, or to support a function or process is certain circumstances. There are two possible alternatives to support configurable functions: configurable kernels and selectable kernels.

Configurable Kernels

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

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

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

Selectable Kernels

A device may support selectable kernel configurations which means that the kernel configurations used at a single device may vary based upon characteristics of the transaction rather than being set at the time of device installation. The selection criteria logic must be checked to ensure that it selects the correct configuration. All selectable configurations must be EMV type approved. The configuration should be selected prior to the issuance of the Get Processing Options command so that the correct device information can be sent to the card, if requested in the PDOL. For examples on using a selectable kernel, refer to Section 3.19: Visa Easy Payment Service (VEPS) Transactions.

Visa recommends that acquirers consider the use of selectable kernels as a best practice since there is the potential for interoperability problems with configurable kernels if they are not configured correctly at the time of installation.

7.4 Resetting Terminal Clock

Preferably, EMVCo requires that devices have a clock with date and time which is either autonomous or updated based on online messages. The clock should be synchronized regularly to ensure it is accurate and any seasonal time shifts have been taken into account.

Vendors should preferably ensure that the terminal clock is reset with each host response or when polled for the collection of transactions for clearing and settlement. Integrated systems may have a central date and time that is distributed amongst a network of terminals. Any manual adjustment to the clock by a merchant should only be possible with authorization via methods such as key switch or a password.

The terminal clock should have a battery backup in the case where the terminal may lose power without resynchronization of the clock when the power is restored.

8. Acquirer Considerations

This chapter provides a brief overview of acquirers' unique responsibilities for chip infrastructure support to ensure that acquirers support Visa requirements and best practices for transaction acceptance devices.

8.1 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. Electronic signature capture is a growing practice in several countries. Country rules differ on electronic signature capture so acquirers should check with their Visa representative to determine local rules and requirements.

Visa rules and regulations require a device that captures electronic signatures to have proper controls in place to ensure the security of the stored signatures and other cardholder data in accordance with the PCI DSS. It must also store and reproduce a signature on only a transaction-specific basis, in relation to the transaction for which the signature was obtained, and must reproduce a signature only upon specific written request from the acquirer or in response to a retrieval request.

For more information, see Section 6.10.1: Cardholder Data Security.

8.2 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 may be allowed for Deferred Authorization transactions but only for the minimum time necessary to complete the transaction.

8.3 Deploying EMV-Compliant Devices

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

- When selecting software for devices, determine the EMV kernel identifier and review the listing of approved kernels at www.emvco.com. The later the version of specifications and test plan, the less likely that any in-the-field interoperability problems will arise.
- Only implement software that incorporates kernels based on EMV specifications 4.1 or later, preferably based on the latest specifications. A kernel based on earlier specifications (3.1.1 or 4.0) is more likely to have problems in the field.

- As interoperability problems are uncovered globally, new testing is put in place at EMVCo-accredited laboratories. Deployers should plan to refresh the software in their devices every few years to ensure that they have the latest fixes and functionality.
- 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.
- Deployers will need to have a means of updating public keys in their EMV devices.

Although this does not happen very often, it should be completed in a timely manner when needed.

- An automated device management system will make key and software updates much simpler and quicker to implement. Device management systems will also facilitate asset management, track errors, and report problem devices. The long-term benefits of device management systems will generally provide a positive business case for implementation. See Chapter 7: Device Management Systems for a further discussion of recommended functionality.
- With the emergence of new functionality such as authentication methods, deployers who do not use a flexible format for their device-to-acquiring-host messaging should plan to migrate to a format based on XML, TLV, or a similar flexible system. The length of variable length data elements may change over time (as new requirements are introduced), and so the flexible format should allow for the length of data elements sent in device-to-acquirer host messages to change/grow over time.

8.4 Fallback Processing

Acquirers should establish monitoring procedures to ensure Fallback levels are kept to a minimum. High levels of Fallback may indicate problems with a device or, alternatively, a need for further merchant education.

Visa has enacted a global monitoring program to identify acquirer/country combinations with high levels of international, and where applicable, domestic Fallback. Acquirers identified will need to take corrective action.

Fallback transactions can be identified by the following combination of values:

Table 8–1: Magnetic-Stripe Fallback Data Elements

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

Table 8–2: Key/Manual-Entry Fallback Data Elements

Field Location	Field Name	Value
V.I.P. Field 22	POS Entry Mode	01 (key/manual entry)
V.I.P. Field 60.2	Terminal Entry Capability	5 (chip device)

Merchants/acquirers need to correctly identify Fallback transactions.

Acquirers can use this information to locate fallback transactions for monitoring purposes.

If present, acquirers may also check V.I.P. Field 60.3, Chip Condition Code which provides information that can be used for trend analysis and to support monitoring procedures. This field, however, should only be used for analysis purposes and not on a per-transaction basis. If present, the Chip Condition Code values may be used to indicate the following:

Table 8–3: Chip Condition Code Values

Value	Description	Usage
1	Magnetic stripe Service Code begins with 2 or 6 and the last chip card read at a chip-capable device was either a successful chip read or the transaction was not a chip transaction.	If the analysis shows a large number of transactions for a given device with the value of 1, this could indicate a problem with merchant procedures since the last transaction was a successful chip transaction. The acquirer should assist the merchant with additional training.
2	Magnetic stripe Service Code begins with 2 or 6 and the last chip card read at a chip-capable device was an unsuccessful chip read.	If the analysis shows a large number of transactions for a given device with the value of 2, this may indicate a problem with the device and the device may need to be upgraded.

For contact-chip transactions, this field should not be present or should contain a value of 0.

8.5 Temporary Inability to Authorize

Arrangements between acquirers and merchants may allow merchants to accept above floor limit transactions when the terminal is unable to go online. These mechanisms ensure the cardholder is not inconvenienced and the merchant is able to continue conducting their business. The recommended approach to address this is to employ Deferred Authorizations.

Note: A merchant may operate in an "always-online" mode, even though the floor limit is above zero for their market segment. In the event of an outage, such a merchant could choose to invoke offline approval processing for under-floor transactions, while using Deferred Authorization for all above-floor-limit transactions.

For more information, refer to Section 3.12.2: Deferred Authorization.

8.6 Recovery for Offline Transactions

As a best practice, acquirers should ensure that POS devices receive regular maintenance, such as battery replacement.

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.

To reduce the impact of losing captured transactions, acquirers should ensure their devices are cleared every day and merchants are educated accordingly. Use of nonvolatile journaling (in accordance with PCI DSS requirements) is also recommended.

8.7 Application Performance Considerations

A contact chip device must provide fast, efficient processing of chip card transactions. Much can be gained in transaction time by optimizing the software in the device.

As a best practice, the application transaction time for chip cards should not exceed the time for the same type of transaction performed online with magnetic stripe cards. Targeted transaction times may vary for different national environments.

Much of the communication between the device and chip card can take place while waiting for a manual action from either the cardholder or the merchant. Examples include:

- Initiating a transaction immediately after the card is inserted in the device.

- De-energizing the chip after completion of the transaction, instead of waiting for the receipt to be printed (if applicable), so that the cardholder can remove the card while the receipt is being printed.
- Processing some or all of the steps concurrently instead of sequentially (for example, Offline Data Authentication, processing restrictions, cardholder verification, and terminal risk management).

For more information, refer to Appendix C: Device Performance for EMV Transactions.

8.8 Card Expiration Date Processing

8.8.1 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. The acquirer and the device, however, do not need to interrogate the expiration date above and beyond normal EMV processing.

8.8.2 Magnetic Stripe Transactions

If the cardholder presents an expired magnetic-stripe-only card, a merchant must verify the cardholder's identity and request authorization regardless of the merchant's floor limit. If an authorization cannot be performed, the transaction should be terminated.

If the issuer approves the authorization for an expired magnetic-stripe card, the merchant should proceed with the transaction.

8.9 Data Element Considerations

8.9.1 Application PAN Sequence Number

The Application PAN Sequence Number (Tag '5F34') is an EMV data element that issuers may use to identify a specific card when two or more cards have been issued under a single PAN. It allows differentiation of multiple cards having the same PAN.

If present on the card, this data must be included in the online authorization message in the Card Sequence Number field (V.I.P. Field 23). Failure to do so could result in unnecessary authentication failures.

The format of the Application PAN Sequence Number is described in the EMV and VIS specifications as 2 decimal digits (n 2—1 byte of 2 decimal nibbles). Card Sequence Number is described in the *Visa Smart Debit/Credit System Technical Manual* as three decimal digits (n 3 using Binary-Coded Decimal (BCD)—3 decimal nibbles). Card Sequence Number is right-justified and zero-filled on the left; thus, this field is zero-filled in the first byte and the Application PAN Sequence Number is placed in the second byte.

During testing and certification of the acquirer's BASE I, SMS POS, and SMS ATM systems, Visa regional staff verify the correct handling for both the presence and absence of the Application PAN Sequence Number and ensure that the field is applied in the correct format.

8.9.2 IFD Serial Number

Because there is no global standard for the use of the IFD Serial Number (Tag '9F1E'), its use has resulted in unnecessary declines. To prevent this from happening, VisaNet now deletes this field from messages prior to sending them to the issuer. Device deployers and acquirers are, therefore, advised not to supply this optional VisaNet field in authorization requests.

8.9.3 Issuer Application Data

The acquirer must populate the VisaNet authorization message with the Issuer Application Data (Tag '9F10') sent from the card. This data must be sent from the acquiring device through the acquirer to VisaNet without modification. Since different payment schemes have different lengths and formats for this field, systems should not edit, format, or parse this field.

Acquirers must populate the data in V.I.P. Field 55[45] with the appropriate EMV tags including Issuer Application Data (Tag '9F10'), which can be up to 32 bytes.

The TCR 7 of Transaction Code 05 (TC 05) and Transaction Code 07 (TC 07) needs to be populated with Issuer Application Data, bytes 1 through 32, if present.

8.9.4 Application Cryptogram and Card Authentication

The Application Cryptogram data element, which is 8 bytes, is generated by the card and passed to the device. The issuer checks the cryptogram (generally an ARQC for online transactions) before authorizing the transaction.

Acquirers must include the cryptogram in V.I.P. Field 55 (Tag '9F26').[46]

[45] 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.
[46] Or in Expanded Third Bit Map, V.I.P. Field 136, if applicable.

This data must be sent through from the device to the acquirer and to VisaNet without modification. Systems should not edit, format, or parse this field as it may lead to the issuer declining the transaction.

Modification or failure to pass the correct fields may result in the cryptogram calculation failing at the issuer host and the transaction being declined. This includes the Amount Authorized field (Tag '9F02' in Field 55 or Field 147).

8.9.5 Issuer Authentication Data

The Issuer Authentication Data element, which is 8-16 bytes (plus length byte), is sent from the issuer to the card as part of the authorization response.

Most acquirers receive this variable-length data in V.I.P. Field 55 (Tag '91').[47]

This data must be sent through the network and the acquirer to the acquiring device without modification. Systems should not edit, format, or parse this field.

[47] 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

9. Considerations for Device Approvals

This chapter provides information for acquirers and device vendors to consider for EMV type approval and Visa's terminal testing and validation requirements.

- **Contact Chip Transactions**—To accept Visa contact chip transactions, devices must comply with the current version of EMV contact chip specifications and contain components approved for EMV Level 1 and Level 2 by an EMVCo-accredited laboratory.
- **Contactless Chip Transactions**—To accept Visa contactless chip transactions, devices must comply with the current version of EMV contactless chip or VCPS specifications and contain an approved EMV Level 1 contactless reader. Additional testing by an accredited laboratory is required for contactless devices.

As discussed below, approved, unmodified components may be used across a family of devices. Although the term "EMV-approved device" is commonly used, an approved device is actually one that contains both an approved reader (Level 1) and an approved software kernel (Level 2).

After EMV type approval, devices must also comply with various Visa validation programs, such as the Acquirer Device Validation Toolkit (ADVT) and the Contactless Device Evaluation Toolkit (CDET) or regional variations.

9.1 EMV Level 1

EMV Level 1 approval is given for the interface module (i.e., the chip card reader) rather than for the device on which it is tested. An interface module 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. The three main functional components are the mechanical, electrical, and logical chip card interfaces.

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

9.2 EMV Level 2

EMV Level 2 approval is not tied to a particular model of a particular type of hardware platform. The approval letter notes, however, the hardware configuration that was used for testing.

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

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

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

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

9.3 EMVCo Approvals and Renewals

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

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

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

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

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

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

9.4 Testing Recommendations

Vendors should leave the device containing the interface module or application kernel at the EMVCo-accredited testing laboratory until an approval letter is received from the EMVCo secretariat. Minor issues found in the testing report can be easily resolved if the device has remained under control of the testing laboratory. If the device has left the laboratory, significant re-testing may be required to ensure that no changes have been introduced since the device left the laboratory.

9.5 Kernel Modularization

Device vendors should adopt a modular approach to design so that minor changes can be made without the need for major modification.

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 specifications, such as display

Functionality should be outside the kernel so that these functions may be updated without requiring a kernel update and subsequent re-approval. For example, display messages can reside in a table outside of the kernel. The EMV module can then indicate simply the table entry to be used in a particular situation. This allows language modification without changing the kernel.

9.6 Contactless Reader Approvals and Renewals

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

Additionally, Visa recognizes the contactless Level 1 (analog and digital) and the contactless Level 2 (*EMV Contactless Specifications*) testing offered by EMVCo for devices. Contactless devices should contain a contactless Level 1 reader that has been tested and approved by EMVCo prior to submitting the device to a Visa or EMVCo accredited laboratory for Level 2 application testing, after which it is submitted to a Visa accredited laboratory for interoperability (cross) testing. The approval and renewal process for contactless devices is defined in the *Visa Device Testing Requirements* document that can be downloaded from the Visa Technology Partner website.

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

To facilitate the testing of devices, Visa and EMVCo have recognized a number of independent laboratories to functionally test devices containing contactless payment acceptance on behalf of Visa and EMVCo, respectively. If the device is successfully tested, Visa/EMVCo issues letters of approval[48] to the device vendor that submitted the device for testing. The approval applies internationally, unless restrictions are specified in the letter of approval. Approval is not transferable from one vendor's product to another.

Upon successful completion of official testing:

- For products completed through the Visa testing process, the device will appear on the Approved Acceptance Device Products Lists located at the Visa Technology Partner site (https://technologypartner.visa.com).
- When a device product is approved by Visa, it is assigned a renewal date which is communicated to the device vendor in the letter of approval and also appears on the Visa Approved Products List. The renewal date is typically two years after the date of approval unless otherwise noted.
- As a device approaches its renewal date, Visa reviews the product details to ensure that it complies with all current Visa policies and includes a payment application(s) that Visa continues to support. Further information regarding Visa's current renewal policies is available from Visa Technology Partner site (https://technologypartner.visa.com).
- For products completed through EMV testing, the transaction acceptance device will appear on one of the Approved Products Lists located on the EMVCo website.

9.7 Acquirer Device Validation Toolkit (ADVT)

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

Visa has consequently developed the Acquirer Device Validation Toolkit (ADVT). The toolkit is a set of test cards and test scripts that acquirers or vendors can use on devices that have already received EMV Level 1 and Level 2 approval and are configured for deployment (that is, after the country code, floor limits, and other processing parameters are set up in the device).

The *ADVT User Guide* provides details of the specific conditions that determine the use of ADVT and is part of the ADVT package.

Acquirers that do not comply with this requirement may be subject to fines and penalties as defined in Visa rules and regulations.

[48] The reader (Level 1) and application kernel (Level 2) will 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.

In the U.S. Region, refer to H.3.3: Visa U.S.A. References for further documentation on testing requirements.

9.7.1 ADVT and EMVCo Approval

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

9.7.2 ADVT and Expired EMV Approvals

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

This rule only applies where the results of ADVT testing are to be made available to Visa. Other uses of ADVT, such as for internal regression testing, are not affected.

This will not affect deployed devices or the deployment of devices already approved against ADVT. However, it will prevent the deployment of new and updated device configurations that use expired hardware or software.

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

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

9.7.3 ADVT Usage Guidelines

This section outlines the scenarios where ADVT usage is:

- Required
- Recommended
- Not Required

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

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

Refer to the *ADVT User's Guide*, Appendix E: ADVT Testing Use Cases for further information.

ADVT Usage: Required

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

- **New Device**—Deployment of a new EMV card accepting device containing any of the following:
  - New EMV kernel
  - New version of payment application
  - New terminal-to-host message protocol
- **Modified Device**—Modification or reconfiguration of an existing device to make any of the following changes:
  - Major changes to the EMV-approved kernel (as defined in EMV Bulletin 11 available on www.emvco.com)
  - Changes to the payment component of the terminal application, affecting EMV processing
  - Changes to the Cardholder Verification Method (CVM) capabilities
- **Merchant/Acquirer Network Architecture Change**—Changes to a merchant's or acquirer's network architecture. For example, in a case where a merchant has switched acquirers, even though their terminal configuration might remain the same.
- **New Terminal Hardware Model**—Introduction of a new model[49] of terminal hardware.

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

- **Dynamic Currency Conversion**—Introduction of Dynamic Currency Conversion (DCC) functionality.
- **Cash-Back**—Addition of cash-back functionality.
- **Visa Request**—As requested by Visa based on evidence of an acceptance or interoperability problem affecting the device or connectivity to VisaNet.

ADVT Usage: Recommended

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

- **Acceptance/Interoperability Problem**—A strong suspicion by Visa or an acquirer of the presence of an acceptance or interoperability problem affecting the device or connectivity to VisaNet.
- **Minor Modifications**—Minor modifications or reconfiguration of existing terminals for any of the following:
  - Change of Language Support
  - New communications interface (e.g., from dial-up to high-speed)
  - Upgrades or modifications to the acquirer host systems which affect the transmission of chip data (at a minimum, the ADVT online tests must be performed on at least one EMV chip-reading device)

ADVT Usage: Not Required

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

- **Terminal in Same Family**—On individual terminals that all fall within the same terminal family (e.g., payment application, EMV kernel, and chip transaction flows are all the same). Consult with your terminal supplier to verify that the terminals fall within the same terminal family.
  Note: Third party processors implementing "terminals in the same family" for different clients within the same country or for different clients in a different country are not required to use the ADVT on these devices.
- **Currency Code/Country Code Change**—Change of supported Currency Code/Country Code on the same acquirer host platform. If on a different host platform or different protocol, testing is required.
- **Minor EMV Kernel Changes**—Minor changes to the EMV-approved kernel (as defined in EMV Bulletin 11 available on www.emvco.com).
  Note: Replacing the Interface Modules (IFM) with another approved module is defined as a minor change.
- **Non-Payment Processing Software Change**—Change to software that does not affect payment processing (e.g., screen layout and report generation on a POS terminal, advertising graphics on an ATM).
- **New Peripheral Device**—Addition of a new peripheral device not requiring changes to the existing code (e.g., a new printer or cash dispenser module).

- **Online PIN-Only PIN Entry Device (PED)**—Addition of a new Online PIN-only PED.
- **Terminal-to-Host Message Protocol Change**—Change to the terminal-to-host message protocol which does not affect authorization messages.
- **CA Public Key Change**—Change to CA Public Keys used for Offline Data Authentication (ADVT testing does not use production keys).
- **New Version of ADVT**—Introduction of a new version of ADVT by Visa provided the device has already undergone successful validation using an earlier version of ADVT in accordance with these guidelines.

9.7.4 ADVT Ordering Process

This section provides information on ordering the ADVT.

- All Regions (except Europe Region):
  - For copies of the ADVT, contact Merrill Corporation: STCVisaFulfillment@merrillcorp.com
  - For general information, contact: chiptoolkits@visa.com
- Europe Region:
  - For copies of the ADVT, contact: ADVTorders@visa.com
  - For general information, contact: ADVTK_EU@visa.com

9.7.5 Future ADVT Requirements

Visa may continue to enhance tools and procedures associated with ADVT and will notify acquirers in advance of such changes. The goal of this strategy is to provide a more comprehensive end-to-end testing environment and process that enables acquirers to validate device configurations with the ADVT.

More information on the ADVT can be found at Visa Technology Partner site (https://technologypartner.visa.com).

9.8 Contactless Device Evaluation Toolkit (CDET)

Similar to the use of the ADVT on contact card acceptance devices, contactless acceptance devices need to comply with Visa's Contactless Device Evaluation Toolkit (CDET). CDET is a set of test cards and an accompanying user guide that allows acquirers to validate the correct configuration of their contactless readers. The toolkit is also a self-administered solution.

Acquirers and vendors should contact their Visa representative to discuss the process for obtaining the CDET. Acquirers should also ensure compliance with any additional regional requirements for contactless testing.

For acquirers and device vendors operating in the Europe Region territories, the Visa payWave Test Tool (VpTT) is mandated instead of CDET. The VpTT can be obtained by emailing the Europe Region contactless mailbox (contactlesstest@visa.com).

9.9 Visa payWave Test Tool (VpTT)

The VpTT was developed in the Europe Region to address issues of timing and user interface (lights and beeps) as well as interoperability and acceptance. It helps to ensure a common cardholder experience with all contactless terminals across the VE region.

The VpTT testing process is mandated for all contactless terminals deployed in VE and follows the same rules on retesting as apply to the ADVT. Further information can be obtained by emailing the Europe Region contactless mailbox (contactlesstest@visa.com).

9.10 Chip Compliance Reporting Tool (CCRT)

The Chip Compliance Reporting Tool (CCRT) was originally developed by Visa to replace manual methods used previously for reporting of test results following execution of Acquirer Device Validation Toolkit (ADVT) testing. CCRT is a web-based, user-friendly tool that enables chip acquirers or their processors to complete and submit the mandatory compliance reports via a globally available and automated online system. Hosted on Visa Online (VOL), CCRT is designed in accordance with Visa's three-tier architectural requirements and provides a high-level of application and data security.

CCRT currently supports device testing submission requirements for:

- Acquirer Device Validation Toolkit (ADVT)
- quick Visa Smart Debit/Credit Device Module (qVSDC DM)
- Contactless Device Evaluation Toolkit (CDET)
- Visa payWave Test Tool (VpTT)

Acquirers must use CCRT for ADVT, CDET, qVSDC DM, and VpTT compliance reporting. Visa does not permit alternative methods for submission of results.

9.11 Payment Card Industry Security Standards Council Requirements

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

- Data Security Standards (PCI DSS)
- Payment Application Data Security Standards (PA-DSS)

- PCI PIN Security Requirements
- PCI PTS POI Modular Security Requirements

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

9.11.1 PIN Entry Devices

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

The PED and EPP may be integrated, as in some standalone POS terminals, or the EPP may be just one component of a PED, as in an ATM. Visa mandates relating to usage of PCI PIN Transaction Security (PTS) approved PEDs can be reviewed from https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php.

Refer to the following section for more information on PTS.

9.11.2 PED Testing Requirements

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

For information on PCI PIN entry device security requirements, see https://www.pcisecuritystandards.org/security_standards/documents.phpd.

9.11.3 Payment Application Data Security

Compliance mandates are in place that require all new merchants to be PCI-DSS compliant, including the use of payment application software that uses Payment Application Data Security Standard (PA-DSS) compliant applications.

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

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

More information can be found at www.visa.com.

PCI Security Standards Council (PCI SSC) guidance on how merchants can securely accept payments using mobile devices can be found at the following location: https://www.pcisecuritystandards.org/documents/accepting_mobile_payments_with_a_smartphone_or_tablet.pdf

Appendix A. Track 1 Data Specifications

This appendix describes Visa standards for the contents of Track 1 of the magnetic stripe and the magnetic stripe image on the integrated chip. Visa requirements conform to ISO 7811-2 and ISO 7813.

A.1 Track 1 Content Requirements

This section provides information about the record format, character set, and data elements for Track 1. Requirements for the contents of the magnetic stripe conform to ISO 7813. An issuer must comply with the Track 1 encoding requirements contained in this appendix, as outlined in the following points:

- The magnetic stripe on a Visa card or Visa Electron card (including Instant Issue and Prepaid cards) must be encoded on both Track 1 and Track 2, as specified in this manual.
- Magnetic-stripe data encoding must begin in sequence from the right-hand side of the card as viewed from the back, with the encoded tracks at the top.
- Service Code values must be encoded on a Visa Card or Visa Electron Card, as specified in this manual. An issuer may encode its card acceptance policies in the Service Code field of the magnetic stripe using all valid Service Codes.
- The centerline of the first data bit (start sentinel) to be recorded on the magnetic stripe must be 7.44mm ± 0.51mm from the right edge of the Visa card or Visa Electron card. The centerline of the last data bit to be recorded on the magnetic stripe must not extend closer than 6.93mm from the left edge of the Visa card or Visa Electron card.
- The lead-in to the first data bit and the distance from the last data bit to the end of the magnetic stripe must be clocking bits (i.e., zeroes).
- Data on the magnetic stripe must be encoded at 210 bits per inch on Track 1 and 75 bits per inch on Track 2, and contain at least the required information in the various fields as specified in this manual.
- All of the following must conform to ISO 7811-2:
  - Physical properties
  - Performance characteristics
  - Density
  - Signal level
  - Recording angle tolerances
  - Error detection
  - Permissible surface variation
  - Character sets
  - Appearance of the magnetic stripe

A.2 Record Format

The following points apply to Track 1 record format:

- The PIN Verification Data field is optional for all cards.
- The Discretionary Data field is optional for all cards.
- The Authorization Control Indicator (ACI) in the Visa-Reserved field is optional.

Note: A Card Verification Value (CVV) is required in the Visa-Reserved field on all Visa and Plus cards. CVV is not required on Plus cards.

Track 1 Record Format lists the Track 1 field names and their length. The maximum length of Track 1 is 79 characters. Refer to Data Element Descriptions for more information. Table A–1 describes Track 1 Record Format.

Table A–1: Track 1 Record Format

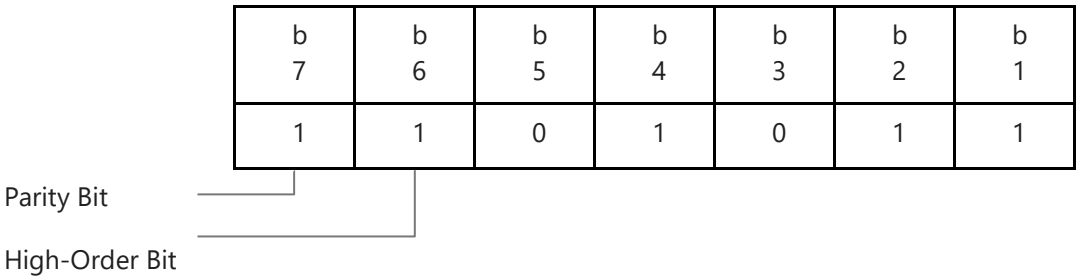
Field Number	Length	Field Name		
1	1	Start Sentinel		
2	1	Format Code		
3	12-19	Primary Account Number (PAN)		
4	1	Separator		
5	2–26	Cardholder Name		
6	1	Separator		
7	4	Card Expiration Date		
8	3	Service Code		
9	0 or 5	PIN Verification Data		
		Position	**Length**	**Content**
		1	1	PIN Verification Key Index (PVK)
		2 to 5	4	PIN Verification Value (PVV)
10	Varies[50]	Discretionary Data		
11	11[51]	Visa-Reserved Field		
		Position	**Length**	**Content**
		1 to 2	2	Zero Fill
		3 to 5	3	Card Verification Value (CVV)
		6 to 7	2	Zero Fill
		8	1	Authorization Control Indicator (ACI)
		9 to 11	3	Zero Fill
12	1	End Sentinel		
13	1	Longitudinal Redundancy Check (LRC)		

[50] The length of this field depends on the lengths of fields 3, 5, and 9.
[51] The length is always the last 11 positions of Track 1, excluding the End Sentinel and Longitudinal Redundancy Check.

A.2.1 Character Set

The bit-sequence pattern for the letter K is illustrated in Figure A-1.

Figure A–1: Letter K Bit Sequence Pattern



Note: *bn* = bit position number "*n*." The parity bit is automatically generated and encoded by the encoding machine.

The encoding equipment must encode the magnetic stripe data of Track 1 in accordance with the bit sequence patterns specified in Figure A–1.

Table A–2 describes the Track 1 character set. This table corresponds to the comparable table in ISO 7811-2.

Data formats to be provided to an encoding machine are specified by the hardware manufacturer. The encoding device must use odd parity to encode data characters. Clocking bits for synchronization are not considered as data.

Additionally, an even-parity Longitudinal Redundancy Check (LRC) character must be the last character in a track record.

Table A–2: Track 1 Character Set

Char	Binary						
	P	2^5	2^4	2^3	2^2	2^1	2^0
space	1	0	0	0	0	0	0
!	0	0	0	0	0	0	1
"	0	0	0	0	0	1	0
#	1	0	0	0	0	1	1
$	0	0	0	0	1	0	0
%	1	0	0	0	1	0	1
&	1	0	0	0	1	1	0
'	0	0	0	0	1	1	1
(	0	0	0	1	0	0	0

Char	Binary						
	P	2^5	2^4	2^3	2^2	2^1	2^0
)	1	0	0	1	0	0	1
*	1	0	0	1	0	1	0
+	0	0	0	1	0	1	1
,	1	0	0	1	1	0	0
-	0	0	0	1	1	0	1
.	0	0	0	1	1	1	0
/	1	0	0	1	1	1	1
0	0	0	1	0	0	0	0
1	1	0	1	0	0	0	1
2	1	0	1	0	0	1	0
3	0	0	1	0	0	1	1
4	1	0	1	0	1	0	0
5	0	0	1	0	1	0	1
6	0	0	1	0	1	1	0
7	1	0	1	0	1	1	1
8	1	0	1	1	0	0	0
9	0	0	1	1	0	0	1
:	0	0	1	1	0	1	0
;	1	0	1	1	0	1	1
<	0	0	1	1	1	0	0
=	1	0	1	1	1	0	1
>	1	0	1	1	1	1	0
?	0	0	1	1	1	1	1
@	0	1	0	0	0	0	0
A	1	1	0	0	0	0	1
B	1	1	0	0	0	1	0
C	0	1	0	0	0	1	1
D	1	1	0	0	1	0	0
E	0	1	0	0	1	0	1
F	0	1	0	0	1	1	0

Char	Binary						
	P	2^5	2^4	2^3	2^2	2^1	2^0
G	1	1	0	0	1	1	1
H	1	1	0	1	0	0	0
I	0	1	0	1	0	0	1
J	0	1	0	1	0	1	0
K	1	1	0	1	0	1	1
L	0	1	0	1	1	0	0
M	1	1	0	1	1	0	1
N	1	1	0	1	1	1	0
O	0	1	0	1	1	1	1
P	1	1	1	0	0	0	0
Q	0	1	1	0	0	0	1
R	0	1	1	0	0	1	0
S	1	1	1	0	0	1	1
T	0	1	1	0	1	0	0
U	1	1	1	0	1	0	1
V	1	1	1	0	1	1	0
W	0	1	1	0	1	1	1
X	0	1	1	1	0	0	0
Y	1	1	1	1	0	0	1
Z	1	1	1	1	0	1	0
[	0	1	1	1	0	1	1
\	0	1	1	1	1	0	0
]	0	1	1	1	1	0	1
^	0	1	1	1	1	1	0
_	1	1	1	1	1	1	1

Note: This coded character set is identical to the coded character set in ISO/IEC 7811-4 and is derived from ASCII.

A.3 Encoding Examples

This section contains examples of Track 1 encoding.

Note: The examples provide a sample format only and should not be followed literally when encoding Track 1 of the magnetic stripe.

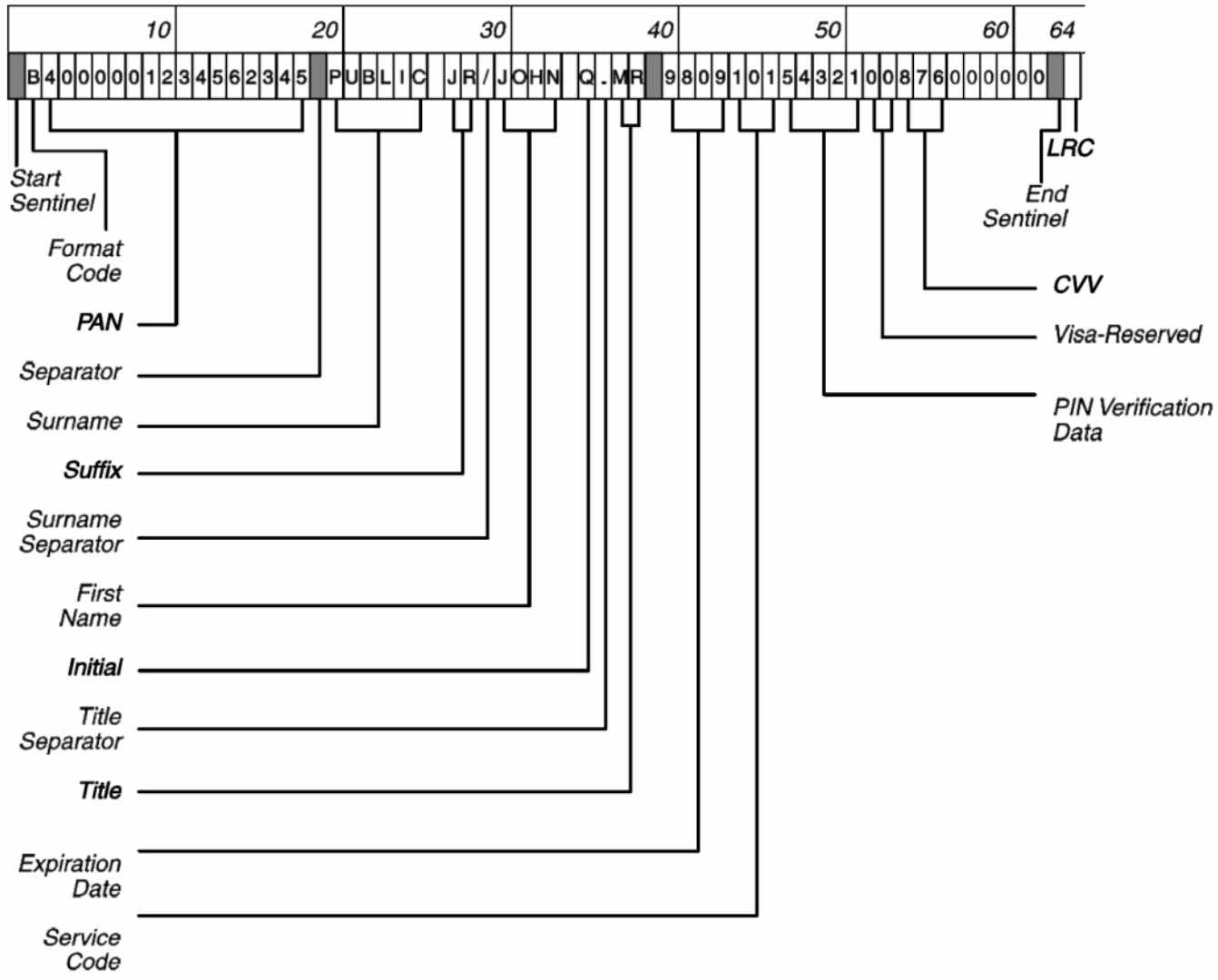
- Figure A–2 illustrates encoding with the PIN Verification Data field. The Visa-Reserved field shows the position of the CVV.
- Figure A–3 illustrates encoding with the Discretionary Data field. The Visa-Reserved field shows the position of the CVV.
- Figure A–4 illustrates encoding with both optional fields. The Visa-Reserved field shows the position of the CVV.

Example: Encoding With PIN Verification Data Field

Information to be encoded:

- PAN: 4000 0012 3456 2345 (16 digits)
- Cardholder Name: MR JOHN Q PUBLIC JR
- Expiration Date: 09/98
- Service Code: 101
- PIN Verification Data: 5 (PVKI) and 4321 (PVV)
- Discretionary Data: none
- Visa-Reserved: 11 characters with 876 for the CVV and the remaining positions are zero-filled

Figure A–2: Encoding With PIN Verification Data Field

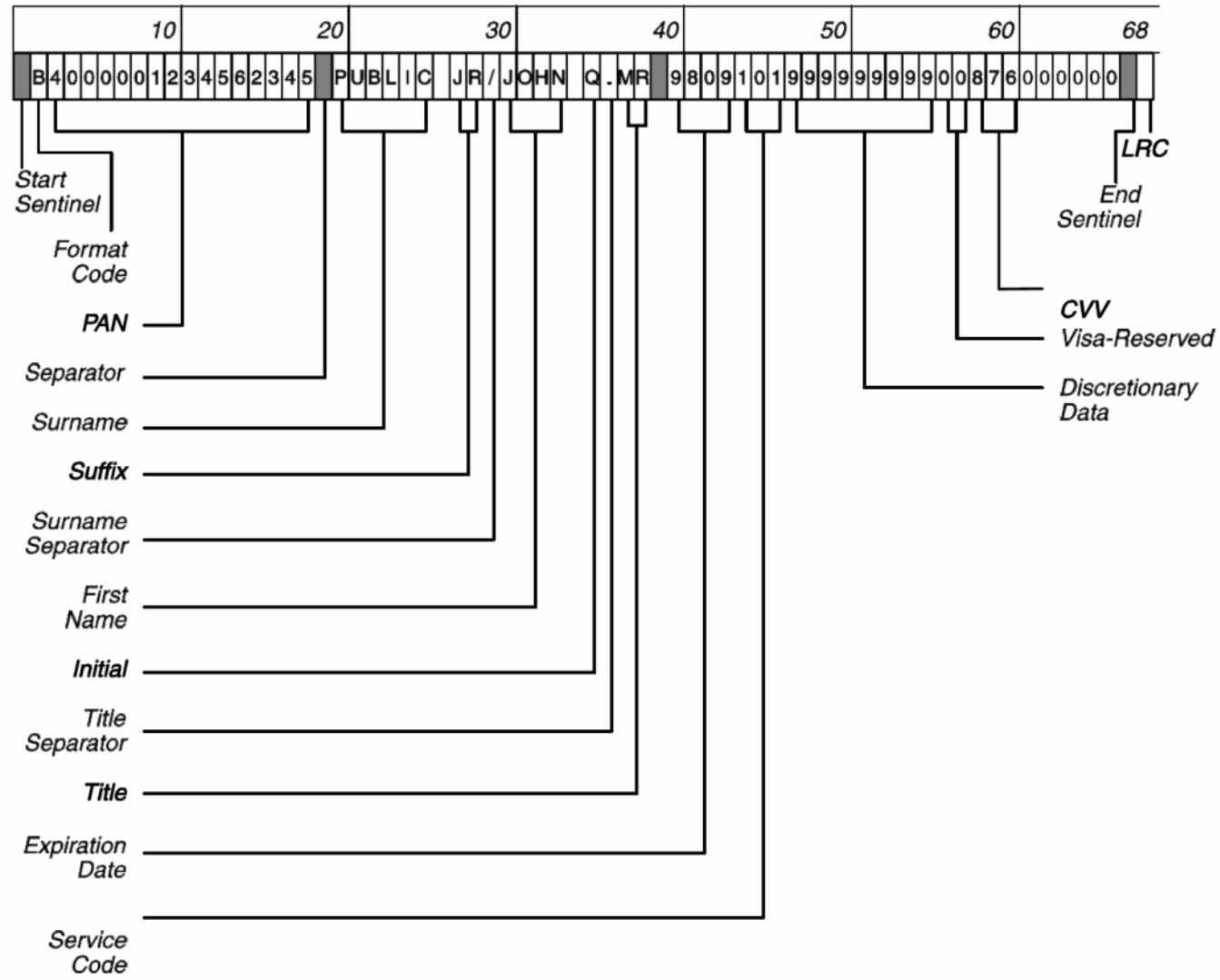


Example: Encoding With Discretionary Data Field

Information to be encoded:

- PAN: 4000 0012 3456 2345 (16 digits)
- Cardholder Name: MR JOHN Q PUBLIC JR
- Expiration Date: 09/98
- Service Code: 101
- PIN Verification Data: none
- Discretionary Data: 999999999
- Visa-Reserved: 11 characters with 876 for the CVV and the remaining positions are zero-filled

Figure A–3: Encoding With Discretionary Data Field

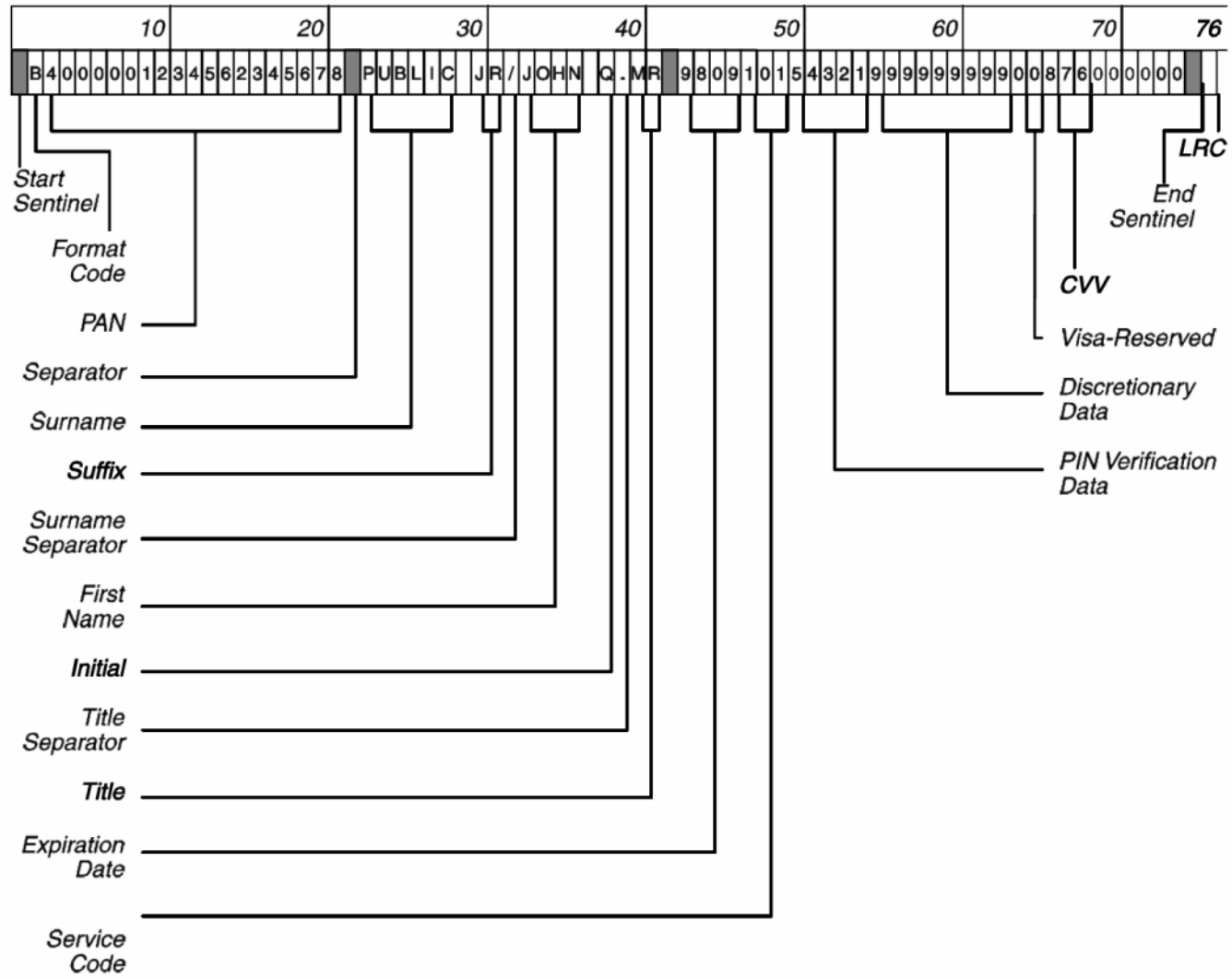


Example: Encoding With PIN Verification Data and Discretionary Data Fields

Information to be encoded:

- PAN: 4000 0012 3456 2345 678 (19 digits)
- Embossed Cardholder Name: MR JOHN Q PUBLIC JR
- Embossed Expiration Date: 09/98
- Service Code: 101
- PIN Verification Data: 5 (PVKI) and 4321 (PVV)
- Discretionary Data: 999999999
- Visa-Reserved Field: 11 characters with 876 for the CVV and the remaining positions are zero-filled

Figure A–4: Encoding With PIN Verification and Discretionary Data Fields



A.4 Data Element Descriptions

This section describes the data elements encoded on Track 1 of the magnetic stripe. Table A–3 describes the Start Sentinel.

Table A–3: Field 1—Start Sentinel

Attributes	1 alphanumeric
Description	Indicates the initial data position on the track.
Valid value	%

Table A–4 describes the Format Code data element encoded on Track 1 of the magnetic stripe.

Table A–4: Field 2—Format Code

Attributes	1 alphanumeric
Description	Specifies the format for Track 1 encoding
Valid value	B

Table A–5 describes the PAN data element encoded on Track 1 of the magnetic stripe.

Table A–5: Field 3—Primary Account Number (PAN)

Attributes	12 to 19 alphanumerics
Description	A series of digits used to identify a customer account or relationship. The first digits of the Primary Account Number specify the Bank Identification Number (BIN), which must be unique to the interchange system and network.
Valid value	0 to 9

Table A–6 describes the Separator data element encoded on Track 1 of the magnetic stripe.

Table A–6: Field 4—Separator

Attributes	1 alphanumeric
Description	Indicates the end of a variable-length field such as the PAN field.
Valid value	^ (caret)
Usage	The separator used in fields 4 and 6 of the track record is identically defined.

Issuers must encode on Track 1 of the magnetic stripe Cardholder Name data elements as contained in Field 5—Cardholder Name, shown in Table A–7.

Table A–7: Field 5—Cardholder Name

Attributes	2 to 26 alphanumerics
Description	Cardholder's name
Valid value	Surname; hyphen (-) permitted for hyphenated surnames Suffix (optional) Surname separator (/) First name and/or initials Title separator (.) if a title is to be encoded Title (optional)
Usage	Two delimiters are used in this field to mark the end of the surname (or surname and suffix) and to mark the presence of a title: The surname separator (/) and title separator (.). The format is the same as that specified in ISO 7813, Identification Cards—Financial Transaction Cards. ISO 7813 requires: "Minimum encoded data shall be a single alpha character (as surname) and the surname separator." It is recommended that no spaces be encoded between the last character of the name or title and the beginning of the next field. It is required to populate the cardholder's name field as it cannot be left blank. Depending on programs and issuers, generic cardholder names can be used whether they are unembossed or embossed. An embossed Visa card must be personalized with a cardholder name on the face of the card. An unembossed Visa card or Visa Electron card may be issued without a cardholder name or generic cardholder identifier. The card may bear either the cardholder name or the generic identifier on the face of the card. If Track 1 on an unembossed Visa flag card does not contain a specific cardholder name, the generic name VISA CARDHOLDER may be encoded in this field. In all other respects, the contents of Track 1 of the magnetic stripe on unembossed cards must be encoded in the same manner as the requirements for traditional embossed cards. If Track 1 on a Visa Electron card does not contain a specific cardholder name, the generic name VISA ELECTRON CARDHOLDER must be encoded in this field. It is possible that cards issued out of branches may not have the cardholder name information encoded on Track 1. For airline ticketing, the customer name is the same as that encoded on the stripe. Therefore, an airline would identify a passenger by the encoded surname, with other names and any title used in the order in which they are encoded, that is, the data following the surname separator (/). The format of the name on Track 1 allows for a minimum field length of two positions. The minimum accommodates cases in which a cardholder has a one-character name. Therefore, the second character must be the surname separator to mark the end of the surname. While the formats of encoded names and embossed names will differ, an issuer should try to keep the content of the encoded and embossed names the same.

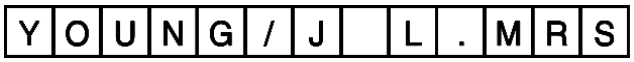
A.4.1 Cardholder Name Usage Examples

In Figure A–5, the cardholder's name is embossed as DR THOMAS A HARRIS JR. Note that the title separator (.) follows the first name THOMAS and the initial A.

Figure A–5: Cardholder Name Usage Example 1

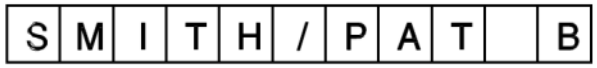
In Figure A–6, the cardholder's name is embossed with initials, such as MRS J L YOUNG.

Figure A–6: Cardholder Name Usage Example 2



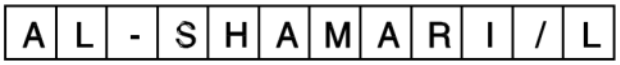
In Figure A–7, the cardholder's name is embossed without a title, such as PAT B SMITH. No title separator () or title is encoded

Figure A–7: Cardholder Name Usage Example 3



In Figure A–8, the cardholder's surname is hyphenated, such as L AL-SHAMARI.

Figure A–8: Cardholder Name Usage Example 4



In Figure A–9, the generic name VISA CARDHOLDER is encoded as follows.

Figure A–9: Cardholder Name Usage Example 5

In Figure A–10, the generic name VISA ELECTRON CARDHOLDER is encoded as follows.

Figure A–10: Cardholder Name Usage Example 6

Table A–8: Field 6—Separator describes the Separator data element encoded on Track 1 of the magnetic stripe.

Table A–8: Field 6—Separator

Attributes	1 alphanumeric
Description	Indicates the end of a variable-length field such as the PAN field.
Valid value	^ (caret)
Usage	The separator used in fields 4 and 6 of the track record is identically defined.

Table A–9: Field 7—Card Expiration Date describes the Card Expiration Date data element encoded on Track 1 of the magnetic stripe.

Table A–9: Field 7—Card Expiration Date

Attributes	4 numerics in the format: YYMM
Description	Year and month after which the card can no longer be used.
Valid value	YY must be 00 to 99; MM must be 01 to 12
Usage	The YYMM format follows ISO conventions for machine-processable dates. All cards with a Visa, Visa Electron, or Delta mark must have a finite expiration date that is no more than 20 years from the date of card issue. The expiration date on a Visa Card, Visa Electron Card, or Card bearing the Plus Symbol must not be later than the expiration date of the Issuer's Public Key, or any security feature containing an expiration date in a Chip, if one is present on the Card.

Table A–10 describes the Service Code data element encoded on Track 1 of the magnetic stripe.

Table A–10: Field 8—Service Code

Attributes	3 numerics
Description	A sequence of digits that, taken as a whole, defines various services; differentiates cards used in international or national interchange; designates PIN requirements; and identifies card restrictions.
Valid value	The values allowed are made up of three individual digits: 1, 2, and 3. To be valid, each digit must be one of the acceptable values listed in Table A-11. These service code values apply to Visa card products (Visa, Visa Electron, I and Plus cards). Not all combinations of individually valid digit values result in a valid service code. Also, while a large number of service codes can be constructed from these values, only specific service codes are authorized for individual Visa card products. Table A-12 describes the service code values that are currently valid for Visa card products.

Table A–11 describes the Service Code Digit Value data element encoded on Track 1 of the magnetic stripe.

Table A–11: Service Code Digit Value Descriptions

Digit	Value	Description
1	0	Invalid for Visa card products
	1	International Card
	2	International Card—EMV chip, debit or credit
	3	Invalid for Visa card products
	4	Invalid for Visa card products
	5	National use only
	6	National use only—EMV chip, debit or credit
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products
2	0	Normal authorization
	1	Invalid for Visa card products
	2	Positive authorization
	3	Invalid for Visa card products
	4	Invalid for Visa card products
	5	Invalid for Visa card products
	6	Invalid for Visa card products
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products
3	0	PIN required
	1	Normal verification
	2	Goods and services only
	3	ATM only
	4	Invalid for Visa card products
	5	Invalid for Visa card products
	6	Prompt for PIN if PIN pad present
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products

Note: "Normal authorization" means normal floor limits apply. "Positive authorization" means that the transaction must go online, regardless of the merchant floor limit. Note that this applies only to magnetic-stripe read transactions.

Table A–12 describes the PIN Verification element encoded on Track 1 of the magnetic stripe.

Table A–12: Field 9—PIN Verification

Attributes	5 numerics
Description	Information needed to verify a PIN using the Visa PIN Verification Value (PVV)
Valid value	Numerics 0 to 9 Position 1: PIN Verification Key Index (PVKI) = 0 or 1 to 6 Position 2 to 5: PIN Verification Value (PVV)
Usage	If not needed, the field can be omitted from the stripe. If the issuer (BIN) uses the PIN Verification Service (PVS) for some, but not all issued cards, the PIN Verification field (both PVKI and PVV) should be zero-filled on those cards not using the PVS. If the issuer does not use the PVS for any cards in a card range, the zero-fill requirement is not needed. Refer to Chapter 6 for more information on the PVKI and PVV.

Table A–13 describes the discretionary data element encoded on Track 1 of the magnetic stripe.

Table A–13: Field 10—Discretionary Data

Attributes	8 to 10 alphanumerics
Description	Information that the issuer uses for on-us transactions and wants to have transmitted through the V.I.P. System for inquiries on interchange transactions. Visa Fleet Service Purchasing cards with a BIN range of 448450 to 448699 are required to use the last three positions of the discretionary data field to provide instructions for customized prompts.
Valid value	Any value in the character ranges 0 to 9 and A to Z, a space, a comma, or a slash (/). Visa Fleet Service Purchasing cards. Position 1: Reserved = 0 Position 2: Service Enhancement Indicator = 0, 1, or 2 Position 3: Service Prompt = 0, 1, 2, 3, 4, or 5
Usage	On Track 1, the length of this optional field is based on the lengths of the Cardholder Name field and on the presence or absence of the PIN Verification Data field and Fleet Service field. If the Cardholder Name field contains 26 characters (the maximum allowed), then 8, 11, 13, or 16 positions are available for discretionary data, as shown in Table A-15.

Attributes	8 to 10 alphanumerics
Note	Track 1 Discretionary Data is defined in EMV and VIS as the discretionary data portion of the magnetic stripe Track 1 according to ISO 7813. However, the definition of Track 1 Discretionary Data as defined in this manual (Visa PTSM) is not the same as the definition in ISO 7813. The Visa PTSM definition of Track 1 Discretionary Data excludes the PVKI, PVV, and the Visa Reserved field from its definition of Track 1 Discretionary Data. The Visa PTSM definition of Track 1 Discretionary Data is thus a subset of the Track 1 Discretionary Data defined by ISO 7813. The Visa PTSM Track 1 record format has the Service Code followed by the (optional) 5-digit PVKI and PIN Verification Value (PVV), followed by the Discretionary Data, followed by the Visa Reserved field, and then followed by the End Sentinel. If Track 1 Discretionary Data is personalized: • For VSDC (i.e., EMV/VIS), it shall be personalized as defined in ISO 7813 (that is, including the PVKI, PVV, and Visa Reserved fields). • For MSD, it shall be personalized as defined in the Visa PTSM (that is, excluding the PVKI, PVV, and Visa Reserved fields).

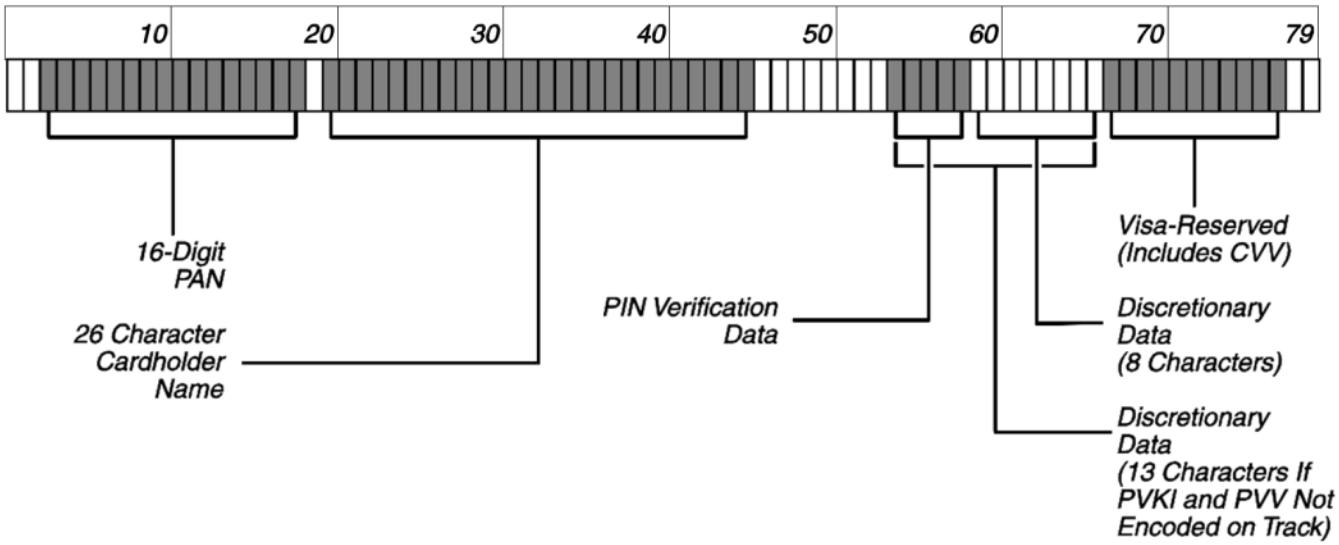
Table A–14 describes the matrix for the Discretionary data field encoded on Track 1 of the magnetic stripe.

Table A–14: Matrix for Discretionary Data Field

	PIN Verification length = 0	PIN Verification length = 5
16-digit PAN	13	8
19-digit PAN	16	11

Figure A–11 illustrates a 16-digit PAN, 26-position name, and 5-position PIN Verification field.

Figure A–11: PIN Verification Field



When the Cardholder Name field contains fewer than 26 characters, the issuer can increase the length of the Discretionary Data field by the number of unused positions.

Note: At the issuer's option, the Card Verification Value (CVV) located in the Visa-Reserved field can also be placed in the Discretionary Data field for ease of issuer verification.

Table A–15 describes the Visa-Reserved data element encoded on Track 1 of the magnetic stripe.

Table A–15: Field 11—Visa-Reserved

Attributes	11 alphanumerics
Description	Last 11 positions of Track 1, excluding the End Sentinel and LRC character. Track 1 can vary in length depending on the presence or absence of the PIN Verification Data and Discretionary Data fields. The location of the last 11 positions of the track varies accordingly. See Section A.3: Encoding Examples for examples. This fixed-length, required field is used by Visa for the following subfields: • 11.1 Card Verification Value • 11.2 Authorization Control Indicator
Valid value	Positions 1 to 2: zeroes Positions 3 to 5 (CVV): 3 numerics Position 6 to 7: zeroes Position 8 (ACI): A to Z or zero Positions 9 to 11: zeroes

Table A–16 describes the CVV data element encoded on Track 1 of the magnetic stripe.

Table A–16: Field 11.1—Card Verification Value (CVV)

Attributes	3 numerics (positions 3–5 of the Visa-Reserved field)
Description	CVV is required on Track 1 of all Visa, Visa Electron, and Plus cards. Unique check value calculated from the data encoded in the stripe using a secure cryptographic process and a key known only to the issuer and Visa. Once encoded on the stripe, the CVV deters counterfeit card usage by validating encoded card information during the authorization process. The algorithm to calculate the CVV is described in the *Visa Payment Technology Standards Manual*.
Valid value	0 to 9 When the CVV is first implemented, issuers using Visa verification to verify CVVs must supply Visa with the expiration date of the card series such that all cards expiring on or after this date are encoded with the CVV.

Table A–17 describes the Authorization Control Indicator data element encoded on Track 1 of the magnetic stripe.

Table A–17: Field 11.2—Authorization Control Indicator

Attributes	1 alphanumeric (position 8 of the Visa-Reserved field)
Description	Used for optional PCAS processing that describes the level of risk and the issuer's PIN policies associated with the cardholder. The risk levels reflect the best (lowest) risk to the worst (highest) risk, from A to D, respectively.
Valid value	Zero, C, Z, Y, or X. Use zero when an ACI code is not included. If the ACI code is included, select C, Z, Y, or X as appropriate for the risk level (see Table A-19).

Table A–18 describes the ACI data element encoded on Track 1 of the magnetic stripe.

Table A–18: ACI Values

ACI	Risk Level	PIN Policy
C	A	Optional
Z	B	Optional
Y	C	Optional
X	D	Optional

Table A–19 describes the End Sentinel data element encoded on Track 1 of the magnetic stripe.

Table A–19: Field 12—End Sentinel

Attributes	1 alphanumeric
Description	Character that follows the final character of data recorded on the track.
Valid value	?

Table A–20 describes the LRC data element encoded on Track 1 of the magnetic stripe.

Table A–20: Field 13—Longitudinal Redundancy Check (LRC)

Attributes	1 character
Description	Verification value that ensures that no data has been lost in the stripe-reading process. The LRC is equivalent to a check digit of the entire track, including the control characters.
Valid value	Any computed value
Usage	The LRC character is calculated using the following procedure: The value of each bit in the LRC character, excluding the parity bit, is defined such that the total count of 1 bit encoded in the corresponding bit location of all characters of the data message, including the Start Sentinel, data, End Sentinel, and LRC characters, is even. The parity bit in the LRC character is not a parity bit for the individual parity bits of the data message; it is the parity bit for the LRC character.

Appendix B. Track 2 Data Specifications

This appendix describes Visa standards for the contents of Track 2 of the magnetic stripe and the Track 2 Equivalent Data of the chip card. Visa requirements conform to ISO 7811-2 and ISO 7813. This information is excerpted from the *Payment Technology Standards Manual*

Note: For chip cards, the equivalent of the magnetic stripe track 2 data (with specific settings required for a chip card program) is placed on the chip in Track 2 Equivalent Data (Tag 57).

B.1 Track 2 Content Requirements

Requirements for the contents of a magnetic stripe conform to ISO 7813.

B.1.1 Magnetic Stripe Encoding Requirements

- The magnetic stripe on a Visa card or Visa Electron card (including Instant Issue and Prepaid cards) must be encoded on both Track 1 and Track 2, as specified in this manual.
- Magnetic stripe data encoding must begin in sequence from the right-hand side of the card as viewed from the back, with the encoded tracks at the top.
- Service Code values must be encoded on a Visa card or Visa Electron card, as specified in this manual. An issuer may encode its Card acceptance policies in the Service Code field of the magnetic stripe using all valid Service Codes.
- The centerline of the first data bit (start sentinel) to be recorded on the magnetic stripe must be 7.44mm ± 0.51mm from the right edge of the Visa card or Visa Electron card. The centerline of the last data bit to be recorded on the magnetic stripe must not extend closer than 6.93mm from the left edge of the Visa card or Visa Electron card.
- The lead-in to the first data bit and the distance from the last data bit to the end of the magnetic stripe must be clocking bits (i.e., zeroes).
- Data on the magnetic stripe must be encoded at 210 bits per inch on Track 1 and 75 bits per inch on Track 2, and contain at least the required information in the various fields as specified in this manual.
- All of the following must conform to ISO 7811-2:
  - Physical properties
  - Performance characteristics
  - Density
  - Signal level
  - Recording angle tolerances
  - Error detection

- Permissible surface variation
- Character sets
- Appearance of the magnetic stripe

B.2 Record Format

An issuer must comply with the Track 2 encoding requirements as contained in this appendix. Table BP1 displays the Track 2 record format. The maximum length of Track 2 is 40 characters, which must include the Start Sentinel, field separator, End Sentinel, and Longitudinal Redundancy Check (LRC).

Note: The Start Sentinel, End Sentinel, and LRC are not included in the authorization message and are not present in the Track 2 Equivalent Data of chip cards.

Table B–1: Track 2 Record Format

Field Number	Length	Field Name
1[52]	1	Start Sentinel
2	12 to 19	Primary Account Number (PAN)
3	1	Separator
4	4	Card Expiration Date
5	3	Service Code
6	0 or 5	PIN Verification Data
7	varies[53]	Discretionary Data[54]
8[45]	End Sentinel	
9[45]	1	Longitudinal Redundancy Check (LRC)

[52] Fields 1, 8, and 9 are not sent in online messages but are necessary for magnetic stripe-reading devices.
[53] The length depends on the lengths of fields 2 and 6. Refer to Section B.5.
[54] Contains the 3-digit Card Verification Value (CVV, iCVV, or a placeholder for dCVV depending on the card program). Refer to Table B–11 for more information.

B.3 Character Set

Table B–2 describes the Track 2 character set on the magnetic stripe. This table corresponds to the character set table in ISO 7811-2, Section 10.1.3.

The hardware manufacturer specifies the data formats provided to an encoding machine.
The encoding device must encode data characters using odd parity. Clocking bits for synchronization are not considered data.

An even-parity LRC character must be the last character in a track record.

Table B–2: Track 2 Character Set

Char	Binary				
	P	**2^3**	**2^2**	**2^1**	**2^0**
0	1	0	0	0	0
1	0	0	0	0	1
2	0	0	0	1	0
3	1	0	0	1	1
4	0	0	1	0	0
5	1	0	1	0	1
6	1	0	1	1	0
7	0	0	1	1	1
8	0	1	0	0	0
9	1	1	0	0	1
:	1	1	0	1	0
;	0	1	0	1	1
<	1	1	1	0	0
=	0	1	1	0	1
>	0	1	1	1	0
?	1	1	1	1	1

Note: This coded character set is identical to the coded character set in ISO/IEC 7811-6 and is derived from ASCII.

B.4 Magnetic Stripe Encoding and Track 2 Equivalent Data Examples

This section contains three examples of Track 2 encoding of the magnetic stripe. The first two examples are magnetic stripe cards and the last one is a chip card (it includes the personalization data for the Track 2 Equivalent Data on the chip).

Table B–3: Magnetic Stripe Encoding and Track 2 Equivalent Data Examples

Examples	PAN Length	Encoding Components
Example 1: Magnetic Stripe Card Note: Card represents an Interlink mark on a Visa Debit Card	16-Digit PAN	Magnetic Stripe: 101 Service Code PIN Verification Data Discretionary Data (CVV in first 3 digits plus additional Discretionary Data)
Example 2: Magnetic Stripe Card	16-Digit PAN	Magnetic Stripe: 120 Service Code No PIN Verification Data Discretionary Data (CVV only)
Example 3: Chip Card	19-Digit PAN	Magnetic Stripe: 201 Service Code PIN Verification Data Discretionary Data (CVV in first 3 digits plus additional Discretionary Data)
		Chip: Track 2 Equivalent Data on the chip Discretionary Data includes: iCVV in the first 3 digits Additional Discretionary Data 'F' added to the end of the Discretionary Data to ensure whole bytes

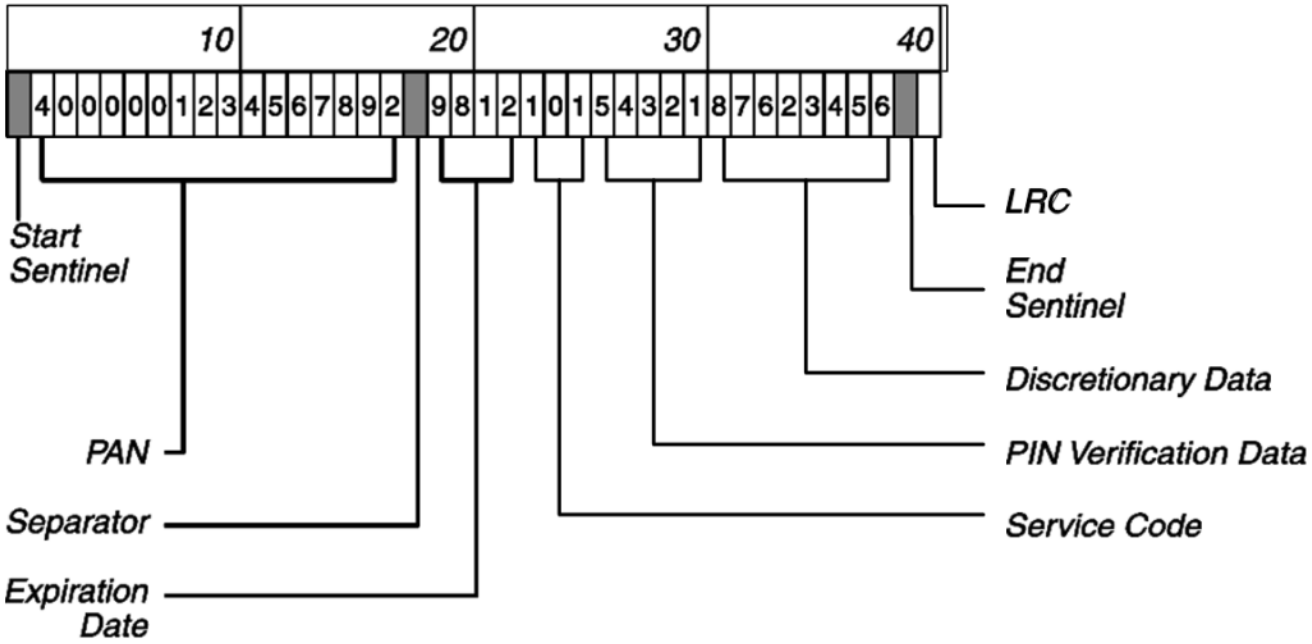
Note: These examples provide a sample format only and should not be followed literally when encoding the magnetic stripe or personalizing the chip.

Example 1: Magnetic Stripe Encoding With PIN Verification Data, Discretionary Data, and CVV

Track 2 Data:

- PAN: 4000 0012 3456 7892 (16 digits)
- Expiration Date: 12/98
- Service Code: 101
- PIN Verification Data: 5 (PVKI) and 4321 (PVV)
- Discretionary Data: 87623456 (first three positions = CVV)

Figure B–1: Magnetic Stripe Encoding With PIN Verification Data, Discretionary Data, and CVV (Example 1)

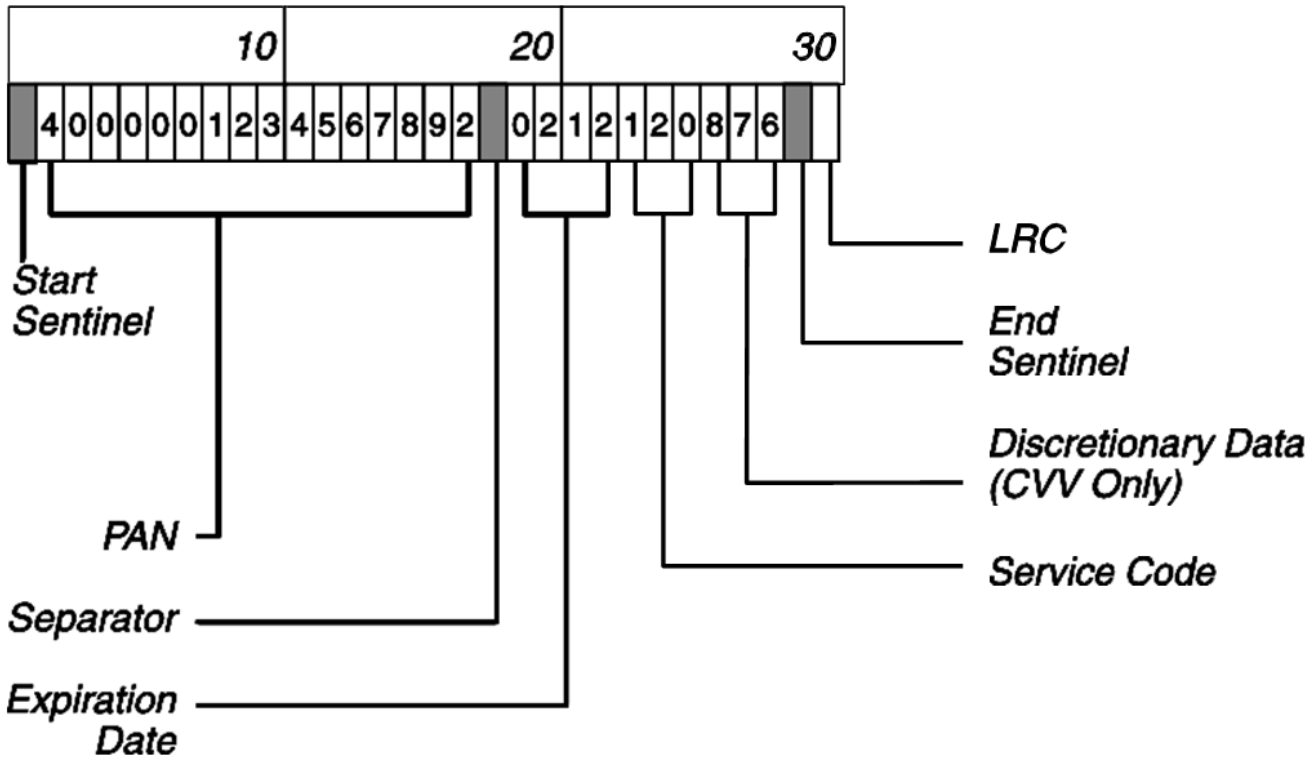


Example 2: Magnetic Stripe Encoding With Discretionary Data Field (CVV Only)

Track 2 Data:

- PAN: 4000 0012 3456 7892 (16 digits)
- Expiration Date: 12/02
- Service Code: 120
- PIN Verification Data: none
- Discretionary Data: 876 (CVV only)

Figure B–2: Magnetic Stripe Encoding With Discretionary Data Field (CVV Only) (Example 2)

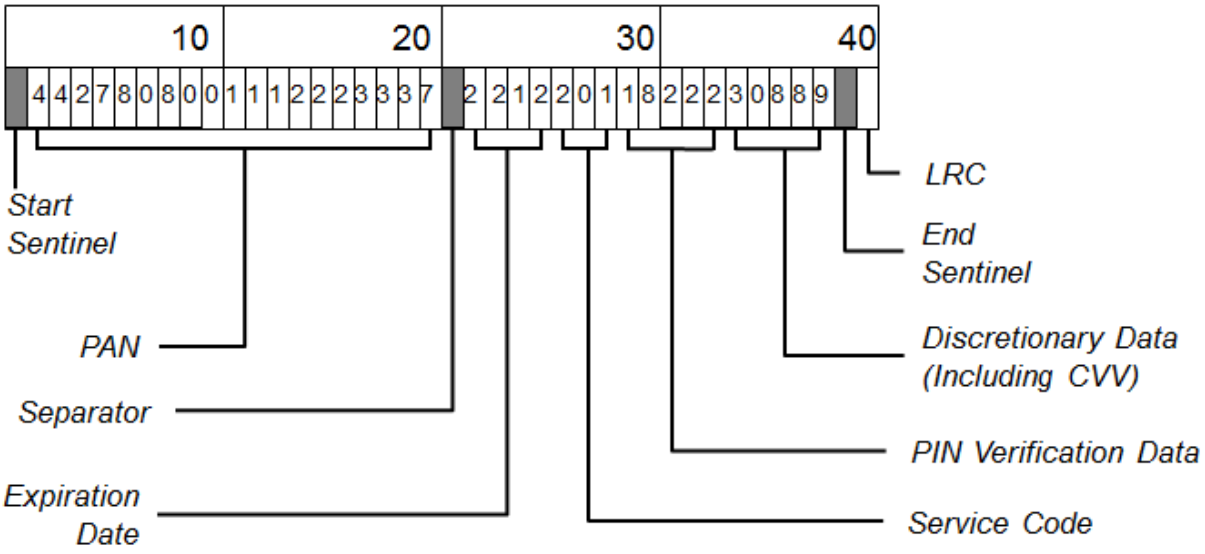


Example 3: Magnetic Stripe Encoding With PIN Verification Data and Discretionary Data Fields

Track 2 Data:

- PAN: 4427 8080 0111 2223 337 (19 digits)
- Expiration Date: 12/22
- Service Code: 201
- PIN Verification Data: 1 (PVKI) and 8222 (PVV)
- Discretionary Data:
  - Magnetic Stripe: 30889 (first three positions = CVV followed by Issuer Discretionary Data)
  - Track 2 Equivalent Data on the Chip: 39289F (first three positions = iCVV followed by Issuer Discretionary Data and ending with an 'F' to ensure whole bytes)
  - Note 1: CVV on magnetic stripe differs from iCVV in the Track 2 Equivalent Data on the chip.
  - Note 2: The Discretionary Data layout when supporting dCVV is not shown.

Figure B–3: Magnetic Stripe Encoding With PIN Verification and Discretionary Data followed by the content of Track 2 Equivalent Data on the Chip (Example 3)



Track 2 Equivalent Data on the Chip:

- 44278080011122233 7D22122011822239289F
- Note: Data contains 'D' separator between the PAN and the expiration date and an 'F' added to the end of the Discretionary Data to ensure whole bytes

B.5 Data Element Descriptions

This section describes the data elements encoded on Track 2 of the magnetic stripe or the Track 2 Equivalent Data of the chip card.

Table B-3 describes the Start Sentinel encoded on the Track 2 of the magnetic stripe.

Note: The Start Sentinel is not included in the authorization message and is not present in the Track 2 Equivalent Data of the chip.

Table B–4: Field 1—Start Sentinel

Attributes	1 alphanumeric
Description	Indicates the initial data position on the track.
Valid value	; (semicolon)

Table B–5 describes the PAN data element encoded on Track 2 of the magnetic stripe or the Track 2 Equivalent Data of the chip.

Table B–5: Field 2—Primary Account Number (PAN)

Attributes	12 to 19 numerics
Description	A series of digits used to identify a customer account or relationship. The first digits of the Primary Account Number specify the Bank Identification Number (BIN), which must be unique to the interchange system and network.
Valid value	0 to 9
Usage	When encoded on the magnetic stripe or in the Track 2 Equivalent Data, the PAN must not include any spaces

Table B–6 describes the Separator data element encoded on Track 2 of the magnetic stripe or the Track 2 Equivalent Data of the chip.

Note: Use of multiple separators may cause problems in some acquiring systems.

Table B–6: Field 3—Separator

Attributes	1 alphanumeric
Description	Indicates the end of a variable-length field such as the PAN field. Only one separator is generally positioned on the track.
Valid value	Magnetic Stripe: = (equal sign) Track 2 Equivalent Data: D

Table B–7 describes the Card Expiration Date data element encoded on Track 2 of the magnetic stripe or the Track 2 Equivalent Data of the chip.

Table B–7: Field 4—Card Expiration Date

Attributes	4 numerics in the format YYMM
Description	Year and month after which the card can no longer be used
Valid value	YY must be 00 to 99 MM must be 01 to 12
Usage	The YYMM format follows ISO conventions for machine-processed dates. The expiration date on a Visa Card, Visa Electron Card, or Card bearing the Plus Symbol must not be later than the expiration date of the Issuer's Public Key, or any security feature containing an expiration date in a Chip, if one is present on the Card.

Table B–8 describes the Service Code data element encoded on Track 2 of the magnetic stripe or the Track 2 Equivalent Data of the chip.

Table B–8: Field 5—Service Code

Attributes	3 numerics
Description	**Magnetic Stripe** A sequence of digits that, taken as a whole, is used to do the following: • Define various service attributes • Differentiate cards used in international or national interchange • Designate PIN requirements • Identify card restrictions **Track 2 Equivalent Data (Chip)** 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).
Valid Value	The values allowed are made up of three individual digits: 1, 2, and 3. To be valid, each digit must be one of the acceptable values listed in Table BP8. These Service Code values apply to Visa card products (Visa, Visa Electron, Plus cards). For chip cards, the Service Code on both the magnetic stripe and in the Track 2 Equivalent Data must begin with a 2 or 6. This value indicates to the chip device that the card is a chip card and that the chip device must initiate the transaction using the chip. Not all combinations of individually valid digit values result in a valid service code. Also, while a large number of service codes can be constructed from these values, only specific service codes are authorized for individual Visa card products.

Table B–9 describes the Service Code Digit Value data element encoded on Track 2 of the magnetic stripe or the Track 2 Equivalent Data of the chip.

Table B–9: Service Code Digit Value Descriptions

Digit	Value	Description
1	0	Invalid for Visa card products
	1	International Card
	2	International Card—EMV chip, debit or credit
	3	Invalid for Visa card products
	4	Invalid for Visa card products
	5	National use only
	6	National use only—EMV chip, debit or credit
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products
2	0	Normal authorization
	1	Invalid for Visa card products
	2	Positive authorization
	3	Invalid for Visa card products
	4	Invalid for Visa card products
	5	Invalid for Visa card products
	6	Invalid for Visa card products
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products
3	0	PIN required
	1	Normal verification
	2	Goods and services only
	3	ATM only
	4	Invalid for Visa card products
	5	Invalid for Visa card products
	6	Prompt for PIN if PIN pad present
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products

Note: "Normal authorization" means normal floor limits apply. "Positive authorization" means that the transaction must go online, regardless of the merchant floor limit. Note that this applies only to magnetic-stripe read transactions.

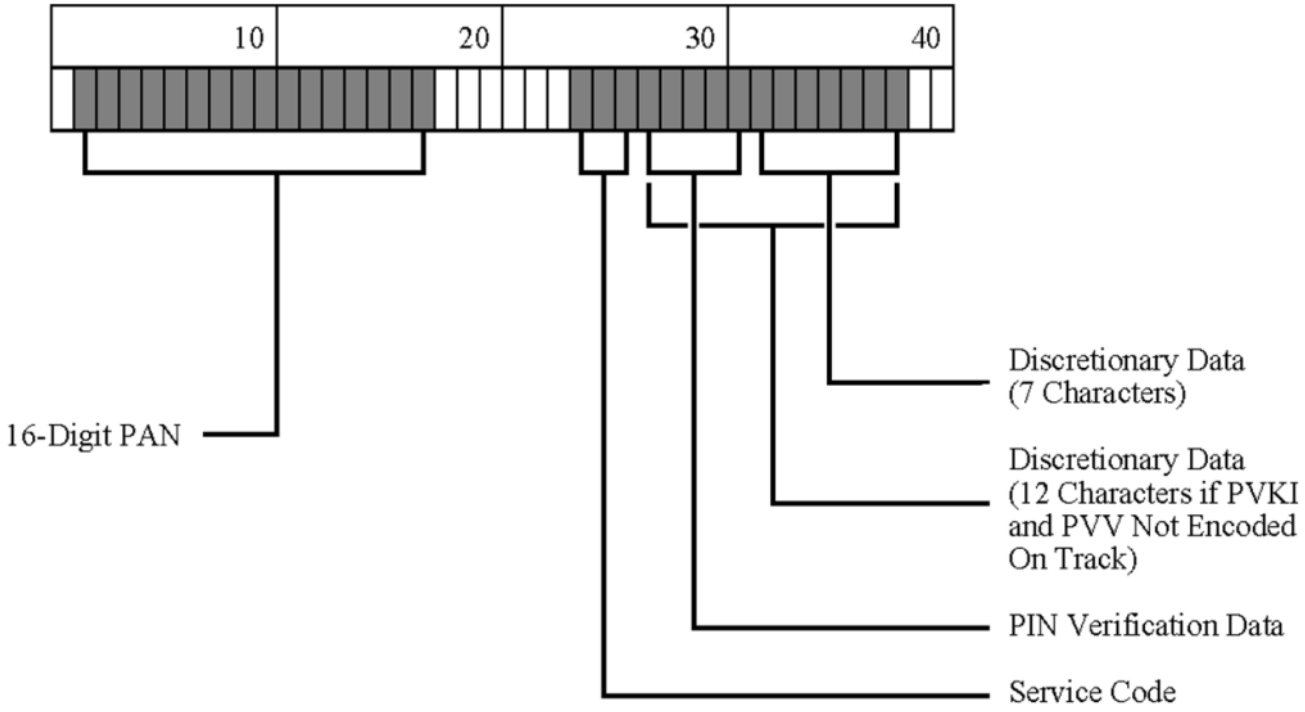
Table B–10 describes the PIN Verification Data field encoded on Track 2 of the magnetic stripe or the Track 2 Equivalent Data of the chip.

Table B–10: Field 6—PIN Verification

Attributes	5 numerics
Description	Used to verify a PIN. Generally called Visa PVV or PIN offset value.
Valid value	Numerics 0 to 9 Position 1: PIN Verification Key Index (PVKI) = 0 or 1 to 6 Positions 2–5: PIN Verification Value (PVV)
Usage	If not needed, the field can be omitted from the magnetic stripe or the Track 2 Equivalent Data of the chip. If the issuer (BIN) uses the PIN Verification Service (PVS) for some, but not for all issued cards, the PIN Verification Data field (both PVKI and PVV) should be zero-filled on those cards not using the PVS. If the issuer does not use the PVS for any cards in a card range, the zero-fill requirement is not needed. Refer to the *Payment Technology Standards Manual* for more information on the PVKI and PVV.

Figure B–4 illustrates a 16-digit PAN and a 5-position PIN Verification field.

Figure B–4: PIN Verification Field



Error! Reference source not found. describes the Discretionary Data element encoded on Track 2 of the magnetic stripe or the Track 2 Equivalent Data of the chip.

Table B–11: Field 7—Discretionary Data

Attributes	Up to 17 numerics
Description	Includes the Card Verification Value (CVV, iCVV, or a placeholder for dCVV) plus any valid information that the issuer wants to have transmitted in the transaction or is required based on the card program. • Magnetic Stripe Cards—CVV must be encoded in the Discretionary Data portion of Track 2 of the magnetic stripe on all Visa, Visa Electron, and Plus cards. • Chip Cards—iCVV must be personalized in the Discretionary Data portion of the Track 2 Equivalent Data on all newly issued and reissued cards. • Chip Cards Supporting MSD CVN 17 or qVSDC—Discretionary Data in the Track 2 Equivalent Data is personalized with: - iCVV (iCVV is mandatory) - Optionally followed by a 4-digit placeholder for the 4 rightmost digits of the ATC (if the ATC Insertion Option is supported) - Note: During the transaction, if the chip card supports the ATC Insertion Option, it will calculate the ATC and insert it in the Discretionary Data portion of the Track 2 Equivalent Data to send to the device - Discretionary Data Example: 1230000 • Chip Cards Supporting MSD Legacy With dCVV—Discretionary Data in the Track 2 Equivalent Data is personalized as follows: - 3-digit placeholder for dCVV - Followed by a 4-digit placeholder for the 4 rightmost digits of the ATC - Followed by the 1-digit Contactless Indicator (which must contain a value greater than 0) - Note: During the transaction, the chip card will calculate the dCVV and ATC and insert them in the Discretionary Data portion of the Track 2 Equivalent Data to send to the device For chip cards, if the entire number of nibbles in the Track 2 Equivalent Data is an odd number, an 'F' should be added to the Discretionary Data to ensure full bytes.
Valid value	Any valid non-control or non-reserved character listed in Table B–2.

Usage	On Track 2, the maximum length of this optional field is based on the length of the Primary Account Number (PAN) and on the presence or absence of the PIN Verification field. Because Discretionary Data fields are optional, they should not be filled with pad characters solely with the intent to fill all positions on Track 2. The 3-digit CVV must be encoded in the Discretionary Data field. While Visa recommends placing the CVV at the start of this field, any three contiguous positions can be used. Figure B–5 illustrates the recommended placement of the CVV in an 8-digit Discretionary Data field. iCVV is mandatory for contact chip, MSD with CVN 17, and qVSDC. iCVV is only placed on the chip (Track 2 Equivalent Data); it is not applicable to the magnetic stripe. dCVV is mandatory for MSD Legacy. **Note:** *If Visa is to provide CVV, iCVV, or dCVV validation for an issuer, the issuer must provide Visa with the location of the CVV/iCVV/dCVV on Track 2 Equivalent Data for verification purposes. The issuer describes the location by giving its displacement from the end of the Service Code field. For example, in Figure B–5, the displacement is 5. If the PIN Verification field was not encoded on the stripe, the displacement would be 0. For details on calculating the CVV/iCVV/dCVV, refer to the* Visa Payment Technology Standards Manual.
Note	Track 1 Discretionary Data is defined in EMV and VIS as the discretionary data portion of the magnetic stripe Track 1 according to ISO 7813. However, the definition of Track 1 Discretionary Data as defined in this manual (Visa PTSM) is not the same as the definition in ISO 7813. The Visa PTSM definition of Track 1 Discretionary Data excludes the PVKI, PVV, and the Visa Reserved field from its definition of Track 1 Discretionary Data. The Visa PTSM definition of Track 1 Discretionary Data is thus a subset of the Track 1 Discretionary Data defined by ISO 7813. The Visa PTSM Track 1 record format has the Service Code followed by the (optional) 5-digit PVKI and PIN Verification Value (PVV), followed by the Discretionary Data, followed by the Visa Reserved field, and then followed by the End Sentinel. If Track 1 Discretionary Data is personalized: • For VSDC (i.e., EMV/VIS), it shall be personalized as defined in ISO 7813 (that is, including the PVKI, PVV, and Visa Reserved fields). • For MSD, it shall be personalized as defined in the Visa PTSM (that is, excluding the PVKI, PVV, and Visa Reserved fields).

Figure B–5: Discretionary Data Field

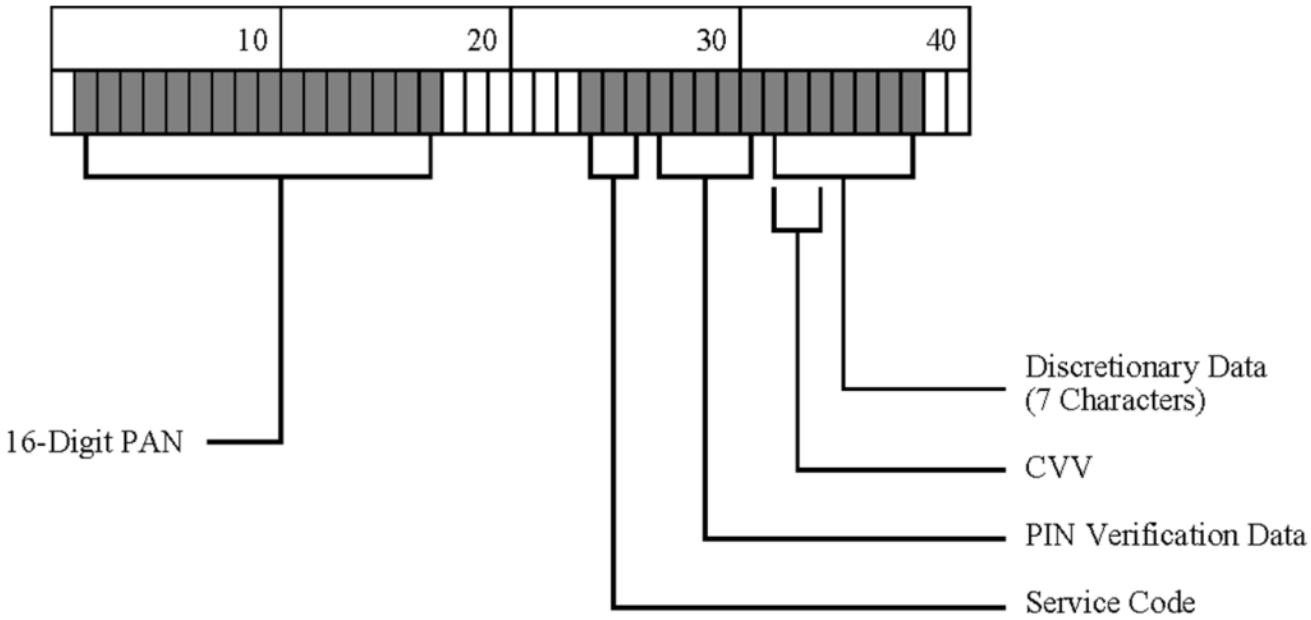


Table B–12 describes the End Sentinel element encoded on Track 2 of the magnetic stripe.

Note: The End Sentinel is not applicable to the Track 2 Equivalent Data on the chip.

Table B–12: Field 8—End Sentinel

Attributes	1 alphanumeric
Description	Indicates the final data position on the track.
Valid value	? (question mark)

Table B–13 describes the Longitudinal Redundancy Check element encoded on Track 2 of the magnetic stripe.

Note: The LRC is not applicable to the Track 2 Equivalent Data on the chip.

Table B–13: Field 9—Longitudinal Redundancy Check (LRC)

Attributes	1 character
Description	Verification value that ensures that no data has been lost in the stripe-reading process. The LRC is equivalent to a check digit of the entire track including the control characters.
Valid value	Any computed value
Usage	The LRC character is calculated using the following procedure: • The value of each bit in the LRC character, excluding the parity bit, is defined such that the total count of 1 bit encoded in the corresponding bit location of all characters of the data message, including the Start Sentinel, data, End Sentinel, and LRC characters, is even. • The parity bit in the LRC character is not a parity bit for the individual parity bits of the data message: it is the parity bit for the LRC character.

Appendix C. Device Performance for EMV Transactions

This appendix discusses various factors that are under the control of the device implementer (either the application developer or system integrator) to increase the speed of authorization, thus enhancing the cardholder experience while providing reduced transaction and queue times for the merchant. The many direct factors that influence device performance include clock speed, word size, and programming language used.

EMV functionality is only one part of the point-of-service application as a whole. Poorly executed systems integration can easily overshadow the most efficient EMV kernel. Device vendors should take into consideration any opportunity to overlap EMV and non-EMV functions. For example, a dial device may be able to pre-dial while EMV processing is being completed, particularly if online processing is required, due to use of Online PIN or because of terminal risk management.

Online authorizations can be optimized through implementation of fast communication technologies (such as always-on or broadband). In many cases, the benefits of customer satisfaction and higher throughput can offset additional communication costs.

The cardholder experience is the final measure of acceptable performance. This experience is based on the synergy, or lack thereof, of all factors, and no one factor can be singled out. Vendors who do not produce a device appropriately responsive to a bank or merchant's customers are likely to be negatively affected in the market place.

EMVCo has documented best practices in the *EMV Optimising Contact Chip Transaction Times Best Practices*, available at www.emvco.com.

C.1 Device Factors Influencing Transaction Duration

A device that supports VSDC cards must provide fast, efficient processing of contact-chip transactions. As a best practice, the application transaction time for VSDC cards should not exceed the time for the same type of transaction performed online with magnetic stripe cards. Optimal transaction times for different countries may vary.

C.1.1 Cryptographic Factors

RSA processing is the single largest component of the processing impact of EMV functionality. Cryptographic efficiency can be achieved with specialized electronics, whether exponentiation circuitry, dedicated cryptographic Application Specification Integrated Circuits (ASICs), Security Application Modules (SAMs), or other alternatives. The cost considerations of these alternatives, however, may drive vendors to attempt RSA processing in the mainline application within the main processor chip.

In these cases, it is crucial to use efficient algorithms. The specialized knowledge required to develop such algorithms may make it cost efficient to license the intellectual property rights to use algorithms developed by specialists in the field. The importance of efficient RSA operations can be shown by how often the processing is invoked, for example:

- An SDA transaction has two RSA device operations: one with the VSDC CA Public Key and one with the issuer public key.
- A DDA or CDA transaction has three RSA device operations: one with the VSDC CA Public Key, one with the issuer public key, and one with the ICC public key. There is also one ICC operation that uses the ICC private key.
- A DDA and Offline Enciphered PIN transaction where the same ICC key is used for enciphered PIN and DDA involves four RSA device operations: one with the VSDC CA Public Key, one with the issuer public key, and two with the ICC public key. In addition, two ICC operations use the ICC private key.
- When different ICC keys are used for Offline Enciphered PIN and DDA, the transaction has five RSA device operations: one with the VSDC CA Public Key, two with the issuer public key, and two with ICC public keys. Again, two ICC operations use ICC level private keys.

Because EMV processing is only a part of the point-of-service application, it may be cost efficient to have the processing performed by SAMs or co-processors. Co-processors optimized for cryptographic functions can offload a significant amount of the overall processing demand and may be a more cost-effective alternative to upgrades to the main processing chip.

RSA cryptography is considerably more demanding than DES processing. Co-processors that are sufficient for DES processing, such as those residing in a tethered PIN pad or integrated security module, may be inadequate for the RSA components in Offline Enciphered PIN processing.

C.1.2 Communications Speed to Cards

The communication speed between a card and a device can impact transaction throughput. With EMV 3.1.1, this speed is set, but EMV 4.1 allows higher speeds (smaller dividers) and EMV 4.2 requires this support. Devices should support EMV 4.1 or higher, where possible, to take advantage of higher throughput.

C.1.3 Application Optimization

The demands of EMV processing, particularly RSA functions, require that efficient coding techniques be employed. Efficient coding may be one of the most significant factors in producing responsive applications.

Field experience has shown that applications developed with a primary focus on simply providing EMV functionality can often be dramatically improved by undertaking an optimization effort. (Optimization often suffers when code is produced against tight deadlines.) For EMV functionality, it is important to focus on efficiency of the RSA algorithm, particularly if it is implemented in software to be executed on the main processing chip. Because of the mathematical expertise required to develop truly efficient code, some vendors have found it more cost effective to purchase RSA implementations. In house developers should be familiar with efficient squaring techniques, as those discussed in Bruce Schneier's *Applied Cryptography*.

It is equally important that the application integrator, combining the EMV kernel with existing customized applications, pay attention to performance implications.

C.2 Process Overlap: Multitasking or Interleaving

The device application developer must look for opportunities for true multitasking or at least for apparent multitasking, such as performing processing while waiting for a manual action from either the cardholder or the merchant. Effective process interleaving can also have a significant impact on overall throughput, thus compensating for other deficiencies.

Transactions should be initiated as soon as the card is inserted into the device. Taking advantage of wait times in one process to work on another process, such as overlapping SDA or DDA processing with PIN entry, is another important technique for speeding throughput. Vendors have a long history of exploiting opportunities to overlap processing. The relative novelty of EMV processing brings new challenges and opportunities. Pre-printing of receipt headers (where printed receipts apply), pre-dialing of authorization numbers, and taking advantage of human interactions such as amount and PIN entry continue, however, to provide opportunities to present the appearance of prompt throughput to the consumer.

The device should also be prepared to take advantage of information in the records presented by the card as soon as it is available. For example, if the card has the CVM List as one of the first records read, preparation for CVM processing can begin (prompt for PIN) and possibly online processing (if Online PIN is the mutually supported CVM). Other useful pieces of data are the PAN (for additional controls based on BIN), issuer's country code (for domestic or international considerations), and Application Usage Control (for environmental restrictions, such as ATM-only applications). Evaluating processing restrictions early in the flow of records may allow the device to avoid unnecessary processing. The device may also begin pre-dialing if an online transaction is likely.

Once the appropriate information is read during the read-data phase and at any time prior to terminal action analysis, the device can process the steps for Offline Data Authentication, processing restrictions, cardholder verification, and terminal risk management in any order. Multitasking or interleaving can be used to optimize the processing of these steps.

Certificate extraction should commence as soon as feasible. Application developers in countries with a high percentage of domestic transactions and relatively few issuers may want to consider caching extracted certificates. EMV requires that the issuer certificate still be transferred from the card to the device, but caching can eliminate extraction time. (If a VSDC CA key is updated, the cache should be emptied.)

A prompt for the PIN can also be used to confirm application selection and transaction amount.

Transaction amount entry and PIN entry provide two opportunities for processing other functions such as data authentication.

Switching the power off to the card after completion of the transaction instead of waiting for the receipt to be printed (if applicable) allows the cardholder to remove the card while the receipt is being printed. A message should be displayed to the cardholder when the card can be removed.

C.3 Card Interaction

Card-processing speed is dependent on the capability of the card and the clocking provided by the device. All cards must support the range of clock speeds that are defined in EMV. The clock speed supplied by the device, however, affects card-processing times, particularly cryptographic processes (such as DDA, CDA, and enciphered PIN). Devices should provide clocking at the highest allowable speed, currently 5 MHz.

C.4 Device and Application Architectures

Applications that are designed to support integrated POS environments may distribute EMV processing across servers, tills, and transaction acceptance devices. Efficient processing demands that sufficient power resides at each point to properly process transactions and that sufficient communication capacity exists between components to avoid bottlenecks.

Techniques for application development may include pre-coded modules that can be rapidly assembled into complex applications. This development speed may, however, affect application performance.

C.5 Application Development Considerations

Other considerations for application development include:

- **Project Deadlines**—Project deadlines must be realistic. When deadlines for delivery of new applications are overly ambitious, insufficient time and attention may be paid to the previously discussed issues. Time must be allocated for both application development and integration and for optimization efforts.
- **Economic Factors**—Optimizing a customized application may require additional development costs, which may be unacceptable to the purchaser.
- **Application Integration**—The EMV kernel is only one functional area of the overall retail or banking application. The intensive computation required for RSA processing is a significant component of overall response time, but it is only one component and it must be integrated with the overall application.
- **International Requirements**—Domestic environments may have little use for some features, such as Offline Enciphered PIN. Applications that provide acceptable performance for domestic requirements may not, therefore, be able to support international cards that request functions not common in the local environment. The acquirer or device deployer needs to make an economic decision regarding provision of optimal support for these features.

C.6 Transaction Receipt Requirements

Where a printer is used for receipts, to improve printing time, no more data should be printed on a receipt than is required by Visa rules and regulations and local law. The device should print as much of the receipt as possible prior to completing transaction processing.

Subject to Visa rules and regulations and local legislation, a receipt may be optional (for example, under VEPS). Eliminating receipt printing, where feasible, can improve transaction throughput.

Note: Receipts must be made available at cardholder request.

C.7 Retail Environment

Performance of an EMV kernel in a laboratory or a vendor's development setting can only partially reflect actual performance when the kernel is integrated with a payment application and deployed in a retail environment. It is recommended that device deployers set their own transaction performance requirements and develop concise test scripts that reflect those requirements. Vendors should demonstrate their ability to meet these requirements with the application to be deployed in the local environment.

Appendix D. EMV Tag to VisaNet Data Element Mapping

This appendix provides data mapping information between the EMV data elements and the VisaNet (V.I.P. and BASE II) messages. (See the *Visa Smart Debit/Credit System Technical Manual*.) It is intended for acquirers and vendors to help them understand the new chip data required in the device-to-acquirer message and the acquirer-to-VisaNet message. It may also be used by issuers in upgrading their hosts to support the new data.

D.1 Mapping Information for Host and Device Data Capture Environments

This section outlines the mapping information for host and device-data capture environments:

- **Host Data Capture**—For host-data capture acquirers (including ATM and single-message acquirers), the acquirer uses the authorization message to create the clearing message. The mapping of information from the V.I.P. field to the BASE II field is, therefore, applicable and can be used in creating the clearing message.
- **Device Data Capture**—For device-data capture acquirers, the acquirer does not use the authorization message to create the clearing message. Rather, the acquirer uses data from the device to create the clearing message. The values for several of these data elements differ from their counterparts in the authorization message, including the Card Verification Results, TVR, and, in some cases, the amount (either Cryptogram Amount or Amount, Authorized). The mapping of information from the EMV/VSDC data element to the BASE II data element is, therefore, applicable and can be used in creating the clearing message, but the mapping of information from the V.I.P. field to the BASE II field is not applicable (especially for the above-mentioned fields).

D.2 Sensitive Cardholder Information

While Visa allows non-Visa/non-EMV tags to be sent in Field 55, there are tags that must **not** be sent in this field as they include sensitive cardholder information that may be inadvertently logged by systems that do not expect Field 55 to contain sensitive cardholder information.

Specifically, acquirers shall **not** include the following tags in Field 55:

Table D–1: Chip Data Not Sent in Field 55

Tag	Chip Data	Equivalent data sent in:
'56'	Track 1 Equivalent Data	Not sent in chip transactions
'57'	Track 2 Equivalent Data	Field 35
'5A'	Application PAN	Field 2
'5F20'	Cardholder Name	Not sent in chip transactions
'5F24'	Application Expiration Date	Field 14
'99'	Transaction PIN	Field 52
'9F0B'	Cardholder Name—Extended	Not sent in chip transactions
'9F1F'	Track 1 Discretionary Data	Not sent in chip transactions
'9F20'	Track 2 Discretionary Data	Field 35

Note: Track 1 Equivalent Data (Tag '56') and Track 2 Discretionary Data (Tag '9F20') are not personalized on Visa card applications, but are included in the above list for completeness.

If any of these fields are found in Field 55, Visa will drop them from the message prior to forwarding the transaction to the issuer (or any other downstream entities). For further information, refer to the *October 2013 Business Enhancements Release*, Article 5.3.

D.3 EMV Tag to VisaNet Data Element Mapping Table

Table D–2 highlights the following information:

- **EMV Data Element**—This column contains the name of the data element, as specified in the EMV and VIS specifications.
- **EMV Tag**—This column contains the tag associated with the data element, as specified in the EMV and VIS specifications.
- **EMV Origin**—This column specifies where the data element comes from (for example, card or device).
- **VisaNet Data Element**—This column contains the name of the data element, as specified in the VisaNet manuals.
- **VisaNet Authorization Requirement**—This column states whether the data element is mandatory, optional, or conditional in the authorization message.
- **VisaNet Authorization V.I.P. Field**—This column outlines the V.I.P. field location for the data element. For many of the chip data elements, the acquirer, issuer, or both has the option to support the data element in the third bit map or Field 55. The information is noted in this column.
- **VisaNet Clearing Requirement**—This column states whether the data element is mandatory, optional, or conditional in the clearing message.
- **VisaNet BASE II**—This column outlines the BASE II field location for the data element.

The data element values must, therefore, not be altered or manipulated because they are transferred from either the card or the device to the acquirer and then from the acquirer to VisaNet in the online message. The device vendor must ensure that these data elements have integrity in the device-to-acquirer message and the acquirer must ensure that they have integrity in the online message to the issuer.

Important: Most countries require acquirers to submit chip data using Field 55, although there are some countries that continue to allow acquirers to support the chip data using the Expanded Third Bit Map. Contact your Visa representative for the requirements in your country.

Table D–2: EMV/VisaNet Data Elements and Tags

EMV Data Element	Tag	Origin	VisaNet Data Element	Authorization Requirement	V.I.P. Field[55]	Clearing Requirement	BASE II	Notes
Amount Authorized	'9F02' (L 6)	Device (Amount, Authorized without adjustments)	Cryptogram Amount/ Amount Authorized (V.I.P.)`Authorized Amount (TCR 5, BASE II)`Cryptogram Amount (TCR 7 BASE II)	Mandatory	147 or 55	Mandatory	TCR 5, pos. 20–31, or TCR 7, pos. 87–98	• This must be the amount of the transaction, as used by the card to generate the cryptogram. • If the acquirer is not participating in Custom Payment Service (CPS), the acquirer can provide the cryptogram amount (which is the amount used by the card to generate the cryptogram) in Authorized Amount (TCR 5) or Cryptogram Amount (TCR 7). If both fields are used, they should contain the same value. From a VisaNet perspective, if both fields are present, the amount in Cryptogram Amount (TCR 7) is used for cryptogram validation. If the acquirer is participating in CPS, the acquirer provides the cryptogram amount (which is the amount used by the card to generate the cryptogram) in Cryptogram Amount (TCR 7). For these transactions, the amount provided in Authorized Amount (TCR 5) is used for CPS purposes. • The Amount, Authorized is placed in BASE II TCR 5, positions 20–31, when the cryptogram amount matches the authorized amount and in TCR 7, positions 87–98, when the cryptogram amount differs from the authorized amount. When the TCR 5 field is used for cryptogram amount, positions 87–98 in the TCR 7 are filled with spaces.
Amount, Other	'9F03' (L 6)	Device (based on the cash back amount of the transaction)	Cryptogram Cashback Amount/ Amount, Other (V.I.P.)`Cash back (BASE II)	Conditional	149 or 55	Conditional	TCR 1, pos. 158–166	Only applicable if the POS transaction is for purchase with cash back.

[55] 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.

EMV Data Element	Tag	Origin	VisaNet Data Element	Authorization Requirement	V.I.P. Field[55]	Clearing Requirement	BASE II	Notes
Application Cryptogram	'9F26' (L 8)	Card	Cryptogram/ Application Cryptogram	Mandatory	136 or 55	Mandatory	TCR 7, pos. 49–64	The cryptogram is generated by the card and passed to the device in response to the GENERATE AC command.
Application Interchange Profile	'82' (L 2)	Card	Application Interchange Profile	Mandatory	13 or 55	Mandatory	TCR 7, pos. 45–48	
Application PAN Sequence Number	'5F34' (L 1)	Card	Card Sequence Number (L 2)	Conditional	23	Conditional	TCR 7, pos. 7-9	• If this tag is present on the card, the device must forward it to the acquirer in the device-to-acquirer message and the acquirer must forward it to the issuer in the acquirer-to-VisaNet message unaltered. • The Card Sequence Number must match what was received from the card or cryptogram validation fails.
Application Transaction Counter	'9F36' (L 2)	Card	Application Transaction Counter	Mandatory	13 or 55	Mandatory	TCR 7, pos. 41–44	
Authorization Response Code	'8A'	Issuer (for online authorizations) Device (for offline authorizations)	Response Code	Mandatory	39	Mandatory	TCR 5, pos. 35–36	• If the transaction is online authorized, the issuer provides the authorization response in V.I.P. Field 39. The acquirer forwards the information to the device via Tag 8A. • If the transaction is offline authorized, the device provides the authorization decision to the acquirer in the clearing message. The acquirer formats this information in the BASE II clearing message in the TCR 5. It contains one of the following values: – **Y1** = Offline approved – **Y3** = Unable to go online; offline approved • Other values include: – **Z1** = Offline declined – **Z3** = Unable to go online; offline declined Z1 and Z3 are not generally provided on clearing transactions as they represent declines.

EMV Data Element	Tag	Origin	VisaNet Data Element	Authorization Requirement	V.I.P. Field[55]	Clearing Requirement	BASE II	Notes
Cardholder Verification Method Results (CVMR)	'9F34'	Terminal	CVMR	Optional	55	n/a	n/a	This is expected to be mandated in VE in October 2015.
Dedicated File (DF) Name (contains AID)	'84' (L5-16)	Card	Dedicated File (DF) Name	Optional	55	n/a	n/a	Contains the Application Identifier (AID) that was selected to initiate the transaction. This data element may need to be transported from the device to the acquirer (and any other routing entities) to support routing.[56] It does not, however, need to be provided in messages to VisaNet. For routing purposes, only the RID portion of the DF Name needs to be examined.
Issuer Application Data	'9F10' (32 bytes of data for a total of 33 bytes)	Card	Issuer Application Data	Mandatory	134 or 55	Mandatory	Byte 1, Pos. 117-118 Bytes 2–3, pos. 65–68 Bytes 4–7, pos. 79–86 Bytes 8–16, pos. 101–116 Bytes 17–32, pos. 119-150	• The format of the Issuer Application Data may vary by card, but this is transparent to the acquirer. • In authorization messages, expanded third bit map acquirers send the entire contents of the Issuer Application Data as provided by the card in V.I.P. Field 134, which has been expanded to 33 bytes (1 byte length byte and up to 32 bytes of data).
Issuer Authentication Data	'91' (L8–16)	Issuer	Issuer Authentication Data	Conditional	140 or 55	n/a	n/a	• If present in the response, it is present in the authorization response to the acquirer and the acquirer must include it in the device-to-acquirer message. • The content of the Issuer Authentication Data is transparent. It should be passed, as is, to the device. No format conversion from EBCDIC to ASCII is required.

[56] In the U.S., the DF Name must be transported from the device to the acquirer as of October 2015.

EMV Data Element	Tag	Origin	VisaNet Data Element	Authorization Requirement	V.I.P. Field[55]	Clearing Requirement	BASE II	Notes
Issuer Script 1 Results	'9F5B' (L var.)	Device (based on the results of applying the Issuer Script)	Issuer Script Results	Conditional	143 or 55	Conditional	TCR 7, pos. 159–168	• This data element is present only in reversals (0400) or clearing messages when there is an Issuer Script. It is not present in authorization messages (0100/0200). The device sends this tag when there is a reversal. • Reversal—If the issuer provides any Issuer Scripts in the response along with an approval authorization response but the card overrides the issuer's authorization with a decline, a reversal must be generated. The reversal must contain the Issuer Script results if the authorization response contained any Issuer Scripts. • Clearing—If the issuer provides Issuer Script in the response and the transaction is approved, the script results must be provided to the issuer in the clearing message. • If there is no reversal or clearing message from the device, Issuer Script Results are not provided by this tag. The results of script processing are sent in the next online authorization in the Card Verification Results in Tag '9F10', byte 4.
Issuer Script Template 1	'71' (L var.)	Issuer	Issuer Script	Conditional	142 or 55	n/a	n/a	• The issuer may provide this information in the response when applicable. The issuer provided Tag "71' or '72' (not both). • If present in the response, the acquirer must forward it to the device in the device-to-acquirer message
Issuer Script Template 2	'72' (L var.)	Issuer	Issuer Script	Conditional	14 or 55	n/a	n/a	• The issuer may provide this information in the response when applicable. The issuer provides Tag '71' or '72' (not both). • If present in the response, the acquirer must forward it to the device in the device-to-acquirer message

EMV Data Element	Tag	Origin	VisaNet Data Element	Authorization Requirement	V.I.P. Field[55]	Clearing Requirement	BASE II	Notes
POS Entry Mode	'9F39'	'9F39'	POS Entry Mode Code (V.I.P.) POS Entry Mode (BASE II)	Mandatory	22	Mandatory	TCR 0, pos. 162–163	Valid values are: • 01—Manually entered PAN (customer present) • 02—Magnetic stripe read and CVV may be unreliable (normally used only if full magnetic stripe cannot be transmitted) • 05—Chip transaction • 07—Contactless using qVSDC rules • 08—Manually entered PAN (mail order/telephone order/e-commerce) • 90—Magnetic stripe read (full magnetic stripe transmitted in message) • 91—Contactless using MSD rules • 95—Chip transaction and CVV may be unreliable (normally used only VisaNet when it detects certain errors)
Chip Condition Code	n/a	Device	Chip Condition Code	Optional	60.3	Optional	TCR 1, pos. 167	• For magnetic-stripe-read transactions, the valid values in this field are: – **0**—Not applicable; subsequent subfields in V.I.P. Field 60 are present. – **1**—Magnetic stripe Service Code begins with 2 or 6 and the last chip card read at chip-capable device was either a successful chip read or the transaction was not a chip transaction. – **2**—Magnetic stripe Service Code begins with 2 or 6 and the last chip card read at chip-capable device was an unsuccessful chip read. • For contact chip transactions, this field should not be present or should contain **0**.
Terminal Capabilities	'9F33' (L 3)	Device	Terminal Capability Profile	Mandatory	130, or 55	Mandatory	TCR 7, pos. 16–21	
Terminal Country Code	'9F1A'(L 2)	Device	Terminal Country Code	Mandatory	145 or 55	Mandatory	TCR 7,pos. 22–24	

EMV Data Element	Tag	Origin	VisaNet Data Element	Authorization Requirement	V.I.P. Field[55]	Clearing Requirement	BASE II	Notes
Terminal Entry Capability	n/a	Device or acquirer	Terminal Entry Capability (V.I.P.) POS Terminal Capabilities (BASE II)	Mandatory	60.2	Mandatory	TCR 0, pos. 158.	The VisaNet chip value is to be used only if the device is capable of reading and processing the contact chip data
Terminal Transaction Date	'9A' (L 3)	Device	Terminal Transaction Date/ Transaction Date	Mandatory	146 or 55	Mandatory	TCR 7, pos. 10–15	
Terminal Verification Results	'95' (L 5)	Device (populated based on the results of each transaction)	Terminal Verification Results	Mandatory	131 or 55	Mandatory	TCR 7, pos. 69–78	
Transaction Currency Code	'5F2A' (L 2)	Device	Authorization Currency Code/ Cryptogram Currency Code/ Transaction Currency Code	Mandatory	148 or 55	Mandatory	TCR 5, pos. 32–34	
Transaction Type	'9C' (L 1)	Device (based on the type of transaction)	Cryptogram Transaction Type/ Transaction Type	Mandatory	144 or 55	Mandatory	TCR 7, pos. 5-6	
Unpredictable Number	'9F37' (L 4)	Device	Unpredictable Number	Mandatory	132 or 55	Mandatory	TCR 7, pos. 33–40	
n/a	n/a	n/a	Card Authentication Reliability Indicator	Mandatory	60.7	n/a	n/a	Acquirers need to populate this subfield with the appropriate value indicating the integrity of the cryptogram data.
n/a	n/a	n/a	VSDC Transaction Indicator	Mandatory	60.6	n/a	n/a	Acquirers need to populate this field correctly in either V.I.P. Field 55 or in the expanded third bit map. Acquirers need to populate this field correctly in either V.I.P. Field 55 or in the expanded third bit map.

Appendix E. Placement of Contactless Readers

This appendix contains recommendations developed by Visa as general guidance for the placement of contactless devices in a merchant retail environment. 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. Merchants and acquirers are advised to consult with their Visa representatives.

Note: If a device is to accept Visa contactless cards, the contactless device must be tested by a Visa-recognized laboratory and receive an approval from Visa prior to its placement in a merchant retail environment. Merchants should, in general, consult with their acquirers and contactless card reader manufacturers to determine the current approval status of their contactless card readers. See www.visa.com/industryservices for lists of contactless card readers as they are approved.

E.1 Compliance With Local Regulatory Requirements

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

E.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.

E.3 Proximity to Transmitting Devices

Active transmitting devices (for example, mobile telephones, personal digital assistants, and pagers) 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.

E.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 (for example, personal computers, lighted displays, cooking appliances, or refrigeration equipment).

To protect contactless cards from problems at the point of sale, 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 (for example, 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.

E.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 (for example, 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.

E.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.

E.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.

E.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: Terminal 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 F. Visa U.S. Common Debit AID

This appendix 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 *EMF U.S. Debit Technical Solution* white paper developed by the EMV Migration Forum (EMF) Debit Technical Working Group.

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').

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 3.3.7: Application Label and Application Preferred Name. Note also that merchants may choose to offer enhanced descriptors for debit applications as further described in Section 4.4.2 of the *Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide*.

F.1 Background

To support debit routing, U.S. Covered Visa Debit Cards[57] will be issued with both the Visa AID and the Visa U.S. Common Debit AID and both AIDs may be present in U.S. terminals. When the Visa U.S. Common Debit AID is the AID selected for the transaction, U.S. merchants and acquirers can use BIN routing logic to route these transactions to the appropriate debit network. When the Visa AID is selected, the transaction must be routed to Visa.

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

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

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

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

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

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

Recommended PIN opt-out options include:

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

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

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

F.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 to the Visa U.S. Common Debit AID using special terminal logic, if they so desire. See F.3.2: Special Application Selection Logic.

F.3.1 Select 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 the Visa AID must be routed to a Visa network).

F.3.2 Special Application Selection Logic

Another approach is for the terminal to identify cards that contain both the Visa AID and the Visa U.S. Common Debit AID and eliminate one of the AIDs from the Candidate List (when these AIDs share the same funding source ["debit pairs"]). The remaining AID can then be used for routing purposes. This approach, and other options, are discussed in more detail in Section 4.4 and Appendices D and E of the *Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide*.

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

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

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

This approach is discussed in more detail in Section 4.5 and Appendices D and E of the *Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide*.

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

Assumptions for EMV Processing Approaches

1. U.S. Covered Visa Debit Cards will contain a Visa U.S. Common Debit AID in addition to the 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 will result in two eligible AIDs. Either the highest priority AID can be selected to initiate the transaction or the two AIDs can be presented to the cardholder for selection. Merchants that wish to maintain routing flexibility will need to deploy specific logic in their readers/terminals to ensure the Visa U.S. Common Debit AID is used for debit functionality, in addition to the non-paired Visa AID for credit functionality.
3. The terminal must pass the AID (contained in the DF Name, Tag '84') used to initiate the transaction to the acquirer or other routing entity in the transaction message to enable the acquirer or other routing entities to perform appropriate routing.

U.S. Territories and Protectorates

If there is a business need in a U.S. Territory to support the Visa U.S. Common Debit AID, the terminal should set the Terminal Country Code (Tag '9F 1A') to '08 40' *for the Visa U.S. Common Debit AID only*. This will allow acceptance of the Visa U.S. Common Debit AID.

Appendix G. Contactless ATM Requirements

This appendix outlines the requirements and recommendations to support the acceptance of contactless cards and other contactless form factors at ATMs.

Note: This appendix focuses on Visa, Visa Electron, and Plus transactions at ATMs.

G.1 Transaction Processing Overview

Pre-Requisite: The EMV-compliant ATM has been upgraded for qVSDC (VCPS 2.1.1), has undergone required testing, and received the appropriate approvals. For more information on testing and approvals, refer to Section G.2.1: Device Testing and Certification.

Important: The contactless transaction flow at an ATM follows a similar path to that of a POS transaction, with the key differences that ATMs are online-only, do not perform Pre-Processing, do not perform Offline Data Authentication, and only support Online PIN as the CVM.

1. **Transaction Initiated**—The cardholder initiates a contactless transaction by tapping the card on the contactless landing plane. The device obtains and reads the PPSE from the card.
2. **Application Selected**—The ATM selects the highest priority, mutually supported contactless application.[58]
3. **Data and Cryptogram Obtained**—The transaction begins with the ATM obtaining data from the contactless card. This includes the ATM sending the card the GET PROCESSING OPTIONS command. Since the amount and transaction type are not known at this time, the ATM sends the card a zero amount and a default transaction type of Cash Disbursement to use in cryptogram generation. The card responds to GET PROCESSING OPTIONS with data including the cryptogram.

   If additional card data is required for the transaction, the ATM sends one or more READ RECORD commands to the card to retrieve the additional data.

   Note: Assuming that the cardholder requests a Visa-related service (i.e., Cash Disbursement, Balance Inquiry, or Funds Transfer) in Step 6 below, the ATM will submit the cryptogram and its associated data in the online authorization request to the issuer (refer to Step 8).

   Now that the ATM has all the information it needs from the card, the interaction between the ATM and the card is complete. The ATM powers off the contactless interface and informs the cardholder that the card can be removed from the landing plane.

[58] If the ATM supported a separate domestic debit application selection process, it would take place at this time.

4. **ATM Offline Check Performed**—The ATM may optionally perform the ATM Offline Check Processing Restriction. With this check, the ATM reviews the Card Transaction Qualifiers (CTQ) (obtained from the card) and may also review the Application Usage Control (AUC) (also obtained from the card). This information is used to determine whether the contactless ATM transaction should be sent online, declined offline, or switched to the contact chip interface. When the ATM Offline Check Processing Restriction is not supported, all contactless ATM transactions are sent online.

   Note: The ATM Offline Check is strongly recommended in the Europe Region and optional everywhere else.

   Exception: If the ATM is unable to proceed with the transaction based on the results of the ATM Offline Check, the ATM will display an appropriate message to the cardholder about the next step (the cardholder is requested to insert his/her card into the ATM to complete the transaction or use another card).

5. **Online PIN Requested**—The cardholder is requested to enter his/her Online PIN. The PIN is captured and may be submitted in the online authorization request in Step 7.

6. **ATM Services Offered**—The ATM presents its services to the cardholder and the cardholder selects a Visa-related service (such as Cash Disbursement, Balance Inquiry, or Funds Transfer).

   Note: An ATM enabled to support contactless transactions should aim to support the same range of Visa transaction types for contactless transactions as for contact chip.

7. **Online Authorization**—The ATM sends an online authorization request to the issuer. This message includes the cryptogram obtained from the card in Step 3 as well as the Online PIN obtained from the cardholder in Step 5. While the amount and transaction type associated with the cryptogram are zero and Cash Disbursement respectively, the amount and transaction type in the standard authorization message fields reflect the actual amount of the transaction and its transaction type.

   Note: This means that the amount in Field 4 and Field 55/Expanded Third Bit Map and the Transaction Type in Field 3 and Field 55/Expanded Third Bit Map may not match.

8. **Service Processed**—Assuming that the transaction is approved, the ATM carries out the service (e.g., dispensing cash, displaying available balance, transferring funds, etc.).

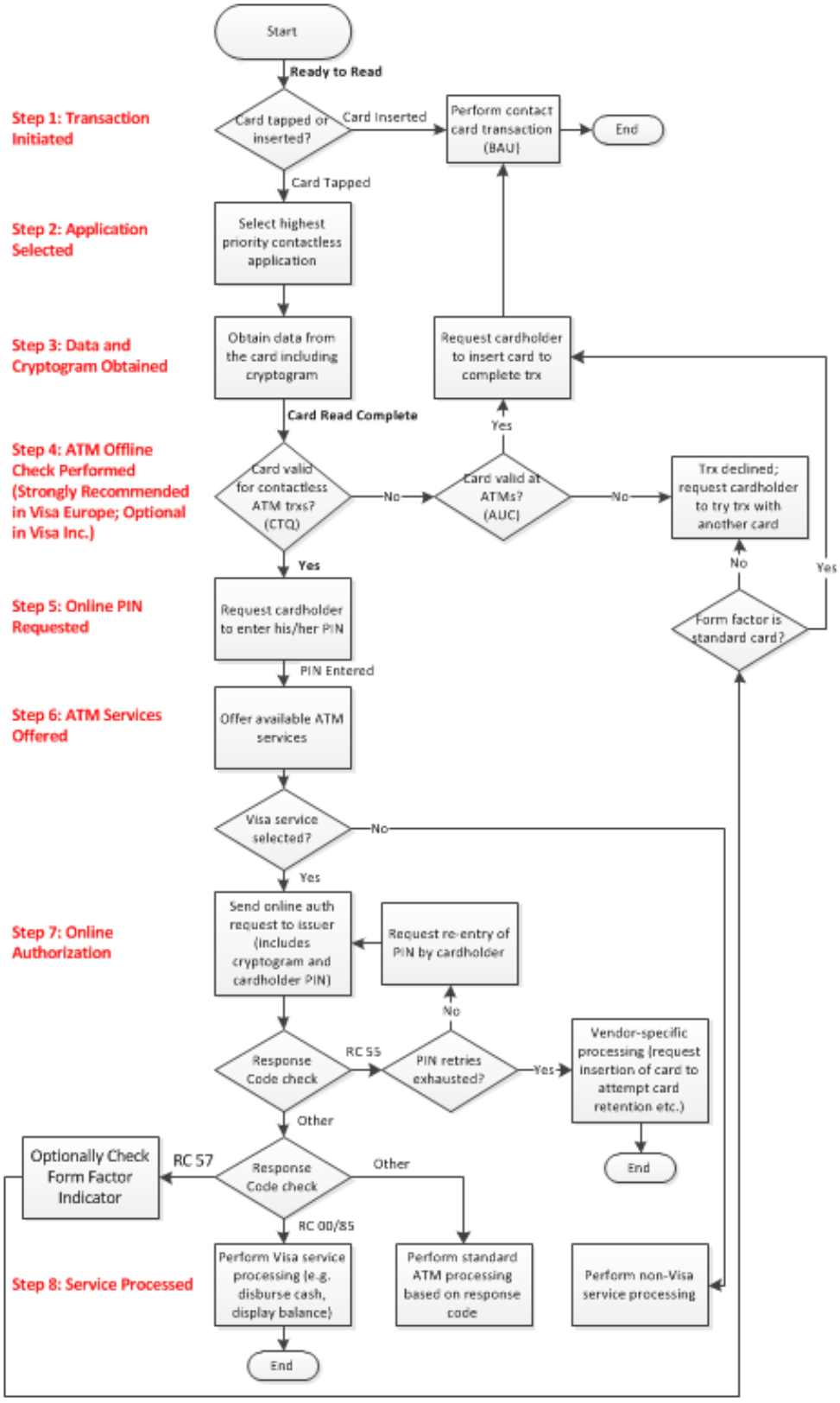
   Exception: If Visa declines the transaction with Response Code 57, the ATM may optionally check the Form Factor indicator and, based on the form factor used, can use this information to display a tailored message to the cardholder about the next. For example: “Insert card” or “Use another card to complete the transaction”.

   Transaction Chaining (Not Outlined in the Flow Diagram)—If the cardholder would like to perform another transaction (for example, a Cash Disbursement after a Balance Inquiry), PIN entry is required but re-tapping the card on the contactless interface differs depending on whether the transaction is financial or non-financial:

a) **Financial Transactions (e.g., Cash Disbursements)**—PIN entry is required and re-tapping is recommended.

b) **Non-Financial Transactions (e.g., Balance Inquiries)**—PIN entry is required and re-tapping is optional.

Figure G–1: Contactless ATM Transaction Flow



G.2 Requirements

This section outlines the requirements associated with contactless-enabled ATMs.

G.2.1 Device Testing and Certification

The device must be tested prior to deployment. The testing requirements differ depending on whether the device was developed to:

- *VCPS* (Table G–1: VCPS—Device Testing)
- *EMV Contactless Specifications for Payment Systems* (Table G–2: EMV Contactless Specifications for Payment Systems—Device Testing)

Refer to the appropriate table for the testing information.

The table below summarizes the contactless specific elements of a terminal implemented using *VCPS* that require testing and approval.

Table G–1: VCPS—Device Testing

Component	Tested/Certified by	Reference
Contactless-Enabled ATM[59]	Europe Region: Acquirer through VpTT (test results approved by the Europe Region)	This document Europe Region: Visa Europe payWave Terminal Test Procedures
	Visa (except for Europe Region): Acquirer through Acquirer Device Validation Tool (ADVT) and Contactless Device Evaluation Tool (CDET)	This document Visa Inc.: ADVT User Guide, CDET User Guide
Visa Contactless Reader Application	Visa Inc. Approval Services	*Visa Contactless Payment Specification*
Contactless Communication Layer	EMVCo	*EMV Contactless Specifications for Payment Systems* (Book D)

[59] If supported, the ATM Offline Check processing restriction described in Section G.2.12: ATM Offline Check Processing Restriction must be implemented in the ATM system (not the reader kernel).

The table below summarizes the contactless specific elements of a terminal implemented using *EMV Contactless Specifications for Payment Systems* that require testing and approval. The highlighted row identifies the differences between devices implemented using *EMV* and *VCPS*.

Table G–2: EMV Contactless Specifications for Payment Systems—Device Testing

Component	Tested/Certified by	Reference
Contactless-Enabled ATM[60]	Europe Region: Acquirer through VpTT (test results approved by the Europe Region)	This document Europe Region: Visa Europe payWave Terminal Test Procedures
	Visa (except Europe Region): Acquirer through Acquirer Device Validation Tool (ADVT) and Contactless Device Evaluation Tool (CDET)	This document Visa Inc.: ADVT User Guide, CDET User Guide
EMVCo contactless reader application (including Entry Point and Kernel C-3)	EMVCo	*EMV Contactless Specifications for Payment Systems* (Books A, B, C-3)
Contactless Communication Layer	EMVCo	*EMV Contactless Specifications for Payment Systems* (Book D)

G.2.2 Supported Interfaces

An ATM which is capable of processing contactless transactions shall also be capable of processing contact chip and magnetic-stripe transactions.

G.2.3 Mandatory and Not Supported Features

The contactless-enabled ATM shall support all mandatory features and transaction types listed in the following table to the extent described.

The contactless-enabled ATM shall either not support, or shall disable, all features and transaction types listed in the below table as 'Not supported'.

[60] If supported, the ATM Offline Check processing restriction described in Section G.2.12: ATM Offline Check Processing Restriction must be implemented in the ATM system (not the reader kernel).

Table G–3: Mandatory and Not Supported Features

Contactless ATM Features	Requirements
MSD	Not supported[61]
qVSDC	**Mandatory**
Offline Authorization	Not supported
Online Authorization	**Mandatory**
Online PIN	**Mandatory** This is the only Cardholder Verification Method permitted at ATMs
Signature	**Mandatory** In order to maximize card acceptance, support for Signature CVM must be indicated, although Online PIN will be the CVM that is performed for all contactless-initiated ATM transactions
Receipts	**Mandatory** Same requirements as contact; Refer to the Section 2.7: Transaction Receipts for details
Consumer Device CVM (CDCVM)	**Mandatory** Support for CDCVM is mandatory in *Visa Contactless Payment Specification* and *EMV Contactless Specifications for Payment Systems* Kernel 3, although Online PIN will be the CVM that is performed for all contactless-initiated ATM transactions
Pre-Processing[62]	Not supported[63] Contactless-enabled ATMs do not perform pre-processing and the reader is always initiated in the **Ready to read** state
Offline Data Authentication (For qVSDC – fDDA)	Not supported
Dynamic Reader Limits	Not supported
Capability to display and print Available Offline Spending Amount	Not supported
Contact Chip	**Mandatory**
Issuer Update Processing	Not supported for contactless (but **Mandatory** for contact)

[61] MSD acceptance remains optional in the U.S. region but is strongly discouraged.
[62] As described in *Visa Contactless Payment Specification* and *EMV Contactless Specifications for Payment Systems*.
[63] As per the *Visa Contactless Payment Specifications*, 'pre-processing' refers to a terminal obtaining the transaction amount and performing the reader risk management prior to a contactless transaction being initiated.

Contactless ATM Features	Requirements
ATM Offline Check	**Strongly Recommended** in the Europe Region **Optional** in all other countries
Form Factor Indicator Check	**Optional**
Form Factor Indicator	**Conditional** Must be provided in authorization message if present on card
Customer Exclusive Data	**Conditional** Must be provided in authorization message if present on card

G.2.4 Security Considerations

Contactless-enabled ATM vendors should follow industry best practices when designing and developing solutions to ensure payment data and transaction security.

Vendors should take all reasonable steps to design the ATM such that the contactless reader cannot be covered or obscured by a fraudster seeking to force a compromised magnetic-stripe slot to be used.

Contactless readers should be integrated into the overall design of the ATM in a seamless manner and avoid the appearance of being an external attachment.

The contactless-enabled ATM shall provide a mechanism to protect all Visa contactless configuration data from being loaded, altered, or deleted without the appropriate authority (for example, by the acquirer or merchant).

G.2.5 ATM Transaction States

In terms of the processing defined in *Visa Contactless Payment Specification* and *EMV Contactless Specifications for Payment Systems*, when a contactless card is presented to the reader at a contactless-enabled ATM, the interaction between the two is limited to that performed between the following two transaction states:

- **Ready to read**—The reader is ready to read a contactless card. **Note:** Contactless ATMs do not support Pre-Processing.
- **Card read complete**—The interaction between the card and the reader is complete and the cardholder can remove the card from the landing pad.

The contactless transaction stops at this stage, and the contactless-enabled ATM continues with all further processing.[64]

Indication of the **Card read complete** transaction state to the cardholder is required. This may be done using either a dedicated message for this purpose or a message that indicates the next step to be taken by the cardholder. For example, if the next step to be taken by the cardholder is the entry of their PIN, the vendor or service provider may choose to display a message to the cardholder stating, "Please enter your PIN" as the indication of the **Card read complete** transaction state.

G.2.6 Performance Requirements

Per the *Visa Contactless Payment Specification* and the *EMV Contactless Specifications for Payment Systems* the time between:

- Card discovery (the start of the first ISO 14443-3 command from the reader to which the card responds), and;
- The completion of card read (the point at which communication is no longer required with the card such that the contactless interface can be powered off)[65]

Shall not exceed 500ms for a transaction where the card read completes successfully with no communication errors.

400ms of the 500ms is reserved for card processing and radio frequency (RF) level communication from the card to the reader. Consequently, all contactless-enabled ATM system processing and RF-level communication from the reader to the card shall be performed within 100ms.

[64] Unless "transaction chaining" takes place (i.e., where the cardholder wants to perform another transaction during the same session). If the subsequent transaction is a financial transaction, PIN entry is required and re-tap is recommended; if the subsequent transaction is non-financial transaction, PIN entry is required and re-tap is optional.

[65] *EMV Contactless Specifications for Payment Systems* Book A section 10.1 describes the methods by which the performance can be measured. Some contactless-enabled ATMs may not provide a user interface indication to the cardholder that their card may be removed. Therefore, terminals without an audio or visual indication of card read complete must make special provision for testing as described therein.

G.2.7 Data Elements and Configuration Parameters

The contactless-enabled ATM shall support the configurable data elements and parameters listed in the following table.

Table G–4: Mandatory Data Elements and Configuration Parameters

Name	Tag	Description
Application Identifier (AID)	'9F06'	AIDs for Visa payment applications supported by the contactless-enabled ATM. This may include regional or program specific AIDs. Requirement: Same as contact.
Merchant Name and Location	'9F4E'	Indicates name of the contactless-enabled ATM service provider / member and the location of the ATM. Consumer devices such as mobile phones may use this data element in their history logs. Requirement: Same as contact.
Terminal Country Code	'9F1A'	Identifies the country in which the contactless-enabled ATM is located. Encoded according to ISO/IEC 3166-1.
Terminal Transaction Qualifiers (TTQ)	'9F66'	Indicates the terminal reader capabilities, requirements, and preferences to the contactless card. See the following table for required TTQ settings.
Transaction Currency Code	'5F2A'	The currency code for the transaction. Encoded according to ISO/IEC 4217.
Transaction Date	'9A'	Local date that the transaction was performed.

TTQ Settings

The contactless-enabled ATM shall configure TTQ (Tag '9F66') as shown in the following table:

Note: The contactless-enabled ATM indicates in TTQ that it supports the contactless CVM methods shown in the following table even though it will only perform Online PIN for cardholder verification. This ensures that the card application will not request termination of the transaction due to contactless-enabled ATM's inability to support a given type of cardholder verification (e.g., Signature).

Table G–5: TTQ Settings

Name	Tag	Description
1	8	0b = MSD *not supported*
	7	RFU (0b)
	6	1b = qVSDC supported
	5	1b = EMV Contact Chip supported
	4	0b = Online capable reader[66]
	3	1b = Online PIN supported
	2	1b = Signature supported[67]
	1	0b = ODA for Online Authorizations not supported
2	8	1b = Online Cryptogram required
	7	0b = CVM not required
	6	0b = (Contact Chip) Offline PIN not supported
	5-1	RFU (00000b)
3	8	0b = Issuer Update Processing not supported
	7	1b = Mobile functionality supported (Consumer Device CVM)[68]
	6-1	RFU (000000b)
4	8-1	RFU ('00')

G.2.8 Amount and Transaction Type

Since the amount and transaction type are not known when the ATM requests the cryptogram from the card, the ATM provides the card with a zero amount and a Cash Disbursement transaction type to use in cryptogram generation.

This means that:

- Cryptogram Amount (Tag '9F02') sent in Field 55/Expanded Third Bit Map of the online authorization request will be zero and, in the case of Cash Disbursement, will have a different value from Field 4 (Transaction Amount).

[66] A value of '0b' indicates that the reader is online capable.
[67] The contactless-enabled ATM should indicate support for Signature CVM even though signature verification will not be performed, as this may prevent some cards being rejected unnecessarily.
[68] The contactless-enabled ATM should indicate support for Consumer Device CVM (CDCVM) even though online PIN will be performed, as this may prevent some cards being rejected unnecessarily

- Cryptogram Transaction Type (Tag '9C') will be set to '01-Cash Disbursement' and may be different from the value in Field 3.1 (Transaction Type) in the event that the resulting transaction is not a Cash Disbursement.

When re-tapping is supported with transaction chaining (i.e., re-tapping is recommended for financial transactions and optional for non-financial transactions), the cryptographic data may be updated to include the correct cryptographic amount and transaction type. For more information on transaction chaining, refer to Section G.2.16: Transaction Chaining.

G.2.9 Issuer Updates (Not Supported)

Issuer update processing for contactless transactions is not supported. The ATM shall discard any Issuer Authentication data or Issuer Scripts that are received in an online authorization response.

G.2.10 PIN Services

Background:

Standard Visa PIN Management Services allow ATMs to provide a PIN change / unblock service over the contact interface of VSDC cards.

The PIN change process allows a card that supports Offline PIN to update it in the card via an Issuer Script, synchronizing it with the changed Online PIN value held in the issuer host. If the Issuer Script is not successfully applied to the card then the ATM generates a reversal message to the issuer host, backing out the Online PIN change, too. This process ensures that the two PIN values are kept in synchronization with each other.

Because Issuer Script is not supported via the contactless interface, Visa PIN Management is only supported over the contactless interface for cards and devices that do not support Offline PIN (i.e., for these cards, the Online PIN can be changed and since Offline PIN is not supported, synchronization of the Offline PIN value with the Online PIN value using Issuer Script is not applicable).

Requirement:

Contactless-enabled ATMs shall not offer the Visa PIN Management Service for transaction sessions initiated over the contactless interface by cards or payment devices potentially supporting Offline PIN. These cards or payment devices shall be recognized by means of the Form Factor Indicator.

Note: Because the Visa PIN Management Service is still permitted over the contact interface at contactless-enabled ATMs, the vendor / service provider can choose how to inform or instruct the cardholder after they have tapped their contactless card. For example, PIN change / unblock may not appear on the ATM display menu at all. Alternatively, it may be offered on the menu, but if the choice is selected, a display message informs the cardholder to insert their card instead and the session terminated. Such options are at vendor / service provider discretion.

G.2.11 Online Authorization and Clearing Data Elements

The following table outlines the data element values that contactless-enabled ATMs use in online authorizations and clearing messages to distinguish them from contact-initiated transactions.

Table G–6: POS Entry Mode and Terminal Entry Capability

Data Element	Field	Value
POS Entry Mode	22 TCR 0, pos. 162–163	07 (Contactless transaction)
Terminal Entry Capability	60.2 TCR 0, pos. 158	5[69] (Contact chip, magnetic stripe, or contactless capable terminal)

Customer Exclusive Data

Customer Exclusive Data (Tag '9F7C') shall be captured and stored for use in online authorization messages if:

- This data element is provided to the reader by the card, and;
- The communications protocol between the contactless-enabled ATM and acquirer supports the transmission of this data element.

Form Factor Indicator

Form Factor Indicator (Tag '9F6E')[70] shall be captured and stored for use in online authorization messages and clearing records if this data element is provided to the reader by the card (regardless of whether the ATM supports the Form Factor Indicator check outlined in Section G.2.13: Checking the Form Factor Indicator.

[69] Because contact chip is supported, a value of 5 is used for this field in all transactions including Visa contactless transactions. Contactless-only ATMs are not permitted.

[70] **Visa Inc.:** Visa Inc. has mandated that all issuers must personalize the FFI in all contactless cards and mobile devices from **October 1, 2015** (April 2015 in AP and CEMEA). Acquirers must provide the FFI to Visa in authorization and clearing messages from **October 2015** if provided by the contactless card or mobile device.

Europe Region: Europe Region has mandated that issuers must personalize the FFI in all contactless cards and mobile devices from **May 1, 2014**. Acquirers must provide the FFI to the Europe Region in authorization and clearing messages from **April 17, 2015** if provided by the contactless card or mobile device.

G.2.12 ATM Offline Check Processing Restriction

EMV Contactless Specifications for Payment Systems, Book C-3, Req 5.5.1.5 defines a method by which a contactless-enabled ATM is able to determine whether or not a presented contactless card supports:

- Contactless ATM transactions without having to send an online authorization request to Visa.
- ATM transactions over the contact interface. This provides the opportunity for the ATM to request the cardholder to insert the card rather than simply informing the cardholder that the transaction cannot be completed. This provides a clean and convenient consumer experience for cardholders.

In the Europe Region, contactless-enabled ATMs are strongly recommended to support this check while it is optional in all other countries/regions.

G.2.13 Checking the Form Factor Indicator

If Visa declines the ATM transaction with Response Code 57 (indicating that the issuer has not turned on contactless support), the ATM may optionally check the Form Factor Indicator (if present).

The information obtained from the Form Factor indicator can be used by the ATM to determine the best message to display to the cardholder about the next step in the transaction:

- If FFI, Byte 1, bits 8-6 = 001 (FFI version number 1) and FFI, Byte 1, bits 5-1 = 00000 (standard card), the ATM shall display an appropriate message to prompt the customer to insert their card into the ATM for service. For example, "Your issuing institution does not support this transaction type. Please insert your card into the ATM to perform your transaction."
- If FFI indicates that the cardholder tapped any other form factor or version number, then the ATM shall terminate the transaction and shall display an appropriate message to prompt the customer to try another card or product. For example, "Your issuing institution does not support this transaction type. Please use an alternative card."

If the FFI is not returned by the card, the ATM shall terminate the transaction and the cardholder shall be prompted to use another card.

G.2.14 Dynamic Currency Conversion (DCC) (Europe Region Only)

Contactless-enabled ATMs offering the DCC service in the Europe Region shall not present the DCC option and the relevant DCC transaction information (exchange rate, amount to be charged in application currency) to the cardholder until after the PIN has been entered, a cash disbursement has been requested, and the required amount entered.

G.2.15 Receipt Requirements

Receipt requirements are the same as for contact chip cash disbursements at ATMs. Refer to the Section 2.7: Transaction Receipts for details.

G.2.16 Transaction Chaining

For contactless-initiated ATM transactions, acquirers are permitted to prompt the cardholder to select additional transaction services in the same session (this is referred to as "transaction chaining".

For each additional transaction in the same session, cardholders must be prompted to re-enter their PIN but re-tapping differs depending on whether the transaction is financial or non-financial:

Table G–7: Transaction Chaining Requirements

Data Element	PIN Entry	Re-Tapping
Financial Transactions (e.g., Cash Disbursements)	Mandatory	Recommended
Non-Financial Transactions (e.g., Balance Inquiries)	Mandatory	Optional

Note: When re-tapping does not take place, the cryptogram data will be the same as the initial transaction although the standard authorization data containing the amount and the transaction type will reflect the current transaction. Because the same cryptogram data is used on both transactions, the two transactions will contain the same Application Transaction Counter (ATC).

G.2.17 Transaction Initiation

Contactless-enabled ATMs should be implemented in such a way that cardholders do not need to perform any action in order to indicate a desire to use a contactless card to initiate a transaction. This means that the contactless reader should be in the **Ready to read** state as the cardholder approaches the ATM. If the cardholder chooses to insert their card in order to perform a contact chip or magnetic-stripe transaction, then the contactless interface should be powered off so as not to interfere with the transaction. Similarly, if the cardholder initiates a transaction through the contactless interface, the card slot should be disabled.

Disablement of Unused Interface

The contactless interface shall always be powered off when initiating, and for the duration of, ATM transactions conducted over other interfaces (i.e., contact chip or magnetic stripe). The contactless-enabled ATM shall not initiate a contactless transaction if a card is inserted into the ATM's contact reader.

Conversely, the contact chip and magnetic-stripe interface shall be disabled after a contactless transaction has been initiated.

Unintentional Initiation of Contactless Transaction

The contactless-enabled ATM shall be designed to avoid accidental initiation of a contactless transaction. The contactless reader shall be situated so that a card can be inserted into the ATM's contact reader without initiating a contactless read.

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 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 together).

Ready to Read

The contactless interface shall be ready to read a contactless card (discovery processing initiated) without the need for explicit cardholder activation.

For example, the contactless interface may be always active, or the contactless interface may be activated by detection of the presence of a cardholder.

Note: If the contactless-enabled ATM activates the contactless reader by detection of the presence of a cardholder, it may also power off the contactless reader by detection of the absence of a cardholder.

G.2.18 User Interface Requirements

The user interface design should enable cardholders to easily understand the status of their contactless-initiated ATM transactions by the use of clear indications and messages. The user interface design should adhere to one of the two options outlined in the *EMV Contactless User Interface Guidelines*. Contactless transaction states and error conditions should be handled and captured appropriately.

The user interface requirements described in this section are illustrated with an example display containing the required or recommended message. The details of the display design and implementation are left to the ATM vendor.

For brand standards, refer to the *Visa Product Brand Standards*.

Card Read Complete

As defined in the Ready to Read section (refer to Section G.2.17: Transaction Initiation), a contactless-enabled ATM will always be in the **Ready to read** state when a cardholder approaches it. When the card is presented, the contactless reader performs the necessary interaction with the card until all required data has been read from it. The **Card read complete** state is then reached and the contactless interface shall be powered off. At this time, the card can safely be removed.

The contactless interface shall remain powered off until the current function or session has been completed.

The reader should not wait for the card to be removed before powering down the contactless interface once the card read has completed.

Card Read Complete: Indication

Upon entering the Card Read Complete state (i.e., when all application data has been successfully read from the card), the contactless-enabled ATM shall indicate this to the cardholder.

This indication can be a distinct card read complete message, an indication to the cardholder of the next action to be taken, or a combination of these messages. The following provides examples:

Example: Card Read Complete

Example: The cardholder must enter their PIN.

Example: The cardholder must insert their card into the reader in order to perform a contact or magnetic stripe transaction, indicating that contactless is not available for this transaction.

Example: The cardholder must use an alternative card.

Card Read Complete Indication: Performance

The card read complete indication shall be given within the performance constraints. Refer to Section G.2.6: Performance Requirements.

Note: The contactless-enabled ATM is not required to complete deactivation of the contactless card, as specified in *EMV Contactless Specifications for Payment Systems*, prior to indicating card read complete.

G.2.19 Consumer Interaction Required

When a consumer device indicates to the reader that consumer interaction is required, the contactless-enabled ATM shall display the "See phone for instructions" message (as specified in *EMV Contactless Specifications for Payment Systems*) and power down the contactless interface.

Note: The consumer's device indicates that consumer interaction is required by responding to the GET PROCESSING OPTIONS command with SW1 SW2 = '6986'.

Consumer device processing is outside the scope of this document. The consumer's device may, for example, be requested to perform some activity on the phone to put it in a state in which it is able to perform payment processing such as entry of a passcode or update of credentials.

Consumer Interaction Required: Return to Discovery Processing

Between 1000ms and 1500ms after powering down the contactless interface to permit the consumer interaction to take place, the reader shall return to discovery processing.

The "See phone for instructions" message shall be retained on the display (as specified in *EMV Contactless Specifications for Payment Systems*).

Note: The retained message could optionally be extended to clarify any further action required by the cardholder. For example, "See phone for instructions then tap it again".

Note: After the reader has returned to discovery processing as described above, the cardholder may:

- Re-present the same consumer device as was used for the original transaction after having performed any necessary interaction (for example, enter their passcode on a mobile phone).
- Choose to present a different contactless card or consumer device.
- Choose to insert a card into the contact reader.

The reader does not retain any card information from the original transaction. If a contactless card is detected, the reader will perform a SELECT PPSE and continue normal processing based on the response from the card. If a contact card is inserted, the contactless reader will be powered down as specified in this document and a normal contact or magnetic stripe ATM transaction will be performed.

G.2.20 Switch to Another Interface Required

Switch Interface Required

If either:

- The card indicates that the transaction should be attempted over a different interface (GET PROCESSING OPTIONS response SW1 SW2 = '6984').

or:

- The ATM identifies that the transaction should be attempted over a different interface (as described in sections *G.2.12 and G.2.13*).

The contactless-enabled ATM shall:

- Power down the contactless interface.
- Discard all card data captured from the contactless-initiated transaction.
- Display the "Please insert card" message (as specified in *EMV Contactless Specifications for Payment Systems*) to indicate that the transaction should be re-started using contact chip or magnetic stripe.

Switch Interface: Enable All Other Interfaces

Immediately after the indication to switch interfaces has been displayed, the reader shall enable all interfaces other than contactless (i.e., contact chip and magnetic stripe).

G.2.21 Error Conditions

Due to the nature of contactless communications and cardholder behavior, communication errors are likely to occur on a relatively frequent basis. From a user interface perspective, it is required that contactless-enabled ATMs do not report, display, or act on recoverable communication errors other than to attempt to re-establish communication with the card or, in the case of an unrecoverable communication error, restart Discovery Processing as specified in *Visa Contactless Payment Specification* and *EMV Contactless Specifications for Payment Systems*.

Unrecoverable communication errors are described in *EMV Contactless Specifications for Payment Systems,* Book D as transmission, protocol, or timeout errors. In all cases, the response of the reader is the same, as defined in the below section titled Error Condition – No Response From Card.

Contactless ATMs must be capable of capturing and logging the error conditions described in the following sections:

- Error Condition: No Response From Card
- Error Condition: Collision Detected
- Error Condition: Unsupported Card or Application Error

Error Condition: No Response From Card

If an unrecoverable communication error (as defined in *EMV Contactless Specifications for Payment Systems*) occurs between the card and reader:

- The contactless-enabled ATM shall not display or report the error to the cardholder.
- The reader shall return to Discovery Processing and attempt to re-initiate communication with the card.

Error Condition: Collision Detected

If the reader detects multiple cards during discovery processing, the contactless-enabled ATM shall display the "Please present one card only" message (as specified in *EMV Contactless Specifications for Payment Systems*).

After the cards have all been removed, the reader shall restart discovery processing.
It is recommended for the ATM to attempt multiple discovery cycles to detect potential collisions and thus ensure that only one card is present. This will prevent the initiation of a transaction with an unexpected card.

Error Condition: Unsupported Card or Application Error

If any of the following conditions are true:

- A payment card containing the Proximity Payment Systems Environment (PPSE) is presented and no mutually supported AID is found;
- A supported AID is found in the PPSE, but a contactless transaction cannot be completed after a Visa application has been selected due to any application error condition not already covered in the above sections "Error Condition: No Response From Card" and "Error Condition: Collision Detected" including:
  - Mandatory data is not present
  - Redundant primitive data elements are encountered

Then the following processing shall be performed:

- The contactless-enabled ATM shall abort the transaction, regardless of whether the data has been successfully read from the card.
- The contactless-enabled ATM shall display the "Insert, swipe, or try another card" message (as specified in *EMV Contactless Specifications for Payment Systems*).
- After the card has been removed and the message has been displayed long enough for the cardholder to read it, the contactless-enabled ATM shall clear the message and the reader shall restart discovery processing.

Appendix H. Region and Country-Specific Requirements and Recommendations

This appendix provides a summary of region and country-specific requirements and recommendations.

H.1 Europe Region

This section provides a summary of requirements and recommendations for acquirers in the Europe Region as of the publication of this document. It contains the following sections:

- Czech Republic, Poland, and Slovakia
- Finland, France, Italy, Turkey, and the United Kingdom
- All of the Europe Region

H.1.1 Czech Republic, Poland, and Slovakia

Dual-Interface Mandate

Effective 1 January 2014

- Any new terminals deployments must support dual-interface (contact chip and contactless) processing.

Effective 1 January 2018

- All new and existing terminals must support dual-interface processing.

H.1.2 Finland, France, Italy, Turkey, and the United Kingdom

Application Selection Requirements

These Application Selection requirements apply to all acceptance devices deployed in countries where Visa SimplyOne cards are already in the environment, or where commitments to issue in significant number by the end of 2012 have been received: Finland, France, Italy, Turkey and the United Kingdom.

As these requirements and recommendations improve transaction speed when multi-application chip cards are used, their implementation at all acceptance devices throughout the Europe Region is strongly recommended in line with other regular device software updates.

The following requirements are required for all new acceptance devices deployed as of 1 March 2013, and for all acceptance devices in the market as of 1 March 2015.

- Except in the exception cases listed below, if more than one application is mutually supported by the card and the acceptance device, the acceptance device:
  - Must not automatically select an application.
  - Must always present to the cardholder a choice between (but not exclusively) all mutually supported Visa applications.
  - Must present as many options as possible on one screen display (that is, selection by confirmation is no longer permitted).
    - When not all options can physically be presented on one screen, clear prompts must indicate how to see any choice not visible on the first screen.
- There are six types of transactions when the terminal is exempted from presenting all applications for choice:

  1. Contactless transactions: automatic selection is mandatory for contactless transactions.
  2. Chip-initiated transactions that occur as a result of a contactless transaction which require completion in contact chip mode: the application used for the initial contactless transaction should automatically be selected during the subsequent contact chip transaction.
  3. Transactions on devices that are currently exempted by Visa rules from use of a PIN Entry Device (currently road and bridge tolls, some vending machines and unattended devices in parking environments). On those devices, automatic selection of the primary application is permitted.
  4. Transactions with Visa cards that, under conditions agreed with Visa, also contain non-Visa payment applications which are considered 'equivalent' from a cardholder's perspective (i.e., co-badged cards). When that is the case, Visa rules allow an acceptance device to not display all applications and recommends presenting for cardholder choice only one of the 'equivalent' applications in order to not confuse the cardholder. That is, the acceptance device may explicitly pre-select which of the equivalent applications to present to the cardholder for choice. If such a 'pre-selection' is performed, the equivalent application which has the highest priority indicator on the card is the one that must be presented for choice to the cardholder.
  5. Transactions at an ATM where the cardholder performs multiple operations with a single account (for example, checking the balance and making a cash withdrawal): the ATM is permitted to re-select the application used in the first part of the transaction.
  6. Transactions where an acceptance device supporting a selectable kernel configuration has restarted a transaction after cardholder selection has already taken place, in order to try to complete a transaction using another kernel configuration allowed by Visa: the device may automatically re-select the application that was selected in the first place.

Further details on these requirements, as well as recommendations for best practices regarding Application Selection can be found in the document 'Visa EMV Application Selection Requirements and Recommendations' available on Visa Online:

https://www.eu.visaonline.com/eu_BusinessPublications/download.asp?file=pdf6003663130231960000

H.1.3 All Europe Region

VCPS 2.1.1

Effective 1 June 2012

- All merchant businesses not accepting contactless payments at any outlets prior to 1 June 2012 must, when they begin accepting contactless payments, only deploy transaction acceptance devices compliant with VCPS 2.1.1 or above.

Effective 1 January 2014

- All newly deployed contactless enabled transaction acceptance devices must be compliant with VCPS 2.1.1 or above; and
- All installed and activated contactless enabled transaction acceptance devices must have migrated to VCPS 2.1.1 or above.

Dynamic Currency Conversion

Effective 4 April 2014

- Dynamic Currency Conversion (DCC) on contactless payments may only be offered where the transaction amount is above the Reader Cardholder Verification Method (CVM) Limit.

Terminal Requirements and Implementation Guide 1.3

Effective 31 March 2014

- All newly deployed and upgraded contactless enabled transaction devices must comply with version 1.3 of the Terminal Requirements and Implementation Guidelines (TIG).

Effective 31 March 2015

- All newly deployed and all existing contactless enabled transaction acceptance devices must comply with version 1.3 or subsequent versions of the TIG.

No CVM

Effective 1 April 2014

- All newly deployed, EMV online-capable UATs, excluding ATMs, must support 'No CVM required' as part of its CVM capabilities.
- Liability under Reason Code 81 – Fraud Card Present Environment – will move to the issuer if that issuer sends an Approval Response for a chip initiated online authorized transaction that took place in a Card-Present environment at an EMV online-capable UAT.

Effective 1 July 2015

- All EMV online-capable UATs, excluding ATMs, must support 'No CVM required' as part of its CVM capabilities.

This appendix provides a summary of requirements for acquirers in Visa Asia Pacific as of the publication of this document.

H.2 Visa Asia Pacific and Central Europe, Middle East, and Africa

This section provides a summary of requirements and recommendations for acquirers in Visa Asia Pacific (AP) and Visa Central Europe, Middle East, and Africa (CEMEA) as of the publication of this document.

H.2.1 Visa AP Wave Requirements

Vendors developing products for the AP region must comply with *Visa Contactless Payment Service - Visa Asia Pacific* requirements. Acquirers and vendors can contact their local Visa representative to obtain more details.

H.2.2 Visa AP and CEMEA Mandates

Visa has made the following updates to the Visa Rules for clients in AP and CEMEA regions:

Effective 1 April 2015

- All new proximity payment readers must support VCPS 2.1.3 or later, or the equivalent EMV contactless kernel 3.

Effective 1 January 2018

- All proximity payment readers must support VCPS 2.1.3 or later, or the equivalent EMV contactless kernel 3.

H.2.3 Visa AP and CEMEA Additional Acquirer Requirements

Effective 1 April 2015 for new proximity payment readers and **effective 1 January 2018** for all proximity payment readers, the following features, currently optional in the VCPS 2.1 specifications, will become required for acquirers in AP and CEMEA:

- Acquirers must support the APID and set it to the value defined in VCPS 2.1.
- Acquirers must **not** support MSD contactless transactions.
- Acquirers must disable the Reader Contactless Transaction Limit.
- Acquirers must enable the CVM Transaction Limit and set it to the value defined in the Visa rules.
- Acquirers must enable the reader Contactless Floor Limit and set it to the value defined in the Visa rules.
- Acquirers and merchants must include the FFI in authorization messages and clearing records when it is provided by the Visa payWave card or proximity payment device.

H.3 Visa U.S.A.

This section provides a summary of requirements and recommendations for acquirers in Visa U.S.A.

H.3.1 Visa U.S.A. Mandates

Visa has made the following updates to the Visa Rules for clients in Visa U.S.A.:

Effective 10 April 2015

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

Effective 1 April 2016

- All contactless terminals in the U.S. must comply with VCPS 2.1.1 (or higher) and be capable of supporting contactless chip (qVSDC) functionality. Any terminals that do not meet this requirement must be removed.

Note: Visa is currently evaluating time frames under which to establish a sunset date for the contactless MSD processing path.

H.3.2 Visa U.S.A. Additional Acquirer and Merchant Requirements

Effective 1 April 2015 for new contactless readers and **effective 1 January 2018** for all contactless readers, the following will become required for acquirers and merchants in Visa U.S.A.:

- Acquirers and merchants must disable the Reader Contactless Transaction Limit or set it to its maximum value.
- Acquirers and merchants must enable the CVM Transaction Limit and set it to the value defined in the Visa rules (i.e., 0 or up to the VEPS Limit for participating merchants in that Merchant Category Code).
- Acquirers and merchants must enable the reader Contactless Floor Limit and set it to the value defined in the Visa rules (i.e., 0).
- Acquirers and merchants must include the Form Factor Indicator (FFI) in authorization messages and clearing records when it is provided by the Visa payWave card or proximity payment device.

Effective 1 October 2015, the Dedicated File (DF) Name (Tag '84') must be carried in every authorization/full financial request from the device (contact or contactless) to the acquirer.

H.3.3 Visa U.S.A. References

- Visa U.S. EMV® Chip Terminal Testing Requirements
- U.S. Minimum Terminal Configuration ADVT Use Cases
- Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide
- U.S. Visa Debit Test Cases
- Visa Minimum U.S. Online Only Terminal Configuration

Appendix I. Reference Materials

This appendix provides a list of materials referenced in this document, which incorporates information from a variety of sources. These materials are publicly available at the websites listed.

I.1 Available at www.emvco.com

- *EMV Integrated Circuit Card Specifications for Payment Systems*
- *EMV Contactless Specifications for Payment Systems* (consist of seven books)
- *EMV Optimising Contact Chip Transaction Times Best Practices*
- *Recommendations for EMV Processing for Industry-Specific Transaction Types*
- *EMV Acquirer and Terminal Security Guidelines*

EMVCo has documented a number of best practices for devices, which can be found at www.emvco.com on the Advisories site.

EMVCo has documented a number of interoperability advisories which are designed to make acquirers and device vendors of any issues or problems arising from the use of EMV products. The advisories can be found at www.emvco.com

I.2 Available at www.pcisecuritystandards.org

- *Payment Card Industry (PCI) Data Security Standard (DSS)*
- *Payment Card Industry (PCI) DSS Wireless Guidelines*
- *Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS)*
- *Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*
- *Skimming Prevention Best Practices for Merchants*

I.3 Available from Visa

The Visa materials listed in the below table may have controlled availability. Acquirers may download these from Visa Online, if they have access. Otherwise, they should contact their local Visa representative to obtain access to Visa Online or access to the documents. Licensed vendors, who have been given approval, may download licensed Visa materials from the Technology Partner site (https://technologypartner.visa.com).

Table I–1: Visa Reference Materials

Title and Description
Acquirer Device Validation Toolkit (ADVT) User Guide Accompanies the ADVT, which is a deck of test cards, developed to provide a greater degree of service quality assurance to chip acquirers and device vendors developing and deploying chip reading devices. Its purpose is to validate the configuration of their EMV chip-reading devices. Available as part of the toolkit.
International Transactions Guide
Prepaid Product Risk Management Best Practices
qVSDC Device Module Test Cases Use of the qVSDC-DM is required to complete self-testing of the device as part of the approval process for Visa payWave acquirers deploying a qVSDC supporting reader.
Visa Branding for Payment Terminals Contains guidelines and artwork for use by acquirers, merchants and partners to accurately reproduce the Visa Brand mark and Contactless Symbol on payment terminals.
Visa Contactless Device Evaluation Toolkit User Guide Accompanies the CDET toolkit, which provides a means for contactless card reader suppliers and Visa acquirers (or agents) implementing a contactless chip program to test devices prior to deployment. Available as part of the toolkit.
Visa Contactless Payment Specification Version 2.0.2—including additions and clarifications. Defines the requirements for conducting Visa payWave transactions at point of sale devices and chip data messages.
Visa Contactless Payment Specification Version 2.1—including all published updates. Defines the requirements for conducting Visa payWave transactions at point of sale devices and chip data messages.
Visa Core Rules and Visa Product and Service Rules (Available at Visa.com)
Visa Easy Payment Service—Acquirer Program Guide
Visa Europe Contactless Terminal Requirements and Implementation Guide (Available from the Europe Region by contacting contactlessVE@visa.com)
Visa Global ATM Member Guide Designed to provide information necessary for Visa and Plus clients to successfully use the Visa Global ATM network and establish, manage, or sponsor ATM cash access programs.
Visa Integrated Circuit Card Specifications (VIS) Based on EMV, and provides the technical details of chip card functionality related to Visa Smart Debit and Visa Smart Credit transactions.
Visa Payment Acceptance Best Practices for Retail Petroleum Merchants

Title and Description
Visa Payment Technology Standards Manual Describes the visa standards applied to PINs, CVV techniques, management of cryptographic keys, and Track 1 and Track 2 for both magnetic stripe and chip.
Visa payWave Acquirer Implementation Guide Provides implementation guidelines for acquirers wishing to implement contactless devices that accept Visa payWave cards. Guides for VCPS 2.0.2 and VCPS 2.1 are available.
Visa payWave for Mobile—Service Description Defines requirements relating to the support of Visa payWave on a mobile device and the impact to issuers, acquirers and acceptance devices.
Visa payWave Technical Implementation Guide—Acquirer Provides acquirers with technical requirements, system changes and implementation information required to participate in a VCPS program. Guides for VCPS 2.0.2 and VCPS 2.1 are available.
Visa Security Best Practices for Mobile Payment Acceptance Solutions
Visa Smart Debit/Credit (VSDC) Acquirer Implementation Guide Provides guidelines and best practices relating to implementation of contact chip including support for offline-capable devices and offline processing options.
Visa Smart Debit/Credit (VSDC) Certification Authority Technical Requirements Describes the interface formats and media requirements for data exchanged between a VSDC issuer and the VSDC Certification Authority (CA).
Visa Smart Debit/Credit (VSDC) System Technical Manual Provides detailed information for VisaNet chip-based debit/credit processing, including an overview of required host system changes. This document is designed to complement the payment service rules and VIS.
Visa Transaction Acceptance Device Requirements (TADR) For ease of reference and to facilitate client access to device requirements not found in the *Visa Core Rules and Visa Product and Service Rules*, Visa consolidated most of these rules into TADR document.

Appendix J. Acronyms and Glossary

This appendix contains a list of acronyms, terms, and definitions commonly used to describe transaction acceptance devices and card readers.

Term	Definition
Account Verification	A Card-Not-Present transaction that verifies that an account is valid and in good standing. Also known as Account Number Verification.
Acquirer	A Visa client financial institution that signs a merchant or disburses currency to a cardholder in a cash disbursement and, directly or indirectly, enters the resulting transaction receipt into interchange.
Acquirer Device Validation Toolkit (ADVT)	A set of cards or simulated cards and test scenarios used to validate new or upgraded EMV chip devices.
American National Standards Institute (ANSI)	A U.S.A. standards accreditation organization.
Antenna	An antenna is embedded into a contactless card to allow the card to communicate with the contactless reader. The antenna may be placed around the border of the card, throughout the main area of the card, or within a small locale of the card.
Application Authentication Cryptogram (AAC)	A cryptogram generated by the card for declined transactions (online and offline).
Application Cryptogram	Cryptogram generated by the card application.
Application Identifier (AID)	A data element that identifies the application in a card or terminal, such as Visa Debit/Credit or Visa Electron. It is composed of the Registered Application Provider Identifier (RID) and the Proprietary Application Identifier Extension (PIX). As described in ISO/IEC 7816-5.
Application Interchange Profile (AIP)	Information stored on the card that tells the terminal whether or not the card supports certain functions.
Application File Locator (AFL)	Indicates the location (SFI, range of records) of the Application Elementary Files (AEFs) related to a given application.
Application Selection Indicator	A data element that indicates whether the associated AID in the device must match the AID in the card exactly, including the length of the AID, or only up to the length of the AID in the device.
Application Transaction Counter (ATC)	A counter of the number of transactions processed by the card since the application was put on the card and is used in device velocity checking.
Application Usage Control (AUC)	Information stored on the card that tells the terminal how the card is allowed to be used—for example, are international transactions allowed?
Authorization Request Cryptogram (ARQC)	An application Cryptogram generated by a Chip Card when requesting Online Authorization.

Term	Definition
Authorization Response	An Issuer, Authorizing Processor, or Stand-In Processing reply to an Authorization Request or Account Number Verification. The U.S. Regional Operating Regulations refers to the following types of Authorization Response: • Approval Response • Decline Response • Pickup Response • Referral Response
Authorization Response Cryptogram (ARPC)	Cryptogram generated by the issuer host and sent to the card as part of the online authorization process that allows the card to authenticate the response from the issuer.
Automated Dispensing Machine	A UCAT that authorizes all transactions and requires PINs
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.
B	Binary representation
CA	See Certification Authority.
Candidate List	A list of applications mutually supported by both the card and the Transaction Acceptance Device (TAD). The Candidate List is built by the TAD during Application Selection.
Card Authentication	A means of validating whether a card used in a transaction is the genuine card issued by the issuer.
Card Authentication Method (CAM)	See Online Card Authentication.
Card/Integrated Circuit	In general, the term "card" is used to describe the function performed by the VSDC application on the card or transaction initiation device. When it is necessary to distinguish between the chip itself and another card feature such as the magnetic stripe, the term "integrated circuit" may be used.
Cardholder Selection of the Application	Process by which the cardholder selects the application to be used for the transaction.
Cardholder Verification Method (CVM)	Instructions encoded within a chip that define how the authenticity of a cardholder's identity is to be verified.
Cardholder Verification Value (CVV)	A unique check value encoded on the magnetic stripe or chip on a card. It is used to validate card information from the magnetic stripe during the authorization process and to detect counterfeit cards. The CVV is calculated from data encoded on the magnetic stripe using a secure cryptographic process. Also refer to iCVV.
Cardholder Activated Device	A UCAT.
Certification Authority	In general, an entity responsible for establishing and vouching for the authenticity of public keys through issuance and management of public key certificates.

Term	Definition
Chargeback	A transaction that an issuer returns to an acquirer.
Chip card	A Card embedded with a Chip that communicates information to a Transaction Acceptance Device (TAD).
Chip-Capable Terminal	A terminal that allows the optional addition of a chip reader/writer (even if the functionality to read/write to a chip is not activated).
Chip-Enabled Terminal	A chip-capable terminal with all necessary functionality activated for reading and writing chip data and performing a chip payment transaction.
Clearing	All of the functions necessary to collect a clearing record from an acquirer in the transaction currency and deliver it to the issuer in the billing currency, or to reverse this transaction.
Clearing Record	A record of a presentment, chargeback, representment, or reversal in the format necessary to clear the transaction. Also referred to as a clearing transaction.
Cn	Compressed numeric: Each byte is used to represent two decimal digits, and the decimal number is padded with trailing hexadecimal FFs.
Combined DDA/Application Cryptogram Generation (CDA)	A type of Offline Data Authentication where the card combines generation of a cryptographic value (dynamic signature) for validation by the terminal with generation of the Application Cryptogram to ensure that the Application Cryptogram came from the valid card. (Note that CDA is not supported in qVSDC.)
Consumer Device CVM	A cardholder verification method performed on and verified by the consumers payment device, independent of the terminal.
Contactless	A chip transaction where the communication between the card and the device does not take place over a contact interface.
Contactless Device Evaluation Toolkit (CDET)	The Contactless Device Evaluation Toolkit (CDET) is a test card solution that can be used to perform quality assurance testing by acquirers in the process of deploying Visa payWave contactless acceptance readers and by device vendors building Visa payWave acceptance devices.
Contactless Symbol	A symbol that is placed on contactless cards and devices to indicate contactless support and acceptance.
Cryptographic Key	The numeric value entered into a cryptographic algorithm that allows the algorithm to encrypt or decrypt a message.
Cryptogram	A value resulting from a combination of specific key data elements that are used to validate the source and integrity of data.
Cryptography	The study of mathematical techniques for providing aspects of information security, such as confidentiality, data integrity, authentication, and nonrepudiation.
CVM List	An issuer-defined list contained within a chip establishing the hierarchy of preferences for verifying a cardholder's identity.
Data Authentication	Validation that data stored in the ICC has not been altered since card issuance. See also Offline Data Authentication.
Data Encryption Standard (DES)	The data encryption standard defined in American National Standards Institute X3.92-1981 for encrypting and decrypting binary coded data.

Term	Definition
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.
Derived Unique Key Per Transaction (DUKPT)	A symmetric algorithm encryption technique that uses a unique DES key derived from the previous DES key to encrypt the PIN for each new transaction.
Digital Signature	A cryptogram generated by encrypting a message digest (or hash) with a private key that allows the message content and the sender of the message to be verified.
Dual Interface Terminal	A terminal that supports both contact and contactless cards. The terminal may enable this support by having a contactless reader attached to it to facilitate contactless acceptance or alternatively have contact and contactless chip capabilities integrated into the one device.
Dynamic Card Verification Value (dCVV)	A CVV process where the CVV value is dynamically generated during the contactless transaction. Also see Card Verification Value (CVV).
Dynamic Data Authentication (DDA)	A type of dynamic authentication performed offline, where the card generates a cryptographic signature using transaction-specific data elements for validation by the terminal to protect against skimming and modification of the data exchanged between card and terminal.
Dynamic Data Authentication Data Object List (DDOL)	The card-originated data element that is used for constructing the INTERNAL AUTHENTICATE command.
EMV Integrated Circuit Card Specifications for Payment Systems	Technical specifications developed (jointly by Europay International, MasterCard International, and Visa International) to provide standards for processing debit and credit transactions, and ensure global interoperability for the use of chip technology in the payment industry.
EMVCo	EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications.
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	When a chip card is accepted via its magnetic stripe, typically due to an inoperative chip on the card or a malfunction of the terminal chip reader.

Term	Definition
Fast DDA (fDDA)	A faster version of DDA that is suitable to the requirements of a contactless transaction. During fDDA, the Transaction Acceptance Device (TAD) 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 integrated circuit card (ICC) data in ISO authorized messages sent and received by acquirers and issuers.
File Control Information (FCI)	Data provided in a card response when the card application is selected (using a SELECT command) by a Transaction Acceptance Device (TAD).
Floor Limit	A currency amount below which an online authorization is not required for a single transaction unless a Service Code is present which requires online authorization. Visa regions and countries establish floor limits for specific types of merchants.
Form Factor Indicator	Indicates the form factor of the consumer payment device and the type of contactless interface over which the transaction was conducted. This information is made available to the issuer host. Please check with your Visa representative regarding which form factors are supported for your environment.
ICC Card Verification Value (iCVV)	An alternate Card Verification Value that an issuer may encode on a Chip instead of the standard Card Verification Value contained in the Magnetic Stripe of the Chip Card.
IFD	Interface device
Integrated Circuit Card (ICC)	A card embedded with a chip that communicates information to a point-of transaction device.
IFM	Interface Module. It is the hardware or chip reader developed to EMV 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 Application Data	A data element that contains proprietary application data for transmission to the issuer in an online transaction.

Term	Definition
Issuer Authentication	Validation by the card of the authorization response to ensure the integrity of the authorization response and validate the issuer (or an authorized proxy for the issuer) as the source of the response. The card optionally may require successful Issuer Authentication to update internal counter or other data or to allow a card approval other than an online approval. See Authorization Response Cryptogram (ARPC).
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. One form of Post-Issuance Updates.
Kernel	A piece of software developed to EMV specifications that interacts with the chip card and is integrated into the device application.
Limited Amount Terminal	A UCAT that only processes under-floor transactions.
Magnetic Stripe	The magnetic stripe on a card that is encoded with the necessary information to complete a transaction.
Magnetic Stripe Terminal	A terminal that reads the magnetic stripe on a card.
Magnetic Stripe Data (MSD)	Data contained in a Magnetic Stripe and replicated in a chip.
Magnetic Stripe Data (MSD) CVN 17	MSD transaction with track data and an Application Cryptogram.
Magnetic Stripe Data (MSD) Legacy	MSD transaction with track data and without an Application Cryptogram. Referred to as "MSD Legacy" because it is an MSD transaction as defined in VCPS 1.4.2. MSD Legacy is included in VCPS 2.0.2 and VCPS 2.1.1 to allow for backwards compatibility to VCPS 1.4.2.
Magnetic Stripe Image	The minimum Chip payment data replicating the Magnetic Stripe information required to process an EMV-Compliant Transaction.
Mobile Payment Device	A portable electronic device with wide area communication capabilities that can be enabled with Visa payWave functionality. Mobile devices include mobile handsets, handhelds, smartphones and other consumer electronic devices, such as suitably equipped PDAs.
Mobile Payment Acceptance Device (also known as Mobile Point of Sale or mPOS)	A contactless payment device that resides in a portable electronic device that can access a wireless network.
mPOS	See Mobile Payment Acceptance Device.
N	Numeric: Each byte is used to represent two decimal digits, and the decimal number is padded with leading hexadecimal zeroes.

Term	Definition
N/A	Not applicable
Offline Data Authentication	A process whereby the card is validated at the point of transaction using RSA public key technology to protect against counterfeit or skimming.
Offline Enciphered PIN	A cardholder verification methodology defined in EMV in which the cardholder PIN is entered at a POS device, encrypted there with an ICC public key, and sent to the ICC where it is validated.
Offline Capable Chip Device	A contact chip device that supports both offline and online processing.
Offline Decline	A transaction that is negatively completed (declined) at the point of transaction between the card and terminal without an online authorization request to the issuer.
Offline PIN	A PIN value 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 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 Transactions	A transaction that takes place without the need for an online authorization message to the acquirer.
Online Authorization	A method of requesting an authorization through a data communications network other than voice to an issuer, an authorizing processor, or stand-in processing.
Online Capable Chip Device	A contact chip device that supports both offline and online processing.
Online Card Authentication	Validation of the card by the issuer to protect against data manipulation and data copying. Also known as CAM (Card Authentication Method). 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 Only	A card acceptance terminal that requires that all transactions be sent online for authorization.
Online PIN	A process used to verify the Cardholder's identity by sending an encrypted PIN value to the issuer or the issuer's agent for validation in an Authorization Request.
Partial Name Selection	The Application Selection process where the device AID uses only a partial name.

Term	Definition
Payment Card Industry (PCI)	A consortium of payment card industry representatives, which became formalized as the PCI Security Standards Council.
PCI Payment Application Data Security Standards (PA-DSS)	PCI requirements relating to application security.
PCI PIN Transaction Security (PTS)	PCI requirements relating to PIN security formerly known as PCI-PED.
Payment System Environment	The data element on a chip card that contains a list of applications supported on the card. The PSE is used during the Directory Selection Method of Application Selection.
Personal Identification Number (PIN)	A personal identification alpha or numeric code that identifies a cardholder in an authorization request originating at a device with electronic capability.
PIN Entry Device (PED)	A secure device that allows cardholders to enter their PINs.
Point of Service (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 receipt.
Primary Account Number (PAN)	An issuer-assigned number that identifies a cardholder's account.
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.
Processing Options Data Object List (PDOL)	Contains a list of a device resident data objects (tags and lengths) needed by the card in processing the GET PROCESSING OPTIONS command.
Proximity Coupling Device (PCD)	The reader/writing device that uses inductive coupling to provide power to the consumer device, such as a contactless card or a cell phone, and also to control the data exchange with the consumer device.
Proximity Payments Systems Environment (PPSE)	A list of supported Application Identifiers (AIDs), Application Labels, and Application Priority Indicators for applications that are accessible over the contactless interface. This list will be provided by the card in the FCI with all directory entries in the card response to SELECT of the PPSE ('2PAY.SYS.DDF01').
Public Key	The public component of an asymmetric key pair. The public key is usually publicly exposed and available to users. A certificate to prove its origin often accompanies it. In RSA, the public key consists of the public key exponent and the public key modules.

Term	Definition
Public Key Algorithm	A cryptographic algorithm that allows the secure exchange of information and message authentication but that does not require a shared secret key, through the use of two related keys: a public key that may be distributed in the clear and a private key that is kept secret.
Public Key Certificate	An asymmetric transformation of the public key by a CA and intended to prove to the public key recipient the origin and integrity of the public key.
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.
qVSDC	Contactless processing option that follows an expedited EMV processing model and chip processing rules to provide a quick transaction over the contactless interface.
qVSDC Device Module	A mandatory set of test scripts and test cases for acquirers using approved qVSDC readers and an approved Transaction Acceptance Device (TAD) to help verify that the combination is correctly configured and does not contribute to interoperability problems.
Random Selection	A capability of an online-capable EMV compliant device that allows for random selection of transactions for online processing.
Reader Cardholder Verification Method Limit	A limit in the contactless reader. When the amount is above this limit, the qVSDC transaction requires cardholder verification.
Reader Contactless Floor Limit	A limit in the contactless reader. When the amount is above this limit, a qVSDC transaction is not permitted and the transaction must be sent online.
Reader Contactless Transaction Limit	A limit in the contactless reader. When the amount is above this limit, an offline qVSDC transaction is not permitted (the transaction may proceed over another interface).
RSA	A public key cryptosystem developed by Rivest, Shamir, and Adleman, widely known as RSA. It is used for data encryption and authentication.
Secure Hash Algorithm (SHA-1)	This algorithm is standardized as FIPS 180-2. SHA-1 takes as input messages of arbitrary length and produces a 20-byte hash value.
Self-Service Terminal	A UCAT that authorizes all transactions but does not support PIN.
Selectable Kernel	A method defined in EMV where a terminal can change certain of its capabilities (e.g., supported CVMs) depending on transaction characteristics (e.g. amount or cashback transaction).

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.
Small Ticket Transaction	An electronically read authorized transaction at or below a locally selected limit, presented by a merchant with a qualified Merchant Category Code, that is conducted in a face-to-face environment. For the applicable operating regulations and a list of qualified Merchant Category Codes, see the Visa rules and regulations. See VEPS.
Standard Floor Limit	A floor limit that varies by merchant type, as specified in the Visa rules and regulations.
Status Check	An authorization request for US $1 or local equivalent.
Static Data Authentication (SDA)	A type of Offline Data Authentication where the device validates a cryptographic value placed on the card during personalization. The validation protects against some types of counterfeit but does not protect against skimming.
Symmetric Algorithm	An algorithm in which the key used for encryption is identical to the key used for decryption. TDEA is the best known symmetric encryption algorithm.
Terminal Action Code (TAC)	Visa-defined rules in the device which the device uses to determine whether a transaction should be declined offline, sent online for an authorization, or declined if online is not available.
Terminal Floor Limit	A data element that indicates the transaction amount equal to or greater than which the device will send the transaction online.
Terminal Risk Management	Offline checks such as floor limit checks and exception file checks that are performed by the device.
Terminal Verification Results (TVR)	A set of indicators from the VSDC device, recording the results of offline and online processing. These indicators are available to issuers in the online message and clearing transaction.
Track 2 Equivalent Data	Image of Track 2 from the magnetic stripe that is part of the card's chip data.
Transaction Acceptance Device (TAD)	A device that accepts and processes Visa, Visa Electron, and/or Plus transactions.
Transaction Acceptance Device Requirement (TADR)	A requirement for devices that accept and process Visa, Visa Electron, and/or Plus transactions.
Transaction Certificate (TC)	An Application Cryptogram generated by the card for an accepted transaction.

Term	Definition
Transaction Status Information (TSI)	A value that indicates the functions that have been performed in the device.
Transaction Type	A data element that indicates the type of financial transaction, represented by the values of the first two digits of Processing Code as defined by Visa.
Triple Data Encryption Algorithm (TDEA)	TDEA (sometimes referred to as Triple DES) as defined in ISO/IEC 18033 Information technology—Security techniques—Encryption algorithms—Part 3: Block ciphers.
Triple Data Encryption Standard (TDES)	The data encryption standard used with a double-length DES key. Sometimes referred to as TDEA or DES3.
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 uniqueness to the generation of the Application Cryptogram.
Visa Easy Payment Service (VEPS)	Visa Easy Payment Service (VEPS) is the new global name for the No Signature Required (NSR) program and Small Ticket Transaction program as defined outside the United States.
Visa Electron	A Visa payment program.
Visa Integrated Circuit Card Specification (VIS)	Chip card and application specifications developed by Visa for VSDC programs. VIS serves as a companion guide to the EMV specifications.
VisaNet Integrated Payment (V.I.P.) System	The systems and services through which Visa delivers online financial processing, authorization, clearing, and settlement services to clients.
Visa payWave Test Tool (VpTT)	The mandated Europe Region tool to test Visa payWave contactless acceptance devices against the Europe Region's implementation requirements.
Visa rules and regulations	The operating regulations in the merchant's or acquirer's country. This includes the *Visa Core Rules and Visa Product and Service Rules*.
Visa Smart Debit/Credit (VSDC)	The Visa service offerings for chip-based debit and credit programs. These services, based on EMV and VIS specifications, are supported by VisaNet processing, as well as by Visa rules and regulations.
VSDC Certification Authority	An entity that issues and manages digital certificates for use on Visa Chip Cards in accordance with Visa specified requirements.
Zero Floor Limit	A floor limit with a currency amount of zero. Online authorization is required for all zero-floor-limit transactions.