Visa Contactless Payment Specification

Version 2.1

May 2009

Welcome to the Visa Contactless Payment Specification

THIS SPECIFICATION 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.

THE INFORMATION CONTAINED HEREIN IS PROPRIETARY AND CONFIDENTIAL AND MUST BE MAINTAINED IN CONFIDENCE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE WRITTEN AGREEMENT BETWEEN YOU AND VISA INC., VISA INTERNATIONAL SERVICE ASSOCIATION, AND/OR VISA EUROPE LIMITED.

Revision Log

The following sections outline the changes and additional functionality in this specification since the publication of the *Visa Contactless Payment Specification 2.0.2, Including Additions and Clarifications 3.0*.

General

- Separated reader requirements and card requirements.
- Reorganized and rephrased sections and requirements to more clearly define requirements for cards and readers.
- Contactless VSDC is no longer a supported contactless path for VCPS.
- The VCPS Data Elements table has been extended to be more comprehensive.
- Added the "Commands and Secure Messaging" appendix, specifying the supported commands for contactless.
- "Definitions and Acronyms" section has been replaced with a "Glossary", and moved to the end of the specification.
- The "MSD, qVSDC, VSDC, and EMV" appendix has been removed.
- Added Issuer Update Processing functionality for readers and cards.
- Added ability for the issuer to personalize, and the reader to recognize, an issuer preference to request online processing when the card application is expired.
- Added support for the Cryptogram Information Data (CID) for qVSDC readers and cards.
- Defined behavior for cash, cashback, and refund transactions for readers and cards.

Reader

- Added a new appendix providing guidelines for data that may need to be transmitted from the reader to the terminal (dependent on reader-terminal architecture).
- Added a new appendix defining the messaging requirements for acquirers supporting VCPS.
- Added qVSDC reader support for the "Consumer Device CVM", a CVM performed on the consumer's payment device (independent of the reader).
- Added qVSDC reader processing when the response to the GPO command is SW1 SW2 = '6986', instructing the reader to briefly power down the contactless interface before returning to Discovery Processing.

- Added qVSDC reader support for the reader data element Merchant Name and Location.
- Added the qVSDC reader ability to include the Form Factor Indicator and Customer Exclusive Data in messages to the acquirer.
- Added qVSDC reader Dynamic Reader Limits functionality.
- Removed support for fDDA v00.

Card

- qVSDC path support for Cryptogram Version Number 18 has been introduced, including support for the Card Status Update (CSU).
- Streamlined qVSDC has been moved to the new "Streamlined qVSDC" appendix. Added the ability to support Online PIN and return records for Streamlined qVSDC implementations. References to an offline-capable Streamlined qVSDC solution were removed.
- Added a new appendix defining additional requirements for "Dual-Interface Contactless and Contact Cards".
- Added a new appendix further defining VCPS requirements for transaction logging.
- Commands supported by the application over the contactless interface have been restricted to the commands defined in this specification.
- For dual-interface cards, added the ability for the issuer to disable VCPS (contactless) functionality. Disabling VCPS (contactless) functionality may be performed during personalization, or post-issuance via issuer script commands.
- For dual-interface cards, records are only accessible over the interfaces for which they are defined.
- Added Offline Data Authentication (ODA) for Online Authorizations functionality, allowing the card application to return offline authentication data even when requesting an online approval. Note that this functionality is not intended for use in standard POS environments, and the card application does not return offline authentication data for online authorizations when used with readers compliant to this specification.
- For Issuer Discretion Data Options (IDDO) returning a MAC, added the option to pad the issuer discretionary data with a mandatory '80' byte for MAC computations.
- For Issuer Discretion Data Options (IDDO) returning a MAC, changed application processing to compute and return a MAC regardless of the cryptogram type (when using CVN10 or CVN17).
- In qVSDC Card Action Analysis, added the ability to support up to five (5) alternate currencies for domestic velocity checking.
- In qVSDC Card Action Analysis, added the ability to configure card processing based on the Issuer Country Code and Terminal Country Code.

- In qVSDC Card Action Analysis, changed the transaction disposition for some existing checks to improve the cardholder experience.
- In qVSDC Card Action Analysis, added the ability to count the number of card requested qVSDC offline (and card requested qVSDC online) transactions. A velocity check for qVSDC contactless transactions has been included.
- In qVSDC Card Action Analysis, added support for the Consecutive Transaction International Upper Limit as a risk management option.
- In qVSDC Card Action Analysis, added the ability for the issuer to indicate that "(Contact Chip) Offline PIN" is preferred when a CVM is required. "(Contact Chip) Offline PIN" is not a contactless CVM, but it allows the issuer to request a contact chip transaction when a CVM is required.
- In qVSDC Card Action Analysis, the Card Additional Processes "Prepaid" bit (and associated functionality) has been removed.
- In qVSDC Card Action Analysis, removed the Low Value OR CTTA check.
- In qVSDC Card Action Analysis, removed the Amount, Authorized of zero check.
- In qVSDC Card Action Analysis, removed the New Card checks.
- In qVSDC Card Action Analysis, removed the "CVM Required for Non-matching currency transactions" option.
- Defined the contents of the Form Factor Indicator.
- Changed the minimum ICC Private Key size requirements. Card applications implementing offline functionality shall now support ICC Private Keys up to 1408-bits.
- Changed the card application response when no matching contactless path is found from SW1 SW2 = '6984' to SW1 SW2 = '6985'.

Contents

Tables

Figures

Requirements

1 Introduction

New technology is presenting Visa with opportunities to provide enhanced payment services. One such new technology is the ability to communicate between two entities, for instance a card and a reader, over a contactless interface.

New technology also brings challenges and changes to existing business and technical environments. To ensure consistent cardholder experience and prevent transactions from being interrupted, it is crucial that the time in which the cardholder holds the payment card close to the reader (i.e. when the card is in the field) be as minimal as possible.

Visa offers two ways to conduct payment over the contactless interface. Magnetic stripe contactless payment (Magnetic Stripe Data, MSD) and quick Visa Smart Debit/Credit (qVSDC) payment allow for quick transactions over the contactless interface.

The two approaches to contactless payment are briefly introduced in the following sections.

1.1 MSD – Magnetic Stripe Data

The MSD contactless transaction operates under magnetic stripe payment service rules according to Visa Operating Principles and Regulations. For MSD, card capabilities will be communicated to the reader (dongle, card reader, or other terminal device) as described in the card requirements in this document.

The requirements for MSD are defined in this document.

1.2 qVSDC – Quick Visa Smart Debit/Credit

qVSDC uses EMV commands and constructs whenever possible, to utilize issuer and acquirer investment in EMV. It compresses multiple EMV commands into as few commands as possible to save time and allow cryptographic operations to be done up front as opposed to later when the card is leaving the field. It features:

- An online transaction with online card authentication
- An offline transaction with offline data authentication and a clearing cryptogram for below floor limit transactions, and an option of restricting offline transaction values using low value limits.

The requirements for qVSDC are defined in this document.

1.3 Global Interoperability

Global interoperability is achieved by requiring cards to support both MSD and qVSDC, and readers to support either MSD or qVSDC.

2 General Information

2.1 Audience

This document is intended for clients, Visa regions, and vendors for use in Visa contactless programs.

2.2 Scope

This specification describes the globally interoperable contactless solution. It addresses the requirements for:

- MSD
- qVSDC
- Reader or card application-level requirements that are not covered in [VIS], as well as differentiation from contact card or contact device Operating Regulations or other VSDC product requirements

Contactless VSDC is no longer supported in this specification.

Requirements for physical characteristics, power and signal interfaces, initialization, collision detection, and transmission protocols are specified in [EMV CL]. Card and reader products are required to be compliant to one of the [EMV CL] specifications.

Any additional requirements beyond those specified in [EMV CL] are addressed in this document.

2.3 Reference Materials

The following documents are referenced in this specification.

[EMV] EMV ICC Specifications for Payment Systems, Version 4.2, June 2008. Integrated Circuit Card Specifications for Payment Systems.

[EMV CL] EMV PayPass - ISO/IEC 14443 Implementation Specification, Version 1.1, March 2006. EMV Contactless Specifications for Payment Systems

or

EMV Contactless Communications Protocol Specification, Version 2.0, August 2007. EMV Contactless Specifications for Payment Systems.

[EMV CL 1 1] EMV PayPass - ISO/IEC 14443 Implementation Specification, Version 1.1, March 2006. EMV Contactless Specifications for Payment Systems

[EMV CPS] EMV Card Personalization Specification, Version 1.1, July 2007. EMV Card Personalization Specification (EMV CPS); latest version available on EMVCo.com

EMV Specification Update Bulletins; latest version available on EMVCo.com

[EMV EP] EMV Entry Point Specification, Version 1.0, May 2008. EMV Contactless Specifications for Payment Systems: Entry Point Specification.

[ISO 639] ISO/FDIS 639-1. Codes for the Representation of Names and Languages (Alpha-2 code).

[ISO 3166] ISO 3166. Codes for the Representation of Names and Countries.

[ISO 4217] ISO 4217. Codes for the Representation of Currencies and Funds.

[ISO 7811] ISO/IEC 7811. Identification Cards – Recording Technique.

[ISO 7813] ISO/IEC 7813. Identification Cards – Financial Transaction Cards.

[ISO 7816-4] ISO/IEC 7816-4. Identification Cards – Integrated Circuit Cards with Contacts – Part 4: Interindustry Commands for Interchange.

[ISO 7816-5] ISO/IEC 7816-5. Identification Cards – Integrated Circuit Cards with Contacts – part 5: Numbering System and Registration Procedure for Application Identifiers.

[ISO 8583] ISO 8583. Financial transaction card originated messages – Interchange message specifications

[ISO 8859] ISO/IEC 8589. Information Processing – 8-bit Single-Byte Coded Graphic Character Sets.

[ISO 14443] ISO/IEC 14443. Identification cards – Contactless integrated circuit(s) cards – Proximity cards

Part 1: Physical characteristics

Part 2: Radio frequency interface power and signal interface

Part 3: Initialization and anticollision

Part 4: Transmission protocol

[VCPS 1 4 2] Visa Contactless Payment Specification, Version 1.4.2, December 2004. Additions and Clarifications, Version 1.1, February 2006. Visa's specification for contactless payment transactions.

[VCPS UI] Visa Contactless Payment Specification: User Interface Guidelines, Version 1.0, September 2008.

[VIS] Visa Integrated Circuit Card Specification, Version 1.5, May 2009 – Provides technical details related to VIS transactions and functions performed by the chip card.

[VSDC PERSO] VSDC Personalization Specification, Version 2.0 – Guide to personalization of VSDC applications using the Common Personalization approach described in [EMV CPS].

[VPTSM] Visa Payment Technology Standards Manual, October 1, 2007 – Describes the standards applied to PINs, CVV techniques, management of cryptographic keys, and Track 1 and Track 2 for both magnetic stripe and chip.

3 Terminology and Conventions

Many of the definitions, acronyms, and notations in this document are new with contactless technology or are based on contact chip technology (EMV). This document assumes a level of familiarity with both contactless technology and EMV. For those who are less familiar, this explanation of terms and conventions is placed early in the document for your reference.

3.1 Terminology and Notation

This specification uses the following terminology and notations.

3.1.1 Requirement Terminology

The terminology for requirements are as follows:

- use of the word “shall” denotes a mandatory requirement
- use of the word “should” denotes a recommendation
- use of the word “may” denotes an optional feature

For presence of tags in the commands and responses, the following notation is used:

- M: Mandatory tag – shall always be present, otherwise the reader terminates the transaction
- R: Required tag – shall always be present, but the reader does not terminate the transaction if the tag is not returned
- C: Conditional tag – shall be present under certain conditions, but the reader does not terminate the transaction if the tag is not returned.
- O: Optional tag – may or may not be present

3.1.2 Reader Processing Terminology

The following phrases are used in this specification to indicate that the reader should stop the current contactless application, unless explicitly indicated otherwise.

- “Terminate the transaction”: Stop the current application. Subsequent reader processing is outside the scope of this specification. Contact your Visa regional representative for the requirements applicable for your region.
- “Power(s/ing) off the contactless interface”: Stop the current application, and stop generating the RF Field (in order to put the PICC into the POWER-OFF state as defined in [EMV CL]). Subsequent reader processing is outside the scope of this specification. Contact your Visa regional representative for the requirements applicable for your region.
- “Switch interface(s)”: Stop the current application, power off the contactless interface, and advise the cardholder that the transaction should be attempted over another reader/terminal interface. When switching to another interface, the transaction amount shall be known by the reader-terminal and the merchant shall not be required to reenter the transaction amount.

Note: When the reader is required to power off the contactless interface, it shall do so immediately and shall not perform an [EMV CL] Removal unless explicitly stated otherwise. (An [EMV CL] Removal is performed to ensure that the PICC has been removed from the PCD field)

3.1.3 Implementation and Support Terminology

The following terminology is used in this specification to describe the implementation and configuration requirements for card and reader functionality:

- *Implementation-Mandatory:* Card or reader shall implement this functionality.
- *Implementation-Conditional:* Card or reader shall implement this functionality if the defined conditions are met. Conditions vary based on the functionality in question.
- *Implementation-Optional:* Card or reader may implement this functionality, at the discretion of the implementer.
- *Issuer-Mandatory* (for card) or *Acquirer-Merchant-Mandatory* (for reader): Issuer or acquirer-merchant shall enable this functionality.
- *Issuer-Conditional* (for card) or *Acquirer-Merchant-Conditional* (for reader): Issuer or acquirer-merchant shall enable this functionality if the defined conditions are met. Conditions vary based on the functionality in question.
- *Issuer-Optional* (for card) or *Acquirer-Merchant-Optional* (for reader): Issuer or acquirer-merchant may enable this functionality, at their discretion.

The card and reader functionality defined in this specification are *Implementation-Mandatory*, except where explicitly stated otherwise. This specification may also explicitly reiterate that specific functionality is *Implementation-Mandatory* to avoid potential ambiguity.

When used to describe requirements and conditions for card or reader functionality, the following terminology may be used:

- “Implement(ed)”: Card or reader is capable of performing the functionality. The phrase "implement support for" may also be used.
- “Enable(d)”: Card or reader functionality has been activated (i.e. turned on).
- "Disable(d)": Card or reader functionality has been deactivated (i.e. turned off).
- “Support(ed)”: Card or reader functionality is both implemented and issuer/acquirer-merchant enabled.

3.1.4 Card and Reader Terminology

3.1.4.1 Reader

The word *reader* is used in this specification for the merchant device communicating with the card.

The use of this word is not intended to dictate any specific implementation. Specifically there are two scenarios in which typically a reader is used for a contactless transaction:

- Either as a reader (also called a dongle or PCD) separated from, but communicating with, a POS device.
- Or as a reader integrated into a POS device.

No required implementation shall be implied from this specification perspective.

The word *reader* in this specification will therefore cover both scenarios unless explicitly stated otherwise. It is not intended to imply in which physical component (the reader or the POS device) a specific action is performed.

3.1.4.2 Card

The word *card* is used in this specification for the consumer device that contains the contactless payment application communicating with a payment reader.

The term card ordinarily implies a typical credit card-sized payment card, but in this specification it indicates any type of consumer device that can operate over a contactless interface; for instance, a mobile phone or a key fob.

3.1.5 "Else" with Parenthesized Text

Parenthesized text following the statement "Else" is provided as supplemental information, and does not denote a condition that must be satisfied.

Ex. If *Condition*, then the card shall…

Else (Text), the card shall…

In the example above, the parenthesized "(Text)" is merely supplemental information, and does not constitute a condition that must be satisfied.

3.1.6 Presence of Data Elements

If a card condition evaluates a data element that is not present, then the specific condition referencing the data element shall evaluate to FALSE, unless explicitly stated otherwise. For card requirements or statements with multiple conditions, all other conditions in the requirement or statement are unaffected and evaluated as normal.

If a card action is to be performed on a data element that is not present, then the specific action is not performed. For requirements where multiple actions are to be taken, all other actions in the set are unaffected and performed as normal.

3.1.7 Format of Indicators

Although the indicators used in this specification are explicitly assigned the values of 0 or 1, the format of these internal indicators within an implementation is at the discretion of the implementer.

Performance and security considerations should both be weighed when deciding on the implementation of internal indicators.

3.1.8 Value Representation

0 to 9	10 decimal digits. Decimal numbers are not enclosed in quotation marks.
'0' to '9' and 'A' to 'F'	16 hexadecimal characters
xb, xxb	Binary values. Bit values are appended with the character “b” (e.g. 1b and 0000b). Bits within a byte are numbered from right to left, where the low-order bit (bit 1) is the rightmost bit and the high-order bit (bit 8) is the leftmost bit.
‘Bit Name’	The bit defined as “Bit Name” within a data element. Bit names are enclosed in single curly quotation marks.

3.1.9 Coding of RFU Values in Data Elements

Values in data elements marked as RFU (Reserved for Future Use) shall be set to zero, and both the reader and card shall not; act on, operate on, or verify RFU data.

Coding of data marked as RFU shall follow the same rules as defined in [EMV] Book 3 section 6.3.6.

3.1.10 Flowcharts

Flowcharts are used to provide a high-level illustration of the processing. The flowcharts may be simplified to illustrate a concept, and may not include all the steps that are performed. Implementations are not required to strictly follow the flowcharts, and are instead required to comply with the requirements in the related text. In the case of a discrepancy between the flowchart and the related text, the text shall take precedence.

Please notify Visa of any discrepancies at techquest@visa.com so that they can be evaluated and clarified as appropriate.

4 Overview of the Contactless Approach

The approach to contactless payment processing uses existing infrastructure while acknowledging that contactless payment is being targeted for new markets where quick transactions are a business requirement.

4.1 Contactless Programs and EMV

While patterned on EMV, all of Visa's contactless implementations have the following differences:

- Level 1 (contact versus contactless technology)
- Mandatory use of the PPSE

qVSDC and MSD are both based on [EMV] card and terminal application specifications. [EMV] constructs, commands, data elements, and functionality are utilized where possible. Contactless VSDC is no longer supported in this specification.

qVSDC and MSD are contactless paths under a single Visa AID. Card application processing is determined by the path within the Visa application (a single AID).

Note: For dual-interface cards supporting VIS, VIS is supported in the same application under the same single Visa AID. When using the contact interface, path determination is not performed and VIS processing is used.

The following descriptions summarize at a high level the similarities and differences for qVSDC and MSD.

4.1.1 qVSDC

To minimize the interaction time between the card and the reader, qVSDC readers support Reader Preliminary Transaction Processing (Pre-processing). The Amount, Authorized (tag '9F02') is obtained and transaction-based risk management is performed before requesting that the card be presented and initiating card discovery.

To further decrease transaction time, qVSDC moves the following risk management features to an earlier point in the transaction (Initiate Application Processing):

- Card risk management
- Online card authentication
- Offline card authentication
- Cryptogram generation

For online transactions, no commands are necessary after the application has been selected, other than the GET PROCESSING OPTIONS command. For offline transactions, DDA related data is read (using READ RECORD) and the reader validates the dynamic signature after the card has left the field.

4.1.2 MSD

In addition to existing risk management features associated with the physical magnetic stripe, MSD offers dynamic online card authentication.

4.2 qVSDC

Contactless interaction is defined by the amount of time the cardholder can reasonably and consistently hold the card in position. qVSDC, which is based on EMV concepts and uses the existing Visa systems and rules of operation, addresses this human requirement while protecting the investments already made in the magnetic stripe and chip (EMV) infrastructure.

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.

In addition to a full qVSDC path incorporating all of the Card Action Analysis described in section 6.4, a streamlined version of qVSDC Card Action Analysis is specified to offer simplified qVSDC online-only implementations. Details on supporting qVSDC streamlined functionality are found in Appendix H.

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 GPO command response uses EMV Format 2, but is not fully EMV-compliant because it does not always contain the AFL.

qVSDC offers support for Offline Data Authentication (using fDDA) and is compliant with EMV in this processing, with the following exceptions:

- Generation of the dynamic signature is initiated by the GPO 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 GPO command, rather than generating the dynamic signature at the end of the transaction when the card may be moving away from the reader RF field.

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

[VIS] counters and indicators, other than those specified in this document, are not impacted during qVSDC processing.

4.3 MSD

Magnetic Stripe Data (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 the Dynamic Card Verification Value (dCVV), as defined in Appendix B. MSD Legacy is defined in this specification to support backwards compatibility with [VCPS 1 4 2] cards and readers.
- MSD CVN17 offers an EMV strength application cryptogram.

To meet the agreed requirements for global interoperability, the MSD path supports Cryptogram Version Number 17. It has been agreed that a migration from dCVV to Cryptogram Version Number 17 will take place for MSD readers, and that MSD readers will support Cryptogram Version Number 17. An MSD market is not a full data market, and Cryptogram Version Number 10 and Cryptogram Version Number 18 are not supported in these markets.

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 that all mandatory EMV data elements 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.

4.4 Global Interoperability for qVSDC and MSD

Contactless global interoperability is achieved by requiring cards to support both MSD **and** qVSDC, and readers to support either MSD **or** qVSDC. Readers are not precluded from supporting both MSD and qVSDC.

Table 4-1 describes global interoperability for contactless cards and readers:

Table 4-1: Summary of Possible Reader / Card Interactions

Contactless Card Capability Reader Configuration	qVSDC and MSD
qVSDC-only	qVSDC
MSD-only	MSD
qVSDC and MSD	qVSDC

For card vendors that wish to allow support for domestic solutions as well as the globally interoperable solution, a method is defined in [VSDC PERSO]. This method as defined allows issuers to turn off MSD or qVSDC during personalization to support domestic only solutions. The method described is not mandatory and other methods for supporting this functionality are permitted.

4.5 Processing Overview

This section provides an overview of a VCPS transaction. This is followed by a transaction flow showing the order in which these functions are performed and the commands sent by the reader to the card. Functions are mandatory unless specified otherwise.

4.5.1 Processing Prior to Enabling the Contactless Interface

Reader processing performed prior to powering on the contactless interface and prompting for card presentment.

To minimize the duration in which the card must remain within the reader RF field, the reader may obtain the transaction amount and perform some risk management checks prior to prompting for card presentment.

4.5.2 Discovery Processing

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

4.5.3 Application Selection

Application Selection is performed immediately after activation of the contactless card, and is the process of determining which of the applications that are supported by both the card and reader will be used to conduct the transaction. This process is performed in two steps:

1. The reader builds a candidate list of mutually supported applications. This process is modeled after the [EMV] Directory Selection Method, except that support for the Directory Selection Method is mandatory for readers (and cards), and the PPSE is used in place of the PSE.
2. A single application from the candidate list is identified and selected to process the transaction.

The response message from the card includes the Processing Options Data Object List (PDOL), to identify the reader data needed to perform Initiate Application Processing.

4.5.4 Initiate Application Processing

During Initiate Application Processing, the reader signals to the card that transaction processing is beginning. The reader accomplishes this by sending the GET PROCESSING OPTIONS command to the card. When issuing this command, the reader supplies the card with any data elements requested by the card in the Processing Options Data Object List (PDOL).

The contactless path(s) that are mutually supported by the card and reader are determined, and a contactless path (qVSDC or MSD) is chosen to process the transaction. Subsequent transaction processing is performed according to the requirements of the contactless path chosen.

Initiate Application Processing is where the card performs Card Action Analysis, (conditionally) generates the Application Cryptogram, (conditionally) generates the signature for Offline Data Authentication, and returns card application data.

4.5.5 Read Application Data (Conditional)

Read Application Data is performed if the Application File Locator was returned by the card during Initiate Application Processing.

During Read Application Data, the reader reads the remaining card application data necessary to process the transaction. Note that in VCPS, the card may return application data during Initiate Application Processing and Read Application Data.

4.5.6 Card Read Complete

During Card Read Complete, the reader indicates to the cardholder that exchange of data between the reader and the card is complete, and the card may be removed from the reader field.

The reader determines whether all mandatory data elements for the transaction were returned by the card, and whether any redundant primitive data elements were returned by the card. Primitive data elements are redundant if more than one occurrence of the primitive data element was returned by the card during Initiate Application Processing and Read Application Data.

The reader terminates the transaction if all mandatory data elements were not returned or redundant primitive data elements were returned.

For MSD transactions, subsequent transaction processing is outside the scope of this specification.

4.5.7 Processing Restrictions (Conditional)

Processing Restrictions is implemented for readers supporting any of the Processing Restriction checks.

During Processing Restrictions, the reader checks the application expiration date, application usage, and may check whether the card application is on the Terminal Exception File.

4.5.8 Offline Data Authentication (Conditional)

Offline Data Authentication is implemented for readers supporting offline transactions, and is performed for card requested offline transactions.

During Offline Data Authentication, the reader verifies the dynamic signature returned by the card and authenticates the data from the card.

4.5.9 Cardholder Verification (Conditional)

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

4.5.10 Online Processing (Conditional)

Online Processing is implemented for qVSDC readers supporting online transactions. Online Processing is performed when online processing is required for the transaction.

During Online Processing, the reader sends an authorization request to the issuer host. Online Processing allows the issuer host to review and authorize or decline transactions using the issuer’s host based risk management parameters. In addition to performing traditional online fraud and credit checks, host authorization systems can perform online card authentication using the card-generated cryptogram. The issuer may also perform online card authentication with a Transaction Certificate type application cryptogram when Offline Data Authentication has failed, an option that is configured by the issuer on their cards.

4.5.11 Completion

Completion is performed by the reader to conclude transaction processing. The reader indicates to the cardholder the outcome of the transaction.

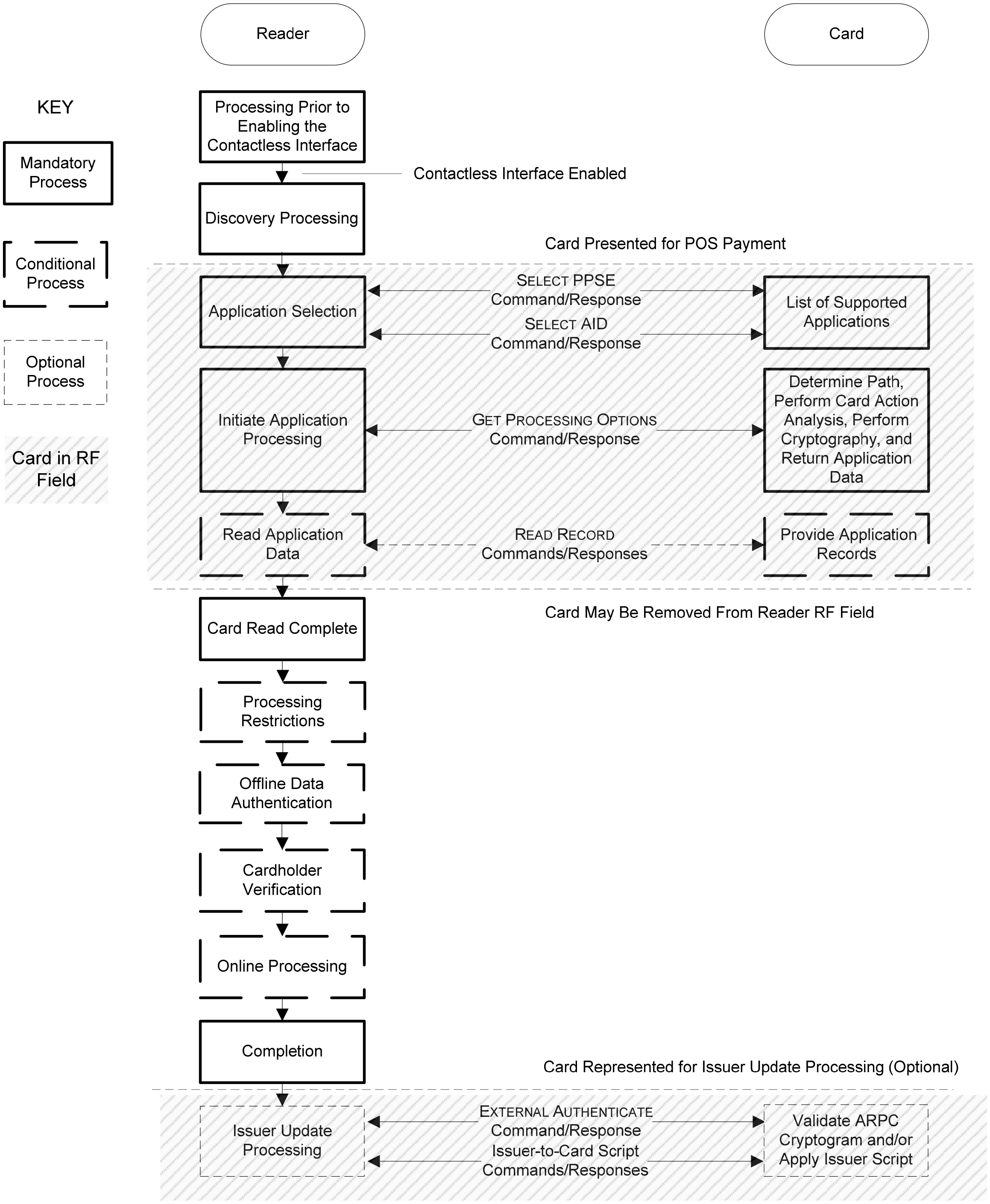
4.5.12 Issuer Update Processing (Optional)

Issuer Update Processing is an implementation and acquirer-merchant option for readers implementing qVSDC. If supported by both card and reader, Issuer Update Processing is performed when the authorization response message contains Issuer Authentication Data and/or an Issuer Script Template.

During Issuer Update Processing, the card application may be updated by the issuer through use of the EXTERNAL AUTHENTICATE command to perform issuer authentication to (re)set risk management counters and indicators, and/or through the application of issuer script commands.

The cardholder is instructed to present their card once more, and Issuer Update Processing is performed to update risk management counters and indicators on the card, and/or to update card data elements.

Figure 4-1: Sample Transaction Flow


Reader
Card
KEY
Mandatory Process
Conditional Process
Optional Process
Card in RF Field
Processing Prior to Enabling the Contactless Interface
Contactless Interface Enabled
Discovery Processing
Card Presented for POS Payment
Application Selection
SELECT PPSE Command/Response
SELECT AID Command/Response
List of Supported Applications
Initiate Application Processing
GET PROCESSING OPTIONS Command/Response
Determine Path, Perform Card Action Analysis, Perform Cryptography, and Return Application Data
Read Application Data
READ RECORD Commands/Responses
Provide Application Records
Card Read Complete
Card May Be Removed From Reader RF Field
Processing Restrictions
Offline Data Authentication
Cardholder Verification
Online Processing
Completion
Card Represented for Issuer Update Processing (Optional)
Issuer Update Processing
EXTERNAL AUTHENTICATE Command/Response
Issuer-to-Card Script Commands/Responses
Validate ARPC Cryptogram and/or Apply Issuer Script

4.6 Transaction Timing

Business needs dictate that the “card-in-field” time for contactless transactions are to be minimized. “Card-in-field” time is the duration in which the cardholder is required to keep their card in the reader RF field for a contactless transaction.

4.6.1 Timings for Card and Reader Interaction

Req 4.1 (Transaction Timing)

qVSDC and MSD transaction times shall not 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 time does not include the time required to go online for an authorization or for the qVSDC reader to validate a dynamic signature for offline data authentication.

Please contact your Visa regional representative for any additional performance requirements that may be applicable for your region.

5 Reader Requirements

The reader functionality and requirements defined in this specification are *Implementation-Mandatory*, except where explicitly stated otherwise.

5.1 Contactless Communication Protocol Requirements

Reader requirements for the contactless communication protocol are specified in [EMV CL]. This section specifies supplemental reader requirements for the contactless communication protocol.

Req 5.1 ([EMV CL] MBLI)

For readers supporting only [EMV CL 1 1], the reader shall support MBLI = 0 and MBLI = 1 for Type B.

Req 5.2 ([EMV CL] FWI)

For readers supporting only [EMV CL 1 1], the reader shall support FWI values (see [EMV CL] for the FWI definition) of up to 'B' for Type A cards.

5.2 General Reader Requirements

This section defines general reader requirements that may be applicable across multiple functions of the VCPS transaction flow.

qVSDC and MSD are both based on [EMV] card and terminal application specifications. [EMV] constructs, commands, data elements, and functionality are leveraged where possible.

5.2.1 Reader Requirements

Req 5.3 (Offline-capable Readers)

Offline-capable readers shall support fDDA.

Req 5.4 (Receipts)

Receipts are not detailed in this specification, however the following applies:

Readers shall provide receipts as required by Visa Operating Regulations (both international and regional).

Req 5.5 (POS Supports Multiple Interfaces)

For POS devices capable of accepting transactions over multiple interfaces, all permitted interfaces should be made available to the merchant/cardholder to perform a transaction. However, to prevent interference between the contact chip and contactless interfaces, the reader shall always power down the contactless interface prior to the POS device resetting the card to initiate a contact chip transaction. The contactless interface shall remain powered down for the duration of the transaction conducted over the contact chip interface.

5.2.2 qVSDC Reader Requirements

When the qVSDC-enabled reader is idle, the contactless interface should not be powered unless the reader also supports non-Visa functionality requiring the field to be energized. While the operation of non-Visa functionality is outside the scope of this specification, it is recommended that the same principle should be applied, and that the contactless interface should be powered down when the reader is idle.

Req 5.6 (qVSDC Message Requirements)

Data requirements for qVSDC online messages and clearing records shall be as specified in Appendix K.2.

Req 5.7 (qVSDC Messages - FFI and CED)

Implementation-Conditional: This functionality shall be implemented if qVSDC is implemented in the reader.

The reader shall make the Form Factor Indicator and Customer Exclusive Data available for inclusion in messages to the acquirer (when returned by the card application).

Please check with your Visa regional representative regarding the required support for these data elements in acquirer messaging.

Note: Inclusion of the Form Factor Indicator and Customer Exclusive Data in MSD CVN17 online messages and clearing records is always supported by the MSD-enabled reader. See Appendix K.1.2.

Req 5.8 (Interrupted Card Read)

If a contactless transaction is in progress (and Read Application Data has not been completed) when a contact chip transaction is initiated, then the reader shall switch interfaces.

Design consideration should be given to placement of the contactless reader relative to other card interfaces. The contactless reader should not be placed such that it is frequently activated when cardholders attempt to use other interfaces.

5.2.3 MSD Reader Requirements

Readers supporting MSD-only do not normally power off the contactless interface when the reader is idle. However, some MSD-only reader implementations may power off the contactless interface when the reader is idle. For example, MSD-only readers that are portable and battery-powered.

Readers supporting MSD can, by default, process MSD CVN17 and MSD Legacy transactions (see the Glossary for the definition of MSD CVN17 and MSD Legacy). However, the acquirer-merchant is able to disable support for MSD CVN17 transactions.

Req 5.9 (Disable MSD CVN17 Functionality)

Implementation-Conditional: If MSD is implemented in the reader, then the reader shall have a configurable option to disable support for MSD CVN17 transactions.

Acquirer-Merchant-Optional: If MSD is implemented in the reader, then it shall be an acquirer-merchant configurable option to enable or disable support for MSD CVN17 transactions.

If the reader does not support MSD CVN17 transactions, then the data requirements for MSD online messages and clearing records shall be as specified in Appendix K.1.1.

Note: Unless MSD CVN17 support is disabled, the MSD reader is able to process MSD CVN17 transactions, regardless of the setting of the 'Online Cryptogram Required' by reader setting (TTQ byte 2 bit 8).

Req 5.10 (MSD Messaging Requirements)

If MSD CVN17 functionality is disabled on the reader (see Req 5.9), then data requirements for MSD online messages and clearing records shall be as specified in Appendix K.1.1.

If MSD CVN17 functionality is enabled on the reader (see Req 5.9), then data requirements for MSD online messages and clearing records shall be as specified in Appendix K.1.2.

Req 5.11 (MSD Messages - TTQ)

Implementation-Conditional: This functionality shall be implemented if MSD is implemented in the reader.

If MSD CVN17 is enabled on the reader (see Req 5.9), then the reader shall make the TTQ available for inclusion in messages to the acquirer.

Please check with your Visa regional representative regarding the required support for this data element in acquirer messaging.

5.2.4 Reader Configuration Requirements

This section defines some of the configuration requirements for readers. Configuration of the reader shall conform to these requirements, but the reader need not enforce configuration requirements.

5.2.4.1 Reader Configuration Requirements

Readers are only required to support either qVSDC or MSD, but are not precluded from supporting both. Readers supporting both qVSDC and MSD (i.e. concurrently enabled) may be desired for some migration situations.

Req 5.12 (qVSDC and MSD Support)

Readers shall support either qVSDC or MSD, and may support both.

If MSD is supported by the reader, then the reader shall indicate MSD is supported in the Terminal Transaction Qualifiers (TTQ byte 1 bit 8 is 1b).

If qVSDC is supported by the reader, then the reader shall indicate qVSDC is supported in the Terminal Transaction Qualifiers (TTQ byte 1 bit 6 is 1b).

Req 5.13 (MSD Cryptogram Version Number 17)

If MSD-only is supported by the reader **and** MSD CVN17 functionality is enabled, then the reader shall indicate Online Cryptogram Required (TTQ byte 2 bit 8 is 1b).

Req 5.14 (Issuer Update Processing and Online Capability)

If Issuer Update Processing is supported by reader (TTQ byte 3 bit 8 is 1b), then the reader shall support online processing (TTQ byte 1 bit 4 is 0b).

Req 5.15 (qVSDC Transactions with Amount Zero)

qVSDC transactions shall either be sent online or conducted over another interface when the Amount, Authorized is zero.

Reader Risk Parameters are configured in the qVSDC-enabled reader to enforce this requirement.

5.2.4.2 qVSDC and MSD Supported by Reader Configuration Requirements

Readers supporting both qVSDC and MSD shall adhere to the reader requirements for qVSDC and MSD. If discrepancies are found between qVSDC and MSD reader requirements, then qVSDC reader requirements shall take precedence.

Following are additional requirements for readers with both qVSDC and MSD supported at the same time.

Req 5.16 (qVSDC and MSD Supported: Online Cryptogram Not Required)

Req 5.13 (MSD Cryptogram Version Number 17) shall not apply. Reader request for an online cryptogram shall only be set as a result of Reader Preliminary Transaction Processing as specified for qVSDC.

Req 5.17 (qVSDC and MSD Configurations)

Readers that support both qVSDC and MSD active at the same time shall be configurable to support qVSDC-only, MSD-only, and both qVSDC and MSD.

5.2.5 Reader Processing Requirements

Req 5.18 (Purchase Transactions)

Implementation-Conditional: Implementation support for the purchase of goods and services is implementation-mandatory. However, the associated cashback functionality is implementation-conditional on reader support for cashback.

For transactions to purchase goods or services, with or without cashback, the qVSDC-enabled reader shall use:

- Transaction Type '00'.
- Amount, Authorized shall be the sum of the purchase amount and the cashback amount (if present).
- Amount, Other shall be the cashback amount (if present).

Note: Acquirers-merchants may wish to use a different Terminal Transaction Qualifiers (TTQ) value and different Reader Risk Parameters for purchase transactions with cashback than is used for purchase transactions without cashback. The reader should allow the acquirer-merchant to configure the TTQ and Reader Risk Parameters for purchase transactions with cashback independently from purchase transactions without cashback.

Req 5.19 (Cash Transactions)

Implementation-Conditional: This functionality shall be implemented if the reader supports cash transactions.

For cash transactions, the qVSDC-enabled reader shall use:

- Transaction Type '01'.
- Amount, Authorized shall be the transaction amount.

Note: Acquirers-merchants may wish to use a different Terminal Transaction Qualifiers (TTQ) value and different Reader Risk Parameters for cash transactions than is used for purchase transactions (with or without cashback). The reader should allow the acquirer-merchant to configure the TTQ and Reader Risk Parameters for cash transactions independently from purchase transactions.

VCPS transactions directly result in the purchase of goods or services and/or in the disbursement of cash. Refunds and credits are commonly employed to support the retail or cash disbursement environment, but do not directly result in the purchase of goods or services, nor in the disbursement of cash. VCPS functionality can be used to support refunds and credits, and shall comply with the following requirement for the Transaction Type and Amount, Authorized values used. However, all other reader processing for refunds and credits is outside the scope of this specification.

Note: An AAC returned by the card application for refunds and credits simply indicates completion of card action analysis, and should not be treated as a "decline" of the refund.

Req 5.20 (Refund Transactions)

Implementation-Conditional: This functionality shall be implemented if the reader supports refunds/credits.

For refunds and credits, the qVSDC-enabled reader shall use:

- Transaction Type '20'.
- Amount, Authorized shall be the refunded/credited amount.

Req 5.21 (Form Factor Indicator)

If the Form Factor Indicator (FFI) is returned by the card application, then the qVSDC-enabled reader shall replace FFI byte 4 bits 4-1 with the value 0000b (indicating that the transaction was conducted using [ISO 14443]) prior to making the FFI available for inclusion in messages to the acquirer.

Req 5.22 (Unpredictable Number)

If the reader is to return to Discovery Processing after card presentment, then the reader shall discard any previously generated (Reader-Terminal) Unpredictable Number and shall generate a new (Reader-Terminal) Unpredictable Number for use in subsequent transaction processing.

Req 5.23 (Unrecoverable [EMV CL] Error)

If an unrecoverable [EMV CL] error occurs during an application command (e.g. unrecoverable time-out error) followed by a Reset as defined in [EMV CL], then the reader shall discard the current transaction data and shall return to Discovery Processing.

[EMV CL] errors are defined in the [EMV CL] Definitions section.

Req 5.24 (Cardholder Messaging)

For contactless transactions, the reader (or terminal) shall clearly communicate to the cardholder and merchant:

- Present the card
- The progress of the transaction
- The outcome of the transaction – approve, decline, or terminate

Recommended cardholder messages and indications for various transaction states are defined in [VCPS UI].

The qVSDC-enabled reader may display the Amount, Authorized (tag '9F02') when prompting for a card to be presented.

If the card provides the Available Offline Spending Amount, then the qVSDC-enabled reader may display this when it indicates a successful card read and may print it on the transaction receipt.

Note: This specification indicates when communication with the cardholder and merchant occurs, but does not specify the means of communication. User interface requirements are specified on a regional basis.

Req 5.25 (Erroneous Data)

It is the responsibility of the issuer to ensure that data in the card is formatted correctly, and no format checking other than that specifically defined is required on the part of the reader.

However, if in the course of normal processing the reader recognizes that data is incorrectly formatted, then the reader shall terminate the transaction unless otherwise specified. Incorrectly formatted data includes, but is not limited to, the bulleted list provided in [EMV] Book 3 section 7.5.

5.3 Processing Prior to Enabling the Contactless Interface

In order to minimize the time that the card must be in the field, qVSDC-enabled readers supporting variable transaction amounts perform processing prior to powering on the contactless interface and prompting for card presentment.

For qVSDC-enabled readers supporting [EMV EP], Processing Prior to Enabling the Contactless Interface need not be performed as specified in this section, and may be supported as defined in [EMV EP].

5.3.1 Pre-processing Required Check

Req 5.26 (Pre-processing Performed)

Reader Preliminary Transaction Processing (Pre-processing), as described in section 5.3.2, shall be performed by qVSDC-enabled readers supporting variable transaction amounts. The reader contactless interface shall not be powered on until Pre-processing has been completed.

Req 5.27 (No Pre-processing Performed)

If Pre-processing is not performed, then the reader shall immediately power on the contactless interface and proceed to Discovery Processing. The reader shall generate the (Reader-Terminal) Unpredictable Number.

If the transaction amount is not a predefined value or has not been obtained, then the reader shall use a value of all zeros for the Amount, Authorized.

5.3.2 Reader Preliminary Transaction Processing (Pre-processing)

Implementation-Conditional: Pre-processing shall be implemented for readers that implement both qVSDC and variable transaction amounts. All Reader Risk Parameter Checks shall be implemented. Pre-processing shall be performed for qVSDC-enabled readers supporting variable transaction amounts.

The qVSDC-enabled reader performs Pre-processing to obtain the transaction amount and perform reader risk management. The result of reader risk management is the setting of appropriate bits in the Terminal Transaction Qualifiers (TTQ), and determination of whether the contactless interface is to be powered on. Modification of TTQ bits during Pre-processing is transient, and shall not affect the TTQ value obtained for subsequent transactions.

For devices where the transaction amount is a fixed value, TTQ bit settings are already known and need not be determined on a transaction by transaction basis.

5.3.2.1 Pre-processing Data Initialization

Req 5.28 (Amount, Authorized)

The reader shall obtain the Amount, Authorized (tag '9F02').

Req 5.29 (Reader Unpredictable Number)

The reader shall generate the (Reader-Terminal) Unpredictable Number (tag '9F37').

Req 5.30 (Contactless Application Not Allowed)

The Contactless Application Not Allowed indicator and TTQ byte 2 bits 8-7 are transient values, and reset to 0 at the start of Pre-processing.

5.3.2.2 Reader Risk Parameters Checking

Acquirer-Merchant-Optional: If Pre-processing is implemented, then the acquirer-merchant shall have the capability to enable and disable each individual reader risk parameter check defined below.

Req 5.31 (Status Check)

The default setting for this check shall be disabled.

If the Amount, Authorized is a single unit of currency (that is, if a Status Check is being requested), then the reader shall indicate Online Cryptogram Required (set TTQ byte 2 bit 8 to 1b).

Note: Use of status checks is limited to automated fuel dispensing environments.

Req 5.32 (Amount, Authorized of Zero Check)

If the Amount, Authorized is zero, an online-capable reader shall have the following configurable options (at most one option may be enabled at a time):

- Option 1 - Indicate Online Cryptogram Required (set TTQ byte 2 bit 8 to 1b).
- Option 2 - Set the Contactless Application Not Allowed indicator for Visa AIDs to 1.

The default behavior is Option 1, but devices shall be capable of being configured to use Option 2 instead.

Req 5.33 (Amount, Authorized of Zero Check)

If the Amount, Authorized is zero, then an offline-only reader shall set the Contactless Application Not Allowed indicator for Visa AIDs to 1.

Req 5.34 (Reader Contactless Transaction Limit (RCTL) Check)

If the Amount, Authorized is greater than or equal to the Reader Contactless Transaction Limit, then the reader shall set the Contactless Application Not Allowed indicator for Visa AIDs to 1.

Note: It is strongly recommended that the Reader Contactless Transaction Limit Check be disabled.

Req 5.35 (Reader CVM Required Limit Check)

If the Amount, Authorized is greater than or equal to the Reader CVM Required Limit, then the reader shall indicate CVM Required (set TTQ byte 2 bit 7 to 1b).

Req 5.36 (Reader Contactless Floor Limit Check)

If the Amount, Authorized is greater than either the Reader Contactless Floor Limit or (if the Reader Contactless Floor Limit is not present) the applicable Terminal Floor Limit (tag '9F1B'), then the reader shall indicate Online Cryptogram Required (set TTQ byte 2 bit 8 to 1b).

5.3.2.3 Power On Contactless Interface

Req 5.37 (Power On Contactless Interface)

Upon successful completion of Reader Pre-processing, the reader shall power on the contactless interface and shall proceed to Discovery Processing.

However, if the Contactless Application Not Allowed indicator (or equivalent indicator) is 1 for all reader supported applications, then the reader may leave the contactless interface powered off and may switch to another interface.

5.4 Discovery Processing

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

For qVSDC-enabled readers supporting [EMV EP], Discovery Processing need not be performed as specified in this section, and may be supported as defined in [EMV EP].

Req 5.38 (Request Card)

The reader shall request that the card be presented and shall perform polling and collision detection as defined in [EMV CL].

Req 5.39 (Collision)

If multiple contactless payment cards are simultaneously detected prior to application selection, then the reader shall indicate this condition to the cardholder and shall request placement of a single payment card.

Req 5.40 (Power Off Contactless Interface)

qVSDC-enabled readers shall support powering off the contactless interface for the following situations:

- Upon merchant command. For example, to cancel the transaction.
- After a pre-defined timeout period.

5.5 Application Selection

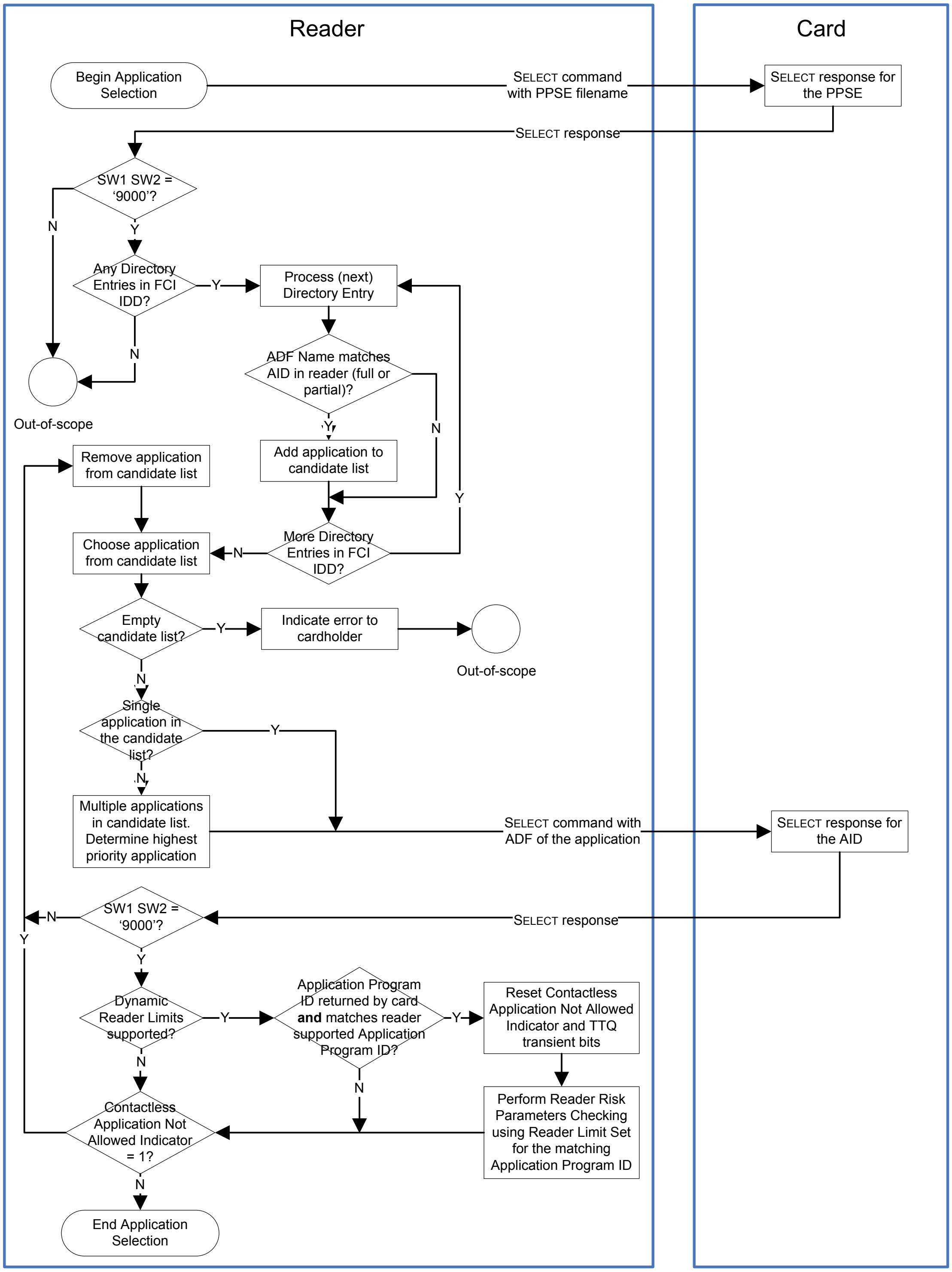
Application Selection is performed immediately after activation of the contactless card, and is the process of determining which of the applications that are supported by both the card and reader will be used to conduct the transaction. This process is performed in two steps:

1. The reader builds a candidate list of mutually supported applications.
2. A single application from the candidate list is identified and selected to process the transaction.

For qVSDC-enabled readers supporting [EMV EP], Application Selection (up to activation of the Visa kernel) need not be performed as specified in this section, and may instead be supported as defined in [EMV EP]. When the SELECT response is received and the Visa kernel activated, the remainder of Application Selection shall be performed as specified in this section.

Figure 5-1: Application Selection Using Directory Selection Method briefly outlines reader processing to perform Application Selection using the Directory Selection Method.

Figure 5-1: Application Selection Using Directory Selection Method


Reader
Card
Begin Application Selection
SELECT command with PPSE filename
SELECT response for the PPSE
SELECT response
SW1 SW2 = '9000'?
N
Y
Any Directory Entries in FCI IDD?
Y
Process (next) Directory Entry
N
ADF Name matches AID in reader (full or partial)?
Out-of-scope
Y
N
Add application to candidate list
Remove application from candidate list
Y
Choose application from candidate list
N
More Directory Entries in FCI IDD?
Empty candidate list?
Y
Indicate error to cardholder
Out-of-scope
N
Single application in the candidate list?
Y
N
Multiple applications in candidate list. Determine highest priority application
SELECT command with ADF of the application
SELECT response for the AID
N
SW1 SW2 = '9000'?
SELECT response
Y
Y
Dynamic Reader Limits supported?
Y
Application Program ID returned by card and matches reader supported Application Program ID?
Y
Reset Contactless Application Not Allowed Indicator and TTQ transient bits
N
N
Perform Reader Risk Parameters Checking using Reader Limit Set for the matching Application Program ID
Contactless Application Not Allowed Indicator = 1?
N
End Application Selection

5.5.1 SELECT Command

To facilitate Application Selection, support for the SELECT command is required.

Req 5.41 (SELECT Command)

The reader shall support the SELECT command, as defined in Appendix G of this specification.

Req 5.42 (DF Names)

The reader shall support DF Names (AIDs) (tag '4F') up to the full 16 byte maximum length.

5.5.2 Directory Selection Method using PPSE

The construction of the candidate list is modeled after the [EMV] Directory Selection Method, except that support for the Directory Selection Method is mandatory for readers (and cards), and the PPSE is used in place of the PSE.

The use of proprietary selection methods is not precluded, but is outside the scope of this specification. Users of proprietary selection methods should be aware of the potential negative impact on performance introduced by any increase in the number of commands. The proprietary selection method also needs to deal with the complexity of priorities amongst all available brands and applications. If the proprietary selection method is unsuccessful and the Directory Selection Method using the PPSE is to be used, this may require that the reader power off the contactless interface.

Req 5.43 (PPSE)

The reader shall support the Directory Selection Method using the PPSE, as defined in this section.

The reader shall perform the following procedure to determine the application to be selected:

Req 5.44 (SELECT PPSE)

The reader shall, using the SELECT command, select the PPSE with a file name of '2PAY.SYS.DDF01'.

If the reader receives SW1 SW2 = '9000' in response to the SELECT command, then the reader shall continue processing.

Else (reader receives SW1 SW2 ≠ '9000'), reader processing is outside the scope of this specification.

Req 5.45 (FCI Issuer Discretionary Data Processing)

Beginning with the first Directory Entry (tag '61'), the reader shall sequentially process each Directory Entry (tag '61') from the FCI Issuer Discretionary Data (tag 'BF0C').

Req 5.46 (Empty FCI at qVSDC-Enabled Reader)

If there is no Directory Entry (tag '61') in the FCI Issuer Discretionary Data (tag 'BF0C'), then reader processing is outside the scope of this specification.

Req 5.47 (Building the Candidate List)

The reader shall examine the ADF Name (tag '4F') of each Directory Entry (tag '61').

If the ADF Name (tag ‘4F’) in the Directory Entry (tag ‘61’) matches an AID in the reader, then the reader shall add the application to the candidate list. The application information added to the candidate list shall include the ADF Name (tag ‘4F’) and the Application Priority Indicator (tag ‘87’, if present).

The ADF Name (tag ‘4F’) matches an AID in the reader if:

- The ADF Name has the same length and value as the AID (full match)
- **or** the ADF Name begins with the entire AID (partial match).

If the ADF Name (tag ‘4F’) is not coded according to [EMV] Book 1 section 12.2.1, then the reader shall ignore the Directory Entry.

5.5.3 Final Selection

Once the reader determines the list of mutually supported applications, it shall perform the following procedure to select an application.

Req 5.48 (Candidate List – Empty)

If there are no mutually supported applications in the candidate list, then the reader shall indicate an error to the cardholder. Subsequent processing is outside the scope of this specification.

Req 5.49 (Candidate List – Single Application)

If there is only one mutually supported application in the candidate list, then the reader shall select the application.

Req 5.50 (Candidate List – Multiple Applications)

If multiple applications are supported in the candidate list, then:

- The reader shall select the application with the highest priority.
- Applications with an Application Priority Indicator (tag '87', bits 4-1) value of 0000b, or no Application Priority Indicator (tag '87') at all, are considered to be of (equal) lowest priority.
- In the case of multiple candidates with equal priority, the candidates shall be selected in the order listed in the PPSE.

Req 5.51 (Select Application)

The reader shall send the SELECT command with the ADF Name (tag '4F') of the selected application. If the selected application is not a Visa AID, then subsequent reader processing is outside the scope of this specification.

If the reader receives SW1 SW2 = '9000' in response to the SELECT command, then the reader shall:

- If Issuer Update Processing is supported by the reader, then the reader shall commit the full ADF Name (AID) of the selected application to memory, for possible use during Issuer Update Processing.
- Continue processing the transaction.

Else (reader receives SW1 SW2 ≠ '9000'), the reader shall remove the application from the candidate list and shall return to the beginning of Final Selection processing.

5.5.4 Dynamic Reader Limits (DRL) Functionality

Implementation-Optional: Implementers may implement support for DRL functionality for qVSDC readers.

Acquirer-Merchant-Optional: If implemented, DRL functionality shall be acquirer-merchant configurable to be enabled or disabled. If enabled, the acquirer-merchant shall be able to configure the number of Application Program IDs to use.

DRL functionality allows the reader to apply different Reader Limit Sets for different card applications (even if they have the same AID), allowing the reader to vary Reader Risk Parameters on a transaction by transaction basis.

For example, a reader may apply one set of Reader Risk Parameters for domestic Visa credit applications, and apply another set of Reader Risk Parameters for international Visa credit applications.

The Application Program Identifier (Application Program ID) is the optional Visa proprietary card application data element that identifies the Reader Risk Parameters applicable to the selected application. The reader examines the Application Program ID returned by the card in the SELECT response and applies the corresponding Reader Risk Parameters.

If DRL functionality is enabled, then the qVSDC-enabled reader performs DRL processing to determine the Reader Risk Parameters (see section 5.3.2.2) to use for the selected application.

5.5.4.1 Reader Limit Set

The value of limits used in Reader Risk Parameters checking, and whether individual checks are enabled or disabled, are specified in a Reader Limit Set. The Reader Limit Set indicates whether each of the individual checks are enabled or disabled, and the value of the limit when the corresponding check is enabled.

Req 5.52 (Reader Risk Parameters)

Each Reader Limit Set shall allow the acquirer-merchant to configure the following Reader Risk Parameters:

- Status Check – Configurable to indicate whether this check is enabled or disabled.
- Amount, Authorized of Zero Check – Configurable to indicate whether this check is enabled or disabled. If enabled, configurable to indicate whether Option 1 or Option 2 is to be used.
- Reader Contactless Transaction Limit Check – Configurable to indicate whether this check is enabled or disabled, and the value of this limit when enabled.
- Reader CVM Required Limit Check – Configurable to indicate whether this check is enabled or disabled, and the value of this limit when enabled.
- Reader Contactless Floor Limit Check – Configurable to indicate whether this check is enabled or disabled, and the value of this limit when enabled.

Req 5.53 (Reader Limit Sets)

The reader shall support a default Reader Limit Set, to be used when no matching Application Program ID (or no Application Program ID at all) is returned in the SELECT response. The default Reader Limit Set contains the Reader Risk Parameters used during Reader Preliminary Transaction Processing (Pre-processing).

In addition to support for the default Reader Limit Set, the reader shall implement support for a minimum of 4 unique Application Program IDs and 4 corresponding Reader Limit Sets. Implementations may optionally support more than 4 Application Program IDs and corresponding Reader Limit Sets.

5.5.4.2 Dynamic Reader Limits (DRL) Processing

DRL Processing is performed to determine the Reader Limit Set applicable to the selected application. When a matching Application Program ID is returned by the card application, the reader replaces the results of Reader Risk Parameters Checking that used the default Reader Limit Set (performed during Pre-processing) with the results of Reader Risk Parameters Checking using the matching Reader Limit Set.

If DRL functionality is supported, the reader shall perform the following procedure:

Req 5.54 (Application Program ID)

The reader examines the Application Program ID returned in the SELECT response to determine which Reader Limit Set to apply.

If no Application Program ID is returned **or** the Application Program ID does not match any reader supported Application Program ID, then the reader shall use the results of Reader Preliminary Transaction Processing (Pre-processing) and proceed with the Contactless Application Allowed Check (section 5.5.5).

Else (the Application Program ID matches a supported reader Application Program ID), the reader shall:

- Reset the Contactless Application Not Allowed indicator to 0 and the transient bits of the TTQ (byte 2 bits 8-7) to 0b.
- Perform Reader Risk Parameters Checking using the Reader Limit Set that corresponds to the matching Application Program ID. Reader Risk Parameters Checking is performed as defined in section 5.3.2.2.
- Proceed with the Contactless Application Allowed Check (section 5.5.5).

Note: If not precluded by reader support for other payment systems, some reader processing performed during Dynamic Reader Limits Processing may be performed during Reader Preliminary Transaction Processing (Pre-processing). To minimize the processing performed while the card is in the reader field, it is recommended that readers perform Reader Risk Parameters Checking for each supported Application Program ID during Pre-processing. The value of the Contactless Application Not Allowed indicator and the TTQ are then stored for each Application Program ID, and used by the reader if the corresponding Application Program ID is returned by the card application.

5.5.5 Contactless Application Allowed Check

Implementation-Conditional: This section shall be supported if Pre-processing is supported.

The reader examines the Contactless Application Not Allowed indicator to determine whether the selected application is allowed to transact over the contactless interface.

Req 5.55 (Contactless Application Not Allowed)

If the Contactless Application Not Allowed indicator is 1, then the reader shall remove the application from the candidate list and return to the beginning of Final Selection processing.

Else (the Contactless Application Not Allowed indicator is 0), the reader shall continue processing the transaction.

5.6 Initiate Application Processing

During Initiate Application Processing, the reader issues the GET PROCESSING OPTIONS (GPO) command to the card, and includes any data that the card has requested in the PDOL during Application Selection. Application data necessary to process the transaction is returned by the card application during Initiate Application Processing, and may also be returned during Read Application Data.

5.6.1 GET PROCESSING OPTIONS (GPO) Command

To facilitate Initiate Application Processing, support for the GPO command is required.

Req 5.56 (GPO Command)

The reader shall support the GET PROCESSING OPTIONS (GPO) command, as defined in Appendix G of this specification.

Data Object List (DOL) coding is performed according to [EMV] Book 3 section 5.4. Readers shall be able to provide the value of reader data elements (defined in Appendix D) requested by the card application.

Req 5.57 (Format 1 and Format 2)

Readers shall support GPO responses in [EMV] Format 1 and [EMV] Format 2, as defined in Appendix G of this specification.

Req 5.58 (Recognized and Unrecognized Data)

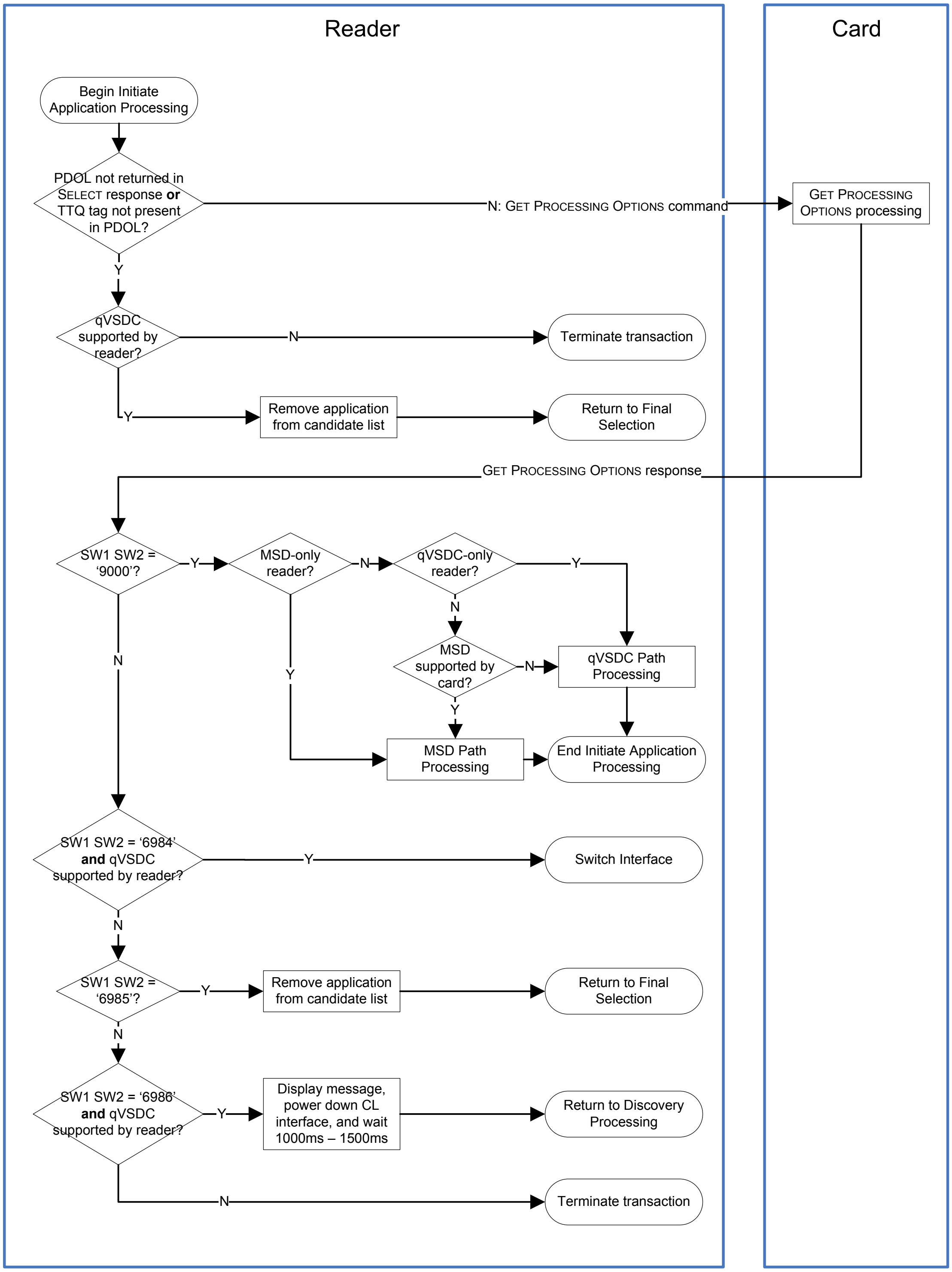
The reader shall store all recognized data elements read, whether mandatory or optional, for later use in transaction processing. Data elements that are not recognized by the reader (that is, their tags are unknown by the reader) may be ignored and do not need to be stored.

Note: As the card application may return application data in both the GPO response and in records, the reader does not check for the presence of mandatory data elements until Card Read Complete.

5.6.2 Initiate Application Processing

Figure 5-2: Initiate Application Processing (Reader) briefly outlines reader processing to perform Initiate Application Processing.

Figure 5-2: Initiate Application Processing (Reader)


Reader
Card
Begin Initiate Application Processing
PDOL not returned in SELECT response **or** TTQ tag not present in PDOL?
N: GET PROCESSING OPTIONS command
GET PROCESSING OPTIONS processing
Y
qVSDC supported by reader?
N
Terminate transaction
Y
Remove application from candidate list
Return to Final Selection
GET PROCESSING OPTIONS response
SW1 SW2 = '9000'?
Y
MSD-only reader?
N
qVSDC-only reader?
Y
N
MSD supported by card?
N
qVSDC Path Processing
Y
Y
MSD Path Processing
End Initiate Application Processing
N
SW1 SW2 = '6984' **and** qVSDC supported by reader?
Y
Switch Interface
N
SW1 SW2 = '6985'?
Y
Remove application from candidate list
Return to Final Selection
N
SW1 SW2 = '6986' **and** qVSDC supported by reader?
Y
Display message, power down CL interface, and wait 1000ms – 1500ms
Return to Discovery Processing
N
Terminate transaction

Prior to initiating the transaction with the card, the reader checks the SELECT response for the presence of the Processing Options Data Object List (PDOL, tag '9F38'), and for the presence of the Terminal Transaction Qualifiers (TTQ, tag '9F66') tag in the PDOL.

Req 5.59 (PDOL in SELECT Response)

If **either** of the following is true:

- the PDOL (tag '9F38') is not present in the SELECT response
- **or** TTQ tag '9F66' is not present in the PDOL

Then:

- If qVSDC is supported by the reader, then the reader shall remove the application from the candidate list and return to the beginning of Final Selection processing.

  Else (MSD-only reader), the reader shall terminate the transaction.

Note: The reader does not perform any processing based on the length of reader-terminal data elements requested by the card application in the PDOL. For example, the length of the TTQ requested by the card application in the PDOL has no impact on reader processing.

The reader shall perform the following procedure to initiate the transaction with the card.

Req 5.60 (Issue GPO Command)

The reader shall issue the GET PROCESSING OPTIONS (GPO) command. The command data field is a data object coded according to the PDOL provided by the card, preceded by the Command Template tag and length.

Req 5.61 (GPO Response SW1 SW2)

If the reader receives SW1 SW2 = '9000' in response to the GPO command, then the reader shall continue Initiate Application Processing.

Else, if the reader receives SW1 SW2 = '6984' in response to the GPO command **and** qVSDC is supported by the reader, then the reader shall switch interfaces.

Else, if the reader receives SW1 SW2 = '6985' in response to the GPO command, then the reader shall remove the application from the candidate list and shall return to the beginning of Final Selection processing.

Else, if the reader receives SW1 SW2 = '6986' in response to the GPO command **and** qVSDC is supported by the reader, then the reader shall:

- Indicate to the cardholder to refer to their payment device for further instructions and immediately power down the contactless interface.

  Note: SW1 SW2 = '6986' is not returned by cards compliant to this specification. However, reader behavior is defined in this specification to support consumer payment devices that are capable of informing the cardholder of the subsequent action to take. For example, the consumer payment device may be a mobile handset capable of instructing the consumer of the action to take.

- After a duration of between 1000ms and 1500ms, the reader shall power up the contactless interface and return to Discovery Processing. Any message displayed to the cardholder shall continue to be displayed during the subsequent Discovery Processing.

Else (SW1 SW2 does not match any of the above), the reader shall terminate the transaction.

Req 5.62 (Contactless Path Determination)

The reader has received SW1 SW2 = '9000' in response to the GPO command, and determines the contactless path for the transaction.

If the reader is MSD-enabled and is not qVSDC-enabled, then the reader shall continue processing. For all subsequent reader processing with different behavior based on path, the reader shall proceed with MSD Path Processing.

If the reader is qVSDC-enabled and is not MSD-enabled, then the reader shall continue processing. For all subsequent reader processing with different behavior based on path, the reader shall proceed with qVSDC Path Processing.

If the reader is both MSD-enabled and qVSDC-enabled, then the reader shall examine the Application Interface Profile (AIP, tag '82') returned in the GPO response to determine subsequent processing:

- If the card indicates MSD is supported (AIP byte 2 bit 8 is 1b), then the reader shall continue processing. For all subsequent reader processing with different behavior based on path, the reader shall proceed with MSD Path Processing.

  Else, if the card indicates MSD is not supported (AIP byte 2 bit 8 is 0b), then the reader shall continue processing. For all subsequent reader processing with different behavior based on path, the reader shall proceed with qVSDC Path Processing.

  Else (the AIP was not returned in the GPO response or was incorrectly formatted), the reader shall terminate the transaction.

5.7 Read Application Data

The reader performs Read Application Data if an Application File Locator (AFL) was returned during Initiate Application Processing, and proceeds to Card Read Complete if an AFL is not returned.

During Read Application Data, the reader uses the READ RECORD command to retrieve the card data necessary to process the transaction.

5.7.1 READ RECORD Command

Req 5.63 (READ RECORD Command)

The reader shall support the READ RECORD command, as defined in Appendix G of this specification.

5.7.2 Read Application Data

The reader shall perform the following procedure to read the card application data.

Req 5.64 (Application File Locator)

If the Application File Locator (AFL, tag '94') is returned during Initiate Application Processing, then the reader shall perform Read Application Data as specified in [EMV] Book 3, section 10.2.

If the Application File Locator (AFL, tag '94') was not returned during Initiate Application Processing, then the reader shall proceed to Card Read Complete.

5.8 Card Read Complete

After Read Application Data has been completed, the reader indicates to the cardholder that card read is complete, and the cardholder should remove their card from the reader’s RF field. The reader checks the application data returned by the card to ensure that all mandatory data for the transaction has been returned, and that redundant primitive data was not returned. Primitive data elements are redundant if more than one occurrence of the primitive data element was returned by the card during Initiate Application Processing and Read Application Data.

The reader shall perform the procedure described in this section for Card Read Complete.

5.8.1 Cardholder Messaging

Req 5.65 (Card Read Complete Cardholder Messaging)

The reader shall indicate to the cardholder and merchant that card read is complete and that the card may be removed, but that the transaction is still in progress.

Note: As with all cardholder indication and messaging requirements, this cardholder indication may vary per regional requirements. For example, indication that the card read is complete may consist simply of activating indicator lights with an audible beep. Contact your Visa regional representative for additional guidance on cardholder indication and messaging requirements for your region.

Req 5.66 (Card Read Complete)

If qVSDC is supported by the reader, then the reader shall power off the contactless interface and continue processing the transaction. Powering off the contactless interface in this requirement does not include stopping the current application.

Else (MSD-only supported by reader), the reader shall perform an [EMV CL] Removal and continue processing the transaction.

5.8.2 Mandatory and Redundant Data

The reader examines application data returned by the card during Initiate Application Processing and Read Application Data to determine whether all mandatory data elements were returned, and whether redundant primitive data elements were returned.

Req 5.67 (Mandatory Data)

The reader shall ensure that all mandatory data elements are returned by the card. Whether data elements are mandatory depends upon the processing path (qVSDC or MSD) determined by the reader during Initiate Application Processing.

If any mandatory data elements are not present for the applicable path, then the reader shall terminate the transaction.

Req 5.68 (Redundant Data)

Redundant primitive data elements are not permitted.

If the reader encountered more than one occurrence of a single primitive data element while reading data from the card during Initiate Application Processing and Read Application Data, then the reader shall terminate the transaction.

5.8.3 Determine Card Transaction Disposition

5.8.3.1 qVSDC Path Processing

The reader shall perform the procedure defined in this section for qVSDC transactions.

Req 5.69 (Cryptogram Information Data)

If the Cryptogram Information Data (CID) is not returned by the card, then the reader shall:

- Construct the CID and initialize it with a value of '00'.
- Set CID bits 8-7 to the value of Issuer Application Data byte 5 bits 6-5 using identical bit settings.

Note: Issuer Application Data byte 5 contains Card Verification Results (CVR) byte 2, indicating the cryptogram type.

Req 5.70 (Cryptogram Type Transaction Disposition)

The reader examines the Cryptogram Information Data (CID) to determine the cryptogram type (TC, ARQC, or AAC).

If an Application Authentication Cryptogram (AAC) is returned by the card, then the reader shall set the Decline Required by Reader Indicator to 1.

If an Authorization Request Cryptogram (ARQC) is returned by the card **or** Online Cryptogram Required by the reader (TTQ byte 2 bit 8 is 1b), then the reader shall set the Online Required by Reader Indicator to 1.

If the cryptogram type cannot be determined (TC, ARQC, or AAC), then the reader shall set the Decline Required by Reader Indicator to 1.

Note: A reader indicator is not set when the cryptogram type is a TC.

5.8.3.2 MSD Path Processing

The reader shall perform the procedure defined in this section for MSD transactions.

Processing to determine the transaction disposition need not be performed, as all MSD transactions require online processing.

If needed, the following requirement allows for the Track 2 and Track 1 data to be formatted into a suitable magnetic stripe format.

Req 5.71 (Formatting Track 2 Data)

Acquirer-Merchant-Optional: This functionality shall be configurable to be enabled or disabled at acquirer-merchant discretion.

If formatting of Track 2 is enabled, then the reader shall format the Track 2 data into the magnetic stripe format as defined in Appendix F.2 Creating Track 2.

Req 5.72 (Constructing Track 1 Data)

Acquirer-Merchant-Optional: This functionality shall be configurable to be enabled or disabled at acquirer-merchant discretion.

If construction of Track 1 is enabled, then the reader shall construct the Track 1 data as defined in Appendix F.1 Creating Track 1.

MSD transactions are processed under magnetic stripe payment rules, subject to Visa rules and regulations.

Req 5.73 (Subsequent MSD Processing)

Subsequent MSD transaction processing is outside the scope of this specification. Please contact your Visa regional representative for the processing requirements applicable to your region.

However, MSD transactions shall always be online authorized. The minimum data requirements for MSD online messages are specified in Appendix K.1.

5.9 Processing Restrictions

The reader performs Processing Restrictions to determine whether there are restrictions for the transaction. The reader checks the application expiration date, application usage, and may check whether the card application is on the Terminal Exception File.

5.9.1 qVSDC Path Processing

The reader shall perform the procedure defined in this section for qVSDC transactions.

Req 5.74 (Application Expired Check)

Implementation-Conditional: The Application Expired Check shall be implemented for readers supporting offline transactions.

This check shall be performed if a Transaction Certificate (TC) is returned by the card application.

If the Terminal Transaction Date (local to the reader-terminal) is greater than the Application Expiration Date, then the application has expired. The reader shall examine the Card Transaction Qualifiers (CTQ) to determine further processing:

- If 'Go Online If Application Expired' indicated by card (CTQ byte 1 bit 4 is 1b), then the reader shall set the Online Required by Reader Indicator to 1.

  Else, the reader shall set the Decline Required by Reader Indicator to 1.

Req 5.75 (Terminal Exception File Check)

Implementation-Optional: Terminal Exception File checking is an implementation option.

Acquirer-Merchant-Optional: If implemented, then the Terminal Exception File Check shall be acquirer-merchant configurable to be enabled or disabled.

This check shall be performed if a Transaction Certificate (TC) is returned by the card application.

If the Application PAN is present on the Terminal Exception File, then the reader shall set the Decline Required by Reader Indicator to 1.

Req 5.76 (Application Usage Control - Cash Transactions)

Implementation-Conditional: This functionality shall be implemented if the reader supports cash transactions.

This check shall be performed for cash transactions.

If **either** of the following is true:

- Issuer Country Code matches the Terminal Country Code **and** the card application is 'Valid for domestic cash transactions' (AUC byte 1 bit 8 is 1b)
- Issuer Country Code does not match the Terminal Country Code **and** the card application is 'Valid for international cash transactions' (AUC byte 1 bit 7 is 1b)

Then the cash transaction is allowed and the reader continues processing the transaction.

Else (application is not valid for the cash transaction, or Issuer Country Code or AUC is not returned by the card application), the reader shall examine the Card Transaction Qualifiers to determine further processing:

- If 'Switch Interface for Cash Transactions' supported by card (CTQ byte 1 bit 3 is 1b), then the reader shall switch to another interface.

  Else ('Switch Interface for Cash Transactions' not supported by card or CTQ not returned), the reader shall set the Decline Required by Reader Indicator to 1.

Req 5.77 (Application Usage Control - Cashback Transactions)

Implementation-Conditional: This functionality shall be implemented if the reader supports transactions with cashback.

This check shall be performed for transactions with cashback.

If **either** of the following is true:

- Issuer Country Code matches the Terminal Country Code **and** 'Domestic cashback allowed' by card application (AUC byte 2 bit 8 is 1b)
- Issuer Country Code does not match the Terminal Country Code **and** 'International cashback allowed' by card application (AUC byte 2 bit 7 is 1b)

Then the transaction with cashback is allowed and the reader continues processing the transaction.

Else (application is not valid for the transaction with cashback, or Issuer Country Code or AUC is not returned by the card application) , the reader shall examine the Card Transaction Qualifiers to determine further processing:

- If 'Switch Interface for Cashback Transactions' supported by card (CTQ byte 1 bit 2 is 1b), then the reader shall switch to another interface.

  Else ('Switch Interface for Cashback Transactions' not supported by card or CTQ not returned), the reader shall set the Decline Required by Reader Indicator to 1.

5.10 Offline Data Authentication

Offline Data Authentication is performed by the reader to verify the dynamic signature and authenticate the data from the card.

5.10.1 qVSDC Path Processing

Implementation-Conditional: Offline Data Authentication shall be implemented for readers supporting offline transactions. Offline Data Authentication is performed for card requested offline transactions.

The reader shall perform the procedure defined in this section for qVSDC transactions if the Online Required by Reader Indicator is 0 **and** the Decline Required by Reader Indicator is 0.

Req 5.78 (fDDA Verification)

The reader shall verify the fDDA dynamic signature according to [EMV] and the definition of fDDA in Appendix A.

If either fDDA fails or the reader is unable to perform fDDA, then the reader shall examine the Card Transaction Qualifiers (CTQ) to determine further processing:

- If ‘Go Online If ODA Fails’ indicated by card (CTQ byte 1 bit 6 is 1b) **and** Online supported by reader, then the reader shall set the Online Required by Reader Indicator to 1 and continue processing the transaction.

  Else, if ‘Switch Interface If ODA Fails’ indicated by card (CTQ byte 1 bit 5 is 1b) **and** EMV contact chip supported by reader, then the reader shall switch to another interface. For this case, the reader is aware that contact chip is supported, and shall explicitly indicate that the contact chip interface is to be used.

  Else (neither of the above or CTQ not returned), the reader shall set the Decline Required by Reader Indicator to 1 and continue processing the transaction.

5.11 Cardholder Verification

The reader determines if a Cardholder Verification Method (CVM) is to be performed. The CVMs that may be supported for VCPS are Online PIN, Consumer Device CVM, and Signature.

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

5.11.1 qVSDC Path Processing

Implementation-Mandatory: Cardholder Verification shall be implemented for qVSDC-enabled readers.

Acquirer-Merchant-Optional: The acquirer-merchant shall be able to enable and disable the supported CVMs. However, support for the Consumer Device CVM shall be enabled (TTQ byte 3 bit 7 is 1b).

The reader shall perform the procedure defined in this section for qVSDC transactions if the Decline Required by Reader Indicator is 0.

Req 5.79 (CTQ Not Returned by Card)

If the reader requires a CVM and the Card Transaction Qualifiers (CTQ, tag '9F6C') is not returned by the payment application:

- A reader that supports Signature, in addition to any other CVMs, shall acquire a signature for the transaction.
- A reader that supports only the Consumer Device CVM and Online PIN shall perform Online PIN.
- A reader that supports only the Consumer Device CVM shall set the Decline Required by Reader Indicator to 1.

Note: Reader support for the Consumer Device CVM is mandatory, as is indication of its support in the Terminal Transaction Qualifiers. In addition to supporting the Consumer Device CVM, the reader may optionally be configured to support Online PIN and/or Signature.

Req 5.80 (CTQ Returned by Card)

If the CTQ (tag '9F6C') is returned by the payment application, then the reader shall examine the CTQ (in the order specified below) to determine the CVM to be performed:

- If Online PIN Required by card (CTQ byte 1 bit 8 is 1b) and Online PIN supported by reader, then the reader shall perform Online PIN. The reader shall not examine the remaining CTQ bits for CVM processing.

  Else (Online PIN not required or not supported), if Consumer Device CVM Performed by card (CTQ byte 2 bit 8 is 1b), then:

  – If the Card Authentication Related Data was returned during the transaction, then:

    - If Card Authentication Related Data bytes 6-7 match CTQ bytes 1-2 (respectively), then CVM processing is complete and the reader shall not examine the remaining CTQ bits for CVM processing.

      Else (Card Authentication Related Data bytes do not match CTQ bytes), the reader shall set the Decline Required by Reader Indicator to 1. CVM processing is complete and the reader shall not examine the remaining CTQ bits for CVM processing.

    Else (Card Authentication Related Data was not returned during the transaction), if the cryptogram type is an ARQC, then CVM processing is complete and the reader shall not examine the remaining CTQ bits for CVM processing.

Else (Card Authentication Related Data was not returned during the transaction and cryptogram type is not an ARQC), the reader shall set the Decline Required by Reader Indicator to 1. CVM processing is complete and the reader shall not examine the remaining CTQ bits for CVM processing.

Note: For qVSDC online requests, the payment application response does not normally contain the Card Authentication Related Data. Consequently, the reader cannot ensure that the CTQ is verifiably unaltered after transmission by the payment application. However, the issuer may examine CVR byte 2 bit 3 to determine whether a Consumer Device CVM was successfully performed.

Else (Neither Online PIN required nor Consumer Device CVM performed), if Signature Required (CTQ byte 1 bit 7 is 1b) and the reader supports Signature (TTQ byte 1 bit 2 is 1b), then the reader shall acquire a signature for the transaction.

Else (None of the above), a common CVM was not indicated in the CTQ and a CVM is not performed.

Note: Cardholder Verification processing to determine the CVM to perform for the transaction, if any, is performed in this section. However, actual performance of the CVM need not take place during this point in the transaction (e.g. acquiring a signature for the transaction).

Req 5.81 (CVM Required and CVM Not Performed)

If the reader requires a CVM and a CVM will not be performed, then the reader shall set the Decline Required by Reader Indicator to 1.

5.12 Online Processing

The reader sends an authorization request to the issuer host. Online Processing allows the issuer host to review and authorize or decline transactions using the issuer’s host based risk management parameters.

5.12.1 qVSDC Path Processing

Implementation-Conditional: Online Processing shall be implemented for qVSDC readers supporting online transactions.

The reader shall perform the processing defined in this section for qVSDC transactions if the Online Required by Reader Indicator is 1 **and** the Decline Required by Reader Indicator is 0.

Req 5.82 (qVSDC Online Authorization)

The reader shall send an online authorization request message to the acquirer. The minimum data requirements for qVSDC online messages are specified in Appendix K.2.

5.13 Completion

5.13.1 qVSDC Path Processing

The reader shall perform the procedure defined in this section for qVSDC transactions.

Req 5.83 (qVSDC Online Processing Performed)

When Online Processing is performed and an authorization response message is received, the reader shall examine the authorization response message to determine subsequent processing.

If **all** of the following are true:

- Issuer Update Processing supported by reader
- **and** Issuer Update Processing supported by card (CTQ returned by card and CTQ byte 2 bit 7 is 1b)
- **and** Issuer Authentication Data or Issuer Script Template(s) received in authorization response message

Then the reader shall proceed with Issuer Update Processing.

Else, the reader shall proceed with Transaction Approved (section 5.13.2) or Transaction Declined (section 5.13.3) based upon the authorization response.

Req 5.84 (qVSDC Online Processing Not Performed)

When Online Processing is not performed (or performed and an authorization response message is not received), the reader shall examine internal reader transaction disposition indicators to determine subsequent processing.

If Online Required by Reader Indicator is 1 **or** Decline Required by Reader Indicator is 1, then the reader shall proceed with Transaction Declined (section 5.13.3).

Else (neither Online nor Decline Required), the reader shall proceed with Transaction Approved (section 5.13.2).

5.13.2 Transaction Approved

Req 5.85 (Cardholder Messaging for Approved)

The reader shall indicate to the cardholder and merchant that the transaction has been approved.

If the Available Offline Spending Amount (AOSA) is returned by the card, then readers that support displaying or printing the AOSA shall do so.

5.13.3 Transaction Declined

Req 5.86 (Cardholder Messaging for Declined)

The reader shall decline the transaction and indicate to the cardholder and merchant that the transaction has been declined.

If the Available Offline Spending Amount (AOSA) is returned by the card, then readers that support displaying or printing the AOSA shall do so.

Req 5.87 (Do Not Reattempt Transaction)

The reader shall not attempt to perform the transaction over another interface.

5.14 Issuer Update Processing

Implementation-Optional: Issuer Update Processing is an implementation option for readers implementing qVSDC, and if supported, must meet the requirements of both sections 5.14.1 and 5.14.2.

Acquirer-Merchant-Optional: If implemented, support for Issuer Update Processing is acquirer-merchant optional. Reader support for Issuer Update Processing is indicated to the card by setting ‘Issuer Update Processing supported’ by reader (TTQ byte 3 bit 8 to 1b).

If supported, Issuer Update Processing is conditionally performed for qVSDC Path Processing (see section 5.13.1).

5.14.1 Issuer Update Commands

To facilitate Issuer Update Processing, support for the EXTERNAL AUTHENTICATE command and issuer script processing is required.

Req 5.88 (EXTERNAL AUTHENTICATE Command)

The reader shall support the EXTERNAL AUTHENTICATE command, as defined in Appendix G.5 of this specification.

Req 5.89 (Issuer Scripts)

The reader shall support Issuer Scripts according to [EMV] Book 3 section 10.10, and [EMV] Book 4 section 6.3.9, except for the following:

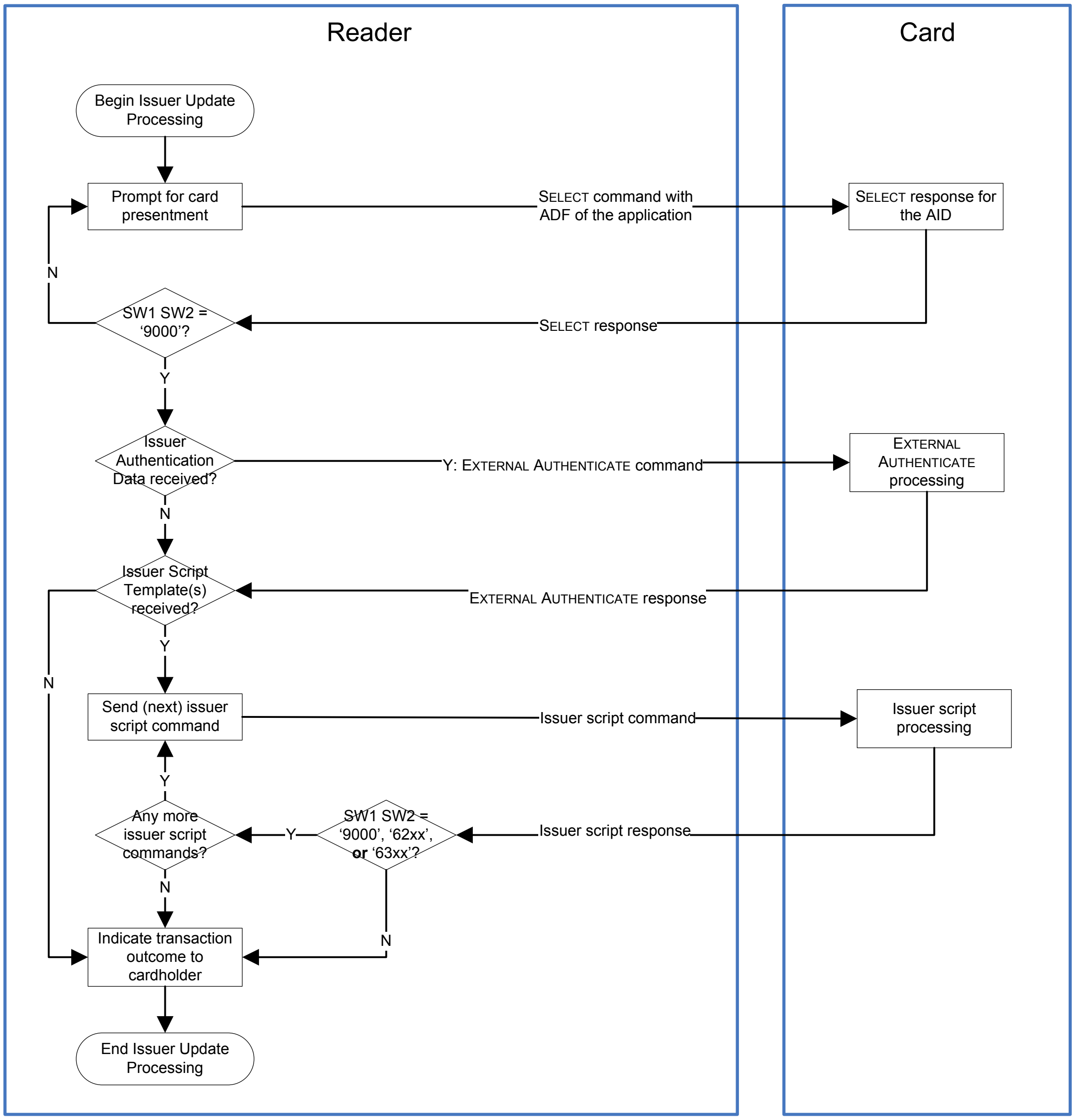
- Unlike [EMV], Issuer Script Templates with tag '71' or '72' are processed and issued by the reader in the same manner. There is no GENERATE AC command, and Issuer Script Templates with tag '71' and '72' are both processed during Issuer Update Processing.
- No processing is performed on the Transaction Status Information (TSI) or Terminal Verification Results (TVR).

5.14.2 Issuer Update Processing

The reader performs Issuer Update Processing as defined in this section.

Figure 5-3: Issuer Update Processing (Reader) briefly outlines reader processing to perform Issuer Update Processing.

Figure 5-3: Issuer Update Processing (Reader)


Reader
Card
Begin Issuer Update Processing
Prompt for card presentment
SELECT command with ADF of the application
SELECT response for the AID
N
SW1 SW2 = '9000'?
SELECT response
Y
Issuer Authentication Data received?
Y: EXTERNAL AUTHENTICATE command
EXTERNAL AUTHENTICATE processing
N
Issuer Script Template(s) received?
EXTERNAL AUTHENTICATE response
Y
N
Send (next) issuer script command
Issuer script command
Issuer script processing
Y
Any more issuer script commands?
Y
SW1 SW2 = '9000', '62xx', or '63xx'?
Issuer script response
N
N
Indicate transaction outcome to cardholder
End Issuer Update Processing

The reader shall perform the following procedure to perform Issuer Update Processing.

Req 5.90 (Prompt for Card)

The reader shall prompt the cardholder to (re)present their contactless card for Issuer Update Processing, and Discovery Processing shall be performed as specified in section 5.4.

If the reader powers off the contactless interface as described in Req 5.40 (Power Off Contactless Interface), then the reader shall proceed to Req 5.94 (Second Tap Completed).

Req 5.91 (SELECT Application)

The reader shall issue a SELECT command specifying the full ADF Name (AID) of the contactless card application from the previous transaction. This AID will have been previously committed to memory by the reader.

If the reader receives SW1 SW2 = '9000' in response to the SELECT command, then the reader shall continue processing.

Else (reader receives SW1 SW2 ≠ '9000'), the reader shall return to Prompt for Card.

Req 5.92 (EXTERNAL AUTHENTICATE Command)

If Issuer Authentication Data was received in the authorization response message, then the reader shall issue an EXTERNAL AUTHENTICATE command using the Issuer Authentication Data received.

Note: The reader does not perform processing based on the card response to the EXTERNAL AUTHENTICATE command. The reader continues Issuer Update Processing regardless of the SW1 SW2 value returned by the card.

Req 5.93 (Issuer Script Commands)

The reader issues issuer script command(s) if an Issuer Script Template was received in the authorization response. Issuer Script Templates shall follow Issuer Script Template 1 or 2, and an Issuer Script Template may have multiple issuer script commands.

In this version of the specification, at most one Issuer Script Template is supported in the response message. However, readers shall parse all Issuer Script Templates received and issue the corresponding issuer script commands.

The reader shall parse each Issuer Script Template to retrieve each issuer script command, and shall transmit the commands to the card one by one.

If the response to an issuer script command is not SW1 SW2 = '9000', '62xx', or '63xx', then the reader shall not send any further issuer script commands and shall discontinue Issuer Script Command(s) processing.

Req 5.94 (Second Tap Completed)

The reader shall indicate to the cardholder the transaction outcome based on the issuer authorization response, regardless of the results of Issuer Update Processing.

If the Available Offline Spending Amount (AOSA) was returned by the card (during Initiate Application Processing or Read Application Data), then readers that support displaying or printing the AOSA shall not do so.

6 Card Requirements

The card functionality and requirements defined in this specification are *Implementation-Mandatory*, except where explicitly stated otherwise.

6.1 Contactless Communication Protocol Requirements

Card requirements for the contactless communication protocol are specified in [EMV CL].

6.2 General Card Requirements

This section defines general card requirements that may be applicable across multiple functions of the VCPS transaction flow.

qVSDC and MSD are both based on [EMV] card and terminal application specifications. [EMV] constructs, commands, data elements, and functionality are leveraged where possible.

6.2.1 Card Requirements

Req 6.1 (Atomic Commands)

The card shall process each command as a single atomic operation. Commands shall be processed in their entirety or not at all, with the following exception(s):

- Incrementing the Application Transaction Counter (ATC) shall be immediate and irreversible.
- Resetting the Last Contactless Application Cryptogram Valid Indicator to 0 shall be immediate and irreversible.

Req 6.2 (Counter Overflow)

Counters shall not be incremented above their maximum possible value (an overflow) and shall not be decremented below zero.

If increment of a counter would result in an overflow, then the application shall set the counter to the maximum possible value.

If decrement of a counter would result in a value less than zero, then the application shall set the counter to a value of zero.

For the evaluation of conditions, if incrementing a counter would result in an overflow or decrementing a counter would cause a negative value to be used for the comparison, then the result of the comparison shall be that velocity checking counters were exceeded.

Req 6.3 (Dual-Interface Contactless and Contact Cards)

Dual-interface contactless and contact cards supporting both [VCPS] and [VIS] shall implement the functionality and requirements for dual-interface cards defined in Appendix I Dual-Interface Contactless and Contact Cards.

Req 6.4 (Commands Restricted by Interface)

This requirement is only applicable after the card application has been personalized.

The card application shall only support and process commands received over the contactless interface if they are explicitly defined in Appendix G.

If a command is received over an unsupported interface (for that command), then the card application shall respond with an error SW1 SW2 ('6A81' is recommended).

Req 6.5 (qVSDC and MSD Path Support)

Cards shall implement both qVSDC and MSD.

For qVSDC path processing, the following GPO responses shall be issuer configurable to be enabled or disabled:

- qVSDC Offline GPO Response (if offline implemented): see Table 6-2 using Condition column "Offline (with ODA)"
- qVSDC Online with ODA GPO Response: see Table 6-2 using Condition column "Online (with ODA)"
- qVSDC Online/Decline without ODA GPO Response: see Table 6-2 using Condition column "Online and Decline (without ODA)"

For MSD path processing, the following GPO responses shall be issuer configurable to be enabled or disabled:

- MSD CVN17 with ODA GPO Response: see Table 6-3 using Condition column "Online (with ODA)"
- MSD CVN17 without ODA GPO Response: see Table 6-3 using Condition Online (without ODA)"
- MSD Legacy GPO Response: see Table 6-4

If Card Action Analysis results in a transaction disposition with a disabled GPO response, then the card application shall not perform the processing for the transaction disposition and shall respond to the GPO command with error SW1 SW2 = '6985'.

Req 6.6 (Cryptogram Version Number)

The qVSDC path shall implement support for Cryptogram Version Number 10 and Cryptogram Version Number 17, and may implement support for Cryptogram Version Number 18 at implementer discretion. The Cryptogram Version to be used for cryptogram generation shall be issuer configurable, and indicated by the issuer in the Cryptogram Version Number of the Issuer Application Data returned for qVSDC transactions.

The MSD path shall support Cryptogram Version Number 17. The Cryptogram Version to be used for cryptogram generation shall be Cryptogram Version Number 17, and shall be indicated by the issuer in the Cryptogram Version Number of the Issuer Application Data returned for MSD transactions.

Req 6.7 (Application Permanently Blocked)

If incrementing the ATC results in the ATC reaching its maximum value, then the application shall be permanently blocked as follows:

- APPLICATION UNBLOCK shall be permanently disabled. The APPLICATION UNBLOCK command is defined in Appendix G.5.2.
- Linked applications shall be permanently blocked, and APPLICATION UNBLOCK shall be permanently disabled for those linked applications. Applications may have been linked as defined in [VIS].
- Cryptographic operations shall be disabled.
- The application shall respond to the SELECT command with SW1 SW2 = '6283' (indicating application blocked).
- The application shall respond to the GET PROCESSING OPTIONS command with error SW1 SW2 = '6985', which permits another application to be selected.

Req 6.8 (Dynamic CVV)

Card applications shall implement dCVV (including the ATC Insertion Option) as defined in Appendix B, and dCVV functionality shall be configurable to be enabled or disabled at issuer discretion.

Req 6.9 (Offline-capable Cards)

Offline-capable cards shall support fDDA.

Req 6.10 (Transaction Logging)

Implementation-Optional: Implementation of transaction logging is at implementer discretion.

Issuer-Optional: If transaction logging is implemented, the issuer shall be able to enable and disable transaction logging.

Card applications may support transaction logging as defined in Appendix L.

Due to the increase in application processing times when transaction logging is used, it is strongly recommended that issuers not enable transaction logging.

6.2.2 Card Personalization Requirements

6.2.2.1 Card Personalization Specifications

[EMV CPS] is recommended for all contactless implementations.

[VSDC PERSO] defines the Common Personalization requirements for VCPS.

6.2.2.2 Card Personalization Requirements

This section defines some of the personalization requirements for card applications. Personalization of the card application shall conform to these requirements, but the card application need not enforce personalization requirements.

Req 6.11 (qVSDC and MSD Support)

Cards shall be personalized to support both qVSDC and MSD.

For qVSDC path processing, the following GPO responses shall be enabled:

- qVSDC Offline GPO Response (if offline implemented)
- qVSDC Online/Decline without ODA GPO Response

Enabling of the qVSDC Online with ODA GPO Response is an issuer option.

For MSD path processing, the following GPO responses shall be enabled:

- MSD CVN17 without ODA GPO Response
- MSD Legacy GPO Response

Enabling of the MSD CVN17 with ODA GPO Response is an issuer option.

For domestic-only applications, both qVSDC and MSD do not need to be personalized, and either qVSDC or MSD may be personalized. If qVSDC is personalized for a domestic-only application, then the qVSDC path shall be personalized to conduct only domestic transactions.

Req 6.12 (Application Interchange Profile)

The Application Interchange Profile (AIP) returned for the qVSDC path shall:

- Indicate MSD is not supported by card (AIP byte 2 bit 8 is 0b).
- If fDDA supported by card, then indicate ‘DDA is supported’ by card (AIP byte 1 bit 6 is 1b).

The Application Interchange Profile (AIP) returned for the MSD path shall:

- Indicate MSD is supported by card (AIP byte 2 bit 8 is 1b).

Req 6.13 (MSD Legacy Personalization)

The card MSD Legacy GPO Response shall be personalized as follows:

- dCVV shall be supported and returned in the MSD Legacy GPO Response. dCVV is performed as defined in Appendix B.
- Track 2 Equivalent Data shall be personalized with an iCVV or placeholder value (not a valid CVV), and shall be personalized with a placeholder value for the ATC.

Req 6.14 (Low Value Checks)

The card shall not be personalized to support both the Low Value Check (CAP byte 1 bit 8 is 1b) **and** the Low Value AND CTTA Check (CAP byte 1 bit 7 is 1b).

6.2.2.3 Card Personalization Options

Req 6.15 (CVV and iCVV)

The CVV present in the magnetic stripe shall not be personalized in the track data on the chip. It is recommended that the iCVV be used in the track data returned for qVSDC transactions and MSD CVN17 transactions. (MSD Legacy transactions support dCVV)

The iCVV was developed for contact chip to prevent the skimming of track data from the chip and using it to make a magnetic stripe card. Using the iCVV for track data for contactless transactions serves the same purpose.

6.3 Application Selection

Application Selection is performed immediately after activation of the contactless card, and is the process of determining which of the applications that are supported by both the card and reader will be used to conduct the transaction. This process is performed in two steps:

1. The reader builds a candidate list of mutually supported applications.
2. A single application from the candidate list is identified and selected to process the transaction.

The Application Selection procedure performed by the reader is defined in section 5.5 Application Selection.

6.3.1 SELECT Command

To facilitate Application Selection, support for the SELECT command is required.

Req 6.16 (SELECT Command)

The card shall support the SELECT command, as defined in Appendix G of this specification.

Req 6.17 (Accepting the SELECT Command)

The card shall accept a SELECT command using the AID, whether or not that command was immediately preceded by a SELECT of the PPSE.

Req 6.18 (Application Blocked)

If the selected application is blocked (application blocked or application permanently blocked), then the Status Word in response to the SELECT command shall be SW1 SW2 = '6283'.

Note: MSD and qVSDC shall be supported as contactless paths within a single card application under a single Visa AID. Paths in a card application are accessed through one Visa AID, and paths cannot be directly accessed. For dual-interface cards supporting VIS, VIS is supported in the same application under the same single Visa AID. When using the contact interface, path determination is not performed and VIS is used.

6.3.2 Proximity Payment System Environment (PPSE)

To facilitate Application Selection using the Directory Selection Method, support for the PPSE is required.

Req 6.19 (PPSE)

The card shall support the Proximity Payment System Environment (PPSE). The PPSE is a DDF with the name '2PAY.SYS.DDF01' that contains a list of the applications supported by the card over the contactless interface.

The File Control Information (FCI) in the response to the SELECT of the PPSE is defined in Appendix G.4.

Req 6.20 (PPSE Personalization)

The PPSE shall be personalized on all contactless cards using the file name ‘2PAY.SYS.DDF01’. The AIDs of the contactless financial applications on the card shall be provided in response to SELECT of the PPSE within the FCI.

Req 6.21 (PPSE Personalization – Application Priority Indicator)

If more than one contactless application is personalized on the card, then the Application Priority Indicator (tag ’87) shall be personalized in the PPSE Directory Entry (tag ‘61’) for each application.

Note: It is recommended that, whenever possible, only one application should be listed in the FCI of the PPSE in order to meet timing requirements. If more than one application is required, the number of applications should be kept to a minimum.

6.3.3 Personalization Requirements

In addition to the personalization requirements for the PPSE, this section describes (some) of the personalization requirements that may impact Application Selection processing.

Req 6.22 (AID Personalization)

The AID shall have a minimum length of 7 bytes if a single contactless application is supported.

If multiple contactless applications with the same Visa AID are supported, a minimum length of 8 bytes shall be personalized to allow for an extension to differentiate between them. For example:

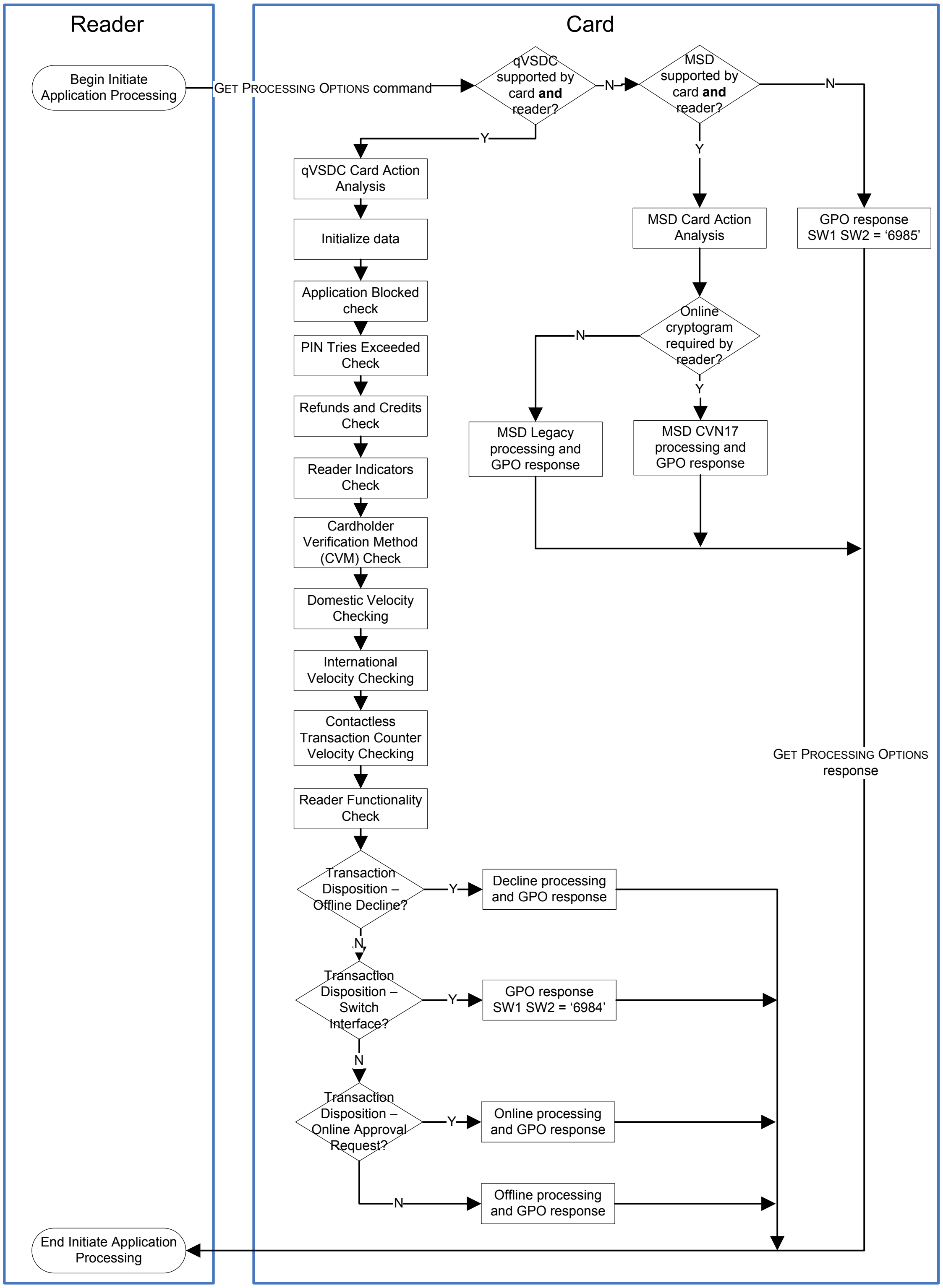
- A0 00 00 00 03 10 10 01
- A0 00 00 00 03 10 10 02

6.4 Initiate Application Processing

The card processes the GET PROCESSING OPTIONS command, determines the processing path, performs issuer risk management checks, and responds to the reader with application data to process the transaction.

Figure 6-1: Initiate Application Processing (Card) briefly outlines card application Initiate Application Processing.

Figure 6-1: Initiate Application Processing (Card)


Reader
Card
Begin Initiate Application Processing
GET PROCESSING OPTIONS command
qVSDC supported by card and reader?
N
Y
MSD supported by card and reader?
N
Y
qVSDC Card Action Analysis
Initialize data
Application Blocked check
PIN Tries Exceeded Check
Refunds and Credits Check
Reader Indicators Check
Cardholder Verification Method (CVM) Check
Domestic Velocity Checking
International Velocity Checking
Contactless Transaction Counter Velocity Checking
Reader Functionality Check
MSD Card Action Analysis
GPO response SW1 SW2 = '6985'
Online cryptogram required by reader?
N
Y
MSD Legacy processing and GPO response
MSD CVN17 processing and GPO response
GET PROCESSING OPTIONS response
Transaction Disposition – Offline Decline?
Y
N
Decline processing and GPO response
Transaction Disposition – Switch Interface?
Y
N
GPO response SW1 SW2 = '6984'
Transaction Disposition – Online Approval Request?
Y
N
Online processing and GPO response
Offline processing and GPO response
End Initiate Application Processing

6.4.1 GET PROCESSING OPTIONS (GPO) Command

Req 6.23 (GPO Command)

The card shall support the GET PROCESSING OPTIONS (GPO) command, as defined in Appendix G of this specification.

6.4.2 Processing Options Data Object List (PDOL) Requirements

qVSDC and MSD do not use the CDOLs, DDOL, or default DDOL from [EMV]. Instead, the card requests all reader-terminal data necessary for card processing in the PDOL.

The card requests the Terminal Transaction Qualifiers so that it can decide which card path (qVSDC or MSD) to use, and to determine terminal capabilities and requirements for the transaction. Additional data elements may be requested in support of cryptogram generation, fDDA signature generation, velocity checks, and transaction logging.

The PDOL for the contactless interface contains tags related to both of the paths (qVSDC and MSD), and may include tags other than those described in this specification as the minimum required. Issuers should balance the benefits of requesting additional data in the PDOL against the impact the additional data transfer and processing will have on transaction performance.

The minimum content of the PDOL required for qVSDC is dependent on the Cryptogram Version Number supported (17 or 10/18) and whether the card supports offline qVSDC transactions.

The minimum content of the PDOL required for MSD is always the same, as MSD supports Cryptogram Version Number 17 and is online-only.

The minimum content for the PDOL described in this section is shown as a function of the Cryptogram Version Number and whether or not the qVSDC path is offline capable. However, additional data may be required in the PDOL for other card processing. For example, the Terminal Country Code tag and length may be necessary in the PDOL to support velocity checks using the terminal country code.

Req 6.24 (PDOL Parsing)

The card application shall be capable of parsing the GPO command message data field to retrieve the reader data elements requested by the card in the PDOL. The reader data elements requested by the card in the PDOL are used in subsequent transaction processing.

Req 6.25 (PDOL Tags and Lengths)

In addition to the tags and lengths defined as the minimum required, the card application shall allow for the personalization of additional tags (and corresponding lengths) in the PDOL.

For example, the additional tags may be used in support of card velocity checks and transaction logging.

Additional reader-terminal data elements requested by the card application in the PDOL and not used during card processing are ignored by the card.

Note: For dual-interface cards, a different PDOL may be personalized for the contact interface, as defined in Appendix I.2.

6.4.2.2 Minimum PDOL Content

The minimum PDOL content, as a function of the Cryptogram Version Number and offline capability of the card application, is shown in the following table.

A "✓" mark indicates that the tag and length of the data element is required in the PDOL.

Table 6-1: Minimum PDOL Content

Tag	Length	Data Element Name	CVN17 Online Only	CVN17 Offline Enabled	CVN10 and CVN18
'9F66'	4 bytes	Terminal Transaction Qualifiers (TTQ)	✓	✓	✓
'9F02'	6 bytes	Amount, Authorized	✓	✓	✓
'9F03'	6 bytes	Amount, Other			✓
'9F1A'	2 bytes	Terminal Country Code			✓
'95'	5 bytes	Terminal Verification Results (TVR)			✓
'5F2A'	2 bytes	Transaction Currency Code		✓	✓
'9A'	3 bytes	Transaction Date			✓
'9C'	1 bytes	Transaction Type			✓
'9F37'	4 bytes	Unpredictable Number	✓	✓	✓

Additional tags may be personalized in the PDOL, but issuers should be aware that VCPS readers may not contain all [EMV] terminal data elements. The reader processes unknown tags according to [EMV] Data Object List processing rules.

As previously noted, there is a single PDOL per application per interface. The minimum PDOL for the contactless interface contains the tags for data that supports all application paths (qVSDC and MSD). For example, if the card application supports MSD with Cryptogram Version Number 17 and qVSDC with Cryptogram Version Number 10, the PDOL for this application would contain all of the tags required for Cryptogram Version Number 10 (the tags for Cryptogram Version Number 17 are a subset of the tags required for Cryptogram Version Number 10). The card application then parses the GPO command data to obtain the information required for its processing.

6.4.3 Contactless Transaction Hierarchy

The card shall determine the contactless path through which to process the transaction.

The order of selection for processing is governed by the requirement to use the most appropriate method supported by both the card and reader: qVSDC or MSD. qVSDC supports quick online and offline transactions. MSD is used in markets that operate under magnetic stripe rules and do not support full chip data.

Note: The concept of paths as defined for VCPS contactless applications (qVSDC and MSD) does not exist for VIS applications. For contact transactions, the paths are not evaluated and VIS is performed.

Req 6.26 (Card Contactless Path Determination)

If qVSDC is supported by the card and qVSDC is supported by the reader (TTQ byte 1 bit 6 is 1b), then the card shall proceed with qVSDC Path Processing. For all subsequent card processing with different behavior based on path, the card shall proceed with qVSDC Path Processing.

Else, if MSD is supported by the card and MSD is supported by the reader (TTQ byte 1 bit 8 is 1b), then the card shall proceed with MSD Path Processing. For all subsequent card processing with different behavior based on path, the card shall proceed with MSD Path Processing.

Else (No Matching Contactless Transaction Path), the card shall respond to the GPO command with error SW1 SW2 = '6985' (indicating that the reader should attempt to select another application).

6.4.4 Card Action Analysis – qVSDC Path Processing

The card performs qVSDC Card Action Analysis to determine its transaction disposition and responds to the GPO command accordingly. Checks and processing are performed in the order shown.

Implementations are not required to strictly follow the processing described in this section, so long as they behave in a way that is indistinguishable (seen as a black box responding to the command) from the behavior described.

The following card internal indicators are set during qVSDC Card Action Analysis based on processing and issuer risk management parameters. After completing card risk management processing checks, the internal indicators are evaluated to determine the card's transaction disposition. The card internal indicators are initialized at the start of qVSDC Card Risk Management Processing.

Transaction Disposition Indicators:

- Decline Required by Card Indicator
- Switch Interface Required by Card Indicator
- Online Required by Card Indicator

Other Indicators:

- Matching Currency Indicator
- International Transaction Indicator
- Contact Chip Supported Indicator
- Issuer Update Processing Supported Indicator
- Last Contactless Application Cryptogram Valid Indicator

6.4.4.1 qVSDC Card Risk Management Processing

The card performs qVSDC risk management checks to determine its transaction disposition.

Initialization of Data

Prior to performing qVSDC risk management checks, the card initializes the value of its internal data elements.

Note: Explicit initialization of some card internal data elements listed in this section may not be necessary, if the transient nature of those internal data elements results in their already being initialized to zero.

Req 6.27 (Initialization of Simple Internal Indicators)

The card shall:

- Reset the Decline Required by Card Indicator to 0.
- Reset the Switch Interface Required by Card Indicator to 0.
- Reset the Online Required by Card Indicator to 0.
- Reset the Last Contactless Application Cryptogram Valid Indicator to 0.

Req 6.28 (Initialization of Matching Currency Indicator)

The card compares the Transaction Currency Code with 1) the Application Currency Code, and with 2) the Conversion Currency Codes in the Currency Conversion Parameters. The transaction is a matching currency transaction if the Transaction Currency Code matches the Application Currency Code, or matches any of the Conversion Currency Codes in the Currency Conversion Parameters.

If the Transaction Currency Code matches the Application Currency Code, then the card shall set the Matching Currency Indicator to 1 and shall set the Amount, Approximated to the value of the Amount, Authorized.

Else (the Transaction Currency Code does not match the Application Currency Code), if the Transaction Currency Code matches any of the Conversion Currency Codes in the Currency Conversion Parameters, then the card shall:

- Set the Matching Currency Indicator to 1.
- The card shall calculate the (approximate) value of the transaction in the application currency using the Currency Conversion Factor associated with the matching Conversion Currency Code, and shall set the Amount, Approximated to that calculated value.

  Note: For an example of the conversion calculation, please see [VIS] section 11.4.3.9.

Else (neither of the above is true), the card shall reset the Matching Currency Indicator to 0.

Note: If the Transaction Currency Code and/or Application Currency Code are not present, then the condition evaluates to FALSE. Recall that if a card condition evaluates a data element that is not present, then the condition evaluates to FALSE. See section 3.1.6 Presence of Data Elements. This particular check is only explicitly noted to remind the reader of this convention, and it is not noted again for subsequent card application conditions and actions.

Req 6.29 (Initialization of International Transaction Indicator)

Transactions where the Transaction Currency Code does not match the Application Currency Code or any of the supported Conversion Currency Codes are international transactions. Additionally, the issuer may configure the application such that transactions where the Terminal Country Code does not match the Issuer Country Code are also international transactions.

If **either** of the following is true:

- Matching Currency Indicator is 0
- 'Include country code in determining international transactions' supported by card (CAP byte 2 bit 8 is 1b) **and** the Terminal Country Code does not match the Issuer Country Code

Then the card shall set the International Transaction Indicator to 1.

Else, the card shall reset the International Transaction Indicator to 0.

Req 6.30 (Initialization of Contact Chip Supported Indicator)

If **both** of the following are true:

- 'Card Prefers Contact Chip' supported by card (CAP byte 1 bit 2 is 1b)
- **and** EMV contact chip supported by reader (TTQ byte 1 bit 5 is 1b)

Then the card shall set the Contact Chip Supported Indicator to 1.

Else (neither of the above are true), the card shall reset the Contact Chip Supported Indicator to 0.

Req 6.31 (Initialization of Issuer Update Processing Supported Indicator)

If Issuer Update Processing supported by card (CAP byte 2 bit 5 is 1b) **and** Issuer Update Processing supported by reader (TTQ byte 3 bit 8 is 1b), then the card shall set the Issuer Update Processing Supported Indicator to 1.

Else, the card shall reset the Issuer Update Processing Supported Indicator to 0.

Req 6.32 (Initialization of Card Transaction Qualifiers)

The card shall reset CTQ byte 1 bits 8-7 to 00b (indicating Online PIN Not Required and Signature Not Required).

Req 6.33 (Initialization of Issuer Application Data)

The card shall set the CVR to '03 80 00 00' (indicating Second GENERATE AC not requested).

If the card supports Issuer Update Processing (CAP byte 2 bit 5 is 1b), then the card shall:

- Set CVR byte 3 bit 4 to the value of the Issuer Authentication Failure Indicator.
- Set CVR byte 4 bit 4 to the value of the Issuer Script Failure Indicator.
- Set CVR byte 4 bits 8-5 to the value of the Issuer Script Command Counter using identical bit settings.
- If the reader supports Issuer Update Processing (TTQ byte 3 bit 8 is 1b), then the payment application shall indicate that both the payment application and reader support Issuer Update Processing (set Issuer Discretionary Data Identifier bit 8 to 1b).

  Note: Setting of the Issuer Discretionary Data Identifier (IDD ID) is only performed if the IDD ID is personalized.

Req 6.34 (Initialization of Cryptogram Information Data)

The card shall reset the Cryptogram Information Data (CID) to '00'.

Application Blocked

Req 6.35 (Application Blocked Check)

If the application is blocked, then the card shall set the Decline Required by Card Indicator to 1.

Note: Processing of the GPO command is not performed if the application is permanently blocked. See Req 6.7 (Application Permanently Blocked).

PIN Tries Exceeded

Req 6.36 (PIN Tries Exceeded Check)

If **both** of the following are true:

- PIN Tries Exceeded Check supported by card (CAP byte 1 bit 4 is 1b)
- **and** PIN Try Counter (tag '9F17') is zero

Then the card shall:

- Set CVR byte 3 bit 7 to 1b (PIN Try Limit Exceeded).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, the card shall set the Online Required by Card Indicator to 1.

Refunds and Credits

Req 6.37 (Refunds and Credits Check)

If the Transaction Type is '2x' (Refunds/Credits), then the card shall set the Decline Required by Card Indicator to 1.

Reader Indicators

Req 6.38 (Reader Requires an Online Cryptogram Check)

If Online Cryptogram required by reader (TTQ byte 2 bit 8 is 1b), then the card shall set the Online Required by Card Indicator to 1.

Cardholder Verification Method (CVM)

The card determines if a CVM is required for the transaction. A CVM is required for the transaction if either the card or reader require a CVM.

Req 6.39 (CVM Required Check)

If **either** of the following is true:

- CVM Required by reader (TTQ byte 2 bit 7 is 1b)
- Domestic transaction (International Transaction Indicator is 0) **and** Amount, Approximated is greater than the Card CVM Limit

Then a CVM is required for the transaction, and the card shall determine the common CVM to be performed.

Req 6.40 (Determine Common CVM)

If a CVM is required for the transaction, then the card shall attempt to select a common CVM supported by both itself and the reader, as defined in this requirement. If there is more than one CVM supported by both the card and the reader, the selected CVM is chosen based on the following defined CVM hierarchy: 1) Online PIN, 2) (Contact Chip) Offline PIN, or 3) Signature.

Note: '(Contact Chip) Offline PIN' is not a CVM used for contactless transactions, but is instead used to permit issuer preference to switch to a contact chip transaction when a CVM is required.

If **both** of the following are true:

- Online PIN supported by reader (TTQ byte 1 bit 3 is 1b)
- **and either** of the following is true:
  - Domestic transaction (International Transaction Indicator is 0) **and** Online PIN supported by card for domestic transactions (CAP byte 3 bit 8 is 1b)
  - International transaction (International Transaction Indicator is 1) **and** Online PIN supported by card for international transactions (CAP byte 3 bit 7 is 1b)

Then the card shall:

- Indicate Online PIN Required (set CTQ byte 1 bit 8 to 1b).
- Set the Online Required by Card Indicator to 1.

Else, if **both** of the following are true:

- (Contact Chip) Offline PIN supported by reader (TTQ byte 2 bit 6 is 1b)
- **and** (Contact Chip) Offline PIN supported by card (CAP byte 3 bit 6 is 1b)

Then the card shall set the Switch Interface Required by Card Indicator to 1.

Else, if **both** of the following are true:

- Signature supported by reader (TTQ byte 1 bit 2 is 1b)
- **and** Signature supported by card (CAP byte 3 bit 5 is 1b)

Then the card shall indicate Signature Required (set CTQ byte 1 bit 7 to 1b)

Else (no common CVM between card and reader), the card shall set the Switch Interface Required by Card Indicator to 1.

Domestic Velocity Checking

This set of checks shall be performed for domestic transactions (International Transaction Indicator is 0) **and** Online Required by Card Indicator is 0.

Req 6.41 (Low Value Check)

This check shall be performed if the Low Value Check is supported by the card (CAP byte 1 bit 8 is 1b).

If **any** of the following is true:

- Amount, Approximated is greater than VLP Available Funds
- **or** Amount, Approximated is greater than VLP Single Transaction Limit

Then the card shall:

- Set CVR byte 3 bit 6 to 1b (Exceeded velocity checking counters).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, the card shall set the Online Required by Card Indicator to 1.

Else, if Amount, Approximated is greater than or equal to VLP Available Funds minus VLP Reset Threshold, then the card shall:

- Set CVR byte 3 bit 6 to 1b (Exceeded velocity checking counters).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, if the Issuer Update Processing Supported Indicator is 1, then the card shall set the Online Required by Card Indicator to 1.

Req 6.42 (Low Value AND CTTA Check)

This check shall be performed if the Low Value AND CTTA Check is supported by the card (CAP byte 1 bit 7 is 1b).

If **any** of the following is true:

- Amount, Approximated is greater than CTTA Funds
- **or** Amount, Approximated is greater than VLP Available Funds
- **or** Amount, Approximated is greater than VLP Single Transaction Limit

Then the card shall:

- Set CVR byte 3 bit 6 to 1b (Exceeded velocity checking counters).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, the card shall set the Online Required by Card Indicator to 1.

Else, if **any** of the following is true:

- Amount, Approximated is greater than the Cumulative Total Transaction Amount Limit (CTTAL) minus the Cumulative Total Transaction Amount (CTTA)
- **or** Amount, Approximated is greater than or equal to VLP Available Funds minus VLP Reset Threshold

Then the card shall:

- Set CVR byte 3 bit 6 to 1b (Exceeded velocity checking counters).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, if the Issuer Update Processing Supported Indicator is 1, then the card shall set the Online Required by Card Indicator to 1.

Req 6.43 (No Low Value Check Supported)

If neither of the low value checks is supported (CAP byte 1 bits 8-7 are 00b), then the card shall set the Online Required by Card Indicator to 1.

International Velocity Checking

This set of checks shall be performed for international transactions (International Transaction Indicator is 1).

Req 6.44 (International Transaction Not Allowed Check)

If international transactions are not allowed (CAP byte 2 bit 7 is 1b), then the card shall:

- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, the card shall set the Decline Required by Card Indicator to 1.

Req 6.45 (International Transaction Not Allowed Offline Check)

If offline international transactions are not allowed (CAP byte 1 bit 3 is 0b), then the card shall:

- If Online supported by reader (TTQ byte 1 bit 4 is 0b), then the card shall set the Online Required by Card Indicator to 1.

  Else, if the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, the card shall set the Decline Required by Card Indicator to 1.

Req 6.46 (Consecutive Transaction Limit International Check)

This check shall be performed for international transactions (International Transaction Indicator is 1) **and** Online Required by Card Indicator is 0.

If the Consecutive Transaction Counter International (CTCI) is greater than or equal to the Consecutive Transaction International Upper Limit (CTIUL), then the card shall:

- Set CVR byte 3 bit 6 to 1b (Exceeded velocity checking counters).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, the card shall set the Online Required by Card Indicator to 1.

Else, if the Consecutive Transaction Counter International (CTCI) is greater than or equal to the Consecutive Transaction Counter International Limit (CTCIL), then the card shall:

- Set CVR byte 3 bit 6 to 1b (Exceeded velocity checking counters).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, if the Issuer Update Processing Supported Indicator is 1, then the card shall set the Online Required by Card Indicator to 1.

Contactless Transaction Counter Velocity Checking

Req 6.47 (Contactless Transaction Count)

If the Contactless Transaction Counter (CLTC) is greater than or equal to the Contactless Transaction Counter Upper Limit (CLTCUL), then the card shall:

- Set CVR byte 3 bit 6 to 1b (Exceeded velocity checking counters).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, the card shall set the Online Required by Card Indicator to 1.

Else, if the Contactless Transaction Counter (CLTC) is greater than or equal to the Contactless Transaction Counter Lower Limit (CLTCLL), then the card shall:

- Set CVR byte 3 bit 6 to 1b (Exceeded velocity checking counters).
- If the Contact Chip Supported Indicator is 1, then the card shall set the Switch Interface Required by Card Indicator to 1.

  Else, if the Issuer Update Processing Supported Indicator is 1, then the card shall set the Online Required by Card Indicator to 1.

6.4.4.2 Reader Functionality Check

This section contains checks to determine whether the possible transaction outcome indicated by the transaction disposition indicators should be revised, based on supported reader functionality.

Offline-Only Reader

This check shall be performed if the Reader is Offline-Only (TTQ byte 1 bit 4 is 1b).

Req 6.48 (Decline if Online Required Check)

If the Online Required by Card Indicator is 1, then the card shall set the Decline Required by Card Indicator to 1.

6.4.4.3 Transaction Disposition

At the completion of qVSDC risk management processing checks, the card shall examine its internal indicators to determine the transaction disposition. The hierarchy of transaction dispositions is shown in sequence below, and the card transaction disposition shall be the first transaction disposition where the corresponding indicator is set.

Transaction Disposition – (Offline) Decline

The card shall perform the following processing if the Decline Required by Card Indicator is 1.

Req 6.49 (Decline)

The card shall:

- Indicate Application Authentication Cryptogram (AAC) returned (set CVR byte 2 bits 6-5 to 00b and set CID bits 8-7 to 00b).
- Increment the Application Transaction Counter (ATC) by one. The ATC shall be incremented prior to the performance of any cryptographic operations.

  If incrementing the ATC results in the ATC reaching its maximum value, then the application shall be permanently blocked, Req 6.7 (Application Permanently Blocked), and shall respond to the GPO command with error SW1 SW2 = '6985'.
- If ATC Insertion Option supported, then the card shall perform ATC insertion (as described in Appendix B.2 ATC Insertion Option).
- Construct the Issuer Application Data. If an Issuer Discretionary Data Option Identifier (IDDO ID) is supported (see Appendix E), the IDD shall be constructed and the MAC generated (if applicable).
- Generate the AAC type Application Cryptogram and set the Last Contactless Application Cryptogram to the value of the generated Application Cryptogram.
- Set the Last Contactless Application Cryptogram Valid Indicator to 1.
- Construct and send the GPO response in [EMV] Format 2 with the data shown in Table 6-2 using Condition column "Online and Decline (without ODA)".

Transaction Disposition – Switch Interface

The card shall perform the following processing if the Switch Interface Required by Card Indicator is 1.

Req 6.50 (Switch Interface)

The card shall respond to the GPO command with error SW1 SW2 = '6984' (indicating that the reader should switch to another interface).

Transaction Disposition – Online (Approval Request)

The card shall perform the following processing if the Online Required by Card Indicator is 1.

Although Req 6.51 (Tearing Protection - Online Approval Request) involves processing for the READ RECORD command, it is presented here as it may have significant impact to processing of the GPO command for online requested transactions. If the Application File Locator is returned, card and reader communications for online requested transactions are not complete until the last record has been read, thus the data elements updated in this section shall not be committed until the last record has been read. As a consequence, there exists the possibility for transaction tearing even after the GPO response has been sent. The Tearing Protection requirement in this section attempts to minimize the impact of tearing by not committing updated card data elements until the final READ RECORD response is sent.

Req 6.51 (Tearing Protection - Online Approval Request)

The card shall not commit the data elements updated in this section (Transaction Disposition – Online Approval Request) to persistent memory until immediately prior to sending the READ RECORD response for the last record, with the exception of the Application Transaction Counter (as increment of the ATC is effectively immediately). The last record is indicated by the Application File Locator.

If updated data elements have not been committed to persistent memory, then the transient value of these data elements shall be discarded if the card receives another GPO command or the contactless communication session ends (e.g. the card loses power).

Note: When a data element value is returned in the Issuer Application Data (due to an Issuer Discretionary Data Option), the (updated) transient value is used.

Req 6.52 (Contactless Transaction Counter Updates)

If ‘Count qVSDC online transactions’ is supported by card (CAP byte 1 bit 6 is 1b), then the card shall increment the Contactless Transaction Counter (CLTC) by one.

Req 6.53 (Online)

The card shall:

- Indicate Authorization Request Cryptogram (ARQC) returned (set CVR byte 2 bits 6-5 to 10b and set CID bits 8-7 to 10b).
- Increment the Application Transaction Counter (ATC) by one. The ATC shall be incremented prior to the performance of any cryptographic operations.

  If incrementing the ATC results in the ATC reaching its maximum value, then the application shall be permanently blocked, Req 6.7 (Application Permanently Blocked), and shall respond to the GPO command with error SW1 SW2 = '6985'.

- If ATC Insertion Option supported, then the card shall perform ATC insertion (as described in Appendix B.2 ATC Insertion Option).
- Construct the Issuer Application Data. If an Issuer Discretionary Data Option Identifier (IDDO ID) is supported (see Appendix E), the IDD shall be constructed and the MAC generated (if applicable).
- If the card is capable of performing fDDA **and all** of the following are true:
  - the card supports fDDA for Online Authorizations (AIP byte 1 bit 6 is 1b for the qVSDC "Online (with ODA)" GPO response)
  - **and** ODA for Online Authorizations supported by card (CAP byte 2 bit 6 is 0b)
  - **and** ODA for Online Authorizations supported by reader (TTQ byte 1 bit 1 is 1b)

  Then the card shall construct the Card Authentication Related Data and generate the Signed Dynamic Application Data (tag '9F4B'). The Signed Dynamic Application Data shall be generated as defined in Appendix A.

  Note: ODA for Online Authorizations is neither used at nor supported by readers compliant to this specification. However, card functionality is included in this specification to allow for its potential use in acceptance environments where ODA for Online Authorizations is desired.
- Generate the ARQC type Application Cryptogram and set the Last Contactless Application Cryptogram to the value of the generated Application Cryptogram.
- Set the Last Contactless Application Cryptogram Valid Indicator to 1.
- If ODA for Online Authorizations supported by reader (TTQ byte 1 bit 1 is 1b), then construct and send the GPO response in [EMV] Format 2 with the data shown in Table 6-2 using Condition column "Online (with ODA)".

  Else (TTQ byte 1 bit 1 is 0b), construct and send the GPO response in [EMV] Format 2 with the data shown in Table 6-2 using Condition column "Online and Decline (without ODA)".

Transaction Disposition – Offline (Approval Request)

If none of the transaction disposition indicators above indicate that another transaction disposition is required, the card shall request offline approval processing.

Although Req 6.54 (Tearing Protection - Offline Approval Request) involves processing for the READ RECORD command, it is presented here as it has significant impact to processing of the GPO command for offline requested transactions. Card and reader communications for offline requested transactions are not complete until the last record has been read, thus the data elements updated in this section shall not be committed until the last record has been read. As a consequence, there exists the possibility for transaction tearing even after the GPO response has been sent. The Tearing Protection requirement in this section attempts to minimize the impact of tearing by not committing updated card data elements until the final READ RECORD response is sent.

Req 6.54 (Tearing Protection - Offline Approval Request)

The card shall not commit the data elements updated in this section (Transaction Disposition – Offline Approval Request) to persistent memory until immediately prior to sending the READ RECORD response for the last record, with the exception of the Application Transaction Counter (as increment of the ATC is effectively immediately). The last record is indicated by the Application File Locator.

If updated data elements have not been committed to persistent memory, then the transient value of these data elements shall be discarded if the card receives another GPO command or the contactless communication session ends (e.g. the card loses power).

Note: When a data element value is returned in the Issuer Application Data (due to an Issuer Discretionary Data Option), the (updated) transient value is used.

Req 6.55 (Low Value Counter Updates)

If **both** of the following are true:

- International Transaction Indicator is 0
- **and** Low Value Check supported by card (CAP byte 1 bit 8 is 1b)

Then the card shall decrement the VLP Available Funds by the Amount, Approximated.

Req 6.56 (Low Value AND CTTA Counter Updates)

If **both** of the following are true:

- International Transaction Indicator is 0
- **and** Low Value AND CTTA Check supported by card (CAP byte 1 bit 7 is 1b)

Then the card shall:

- Increment the Cumulative Total Transaction Amount (CTTA) by the Amount, Approximated.
- Decrement the VLP Available Funds by the Amount, Approximated.

Req 6.57 (Consecutive Transaction Counter International Counter Update)

If the International Transaction Indicator is 1, then the card shall increment the Consecutive Transaction Counter International (CTCI) by one.

Req 6.58 (Contactless Transaction Counter Update)

The card shall increment the Contactless Transaction Counter (CLTC) by one.

Req 6.59 (Offline)

The card shall:

- Indicate Transaction Certificate (TC) returned (set CVR byte 2 bits 6-5 to 01b and set CID bits 8-7 to 01b).
- Increment the Application Transaction Counter (ATC) by one. The ATC shall be incremented prior to the performance of any cryptographic operations.

  If incrementing the ATC results in the ATC reaching its maximum value, then the application shall be permanently blocked, Req 6.7 (Application Permanently Blocked), and shall respond to the GPO command with error SW1 SW2 = '6985'.
- If ATC Insertion Option supported, then the card shall perform ATC insertion (as described in Appendix B.2 ATC Insertion Option).
- Construct the Issuer Application Data. If an Issuer Discretionary Data Option Identifier (IDDO ID) is supported (see Appendix E), the IDD shall be constructed and the MAC generated (if applicable).
- Construct the Card Authentication Related Data and generate the Signed Dynamic Application Data (tag '9F4B'). The Signed Dynamic Application Data shall be generated as defined in Appendix A.
- Generate the TC type Application Cryptogram and set the Last Contactless Application Cryptogram to the value of the generated Application Cryptogram.
- Set the Last Contactless Application Cryptogram Valid Indicator to 1.
- Construct and send the GPO response in [EMV] Format 2 with the data shown in Table 6-2 using Condition column "Offline (with ODA)".

6.4.4.4 qVSDC Path Processing GPO Response

This section describes the qVSDC GPO Response data.

A number of the data elements shown in the qVSDC GPO response may be returned in either the GPO response or in a record, at issuer discretion. For the purposes of reduced transaction times, it is recommended that these data elements be returned in the GPO response unless they are part of the static data to be signed. However, if there is insufficient space in the GPO response to return all the data elements, then it will be necessary to return some of the data elements in records.

Additional application data may be returned in records, as personalized by the issuer.

Note: Readers compliant to this specification do not perform Offline Data Authentication (ODA) for qVSDC transaction disposition Online and Decline, hence record data is not needed to complete the transaction.

Table 6-2: qVSDC GPO Response Data

Tag	Data Element		Length	Condition		
				Online (with ODA)	**Online and Decline (without ODA)**	**Offline (with ODA)**
'77'	Response Message Template Format 2		var.			
	'82'	Application Interchange Profile (AIP)	2 bytes	Always	Always	Always
	'94'	Application File Locator (AFL)	var.	Always	If returning record data	Always
	'57'	Track 2 Equivalent Data	var. up to 19 bytes	Shall be returned in either the GPO response or in a record.	Always	Shall be returned in either the GPO response or in a record.
	'5F20'	Cardholder Name	var. 2- 26 bytes	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.

Tag	Data Element		Length	Condition		
				Online (with ODA)	**Online and Decline (without ODA)**	**Offline (with ODA)**
	'5F34'	Application PAN Sequence Number (PSN)	1 byte	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.
	'9F10'	Issuer Application Data (IAD)	var. up to 32 bytes	Always	Always	Always
	'9F26'	Application Cryptogram	8 bytes	Always	Always	Always
	'9F27'	Cryptogram Information Data (CID)	1 byte	Always	Always	Always
	'9F36'	Application Transaction Counter (ATC)	2 bytes	Always	Always	Always
	'9F4B'	Signed Dynamic Application Data (SDAD)	N_{IC} bytes	If the SDAD is generated by the application, then it shall be returned in either the GPO response or in a record.	Never	If the SDAD is generated by the application, then it shall be returned in either the GPO response or in a record.
	'9F5D'	Available Offline Spending Amount (AOSA)	6 bytes	The AOSA shall be returned in the GPO response if all of the following are true: • Return AOSA supported by card (CAP byte 1 bit 1 is 1b) • **and** the AOSA was personalized with a value of '01' • **and** the Transaction Currency Code matches the Application Currency Code		
	'9F6C'	Card Transaction Qualifiers (CTQ)	2 bytes	If using CTQ functionality	If using CTQ functionality	If using CTQ functionality
	'9F6E'	Form Factor Indicator (FFI)	4 bytes	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.
	'9F7C'	Customer Exclusive Data (CED)	var. up to 32 bytes	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.

6.4.5 Card Action Analysis – MSD Path Processing

The MSD path transaction disposition always requests online processing (except when the application is blocked). As a consequence, additional checks are not required to determine the transaction disposition and the MSD path can simply respond to the GPO command.

6.4.5.1 MSD CVN17 and MSD Legacy

MSD path processing may return track data with an Application Cryptogram, or it may return track data only. These two "types" of MSD responses are categorized as follows:

- MSD Cryptogram Version Number 17 (MSD CVN17) = MSD transaction with track data and with an Application Cryptogram
- MSD Legacy = MSD transaction with track data and without an Application Cryptogram. This is referred to as "MSD Legacy" because it is the MSD response defined in [VCPS 1 4 2]. The MSD Legacy response is included in this specification to allow for backwards compatibility at readers compliant to [VCPS 1 4 2].

Req 6.60 (MSD CVN17 and MSD Legacy Determination)

If Online Cryptogram Required by reader (TTQ byte 2 bit 8 is 1b), then the card shall proceed with MSD CVN17 Processing.

Else (Online Cryptogram Not Required by reader), the card shall proceed with MSD Legacy Processing.

6.4.5.2 MSD Cryptogram Version Number 17 (MSD CVN17) Processing

Req 6.61 (MSD CVN17 Processing)

The card shall:

- Set the CVR to '03 A0 00 00' (indicating ARQC returned).
- If the application is blocked, then the card shall indicate Application Authentication Cryptogram (AAC) returned (set CVR byte 2 bits 6-5 to 00b).
- Increment the Application Transaction Counter (ATC) by one. The ATC shall be incremented prior to the performance of any cryptographic operations.

  If incrementing the ATC results in the ATC reaching its maximum value, then the application shall be permanently blocked, Req 6.7 (Application Permanently Blocked), and shall respond to the GPO command with error SW1 SW2 = '6985'.
- If ATC Insertion Option supported, then the card shall perform ATC insertion (as described in Appendix B.2 ATC Insertion Option).
- Construct the Issuer Application Data. If an Issuer Discretionary Data Option Identifier (IDDO ID) is supported (see Appendix E), the IDD shall be constructed and the MAC generated (if applicable).

- If the card is capable of performing fDDA **and all** of the following are true:
  - the card supports fDDA for Online Authorizations (AIP byte 1 bit 6 is 1b for the MSD CVN17 "Online (with ODA)" GPO response)
  - **and** ODA for Online Authorizations supported by card (CAP byte 2 bit 6 is 0b)
  - **and** ODA for Online Authorizations supported by reader (TTQ byte 1 bit 1 is 1b)

  Then the card shall construct the Card Authentication Related Data and generate the Signed Dynamic Application Data (tag '9F4B'). The Signed Dynamic Application Data shall be generated as defined in Appendix A.

  Note: ODA for Online Authorizations is neither used at nor supported by readers compliant to this specification. However, card functionality is included in this specification to allow for its potential use in acceptance environments where ODA for Online Authorizations is desired.

- Generate the Application Cryptogram and set the Last Contactless Application Cryptogram to the value of the generated Application Cryptogram. The Cryptogram Version Number 17 algorithm shall be used to generate the Application Cryptogram (see Appendix C).

- Set the Last Contactless Application Cryptogram Valid Indicator to 1.

- If ODA for Online Authorizations supported by reader (TTQ byte 1 bit 1 is 1b), then construct and send the GPO response in [EMV] Format 2 with the data shown in Table 6-3 using Condition column "Online (with ODA)".

  Else (TTQ byte 1 bit 1 is 0b), construct and send the GPO response in [EMV] Format 2 with the data shown in Table 6-3 using Condition column "Online (without ODA)".

6.4.5.3 MSD Legacy Processing

Req 6.62 (MSD Legacy Processing)

The card shall:

- Increment the Application Transaction Counter (ATC) by one. The ATC shall be incremented prior to the performance of any cryptographic operations.

  If incrementing the ATC results in the ATC reaching its maximum value, then the application shall be permanently blocked, Req 6.7 (Application Permanently Blocked), and shall respond to the GPO command with error SW1 SW2 = '6985'.

- Set the Last Contactless Application Cryptogram Valid Indicator to 0.
- If dCVV is supported (MSD Offset is personalized with a value greater than zero), then the card shall generate the dCVV and place it, along with the ATC, in Track 2 Equivalent Data (as described in Appendix B Dynamic CVV (dCVV)).
- Construct and send the GPO response in [EMV] Format 1, returning the Application Interchange Profile (AIP, tag '82') and the Application File Locator (AFL, tag '94'). See Table 6-4.

6.4.5.4 MSD Path Processing GPO Response

MSD CVN17 GPO Response Data

For MSD CVN17 Processing, the GPO response data is shown in Table 6-3: MSD CVN17 GPO Response Data.

A number of the data elements shown in the MSD CVN17 GPO response may be returned in either the GPO response or in a record, at issuer discretion. For the purposes of reduced transaction times, it is recommended that these data elements be returned in the GPO response unless they are part of the static data to be signed. However, if there is insufficient space in the GPO response to return all the data elements, then it will be necessary to return some of the data elements in records.

Additional application data may be returned in records, as personalized by the issuer.

Note: Readers compliant to this specification do not perform Offline Data Authentication (ODA) for MSD transactions, hence record data is not needed to complete the transaction.

Table 6-3: MSD CVN17 GPO Response Data

Tag	Data Element		Length	Condition	
				Online (with ODA)	**Online (without ODA)**
'77'	Response Message Template Format 2		var.		
	'82'	Application Interchange Profile (AIP)	2 bytes	Always	Always
	'94'	Application File Locator (AFL)	var.	Always	If returning record data
	'57'	Track 2 Equivalent Data	var. up to 19 bytes	Shall be returned in either the GPO response or in a record.	Always
	'5F20'	Cardholder Name	var. 2- 26 bytes	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.

Tag	Data Element		Length	Condition	
				Online (with ODA)	**Online (without ODA)**
	'5F34'	Application PAN Sequence Number (PSN)	1 byte	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.
	'9F10'	Issuer Application Data (IAD)	var. up to 32 bytes	Always	Always
	'9F1F'	Track 1 Discretionary Data	var.	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.
	'9F26'	Application Cryptogram	8 bytes	Always	Always
	'9F36'	Application Transaction Counter (ATC)	2 bytes	Always	Always
	'9F4B'	Signed Dynamic Application Data (SDAD)	N_{IC} bytes	If the SDAD is generated by the application, then it shall be returned in either the GPO response or in a record.	Never
	'9F6C'	Card Transaction Qualifiers (CTQ)	2 bytes	If using CTQ functionality	Never
	'9F6E'	Form Factor Indicator (FFI)	4 bytes	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.
	'9F7C'	Customer Exclusive Data (CED)	var. up to 32 bytes	May be returned in either the GPO response or in a record.	May be returned in either the GPO response or in a record.

MSD Legacy GPO Response Data

For MSD Legacy Processing, the GPO response data is the [EMV] Format 1 GPO response data. The lengths shown below for the AIP and AFL are provided as supplemental information, and are not part of the response data field.

Table 6-4: MSD Legacy GPO Response Data

Tag	Data Element	Length	Condition
'80'	Response Message Template Format 1	var.	
	Application Interchange Profile (AIP)	2 bytes	Always
	Application File Locator (AFL)	var.	Always Track 2 Equivalent Data (tag '57') shall be returned in a record. Track 1 Discretionary Data (tag '9F1F') and Cardholder Name (tag '5F20') may be returned in a record at issuer discretion. No additional card application data is used for MSD Legacy transactions.

6.5 Read Application Data

During Read Application Data, the reader uses the READ RECORD command to retrieve the card data necessary to process the transaction. The card receives the READ RECORD command from the reader and returns the requested record.

6.5.1 READ RECORD Command

To facilitate Read Application Data, support for the READ RECORD command is required.

Req 6.63 (READ RECORD Command)

The card shall support the READ RECORD command, as defined in Appendix G of this specification.

The card shall support the personalization and return of the Card Authentication Related Data (tag '9F69') and Signed Dynamic Application Data (tag '9F4B') in records, as personalized by the issuer. Unlike the other data elements normally returned in records, the value of these data elements are conditionally generated by the card application for each transaction.

Req 6.64 (Last Record)

The card shall be capable of knowing when the last record is read. The last record is indicated by the Application File Locator (AFL).

For transactions where fDDA is performed, the Card Authentication Related Data (tag '9F69') shall be generated and present in the last record, prior to responding to the READ RECORD command for the last record.

The Card Authentication Related Data contains the (card) Unpredictable Number, generated by the card prior to generation of the Signed Dynamic Application Data.

Note: The card will not know whether the reader successfully received the final READ RECORD response. This means that tearing is still possible and if it occurs, it will negatively affect the available offline balance. The time window for such an occurrence has been minimized. The reader may still decline the transaction if the expiration date or offline data authentication checks fail, but this should rarely occur for genuine cards.

Req 6.65 (Last Record - Commit Data Elements and Indicators)

The card application shall commit the data elements updated in section 6.4.4.3 to persistent memory immediately prior to sending the READ RECORD response for the last record.

6.6 Issuer Update Processing

Implementation-Optional: Issuer Update Processing is an implementation option.

Issuer-Optional: If implemented, support for Issuer Update Processing is issuer optional. Card support for Issuer Update Processing is enabled by setting CAP byte 2 bit 5 to 1b. 'Card supports Issuer Update Processing at the POS' is indicated in CTQ byte 2 bit 7.

Note: As there is no GPO command issued during Issuer Update Processing, the Authorization Response Cryptogram (ARC) and issuer script MAC(s) are generated by the issuer using the ATC returned during Initiate Application Processing (and sent in the online message).

6.6.1 Issuer Update Commands

If the card application supports Issuer Update Processing, support for the Issuer Update commands is required:

Req 6.66 (Issuer Update Commands)

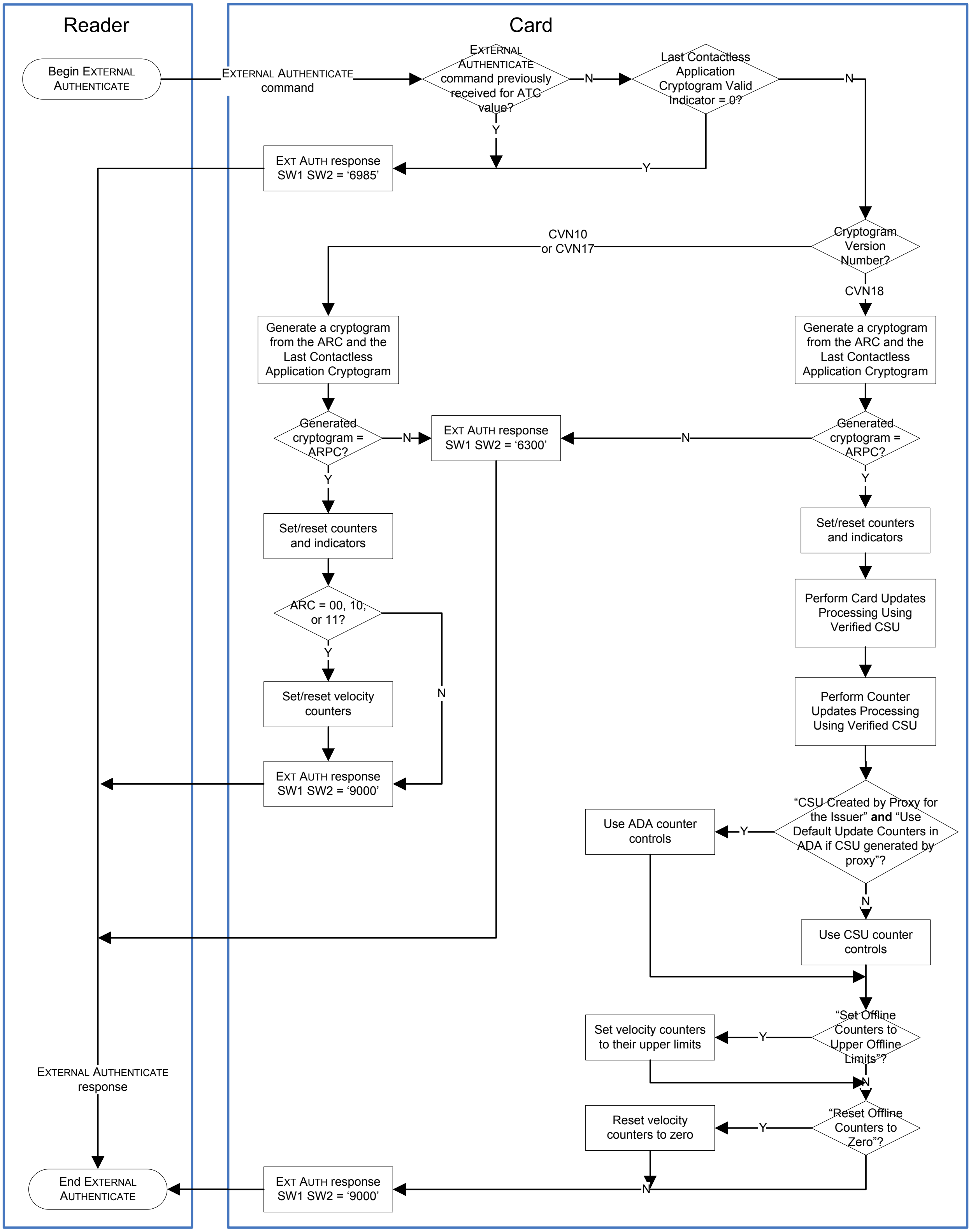
The card shall support the Issuer Update commands, as defined in Appendix G.5 of this specification.

6.6.2 Issuer Authentication Processing

Upon receipt of the EXTERNAL AUTHENTICATE command, the card shall process the command according to the procedure defined in this section.

Figure 6-2: External Authenticate Processing (Card) briefly outlines card application Issuer Authentication processing when the EXTERNAL AUTHENTICATE command is received.

Figure 6-2: External Authenticate Processing (Card)


Reader
Card
Begin External Authenticate
External Authenticate command
External Authenticate command previously received for ATC value?
N
Y
Last Contactless Application Cryptogram Valid Indicator = 0?
N
Y
Ext Auth response SW1 SW2 = '6985'
Cryptogram Version Number?
CVN10 or CVN17
CVN18
Generate a cryptogram from the ARC and the Last Contactless Application Cryptogram
Generate a cryptogram from the ARC and the Last Contactless Application Cryptogram
Generated cryptogram = ARPC?
N
Y
Ext Auth response SW1 SW2 = '6300'
Generated cryptogram = ARPC?
N
Y
Set/reset counters and indicators
Set/reset counters and indicators
ARC = 00, 10, or 11?
Y
N
Set/reset velocity counters
Ext Auth response SW1 SW2 = '9000'
Perform Card Updates Processing Using Verified CSU
Perform Counter Updates Processing Using Verified CSU
"CSU Created by Proxy for the Issuer" and "Use Default Update Counters in ADA if CSU generated by proxy"?
Y
N
Use ADA counter controls
Use CSU counter controls
"Set Offline Counters to Upper Offline Limits"?
Y
N
Set velocity counters to their upper limits
"Reset Offline Counters to Zero"?
Y
N
Reset velocity counters to zero
External Authenticate response
End External Authenticate
Ext Auth response SW1 SW2 = '9000'

6.6.2.1 EXTERNAL AUTHENTICATE Conditions

To determine whether processing of the EXTERNAL AUTHENTICATE command should be performed, the card determines if an EXTERNAL AUTHENTICATE command was previously received for the transaction, and examines the Last Contactless Application Cryptogram Valid Indicator.

Req 6.67 (One EXTERNAL AUTHENTICATE Command Per ATC Value)

The card shall permit at most one EXTERNAL AUTHENTICATE command per ATC value. If an EXTERNAL AUTHENTICATE command was previously received for the ATC value, then the card shall:

- Set the Issuer Authentication Failure Indicator to 1.
- Discontinue processing the command and respond with SW1 SW2 = '6985'.

Req 6.68 (Last Contactless Application Cryptogram Valid Indicator)

If the Last Contactless Application Cryptogram Valid Indicator is 0, then the card shall:

- Set the Issuer Authentication Failure Indicator to 1.
- Discontinue processing the command and respond with SW1 SW2 = '6985'.

6.6.2.2 Cryptogram Version Number 10 and Cryptogram Version Number 17

The card shall perform the procedure specified in this section for Cryptogram Version Number 10 and Cryptogram Version Number 17.

Req 6.69 (EXTERNAL AUTHENTICATE Processing: CVN 10 and CVN 17)

The card shall process the EXTERNAL AUTHENTICATE command and issue the response according to [VIS] section 12.4.3, with the following exception(s):

- The Last Contactless Application Cryptogram shall be used instead of the “ARQC returned in the first GENERATE AC response...”

Req 6.70 (Issuer Authentication Counter and Indicator Resets)

Prior to responding to the EXTERNAL AUTHENTICATE command, the card application shall determine whether the following counters and indicators are to be updated.

If Issuer Authentication is successfully performed, then the card application shall update the following counters and indicators:

- Issuer Authentication Failure Indicator to 0.
- If 'Issuer Script Command Counter is cyclic' (ADA byte 3 bit 2) is 0b, then the card shall reset the Issuer Script Command Counter to zero.
- Issuer Script Failure Indicator to 0.
- Last Successful Issuer Update ATC Register to the value of the ATC.

Req 6.71 (Approval Counter and Indicator Resets)

Prior to responding to the EXTERNAL AUTHENTICATE command, the card application shall determine whether the following counters and indicators are reset.

If **both** of the following are true:

- Issuer Authentication is successfully performed
- **and** Authorization Response Code is 00, 10, or 11 (Issuer approval)

Then the card shall update the following indicators and counters:

- Last Online ATC Register to the value of the ATC.
- If 'Do not reset VLP Available Funds during Issuer Authentication Processing' (ADA byte 2 bit 1) is 0b, then the card shall set the VLP Available Funds to the VLP Funds Limit.
- If 'Do not reset CTTA during Issuer Authentication Processing' (ADA byte 2 bit 2) is 0b, then the card shall reset the Cumulative Total Transaction Amount (CTTA) to zero.
- Consecutive Transaction Counter (CTC) to zero.
- Consecutive Transaction Counter International (CTCI) to zero.
- Contactless Transaction Counter (CLTC) to zero.

6.6.2.3 Cryptogram Version Number 18

Implementation-Conditional: This functionality shall be implemented if support for Cryptogram Version Number 18 is implemented.

The card shall perform the procedure specified in this section for Cryptogram Version Number 18.

Req 6.72 (Generate ARPC)

The card shall:

- Parse out the Authorization Response Cryptogram (ARPC) included in the Issuer Authentication Data for support of Cryptogram Version Number 18 ('12').
- Generate an ARPC from the following input data using the ARPC algorithm and session key derivation method described in the CCD Part of [EMV] Book 2 section 8.1, for a cryptogram defined by the Common Core Definitions (CCD) with a Cryptogram Version of ‘5’:
  - CSU received in the EXTERNAL AUTHENTICATE command data
  - Last Contactless Application Cryptogram
  - If the ‘Proprietary Authentication Data included’ bit of the CSU is 1b, then also include the Proprietary Authentication Data received in the EXTERNAL AUTHENTICATE command

Req 6.73 (Issuer Authentication Results)

Compare the generated ARPC to the ARPC received in the Issuer Authentication Data of the EXTERNAL AUTHENTICATE command.

If the generated ARPC and the ARPC received in the EXTERNAL AUTHENTICATE command data are the same, then Issuer Authentication is considered successful and the card shall:

- Set the Issuer Authentication Failure Indicator to 0.
- If ‘Issuer Script Command Counter is cyclic’ (ADA byte 3 bit 2) is 0b, then the card shall reset the Issuer Script Command Counter to zero.
- Set the Issuer Script Failure Indicator to 0.
- Set the Last Online ATC Register to the value of the ATC.
- Set the Last Successful Issuer Update ATC Register to the value of the ATC
- Continue processing the command.

Else (Issuer Authentication unsuccessful), the card shall:

- Set the Issuer Authentication Failure Indicator to 1.
- Set the ‘Issuer Authentication performed and failed’ bit of the CVR to 1b.
- Indicate that Issuer Authentication failed by responding to the EXTERNAL AUTHENTICATE command with SW1 SW2 = '6300'.

Req 6.74 (CSU Processing)

After successful Issuer Authentication for Cryptogram Version Number 18, the card has verified that the CSU received in Issuer Authentication Data is valid.

The indicators in the CSU are used to update the card as follows:

- If Card Block indicated (CSU byte 2 bit 7 is 1b), then the card shall be blocked as described in Appendix G.5.3.
- If Application Block indicated (CSU byte 2 bit 6 is 1b), then the application shall be blocked as described in Appendix G.5.1.
- If Update PIN Try Counter indicated (CSU byte 2 bit 5 is 1b), then the card shall set the PIN Try Counter to the value contained in the 'PIN Try Counter' bits of the verified CSU (CSU byte 1 bits 4-1).

  The card shall not set the PIN Try Counter to a value greater than the PIN Try Limit. If the value contained in the 'PIN Try Counter' bits of the verified CSU is greater than the value of the PIN Try Limit, then the card shall set the PIN Try Counter to the value of the PIN Try Limit.
- If 'Set Go Online On Next Transaction' indicated (CSU byte 2 bit 4 is 1b), then the card shall set the Go Online On Next Transaction Indicator to 1.

  Else (CSU byte 2 bit 4 is 0b), the card shall set the Go Online On Next Transaction Indicator to 0.

Req 6.75 (CSU and ADA Counter Controls)

The card examines the 'CSU Created by Proxy for the Issuer' bit in the CSU and the 'Use Default Update Counters in ADA if CSU is generated by a proxy' in the Application Default Action (ADA) to determine which of the data elements are used to control the update of counters.

If 'CSU Created by Proxy for the Issuer' (CSU byte 2 bit 3 is 1b) **and** 'Use Default Update Counters in ADA if CSU is generated by a proxy' (ADA byte 4 bit 8 is 1b), then the card shall update the counters according to the ADA Default Update Counters (the "counter control" is ADA byte 4 bits 7-6).

Else, the card shall update the counters according to the CSU Update Counters (the "counter control" is CSU byte 2 bits 2-1).

Req 6.76 (Update Counters)

The card examines the appropriate counter control to determine whether counters and indicators should be updated, and how they're to be updated.

If 'Set velocity-checking counters to Upper Limits' indicated (counter control has the value 01b), then the card shall update the counters to the value of the associated upper limit as follows:

- If 'Do not reset VLP Available Funds during Issuer Authentication Processing' (ADA byte 2 bit 1) is 0b, then the card shall reset the VLP Available Funds to zero.
- If 'Do not reset CTTA during Issuer Authentication Processing' (ADA byte 2 bit 2) is 0b, then the card shall set the Cumulative Total Transaction Amount (CTTA) to the Cumulative Total Transaction Amount Upper Limit (CTTAUL).
- Consecutive Transaction Counter (CTC) to Consecutive Transaction Counter Upper Limit (CTCUL).
- Consecutive Transaction Counter International (CTCI) to Consecutive Transaction International Upper Limit (CTIUL).
- Contactless Transaction Counter (CLTC) to Contactless Transaction Counter Upper Limit (CLTCUL).

If 'Reset velocity-checking counters to zero' indicated (counter control has the value 10b), then the card shall update the counters to the value of the associated upper limit as follows:

- If 'Do not reset VLP Available Funds during Issuer Authentication Processing' (ADA byte 2 bit 1) is 0b, then the card shall set the VLP Available Funds to the VLP Funds Limit.
- If 'Do not reset CTTA during Issuer Authentication Processing' (ADA byte 2 bit 2) is 0b, then the card shall reset Cumulative Total Transaction Amount (CTTA) to zero.
- Consecutive Transaction Counter (CTC) to zero.
- Consecutive Transaction Counter International (CTCI) to zero.
- Contactless Transaction Counter (CLTC) to zero.

Note: The 'Add transaction to velocity-checking counters' counter control is not supported for Issuer Update Processing. The transaction parameters necessary to determine the appropriate counters to update may not be known by the card during Issuer Update Processing.

Req 6.77 (Issuer Authentication Successful)

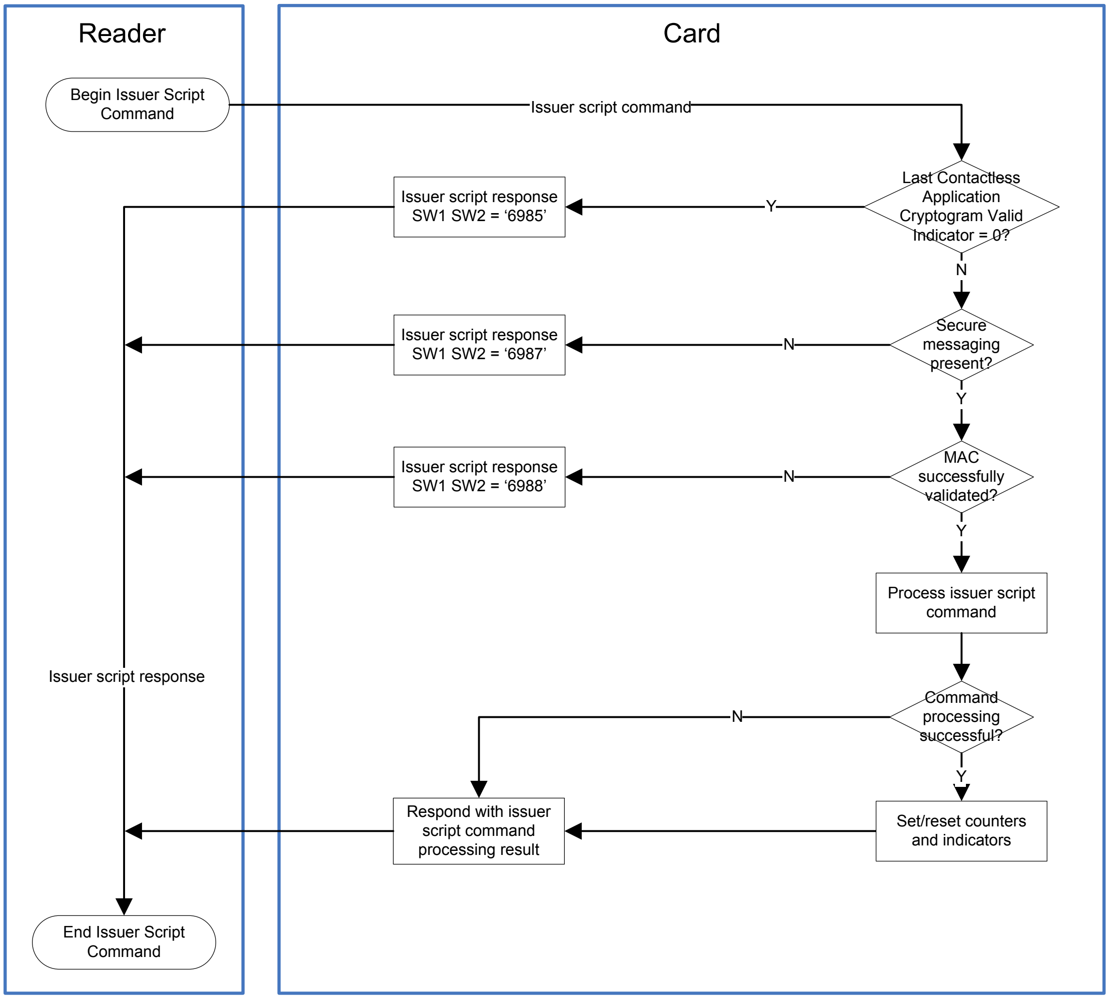
After Issuer Authentication has been successfully completed and CSU processing performed, the card shall indicate that Issuer Authentication was successful by responding to the EXTERNAL AUTHENTICATE command with SW1 SW2 = '9000'.

6.6.3 Issuer Script Processing

Issuer script commands are processed by the card application as defined in this section.

Figure 6-3: Issuer Script Command Processing (Card) briefly outlines card application issuer script processing when an issuer script command is received.

Figure 6-3: Issuer Script Command Processing (Card)


Reader
Card
Begin Issuer Script Command
Issuer script command
Last Contactless Application Cryptogram Valid Indicator = 0?
Y
Issuer script response SW1 SW2 = '6985'
N
Secure messaging present?
N
Issuer script response SW1 SW2 = '6987'
Y
MAC successfully validated?
N
Issuer script response SW1 SW2 = '6988'
Y
Process issuer script command
Command processing successful?
N
Y
Set/reset counters and indicators
Respond with issuer script command processing result
Issuer script response
End Issuer Script Command

Upon receipt of an issuer script command, the card shall process the command according to the procedure shown below.

Req 6.78 (Last Contactless Application Cryptogram Valid Indicator)

If the Last Contactless Application Cryptogram Valid Indicator is 0, then the card shall:

- Set the Issuer Script Failure Indicator to 1.
- Discontinue processing the command and respond with SW1 SW2 = '6985'.

Req 6.79 (MAC Verification)

The card shall perform secure messaging and validate the MAC sent in the secure message, as defined in Appendix G.6.

If MAC validation is successful, then the card shall perform the issuer script command.

Else (an error occurred during validation of the MAC), the card shall:

- Set the Last Contactless Application Cryptogram Valid Indicator to 0.
- Set the Issuer Script Failure Indicator to 1.
- Discontinue processing the command and respond as follows:
  - SW1 SW2 = '6987' if the MAC is missing.
  - SW1 SW2 = '6988' if the MAC is incorrect.

Req 6.80 (Issuer Script Reset of CTTA)

If ‘Do not reset CTTA during Issuer Authentication Processing’ supported by card (ADA byte 2 bit 2 is 1b) **and** a PUT DATA command updating the Cumulative Total Transaction Amount Limit (CTTAL) is successfully performed, then the card shall reset the the Cumulative Total Transaction Amount (CTTA) to zero.

Req 6.81 (Issuer Script Reset of VLP Available Funds)

If ‘Do not reset VLP Available Funds during Issuer Authentication Processing’ supported by card (ADA byte 2 bit 1 is 1b) **and** a PUT DATA command updating the VLP Funds Limit is successfully performed, then the card shall reset the VLP Available Funds to the VLP Funds Limit.

Req 6.82 (Issuer Script Command Result)

If the card is able to successfully validate the MAC and successfully perform the issuer script command, then the card shall:

- Increment the Issuer Script Command Counter by one.

  Note: When the Issuer Script Command Counter (ISCC) has a value of 'F', the resulting value of the ISCC after it is incremented by one is dependent on whether the ISCC is cyclic (ADA byte 3 bit 2). If the ISCC is cyclic, then incrementing the ISCC by one cycles the value back to '0'. Otherwise (the ISCC is not cyclic), incrementing the ISCC by one results in the same value of 'F'.
- Set the Last Online ATC Register to the value of the ATC.
- Set the Last Successful Issuer Update ATC Register to the value of the ATC.
- Respond indicating the issuer script processing result.

Else (Issuer Script command processing is unsuccessful), the card shall:

- Set the Last Contactless Application Cryptogram Valid Indicator to 0.
- Set the Issuer Script Failure Indicator to 1.
- Respond indicating the issuer script processing result.

A Fast Dynamic Data Authentication (fDDA)

In most contactless payment environments, quick transaction speeds are a business requirement. A method of dynamic data authentication, called fDDA (based on DDA as defined in [EMV]) is therefore defined for offline protection against skimming.

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 GPO command, rather than generating the dynamic signature at the end of the transaction when the card may be moving away from the reader field.

The card uses the PDOL to request data from the terminal for fDDA. The card receives the requested data from the reader in the GPO command. The card uses these terminal data elements, along with card data, to create the dynamic signature.

The AFL returned in the GPO points to records containing the RSA certificates and data related to fDDA. Once the last record is read by the reader, the card need no longer remain in the field. The reader then validates the dynamic signature for fDDA. If the validation process fails, the transaction is declined offline, sent online for authorization, or terminated, dependent on issuer preference (as indicated in the CTQ).

Other than the early creation of the dynamic signature, the card leaving the field before DDA is validated, and the lack of reporting of DDA results in authorization and clearing messages; fDDA is EMV-compliant.

In order to accommodate the possibility of new fDDA algorithms and inputs, the card data element fDDA Version Number (part of tag '9F69') is defined to identify the fDDA version used by the card. The fDDA Version Number is returned by the card and used by the reader to determine the fDDA version algorithm to perform. In this version of the specification, only fDDA version '01' is defined and supported.

For cards compliant to this version of the specification, only fDDA version '01' is allowed.

For readers compliant to this version of the specification, only fDDA version '01' is allowed.

For fDDA version '01', the card includes the (Terminal) Unpredictable Number; Amount, Authorized; and Transaction Currency Code received from the reader in the PDOL, combined with the card ATC and Card Authentication Related Data into the calculation of the dynamic signature.

Note: The Static Data Authentication Tag List (tag '9F4A') is supported as defined in [EMV] Book 3 section 10.3 and [EMV] Book 2 section 6 for fDDA processing.

A.1 Dynamic Signature Generation

The concatenation of data and generation of the dynamic signature will be in accordance with [EMV] Book 2 section 6.5.1 Step #2, with the following exception(s):

- For online authorization requests (ARQC), the Signed Data Format input to the DDA hash algorithm ([EMV] Book 2 Table 14) shall be the value '95'. The Signed Data Format of '95' distinguishes the dynamic signature returned for an online authorization request from the dynamic signature returned for an offline authorization request (where Signed Data Format '05' is used).
- For offline approval requests (TC), the Signed Data Format input to the DDA hash algorithm ([EMV] Book 2 Table 14) shall continue to be the value '05'.

The Terminal Dynamic Data elements are not specified in the DDOL (as the DDOL is not a recognized data element for qVSDC). The Terminal Dynamic Data referenced in [EMV] Book 2 Table 14 shall consist of the concatenation of the data elements specified in Table A-1 in the order specified. fDDA fails if any of the data elements required to support fDDA is missing.

Prior to including the Card Authentication Related Data in the Terminal Dynamic Data, the card shall generate and include the (card) Unpredictable Number and CTQ in the Card Authentication Related Data.

Note: If the CTQ is not personalized, then a value of zeros is used in the Card Authentication Related Data.

The ICC Dynamic Data referenced in [EMV] Book 2 Table 14 shall consist of the concatenation of the data elements specified in Table A-2.

Table A-1: Terminal Dynamic Data for input to DDA hash algorithm

Tag	Data Element	Length	Data Source
9F37	Unpredictable Number	4 bytes	Terminal
9F02	Amount, Authorized	6 bytes	Terminal
5F2A	Transaction Currency Code	2 bytes	Terminal
9F69	Card Authentication Related Data	var.	Card

Table A-2: ICC Dynamic Data for input to DDA hash algorithm

Tag	Data Element	Length	Data Source
9F36	Application Transaction Counter (ATC)	2 bytes	Card

A.2 Dynamic Signature Verification

To verify the fDDA dynamic signature, the reader-terminal must first retrieve the Certification Authority Public Key Index, as specified in [EMV] Book 2 section 6.2.

Retrieval of the Issuer Public Key shall then be performed by the reader-terminal in accordance with [EMV] Book 2 section 6.3.

Retrieval of the ICC Public Key shall be performed by the reader-terminal in accordance with [EMV] Book 2 section 6.4.

Verification of the dynamic signature shall then be performed by the reader-terminal in accordance with [EMV] Book 2 section 6.5.2, with the following exception(s):

- The Terminal Dynamic Data elements input to the hash algorithm shall be as specified in Table A-1 instead of being specified in the DDOL (as the DDOL is not a recognized data element for qVSDC). The terminal may treat the tags specified in Table A-1 as default DDOLs for fDDA version '01'.

  Note: The Card Authentication Related Data is variable length. The reader shall use the full Card Authentication Related Data returned by the card for dynamic signature verification.

In any of the following cases, fDDA shall fail:

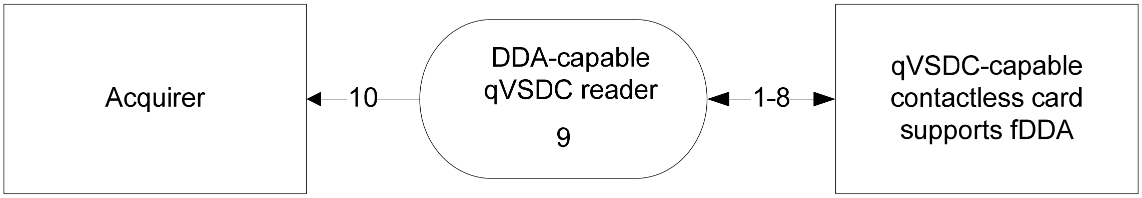
- Application Interchange Profile (AIP) indicates that DDA is not supported by the card (AIP byte 1 bit 6 is 0b).

  Note: Readers compliant to this specification do not perform fDDA dynamic signature verification for card application online approval requests.

- fDDA is supported and data required to support fDDA is missing.
- The version of fDDA requested by the card is not supported by the reader. fDDA v01 is the only supported version of fDDA in this specification.
- The dynamic signature is using a Signed Data Format that is not '05'.

Note: Although card application behavior is specified to be capable of returning a dynamic signature generated using a Signed Data Format of '95', this behavior is not intended to be used at standard POS acceptance environments. Readers compliant to this specification shall use Signed Data Format '05' only (and not Signed Data Format '95') when verifying the dynamic signature.

Figure A-1: Fast DDA (fDDA) qVSDC Example



1. Reader SELECTs PPSE.
2. Card responds with single Visa AID.
3. Reader SELECTs Visa AID.
4. Card responds requesting:
    - Terminal Transaction Qualifiers (tag '9F66')
    - Unpredictable Number (tag '9F37')
    - Amount, Authorized (tag '9F02')
    - Transaction Currency Code (tag '5F2A')
    - Other tags not related to fDDA
5. Reader issues GET PROCESSING OPTIONS providing:
    - Tag '9F66' indicating qVSDC only
    - Tag '9F37' Unpredictable Number
    - Tag '9F02' Amount, Authorized
    - Tag '5F2A' Transaction Currency Code
    - Other card requested data not related to fDDA
6. Card responds with:
    - Dynamic signature
    - AFL listing records related to Offline Data Authentication (fDDA)
    - Other data not related to fDDA
7. Reader reads records indicated in AFL.
8. Card provides RSA certificates and data to validate hash of static data along with Card Authentication Related Data in response to the last READ RECORD.

Card may leave the field.

9. Reader validates dynamic signature.
10. If fDDA fails, the transaction is declined, switched to another interface, or sent online depending on issuer settings.

B Dynamic CVV (dCVV)

Application-level security is the best means of securing a transaction because it does not rely on transport or network, and can provide end-to-end security to the issuer. Translating this concept to the MSD environment results in the generation of a dynamic Card Verification Value (dCVV) for each transaction. The dCVV is then placed in the standard Track 2 Equivalent Data.

dCVV is for use in MSD Legacy transactions, and is not an option for physical magnetic stripe, qVSDC, or VIS transactions.

dCVV is transparent to the reader. The reader does not see any difference in the data because the data read from the card, with the sentinels added by the PCD, looks like a physical magnetic stripe (Track 2). The POS device passes this data to the payment network (in Track 2 and/or Track 1), which passes it to the issuer.

The issuer shall differentiate between a swiped magnetic stripe transaction and an MSD Legacy transaction before deciding whether to check for a dynamic CVV (dCVV) or static CVV.

Upon establishing the transaction as an MSD Legacy transaction, the issuer will generate the dCVV based upon the information provided in the authorization request, and verify this against the dCVV sent in the authorization request.

As implied, this is an online solution, when an issuer or a processor on behalf of the issuer is available to validate the dCVV.

B.1 Detailed Design Discussion

The dCVV methodology leverages current systems and processes and requires minimal changes to involved parties.

Currently, an issuer generates the CVV using two single DES keys along with the account number, expiry date, and service code.

Each contactless card can be personalized with a unique derivation key (UDK, a double length DES key comprised of UDKA and UDKB). The methodology for deriving this UDK is well established in [VIS] (see [VIS] Appendix D.7).

The UDK in the card, along with a count of transactions (the ATC), is used with the standard CVV algorithm to generate a dynamic value for every transaction. This methodology has been borrowed from [VIS], with a single exception: the ATC is first formatted to Binary Coded Decimal (BCD) and only the rightmost four digits are used (whereas the ATC is a 2-byte binary counter in [EMV] and [VIS]).

The ATC is formatted as Binary Coded Decimal (BCD) and the rightmost four digits are then inserted in the Track 2 Equivalent Data. This means that 9,999 is the highest value that can be stored in Track 2 Equivalent Data. Every 10,000th transaction will contain a zero value in the Track 2 Equivalent Data.

For dCVV, only the rightmost four digits of the ATC will be used.

When the 2-byte ATC reaches its maximum value, the application is permanently blocked, as specified in Req 6.7 (Application Permanently Blocked). Additionally, the dCVV calculation shall be disabled, and a fixed value shall be returned in the Track 2 Equivalent Data.

All data elements are sent to the issuer so that the correct dCVV can be generated.

The issuer's Hardware Security Module needs the PAN and PAN sequence number to generate the UDK. The PAN sequence number is assumed to be zero for the calculation of the UDK used for dCVV.

The Master Derivation Keys (MDKs) used to derive the UDKs are part of the same series of keys used for VIS. Because the Derivation Key Index which points to the MDK is not included in online magnetic stripe messages, it shall be stored in VisaNet and in issuer host systems. If a card application supports VIS and MSD, the UDK may be shared (as long as the PAN Sequence Number is zero) or separate keys may be supported.

The issuer needs the ATC for generating the correct dCVV. To minimize the threat of replay attacks, the issuers should keep track of prior ATCs to ensure that the value of the ATC in the current transaction is higher (allowing for earlier transactions that have been batched and delayed by the merchant) than the value in the previous transaction and that no duplicates occur.

The dCVV value is carried in the Track 2 Equivalent Data. The contents of Track 2 Discretionary Data must include the (i)CVV, but the position of the (i)CVV and any additional data in Track 2 Discretionary Data are at issuer discretion (see [VPTSM]). In order to minimize the impact to acquirer systems, the Discretionary Data field in the Track 2 Equivalent Data shall begin with the dCVV in the first three positions. The ATC shall immediately follow the dCVV.

Following the ATC, the Contactless Indicator may be added. The Contactless Indicator is a single digit and its value can be from 0 through 9. A value greater than zero indicates a contactless magnetic stripe transaction. A single value, for example 1, can be personalized on all cards. Multiple values (1, 2, 3) can also be personalized to uniquely identify cards with the same Primary Account Number (PAN).

Note: For details and recommendations on how to personalize the Track 2 Equivalent Data, see Appendix F.

The MSD Offset (tag '9F67', binary 8, 1 byte in length) contains the offset from the beginning of the Track 2 Equivalent Data to the first digit/nibble of the dCVV. The offset is specified in nibbles, with the first digit/nibble of the PAN as 1. Start sentinels and end sentinels are not present in the Track 2 Equivalent Data (on the chip).

Personalizing the MSD Offset with a value greater than zero indicates that the dCVV and ATC shall be calculated and inserted into Track 2 Equivalent Data for MSD Legacy transactions.

B.2 ATC Insertion Option

Implementations shall support insertion of the ATC in Track 2 Equivalent Data for qVSDC and MSD CVN17 transactions, and MSD Offset bit 8 shall be used to activate this functionality. MSD Offset bits 7-1 shall indicate the offset from the beginning of Track 2 Equivalent Data to the first digit of the CVV placeholder.

The MSD Offset is processed as follows (when personalized with a value greater than zero):

- The dCVV and ATC (BCD formatted, rightmost 4-digits) shall be inserted into Track 2 Equivalent Data for MSD Legacy transactions.
- If MSD Offset bit 8 = 1b, then the ATC (BCD formatted, rightmost 4-digits) shall also be inserted into Track 2 Equivalent Data, after the iCVV personalized on the card, for qVSDC transactions and MSD CVN17 transactions.

MSD Offset is used internally by the card. It is not provided to the reader during transaction processing. However, access to the MSD Offset outside transaction processing is not restricted.

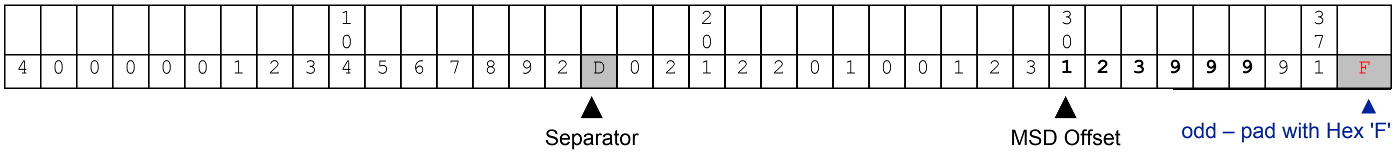
B.3 Example of Track 2 Equivalent Data

Figure B-1 shows an example of Track 2 Equivalent Data as it is read from the chip. The ATC and dCVV have been encoded in Discretionary Data. The card is personalized with an MSD Offset of 30 nibbles/digits.

- PAN: 4000 0012 3456 7892 (16 digits)
- Expiration date: 12/02
- Service code: 201
- PVKI: 0
- PIN verification data: 0123
- Discretionary Data: 123 9999 (first three positions = dCVV, next four positions = ATC)
- Contactless Indicator

Note: The data has been padded with a single hexadecimal 'F' to ensure full bytes. This padding is always done if the number of nibbles is odd.

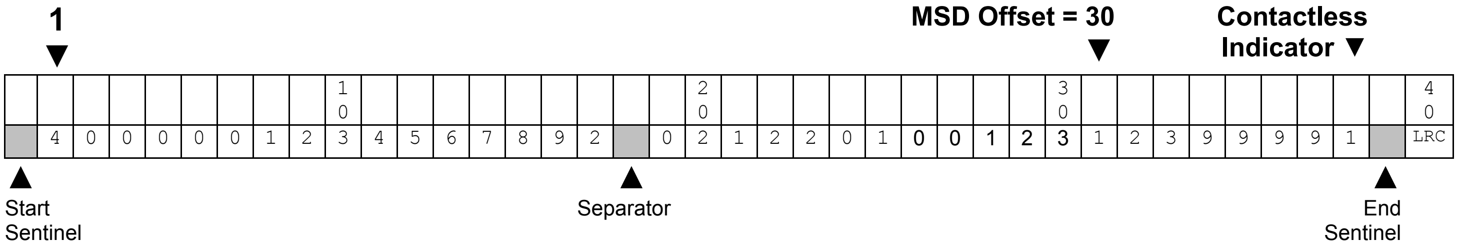
Figure B-1: Example of Track 2 Equivalent Data Read from the Chip



									1 0										2 0										3 0							3 7	
4	0	0	0	0	0	1	2	3	4	5	6	7	8	9	2	D	0	2	1	2	2	0	1	0	0	1	2	3	**1**	**2**	**3**	**9**	**9**	**9**	9	1	F

The reader may take the Track 2 Equivalent Data read from the chip and construct a virtual magnetic stripe that emulates the physical magnetic stripe, and then pass it to the POS device. The 'F' pad character (if present) shall be stripped off and the Start Sentinel, End Sentinel, and LRC shall be added. Figure B-2 illustrates the result.

Figure B-2: Example of Track 2 Equivalent Data Read from Magnetic Stripe



									1 0										2 0										3 0										4 0
	4	0	0	0	0	0	1	2	3	4	5	6	7	8	9	2		0	2	1	2	2	0	1	0	0	1	2	3	1	2	3	9	9	9	9	1		LRC

Note: The start and end sentinels and the LRC are not included in any calculation.

B.4 The dCVV Algorithm

The following steps describe, and Figure B-3 illustrates, the creation of the dCVV.

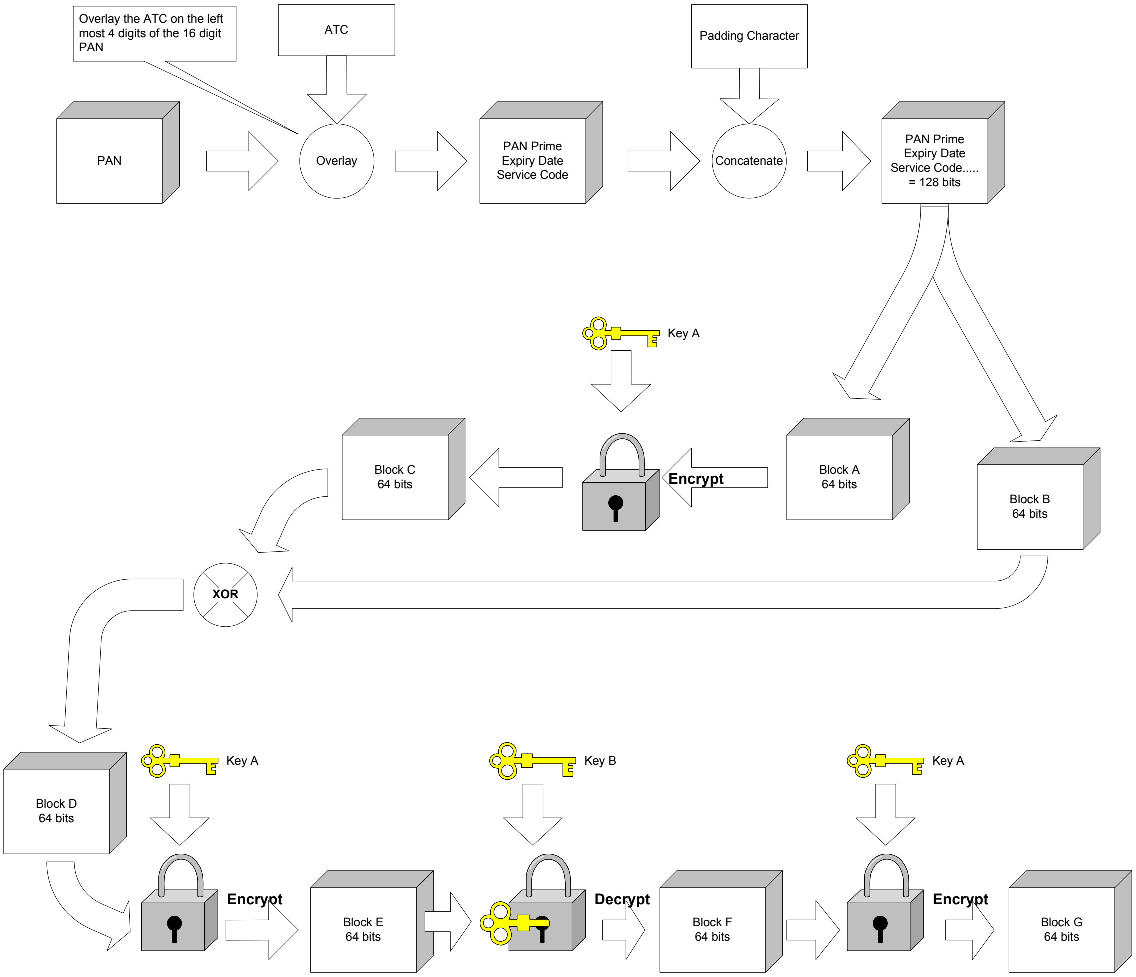
1. Construct a string by replacing the leftmost four digits of the Primary Account Number (PAN) with the ATC. This will be referred to as the altered PAN in subsequent steps.
2. Construct a string of bits by concatenating, from left to right, the following data:

    altered PAN

    Card Expiration Date

    Service Code
3. Place the result of Step 2 into a 128-bit field, right-filling the remaining bits with binary zeros.
4. Split the 128-bit field into two 64-bit blocks. The leftmost 64 bits are Block A, and the rightmost 64 bits are Block B.
5. Encrypt Block A with UDKA. This results in Block C.
6. Exclusive-OR (XOR) Block C with Block B. This results in Block D.
7. Encrypt Block D with UDKA, giving Block E.
8. Decrypt Block E with UDKB, giving Block F.
9. Encrypt Block F with UDKA, giving Block G.
10. Use Block G and, beginning with the leftmost digit, extract all the digits from 0 through 9. Left justify these digits in Block H.
11. Use Block G and, beginning with the leftmost digit, extract the hexadecimal digits from A to F. Then convert each extracted digit to a decimal digit by subtracting 10, giving Block I.
12. Concatenate Block I to the right of Block H.
13. Select the three leftmost digits from the concatenated result in Step 12. These digits are the dCVV.

Figure B-3: Dynamic CVV Algorithm



C Cryptogram Versions

C.1 Cryptogram Version Number 10

Cryptogram Version Number 10 shall be as defined in [VIS] Appendix D, with the following exception(s):

- Reader-terminal data objects input to the cryptographic algorithm are requested by the card in the Processing Options Data Object List (PDOL).

[VIS] Appendix D defines the input parameters, keys, and algorithms associated with the generation of the cryptogram for Cryptogram Version Number 10.

C.2 Cryptogram Version Number 17

Cryptogram Version Number 17 uses the same algorithm and parameters as Cryptogram Version Number 10, but differs in that it does not support all of the data elements required for Cryptogram Version Number 10. Table C-1 lists the data elements in the required order for Cryptogram Version Number 17.

Table C-1: Data Elements included in Cryptogram Version Number 17

Tag	Data Element	Data from Terminal	Input by Card
'9F02'	Amount, Authorized *****	✓	
'9F37'	Unpredictable Number	✓	
'9F36'	Application Transaction Counter (ATC)		✓
'9F10'	Issuer Application Data (IAD) Byte 5 Only byte 5 of the IAD is used for CVN17 cryptogram generation. Though only IAD byte 5 is signed, the entire IAD shall be present in messages. *Note*: IAD byte 5 is CVR byte 2.		✓

* A zero-filled Amount, Authorized is permitted for MSD and does not need to be sent online as a tagged data element in Field 55 or a special field in authorization and clearing messages (see Appendix K.1). If the issuer does not receive the data element, a value of zero shall be substituted when performing cryptogram validation.

C.3 Cryptogram Version Number 18

Cryptogram Version Number 18 shall be as defined in [VIS] Appendix D, with the following exception(s):

- Reader-terminal data objects input to the cryptographic algorithm are requested by the card in the Processing Options Data Object List (PDOL).

[VIS] Appendix D defines the input parameters, keys, and algorithms associated with the generation of the cryptogram for Cryptogram Version Number 18.

D VCPS Data Elements

This appendix defines the data elements used in this specification for financial transaction interchange and their mapping onto data objects.

D.1 Data Element Descriptions

Table D-1 lists the data elements used in VCPS.

Req D.1 (Data Element Requirements)

Readers and cards shall comply with the requirements, where specified and applicable, in Table D-1.

D.1.2 Name

The *Name* column lists the name of the data element, and also includes the following:

- Format (F) of the data element. The [EMV] defined supported formats are as follows:
  - n (numeric)
  - cn (compressed numeric)
  - b (binary or bit string)
  - an (alphanumeric)
  - ans (alphanumeric special)
- Tag (T) of the data element in hexadecimal. Tags in the range 'DF00' – 'DFFE' are context specific data elements that only define the corresponding data element when contained in the listed template tag. This is shown as “DFxx in BFxx”, where 'DFxx' represents the context specific data element, and 'BFxx' represents the template tag containing the context specific data element.

  The meaning assigned to a context-specific tag in one template will be different from the meaning assigned to the same context-specific tag in another template.

  Note: A data element that is defined with both a primitive tag and a context specific primitive tag within a template tag shall reference the same underlying value regardless of the tag used. The data element value shall be personalizable, updateable, and accessible using either tag, subject to the specific restrictions for the data element.
- Length (L) of the data element. The value of the length is shown in decimal. When the length defined for the data object is greater than the length of the actual data, the following rules apply:

- A data element in format n is right-justified and padded with leading hexadecimal zeros
- A data element in format cn is left-justified and padded with trailing hexadecimal 'F's
- A data element in format an is left-justified and padded with trailing hexadecimal zeros
- A data element in format ans is left-justified and padded with trailing hexadecimal zeros

When data is moved from one entity to another (for example, card to reader), it shall always be passed in order from high order to low order, regardless of how it is internally stored. The same rules apply when concatenating data.

- Source (S) of the data element, indicated as “Card”, “Reader”, or “Issuer”.
- Path (P) for which the data element is applicable, indicating qVSDC (“Q”), MSD (“M”), or both (“Q M”). If a card data element is applicable to both paths, then it is further indicated whether the data element is “Shared” on the card between paths or “Exclusive” (separate) on the card for each individual path. Card data elements that are issuer configurable to be either Exclusive or Shared (e.g. record data) are indicated as “E or S”. Data elements that are not applicable for a given path shall be treated as unrecognized data elements when the reader is processing for that path.

  Note: As described above, the letters “Q” and “M” denote that the data element is applicable to the qVSDC path and MSD path, respectively. However, the paths may be further defined to indicate that the data element is applicable only for the *card* path, denoted as “Q_C” and “M_C”, and that *reader* path processing shall treat these data elements as unrecognized data elements.

  For example, the data elements required for Offline Data Authentication are applicable to the card application MSD path (if Offline Data Authentication for Online Authorizations is supported), but are not applicable to the MSD path for readers compliant to this specification.

- Dual Interface (D) indicates that for cards also supporting VIS, the data element is not supported for VIS (“–”), shared with VIS (“Shared”), exclusive/separate between VCPS and VIS (“Exclusive”), or is not applicable ("N/A"). Data elements that are issuer configurable to be either Exclusive or Shared (e.g. record data) are indicated as “E or S”.

  Note: “Exclusive” indicates that the data element can be configured separately. This does not preclude the data element from being configured with the same value.

D.1.3 Requirement

The *Requirement* column lists the requirements for the data element:

- Mandatory – The data element must always be present and provided to the reader if the source is the card. If the data element is not received by the reader, then the reader terminates the transaction.
- Required – The data element must always be present, but the reader does not terminate the transaction if the data element is not present.
- Conditional – The data element is necessary under the conditions specified.
- Optional – The data element is optional.

If the requirement is different for a data element applicable to both the qVSDC path and the MSD path, two sets of requirements are specified in the *Requirement* column (one for each path).

D.1.4 Update Capability, Issuer Update, Retrieval, Secret

This column lists the Update Capability (UC), Issuer Update (IU), Retrieval (R), and Secret data requirements for data elements that have the card as the source. The following sections further describe the values for each of these fields.

Update Capability (UC)

The Update Capability (UC) entry in this column categorizes card-sourced data into the following classifications:

- **Unchanging**—The data element value is set before the first transaction (either by personalization of a starting value, or to a default value) and shall not change.
- **Modifiable**—The data element value is set before the first transaction (either by personalization of a starting value, or to a default value) and the value it contains at the end of one transaction is the value retained for use during the subsequent transaction. The value may only be modified post-issuance using an issuer update, as identified in the Issuer Update (IU) entry listed in this column.
- **Persistent**—The data element value is set before the first transaction (either by personalization of a starting value, or to a default value) and the value it contains at the end of one transaction is the value retained for use during the subsequent transaction. The value may only be modified as part of transaction processing (for example, to indicate events that have occurred during the current transaction which may be used in processing subsequent transactions), and shall not be modified using any issuer script command.

- **Dynamic**—The data element value is set before the first transaction (either by personalization of a starting value, or to a default value) and the value it contains at the end of one transaction is the value retained for use during the subsequent transaction. The value may be modified post-issuance either as part of transaction processing or using an issuer update, as identified in the Issuer Update (IU) entry listed in this column.
- **Transient**—The data element value is reset at the beginning of a transaction, and the value set in one transaction is not retained for the subsequent transaction. The value is modified during transaction processing to indicate events that have occurred during the current transaction.

Data elements classified as *unchanging* or *persistent* may be included as part of an issuer script command to update a record or larger data element which contains the data element and is allowed to be updated. However, the value of the *unchanging* or *persistent* data element after update of the record or larger data element shall be the same as the value before the update. The application is not required to enforce this restriction, it is a requirement on the issuer script command sent to the application.

For example, the Issuer Application Data may be updated by a PUT DATA command, but the value of the CVN and DKI after the update shall be the same as the value before the update. Similarly, the record that contains the Application Expiration Date may be updated, but the value of the Application Expiration Date after the update must be the same as the value before the update.

<u>Issuer Update</u>

The Issuer Update (IU) entry in this column shows whether update of the data element is allowed using an Issuer Update, the command to be used for the update, and any conditions on the support for update.

The following values are used to indicate support for update of data elements:

- **N/A**—indicates that the specification does not define a mechanism to update the data element with an Issuer Update (for example, the data element does not have a tag). However, update of the data element with an Issuer Update is allowed.
- **N**—indicates update of the value of the data element with an Issuer Update is not allowed.

  Note: The data element may be included as part of an update to a record or larger data element that is allowed to be updated. However, the value of this data element after update of the record or larger data element shall be the same as the value before the update. The application is not required to enforce this restriction, it is a requirement on the issuer script command sent to the application.
- **CSU**—indicates that update of the data element is allowed using the functionality associated with the Card Status Updates data element included in the Issuer Authentication Data for CVN18.

- **PIN CHANGE/UNBLOCK**—indicates that update of the data element is allowed using the PIN CHANGE/UNBLOCK command.
- **PUT DATA**—indicates that update of the data element is allowed using the PUT DATA command.
- **UPDATE RECORD**—indicates that update of the data element is allowed using the UPDATE RECORD command.

Implementations are not required to support Issuer Update of application internal data elements returned in the GPO response. Implementations are not precluded from supporting Issuer Update of application internal data elements returned in the GPO response, but support for any such mechanism is outside the scope of this specification.

<u>Retrieval</u>

The Retrieval (R) entry in this column shows whether the data element may be retrieved by the reader and the command to be used for the retrieval. If "(SD)" follows the retrieval command, then the data element shall be retrieved only by special devices and not by readers during financial transactions. If the column is blank for a data element, support for retrieval of the data element is optional.

The following values are used to indicate support for retrieval of data elements:

- **N/A**—indicates that the specification does not define a mechanism to retrieve the data element (for example, the data element does not have a tag). However, retrieval of the data element is allowed.
- **N**—indicates retrieval of the value of the data element shall not be allowed.
- **GET DATA**—indicates that retrieval of the data element is allowed using the GET DATA command. The GET DATA command is not used during financial transactions in this version of the specification.
- **GET DATA (SD)**—indicates that retrieval of the data element using the GET DATA command at special devices shall be supported for use in card approval testing, personalization validation, and investigation of potential interoperability issues.

  Note: The card application is not required to distinguish between the GET DATA command used by readers during financial transactions and the GET DATA command used by special devices. From a card application perspective, there is no difference between the GET DATA and GET DATA (SD) designations.
- **GET PROCESSING OPTIONS (GPO)**—indicates that the data element may be retrieved as part of the data sent in the response to the GET PROCESSING Options command.
- **READ RECORD**—indicates that retrieval of the data element is allowed using the READ RECORD command.
- **SELECT**—indicates that the data element may be retrieved as part of the data sent in the response to the SELECT command.

Secret Data

Data elements identified as Secret in this column shall be stored securely within the card for each application in one or more proprietary internal files. These data elements shall never be retrievable by a reader or any outside source and shall never be updated. The following data elements are secret:

- Unique DEA Key A and Unique DEA Key B
- Data Encipherment DEA Key A and Data Encipherment DEA Key B
- MAC DEA Key A and MAC DEA Key B
- Unique DEA Key for dCVV A and Unique DEA Key for dCVV B
- ICC Private Key

Table D-1: VCPS Data Elements

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Amount, Approximated F: n 12 T: – L: 6 S: Card P: Q D: –	Required	Visa proprietary data element used in qVSDC Card Action Analysis.	UC: Transient IU: N R: N	When the Transaction Currency Code matches a Conversion Currency Code in the Currency Conversion Parameters, the card application calculates the (approximate) value of the transaction using the associated Currency Conversion Factor and stores the resulting value in the Amount, Approximated. When the Transaction Currency Code matches the Application Currency Code, the Amount, Approximated has the same value as the Amount, Authorized.
Amount, Authorized (Numeric) F: n 12 T: 9F02 L: 6 S: Reader P: Q M D: N/A	Required	Authorized amount of the transaction (including Amount, Other and excluding adjustments).	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Amount, Other (Numeric) F: n 12 T: 9F03 L: 6 S: Reader P: Q M D: N/A	Conditional If cashback supported	Secondary amount associated with the transaction representing a cashback amount.	N/A	
Application Capabilities F: b 16 T: DF01 in BF5B L: 2 S: Card P: Q M D: Shared	Conditional If Application Capabilities functionality supported	Visa proprietary data element indicating card application capabilities. For data element usage, see Appendix I.	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	Byte 1 bit 8: 1 = Contactless Functionality Disabled bit 7: 1 = Restrict reset of Contactless Functionality Disabled bit bits 6-1: RFU (000000) Byte 2 RFU ('00')
Application Cryptogram (AC) F: b 64 T: 9F26 L: 8 S: Card P: Q M, Exclusive D: Exclusive	qVSDC: Mandatory MSD: Conditional If Online Cryptogram required by reader	Cryptogram returned by the card in response to the GPO command.	UC: Transient IU: N R: GPO	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Currency Code F: n 3 T: 9F51 L: 2 S: Card P: Q D: Shared	Conditional If currency code restrictions or currency code velocity checks supported	Visa proprietary data element indicating the currency in which the amount is managed according to [ISO 4217].	UC: Unchanging IU: N R: GET DATA (SD)	
Application Default Action (ADA) F: b 32 T: 9F52 L: 4 S: Card P: Q D: Shared	Conditional If Application Default Action functionality supported	Visa Proprietary data element indicating issuer-specified action for the card to take for certain conditions.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Byte 1 bits 8-1: Not used for VCPS Byte 2 bits 8-3: Not used for VCPS bit 2: 1 = Do not reset CTTA during Issuer Authentication processing. *Note:* CTTA is reset to zero during Issuer Script processing if PUT DATA to CTTAL is successful. bit 1: 1 = Do not reset VLP Available Funds during Issuer Authentication processing. *Note:* VLP Available Funds is reset to VLP Funds Limit during Issuer Script processing if PUT DATA to VLP Funds Limit is successful. *– continues –*

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Default Action (ADA) (continued)				Byte 3 *Note:* Support for the functionality associated with byte 3 bits 8-6 is conditional on support for transaction logging. bit 8: 1 = Do not include offline approval requested transactions in the transaction log bit 7: 1 = Do not include online approval requested transactions in the transaction log bit 6: 1 = Include offline declined transactions in the transaction log bit 5: 1 = Reset VLP Available Funds to VLP Funds Limit when Offline PIN successfully verified bit 4: Not used for VCPS bit 3: 1 = Issuer Script MAC Chaining supported bit 2: 1 = Issuer Script Command Counter is cyclic *Note:* Support for the functionality associated with byte 3 bit 1 is conditional on support for [VIS], and allows [VIS] and VCPS applications to count international transactions using the same single counter. bit 1: 1 = CTCI also counts non-matching country code transactions *– continues –*

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Default Action (ADA) (continued)				Byte 4 *Note:* Support for the functionality associated with byte 4 bits 8-6 is conditional on support for Issuer Update Processing and Cryptogram Version Number 18. bit 8: 1 = Use Default Update Counters in ADA if CSU is generated by a proxy bits 7-6: Default Update Counters 00 = Do not update velocity-checking counters 01 = Set velocity-checking counters to Upper Limits 10 = Reset velocity-checking counters to zero 11 = Not used for VCPS bit 5: 1 = Padding method '80' supported bits 4-1: RFU (0000)
Application Definition File (ADF) Name		See entry for "Application Identifier" (tag '4F').		

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Expiration Date F: n 6 YYMMDD T: 5F24 L: 3 S: Card P: Q D: E or S	Conditional If fDDA supported	Date after which the card application expires. For transactions where Offline Data Authentication is performed, the Application Expiration Date is returned. For transactions where Offline Data Authentication is not performed, the Application Expiration Date does not need to be returned.	UC: Unchanging IU: N R: READ RECORD	*Note:* The reader is able to obtain the application's expiration date from Track 2 Equivalent Data when the Application Expiration Date is not returned by the card.
Application File Locator (AFL) F: var. T: 94 L: var. up to 252 S: Card P: Q M, Exclusive D: Exclusive	Conditional If returning record data for the transaction	Indicates the location (SFI, range of records) of the AEFs related to a given application. As with all data elements returned in the GPO response, the card application supports personalization of different AFL data elements for use in the following GPO responses: • qVSDC Offline GPO Response (if offline implemented) • qVSDC Online with ODA GPO Response • qVSDC Online/Decline without ODA GPO Response • MSD CVN17 with ODA GPO Response • MSD CVN17 without ODA GPO Response • MSD Legacy GPO Response	UC: Unchanging IU: N R: GPO The Update Capability and Update of the AFLs for VCPS may not be the same as the AFLs for VIS.	For each file to be read, the Application File Locator contains the following four bytes: Byte1 bits 8-4 = SFI bits 3-1 = 000 Byte 2: First (or only) record number to be read for that SFI (never equal to zero) Byte 3: Last record number to be reader for that SFI (shall be greater than or equal to byte 2) Byte 4: Number of consecutive records involved in authentication of static data, starting with record number in byte 2 (may range from zero to the value of the third byte minus the value of the second byte + 1)

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Identifier (ADF Name) F: b 40-128 T: 4F L: 5-16 S: Card P: Q M, Shared D: Shared	Mandatory	The ADF Name identifies the application as described in [ISO 7816-5]. The AID is made up of the Registered Application Provider Identifier (RID) and the Proprietary Identifier Extension (PIX).	UC: Unchanging IU: N R: SELECT	The Visa RID is 'A000000003'. The global Visa AIDs are: 'A0000000031010': Visa Debit or Credit 'A0000000032010': Visa Electron 'A0000000033010': Interlink 'A0000000038010': PLUS
Application Identifier (AID) F: b 40-128 T: 9F06 L: 5-16 S: Reader P: Q M D: N/A	Required	Identifies the application as described in [ISO 7816-5].	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Interchange Profile (AIP) F: b 16 T: 82 L: 2 S: Card P: Q M, Exclusive D: Exclusive	Mandatory	Indicates the capabilities of the card to support specific functions in the application. VCPS readers shall not act on AIP bit settings that are not supported for VCPS or that are Reserved for Future Use (RFU). As with all data elements returned in the GPO response, the card application supports personalization of different AIP data elements for use in the following GPO responses: • qVSDC Offline GPO Response (if offline implemented) • qVSDC Online with ODA GPO Response • qVSDC Online/Decline without ODA GPO Response • MSD CVN17 with ODA GPO Response • MSD CVN17 without ODA GPO Response • MSD Legacy GPO Response	UC: Unchanging IU: N R: GPO The Update Capability and Update of the AIPs for VCPS may not be the same as the AIPs for VIS.	Byte 1 bit 8: RFU (0) bit 7: Not used for VCPS bit 6: 1 = DDA is supported for qVSDC bit 5: Not used for VCPS bit 4: Not used for VCPS bit 3: Not used for VCPS bit 2: RFU (0) bit 1: Not used for VCPS Byte 2 bit 8: 1 = MSD is supported bits 7-1: RFU (0000000)

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Internal Data Template F: b T: BF5B L: var. S: Card P: Q M, Shared D: –	Conditional If Application Capabilities supported	Visa proprietary data template that contains Visa proprietary context specific tags for application internal data.	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context specific tags are defined in this specification for the Application Internal Data Template: 'DF01' – Application Capabilities
Application Label F: ans 1-16 * T: 50 L: 1-16 S: Card P: Q M, Shared D: E or S * (special characters limited to spaces)	Optional	Mnemonic associated with AID according to [ISO 7816-5]. Used in application selection. Application Label is optional in the File Control Information (FCI) of an Application Definition File (ADF) and optional in an ADF directory entry for VCPS.	UC: Unchanging IU: N R: SELECT	
Application Preferred Name F: ans 1-16 T: 9F12 L: 1-16 S: Card P: Q M, Shared D: E or S	Optional	Preferred mnemonic associated with the AID.	UC: Unchanging IU: N R: SELECT	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Primary Account Number (PAN) F: var. up to cn 19 T: 5A L: var. up to 10 S: Card P: Q D: E or S	Conditional If fDDA supported	Valid cardholder account number. For transactions where Offline Data Authentication is performed, the Application PAN is returned. For transactions where Offline Data Authentication is not performed, the Application PAN does not need to be returned. *Note:* The reader is able to obtain the primary account number from Track 2 Equivalent Data when the Application PAN is not returned by the card.	UC: Unchanging IU: N R: READ RECORD	
Application Primary Account Number Sequence Number (PSN) F: n 2 T: 5F34 L: 1 S: Card P: Q M, E or S D: E or S	Optional	Identifies and differentiates card applications with the same PAN.	UC: Unchanging IU: N R: GPO, READ RECORD	*Note:* Although this field is optional in the card, if it is present in the card it is sent in online messages. If it is not sent in online messages, the value is assumed to be '00' for key derivations.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Priority Indicator F: b 8 T: 87 L; 1 S: Card P: Q M, Shared D: E or S	Conditional If multiple contactless payment applications on card	Indicates the priority of a given application or group of applications in a directory.	UC: Unchanging IU: N R: SELECT	bit 8: Not used for VCPS bits 7-5: RFU (000) bits 4-1: 0000 = No priority assigned xxxx = Order in which the application is to be selected, ranging from 1 to 15, with 1 being the highest priority
Application Program Identifier (Program ID) F: b T: 9F5A L: var. 1-16 S: Card P: Q M, Shared D: –	Optional	Visa proprietary data element identifying the Application Program ID of the card application. When personalized, the Application Program ID is returned in the FCI Issuer Discretionary Data of the Select response (tag 'BF0C'). qVSDC readers that support Dynamic Reader Limits (DRL) functionality examine the Application Program ID to determine the Reader Limit Set to apply.	UC: Unchanging IU: N R: SELECT	Byte 1: bits 8-5: 0000b = Visa global use 0001b = US 0010b = Canada 0011b = VE 0100b = AP 0101b = LAC 0110b = CEMEA bits 4-1: Visa regional discretion Bytes 2-16: Visa regional discretion Application Program ID byte 1 bits 8-5 are assigned to each Visa region. Application Program ID byte 1 bits 4-1 and bytes 2-16 are assigned at the discretion of each Visa region.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Application Transaction Counter (ATC) F: b 16 T: 9F36 L: 2 S: Card P: Q M, Shared D: Shared	qVSDC: Mandatory MSD: Mandatory (if Application Cryptogram returned by card) Required (otherwise)	Count of the number of transactions initiated since personalization. Maintained by the application in the card.	UC: Persistent IU: N R: GET DATA (SD), GPO	Implementations may support personalizing the ATC with an initial value. Initial value is zero unless optionally personalized to an initial starting value. The ATC is incremented by 1 each time a transaction is performed. If the ATC reaches its maximum value, then the application is permanently blocked as specified in Req 6.7 (Application Permanently Blocked).
Application Usage Control (AUC) F: b 16 T: 9F07 L: 2 S: Card P: Q D: E or S	Conditional If supporting cash or cashback	Indicates issuer-specified restrictions on the geographic usage and services allowed for the card application.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Byte 1 bit 8: 1 = Valid for domestic cash transactions bit 7: 1 = Valid for international cash transactions bits 6-1: Not used for VCPS Byte 2 bit 8: 1 = Domestic cashback allowed bit 7: 1 = International cashback allowed bits 6-1: RFU (000000) *Note*: Application Usage Control restrictions for "domestic" and "international" transactions are determined (by the reader) by comparing the Issuer Country Code to the Terminal Country Code.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Authorization Code F: ans 6 * T: 89 L: 6 S: Issuer P: Q D: – * (special characters limited to spaces)	Conditional If Issuer Update Processing supported (From issuer, not passed to card)	Nonzero value generated by the issuer for an approved transaction.	N/A	
Authorization Response Code (ARC) F: an 2 T: 8A L: 2 S:Issuer/Reader P: Q D: –	Conditional If Issuer Update Processing supported	Indicates the transaction disposition of the transaction received from the issuer for online authorizations.	N/A	Codes generated by the issuer are as indicated in [ISO 8583]:1987. • 00, 10, or 11 indicates an issuer approval. • 01 or 02 indicates an issuer referral. • An ARC other than the ones listed above indicates an issuer decline. The following codes are generated by the reader-terminal for the following conditions: • Y1 = Offline approved • Z1 = Offline declined • Y3 = Unable to go online (offline approved) • Z3 = Unable to go online (offline declined)

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Available Offline Spending Amount (AOSA) F: n 12 T: 9F5D L: 6 S: Card P: Q D: Shared	Optional	Visa proprietary data element indicating the remaining amount available to be spent offline. The AOSA is a calculated field used to allow the reader to print or display the amount of offline spend that is available on the card. The card shall not allow this tag to be returned in the GET DATA and GPO response unless this tag is personalized with a value greater than zero. Personalization of this data element does not impact its inclusion in the Issuer Discretionary Data portion of the Issuer Application Data.	UC: Transient IU: N R: GET DATA (SD), GPO	GET DATA of this data element is permitted if it is personalized with a value greater than 0. Inclusion of this data element in the GPO response is permitted if it is personalized with a value of '01' and CAP byte 1 bit 1 is 1b. The Available Offline Spending Amount shall be calculated as follows: If 'Low Value Check supported' by card (CAP byte 1 bit 8 is 1b), then AOSA = VLP Available Funds. Else, If 'Low Value AND CTTA Check supported' by card (CAP byte 1 bit 7 is 1b): AOSA = CTTA Funds Else, AOSA = CTTAL – CTTA If the AOSA cannot be calculated or is a negative value, then the card shall return the AOSA as a value of all zeros.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Card Additional Processes (CAP) F: b 32 T: 9F68 L: 4 S: Card P: Q M, Shared D: Shared	qVSDC: Required * * Card Additional Processes is not required to be personalized for Streamlined qVSDC MSD: Conditional If ODA for Online Authorizations supported	Indicates card processing requirements and preferences.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Byte 1 bit 8: 1 = Low Value Check supported bit 7: 1 = Low Value AND CTTA Check supported bit 6: 1 = Count qVSDC online transactions bit 5: 1 = Streamlined qVSDC supported bit 4: 1 = PIN Tries Exceeded Check supported bit 3: 1 = Offline international transactions are allowed bit 2: 1 = Card Prefers Contact Chip *Note*: Byte 1 bit 2 is used to indicate that the card application prefers contact chip transactions (at contact chip capable devices) to reset risk management parameters or when a contactless transaction is not possible. bit 1: 1 = Return Available Offline Spending Amount (AOSA) Byte 2 bit 8: 1 = Include country code in determining international transactions bit 7: 1 = International transactions are not allowed bit 6: 1 = Disable Offline Data Authentication (ODA) for Online Authorizations bit 5: 1 = Issuer Update Processing supported bits 4-1: RFU (0000)

– continues –

Name (Format; Tag; Length; Source; Path; Dual Interface)	**Requirement**	**Description**	**Update Capability; Issuer Update; Retrieval; Secret**	**Values**
Card Additional Processes (continued)				Byte 3 bit 8: 1 = Online PIN supported for domestic transactions bit 7: 1 = Online PIN supported for international transactions bit 6: 1 = (Contact Chip) Offline PIN supported bit 5: 1 = Signature supported bits 4-1: RFU (0000) Byte 4 RFU ('00')
Card Authentication Related Data F: b T: 9F69 L: var. 7-16 S: Card P: Q M_C D: –	Conditional If fDDA supported	Contains the fDDA Version Number, Card Unpredictable Number, and Card Transaction Qualifiers. For transactions where fDDA is performed, the Card Authentication Related Data is returned in the last record specified by the Application File Locator for that transaction. It is recommended to be personalized at the end of the record, as implementations may require it to be the last data element in the record.	UC: Unchanging (byte 1) Transient (bytes 2-7) IU: N R: READ RECORD	Byte 1: fDDA Version Number ('01') Byte 2-5: (Card) Unpredictable Number Byte 6-7: Card Transaction Qualifiers In this version of the specification, the Card Authentication Related Data personalized on the card has a length of 7 bytes, and is personalized with the value: '01 00 00 00 00 00 00' Card Authentication Related Data bytes 2-7 are replaced with the (Card) Unpredictable Number and Card Transaction Qualifiers values during VCPS transaction processing.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Card CVM Limit F: n 12 T: 9F6B L: 6 S: Card P: Q D: –	Optional	Visa proprietary data element indicating that for domestic contactless transactions where this value is exceeded, a CVM is required by the card. Online PIN and Signature are the CVMs supported by cards compliant to this specification.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Card Status Update (CSU) F: b 32 T: – L: 4 S: Issuer P: Q D: –	Optional Passed from the issuer through the reader	Indicates the disposition of the transaction and requested updates to the card, received from the issuer. The CSU is only used if Issuer Authentication is performed and passes. If ‘Set velocity-checking counters to Upper Limits’ will be used by the issuer (CSU byte 2 bits 2-1 are 01b), then the issuer shall personalize the upper limits for the supported velocity checks.	N/A	Byte 1 bit 8: 1 = Proprietary Authentication Data included bits 7-5: RFU (000) bits 4-1: PIN Try Counter Byte 2 bit 8: 1 = Issuer approves online transaction bit 7: 1 = Card block bit 6: 1 = Application block bit 5: 1 = Update PIN Try Counter bit 4: 1 = Set Go Online On Next Transaction *Note*: The ‘Set Go Online On Next Transaction’ bit is used by dual-interface cards, and does not impact VCPS transaction disposition processing. bit 3: 1 = CSU generated by proxy for the issuer bits 2-1: Update Counters 00 = Do not update offline counters 01 = Set velocity-checking counters to Upper Limits 10 = Reset velocity-checking counters to zero 11 = Not used for VCPS Byte 3: RFU ('00') Byte 4: Issuer discretionary (or '00')

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Card Transaction Qualifiers (CTQ) F: b 16 T: 9F6C L: 2 S: Card P: Q M_C, Exclusive D: –	Conditional If CVM supported or if issuer CTQ preferences supported or if Issuer Update Processing at the POS supported	In this version of the specification, used to indicate to the device the card CVM requirements, issuer preferences, and card capabilities.	UC: Modifiable (byte 1 bits 6-1, byte 2 bits 6-1) Transient (byte 1 bits 8-7, byte 2 bits 8-7) IU: PUT DATA R: GET DATA (SD), GPO	Byte 1 bit 8: 1 = Online PIN Required bit 7: 1 = Signature Required bit 6: 1 = Go Online if Offline Data Authentication Fails and Reader is online capable. bit 5: 1 = Switch Interface if Offline Data Authentication fails and Reader supports VIS. bit 4: 1 = Go Online if Application Expired bit 3: 1 = Switch Interface for Cash Transactions bit 2: 1 = Switch Interface for Cashback Transactions bit 1: RFU (0) Byte 2 bit 8: 1 = Consumer Device CVM Performed *Note*: Bit 8 is not used by cards compliant to this specification, and is set to 0b. bit 7: 1 = Card supports Issuer Update Processing at the POS bits 6-1: RFU (000000)

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Card Verification Results (CVR) F: b 32 T: part of 9F10 L: 4 S: Card P: Q M, Shared D: Shared	Required	Visa proprietary data element indicating the exception conditions that occurred during the current and previous transaction. Transmitted to the reader in the Issuer Application Data.	UC: Unchanging (byte 1) Transient (bytes 2-4) IU: N R: GPO	Byte 1: Length indicator ('03') Byte 2: bits 8–7: 00 = AAC returned in second GENERATE AC 01 = TC returned in second GENERATE AC 10 = Second GENERATE AC not requested 11 = RFU bits 6–5: 00 = AAC returned in GPO 01 = TC returned in GPO 10 = ARQC returned in GPO 11 = RFU bit 4: 1 = Issuer Authentication performed and failed bits 3-1: Not used for VCPS Byte 3: bit 8: 1 = Not used for VCPS bit 7: 1 = PIN Try Limit exceeded bit 6: 1 = Exceeded velocity checking counters bit 5: Not used for VCPS bit 4: 1 = Issuer Authentication failure on last online transaction bits 3-1: Not used for VCPS *– continues –*

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Card Verification Results (CVR) (continued)				Byte 4: bits 8-5: Issuer Script Command Counter bit 4: 1 = Issuer Script processing failed on last transaction bits 3-1: Not used for VCPS
Cardholder Name F: ans 2-26 T: 5F20 L: 2-26 S: Card P: Q M, E or S D: E or S	Optional	Indicates cardholder name according to [ISO 7813].	UC: Unchanging IU: N R: GPO, READ RECORD	For some markets, including the cardholder name on the card will bring up privacy issues as it can be read along with the PAN information. The issuer should take precautions and investigate this situation before personalizing tag '5F20' or including the cardholder's real name in tag '5F20'. It is strongly recommended that this data element not be personalized with the cardholder's real name, and that a generic cardholder name should instead be personalized.
Certificate Authority Public Key F: b T: – L: – S: Reader P: Q D: N/A	Conditional If fDDA supported	Payment system public key used for dynamic data authentication.	N/A	Value generated by Visa and loaded to terminal by acquirer. Up to six Visa public keys must be supported.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Certificate Authority Public Key Check Sum F: b T: – L: 20 S: Reader P: Q D: N/A	Conditional If fDDA supported	A check value calculated on the concatenation of all parts of the Certificate Authority Public Key (RID, Certificate Authority Public Key Index, Certificate Authority Public Key Modulus, Certificate Authority Public Key Exponent) using SHA-1.	N/A	
Certificate Authority Public Key Exponent F: b T: – L: 1 or 3 S: Reader P: Q D: N/A	Conditional If fDDA supported	Value of the exponent part of the Certificate Authority Public Key.	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Certificate Authority Public Key Index (PKI) F: b 8 T: 8F L: 1 S: Card P: Q M_C, E or S D: E or S	Conditional If Offline Data Authentication supported	Identifies the Certificate Authority's public key in conjunction with the RID for use in offline data authentication.	UC: Unchanging IU: N R: READ RECORD	Values assigned by Visa.
Certificate Authority Public Key Index (PKI) F: b 8 T: 9F22 L: 1 S: Reader P: Q D: N/A	Conditional If fDDA supported	Identifies the Certificate Authority's public key in conjunction with the RID for use in offline static and dynamic data authentication.	N/A	Values assigned by Visa.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Certificate Authority Public Key Modulus F: b T: – L: N_{CA} (up to 248) S: Reader P: Q D: N/A	Conditional If fDDA supported	Value of the modulus part of the Certificate Authority Public Key.	N/A	
Command Template F: b T: 83 L: var. S: Reader P: Q M D: N/A	Required	Identifies the data field of a command message.	N/A	
Consecutive Transaction Counter (CTC) F: b 8 T: DF11 in BF56 L: 1 S: Card P: – D: Shared	Conditional If supported for VIS and Issuer Update Processing supported	Visa proprietary data element specifying the number of consecutive offline transactions that have occurred for the card application since the last time a transaction went online. This data element is not used during VCPS transactions, and is included in this appendix only because it may be reset during Issuer Update Processing.	UC: Dynamic IU: CSU, PUT DATA R: GET DATA (SD)	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Consecutive Transaction Counter International (CTCI) F: b 8 T: DF11 in BF57 L: 1 S: Card P: Q D: Shared	Conditional If international velocity checks supported	Visa proprietary data element specifying the number of consecutive offline international transactions that have occurred for the card application since the last time a transaction went online and Issuer Authentication requirements were met. This counter is not used in VCPS transaction processing (i.e. is considered as not present in the application) unless the application has been personalized to support international velocity checks.	UC: Dynamic IU: CSU, PUT DATA R: GET DATA (SD)	Initialized to zero. Incremented by 1 each time an international transaction is approved offline by the card application.
Consecutive Transaction Counter Limit (CTCL) F: b 8 T: 9F58 L: 1 S: Card P: – D: Shared	Conditional If supported for VIS and Issuer Update Processing supported	Issuer-specified preference for the maximum number of consecutive offline transactions allowed for this card application before the card requires online processing. This data element is not used during VCPS transactions, and is included in this appendix only because it is referenced in this specification.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Consecutive Transaction Counter Upper Limit (CTCUL) F: b 8 T: 9F59 L: 1 S: Card P: – D: Shared	Conditional If supported for VIS and Issuer Update Processing supported	Issuer-specified preference for the maximum number of consecutive offline transactions allowed for this card application before the card requires online processing. This data element is not used during VCPS transactions, and is included in this appendix only because it may be used during Issuer Update Processing.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	
Consecutive Transaction International Upper Limit (CTIUL) F: b 8 T: 9F5E and DF31 in BF57 L: 1 S: Card P: Q D: Shared	Conditional If international velocity checking using CTIUL supported	Visa proprietary data element indicating issuer-specified preference for the maximum number of consecutive offline international transactions allowed before the transaction is declined offline if it cannot be processed online.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Consecutive Transaction Counter International Limit (CTCIL) F: b 8 T: 9F53 and DF21 in BF57 L: 1 S: Card P: Q D: Shared	Conditional If international velocity checks supported	Visa proprietary data element specifying the maximum number of consecutive offline international transactions allowed for that card application before a transaction is requested to go online.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	
Contact Chip Supported Indicator F: – T: – L: – S: Card P: Q D: –	Required	Visa proprietary internal indicator used during qVSDC Card Action Analysis. Indicates that a contact chip transaction is preferred by the card and EMV contact chip is supported by the reader.	UC: Transient IU: N R: N	This indicator is a transient value, initialized to a value of 0 at the beginning of the transaction. 1 = Contact chip transaction preferred by card and supported by reader

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Contactless Application Not Allowed Indicator F: – T: – L: – S: Reader P: Q M D: N/A	Required	Visa proprietary internal indicator used during reader transaction processing. Indicates that the transaction cannot be conducted with a Visa application.	N/A	This indicator is a transient value, initialized to a value of 0 at the beginning of the transaction. 1 = Visa contactless application not allowed
Contactless Counters Data Template F: b T: BF55 L: var. S: Card P: Q D: Shared	Conditional If contactless velocity checking (using any of the counters in this template) is supported	Visa proprietary data template that contains Visa proprietary context specific tags for contactless counters and their associated limits.	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context specific tags are defined in this specification for the Contactless Counters Data Template: 'DF11' – CLTC 'DF21' – CLTCLL 'DF31' – CLTCUL 'DF41' – VLP Single Transaction Limit 'DF51' – VLP Available Funds 'DF61' – VLP Reset Threshold 'DF71' – VLP Funds Limit

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Contactless Transaction Counter (CLTC) F: b 8 T: DF11 in BF55 L: 1 S: Card P: Q D: Shared	Conditional If contactless transaction count velocity checks supported	Visa proprietary data element specifying the number of qVSDC transactions that have occurred since the last time a transaction went online and Issuer Authentication requirements were met. This counter is not used in VCPS transaction processing (i.e. it is considered as not present in the application) unless the application has been personalized to support contactless transaction count velocity checks.	UC: Dynamic IU: CSU, PUT DATA R: GET DATA (SD)	Initialized to zero. Incremented by 1 each time a qVSDC transaction occurs.
Contactless Transaction Counter Lower Limit (CLTCLL) F: b 8 T: DF21 in BF55 L: 1 S: Card P: Q D: Shared	Conditional If contactless transaction count velocity checks supported	Visa proprietary data element specifying the maximum number of qVSDC transactions allowed before the card requests contact chip for the transaction (if supported) or online processing for the transaction (if supported), and proceeds offline if not.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Contactless Transaction Counter Upper Limit (CLTCUL) F: b 8 T: DF31 in BF55 L: 1 S: Card P: Q D: Shared	Conditional If contactless transaction count velocity checks supported	Visa proprietary data element specifying the maximum number of qVSDC transactions allowed before the card requests contact chip for the transaction (if supported) or online processing for the transaction(if supported), and declines the transaction if neither is supported.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	
Conversion Currency Code F: n 3 T: part of 9F73 L: 2 S: Card P: Q D: Shared	Conditional If currency conversion is to be performed	Visa proprietary data element in the Currency Conversion Parameters data element that identifies an alternate currency to be converted (using the corresponding Currency Conversion Factor) to the designated currency in which the account is managed (Application Currency Code) according to [ISO 4217].	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	
Counters Data Template F: b T: BF56 L: var. S: Card P: Q D: Shared	Conditional If dual-interface card application and contact velocity checking (using any of the counters in this template) supported	Visa proprietary data template that contains Visa proprietary context specific tags for contact counters and their associated limits.	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context specific tags are defined in this specification for the Counters Data Template: 'DF11' – CTC 'DF21' – CTCL 'DF31' – CTCUL

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Cryptogram Information Data (CID) F: b 8 T: 9F27 L: 1 S: Card P: Q D: N/A	Required	Indicates the type of cryptogram (TC, ARQC, or AAC) returned by the card and the actions to be performed by the reader.	UC: Transient IU: N R: GPO	bits 8–7 00 = AAC 01 = TC 10 = ARQC 11 = RFU bits 6-5: RFU (00) bits 4-1: Not used for VCPS
Cryptogram Version Number F: b 8 T: part of 9F10 L: 1 S: Card P: Q M, E or S D: E or S	Required	Visa proprietary data element indicating the version of the Application Cryptogram algorithm used by the application. Transmitted in the Issuer Application Data.	UC: Modifiable IU: N R: GPO	Values assigned by Visa. The only values supported in this version of VCPS are: '0A' = Cryptogram Version Number 10 (not supported for MSD) '11' = Cryptogram Version Number 17 '12' = Cryptogram Version Number 18 (not supported for MSD)
Cumulative Total Transaction Amount (CTTA) F: n 12 T: – L: 6 S: Card P: Q D: Shared	Conditional If Low Value AND CTTA Check supported	Visa proprietary data element specifying the cumulative total amount of offline domestic transactions in the designated currency (Application Currency Code or supported Conversion Currency Codes) for the card application since the last completed online transaction where Issuer Authentication requirements were met.	UC: Dynamic IU: CSU, PUT DATA R: GPO (if included in the IDD as specified in Appendix E)	Initialized to zero. Incremented by the Amount, Approximated each time a domestic transaction is approved offline by the card application. Reset to zero after Issuer Authentication requirements are met.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Cumulative Total Transaction Amount Funds (CTTA Funds) F: n 12 T: – L: 6 S: Card P: Q D: –	Conditional If Low Value AND CTTA Check supported	Calculated value indicating the amount of offline funds available to spend in the Cumulative Total Transaction Amount.	UC: Transient IU: N R: N/A	Equal to the Cumulative Total Transaction Amount Upper Limit minus the Cumulative Total Transaction Amount (CTTAUL - CTTA). If the Cumulative Total Transaction Amount Upper Limit is not present, equal to the Cumulative Total Transaction Amount Limit minus the Cumulative Total Transaction Amount (CTTAL - CTTA).
Cumulative Total Transaction Amount Limit (CTTAL) F: n 12 T: 9F54 L: 6 S: Card P: Q D: Shared	Conditional If Low Value AND CTTA Check supported	Visa proprietary data element specifying the maximum total amount of offline domestic transactions in the designated currency (Application Currency Code or supported Conversion Currency Codes) allowed for the card application before a transaction is forced to go online.	UC: Modifiable IU: PUT DATA R: GET DATA (SD), GPO (if included in the IDD as specified in Appendix E)	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Cumulative Total Transaction Amount Upper Limit (CTTAUL) F: n 12 T: 9F5C L: 6 S: Card P: Q D: Shared	Optional If Low Value AND CTTA Check supported	Visa proprietary data element specifying the maximum total amount of offline transactions in the designated currency or supported conversion currency codes for the card application before a transaction is declined after an online transaction is unable to be performed. Personalization of the CTTAUL is strongly recommended if the Low Value AND CTTA check is supported.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	
Currency Conversion Factor F: n 8 T: part of 9F73 L: 4 S: Card P: Q D: Shared	Conditional If currency conversion is to be performed	Visa proprietary data element in the Currency Conversion Parameters data element. The Currency Conversion Factor specifies a decimal value used in the conversion algorithm to convert an amount in the currency identified by the corresponding Conversion Currency Code to the designated currency in which the application is managed. This rate is an approximation and should be limited to two significant digits.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Byte 1 bits 8-5: Number of positions the decimal separator shall be shifted from the right to obtain the factor. bits 4-1: The first digit of the currency conversion factor Bytes 2-4 The remaining six digits of the currency conversion factor

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Currency Conversion Parameters F: n T: 9F73 L: var. up to 30 S: Card P: Q D: Shared	Conditional If currency conversion is to be performed	Visa proprietary data element specifying the currency code and conversion factor for converting an amount in an alternate currency to an approximate value in the designated currency in which the account is managed. Conversion Parameters contains one or more sets consisting of a Conversion Currency Code and an associated Currency Conversion Factor. Applications that support Currency Conversion must be able to support up to five alternate currencies.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Bytes 1–2: Conversion Currency Code 1 Bytes 3–6: Currency Conversion Factor 1 Bytes 7–8: Conversion Currency Code 2 Bytes 9–12: Currency Conversion Factor 2 Bytes 13–14: Conversion Currency Code 3 Bytes 15–18: Currency Conversion Factor 3 Bytes 19–20: Conversion Currency Code 4 Bytes 21–24: Currency Conversion Factor 4 Bytes 25–26: Conversion Currency Code 5 Bytes 27–30: Currency Conversion Factor 5
Customer Exclusive Data (CED) F: b T: 9F7C L: var. up to 32 S: Card P: Q M, E or S D: –	Optional	Contains data for transmission to the issuer.	UC: Modifiable IU: PUT DATA, UPDATE RECORD R: GET DATA (SD), GPO, READ RECORD	Customer Exclusive Data, if personalized, consists of one or more Issuer elements. Each element in the CED consists of a 1-byte Visa proprietary Identifier, a 1-byte length, and a value. The Identifiers currently defined for the CED are: '01' – Issuer Proprietary Data '02' through 'FF' – RFU

Name (Format; Tag; Length; Source; Path; Dual Interface)	**Requirement**	**Description**	**Update Capability; Issuer Update; Retrieval; Secret**	**Values**
Data Encipherment DEA Key A F: b 64 T: – L: 8 S: Card P: Q D: Shared	Conditional If dual-interface card application where PIN updates supported and Issuer Update Processing supported	Visa proprietary data element containing an 8-byte DEA key used to support Issuer Script processing when enciphered data is contained in an Issuer Script Command. Data Encipherment DEA Key A is used for encipherment and Data Encipherment DEA Key B is used for decipherment. The derivation key methodology for unique DEA keys is described in [VIS] Appendix D.7.	UC: Unchanging IU: N R: N Secret	
Data Encipherment DEA Key B F: b 64 T: – L: 8 S: Card P: Q D: Shared	Conditional If dual-interface card application where PIN updates supported and Issuer Update Processing supported	Visa proprietary data element containing an 8-byte DEA key used to support Issuer Script processing when enciphered data is contained in an Issuer Script Command. Data Encipherment DEA Key A is used for encipherment and Data Encipherment DEA Key B is used for decipherment. The derivation key methodology for unique DEA keys is described in [VIS] Appendix D.7.	UC: Unchanging IU: N R: N Secret	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Decline Required by Card Indicator F: – T: – L: – S: Card P: Q D: –	Required	Visa proprietary internal indicator used during qVSDC Card Action Analysis. Indicates that the card requires the transaction to be declined offline.	UC: Transient IU: N R: N	This indicator is a transient value, initialized to a value of 0 at the beginning of GPO processing. 1 = Offline decline required by card
Decline Required by Reader Indicator F: – T: – L: – S: Reader P: Q D: N/A	Required	Visa proprietary internal indicator used during transaction processing to indicate that internal reader processes have indicated that the transaction should be declined.	N/A	This indicator is a transient value, initialized to a value of 0 at the beginning of the transaction. 1 = Offline decline required by reader
Dedicated File (DF) Name F: b 40-128 T: 84 L: 5-16 S: Card P: Q M, Shared D: Shared	Required	Identifies the name of the DF as described in [ISO 7816-4].	UC: Unchanging IU: N R: SELECT	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Derivation Key Index (DKI) F: b 8 T: part of 9F10 L: 1 S: Card P: Q M, Shared D: Shared	Required	Visa proprietary data element identifying to the issuer the appropriate issuer's derivation key to derive the card's unique DEA keys for online card and issuer authentication. (The DKI is not used by the card.) Passed to the terminal in Issuer Application Data.	UC: Modifiable IU: N R: GPO	Value assigned by the issuer. If not present, the default value passed is zero.
Directory Entry F: var. T: 61 L: var. S: Card P: Q M, Shared D: Exclusive	Mandatory	Contains one or more data objects relevant to an application directory entry according to [ISO 7816-5].	UC: Unchanging IU: N R: SELECT	
fDDA Version Number F: b 8 T: part of 9F69 L: 1 S: Card P: Q M_C D: –	Conditional If fDDA supported	Contains the version number for the fDDA version supported by the card	UC: Unchanging IU: N R: READ RECORD	'01' = fDDA Version Number 1

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
File Control Information (FCI) Issuer Discretionary Data F: var. T: BF0C L: var. up to 222 S: Card P: Q M, Shared D: E or S	Mandatory for PPSE Conditional for ADF If transaction logging supported	Issuer discretionary part of the FCI.	UC: Unchanging IU: N R: SELECT	
File Control Information (FCI) Proprietary Template F: var. T: A5 L: var. S: Card P: Q M, Shared D: E or S	Mandatory	Identifies the data objects proprietary to [EMV] in the FCI Template according to [ISO 7816-4].	UC: Unchanging IU: N R: SELECT	
File Control Information (FCI) Template F: var. T: 6F L: var. up to 252 S: Card P: Q M, Shared D: E or S	Mandatory	Identifies the FCI template according to [ISO 7816-4].	UC: Unchanging IU: N R: SELECT	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Form Factor Indicator (FFI) F: b 32 T: 9F6E L: 4 S: Card P: Q M, E or S D: –	Optional	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 regional representative regarding which form factors are supported for your region.	UC: Modifiable IU: PUT DATA, UPDATE RECORD R: GET DATA (SD), GPO, READ RECORD	Byte 1: Consumer Payment Device Form Factor bits 8-6: Form Factor Indicator Version Number All values not currently defined are RFU. Defines the meaning of Form Factor Indicator byte 1 bits 5-1, byte 2, and byte 3. The definition of FFI byte 1 bits 5-1, byte 2, and byte 3 are based on the Form Factor Indicator Version Number, and those definitions may vary for each Form Factor Indicator Version Number. 001 = Form Factor Indicator (FFI) Version Number 1 bits 5-1: Consumer Payment Device Form Factor All values not currently defined are RFU. The definitions listed below are for FFI version #1. 00000 = Standard card Card conforming to the physical dimensions for an ID-1 card type, as specified in [ISO 7811], regardless of its transactional capabilities (e.g. magstripe, contact chip, contactless).

– continues –

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Form Factor Indicator (FFI) (continued)				Byte 1, bits 5-1, continued 00001 = Mini-card Physical card form factor, but of reduced physical dimensions (height and width) from an ID-1 card type. 00010 = Non-card Form Factor Non-card form factor that is contactless-only and possesses no communication capability outside the existing financial infrastructure. Examples: Key fobs, watches, wristbands, rings, and stickers 00011 = Mobile Device Non-card form factor that is contactless-only, has consumer input capability, and possesses communication capability outside the existing financial infrastructure. Example: Cellular phones *– continues –*

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Form Factor Indicator (FFI) (continued)				Byte 2: Consumer Payment Device Features (for FFI Version #1) bit 8: 1 = Passcode Capable The Consumer Payment Device has the capability to protect financial transactions with a Passcode. This is separate from the PIN used during the financial transaction. bit 7: 1 = Signature Panel The Consumer Payment Device has a signature panel. bit 6: 1 = Hologram The Consumer Payment Device has a hologram. bit 5: 1 = CVV2 The Consumer Payment Device has CVV2, as defined in the Visa Payment Technology Standards Manual. bit 4: 1 = Two-way Messaging The Consumer Payment Device is able to exchange identifying information between the issuer and consumer. The method and means of this communication is at the discretion of the issuer. bits 3-1: RFU (000) *– continues –*

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Form Factor Indicator (FFI) (continued)				Byte 3 (for FFI Version #1) RFU ('00') Byte 4: Payment Transaction Technology bits 8-5: RFU (0000) bits 4-1: Payment Transaction Technology All values not currently defined are RFU. 0000 = Proximity Contactless interface using [ISO 14443] (including NFC)
Go Online On Next Transaction Indicator F: – T: – L: – S: Card P: Q D: Shared	Conditional If dual-interface card application supporting Issuer Update Processing and supporting CVN18	Visa proprietary data element indicating that subsequent VIS transactions should request online processing. This indicator is used in VIS, and is not evaluated in determining VCPS transaction dispositions. The "Go Online On Next Transaction Indicator" is included in this specification as it may be set and reset during Issuer Update Processing.	UC: Persistent IU: CSU R: N	Set to 1 if the ‘Set Go Online On Next Transaction’ bit of the last verified CSU was set to 1b. Reset to 0 if the ‘Set Go Online On Next Transaction’ bit of the last verified CSU was set to 0b.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Integrated Circuit Card (ICC) Private Key F: b T: – L: N_{IC} S: Card P: Q M_C, Shared D: Shared	Conditional If fDDA supported	Private key part of the ICC public key pair used for fast dynamic data authentication. This data element may take various forms, such as a modulus and secret exponent or Chinese Remainder Theorem coefficients.	UC: Unchanging IU: N R: N Secret	The card shall implement support for ICC key sizes up to and including 1408-bits. Card support for larger ICC key sizes is at implementer discretion.
Integrated Circuit Card (ICC) Public Key Certificate F: b T: 9F46 L: N_I S: Card P: Q M_C, E or S D: E or S	Conditional If fDDA supported	ICC Public Key certified by the issuer. It is strongly recommended that the Certificate Expiration Date (from the ICC Public Key Certificate) match the Application Expiration Date.	UC: Modifiable IU: N R: READ RECORD	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Integrated Circuit Card (ICC) Public Key Exponent F: b T: 9F47 L: 1 or 3 S: Card P: Q M_C, E or S D: E or S	Conditional If fDDA supported	ICC Public Key Exponent used for the verification of the Signed Dynamic Application Data.	UC: Unchanging IU: N R: READ RECORD	A value of '03' is recommended for performance reasons.
Integrated Circuit Card (ICC) Public Key Remainder F: b T: 9F48 L: $N_{IC} – N_I + 42$ S: Card P: Q M_C, E or S D: E or S	Conditional If fDDA supported and entire public key does not fit into certificate	Digits of the ICC Public Key Modulus which do not fit within the ICC Public Key Certificate.	UC: Unchanging IU: N R: READ RECORD	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
International Counters Data Template F: b T: BF57 L: var. S: Card P: Q D: Shared	Conditional If international velocity checking (using any of the counters in this template) is supported	Visa proprietary data template that contains Visa proprietary context specific tags for international counters and their associated limits.	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context specific tags are defined in this specification for the Counters Data Template: 'DF11' – CTCI 'DF21' – CTCIL 'DF31' – CTIUL
International Transaction Indicator F: – T: – L: – S: Card P: Q D: –	Conditional If domestic and international restrictions supported or If domestic and international velocity checks supported	Visa proprietary data element indicating whether the transaction is domestic or international, based on currency code, and may also take into account the country code (configured by the issuer in Card Additional Processes).	UC: Transient IU: N R: N	This indicator is a transient value, set or reset at the beginning of GPO processing. 1 = International transaction 0 = Domestic transaction

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Application Data F: b T: 9F10 L: var. up to 32 S: Card P: Q M, E or S D: E or S	qVSDC: Mandatory MSD: Mandatory (if Application Cryptogram returned by card) Required (otherwise)	Contains proprietary application data for transmission to the Issuer in an online transaction. The first byte indicates the length of the Visa discretionary data. The next 1-15 bytes consist of the concatenated Visa discretionary data. In this version of the specification, the field containing the Visa discretionary data consists of the following: • Length indicator ('06') (1 byte) • Derivation Key Index (1 byte) • Cryptogram Version Number (1 byte) • Card Verification Results (CVR) (4 bytes, including the 1-byte length indicator) If issuer discretionary data is present, then the Visa discretionary data is followed by one byte indicating the length of the issuer discretionary data. The next 1-15 bytes consist of the concatenated issuer discretionary data.	UC: Dynamic IU: N R: GPO	If the Issuer Discretionary Data is personalized with the Issuer Discretionary Data Identifier (IDD ID) and IDD Length as described in Appendix E, the application includes the IDD ID followed by the values of the following data elements in the Issuer Discretionary Data (see Issuer Discretionary Data Identifier for defined values).

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Authentication Data F: b 64-128 T: 91 L: 8-16 S: Issuer P: Q D: –	Optional Passed from the issuer through the reader	Issuer data transmitted to card for Issuer Authentication. The Issuer Authentication Data consists of the following for Cryptogram Version Number 10 ('0A') and Cryptogram Version Number 17 ('11'): • ARPC – first 8 bytes • Authorization Response Code – 2 bytes immediately following ARPC The Issuer Authentication Data consists of the following for Cryptogram Version Number 18 ('12'): • ARPC – first 4 bytes • CSU – 4 bytes immediately following ARPC • optional Proprietary Authentication Data – 1-8 bytes immediately following CSU	N/A	*Note:* For CVN18, the optional Proprietary Authentication Data is only supported for Field 55 issuers. The use of Proprietary Authentication Data is beyond the scope of this specification. *Note:* For CVN18, third bit map issuers may send the 2-byte Authorization Response Code (following the CSU) as part of Issuer Authentication Data sent in the online response, but the 'Proprietary Authentication Data included' bit of the CSU shall be set to 0b, and the Authorization Response Code shall not be processed as optional Proprietary Authentication Data when generating the ARPC.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Authentication Failure Indicator F: – T: – L: – S: Card P: Q D: Shared	Conditional If Issuer Update Processing supported	Visa proprietary data element indicating that Issuer Authentication was performed and failed.	UC: Persistent IU: N R: N	1 = Issuer Authentication was performed and failed
Issuer Code Table Index F: n 2 T: 9F11 L: 1 S: Card P: Q M, Shared D: E or S	Conditional If Application Preferred Name is personalized	Indicates the code table according to [ISO 8859] for displaying the Application Preferred Name.	UC: Unchanging IU: N R: SELECT	Values are: 01 = [ISO 8859], Part 1 02 = [ISO 8859], Part 2 03 = [ISO 8859], Part 3 04 = [ISO 8859], Part 4 05 = [ISO 8859], Part 5 06 = [ISO 8859], Part 6 07 = [ISO 8859], Part 7 08 = [ISO 8859], Part 8 09 = [ISO 8859], Part 9 10 = [ISO 8859], Part 10

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Country Code F: n 3 T: 5F28 L: 2 S: Card P: Q D: E or S	Conditional If Application Usage Control is supported	Indicates the country of the issuer, represented according to [ISO 3166].	UC: Unchanging IU: N R: READ RECORD	Shall match the value of tag '9F57'.
Issuer Country Code F: n 3 T: 9F57 L: 2 S: Card P: Q D: Shared	Conditional If country code restrictions supported	Visa proprietary data element indicating the country of the issuer, represented according to [ISO 3166].	UC: Unchanging IU: N R: GET DATA (SD)	Shall match the value of tag '5F28'.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Discretionary Data Identifier (IDD ID) F: b 8 T: part of 9F10 L: 1 S: Card P: Q M, E or S D: E or S	Optional	Visa proprietary data element indicating the format of the optional issuer discretionary data transmitted in the Issuer Application Data. See Appendix E for additional information on usage of the IDD ID.	UC: Transient (bit 8) Modifiable (bits 7-1) IU: N R: GPO	Bit 8 is a dynamic value and initialized to a value of 0b at the beginning of GPO processing. bit 8: 1 = Indication to the issuer that card and reader support Issuer Update Processing bits 7-5: RFU (000) bits 4-1: IDD Option ID: Identifies the contents in the remaining bytes of issuer discretionary data: '0' = Issuer-defined static data '1' = VLP Available Funds *Note:* IDD Option ID '1' will not be supported in future versions of the specification. Issuers should instead use IDD Option ID '3'. '2' = CTTA *Note:* IDD Option ID '2' will not be supported in future versions of the specification. Issuers should instead use IDD Option ID '4'. '3' = VLP Available Funds followed by CTTA '4' = CTTA followed by CTTAL '5' = AOSA '6' = AOSA followed by Last Successful Issuer Update ATC Register followed by Issuer Script Command Counter '7'-'F' = RFU

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Public Key Certificate F: b T: 90 L: N_{CA} S: Card P: Q M_C, E or S D: E or S	Conditional If Offline Data Authentication supported	Issuer's public key certified by a certificate authority for use in offline data authentication.	UC: Unchanging IU: N R: READ RECORD	
Issuer Public Key Exponent F: b T: 9F32 L: 1 or 3 S: Card P: Q M_C, E or S D: E or S	Conditional If Offline Data Authentication supported	Issuer public key exponent used for the verification of the ICC Public Key Certificate.	UC: Unchanging IU: N R: READ RECORD	A value of '03' is recommended for performance reasons.
Issuer Public Key Remainder F: b T: 92 L: $N_I – N_{CA} + 36$ S: Card P: Q M_C, E or S D: E or S	Conditional If Offline Data Authentication supported and entire public key does not fit into certificate	Portion of the Issuer Public Key Modulus which does not fit into the Issuer PK Certificate.	UC: Unchanging IU: N R: READ RECORD	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Script Command Counter (ISCC) F: b 4 T: – L: – S: Card P: Q D: Shared	Conditional If Issuer Update Processing supported	Visa proprietary data element that indicates the number of Issuer Script Commands containing secure messaging successfully processed by the card application. The ISCC may be configured to be a cyclic counter by setting 'Issuer Script Command Counter is cyclic' (ADA byte 3 bit 2 to 1b). If the ISCC is cyclic, then the ISCC is never reset, and counts from 0 (0000b) to 15 (1111b), after which it cycles back to 0 (0000b).	UC: Persistent IU: N R: GPO	bits 4–1: Number of Issuer Script Commands using secure messaging processed. If the ISCC is not cyclic, then a value of 'F' is equivalent to 15 or more Issuer Script Commands. If the ISCC is cyclic, then incrementing the ISCC when it has a value of 'F' cycles it back to '0'. Ex. 'F' + 1 = '0'
Issuer Script Failure Indicator F: – T: – L: – S: Card P: Q D: Shared	Conditional If Issuer Update Processing supported	Visa proprietary data element that indicates whether Issuer Script processing failed on a previous transaction.	UC: Persistent IU: N R: N	1 = Issuer Script processing failed on a previous transaction
Issuer Script Identifier F: b 32 T: 9F18 L: 4 S: Issuer P: Q D: –	Optional From issuer to reader. Not passed to card.	May be sent in authorization response from issuer when response contains Issuer Script. Assigned by the issuer to uniquely identify the Issuer Script.	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Script Results F: b T: 9F5B L: var. S: Reader P: Q D: N/A	Conditional If Issuer Update Processing supported	Indicates the results of Issuer Script processing. When the reader-terminal transmits this data element to the acquirer, in this version of VCPS, it is acceptable that only byte 1 is transmitted, although it is preferable for all five bytes to be transmitted.	N/A	Byte 1(Issuer Script Result): bits 8-5: Result of the Issuer Script processing performed by the reader: '0' = Issuer Script not performed '1' = Issuer Script processing failed '2' = Issuer Script processing successful bits 4-1: Sequence number of the Issuer Script Command: '0' = Not specified '1'–'E' = Sequence number 1-14 'F' = Sequence number 15 or above Bytes 2-5 (Issuer Script Identifier): Issuer Script Identifier received by the reader, if available; zero filled if not available. Mandatory if more than one Issuer Script Template was received by the reader-terminal. Bytes 1-5 are repeated for each Issuer Script Template processed by the reader-terminal, although in this version of VCPS, only one Issuer Script Template may be transmitted in the response message.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Issuer Script Template 1 F: b T: 71 L: var. S: Issuer P: Q D: –	Optional Passed from issuer through reader	Contains proprietary issuer data for transmission to the card.	N/A	[EMV] specifies that terminals and networks must support a total length for all issuer scripts in an online response of up to 128 bytes. Issuers may send longer issuer scripts only when the issuer knows that longer issuer scripts are supported by all entities transporting the script back to the card.
Issuer Script Template 2 F: b T: 72 L: var. S: Issuer P: Q D: –	Optional Passed from issuer through reader	Contains proprietary issuer data for transmission to the card.	N/A	[EMV] specifies that terminals and networks must support a total length for all issuer scripts in an online response of up to 128 bytes. Issuers may send longer issuer scripts only when the issuer knows that longer issuer scripts are supported by all entities transporting the script back to the card.
Issuer Update Processing Indicator F: – T: – L: – S: Card P: Q D: –	Required	Visa proprietary internal indicator used during qVSDC Card Action Analysis. Indicates that Issuer Update Processing supported by card and Issuer Update Processing supported by reader.	UC: Transient IU: N R: N	This indicator is a transient value, reset at the beginning of the transaction. 1 = Issuer Update Processing supported by card and reader

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Language Preference F: an 2 T: 5F2D L: 2-8 S: Card P: Q M, Shared D: E or S	Optional	1-4 languages stored in order of preference, each represented by 2 lower case alphabetical characters according to [ISO 639].	UC: Unchanging IU: N R: SELECT	
Last Contactless Application Cryptogram F: b 64 T: – L: 8 S: Card P: Q M, Shared D: Shared	Conditional If Issuer Update Processing supported	Visa proprietary data element containing the value of the Application Cryptogram generated during the last VCPS transaction. This data element is not used in VCPS transaction processing (i.e. is considered as not present in the application) unless the application has been personalized to support Issuer Update Processing.	UC: Persistent IU: N R: N	
Last Contactless Application Cryptogram Valid Indicator F: – T: – L: – S: Card P: Q M, Shared D: Shared	Conditional If Issuer Update Processing supported	Visa proprietary data element indicating whether the Last Contactless Application Cryptogram is valid for Issuer Update Processing. This data element is not used in VCPS transaction processing (i.e. is considered as not present in the application) unless the application has been personalized to support Issuer Update Processing.	UC: Persistent IU: N R: N	Initialized with a value of 0. 1 = Last Contactless Application Cryptogram valid 0 = Last Contactless Application Cryptogram invalid

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Last Online ATC Register F: b 16 T: 9F13 L: 2 S: Card P: Q D: Shared	Conditional If Issuer Update Processing supported	ATC value of the last transaction that went online and where issuer authentication was performed.	UC: Persistent IU: N R: GET DATA (SD)	
Last Successful Issuer Update ATC Register F: b 16 T: – L: 2 S: Card P: Q D: Shared	Conditional If Issuer Update Processing supported	Visa proprietary data element containing the ATC value from the last successful Issuer Update (either as a result of Issuer Authentication or issuer scripting).	UC: Persistent IU: N R: GPO (if included in the IDD as specified in Appendix E)	Initialized to a value of zeroes.
Log Entry F: b T: 9F4D L: 2 S: Card P: Q M, Shared D: Shared	Conditional If transaction logging supported	Data element indicating the location (SFI) and the maximum number of transaction log records.	UC: Unchanging IU: N R: SELECT	Byte 1: SFI containing the cyclic transaction log file. Byte 2: Maximum number of records in the transaction log file.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Log Format F: b T: 9F4F L: var. S: Card P: Q M, Shared D: Shared	Conditional If transaction logging supported	List in tag and length format of data elements that are logged by the transaction.	UC: Unchanging IU: N R: GET DATA (SD)	
Matching Currency Indicator F: – T: – L: – S: Card P: Q D: –	Required	Visa proprietary data element indicating whether the transaction is matching currency or non-matching currency. Transactions are considered matching currency when the Transaction Currency Code matches the Application Currency Code, or matches any of the supported Conversion Currency Codes.	UC: Transient IU: N R: N	This indicator is a transient value, set or reset at the beginning of GPO processing. 1 = Matching currency transaction 0 = Non-matching currency transaction
Merchant Name and Location F: ans T: 9F4E L: var. S: Reader P: Q D: N/A	Required (at reader)	Indicates the name and location of the merchant. The reader shall return the value of the Merchant Name and Location when requested by the card in a Data Object List.	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Message Authentication Code (MAC) DEA Key A F: b 64 T: – L: 8 S: Card P: Q M, Shared D: Shared	Conditional If Issuer Update Processing supported or Issuer Discretionary Data Options requiring MAC'ing supported	Visa proprietary data element containing an 8-byte DEA key used to support Issuer Script processing, and to generate the MAC for Issuer Discretionary Data Options. In the triple DES algorithm, the MAC DEA Key A is used for encipherment and the MAC DEA Key B is used for decipherment. The derivation key methodology for unique DEA keys is described in [VIS] Appendix D.7.	UC: Unchanging IU: N R: N Secret	
Message Authentication Code (MAC) DEA Key B F: b 64 T: – L: 8 S: Card P: Q M, Shared D: Shared	Conditional If Issuer Update Processing supported or Issuer Discretionary Data Options requiring MAC'ing supported	Visa proprietary data element containing an 8-byte DEA key used to support Issuer Script processing, and to generate the MAC for Issuer Discretionary Data Options. In the triple DES algorithm, the MAC DEA Key A is used for encipherment and the MAC DEA Key B is used for decipherment. The derivation key methodology for unique DEA keys is described in [VIS] Appendix D.7.	UC: Unchanging IU: N R: N Secret	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
MSD Offset F: b 8 T: 9F67 L: 1 S: Card P: Q M, Shared D: –	Conditional If dCVV or ATC Insertion Option supported	Specifies the offset from the beginning of Track 2 Equivalent Data (tag '57') to the first digit/nibble of the dCVV, as described in Appendix B.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	If the MSD Offset is not personalized, or is personalized with a value of zero, Track 2 Equivalent Data (tag '57') shall be returned exactly as it was personalized. Personalizing the MSD Offset with a value greater than zero indicates that the dCVV and ATC shall be calculated and inserted into Track 2 Equivalent Data for MSD Legacy transactions. bit 8: 1 = (ATC Insertion Option) Insert ATC into Track 2 Equivalent Data for all qVSDC and MSD CVN17 transactions bits 7-1: Offset from the beginning of Track 2 Equivalent Data to the first digit of the CVV placeholder (as described in Appendix B)
Offline Counter Initial Value F: b T: 9F63 L: var. S: Card P: Q D: Shared	Optional	Contains initial values for various counters to be set at personalization time. In this version of the specification, only the Consecutive Transaction Counter International (CTCI) can be initialized during personalization. If this tag is personalized, the CTCI will be set to the value indicated.	UC: Unchanging IU: N R: GET DATA (SD)	In this version of the specification the length of the field is 1 byte, indicating the initial value of the Consecutive Transaction Counter International (CTCI).

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Online Required by Card Indicator F: – T: – L: – S: Card P: Q D: –	Required	Visa proprietary internal indicator used during qVSDC Card Action Analysis. Indicates that the card requires online processing for the transaction, and will decline offline if online processing is unavailable.	UC: Transient IU: N R: N	This indicator is a transient value, reset at the beginning of GPO processing.
Online Required by Reader Indicator F: – T: – L: – S: Reader P: Q D: N/A	Required	Visa proprietary internal indicator used during transaction processing to indicate that internal reader processes have indicated that the transaction should be declined.	N/A	This indicator is a transient value, initialized to a value of 0 at the beginning of the transaction.
Personal Identification Number (PIN) Try Counter F: b 8 T: 9F17 L: 1 S: Card P: Q D: Shared	Conditional If supporting offline PIN for contact chip	Number of PIN tries remaining. Offline PIN is not supported for VCPS transactions. Data elements supporting offline PIN are only listed in this appendix because they are checked or updated in this specification. For additional information on offline PIN and it's associated data elements, see [VIS].	UC: Dynamic IU: CSU, PIN CHANGE/UNBLOCK R: GET DATA	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Personal Identification Number (PIN) Try Limit F: b 8 T: – L: 1 S: Card P: Q D: Shared	Conditional If supporting offline PIN for contact chip	Visa proprietary data element containing the issuer-specified maximum number of consecutive incorrect PIN tries allowed. Offline PIN is not supported for VCPS transactions. Data elements supporting offline PIN are only listed in this appendix because they are checked or updated in this specification. For additional information on offline PIN and it's associated data elements, see [VIS].	UC: Modifiable IU: N/A R: N	
Processing Options Data Object List (PDOL) F: b T: 9F38 L: var. S: Card P: Q M, Shared D: E or S	Mandatory	List of terminal/reader-related data objects (tags and lengths) requested by the card to be transmitted in the GET PROCESSING OPTIONS command.	UC: Unchanging IU: N R: SELECT	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Reader Contactless Floor Limit F: n 12 T: – L: 6 S: Reader P: Q D: N/A	Conditional If Pre-processing supported	Indicates the contactless floor limit of the reader for Visa applications. If the transaction amount is greater than the Reader Contactless Floor Limit, then the reader requires online processing for the transaction.	N/A	
Reader Contactless Transaction Limit F: n 12 T: – L: 6 S: Reader P: Q D: N/A	Conditional If Pre-processing supported	Indicates the contactless transaction limit of the reader for Visa applications. If the transaction amount is greater than or equal to the Reader Contactless Transaction Limit, then a Visa contactless transaction is not permitted. Switching the transaction over to another interface is permitted.	N/A	
Reader CVM Required Limit F: n 12 T: – L: 6 S: Reader P: Q D: N/A	Conditional If Pre-processing supported	Indicates the CVM limit of the reader for Visa applications. If the transaction amount is greater than or equal to the Reader CVM Required Limit, then the reader requires a CVM for the transaction.	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Response Message Template Format 1 F: var. T: 80 L: var. S: Card P: M D: –	Conditional If Online Cryptogram not required by reader	Contains the data objects (without tags and lengths) returned by the card in response to a command.	UC: Transient IU: N R: GPO	
Response Message Template Format 2 F: var. T: 77 L: var. S: Card P: Q M, Exclusive D: –	Required	Contains the data objects (with tags and lengths) returned by the card in response to a command.	UC: Transient IU: N R: GPO	
Short File Identifier F: b 8 T: 88 L: 1 S: Card P: Q M, E or S D: –	Conditional If returning record data for the transaction	Used in the commands related to an application elementary file (AEF) to identify the file. The SFI data object is a binary field with the three high-order bits set to zero.	UC: Unchanging IU: N R: N/A	Values are: 1–10: Governed by joint payment systems 11–20: Payment system specific 21–30: Issuer specific

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Signed Dynamic Application Data (SDAD) F: b T: 9F4B L: N_{IC} S: Card P: Q M_C, Excl. D: Exclusive	Conditional If fDDA supported	Dynamic signature generated by the card and validated by the reader during fDDA processing. The SDAD is issuer configurable to be returned in either the GPO response or in a record. Issuers should consider whether there is sufficient space in the GPO response to accommodate the SDAD and personalize accordingly.	UC: Transient IU: N R: GPO, READ RECORD	
Signed Static Application Data F: b T: 93 L: N_I S: Card P: Q_C M_C, E or S D: Exclusive	Conditional If ODA for Online Authorizations is supported and card is not capable of performing fDDA	Static signature generated from critical card data elements and personalized on the card. This variant of the Signed Static Application Data is not returned by the card when used at readers compliant to this specification, and SDA is neither performed nor supported by readers compliant to this specification. The card functionality is included in this specification only to allow for its potential use in special acceptance environments. Cards that are not capable of performing fDDA, but support Offline Data Authentication for Online Authorizations, use SDA and this variant of the Signed Static Application Data.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	The calculation of the Signed Static Application Data is as specified in [EMV] Book 2, with the following exception: • The Signed Data Format to be signed shall have a value of '93' (instead of '03'). See [EMV] Book 2 Table 3. Use of a Signed Data Format with value '93' prevents the Signed Static Application Data from being used in standard POS acceptance environments.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Static Data Authentication (SDA) Tag List F: – T: 9F4A L: var. S: Card P: Q M_C, E or S D: E or S	Optional	Contains list of tags of primitive data objects whose value fields are to be included in the ICC Public Key Certificate hash result.	UC: Unchanging IU: N R: READ RECORD	The SDA Tag List may not contain tags other than the tag for Application Interchange Profile (AIP).
Switch Interface Required by Card Indicator F: – T: – L: – S: Card P: Q D: –	Required	Visa proprietary internal indicator used during qVSDC Card Action Analysis. Indicates that the card requires the transaction be performed over another interface.	UC: Transient IU: N R: N	This indicator is a transient value, initialized to a value of 0 at the beginning of GPO processing.

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Terminal Country Code F: n 3 T: 9F1A L: 2 S: Reader P: Q D: N/A	Required	Indicates the country of the terminal represented according to [ISO 3166].	N/A	
Terminal Floor Limit F: b 32 T: 9F1B L: 4 S: Reader P: Q D: N/A	Conditional If Pre-processing supported and Reader Contactless Floor Limit is not present	Indicates the floor limit in the terminal.	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Terminal Transaction Qualifiers (TTQ) F: b 32 T: 9F66 L: 4 S: Reader P: Q M D: N/A	Required	Indicates reader capabilities, requirements, and preferences to the card. TTQ byte 2 bits 8-7 are transient values, and reset to zero at the beginning of the transaction. All other TTQ bits are static values, and not modified based on transaction conditions. TTQ byte 3 bit 7 shall be set by the acquirer-merchant to 1b.	N/A	Byte 1 bit 8: 1 = MSD supported bit 7: RFU (0) bit 6: 1 = qVSDC supported bit 5: 1 = EMV contact chip supported bit 4: 1 = Offline-only reader bit 3: 1 = Online PIN supported bit 2: 1 = Signature supported bit 1: 1 = Offline Data Authentication (ODA) for Online Authorizations supported. *Note:* Readers compliant to this specification set TTQ byte 1 bit 1 to 0b. Byte 2 bit 8: 1 = Online cryptogram required bit 7: 1 = CVM required bit 6: 1 = (Contact Chip) Offline PIN supported bits 5-1: RFU (00000) Byte 3 bit 8: 1 = Issuer Update Processing supported bit 7: 1 = Mobile functionality supported (Consumer Device CVM) bits 6-1: RFU (000000) Byte 4 RFU ('00')

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Terminal Verification Results (TVR) F: b 40 T: 95 L: 5 S: Reader P: Q D: N/A	Required	Status of the different functions as seen from the reader/terminal. For qVSDC transactions, all of the TVR bits sent online to the acquirer shall be set to 0b.	N/A	Byte 1: Not used for VCPS ('00') Byte 2: Not used for VCPS ('00') Byte 3: Not used for VCPS ('00') Byte 4: Not used for VCPS ('00') Byte 5: Not used for VCPS ('00')
Track 1 Discretionary Data F: ans T: 9F1F L: var. S: Card P: M D: E or S	Optional	Discretionary data from track 1 of the magnetic stripe according to the [VPTSM]. *Note*: The contents of Track 1 Discretionary Data for VCPS are not the same as for VIS.	UC: Modifiable IU: UPDATE RECORD R: GPO, READ RECORD	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Track 2 Equivalent Data F: b T: 57 L: var. up to 19 S: Card P: Q M, E or S D: E or S	Mandatory	Contains the data elements of the track 2 according to the [ISO 7813], excluding start sentinel, end sentinel, and LRC, as follows: • Primary Account Number: n, 12 to 19 • Field Separator ('D'): b • Expiration Date (YYMM): n 4 • Service Code: n 3 • PIN Verification Field (optional): n 5 • Discretionary Data ○ (i)CVV: n 3 ○ **or** dCVV placeholder (n 3), followed by ATC placeholder (n 4), followed by a 1-digit value (n 1) • Pad with 'F' if needed to ensure whole bytes.	UC: Modifiable * IU: UPDATE RECORD R: GPO, READ RECORD * If dCVV (and/or the ATC Insertion Option) is supported, then the dCVV placeholder (and/or the ATC placeholder) digits of Track 2 Equivalent Data are transient digits.	
Transaction Currency Code F: n 3 T: 5F2A L: 2 S: Reader P: Q D: N/A	Required	Indicates the currency code of the transaction according to [ISO 4217]. The implied exponent is indicated by the minor unit of currency associated with the Transaction Currency Code in [ISO 4217].	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	**Requirement**	**Description**	**Update Capability; Issuer Update; Retrieval; Secret**	**Values**
Transaction Date F: n 6 YYMMDD T: 9A L: 3 S: Reader P: Q D: N/A	Required	Local date that the transaction was authorized.	N/A	
Transaction Type F: n 2 T: 9C L: 1 S: Reader P: Q D: N/A	Required	Indicates the type of financial transaction, represented by the values of the first two digits of Processing Code as defined by Visa.	N/A	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Unique DEA Key A F: b 64 T: – L: 8 S: Card P: Q M, Shared D: Shared	Required	Proprietary Visa data element containing an 8-byte DEA key used for Online Card Authentication, Online Issuer Authentication, and AC generation. Also used for dCVV generation unless the Unique DEA Key for dCVV is personalized. In triple DES, the Unique DEA Key A is used for encipherment and the Unique DEA Key B is used for decipherment. The derivation key methodology for unique DEA keys is described in [VIS] Appendix D.7.	UC: Unchanging IU: N R: N Secret	
Unique DEA Key B F: b 64 T: – L: 8 S: Card P: Q M, Shared D: Shared	Required	Proprietary Visa data element containing an 8-byte DEA key used for Online Card Authentication, Online Issuer Authentication, and AC generation. Also used for dCVV generation unless the Unique DEA Key for dCVV is personalized. In triple DES, the Unique DEA Key A is used for encipherment and the Unique DEA Key B is used for decipherment. The derivation key methodology for unique DEA keys is described in [VIS] Appendix D.7.	UC: Unchanging IU: N R: N Secret	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Unique DEA Key for dCVV A F: b 64 T: – L: 8 S: Card P: M D: –	Conditional If dCVV supported and a different key is used for dCVV generation	Proprietary Visa data element containing an 8-byte DEA key used for dCVV generation. In triple DES, the Unique DEA Key for dCVV A is used for encipherment and the Unique DEA Key for dCVV B is used for decipherment.	UC: Unchanging IU: N R: N Secret	
Unique DEA Key for dCVV B F: b 64 T: – L: 8 S: Card P: M D: –	Conditional If dCVV supported and a different key is used for dCVV generation	Proprietary Visa data element containing an 8-byte DEA key used for dCVV generation. In triple DES, the Unique DEA Key for dCVV A is used for encipherment and the Unique DEA Key for dCVV B is used for decipherment.	UC: Unchanging IU: N R: N Secret	
Unpredictable Number (Card) F: b 32 T: part of 9F69 L: 4 S: Card P: Q M_C, Excl. D: –	Conditional If fDDA supported	Contains the card unpredictable number generated by the card and signed for fDDA. The Unpredictable Number (Card) is generated during GPO processing and returned in the last record as part of the Card Authentication Related Data.	UC: Transient IU: N R: READ RECORD	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
Unpredictable Number (Reader-Terminal) F: b 32 T: 9F37 L: 4 S: Reader P: Q D: N/A	Required	Value to provide variability and uniqueness to the generation of the application cryptogram.	N/A	
VLP Available Funds F: n 12 T: 9F79 and DF51 in BF55 L: 6 S: Card P: Q D: Shared	Conditional If Low Value Check supported or If Low Value AND CTTA Check supported	Visa proprietary data element that provides a counter that is decremented by the transaction amount for qVSDC offline approval requests. This data element is not used in VCPS transaction processing (i.e. is considered as not present in the application) unless one of the low value checks is supported.	UC: Dynamic IU: CSU R: GET DATA (SD), GPO (if included in the IDD as specified in Appendix E)	Initialized to a value of zeros. Issuers may personalize the VLP Available Funds with another initial value.
VLP Funds Limit F: n 12 T: 9F77 and DF71 in BF55 L: 6 S: Card P: Q D: Shared	Conditional If Low Value Check supported or If Low Value AND CTTA Check supported	Visa proprietary data element that provides the issuer limit for the VLP Available Funds, and is the value to which the VLP Available Funds is reset.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	

Name (Format; Tag; Length; Source; Path; Dual Interface)	Requirement	Description	Update Capability; Issuer Update; Retrieval; Secret	Values
VLP Reset Threshold F: n 12 T: 9F6D and DF61 in BF55 L: 6 S: Card P: Q D: Shared	Optional	Visa proprietary data element specifying the minimum value to which the VLP Available Funds is allowed to be decremented before the card requests online processing.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	
VLP Single Transaction Limit F: n 12 T: 9F78 and DF41 in BF55 L: 6 S: Card P: Q D: –	Optional	Visa proprietary data element indicating the maximum amount allowed for a single qVSDC offline transaction.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	

D.2 Data Element Tags

Table D-2: Data Element Tags

Template	Tag	Data Element	Source
	4F	**Application Identifier (ADF Name)**	Card
	50	**Application Label**	Card
	57	**Track 2 Equivalent Data**	Card
	5A	**Application Primary Account Number (PAN)**	Card
	5F20	**Cardholder Name**	Card
	5F24	**Application Expiration Date**	Card
	5F28	**Issuer Country Code**	Card
	5F2A	**Transaction Currency Code**	Reader
	5F2D	**Language Preference**	Card
	5F34	**Application Primary Account Number Sequence Number (PSN)**	Card
	61	**Directory Entry**	Card
	6F	**File Control Information (FCI) Template**	Card
	71	**Issuer Script Template 1**	Issuer
	72	**Issuer Script Template 2**	Issuer
	77	**Response Message Template Format 2**	Card
	80	**Response Message Template Format 1**	Card
	82	**Application Interchange Profile (AIP)**	Card
	83	**Command Template**	Reader
	84	**Dedicated File (DF) Name**	Card
	87	**Application Priority Indicator**	Card
	88	**Short File Identifier**	Card
	89	**Authorization Code**	Issuer
	8A	**Authorization Response Code (ARC)**	Issuer/Reader
	8F	**Certificate Authority Public Key Index (PKI)**	Card
	90	**Issuer Public Key Certificate**	Card
	91	**Issuer Authentication Data**	Issuer
	92	**Issuer Public Key Remainder**	Card
	93	**Signed Static Application Data (SAD)**	Card
	94	**Application File Locator (AFL)**	Card
	95	**Terminal Verification Results (TVR)**	Reader

Template	Tag	Data Element	Source
	9A	**Transaction Date**	Reader
	9C	**Transaction Type**	Reader
	9F02	**Amount, Authorized (Numeric)**	Reader
	9F03	**Amount, Other (Numeric)**	Reader
	9F06	**Application Identifier (AID)**	Reader
	9F07	**Application Usage Control (AUC)**	Card
	9F10	**Issuer Application Data**	Card
	part of 9F10	**Card Verification Results (CVR)**	Card
	part of 9F10	**Cryptogram Version Number**	Card
	part of 9F10	**Derivation Key Index (DKI)**	Card
	part of 9F10	**Issuer Discretionary Data Identifier (IDD ID)**	Card
	9F11	**Issuer Code Table Index**	Card
	9F12	**Application Preferred Name**	Card
	9F13	**Last Online ATC Register**	Card
	9F17	**PIN Try Counter**	Card
	9F18	**Issuer Script Identifier**	Issuer
	9F1A	**Terminal Country Code**	Reader
	9F1B	**Terminal Floor Limit**	Reader
	9F1F	**Track 1 Discretionary Data**	Card
	9F22	**Certificate Authority Public Key Index (PKI)**	Reader
	9F26	**Application Cryptogram**	Card
	9F27	**Cryptogram Information Data (CID)**	Card
	9F32	**Issuer Public Key Exponent**	Card
	9F36	**Application Transaction Counter (ATC)**	Card
	9F37	**Unpredictable Number (Reader-Terminal)**	Reader
	9F38	**Processing Options Data Object List (PDOL)**	Card
	9F46	**Integrated Circuit Card (ICC) Public Key Certificate**	Card
	9F47	**Integrated Circuit Card (ICC) Public Key Exponent**	Card
	9F48	**Integrated Circuit Card (ICC) Public Key Remainder**	Card
	9F4A	**Static Data Authentication (SDA) Tag List**	Card
	9F4B	**Signed Dynamic Application Data (SDAD)**	Card
	9F4D	**Log Entry**	Card
	9F4E	**Merchant Name and Location**	Reader

Template	Tag	Data Element	Source
	9F4F	**Log Format**	Card
	9F51	**Application Currency Code**	Card
	9F52	**Application Default Action (ADA)**	Card
	9F53	**Consecutive Transaction Counter International Limit (CTCIL)**	Card
	9F54	**Cumulative Total Transaction Amount Limit (CTTAL)**	Card
	9F57	**Issuer Country Code**	Card
	9F58	**Consecutive Transaction Counter Limit (CTCL)**	Card
	9F59	**Consecutive Transaction Counter Upper Limit (CTCUL)**	Card
	9F5A	**Application Program Identifier (Program ID)**	Card
	9F5B	**Issuer Script Results**	Reader
	9F5C	**Cumulative Total Transaction Amount Upper Limit (CTTAUL)**	Card
	9F5D	**Available Offline Spending Amount (AOSA)**	Card
	9F5E	**Consecutive Transaction International Upper Limit (CTIUL)**	Card
	9F63	**Offline Counter Initial Value**	Card
	9F66	**Terminal Transaction Qualifiers (TTQ)**	Reader
	9F67	**MSD Offset**	Card
	9F68	**Card Additional Processes**	Card
	9F69	**Card Authentication Related Data**	Card
	part of 9F69	**fDDA Version Number**	Card
	part of 9F69	**Unpredictable Number (Card)**	Card
	9F6B	**Card CVM Limit**	Card
	9F6C	**Card Transaction Qualifiers (CTQ)**	Card
	9F6D	**VLP Reset Threshold**	Card
	9F6E	**Form Factor Indicator (FFI)**	Card
	9F73	**Currency Conversion Parameters**	Card
	part of 9F73	**Conversion Currency Code**	Card
	part of 9F73	**Currency Conversion Factor**	Card
	9F77	**VLP Funds Limit**	Card
	9F78	**VLP Single Transaction Limit**	Card
	9F79	**VLP Available Funds**	Card
	9F7C	**Customer Exclusive Data (CED)**	Card

Template	Tag	Data Element	Source
	A5	**File Control Information (FCI) Proprietary Template**	Card
	BF0C	**File Control Information (FCI) Issuer Discretionary Data**	Card
	BF55	**Contactless Counters Data Template**	Card
BF55	DF11	**Contactless Transaction Counter (CLTC)**	Card
BF55	DF21	**Contactless Transaction Counter Lower Limit (CLTCLL)**	Card
BF55	DF31	**Contactless Transaction Counter Upper Limit (CLTCUL)**	Card
BF55	DF41	**VLP Single Transaction Limit**	Card
BF55	DF51	**VLP Available Funds**	Card
BF55	DF61	**VLP Reset Threshold**	Card
BF55	DF71	**VLP Funds Limit**	Card
	BF56	**Counters Data Template**	Card
BF56	DF11	**Consecutive Transaction Counter (CTC)**	Card
	BF57	**International Counters Data Template**	Card
BF57	DF11	**Consecutive Transaction Counter International (CTCI)**	Card
BF57	DF21	**Consecutive Transaction Counter International Limit (CTCIL)**	Card
BF57	DF31	**Consecutive Transaction International Upper Limit (CTIUL)**	Card
	BF5B	**Application Internal Data Template**	Card
BF5B	DF01	**Application Capabilities**	Card

E Issuer Discretionary Data Options

Implementation-Conditional: Each of the Issuer Discretionary Data Options shall be implemented based on the following conditions:

- Support for Issuer Discretionary Data Option '0' shall be implemented.
- Support for Issuer Discretionary Data Options '1' through '5' shall be implemented if offline qVSDC is implemented.
- Support for Issuer Discretionary Data Option '6' shall be implemented if Issuer Update Processing is implemented.

Issuer-Optional: If implemented, use of the Issuer Discretionary Data Options is at issuer discretion.

E.1 Issuer Discretionary Data Options

In order to permit issuers to more closely track funds at the host, an issuer option was introduced to allow placement of specific data into the Issuer Discretionary Data portion of the Issuer Application Data (tag '9F10'). If personalized, the Issuer Discretionary Data is returned as part of the Issuer Application Data (whenever the Issuer Application Data is returned).

With the exception of IDD Option '0', the IDD data returned by the application is MACed to ensure data integrity when the application uses CVN10 or CVN17.

Note: The IDD data is also included in clearing messages for offline approvals.

E.2 Personalization for IDD

Issuer Discretionary Data (IDD), if present, shall be returned following the Visa Discretionary Data in the Issuer Application Data (tag '9F10').

The Issuer Discretionary Data (IDD) returned varies depending on the option chosen during personalization as described in Table E-1.

Table E-1: IDD Options

IDD Option	Length	IDDO ID	Amount Field(s)	MAC
Issuer-specified constant data	1 to 15 bytes	'0'	Issuer-specified constant data	none
VLP Available Funds	10 bytes	'1'	• Value of VLP Available Funds (5 low-order bytes) *Note:* IDDO ID '1' will not be supported in future versions of the specification. Issuers should instead use IDDO ID '3' or '5'.	4 bytes
Cumulative Total Transaction Amount (CTTA)	10 bytes	'2'	• Value of CTTA (5 low-order bytes) *Note:* IDDO ID '2' will not be supported in future versions of the specification. Issuers should instead use IDDO ID '3' or '4'.	4 bytes
VLP Available Funds and CTTA	15 bytes	'3'	• Value of VLP Available Funds (5 low-order bytes) • Value of CTTA (5 low-order bytes)	4 bytes
CTTA and Cumulative Total Transaction Amount Limit (CTTAL)	15 bytes	'4'	• Value of CTTA (5 low-order bytes) • Value of CTTAL (5 low-order bytes)	4 bytes
Available Offline Spending Amount (AOSA)	10 bytes	'5'	• Value of AOSA (5 low-order bytes)	4 bytes
AOSA and Last Successful Issuer Update ATC Register and Issuer Script Command Counter	14 bytes	'6'	• Value of AOSA (6 bytes) • Value of Last Successful Issuer Update ATC Register (2 bytes) • Value of Issuer Script Command Counter (1 byte) *Note:* The Issuer Script Command Counter used in IDDO ID '6' is right-justified and left padded with 0000b to ensure a whole byte.	4 bytes

Note: The IDD Option ID is specified using the low order nibble of the IDD ID byte. The high order nibble of the IDD ID byte is reserved for other uses. For additional information, see the “Issuer Discretionary Data Identifier” entry in Table D-1.

The IDD Option ID value is used to choose the type of data to be returned in the Issuer Discretionary Data field. By default, Issuer Discretionary Data will not be returned. If the issuer wants to receive Issuer Discretionary Data, the above length byte and identifier byte should be appended to the tag '9F10' personalization value (following the Visa Discretionary Data).

For example, '0A02' would indicate that a 10-byte IDD should be returned in the Issuer Application Data, containing the Identifier ('02'), Cumulative Total Transaction Amount (CTTA), and MAC.

E.3 MAC Calculation

The data to be MACed is the 2-byte Application Transaction Counter (ATC), followed by the amount fields and padding characters, constructed as follows:

Table E-2: MAC Calculation

IDD Option ID	Length of Data Block	Elements	
'1'	8 bytes	ATC	2 bytes
		VLP Available Funds	5 low-order bytes
		padding	1 byte
'2'	8 bytes	ATC	2 bytes
		Cumulative Total Transaction Amount (CTTA)	5 low-order bytes
		padding	1 byte
'3'	16 bytes	ATC	2 bytes
		VLP Available Funds	5 low-order bytes
		Cumulative Total Transaction Amount (CTTA)	5 low-order bytes
		padding	4 bytes
'4'	16 bytes	ATC	2 bytes
		Cumulative Total Transaction Amount (CTTA)	5 low-order bytes
		Cumulative Total Transaction Amount Limit (CTTAL)	5 low-order bytes
		padding	4 bytes
'5'	8 bytes	ATC	2 bytes
		Available Offline Spending Amount	5 low-order bytes
		padding	1 byte
'6'	16 bytes	ATC	2 bytes
		IDD ID	1 byte
		AOSA	6 bytes
		Last Successful Issuer Update ATC Register	2 bytes
		Issuer Script Command Counter	1 byte
		Padding	4 bytes

The 4-byte MAC is generated using a session key derived from the MAC UDK using the first method defined in [VIS] Appendix B.4. Computation of the MAC is as illustrated in [VIS] Figure B-1.

E.4 Padding for IDD MAC Generation

There are two padding methods supported for generation of the IDD MAC.

The first method is similar to the padding method used for CVN 10. This is referred to as the padding method ‘00’, which adds as many bytes of ‘00’ as necessary to obtain a data block with a length divisible by eight (see [VIS] Appendix D.3.2, step 3).

The second method is referred to as the padding method ‘80’, which adds one mandatory ‘80’ byte at the end of the data block and as many bytes of ‘00’ as necessary to obtain a data block with a length divisible by eight. The method is identical to the padding method for [VIS] Secure Messaging for Integrity and Authentication, as described in [VIS] Appendix B.2.4, step 4.

In order for the card to recognize the padding method chosen by the issuer, the Application Default Action indicates the padding method to be used when generating the MAC for inclusion in the Issuer Discretionary Data as follows:

- If ‘Padding method '80'’ is supported (ADA byte 4 bit 5 is 1b), then padding method '80' shall be used.
- If ‘Padding method '80'’ is not supported (ADA byte 4 bit 5 is 0b), then padding method '00' shall be used.

E.5 Issuer Application Data Personalization Example

Visa Discretionary Data (Mandatory)

Length:	'06'	
Value:	'010A03000000'	(assuming CVN 10)

Issuer Discretionary Data

Length:	'0A'	(expected amount length when Issuer Application Data returned)
Value:	'02'	(ID to request Cumulative Total Transaction Amount (CTTA))

The TLV for the above example would be as follows:

```
'9F 10 09
    06 01 0A 03000000
    0A 02'
```

The application uses the personalized IDD length and ID ('0A 02') as an indicator to activate code to supply the Cumulative Total Transaction Amount (CTTA) in the Issuer Discretionary Data when returning the Issuer Application Data. The personalized length includes the MAC.

When the card responds with Issuer Application Data containing the IDD (with the CTTA value = '112233445566', and the MAC = '1A2B3C4D'), the TLV for this example would be:

Tag: '9F10'

Length: '12'

Value: '06010A030000000A0222334455661A2B3C4D'

F Creating Track 1 and Track 2

This appendix describes how an MSD reader shall create Track 1 and Track 2 using information personalized on a card by the issuer as well as how the issuer shall personalize the information used by the reader to build Track 1 and Track 2.

F.1 Creating Track 1

Building Track 1 is an option for MSD readers. If the reader supports the option, this appendix specifies how the reader shall assemble Track 1 using information on the card.

Issuers shall personalize Track 2 Equivalent Data and may in addition personalize two other data elements – Cardholder Name and Track 1 Discretionary Data – that are used to assemble Track 1. If one or both additional data elements are not personalized on the card, the reader will still be able to assemble Track 1 using data elements from Track 2 and default values as specified in this appendix.

Track 1 is assembled using the data elements listed in Table F-1 below.

Table F-1: Data Elements Required for Track 1 and Track 2

Tag	Value	Format	Length	Presence
57	Track 2 Equivalent Data	b	Up to 19	M
5F20	Cardholder Name	ans	2 to 26	O
9F1F	Track 1 Discretionary Data	ans	var.	O

The format of Track 1 data and how to assemble it from the data elements mentioned in Table F-1 is shown in Table F-2.

Table F-2: Track 1 Format

Field #	Field Name	Length	Value
Field 1	Start Sentinel	1	'%'
Field 2	Format Code	1	'B'
Field 3	Primary Account Number (PAN)	var – up to 19	Content of tag '57', position 1 through last position before separator 'D'
Field 4	Field Separator	1	' ^ '
Field 5	Cardholder Name	var – 2 to 26	Content of tag '5F20' or set to default value “space/” - '202F’
Field 6	Field Separator	1	' ^ '
Field 7	Card Expiration Date	4	Content of tag '57', position 1 through 4 following separator 'D'
Field 8	Service Code	3	Content of tag '57', position 5 through 7 following separator 'D'
Field 9	PIN Verification field (PVKI & PVV)	5	Content of tag '57', position 8 through 12 following separator 'D' if the PVV is present
Field 10.1	Track 1 Discretionary Data	see Appendix F.1.1	Content of tag '9F1F' or not present if tag '9F1F' is not present
Field 10.2	Contactless Indicator	1	Content of tag '57', position 20 following separator 'D' if the PVV is present in tag '57' or position 15 following the separator 'D' if PVV is not present
Field 11.1	ATC part 1	2	Content of tag '57', position 16 through 17 following separator 'D' if the PVV is present or position 11 through 12 following separator 'D' if the PVV is not present.
Field 11.2	dCVV	3	Content of tag '57', position 13 through 15 following separator 'D' if the PVV is present or position 8 through 10 following separator 'D' if the PVV is not present.
Field 11.3	ATC part 2	2	Content of tag '57', position 18 through 19 following separator 'D' if the PVV is present or position 13 through 14 following separator 'D' if the PVV is not present.
Field 11.4	Visa reserved	1	'0'
Field 11.5	Visa reserved	3	'000'
Field 12	End Sentinel	1	'?'
Field 13	LRC	1	

Whether or not PVV is present in Track 2 Equivalent Data (tag '57') can be determined from the number of digits after the separator 'D' in Track 2 Equivalent Data. If the number of digits following separator 'D' is 20 (excluding a possible padding of 'F'), the PVV is present, otherwise it is not.

For the content of Track 2 Equivalent Data (tag '57'), see Table F-6.

If tag '5F20' is present on the card, the reader shall in field 5 include the content of the tag and set its length to the length of the tag.

If tag '5F20' is not present on the card, the reader shall in field 5 include the default value '202F' (the value “space/”) and set the length to 2.

If tag '9F1F' is present on the card, the reader shall include the content of the tag in field 10.1 immediately followed by the Contactless Indicator from Track 2 in field 10.2.

If tag '9F1F' is not present on the card, the reader shall not include any default value in field 10.1, set its length to 0, and only include the Contactless Indicator from Track 2 in field 10.2.

If an incorrectly personalized card does not include dCVV, ATC, or Contactless Indicator in Track 2 Equivalent Data, the reader shall nevertheless build Track 1 using the following default values for the data that was not included: 000 for dCVV, 0000 for ATC and 1 for Contactless Indicator.

The maximum length of Track 1 is 79 characters.

F.1.1 Length of field 10.1

Length of field 10.1 is a variable value and shall be set to the length portion of the TLV value for tag '9F1F'. If tag '9F1F' is not present on the card, the length shall be set to 0 and no data inserted into field 10.1.

The maximum length of field 10.1 depends on the length of field 3 and field 5 compared to a maximum length of 79 for Track 1 – as described in this equation:

Maximum length of field 10.1 = 79 – 30 – length of field 3 – length of field 5

For example, if length of field 3 is 16 and length of field 5 is the maximum 26, the maximum length of field 10.1 is 7.

If the content of tag '9F1F' cannot fit within the available space in Track 1, the content shall be right truncated.

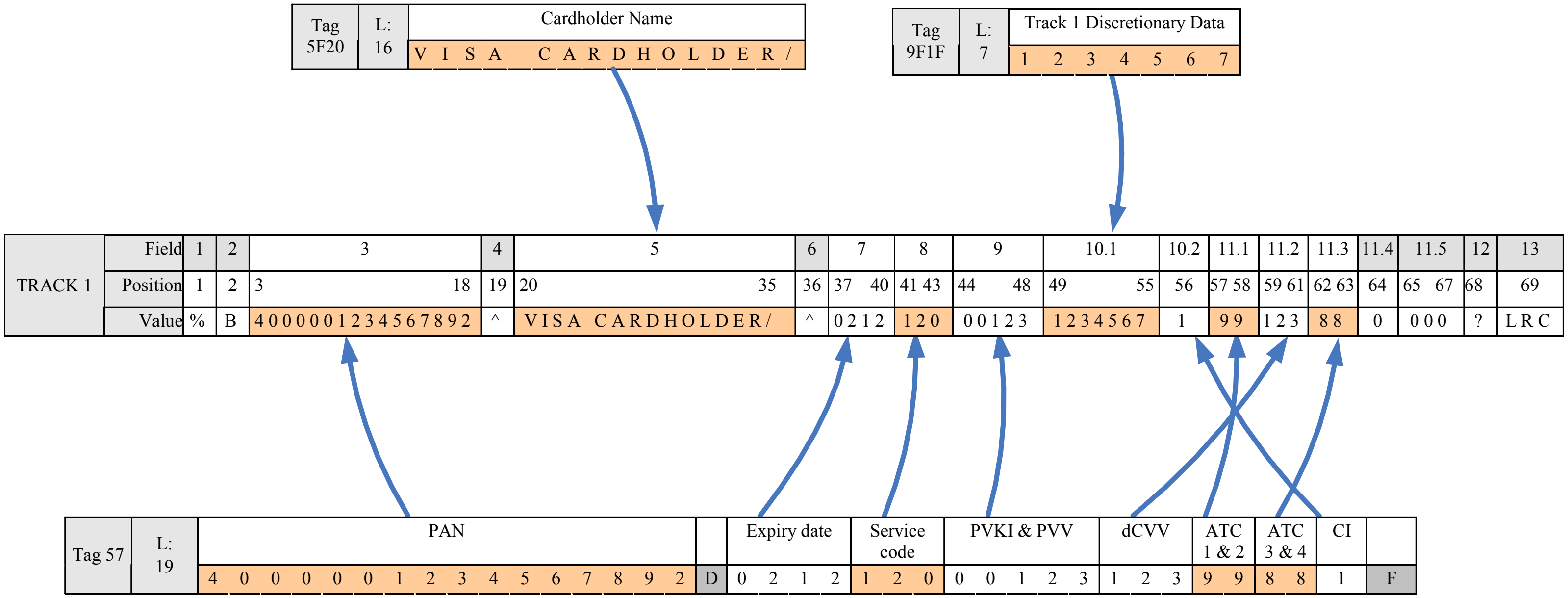
F.1.2 Examples of assembling Track 1

Example 1

In order to illustrate how Track 1 is assembled, the following examples can be used. All of the examples are based on a PAN of 16 digits within Track 2 Equivalent Data.

The first example is outlined in Figure F-1 based on a Cardholder Name of 16 positions and a Track 1 Discretionary Data of 7 positions. This gives a Track 1 as outlined in Table F-3.

Figure F-1: Constructing Track 1 Data – Example 1



Tag 5F20	L: 16	Cardholder Name
		V I S A C A R D H O L D E R /

Tag 9F1F	L: 7	Track 1 Discretionary Data
		1 2 3 4 5 6 7

TRACK 1	Field	1	2	3	4	5	6	7	8	9	10.1	10.2	11.1	11.2	11.3	11.4	11.5	12	13
	Position	1	2	3 18	19	20 35	36	37 40	41 43	44 48	49 55	56	57 58	59 61	62 63	64	65 67	68	69
	Value	%	B	4000001234567892	^	VISA CARDHOLDER/	^	0212	120	00123	1234567	1	99	123	88	0	000	?	LRC

Tag 57	L: 19	PAN		Expiry date	Service code	PVKI & PVV	dCVV	ATC 1 & 2	ATC 3 & 4	CI	
		4 0 0 0 0 0 1 2 3 4 5 6 7 8 9 2	D	0 2 1 2	1 2 0	0 0 1 2 3	1 2 3	9 9	8 8	1	F

Note: Length of tag '57' is measured in bytes while the actual digits are shown.

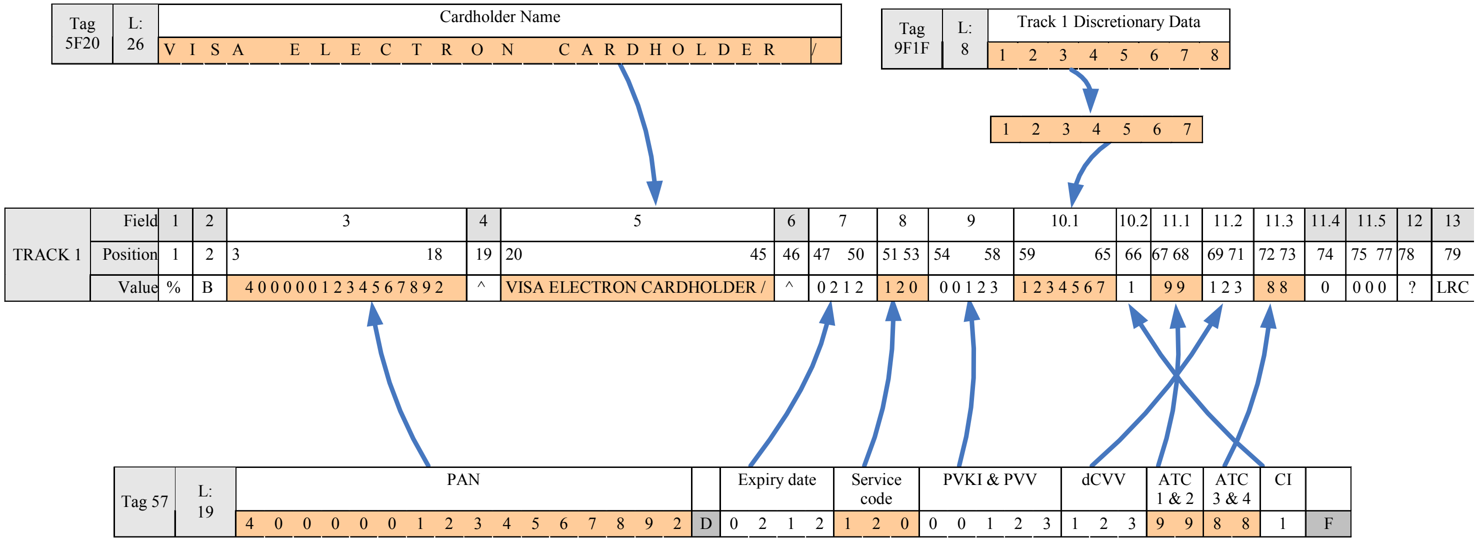
Table F-3: Example 1 of Track 1 Format

Field #	Field Name	Position	Length	Value
Field 1	Start Sentinel	1	1	'%'
Field 2	Format Code	2	1	'B'
Field 3	Primary Account Number (PAN)	3	16	Content of tag '57', position 1 through 16
Field 4	Field Separator	19	1	' ^ '
Field 5	Cardholder Name	20	16	Content of tag '5F20'
Field 6	Field Separator	36	1	' ^ '
Field 7	Card Expiration Date	37	4	Content of tag '57', position 18 through 21
Field 8	Service Code	41	3	Content of tag '57', position 22 through 24
Field 9	PIN Verification field (PVKI & PVV)	44	5	Content of tag '57', position 25 through 29
Field 10.1	Track 1 Discretionary Data	49	7	Content of tag '9F1F'
Field 10.2	Contactless Indicator	56	1	Content of tag '57', position 37
Field 11.1	ATC part 1	57	2	Content of tag '57', position 33 through 34
Field 11.2	(d)CVV	59	3	Content of tag '57', position 30 through 32
Field 11.3	ATC part 2	62	2	Content of tag '57', position 35 through 36
Field 11.4	Visa reserved	64	1	'0'
Field 11.5	Visa reserved	65	3	'000'
Field 12	End Sentinel	68	1	'?'
Field 13	LRC	69	1	

Example 2

The next example is outlined in Figure F-2 based on a Cardholder Name of 26 positions and a Track 1 Discretionary Data of 8 positions. Observe this example truncates the data in tag '9F1F'. The result is outlined in Table F-4.

Figure F-2: Constructing Track 1 Data – Example 2



Tag 5F20	L: 26	Cardholder Name
		VISA ELECTRON CARDHOLDER /

Tag 9F1F	L: 8	Track 1 Discretionary Data
		1 2 3 4 5 6 7 8

1 2 3 4 5 6 7

TRACK 1	Field	1	2	3	4	5	6	7	8	9	10.1	10.2	11.1	11.2	11.3	11.4	11.5	12	13
	Position	1	2	3 18	19	20 45	46	47 50	51 53	54 58	59 65	66	67 68	69 71	72 73	74	75 77	78	79
	Value	%	B	4 0 0 0 0 0 1 2 3 4 5 6 7 8 9 2	^	VISA ELECTRON CARDHOLDER /	^	0 2 1 2	1 2 0	0 0 1 2 3	1 2 3 4 5 6 7	1	9 9	1 2 3	8 8	0	0 0 0	?	LRC

Tag 57	L: 19	PAN		Expiry date	Service code	PVKI & PVV	dCVV	ATC 1 & 2	ATC 3 & 4	CI	
		4 0 0 0 0 0 1 2 3 4 5 6 7 8 9 2	D	0 2 1 2	1 2 0	0 0 1 2 3	1 2 3	9 9	8 8	1	F

Note: Length of tag '57' is measured in bytes while the actual digits are shown.

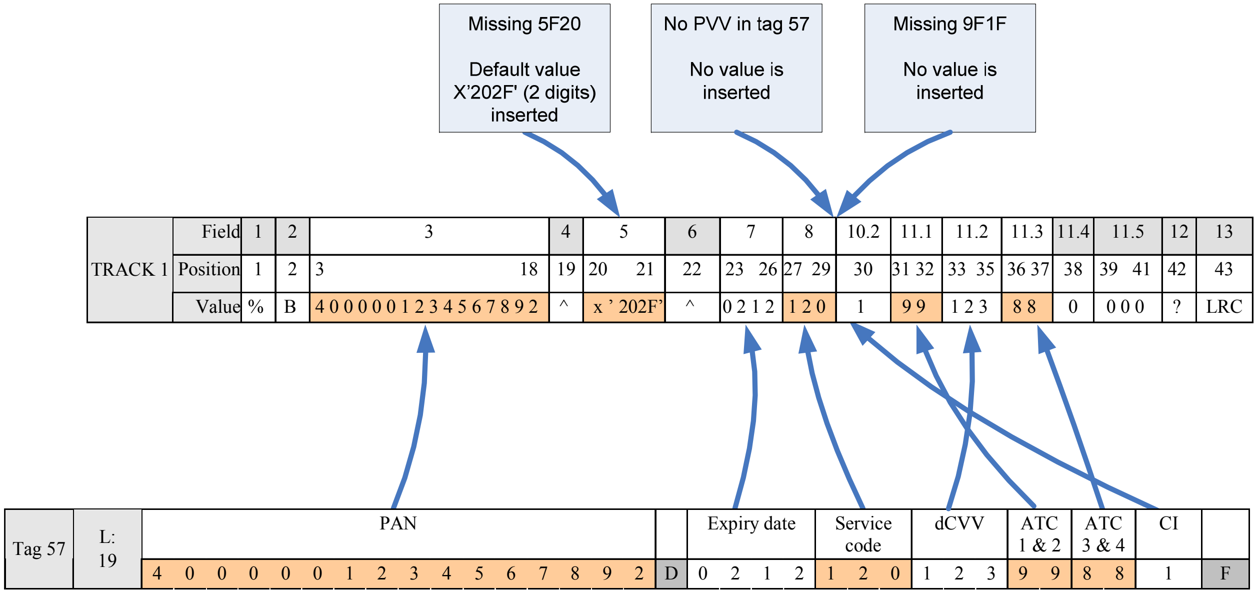
Table F-4: Example 2 of Track 1 Format

Field #	Field Name	Position	Length	Value
Field 1	Start Sentinel	1	1	'%'
Field 2	Format Code	2	1	'B'
Field 3	Primary Account Number (PAN)	3	16	Content of tag '57', position 1 through 16
Field 4	Field Separator	19	1	' ^ '
Field 5	Cardholder Name	20	26	Content of tag '5F20'
Field 6	Field Separator	46	1	' ^ '
Field 7	Card Expiration Date	47	4	Content of tag '57', position 18 through 21
Field 8	Service Code	51	3	Content of tag '57', position 22 through 24
Field 9	PIN Verification field (PVKI & PVV)	54	5	Content of tag '57', position 25 through 29
Field 10.1	Track 1 Discretionary Data	59	7	Content of tag '9F1F' except for the last position that is omitted
Field 10.2	Contactless Indicator	66	1	Content of tag '57', position 37
Field 11.1	ATC part 1	67	2	Content of tag '57', position 33 through 34
Field 11.2	(d)CVV	69	3	Content of tag '57', position 30 through 32
Field 11.3	ATC part 2	72	2	Content of tag '57', position 35 through 36
Field 11.4	Visa reserved	74	1	'0'
Field 11.5	Visa reserved	75	3	'000'
Field 12	End Sentinel	78	1	'?'
Field 13	LRC	79	1	

Example 3

The last example is outlined in Figure F-3 with tags '5F20' and '9F1F' not present on the card and the PVV not present in tag '57'. The reader will use default values/actions as defined in Table F-2. The result is outlined in Table F-5.

Figure F-3: Constructing Track 1 Data – Example 3



Missing 5F20

Default value X'202F' (2 digits) inserted

No PVV in tag 57

No value is inserted

Missing 9F1F

No value is inserted

TRACK 1	Field	1	2	3	4	5	6	7	8	10.2	11.1	11.2	11.3	11.4	11.5	12	13
	Position	1	2	3 18	19	20 21	22	23 26	27 29	30	31 32	33 35	36 37	38	39 41	42	43
	Value	%	B	4 0 0 0 0 0 1 2 3 4 5 6 7 8 9 2	^	x ' 202F'	^	0 2 1 2	1 2 0	1	9 9	1 2 3	8 8	0	0 0 0	?	LRC

Tag 57	L: 19	PAN		Expiry date	Service code	dCVV	ATC 1 & 2	ATC 3 & 4	CI	
		4 0 0 0 0 0 1 2 3 4 5 6 7 8 9 2	D	0 2 1 2	1 2 0	1 2 3	9 9	8 8	1	F

Note: Length of tag '57' is measured in bytes while the actual digits are shown.

Table F-5: Example 3 of Track 1 Format

Field #	Field Name	Position	Length	Value
Field 1	Start Sentinel	1	1	'%'
Field 2	Format Code	2	1	'B'
Field 3	Primary Account Number (PAN)	3	16	Content of tag '57', position 1 through 16
Field 4	Field Separator	19	1	' ^ '
Field 5	Cardholder Name	20	2	Default value '202F' since tag '5F20' is missing
Field 6	Field Separator	22	1	' ^ '
Field 7	Card Expiration Date	23	4	Content of tag '57', position 18 through 21
Field 8	Service Code	27	3	Content of tag '57', position 22 through 24
Field 9	PIN Verification field (PVKI & PVV)	30	0	Not present when PVV is not present in tag '57'
Field 10.1	Track 1 Discretionary Data		0	Not present when tag '9F1F' is missing
Field 10.2	Contactless Indicator	30	1	Content of tag '57', position 32
Field 11.1	ATC part 1	31	2	Content of tag '57', position 28 through 29
Field 11.2	dCVV	33	3	Content of tag '57', position 25 through 27
Field 11.3	ATC part 2	36	2	Content of tag '57', position 30 through 31
Field 11.4	Visa reserved	38	1	'0'
Field 11.5	Visa reserved	39	3	'000'
Field 12	End Sentinel	42	1	'?'
Field 13	LRC	43	1	

F.2 Creating Track 2

Issuers shall personalize Track 2 Equivalent Data for Visa MSD contactless payment. Therefore, the reader is expected to do minimal work compared to Track 1 processing. Track 2 Equivalent Data contains all data elements required to create an emulation of the physical Track 2.

Track 2 Equivalent Data contains the data elements listed in Table F-6.

Table F-6: Data Content for Track 2 Equivalent Data

Tag	Value	Format	Length	Presence
'57'	Track 2 Equivalent Data		var. up to 19	M
	Primary Account Number (PAN)	cn	var. up to cn 19	M
	field separator = 'D'		1	M
	Expiry Date	n	4	M
	Service Code	n	3	M
	PIN Verification Field	n	0 or 5	C
	Track 2 Discretionary Data	n	var.	M
	Padding 'F'	Hex	1	C if required to ensure whole byte

The layout of Track 2 can be mapped directly to Track 2 Equivalent Data as described in Table F-7.

Table F-7: Mapping Track 2 to Track 2 Equivalent Data

Start Sentinel	';'
Primary Account Number (PAN)	PAN
Field Separator	' = '
Expiry Date	Expiration date
Service Code	Service Code
PIN Verification Field	PIN Verification Field (if present)
Track 2 Discretionary Data	Track 2 Discretionary Data
End Sentinel	'?'
LRC	

G Commands and Secure Messaging

G.1 GET DATA Command-Response APDUs

The GET DATA command is used to retrieve primitive and constructed data objects not encapsulated in a record within the current application. Although this command is not issued by readers as part of a VCPS transaction, the card application supports this command to retrieve the data elements listed in Appendix D.1.

The GET DATA command shall be supported as described in [VIS] Appendix C.8, with the following exception(s):

- [VIS] Appendix C.8.2, differentiating card data retrievable at Special Devices and for financial transactions, need not be supported. VCPS data objects retrievable by the GET DATA command are indicated as such in Appendix D.1, regardless of whether the GET DATA is occurring at a Special Device or for a financial transaction.

G.2 GET PROCESSING OPTIONS (GPO) Command-Response APDUs

The GET PROCESSING OPTIONS command initiates the transaction within the card application.

The GET PROCESSING OPTIONS command shall be supported as described in [VIS] Appendix C.9, with the following exception(s):

- Data retrievable using the GET PROCESSING OPTIONS command is not as defined in [VIS] Table C-4.
- The data field returned in the response to the GET PROCESSING OPTIONS command shall be according to [EMV] Format 1 or [EMV] Format 2. For GPO response messages with the data field in Format 2, the AFL is not always included, and the data field may include additional BER-TLV coded data elements. Inclusion of the AFL is conditional on card application processing.

Note: For reader vendors without access to [VIS], support for the GET PROCESSING OPTIONS command is also described in [EMV] section 6.5.8. The exceptions mentioned above also apply to readers.

Card application processing of the GPO command shall be performed as described in section 6.4.

The card application consists of six possible (and potentially distinct) GPO responses for VCPS:

- qVSDC Offline GPO Response (if offline implemented): see Table 6-2 using Condition column "Offline (with ODA)"
- qVSDC Online with ODA GPO Response: see Table 6-2 using Condition column "Online (with ODA)"
- qVSDC Online/Decline without ODA GPO Response: see Table 6-2 using Condition column "Online and Decline (without ODA)"
- MSD CVN17 with ODA GPO Response: see Table 6-3 using Condition column "Online (with ODA)"
- MSD CVN17 without ODA GPO Response: see Table 6-3 using Condition column "Online (without ODA)"
- MSD Legacy GPO Response: see Table 6-4

Note: The qVSDC Online with ODA GPO Response and MSD CVN17 with ODA GPO Response are not returned by the card when used at readers compliant to this specification. The acceptance environment(s) where those GPO responses may be returned are outside the scope of this specification. For dual-interface cards, the GPO response for contact chip transactions is outside the scope of this specification

Req G.1 (GPO Responses)

The card application shall support personalization of each GPO response to return, or not return, the data elements specified for each GPO response (as shown in the corresponding tables for each GPO response).

Issuers are required to personalize the data elements to be returned in the GPO response as required by this specification, but this shall not be enforced by the card application.

Req G.2 (Data Elements in GPO Responses)

A data element may have a different value for each GPO response. The card application shall support personalization of data elements in a GPO response independently of their corresponding values in any other GPO response.

For example, the Application File Locator (tag '94') in each GPO response may be personalized with a different value.

Req G.3 (Additional Data Elements in GPO Responses)

In addition to the data elements explicitly defined for each GPO response, the card application shall support the personalization of additional data elements to be returned in each GPO response. The additional data elements shall be BER-TLV coded.

Note: The functionality specified by this requirement is reserved for possible payment system use. Issuers shall only personalize the data elements that are explicitly permitted for each GPO response.

G.3 READ RECORD Command-Response APDUs

The READ RECORD command reads a file record in a linear file.

The READ RECORD command shall be supported as described in [VIS] Appendix C.13, with the following exception(s):

- Records for application selection, as specified in [EMV] Book 1 section 11.2, need not be supported.

Note: For reader vendors without access to [VIS], support for the READ RECORD command is also described in [EMV] Book 3 section 6.5.11. The exceptions mentioned above also apply to readers.

G.4 SELECT Command-Response APDUs

The SELECT command is used to select an application on the card corresponding to the submitted file name or AID.

The SELECT command shall be supported as described in [VIS] Appendix C.14, with the following exception(s):

- The selection of an application is described in section 5.5 Application Selection of this specification.
- PPSE is used in place of the PSE. Table G-1 defines the FCI returned by a successful selection of the PPSE.

Note: For reader vendors without access to [VIS], support for the SELECT command is also described in [EMV] Book 1 section 11.3. The exceptions mentioned above also apply to readers.

If any of the templates in the SELECT response contain BER-TLV data elements in addition to the data elements explicitly defined, the reader shall be able to parse the SELECT response. Unrecognized data elements for Application Selection are not stored by the reader.

Table G-1: SELECT Response Message Data Field (FCI) of the PPSE

Tag	Value					Length	Presence
'6F'	FCI Template					var.	M
	'84'	DF Name ('2PAY.SYS.DDF01')				'0E'	M
	'A5'	FCI Proprietary Template				var.	M
		'BF0C'	FCI Issuer Discretionary Data			var.	M
			'61'	Directory Entry		var.	M
				'4F'	ADF Name (AID)	'07'–'10'	M
				'50'	Application Label	'04'–'10'	O
				'87'	Application Priority Indicator	'01'	C[1]
			'61'	Directory Entry		var.	O
				'4F'	ADF Name (AID)	'07'–'10'	C[2]
				'50'	Application Label	'04'–'10'	O
				'87'	Application Priority Indicator	'01'	C[1 and 2]
			'61'	Directory Entry		var.	O
				'4F'	ADF Name (AID)	'07'–'10'	C[2]
				'50'	Application Label	'04'–'10'	O
				'87'	Application Priority Indicator	'01'	C[1 and 2]

Table G-2: SELECT Response Status Word

SW1 SW2	Type	Condition
'6283'	Warning	Application blocked
'6A81'	Error	Card blocked
'6A82'	Error	Selected file not found
'9000'	Normal	Successful processing

[1] If more than one contactless application is personalized on the card, then an Application Priority Indicator shall be personalized for each application.

[2] Personalized if the corresponding Directory Entry is present.

G.5 ISSUER UPDATE COMMANDS

Implementation-Conditional: Issuer Update commands shall be supported if Issuer Update Processing is supported.

G.5.1 APPLICATION BLOCK Command-Response APDUs (Issuer Script Command)

The APPLICATION BLOCK command is a post-issuance command that invalidates the currently selected application.

The APPLICATION BLOCK command shall be supported as described in [VIS] Appendix C.2, with the following exception(s):

- Processing of the GENERATE AC command is outside the scope of this specification.
- Following the successful completion of an APPLICATION BLOCK command (either through Issuer Update Processing or through a [VIS] transaction), an invalidated application shall return an Application Authentication Cryptogram (AAC) cryptogram type when an Application Cryptogram is returned in the GPO response.

G.5.2 APPLICATION UNBLOCK Command-Response APDUs (Issuer Script Command)

The APPLICATION UNBLOCK command is a post-issuance command that reverses the Application Block status.

The APPLICATION UNBLOCK command shall be supported as described in [VIS] Appendix C.3.

G.5.3 CARD BLOCK Command-Response APDUs (Issuer Script Command)

The CARD BLOCK command is a post-issuance command that permanently disables all applications in the card.

The CARD BLOCK command shall be supported as described in [VIS] Appendix C.4.

G.5.4 EXTERNAL AUTHENTICATE Command-Response APDUs

The EXTERNAL AUTHENTICATE command performs Issuer Authentication (by verifying a cryptogram) and conditionally resets card counters and indicators.

The EXTERNAL AUTHENTICATE command shall be supported as described in [VIS] Appendix C.5. EXTERNAL AUTHENTICATE command processing is defined in section 6.6.2.

Note: For reader vendors without access to [VIS], support for the EXTERNAL AUTHENTICATE command is also described in [EMV] section 6.5.4.

G.5.5 PIN CHANGE/UNBLOCK Command-Response APDUs (Issuer Script Command)

Implementation-Conditional: If Issuer Update Processing supported and offline PIN for dual-interface card application supported.

The PIN CHANGE/UNBLOCK command is a post-issuance command to unblock the reference PIN or to simultaneously change and unblock the reference PIN.

The PIN CHANGE/UNBLOCK command shall be supported as described in [VIS] section 14.5.4 and [VIS] Appendix C.11.

G.5.6 PUT DATA Command-Response APDUs (Issuer Script Command)

The PUT DATA command is a post-issuance command that updates specific data objects stored in the card.

The PUT DATA command shall be supported as described in [VIS] Appendix C.12, with the following exception(s):

- VCPS data elements that may be updated using the PUT DATA command are indicated as such in Appendix D.1.

G.5.7 UPDATE RECORD Command-Response APDUs (Issuer Script Command)

The UPDATE RECORD command is a post-issuance command that is used to update a record in a file with the data provided in the command data field.

The UPDATE RECORD command shall be supported as described in [VIS] Appendix C.15.

G.6 Secure Messaging

Secure messaging for issuer scripts shall be performed as described in [VIS] Appendix B, except for computation of the MAC, which shall be performed as described in this appendix.

Req G.4 (Secure Messaging)

Secure messaging for issuer scripts shall be performed as described in [VIS] Appendix B, with the following exception(s) in [VIS] Appendix B.2.4, step #2, bullet 3:

- The Last Contactless Application Cryptogram shall be used instead of the “last Application Cryptogram...”
- If Issuer Script MAC Chaining is supported (ADA byte 3 bit 3 is 1b), then the 8-byte value shall be persistent across communication sessions.

Issuer script MAC chaining shall be implementation-mandatory and issuer-optional. Use of issuer script MAC chaining is recommended.

H Streamlined qVSDC

H.1 Streamlined Functionality for qVSDC

Streamlined qVSDC is a simplified, online-only implementation of the card qVSDC path. Streamlined qVSDC, as specified in this appendix, may be implemented by card manufacturers for markets where products containing full qVSDC are not needed. Streamlined qVSDC provides for a simplified, online-only flow through the card qVSDC path, allowing for easier card implementations and potentially reduced transaction times. Streamlined qVSDC deals exclusively with the card qVSDC path, and readers are oblivious to whether the card is processing as full or Streamlined qVSDC. Streamlined qVSDC is not appropriate for all markets and, as such, vendors planning to implement only Streamlined qVSDC should contact their regional representatives.

The requirements specified in this section are intended primarily for implementations containing only Streamlined qVSDC. However, Streamlined qVSDC may also be supported in full qVSDC implementations, allowing for an issuer option to process qVSDC transactions as Streamlined qVSDC.

For full qVSDC implementations supporting this option, if CAP byte 1 bit 5 is 1b **or** if the CAP is not personalized, then Streamlined qVSDC processing is performed.

H.2 Streamlined qVSDC Requirements

Streamlined qVSDC has the same requirements as full qVSDC, except that an abbreviated form of qVSDC Card Action Analysis is performed. In addition, some implementation decisions have been made for Streamlined qVSDC in order to facilitate simple implementations and quick transactions.

Req H.1 (Streamlined qVSDC)

The card streamlined qVSDC implementation shall conform to the card qVSDC path requirements specified in section 6, with the following exception(s):

- The qVSDC path shall not support offline processing. The qVSDC Offline GPO Response is not personalized.
- qVSDC Card Action Analysis shall be performed as defined in this appendix.

H.3 Streamlined qVSDC Card Action Analysis

Streamlined qVSDC shall perform qVSDC Card Action Analysis as defined in this appendix.

The card qVSDC path always returns an online cryptogram in response to the GPO command, when returning a non-error code Status Word.

H.3.1 qVSDC Card Risk Management Processing

Checks and processing are performed in the order shown. Implementations are not required to strictly follow the processing described in this section, so long as they behave in a way that is indistinguishable (seen as a black box responding to the command) from the behavior described.

Initialization of Data

Req H.2 (Initialization of Card Transaction Qualifiers)

The card shall reset CTQ byte 1 bits 8-7 to 00b (indicating Online PIN Not Required and Signature Not Required).

Req H.3 (Initialization of Issuer Application Data)

The card shall set the CVR to '03 80 00 00' (indicating Second GENERATE AC not requested).

Req H.4 (Initialization of Cryptogram Information Data)

The card shall reset the Cryptogram Information Data (CID) to '00'.

Application Blocked

Req H.5 (Application Blocked Check)

If the application is blocked, then the card shall discontinue processing the command and shall respond with SW1 SW2 = '6985'.

Cardholder Verification Method (CVM)

Req H.6 (CVM Required Check)

If CVM Required by reader (TTQ byte 2 bit 7 is 1b), then a CVM is required for the transaction, and the card shall determine the common CVM to be performed.

Req H.7 (Determine Common CVM)

If a CVM is required for the transaction, then the card shall attempt to select a common CVM supported by both itself and the reader, as defined in this requirement. If there is more than one CVM supported by both the card and the reader, the selected CVM is chosen based on the following defined CVM hierarchy: 1) Online PIN, 2) Signature.

If the Card Additional Processes (CAP) is personalized, then:

- If **both** of the following are true:
  - Online PIN supported by reader (TTQ byte 1 bit 3 is 1b)
  - **and either** of the following is true:
    - Online PIN supported by card for domestic transactions (CAP byte 3 bit 8 is 1b)
    - **or** Online PIN supported by card for international transactions (CAP byte 3 bit 7 is 1b)

  Then the card shall indicate Online PIN Required (set CTQ byte 1 bit 8 to 1b).

  Else, if **both** of the following are true:

  - Signature supported by reader (TTQ byte 1 bit 2 is 1b)
  - **and** Signature supported by card (CAP byte 3 bit 5 is 1b)

  Then the card shall indicate Signature Required (set CTQ byte 1 bit 7)

  Else (no common CVM between card and reader), the card shall discontinue processing and respond to the GPO command with SW1 SW2 = '6984'.

Else (the CAP is not personalized), then:

- If Signature is not supported by the reader (TTQ byte 1 bit 2 is 0b), then the card shall discontinue processing and respond to the GPO command with SW1 SW2 = '6984'.

  Else (Signature is supported by the reader), the card shall continue processing the transaction

H.3.2 Transaction Disposition

Req H.8 (Online)

The card shall:

- Indicate Authorization Request Cryptogram returned (set CVR byte 2 bits 6-5 to 10b and set CID bits 8-7 to 10b).
- Increment the Application Transaction Counter (ATC) by one. The ATC shall be incremented prior to the performance of any cryptographic operations.

  If incrementing the ATC results in the ATC reaching its maximum value, then the application shall be permanently blocked, Req 6.7 (Application Permanently Blocked), and shall respond to the GPO command with error SW1 SW2 = '6985'.
- Construct the Issuer Application Data. If an Issuer Discretionary Data Option (IDD Option) is supported (see Appendix E), it shall be constructed and the MAC generated (if applicable).
- If the card is capable of performing fDDA **and all** of the following are true:
  - the card supports fDDA for Online Authorizations (AIP byte 1 bit 6 is 1b for the qVSDC "Online (with ODA)" GPO response)
  - **and** ODA for Online Authorizations supported by card (CAP byte 2 bit 6 is 0b)
  - **and** ODA for Online Authorizations supported by reader (TTQ byte 1 bit 1 is 1b)

  Then the card shall construct the Card Authentication Related Data and generate the Signed Dynamic Application Data (tag '9F4B'). The Signed Dynamic Application Data shall be generated as defined in Appendix A.
- Generate the Application Cryptogram.
- If ODA for Online Authorizations supported by reader (TTQ byte 1 bit 1 is 1b), then construct and send the GPO response in [EMV] Format 2 with the data shown in Table 6-2 using Condition column "Online (with ODA)".

  Else (TTQ byte 1 bit 1 is 0b), construct and send the GPO response in [EMV] Format 2 with the data shown in Table 6-2 using Condition column "Online and Decline (without ODA)".

  Note: The Available Offline Spending Amount (tag '9F5D') is not supported for Streamlined qVSDC.

I Dual-Interface Contactless and Contact Cards

For dual-interface cards that support both [VCPS] and [VIS], this appendix defines additional requirements for dual-interface cards, and identifies the new functionality required of [VIS] to address the functionality introduced by [VCPS].

Dual-interface cards shall implement the functionality and requirements defined in this appendix.

I.1 Contactless and Contact Interfaces

Req I.1 (Contactless and Contact Interfaces)

The card shall not activate the contactless interface if the contact interface is activated.

The card's contact interface should have priority over its contactless interface. If the contactless interface is active and the contact interface is subsequently activated, the card should deactivate the contactless interface and activate the contact interface.

I.2 Processing Options Data Object List (PDOL)

A card application contains a single PDOL for the contactless interface. For a dual-interface card, the contact interface may be personalized with a different PDOL or without a PDOL.

Req I.2 (PDOL)

For a dual-interface card, the card application shall be capable of supporting different PDOL’s based on interface – contact or contactless.

I.3 Reset of Offline Counters using VIS

Counters that are used in VCPS transaction processing are reset either through Issuer Update Processing or through [VIS] transactions, subject to issuer requirements.

Counter reset with Issuer Update Processing is described and specified in section 6.6.

Counter reset with [VIS] transactions are described and specified in [VIS], and are briefly summarized in this section.

I.3.1 [VIS] Counter Resets

The [VIS] specification has been revised to reset the counters and indicators shared by VIS and VCPS, and to reset the counters and indicators used exclusively by VCPS, subject to issuer requirements for resetting of counters.

In addition, VCPS introduced the ‘Reset VLP Available Funds to VLP Funds Limit when Offline PIN successfully verified’ (ADA byte 3 bit 5) option. With this option, the VLP Available Funds is reset to the VLP Funds Limit when the Offline PIN is successfully validated during a VIS transaction (and other processing requirements are met).

See [VIS] for additional details regarding resetting of counters during VIS transactions.

I.3.2 Consecutive Transaction Counter International

qVSDC transactions where the Transaction Currency Code does not match the Application Currency Code or any of the supported Conversion Currency Codes are international transactions. Additionally, the issuer may configure the application such that transactions where the Terminal Country Code does not match the Issuer Country Code are also international transactions. Regardless of the issuer configuration to include international determination based on the country code, the Consecutive Transaction Counter International (CTCI) may be used to count qVSDC international transactions.

This behavior is unlike [VIS], where two separate counters are used to count non-matching currency code transactions and non-matching country code transactions. ADA byte 3 bit 1 (‘CTCI also counts non-matching country code transactions’) is introduced to allow for [VIS] applications to count international transactions using the same single counter.

Req I.3 (VIS CTCI)

If ‘CTCI also counts non-matching country code transactions’ (ADA byte 3 bit 1 is 1b), then [VIS] transactions shall increment the Consecutive Transaction Counter International (CTCI) for non-matching country code transactions.

I.4 Data Accessibility

For dual-interface cards, data used exclusively for contactless transactions are not retrievable via the contact interface. Similarly, data used exclusively for contact transactions are not retrievable via the contactless interface.

Req I.4 (Records Restricted by Interface)

Records for a path, as defined by the Application File Locator(s) for that path, shall only be accessible over the interface(s) supported by that path.

If the record requested by the READ RECORD command is not allowed to be retrieved over the interface, the card shall respond with an error SW1 SW2 ('6A83' is recommended)

For example, a record present only in the AFL for the qVSDC path shall only be accessible over the contactless interface, and a record present in the AFL for both qVSDC and VIS shall be accessible over both the contactless and contact interfaces.

Note: This record retrieval restriction is based only on whether the record was personalized in the AFL for the card paths, regardless of whether or not the AFL was returned by the card prior to the card application receiving the READ RECORD command.

Req I.5 (Transaction Log Records Restricted by Interface)

Implementation-Conditional: If transaction logging is implemented, then this functionality shall be implemented.

Transaction log records shall be issuer configurable to be accessible over the contact interface-only, over the contactless interface-only, or over both interfaces.

Req I.6 (Application Internal Data Elements)

Card internal data elements are indicated as retrievable or not retrievable by the GET DATA command in Table D-1, regardless of the interface over which the command was received.

I.5 Application Capabilities

I.5.1 Contactless Functionality

The ‘Contactless Functionality Disabled’ bit (Application Capabilities byte 1 bit 8) is used to configure whether the dual interface card is permitted to process commands received over the contactless interface. This bit can be personalized, or set post-issuance using the PUT DATA issuer script command, to “disable the contactless functionality” of the card.

Req I.7 (Contactless Functionality Disabled)

When ‘Contactless Functionality Disabled’ is 1b, the card application shall discontinue processing of all commands received over the contactless interface, and shall respond with an error SW1 SW2 ('6A81' is recommended).

I.5.2 Restrict Reset of Contactless Functionality Disabled Bit to PUT DATA

Application Capabilities byte 1 bit 7, ‘Restrict reset of Contactless Functionality Disabled bit’, can be personalized or set post-issuance using the PUT DATA issuer script command to control the conditions under which the ‘Contactless Functionality Disabled’ bit is reset to 0b.

Req I.8 (Restrict Reset of Contactless Functionality Disabled Bit)

If ‘Restrict reset of Contactless Functionality Disabled bit’ is 0b, then the ‘Contactless Functionality Disabled’ bit shall be reset to 0b during the next [VIS] transaction where the card approves the transaction after an online authorization (when Issuer Authentication requirements are met for [VIS]). See [VIS] Appendix H for further details.

If ‘Restrict reset of Contactless Functionality Disabled bit’ is 1b, then the ‘Contactless Functionality Disabled’ bit shall only be reset to 0b through the PUT DATA issuer script command.

Note: Regardless of the setting of the ‘Restrict reset of Contactless Functionality Disabled bit’, the PUT DATA issuer script command can always be used to change the value of the ‘Contactless Functionality Disabled’ bit.

I.6 Issuer Update Processing

Issuer Update Processing introduces new counters and indicators that must be processed during [VIS] transactions. For dual-interface cards supporting Issuer Update Processing, the following counters shall be processed as defined:

- Last Successful Issuer Update ATC Register – During [VIS] transactions, this data element is set to the value of the ATC when [VIS] Issuer Authentication requirements are met, or when an issuer script command is successfully processed.
- Last Contactless Application Cryptogram Valid Indicator – If a [VIS] transaction is initiated, then this indicator shall be set to 0 (during GPO processing).

I.7 DDA and fDDA

The ICC Public Key Certificate used in DDA and fDDA contain a hash of static data from the card application. However, different static data elements are recommended to be signed for VCPS and VIS:

- It is recommended that VCPS not sign any static data. Transaction times are reduced if VCPS does not sign static data, as one fewer record may be returned.

- It is recommended that VIS sign the static data as recommended in [VIS].

Although VIS and VCPS may share the same ICC Public Key Certificate, it is recommended that VCPS and VIS use different ICC Public Key Certificates, and for the VCPS ICC Public Key Certificate not to contain the any static data to be authenticated. Transaction times are reduced since there is less processing.

Even when the hash in the VCPS ICC Public Key Certificate does not contain any static data, the Application PAN and Application Expiration are still protected. The PAN is verified against the Application PAN contained in the ICC Public Key Certificate during DDA and fDDA processing ([EMV] Book 2 section 6.4). To prevent altered Application Expiration Dates, it is strongly recommended that the Certificate Expiration Date (from the ICC Public Key Certificate) match the Application Expiration Date. The Certificate Expiration Date is then validated during DDA and fDDA processing ([EMV] Book 2 section 6.4).

Issuers should balance the benefits of using different ICC Public Key Certificates for VIS and VCPS (reducing transaction times) against the increased complexity of generating and personalizing two ICC Public Key Certificates.

J Reader-Terminal Data

This appendix outlines the data elements that may need to be communicated from the reader to the merchant device connected to the acquirer for each transaction path. The data that needs to be communicated is dependent on the architecture of the reader within the POS acceptance environment, hence the tables below are intended only to provide guidance. The tables do not represent a comprehensive list of all data that must be communicated, and many of the data elements listed below may not need to be communicated at all (depending on reader-terminal architecture).

Table J-1: MSD CVN17 Transactions

Data Element	Tag	Condition
POS Entry Mode	–	Always
Terminal Entry Capability	–	Always
Track 1	–	If Track 1 construction supported
Track 2 Equivalent Data	57	Always
Cardholder Name	5F20	If present in card response
Application PAN Sequence Number	5F34	If present in card response
Amount, Authorized (Numeric)	9F02	A zero-filled value may be used if provided as such to the card.
Issuer Application Data	9F10	Always
Application Cryptogram	9F26	Always
Application Transaction Counter	9F36	Always
Unpredictable Number (Reader-Terminal)	9F37	Always
Terminal Transaction Qualifiers	9F66	Always
Form Factor Indicator	9F6E	If present in card response
Customer Exclusive Data	9F7C	If present in card response

Table J-2: qVSDC Transactions

Data Element	Tag	Condition
POS Entry Mode	–	Always
Terminal Entry Capability	–	Always
Track 2 Equivalent Data	57	Always
Application PAN	5A	If returned by card
Cardholder Name	5F20	If returned by card
Application Expiration Date	5F24	If returned by card
Transaction Currency Code	5F2A	Always
Application PAN Sequence Number	5F34	If returned by card
Application Interchange Profile	82	Always
Terminal Verification Results	95	Always
Transaction Date	9A	Always
Transaction Type	9C	Always
Amount, Authorized (Numeric)	9F02	Always
Amount, Other (Numeric)	9F03	Always
Issuer Application Data	9F10	Always
Terminal Country Code	9F1A	Always
Application Cryptogram	9F26	Always
Cryptogram Information Data	9F27	Always
Application Transaction Counter	9F36	Always
Unpredictable Number (Reader-Terminal)	9F37	Always
Issuer Script Results	9F5B	If Issuer Update Processing supported and issuer scripting performed
Available Offline Spending Amount	9F5D	If returned by card
Form Factor Indicator	9F6E	If returned by card
Customer Exclusive Data	9F7C	If returned by card

K Online Messages and Clearing Records

This appendix outlines the new values for online messages and clearing records required for VCPS transactions.

Regardless of reader-terminal architecture, the acquirer shall be provided the data necessary to construct online messages and clearing records with the new data specified in this appendix. The method and means of providing this information to the acquirer is outside the scope of this specification.

K.1 MSD Acquirers

K.1.1 Acquirers Supporting MSD Legacy Only

This section describes the messaging requirements for acquirers that only support MSD Legacy transactions.

MSD Legacy data requirements for online messages and clearing records are the same as for traditional magnetic stripe transactions, except for new values in existing fields (as shown in Table K-1).

Table K-1: Acquirers Supporting MSD Legacy-Only

Data	Tag	Condition
POS Entry Mode	–	Always A value of 91 for MSD transactions.
Terminal Entry Capability	–	Always A value of 5 (for readers that also support VSDC contact chip) or a value of 8 (for readers that do not also support VSDC contact chip). Check with your Visa regional representative.

K.1.2 Acquirers Supporting MSD CVN17

This section describes the messaging requirements for acquirers that support MSD CVN17 transactions (in addition to supporting MSD Legacy transactions).

MSD CVN17 data requirements for online messages and clearing records are the same as for traditional magnetic stripe transactions, with the addition of new values in existing fields and carrying new data for the CVN17 application cryptogram (as shown in Table K-2).

For full chip acquirers, the new values in existing fields and new data for the CVN17 application cryptogram may include the additional data shown in Table K-3.

Table K-2: Acquirer Supporting MSD CVN17

Data	Tag	Condition
Amount, Authorized	9F02	Conditional Amount, Authorized is conditional for MSD transactions. The real transaction amount may not be provided to the card in the Amount, Authorized for cryptogram generation. In this case, the reader provides a predefined Amount, Authorized value to the card. If the Amount, Authorized provided to the card has a non-zero value, then the reader shall pass the Amount, Authorized to the acquirer and the acquirer shall populate it in the message to the issuer. If the Amount, Authorized provided to the card has a value of all zeros, then the reader shall pass the Amount, Authorized to the acquirer and the acquirer shall either: • Include the Amount, Authorized with a value of all zeros in the message to the issuer. • **or** not include the Amount, Authorized in the message, and the issuer assumes a zero value when performing cryptogram validation. *Note*: When the Amount, Authorized is present in the message, the value of the Amount, Authorized is used for cryptogram validation. When the Amount, Authorized is not present in the message, the value is assumed to be zero for cryptogram validation.
Application Cryptogram	9F26	Conditional If the Application Cryptogram is provided to the reader by the card, then the data must be included in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records.
Application Transaction Counter (ATC)	9F36	Conditional If the Application Transaction Counter (ATC) is

Data	Tag	Condition
		provided to the reader by the card, this data must be present in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records.
Card Sequence Number	5F34	Conditional If the Application PAN Sequence Number (PSN) is provided to the reader by the card, this data must be present in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records.
Customer Exclusive Data	9F7C	Conditional If the Customer Exclusive Data (CED) is provided to the reader by the card, this data must be present in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records.
Form Factor Indicator	9F6E	Conditional If the Form Factor Indicator (FFI) is provided to the reader by the card, this data must be present in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records.
Issuer Application Data	9F10	Conditional If the Issuer Application Data (IAD) is provided to the reader by the card, this data must be present in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records.
POS Entry Mode	–	Always A value of 91 for MSD transactions.
Terminal Entry Capability	–	Always A value of 5 (for readers that also support VSDC contact chip) or a value of 8 (for readers that do not also support VSDC contact chip). Check with your Visa regional representative.
Terminal Transaction Qualifiers	9F66	Conditional This data may be present in online messages and clearing records. See Req 5.11 (MSD Messages - TTQ).
Unpredictable Number (Reader-Terminal)	9F37	Always

K.1.3 MSD Requirements

The following additional requirements are applicable for MSD messages.

Req K.1 (Track 2 and Track 1)

For MSD transactions, either Track 2 and/or Track 1 shall be sent online in the authorization.

Track 1 construction is defined in Appendix F.1 Creating Track 1.

Req K.2 (Primary Account Number and Expiration Date)

The primary account number and application expiration date used in messaging are retrieved from Track 2 Equivalent Data.

K.2 qVSDC Acquirers

K.2.1 Acquirers Supporting qVSDC

This section describes the messaging requirements for acquirers that support qVSDC transactions.

qVSDC data requirements for online messages and clearing records are the same as for VSDC contact chip transactions, except for new values in existing fields and new values in chip fields (as shown in Table K-3).

Table K-3: Acquirers Supporting qVSDC

Data	Tag	Value
Amount, Authorized	9F02	Always
Amount, Other	9F03	Always
Application Cryptogram	9F26	Always *
Application Interchange Profile	82	Always
Application Transaction Counter (ATC)	9F36	Always *
Card Sequence Number	5F34	Conditional If the Application PAN Sequence Number (PSN) is provided to the reader by the card, this data must be included in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records.

Data	Tag	Value
Customer Exclusive Data	9F7C	Conditional If the Customer Exclusive Data (CED) is provided to the reader by the card, this data may be included in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records. See Req 5.7 (qVSDC Messages - FFI and CED).
Form Factor Indicator	9F6E	Conditional If the Form Factor Indicator (FFI) is provided to the reader by the card, this data may be included in online messages and clearing records. Else (data not provided to the reader by the card), the data is not included in online messages and clearing records. See Req 5.7 (qVSDC Messages - FFI and CED).
Issuer Application Data	9F10	Always *
POS Entry Mode	–	Always A value of 07 for qVSDC transactions.
Terminal Capabilities	9F33	Always
Terminal Country Code	9F1A	Always
Terminal Entry Capability	–	Always A value of 5 (for readers that also support VSDC contact chip) or a value of 8 (for readers that do not also support VSDC contact chip). Check with your Visa regional representative.
Terminal Verification Results	95	Always For VCPS transactions, the TVR shall have a value of all zeros when included in online messages and clearing records.
Transaction Currency Code	5F2A	Always
Transaction Date	9A	Always
Transaction Type	9C	Always
Unpredictable Number (Reader-Terminal)	9F37	Always

* For acquirers supporting qVSDC and MSD (and full chip acquirers supporting MSD CVN17), the inclusion of these data elements in MSD online messages and clearing records are conditional on whether they were provided to the reader by the card. See Table K-2.

K.2.2 qVSDC Requirements

The following additional requirements are applicable for qVSDC messages.

Req K.3 (Track 2)

For qVSDC transactions, Track 2 shall be sent online in the authorization.

Req K.4 (Primary Account Number and Expiration Date)

The primary account number and application expiration date used in messaging are retrieved from Track 2 Equivalent Data.

L Transaction Logging

Implementation-Optional: Implementation of transaction logging is at implementer discretion.

Issuer-Optional: If transaction logging is implemented, the issuer shall be able to enable and disable transaction logging. Due to the increase in application processing times when transaction logging is used, it is strongly recommended that issuers not enable transaction logging.

When transaction logging is supported, it shall be supported as described in [EMV] Book 3 Annex D, with the following exception(s):

- Any reader-terminal data element to be logged shall be requested in the Processing Options Data Object List (PDOL).

For VCPS transactions, updates to the log occur:

- Immediately prior to the application response to the GET PROCESSING OPTIONS (GPO) command when an Application File Locator is not returned in the GPO response.
- Immediately prior to the application response to the last READ RECORD command when an Application File Locator is returned in the GPO response. The last record is indicated by the Application File Locator.

The default behavior is to log all online and offline approval requested transactions. However, Application Default Action (ADA) byte 3 includes three bits reserved to control logging of transactions:

- Do not include offline approval requested transactions in the transaction log.
- Do not include online approval requested transactions in the transaction log.
- Include offline declined transactions in the transaction log.

Recognize that VCPS transaction log information represents the card applications view of the transaction outcome, which is not necessarily the same as the actual outcome of the transaction.

Visa recommends only updating the transaction log for the following Transaction Types:

- '00' - Purchase
- '01' - Cash
- '11' - Quasi cash

VIS transactions are logged as defined in [VIS] Appendix I.

Implementations may support an option where log access (that is, reading log records) requires successful verification of a [VIS] Offline PIN. Visa rules for PIN entry and verification apply.

Glossary

This is a glossary of terms used in this specification; it is not intended as a data dictionary. For descriptions of data elements, see Appendix D.

a

alpha

AAC

Application Authentication Cryptogram

AC

Application Cryptogram

acquirer

A Visa customer that signs a merchant or disburses currency to a cardholder in a cash disbursement, and directly or indirectly enters the resulting transaction into interchange.

ADA

Application Default Action

ADF

Application Definition File

AEF

Application Elementary File

AFL

Application File Locator

AID

Application Identifier

AIP

Application Interchange Profile

an

alphanumeric

ans

alphanumeric special

ANSI

American National Standards Institute. A U.S. standards accreditation organization.

AOSA

Available Offline Spending Amount

APDU

Application Protocol Data Unit

application

A computer program and associated data that reside on an integrated circuit chip and satisfy a business function. Examples of applications include payment, stored value, and loyalty.

Application Authentication Cryptogram (AAC)

A cryptogram generated by the card for offline and online declined transactions.

Application Cryptogram

Cryptogram returned by the card in response to the GET PROCESSING OPTIONS command; one of the following cryptogram types:

TC	Transaction Certificate
ARQC	Authorization Request Cryptogram
AAC	Application Authentication Cryptogram

Application Authentication Cryptogram (AAC)

A cryptogram generated by the card application for offline declined transactions.

Application Elementary File

A set of data or records in a file that uses a single Short File Identifier (SFI).

ARC

Authorization Response Code

ARPC

Authorization Response Cryptogram

ARQC

Authorization Request Cryptogram

ATC

Application Transaction Counter

AUC

Application Usage Control

authentication

A cryptographic process that validates the identity and integrity of data.

authorization

A process where an issuer or a representative of the issuer approves a transaction.

authorization controls

Information in the chip application enabling the card to act on the issuer's behalf at the point of transaction. The controls help issuers manage their below-floor-limit exposure to fraud and credit losses. Also known as offline authorization controls.

authorization request

A merchant's or acquirer's request for an authorization.

Authorization Request Cryptogram (ARQC)

The cryptogram generated by the card for transactions requiring online authorization and sent to the issuer in the authorization request. The issuer validates the ARQC during the Online Card Authentication (CAM) process to ensure that the card is authentic and that the authorization request was not created using skimmed data.

Authorization Response Cryptogram (ARPC)

A cryptogram generated by the issuer and sent to the card in the authorization response. This cryptogram is the result of the Authorization Request Cryptogram (ARQC) and the issuer's authorization response encrypted with the Unique Derivation Key (UDK). It is validated by the card during Issuer Authentication to ensure that the response came from a valid issuer.

b

binary

Bank Identification Number (BIN)

A 6-digit number assigned by Visa and used to identify a customer or processor for authorization, clearing, or settlement processing.

BCD

Binary Coded Decimal

BER

Basic Encoding Rules

Binary Coded Decimal

A code for representing decimal digits in a binary format.

byte

8 bits of data.

C

conditional

CA

Certificate Authority

CAM

Card Authentication Method

Candidate List

A list of applications supported by both the card and reader. The Candidate List is built by the reader during Application Selection.

CAP

Card Additional Processes

Card

A consumer device containing the Visa contactless payment application.

Note that the consumer device may not be a plastic card, but for the purposes of this specification, the term card is used to represent the consumer device.

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 Verification Value (CVV)

A unique check value encoded on a card's magnetic stripe and chip to validate card information during an online authorization.

cardholder

An individual to whom a card is issued or who is authorized to use that card.

cardholder verification

The process of determining that the presenter of the card is the valid cardholder.

Cardholder Verification Method (CVM)

A method used to confirm the identity of a cardholder.

cash disbursement

Currency, including travelers checks, paid to a cardholder using a card.

cashback

Cash obtained in conjunction with, and processed as, a purchase transaction.

CDA

Combined DDA/Application Cryptogram generation

CDOL

Card Risk Management Data Object List

CED

Customer Exclusive Data

Certificate Authority (CA)

A trusted central administration that issues and revokes certificates.

Chinese Remainder Theorem

A specific format for private RSA keys that makes the signature calculation faster.

chip

An electronic component designed to perform processing or memory functions.

chip card

A card embedded with a chip that communicates information to a point-of-transaction terminal.

chip-capable

A card acceptance device that is designed and constructed to facilitate the addition of a chip reader/writer.

CID

Cryptogram Information Data

CLA

Class byte of Command Message

clearing

The collection and delivery to the issuer of a completed transaction record from an acquirer.

CLTC

Contactless Transaction Counter

CLTCLL

Contactless Transaction Counter Lower Limit

CLTCUL

Contactless Transaction Counter Upper Limit

cn

compressed numeric

Collision

Transmission by two or more PICCs in the same PCD energizing field and during the same time period, such that the PCD is unable to distinguish from which PICC the data originated.

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

Proximity Card (PICC) or other chip-capable device (for example, a cell phone) that is used by consumers to conduct payment.

Contactless Transaction

A transaction conducted over the contactless interface according to this specification.

Contactless Indicator

An optional indicator in the last position in the magnetic stripe data on the chip. A value greater than zero indicates contactless and may be used to differentiate cards with the same account number.

CPS

Card Personalization Specification

cryptogram

A value that is the result of data elements entered into an algorithm and then encrypted. Commonly used to validate data integrity.

cryptographic key

The numeric value entered into a cryptographic algorithm that allows the algorithm to encrypt or decrypt a message.

cryptography

The art or science of keeping messages secret or secure, or both.

CSU

Card Status Update

CTC

Consecutive Transaction Counter

CTCI

Consecutive Transaction Counter International

CTCIL

Consecutive Transaction Counter International Limit

CTCL

Consecutive Transaction Counter Limit

CTCUL

Consecutive Transaction Counter Upper Limit

CTIUL

Consecutive Transaction International Upper Limit

CTQ

Card Transaction Qualifiers

CTTA

Cumulative Total Transaction Amount

CTTAL

Cumulative Total Transaction Amount Limit

CTTAUL

Cumulative Total Transaction Amount Upper Limit

CTTA Funds

Refers to the value of the Cumulative Total Transaction Amount Upper Limit (CTTAUL) less the Cumulative Total Transaction Amount (CTTA).

If CTTAUL is not personalized, then refers to the value of the Cumulative Total Transaction Amount Limit (CTTAL) less the Cumulative Total Transaction Amount (CTTA).

CVM

Cardholder Verification Method

CVN

Cryptogram Version Number

CVR

Card Verification Results

CVV

Card Verification Value

data authentication

Validation that data stored in the integrated circuit card has not been altered since card issuance. *See also* Offline Data Authentication.

Data Encryption Algorithm (DEA)

An encipherment operation and an inverse decipherment operation in a cryptographic system.

Data Encryption Standard (DES)

The public domain symmetric key cryptography algorithm of the National Institute for Standards and Technology.

dCVV

Dynamic Card Verification Value

DDA

Dynamic Data Authentication

DDF

Directory Definition File

DDOL

Dynamic Data Authentication Data Object List

DEA

Data Encryption Algorithm

Dedicated File Name

Name of file or application as defined in [EMV] and [VIS].

decryption

The process of transforming ciphertext into cleartext.

DES

Data Encryption Standard

DES key

A secret parameter of the Data Encryption Standard algorithm.

DES keys by definition are of odd parity, as indicated in the Federal Information Processing Standards publication FIPS 46-3.

DF

Dedicated file

DF Name

Dedicated File Name

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.

Discovery

Contactless readers poll for contactless cards. When one or more contactless cards enter the field of the contactless reader, this is called discovery.

DKI

Derivation Key Index

DOL

Data Object List

double-length DES Key

Two secret 64-bit input parameters each of the Data Encryption Standard algorithm, consisting of 56 bits that must be independent and random, and 8 error-detecting bits set to make the parity of each 8-bit byte of the key odd.

DRL

Dynamic Reader Limits

Dynamic Card Verification Value (dCVV)

A dynamic signature generated by the card application for MSD Legacy transactions. The dynamic CVV replaces the static CVV placeholder in the Track 2 Equivalent Data.

Dynamic Data Authentication (DDA)

Offline authentication that offers protection against skimming. The card generates an RSA signature using transaction-specific data for validation by the terminal.

Dynamic Signature

A signature generated by the card using dynamic data from both the card and the reader. This signature is validated by the reader to prove that the card is genuine. When used it refers to Signed Dynamic Application Data, tag '9F4B'.

encryption

The process of transforming cleartext into ciphertext.

End Sentinel

Indicator at the end of Track 1 or Track 2 on the magnetic stripe. It is followed by the Longitudinal Redundancy Check.

expired card

A card on which the embossed, encoded, or printed expiration date has passed.

Fast DDA (fDDA)

Leverages DDA as defined in [EMV] and [VIS] specifications. Used in qVSDC transactions to allow the reader to issue READ RECORD commands to obtain Dynamic Data Authentication (DDA) related data from the card and perform the DDA calculations after the card has left the field.

FCI

File Control Information

fDDA

Fast DDA

FFI

Form Factor Indicator

File Control Information

Provided in a card response when the card application is selected (using a SELECT command) by a reader or terminal.

floor limit

A currency amount that Visa has established for single transactions at specific types of merchants, above which online authorization is required.

FWI

Frame Wait time Integer

GPO

GET PROCESSING OPTIONS command

Hardware Security Module (HSM)

A secure module used to store cryptographic keys and perform cryptographic functions.

hash

The result of a non-cryptographic operation, which produces a unique value from a data stream.

Hex

Hexadecimal

HHMMSS

hours, minutes, seconds

HSM

Hardware Security Module

IA

Issuer Authentication

IAD

Issuer Application Data

IAuD

Issuer Authentication Data

IC

integrated circuit

ICC

Integrated Circuit Card

iCVV

An alternate CVV to be used in the image of the Track 2 Equivalent Data personalized on the chip. For MSD Legacy transactions where dCVV is supported, the card application replaces the iCVV or CVV placeholder in Track 2 Equivalent Data with the dCVV.

IDD

Issuer Discretionary Data

IDDO

Issuer Discretionary Data Option

IEC

International Electrotechnical Commission

INS

Instruction byte of Command Message

ISO

International Organization for Standardization

issuer

A Visa customer that issues Visa or Electron cards, or proprietary cards bearing the PLUS or Visa Electron Symbol.

Issuer Authentication

Validation of the issuer by the card to ensure the integrity of the authorization response. *See* Authorization Response Cryptogram (ARPC).

Issuer Update

An update of the card application and its data elements, counters, or indicators due to Issuer Update Processing. The Issuer Update may consist of issuer authentication using the EXTERNAL AUTHENTICATE command and/or application of issuer script commands.

key generation

The creation of a new key for subsequent use.

key management

The handling of cryptographic keys and other related security parameters during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.

Lc

Exact length of data sent by the Terminal Application Layer (TAL) in a Case 3 or 4 command

L_D

Length of the plaintext data in the Command Data Field

Le

Maximum length of data expected by the TAL in response to a Case 2 or 4 command

Longitudinal Redundancy Check

Verification value that ensures no data has been lost in the process of reading the data from the physical magnetic stripe. See the [VPTSM] for additional information.

LRC

Longitudinal Redundancy Check

M

mandatory

MAC

Message Authentication Code

MAC MDK

Master Message Authentication Code DEA Key

MAC UDK

Unique Message Authentication Code DEA Key

magnetic stripe

The stripe on the back of the card that contains the magnetically coded account information necessary to complete a non-chip electronic transaction.

Magnetic Stripe Data (MSD)

Contactless payment using Track 2 Equivalent Data acquired from the chip, or Track 1 constructed from data acquired from the chip, operating under magnetic stripe payment rules.

Magnetic Stripe Image

The minimum chip payment service data replicating information in the magnetic stripe required to process a transaction that is compliant with EMV. (Not allowed as a contactless magnetic stripe solution.)

Master Derivation Key

A double length DES key used to derive card unique keys used in online card authentication.

MBLI

Maximum Buffer Length Index

MCC

Merchant Category Code

MDK

Master Derivation Key

Merchant Category Code (MCC)

A code designating the principal trade, profession, or line of business in which a merchant is engaged.

message authentication code (MAC)

A digital code generated using a cryptographic algorithm which establishes that the contents of a message have not been changed and that the message was generated by an authorized entity.

MSI

Magnetic Stripe Image

MSD

Magnetic Stripe Data

MSD CVN17

MSD transaction with track data and an Application Cryptogram.

MSD-enabled

Card/reader has implemented MSD, and has been personalized/configured to enable the MSD Path.

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 this specification to allow for backwards compatibility to [VCPS 1 4 2].

MSD-only

Card/reader supports MSD and does not support qVSDC.

MSD Path

For transactions conducted over the contactless interface, the MSD Path is an application path taken by the card which results in card behavior defined for MSD. This path is taken for contactless transactions where the reader supports MSD, the card supports MSD, and qVSDC is not mutually supported.

The MSD Path supports only the contactless interface.

multi-application

The presence of multiple applications on a chip card (for example, payment, loyalty, and identification).

n

numeric

N/A

Not Applicable

N_{CA}

Length of the Certification Authority Public Key Modulus

NFC

Near Field Communication

N_I

Length of the Issuer Public Key Modulus

nibble

The four most significant or least significant bits of a byte of data.

N_{IC}

Length of the ICC Public Key Modulus

O

Optional

ODA

Offline Data Authentication

offline approval

A transaction that is positively completed at the point of transaction between the card and terminal without an authorization request to the issuer.

offline authorization

A method of processing a transaction without sending the transaction online to the issuer for authorization.

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. VCPS supports Fast Dynamic Data Authentication (fDDA)

offline decline

A transaction that is negatively completed at the point of transaction between the card and terminal without an authorization request to the issuer.

offline dynamic data authentication

A type of Offline Data Authentication where the card generates a cryptographic value using transaction-specific data elements for validation by the terminal to protect against skimming. Includes both DDA and CDA.

offline PIN

A PIN value stored on the card that is validated at the point of transaction between the card and the terminal.

offline PIN verification

The process whereby a cardholder-entered PIN is passed to the card for comparison to a PIN value stored secretly on the card.

offline-capable

A card acceptance device that is able to perform offline approvals.

offline-only terminal

A card acceptance device that is not capable of sending transactions online for issuer authorization.

online authorization

A method of requesting an authorization through a communications network other than voice to an issuer or issuer representative.

Online Card Authentication (CAM)

Validation of the card by the issuer to protect against data manipulation and skimming. *See* Authorization Request Cryptogram (ARQC).

online PIN

A method of PIN verification where the PIN entered by the cardholder into the terminal PIN pad is DES-encrypted and included in the online authorization request message sent to the issuer.

online-capable terminal

A card acceptance device that is able to send transactions online to the issuer for authorization.

P1

Parameter 1

P2

Parameter 2

PAN

Primary Account Number

Path

An application path taken based on reader/terminal interface and capabilities. The paths defined in this specification are qVSDC and MSD, both supporting only the contactless interface. The VIS path is defined in [VIS], supporting only the contact interface. Card behavior is uniquely defined based on the path taken.

PCD

Proximity Coupling Device

PDOL

Processing Options Data Object List

PICC

Proximity Card

personalization

The process of populating a card with the application data that makes it ready for use.

PIN

Personal Identification Number

PIX

Proprietary Application Identifier Extension

PK

Public Key

PKI

Certificate Authority Public Key Index

plaintext

Data in its original unencrypted form.

PLUS

A global ATM network

POS

Point of Sale

POS Device

A terminal which is installed at the point of sale; e.g., credit card reader, electronic cash register, vending machine.

post-issuance update

A command sent by the issuer through the terminal via an authorization response to update the electronically stored contents of a chip card.

PPSE

Proximity Payment Systems Environment

Pre-processing

Reader Preliminary Transaction Processing

private key

As part of an asymmetric cryptographic system, the key that is kept secret and known only to the owner.

Proximity

In this document, refers to contactless technology as described in [EMV CL].

Proximity Card (PICC)

Identification cards of the card type ID-1 (full size card) operating in proximity to a coupling device.

Proximity Coupling Device (PCD)

The reader/writer device (for example, a dongle) that uses inductive coupling to provide power to the Consumer Device and also to control the data exchange with the Consumer Device.

Proximity Payment 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 FCI with all directory entries in the card response to SELECT of the PPSE ('2PAY.SYS.DDF01').

PSE

Payment System Environment

PSN

Application PAN Sequence Number

public key

As part of an asymmetric cryptographic system, the key known to all parties.

public key cryptographic algorithm

A cryptographic algorithm that allows the secure exchange of information, but does not require a shared secret key, through the use of two related keys—a public key which may be distributed in the clear and a private key which is kept secret.

public key pair

The two mathematically related keys, a public key and a private key which, when used with the appropriate public key cryptographic algorithm, can allow the secure exchange of information, without the secure exchange of a secret.

purchase transaction

A retail purchase of goods or services; a point-of-sale transaction.

PVKI

PIN Verification Key Index

PVV

PIN Verification Value

quasi-cash transaction

A transaction representing a merchant’s sale of items, such as gaming chips or money orders, that are directly convertible to cash.

quick VSDC (qVSDC)

VIS minimized to ensure quick transactions over the contactless interface. Requirements are described in this document.

qVSDC

quick Visa Smart Debit/Credit

qVSDC-enabled

Card/reader has implemented qVSDC, and has been personalized/configured to enable the qVSDC Path.

qVSDC-only

Card/reader supports qVSDC and does not support MSD.

qVSDC Path

For transactions conducted over the contactless interface, the qVSDC Path is an application path taken by the card which results in card behavior defined for qVSDC. This path is taken for contactless transactions where the card and reader both support qVSDC.

The qVSDC Path supports only the contactless interface.

R

required

RCTL

Reader Contactless Transaction Limit

Reader

The merchant device communicating with the card.

See section 3.1.4.1 for additional information.

Reader Risk Parameter

Reader parameters used to perform reader risk management during Reader Preliminary Transaction Processing (Pre-processing).

Reader Limit Set

An acquirer-merchant configurable combination of Reader Risk Parameters to be used during Reader Risk Parameters Checking. The acquirer-merchant is able to enable or disable the individual Reader Risk Parameters in the Reader Limit Set, and to set the value of any corresponding limits.

receipt

A paper record of a transaction generated for the cardholder at the point of transaction.

RF

Radio Frequency

RFU

Reserved for Future Use

RID

Registered Application Provider Identifier

RSA

A public key cryptosystem developed by Rivest, Shamir, and Adleman (RSA), and used for data encryption and authentication.

SAD

Signed Static Application Data

SD

Special Device

SDA

Static Data Authentication

SDAD

Signed Dynamic Application Data

secret key

A key that is used in a symmetric cryptographic algorithm (that is, DES), and cannot be disclosed publicly without compromising the security of the system. This is not the same as the private key in a public/private key pair.

secure messaging

A process that enables messages to be sent from one entity to another, and protects against unauthorized modification or viewing.

session key

A temporary cryptographic key computed in volatile memory and not valid after a session is ended.

SFI

Short File Identifier

SHA-1

Secure Hash Algorithm

Single Unit of Currency

A single unit of currency is one unit of that currency. One dollar U.S. currency, for example, or one pound in British currency. A transaction containing a single unit of currency is used at some merchants to indicate a Status Check on the account.

Start Sentinel

Indicator at the beginning of Track 1 or Track 2 on the magnetic stripe.

Static Data Authentication (SDA)

A type of Offline Data Authentication where the terminal validates a cryptographic value placed on the card during personalization. This validation protects against some types of counterfeit, but does not protect against skimming.

Status Check

An online authorization for a single unit of currency. In some markets, status checks are used as authorizations for automated fuel dispensing, implicitly allowing up to a set amount to be used. The use of status checks is limited to automated fuel dispensing.

Status Word

SW1 and SW2, collectively.

SW1 SW2

Status Byte One and Status Byte Two

TAC

Terminal Action Codes

TAL

Terminal Application Layer

TC

Transaction Certificate

TLV

Tag Length Value

transaction

An exchange of information between a cardholder and a merchant or an acquirer that results in the completion of a financial transaction.

Transaction Certificate

An Application Cryptogram generated when accepting a transaction.

Triple DES

The data encryption algorithm used with a double-length DES key.

TSI

Transaction Status Information

TTQ

Terminal Transaction Qualifiers

TVR

Terminal Verification Results

UDK

Unique Derivation Key

UDKA

Unique Derivation Key A

UDKB

Unique Derivation Key B

Unique Derivation Key

A card-unique double-length DES key derived from a master key and used in online card authentication.

VCPS

Visa Contactless Payment Specification

VCPS Transaction

A transaction conducted over the contactless interface in compliance with this specification.

VIS

Visa Integrated Circuit Card Specification

VIS Path

For transactions conducted over the contact interface, the VIS Path is an application path taken by the card which results in card behavior defined for VIS.

The VIS Path supports only the contact interface.

Visa AID

An AID using the Visa Registered Application Provider Identifier (RID, 'A0 00 00 00 03') that has a Proprietary Application Identifier Extension (PIX) assigned by Visa International.

Visa PIXs:

'1010' – Visa Debit and Visa Credit

'2010' – Visa Electron

'3010' – Interlink

'8010' – PLUS

Regional AIDs using the reserved range of Visa assigned PIXs are permitted.

Visa Certificate Authority (CA)

A Visa-approved organization certified to issue certificates to participants in a Visa payment service.

Visa Contactless Payment Specification (VCPS)

A Visa specification defining requirements for conducting a payment transaction over a contactless interface.

Visa Smart Debit/Credit (VSDC)

The Visa payment service offerings for chip-based debit and credit programs. These services are supported by VisaNet processing, as well as by Visa rules and regulations; and are based on EMV and VIS, VCPS, or EMV Common Core Definitions (CCD) – including Common Payment Application (CPA) – specifications.

VisaNet

The systems and services, including the V.I.P. and BASE II systems, through which Visa delivers online financial processing, authorization, clearing, and settlement services to customers.

VLP

Visa Low-value Payment

VSDC

Visa Smart Debit/Credit

XOR

Exclusive-OR

YDDD

Year, day:

Y	right-most digit of the year (‘0’–’9’)
DDD	Julian day of the year (‘001’–’366’)

YYMM

Year, month:

YY	year (‘00’–’99’)
MM	month (‘01’–’12’)

YYMMDD

Year, month, day:

YY	year (‘00’–’99’)
MM	month (‘01’–’12’)
DD	day (‘01’–’31’)