POS Message Interface
Heartland Integrator's Guide

Version 17.2
November 2017

Heartland

Notice

THE INFORMATION CONTAINED HEREIN IS PROVIDED TO RECIPIENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTY OF TITLE OR NON-INFRINGEMENT. HEARTLAND PAYMENT SYSTEMS, LLC ("HEARTLAND") MAKES NO WARRANTIES OR REPRESENTATIONS THAT THE MATERIALS, INFORMATION, AND CONTENTS HEREIN ARE OR WILL BE ERROR FREE, SECURE, OR MEET RECIPIENT'S NEEDS. ALL SUCH WARRANTIES ARE EXPRESSLY DISCLAIMED.

RECIPIENT'S USE OF ANY INFORMATION CONTAINED HEREIN IS AT RECIPIENT'S SOLE AND EXCLUSIVE RISK. IN NO EVENT SHALL HEARTLAND BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, WHETHER RESULTING FROM BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, EVEN IF HEARTLAND HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. HEARTLAND RESERVES THE RIGHT TO MAKE CHANGES TO THE INFORMATION CONTAINED HEREIN AT ANY TIME WITHOUT NOTICE.

THIS DOCUMENT AND ALL INFORMATION CONTAINED HEREIN IS PROPRIETARY TO HEARTLAND, RECIPIENT SHALL NOT DISCLOSE THIS DOCUMENT OR THE SYSTEM DESCRIBED HEREIN TO ANY THIRD PARTY UNDER ANY CIRCUMSTANCES WITHOUT PRIOR WRITTEN CONSENT OF A DULY AUTHORIZED REPRESENTATIVE OF HEARTLAND. IN ORDER TO PROTECT THE CONFIDENTIAL NATURE OF THIS PROPRIETARY INFORMATION, RECIPIENT AGREES:

(A) TO IMPOSE IN WRITING SIMILAR OBLIGATIONS OF CONFIDENTIALITY AND NONDISCLOSURE AS CONTAINED HEREIN ON RECIPIENT'S EMPLOYEES AND AUTHORIZED THIRD PARTIES TO WHOM RECIPIENT DISCLOSES THIS INFORMATION (SUCH DISCLOSURE TO BE MADE ON A STRICTLY NEED-TO-KNOW BASIS) PRIOR TO SHARING THIS DOCUMENT AND

(B) TO BE RESPONSIBLE FOR ANY BREACH OF CONFIDENTIALITY BY THOSE EMPLOYEES AND THIRD PARTIES TO WHOM RECIPIENT DISCLOSES THIS INFORMATION.

RECIPIENT ACKNOWLEDGES AND AGREES THAT USE OF THE INFORMATION CONTAINED HEREIN SIGNIFIES ACKNOWLEDGMENT AND ACCEPTANCE OF THESE TERMS. ANY SUCH USE IS CONDITIONED UPON THE TERMS, CONDITIONS AND OBLIGATIONS CONTAINED WITHIN THIS NOTICE.

THE TRADEMARKS AND SERVICE MARKS RELATING TO HEARTLAND'S PRODUCTS OR SERVICES OR THOSE OF THIRD PARTIES ARE OWNED BY HEARTLAND OR THE RESPECTIVE THIRD PARTY OWNERS OF THOSE MARKS, AS THE CASE MAY BE, AND NO LICENSE WITH RESPECT TO ANY SUCH MARK IS EITHER GRANTED OR IMPLIED.

To verify existing content or to obtain additional information, please call or email your assigned Heartland contact.

Release Notes

Version 17.2 Release Notes

Chapter/Appendix	Revisions
General Format and Global Changes	• Red change bars added on clarification and project updates. • For clarification purposes only: Some content modified and reformatted (with no change bar), with no impact to development.
Chapter 6: EMV Development Overview	• Removed out of date Version 2.x for approved PED or EPP devices from the following sections: – *6.1.1 Contact Devices, p. 105* – *6.1.2 Contactless Devices, p. 105* • Removed version numbers from the following test plan tables: – *Table 6-2 VSDC Testing, p. 108* – *Table 6-3 M-TIP Testing, p. 108* – *Table 6-4 AEIPS Testing, p. 108* – *Table 6-5 D-PAS Testing, p. 109*
Chapter 7: EMV Terminal Interface	• *Table 7-4 Terminal Data, p. 116*: Added clarification to ISSUER SCRIPT RESULTS from EMVCo document that Bytes 1-5 are repeated. • *Table 7-11 Available AIDs, p. 141*: – Added Note stating that standard credit AIDs for Mastercard and Visa support their fleet, business, corporate, consumer cards, etc. – For Discover U.S. Common Debit AID, removed the note that stated it was not supported for PIN Debit. It is now supported. – CUP: Added Union Pay AIDs.
Chapter 8: EMV Parameter Interface	• *Table 8-2 Platform Identifiers to EMV PDL System, p. 163*: Added a row for the 8583 platform field identifiers for EMV PDL (DE41, DE42, DE62).
Appendix D: EMV Field Definitions	• *Table D-22 Form Factor Indicator, p. 234*: Correction, 9F6E is mandatory for MasterCard contactless.

This page intentionally left blank for duplex printing.

Table of Contents

List of Tables

List of Figures

Chapter 1: Overview

1.1 Introduction

Heartland Payment Systems, LLC (Heartland) is a leading third-party provider of payment card transaction processing, providing the following services:

- Host Network transaction services
- Bankcard, Fleet, Debit and Private Label card processing
- Mobile and e-commerce solutions
- Settlement processing

1.2 Document Purpose

The purpose of this document is to provide information in order to integrate a POS system to Heartland. Topics include:

- *General POS Requirements*
- *Card Brand Information*
- *E3 Processing Overview*
- *EMV Processing Overview*
- *EMV Development Overview*
- *EMV Terminal Interface*
- *EMV Parameter Interface*
- *Industry Codes*
- *Receipt Requirements*
- *State Codes / Region Codes*
- *EMV Field Definitions*
- *EMV PDL Data Examples*
- *Glossary*

REQUIREMENT	**This document is to be used along with Heartland's Network platform specifications (Exchange, POS 8583, NTS, Z01, Portico, SpiDr).** Information found in the Network specifications could override content within this document.

1.3 Audience

The primary audience for this document consists of third-party vendors responsible for developing POS payment systems to interface with the Heartland network. The secondary audience consists of Heartland internal staff responsible for certifying or supporting POS payment applications. All users of this document are assumed to have a basic understanding of POS applications.

1.4 Payment Application Data Security Standards (PA-DSS)

The Payment Card Industry (PCI) Security Standards Council (SSC) has released the Payment Application Data Security Standards (PA-DSS) for payment applications running at merchant locations. The PA-DSS assist software vendors to ensure their payment applications support compliance with the mandates set by the bankcard companies (Visa, Mastercard, Discover, American Express, and JCB).

In order to comply with the mandates set by the bankcard companies, Heartland:

- Requires that the account number cannot be stored as plain, unencrypted data to meet PCI and PA-DSS regulations. It must be encrypted while stored using strong cryptography with associated key management processes and procedures.

  Note: Refer to PCI DSS Requirements 3.4–3.6* for detailed requirements regarding account number storage. The retention period for the Account Number in the shadow file and open batch must be defined and at the end of that period or when the batch is closed and successfully transmitted, the account number and all other information must be securely deleted. This is a required process regardless of the method of transmission for the POS.
- Requires that, with the exception of the Account Number as described above and the Expiration Date, **no** other Track Data is to be stored on the POS if the Card Type is a:
  - Visa, including Visa Fleet;
  - Mastercard, including Mastercard Fleet, and Carte Blanche;
  - Discover, including JCB, UnionPay, Diner's Club, and PayPal;
  - American Express;
  - Debit or EBT.
- This requirement does **not** apply to WEX, FleetCor, Fleet One, Voyager, or Aviation cards; Stored Value cards; Proprietary or Private Label cards.
- Recommends that software vendors to have their applications validated by an approved third party for PA-DSS compliance.
- Requires all software vendors to sign a Non-Disclosure Agreement / Development Agreement.
- Requires all software vendors to provide evidence of the application version listed on the PCI Council's website as a PA-DSS validated Payment Application, or a written certification to HPS testing to Developer's compliance with PA-DSS.
- Requires that all methods of cryptography provided or used by the payment application meet PCI SSC's current definition of 'Strong Cryptography'.

*Refer to *www.pcisecuritystandards.org* for the PCI DSS Requirements document and further details about PA-DSS.

Chapter 2: General POS Requirements

2.1 Address Verification Service

Visa, Mastercard, AMEX and Discover offer an Address Verification Service (AVS) as a risk-management tool for merchants accepting transactions in which:

- neither the card nor the cardholder are present (e.g., mail, telephone order, Internet transactions), or
- the card is present but its magnetic stripe cannot be read by a terminal at the point of sale.

AVS helps reduce the risk of accepting fraudulent transactions by issuer verification of the cardholder's billing address. The AVS Result Code helps the merchant determine whether to accept a particular transaction or to take further follow-up action.

When a merchant accepts a card-not-present transaction, financial liability is also accepted by the merchant in the event the transaction proves to be fraudulent. If the transaction is fraudulent, the dollar value of the transaction may be "charged back" to the merchant. In addition to the "charge back," there are additional costs to process these exception items, plus the loss of merchandise.

Table 2-1 Address Verification Service

AVS Request	Description
Address Verification Request	Address verification may be requested in one of two ways: • by itself, or • as part of an authorization request.
AVS By Itself (AVS Only)	An AVS only request may be used under the following circumstances: • a merchant wants to verify the customer's billing address before requesting an authorization, or • the merchant sent an AVS and an authorization request earlier and received an authorization approval but an AVS "try again later" response.

Table 2-1 Address Verification Service (Continued)

AVS Request	Description
AVS Authorization Request	You may process AVS requests the same way you process authorizations simply by including the AVS information in the authorization request. The authorization and address verification process is as follows: • Customer contacts the merchant to place an order. • The merchant confirms the usual order information including the merchandise description, price, the customer's account number, card expiration date, and shipping address. • The merchant requests the cardholder's billing address (street address and/or ZIP Code) for the card being used. (The billing address is where the cardholder's monthly statement is sent for the card being used.) • The POS system includes the address information with the authorization request to Heartland. • The issuer makes an authorization decision separately from the AVS request. The issuer compares the cardholder billing address with the billing address it has for that account. The issuer returns both the authorization response and a code indicating the address verification results. Like any other transaction, if the issuer declines the authorization request do not complete the transaction for that account. This rule holds true even if you receive an "exact match" on the address verification request.

2.1.1 AVS Data Flow

2.1.2 AVS Result Code Guidelines

Not all Heartland POS message specifications support AVS Result Codes. See your specific POS message specification for details.

For some industries, if the AVS Result Code is not a match, the payment engine automatically declines and voids the transaction to the issuer.

For other industries, the merchant makes the decision on whether to proceed when the AVS information is not an exact match, but the issuer approves the authorization request. See you Heartland Representative for more information.

2.2 Chargeback Protected Limits

The following amounts are the ICR-initiated chargeback protected amounts for approved transactions by the bank card associations.

The merchant may choose to override these amounts. Any amount above the limits listed will **not** include Chargeback Protection.

The merchant is at risk for any amount above these limits.

Table 2-2 Chargeback Protected Limits

Card Type	Description
Visa	• Visa Consumer (including Visa Signature and Sign Preferred), Visa Business (including Visa Signature Business), Visa Corporate, and Visa Purchasing cards offer Chargeback Protection to $100 if the card has been authorized for $1.00. • Visa Fleet cards offer Chargeback Protection to $150 if the card has been authorized for $1.00.
Mastercard	• Mastercard Consumer cards offer Chargeback Protection to $100 if the card has been authorized for $1.00. • Mastercard Corporate, Mastercard Corporate Fleet, and Mastercard Purchasing cards offer Chargeback Protection to $150 if the card has been authorized for $1.00.
Discover Card	• Discover Card offers Chargeback Protection to $100 if the card has been authorized for $1.00. If the merchant has a custom agreement with Discover to authorize for a different amount, chargeback protection is the approved amount.
American Express	• American Express does not offer Chargeback Protection.

2.3 No Signature Required

No Signature Required is a program offered by Visa, Mastercard, AMEX and Discover for consumer and commercial cards. The No Signature Required program allows merchants within certain MCC codes to process transactions without having to obtain the cardholders signature or provide the cardholder with a receipt unless the cardholder requests it.

In order to be eligible for No Signature Required, the following conditions must be met:

- The cardholder must be present at the time of the transaction in a face-to-face environment.
- The merchant name and location must be included in the authorization request.
- The total amount of the transaction must be less than the No Signature Required threshold for the merchant's MCC. Refer to the individual card associations for current information about amounts, MCCs allowed, etc.
- Online authorization must be obtained and the full track data must be included in the authorization message. The track data can be obtained from the chip for EMV transactions or from the magnetic stripe for swiped transactions.

To process a No Signature Required transaction with a chip card (on a chip-card-capable POS terminal), the terminal application must set the Terminal Capabilities field to enable only the No CVM Required card verification method (CVM). This action will cause the chip card not to require a CVM.

2.4 Binary to ASCII Hex Conversion

Since some the Host message formats allow for only printable characters to appear in transaction data fields. Binary fields must be expanded to ensure that no values less than hexadecimal **20** are transmitted.

To convert a binary field to its corresponding ASCII equivalent, remove 4 bits at a time and convert them to the ASCII characters defined below. Performing this conversion procedure will result in a doubling of the field size, i.e., a 20-digit binary field will yield a 40-character ASCII result. After performing the conversion, the resulting ASCII data may then be populated within the transaction data field.

Table 2-3 Binary to ASCII Hex Conversion

BIT Data	ASCII Hex Characters
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

The table below shows examples of data before conversion as well as after the ASCII conversion as the data moves from the POS to the Host.

The order of the fields is arbitrary and the values used below are only provided as an example.

Table 2-4 Binary ASCII Hex Conversion Example

Field Name	RED is Before Conversion		BLUE is after conversion	
UNPREDICTABLE NUMBER	Tag	9F37	Tag	39463337
	Length	04	Length	3034
	Value	00010203	Value	3030303130323033
ISSUER APPLICATION DATA	Tag	9F10	Tag	39463130
	Length	20	Length	3230
	Value	000102030405060708090A0B0C0D0E0F10111213141516171819A1B1C1D1E1F	Value	3030303130323033303430353036303730383039303413042304330443045304631303131313231333134313531363137313831393141314231433144314531 46
APPLICATION CRYPTOGRAM	Tag	9F26	Tag	39463236
	Length	08	Length	3038
	Value	0001020304050607	Value	3030303130323033303430353036303730 37
APPLICATION TRANSACTION COUNTER	Tag	9F36	Tag	39463336
	Length	02	Length	3032
	Value	0001	Value	30303031

Chapter 3: Card Brand Information

3.1 Introduction

This chapter gives an overview of payment cards, embossing information, including Track 1 and Track 2 layouts.

The maximum length of Track 1 is 79 characters. This length includes the START SENTINEL, FIELD SEPARATORS, END SENTINEL and LONGITUDINAL REDUNDANCY CHECK (LRC) fields. The Track 1 overall length will vary by card after the CARDHOLDER NAME field.

The maximum length of Track 2 is 40 characters. This length includes the START SENTINEL, FIELD SEPARATOR, END SENTINEL, and LONGITUDINAL REDUNDANCY CHECK (LRC) fields.

Track Data is sent unaltered.

Track data is defined by a number of *International Organization for Standardization* standards. *ISO/IEC 7810*, *ISO/IEC 7811*, *ISO/IEC 7812*, *ISO/IEC 7813*, *ISO 8583*, and *ISO/IEC 4909*, now define the physical properties of the card, including size, flexibility, location of the magstripe, magnetic characteristics, and data formats. They also provide the standards for financial cards, including the allocation of card number ranges to different card issuing institutions. The standards should be referenced for details on track data.

Refer to the specific POS message specifications (Exchange, POS 8583, NTS, Z01, Portico, SpiDr) to determine cards supported, transactions supported and data requirements.

Note: For chip cards (Service Code 2xx or 6xx) Track 2 is preferred for all card brands.

Table 3-1 Card Brand References to Track Data

Card Type	Track Preference when Swiped	Track Data
American Express	Track 1	• 3.2.1 American Express Track 1 Format X4.16 Standard, p. 30 • 3.2.2 American Express Track 1 Format ISO 7813 Standard, p. 31 • 3.2.3 American Express Track 2 Format X4.16 Standard, p. 33 • 3.2.4 American Express Track 2 Format ISO 7813 Standard, p. 33
AVcard	No preference	• 3.3.1 AVcard Track 1 Format, p. 35 • 3.3.2 AVcard Track 2 Format, p. 35
Centego	Track 2	• 3.4.1 Centego Prepaid Track 1 Format, p. 36 • 3.4.2 Centego Prepaid Track 2 Format, p. 37
Diner's Club (Now processed as Discover)	No preference	• 3.6.1 Diner's Club International Track 1 Format, p. 40 • 3.6.2 Diner's Club International Track 2 Format, p. 41
Discover	No preference	• 3.5.1 Discover Track 1 Format, p. 38 • 3.5.2 Discover Track 2 Format, p. 39
Drop Tank	No preference	• 3.7.1 Drop Tank Track 1 Format, p. 42 • 3.7.2 Drop Tank Track 2 Format, p. 42
EBT	Track 2 only	• 3.9.1 EBT Track 2 Format, p. 44
Fleet One	Track 2 only	• 3.10.1 Fleet One Track 2 Format, p. 45
FleetCor	Track 2 only	• 3.11.1 FleetCor Track 2 Format, p. 46
Heartland Gift Card	Track 2 only	• 3.8.1 Heartland Gift Card Track 2 Format, p. 43
Mastercard	No preference	• 3.13.1 Mastercard Track 1 Format, p. 48 • 3.13.2 Mastercard Track 2 Format, p. 48
Mastercard Corporate	No preference	• 3.13.1 Mastercard Track 1 Format, p. 48 • 3.13.2 Mastercard Track 2 Format, p. 48
Mastercard Fleet	No preference	• 3.14.3 Mastercard Fleet Track 1 Format, p. 51 • 3.14.4 Mastercard Fleet Track 2 Format, p. 52
Mastercard Purchasing	No preference	• 3.15.2 Mastercard Purchasing Track 1 Format, p. 53 • 3.15.3 Mastercard Purchasing Track 2 Format, p. 54
Mills Fleet Farm PLCC	No preference	• 3.15.4 Mills Fleet Farm PLCC Track 1 Format, p. 55 • 3.15.5 Mills Fleet Farm PLCC Track 2 Format, p. 56
Multi Service	Track 2 only	• 3.16.1 Multi Service Swiped Track 2 Format, p. 57
PayPal	No preference	• 3.5.1 Discover Track 1 Format, p. 38 • 3.5.2 Discover Track 2 Format, p. 39
PIN Debit	Track 2 only	Issuer dependent.
Stored Value	Track 2	• 3.18.1 SVS Track 1 Format, p. 58 • 3.18.2 SVS Track 2 Format, p. 58
ValueLink	Track 2	• 3.20.1 ValueLink Track 1 Format, p. 59 • 3.20.2 ValueLink Track 2 Format, p. 60

Table 3-1 Card Brand References to Track Data (Continued)

Card Type	Track Preference when Swiped	Track Data
Visa	Track 2	• *3.21.1 Visa Track 1 Format, p. 61* • *3.21.2 Visa Track 2 Format, p. 62*
Visa Corporate or Business	No preference	• *3.21.1 Visa Track 1 Format, p. 61* • *3.21.2 Visa Track 2 Format, p. 62* Use Visa Track layouts for Visa Corporate or Business.
Visa Fleet	Track 1	• *3.24.2 Visa Fleet Track 1 Format, p. 64* • *3.24.3 Visa Fleet Track 2 Format, p. 65*
Visa Purchasing	No preference	• *3.21.1 Visa Track 1 Format, p. 61* • *3.21.2 Visa Track 2 Format, p. 62* Use Visa Track layouts for Visa Purchasing.
Visa ReadyLink	Track 2	• *3.21.1 Visa Track 1 Format, p. 61* • *3.21.2 Visa Track 2 Format, p. 62* Use Visa Track layouts for Visa ReadyLink.
Voyager Fleet	No preference	• *3.25.2 Voyager Fleet Track 1 Format, p. 68* • *3.25.3 Voyager Fleet Track 2 Format, p. 69*
WEX Fleet	Track 2 only	• *3.26.3 WEX Fleet Track 2 Format, p. 72*

3.2 American Express

American Express issues cards in either of following track formats.

- ANSI X4.16
- ISO 7813

3.2.1 American Express Track 1 Format X4.16 Standard

Table 3-2 American Express Track 1 Format X4.16 Standard

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3varies	15–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (caret)
CARD MEMBER NAME	varies	26	A/N	Field identifies the name of the cardholder and contains a maximum of 26 characters. The format of the field is last name followed by first name and initial. Each cardholder name component is separated as follows: • / (forward slash) = Separates the first and last name. • (space) = Separates first name from the middle name or middle initial. Use only when the cardholder names qualify for separation. • . (period) = Separates the first name and title. **Example:** Last Name/First Name Initial Embossing JOHN P. JONES JR. Mag Stripe JONES/JOHN P.JR
FIELD SEPARATOR	varies	1	A/N	^ (caret)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format. The card expires on the last day of the month.
EFFECTIVE DATE	varies	4	N	The date in YYMM format. The card becomes valid on the first day of the month.
DISCRETIONARY DATA	varies	5	N	
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment. LRC may or may not be present.
UNUSED	varies	17	A/N	Reserved for future use.

3.2.2 American Express Track 1 Format ISO 7813 Standard

Table 3-3 American Express Track 1 Format ISO 7813 Standard

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3varies	15–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
CARD MEMBER NAME	varies	26	A/N	Field identifies the name of the cardholder and contains a maximum of 26 characters. The format of the field is last name followed by first name and initial. Each cardholder name component is separated as follows: • / (forward slash) = Separates the first and last name. • (space) = Separates first name from the middle name or middle initial. Use only when the cardholder names qualify for separation. • . (period) = Separates the first name and title. **Example:** Last Name/First Name Initial Embossing JOHN P. JONES JR. Mag Stripe JONES/JOHN P.JR
FIELD SEPARATOR	varies	1	A/N	^ (carat)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format. The card expires on the last day of the month.
INTERCHANGE DESIGNATOR	varies	1	N	Code indicating whether the American Express card is valid outside the country of issue. • 1 = Available for international interchange • 2 = Chip card • 5 = Available for interchange only in country of issue • 6 = Chip card, available for interchange only in country of issue • 7 = Not available for general interchange • 9 = System test card

Table 3-3 American Express Track 1 Format ISO 7813 Standard (Continued)

Field Name	Position	Length	Format	Value/Description
SERVICE CODE	varies	2	N	Code indicating whether the American Express card is valid for ATM/Cash Access or if a positive authorization is required. • 01 = No restrictions • 02 = No ATM service • 03 = ATM Service only • 06 = No restrictions; prompt for PIN, if PIN pad is present • 10 = No cash advance • 11 = No cash advance or ATM service • 20 = Requires positive authorization by issuer or issuer's agent • 21 = Authorization by issuer only • 22 = Authorization by issuer only; Goods & Services • 23 = Authorization by issuer only; ATM only, PIN required • 26 = Authorization by issuer only; prompt for PIN, if PIN pad is present
EFFECTIVE DATE	varies	4	N	The date in YYMM format. The card becomes valid on the first day of the month.
DISCRETIONARY DATA	varies	5	N	
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.
UNUSED	varies	17	A/N	Reserved for future use.

3.2.3 American Express Track 2 Format X4.16 Standard

Table 3-4 American Express Track 2 Format X4.16 Standard

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2varies	15–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format. The card expires on the last day of the month.
EFFECTIVE DATE	varies	4	N	The date in YYMM format. The card becomes valid on the first day of the month.
DISCRETIONARY DATA	varies	5	N	
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment. LRC may or may not be present.
UNUSED	varies	8	N	Reserved for future use.

3.2.4 American Express Track 2 Format ISO 7813 Standard

Table 3-5 American Express Track 2 Format ISO 7813 Standard

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2varies	15–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format. The card expires on the last day of the month.

Table 3-5 American Express Track 2 Format ISO 7813 Standard (Continued)

Field Name	Position	Length	Format	Value/Description
INTERCHANGE DESIGNATOR	varies	1	N	Code indicating whether the American Express card can be used outside the country of issue. • 1 = Available for international interchange • 2 = Chip card • 5 = Available for interchange only in country of issue • 6 = Chip card, available for interchange only in country of issue • 7 = Not available for general interchange • 9 = System test card
SERVICE CODE	varies	2	N	Code indicating whether the American Express card is valid for ATM/Cash Access or if a positive authorization is required. • 01 = No restrictions • 02 = No ATM service • 03 = ATM Service only • 06 = No restrictions; prompt for PIN, if PIN pad is present • 10 = No cash advance • 11 = No cash advance or ATM service • 20 = Requires positive authorization by issuer or issuer's agent • 21 = Authorization by issuer only • 22 = Authorization by issuer only; Goods & Services • 23 = Authorization by issuer only; ATM only, PIN required • 26 = Authorization by issuer only; prompt for PIN, if PIN pad is present
EFFECTIVE DATE	varies	4	N	The date in YYMM format. The card becomes valid on the first day of the month.
DISCRETIONARY DATA	varies	8	N	
LANGUAGE CODE	varies	2	N	Code indicating non-Canadian versus Canadian cardholders and when a Canadian, whether English or French is the spoken language of the cardholder. • 00 = Non-Canadian Card member • 01 = Canadian Card members (English Language) • 02 = Canadian Card members (French Language)
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	N	Created by the encoding equipment.

3.3 AVcard

The AVcard requires a date check and a MOD-10 check.

3.3.1 AVcard Track 1 Format

Table 3-6 AVcard Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	^ (caret)
ISO PREFIX	3	6	N	601029
ACCOUNT NUMBER	9	13^{max}	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (caret)
CREDIT CARD NAME	varies	26^{max}	A/N	Customer or company name.
FIELD SEPARATOR	varies	1	A/N	^ (caret)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE INDICATOR	varies	3	N	Constant, 701
DISCRETIONARY DATA	varies	15	A/N	Miscellaneous Cardholder Info.
END SENTINEL	varies	1	A/N	? (question mark)

3.3.2 AVcard Track 2 Format

Table 3-7 AVcard Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
ISO PREFIX	2	6	N	601029
ACCOUNT NUMBER	8	13^{max}	N	AVcard Account Number.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	YYMM
SERVICE CODE INDICATOR	varies	3	N	Constant, 701
DISCRETIONARY DATA	varies	15		Miscellaneous Cardholder Info.
END SENTINEL	varies	1	A/N	? (question mark)

3.4 Centego Prepaid Card

PAN must pass MOD 10 check-digit test. (MOD 10 check on first 18 digits, 19th digit is the check digit.)

Cards are embossed with the Account Number.

3.4.1 Centego Prepaid Track 1 Format

Note: Track data must be sent excluding the START SENTINEL, END SENTINEL, and LRC.

Table 3-8 Centego Prepaid Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3–21	19	N	Cardholder's PAN.
FIELD SEPARATOR	22	1	A/N	^ (caret)
CARDHOLDER NAME	23–48	26^{max}	A/N	Contains a maximum of 26 characters.
FIELD SEPARATOR	49	1	A/N	^ (caret)
EXPIRATION DATE	50–53	4	N	The date the card expires in YYMM format.
SECURITY DATA	54–63	10	N	Card verification value.
MEMBER NUMBER	64–74	11	A/N	Club member number.
END SENTINEL	75	1	A/N	? (question mark)
LRC	76	1	A/N	Created by the encoding equipment.

Note: The position ranges are valid for a 26-character cardholder name. The cardholder name is a variable length field delimited by field separators. As a result, position ranges following the CARDHOLDER field will change with varying CARDHOLDER field lengths.

3.4.2 Centego Prepaid Track 2 Format

Table 3-9 Centego Prepaid Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2–20	19	N	Cardholder's PAN.
FIELD SEPARATOR	21	1	A/N	= (equal sign)
EXPIRATION DATE	22–25	4	N	The date the card expires in YYMM format.
SECURITY DATA	26–35	10	N	Card verification value.
END SENTINEL	36	1	A/N	? (question mark)
LRC	37	1	A/N	Created by the encoding equipment.

3.5 Discover Card

Discover Network (now known as DFS Services, LLC) allocates Issuer Identification Number (IIN) ranges to authorized Issuers using the Discover Network.

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number and the Expiration Date.

3.5.1 Discover Track 1 Format

Table 3-10 Discover Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3varies	16–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
CARDHOLDER NAME	varies	varies	A/N	Field identifies the name of the cardholder and contains a maximum of 26 characters. The format of this field is last name followed by first name and initial. A / (forward slash) separates the first and last name. **Example:** Last Name/First Name Initial Embossing John P. Jones III Mag Stripe Jones III/John P
FIELD SEPARATOR	varies	1	A/N	^ (carat)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	Identifies the circumstances under which the card can be used.
SECURITY CODE	varies	13	A/N	
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.5.2 Discover Track 2 Format

Table 3-11 Discover Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2^{varies}	16–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	Identifies the circumstances under which the card can be used.
SECURITY CODE	varies	13	A/N	
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.6 Diner's Club International Card

The Diner's Club International card must also be processed as a Discover Card.

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number and the Expiration Date.

3.6.1 Diner's Club International Track 1 Format

Table 3-12 Diner's Club International Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3varies	14–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
CARDHOLDER NAME	varies	varies	A/N	Field identifies the name of the cardholder and contains a maximum of 26 characters. The format of the field is last name followed by first name and initial. Each cardholder name component is separated as follows: • / (forward slash) = Separates the first and last name. • (space) = Separates first name from the middle name or middle initial. It is also used to separate a title from the first name or middle name or initial. Used to separate a title only when the cardholder names qualify for separation. **Example:** Last Name/First Name Initial Embossing JOHN P. JONES JR. Mag Stripe JONES/JOHN P JR
FIELD SEPARATOR	varies	1	A/N	^ (carat)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
INTERCHANGE QUALIFICATION CODE	varies	3	N	Code indicating the type of interchange that is available on the card. Valid codes: • 101 = Card is valid for unrestricted international interchange. • 587 = Card is valid only in territory of issuance.
EFFECTIVE DATE	varies	4	A/N	The data in YYMM format.
END SENTINEL	varies	1	A/N	? (question mark)

Table 3-12 Diner's Club International Track 1 Format (Continued)

Field Name	Position	Length	Format	Value/Description
LRC	varies	1	A/N	Created by the encoding equipment.

3.6.2 Diner's Club International Track 2 Format

Table 3-13 Diner's Club International Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2varies	14–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
INTERCHANGE QUALIFICATION CODE	varies	3	N	Code indicating the type of interchange that is available on the card. Valid codes: • 101 = Card is valid for unrestricted international interchange. • 587 = Card is valid only in territory of issuance.
EFFECTIVE DATE	varies	4	N	The data in YYMM format.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.7 Drop Tank Card

Use DAMM algorithm when processing these cards. Do not use MOD 10 check.

3.7.1 Drop Tank Track 1 Format

Table 3-14 Drop Tank Track 1 Format

Field Name	Position	Length	Format	Value Description
START SENTINEL	1	1	Hex	% (percent sign)
FORMAT CODE	2	1	A/N	b
ACCOUNT NUMBER	3–20	18	N	Cardholder's PAN (token).
FIELD SEPARATOR	21	1	A/N	^ (caret)
FILLER	22	1	A/N	Space
FIELD SEPARATOR	23	1	A/N	^ (caret)
FILLER	24	1	A/N	Space
END SENTINEL	25	1	A/N	? (question mark)
LRC	26	1	A/N	Created by the encoding equipment. LRC may or may not be present.

3.7.2 Drop Tank Track 2 Format

Table 3-15 Drop Tank Track 2 Format

Field Name	Position	Length	Format	Value Description
START SENTINEL	1	1	Hex	; (semicolon)
ACCOUNT NUMBER	2–19	18	N	Cardholder's PAN (token).
FIELD SEPARATOR	20	1	A/N	= (equal sign)
DATE	21-24	4	N	Expiration date in MMYY format.
END SENTINEL	25	1	A/N	? (question mark)
LRC	26	1	A/N	Created by the encoding equipment. LRC may or may not be present.

3.8 Heartland Gift Card

PAN must pass a MOD 10 check-digit test. The 19th position is the check-digit for the proceeding 18 digits).

Cards are embossed with the Account Number and the printed Access Code on the back.

3.8.1 Heartland Gift Card Track 2 Format

Table 3-16 Heartland Gift Card Track 2 Format

Field Name	Position	Length	Format	Value Description
START SENTINEL	1	1	3B Hex	; (semicolon)
PRIMARY ACCOUNT NUMBER	2–20	19	N	Cardholder's PAN.
FIELD SEPARATOR	21	1	A/N	= (equal sign)
DATE	22–25	4	N	Expiration date in MMYY format. Default expiration is 9999.
SECURITY DATA	26–38	13	N	
END SENTINEL	39	1	A/N	? (question mark)
LRC	40	1	OF Hex	Longitudinal Redundancy Check.

3.9 EBT Card

The POS application must perform a MOD 10 check.

No Specific ISO – No information in the account number or track data identifies the card as a Food Stamp or Cash Benefit card. This identification must come from POS prompts.

3.9.1 EBT Track 2 Format

Table 3-17 EBT Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2–20	19	N	Cardholder's PAN.
FIELD SEPARATOR	21	1	A/N	= (equal sign)
EXPIRATION DATE	22–25	4	N	The date the card expires in YYMM format.
SERVICE CODE	26–28	3	N	120
DISCRETIONARY DATA	29	varies	A/N	
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.10 Fleet One Card

Cards are embossed with the Account Number, Company Name and Vehicle Name / Customer Name.

3.10.1 Fleet One Track 2 Format

Table 3-18 Fleet One Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
CARD ISO/ABA PREFIX	2	6	A/N	501486 Refer to the *Heartland BIN Guide*.
PROMPT CODE	8	2	N	Valid options are 10–19 and 99.
ACCOUNT NUMBER	10	6	N	Fleet company number.
CARD NUMBER	16	4	N	
CHECK DIGIT	20	1	N	0–9
FIELD SEPARATOR	21	1	A/N	= (equal sign)
EXPIRATION DATE	22	4	N	The date the card expires in YYMM format. 9912 or 4912 indicates "does not expire."
MEMBER NUMBER	26	1	N	0–9
PIN OFFSET	27	6	N	Not used.
END SENTINEL	33	1	A/N	? (question mark)
LRC	34	1	A/N	Created by the encoding equipment.

3.11 FleetCor Card

Cards are embossed with the Account Number, Expiration Date, Company Name and Vehicle Name/Customer Name.

3.11.1 FleetCor Track 2 Format

Table 3-19 FleetCor Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
CARD ISO/ABA PREFIX	2	6	A/N	Refer to the *Heartland BIN Guide*.
ISSUER IDENTIFIER	8	5	N	
CARD NUMBER	13	6	N	
FIELD SEPARATOR	19	1	A/N	= (equal sign)
EXPIRATION DATE	20	4	N	The date the card expires in YYMM format. 9912 is a valid value and indicates card does not expire.
DISCRETIONARY DATA	24	0–13	N	Reserved for Future Use. Value is either 0 or NULL.
END SENTINEL	24–37	1	A/N	? (question mark)
LRC	25–38	1	A/N	b

3.12 JCB Card

All JCB cards follow the same track format as Discover. See *3.5 Discover Card, p. 38*.

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number and the Expiration Date.

3.12.1 JCB IIN Ranges on Discover Network

The JCB IIN Ranges are effective only for the domestic United States, and to the extent that other Territories and Protectorates may be included, we will provide you with further information. All other international markets are out of scope at this time. Additionally, ATM transactions will not be enabled for the IIN ranges assigned to JCB.

Refer to the *Heartland BIN Guide*.

3.13 Mastercard

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number and the Expiration Date.

3.13.1 Mastercard Track 1 Format

Table 3-20 Mastercard Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3varies	16–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
CARDHOLDER NAME	varies	2–26	A/N	Contains a maximum of 26 characters.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	Identifies the circumstances under which the card can be used.
DISCRETIONARY DATA	varies	varies	A/N	Contains the CVC.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.13.2 Mastercard Track 2 Format

Table 3-21 Mastercard Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2varies	16–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	Identifies the circumstances under which the card can be used.
DISCRETIONARY DATA	varies	varies	A/N	Contains the CVC.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.14 Mastercard Fleet Card Type

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number, Expiration Date and Cardholder Name.

3.14.1 Mastercard Fleet Card Example

Figure 3-1 Mastercard Fleet Card: Driver Assigned Example

Figure 3-2 Mastercard Fleet Card: Vehicle Assigned Example

3.14.2 Account Number Information

The following section describes the method that can be used by a POS application to identify a Mastercard Fleet Account Number.

Table 3-22 Mastercard Fleet Account Number Information Method

Method	Description
Magnetic Track Identification	The Mastercard Fleet account number is 16 characters in length. Refer to the *Heartland BIN Guide*. The 16th position of the Card's account number is the check digit. It is calculated on the previous fifteen (15) digits. For example, Mastercard Fleet account: 556701000000000 **3**; has a check digit of 3.
Embossed Identification	The Card's embossed account number is 16 characters in length. The Card's account number prefix (first four digits of the embossed account number). Refer to the *Heartland BIN Guide*. The 16th position of the Card's embossed account number is the check digit. The words 'Fuel Only' (optional, based on Product Restriction Code information). Cardholder's Name. Expiration Date.

3.14.3 Mastercard Fleet Track 1 Format

Note: All Mastercard Fleet cards use the entire allocated length of the track. Therefore, space-fill any variable length fields as necessary.

Table 3-23 Mastercard Fleet Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3varies	16–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
CARDHOLDER NAME	varies	26	A/N	Contains a maximum of 26 characters.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	A/N	Identifies the circumstances under which the card can be used.
DISCRETIONARY DATA	varies	22	A/N	
PRODUCT RESTRICTION CODE	varies	1	N	1 to 2 required.
PRODUCT TYPE CODE	varies	1	N	1 to 5 required.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.14.4 Mastercard Fleet Track 2 Format

Table 3-24 Mastercard Fleet Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2varies	16–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	A/N	Identifies the circumstances under which the card can be used.
DISCRETIONARY DATA	varies	up to 11	A/N	The amount of discretionary data available in Track 2 for issuers to use is variable depending on the PAN length for all card brands and card types unless the PAN is defined as a fixed length.
PRODUCT RESTRICTION CODE	varies	1	N	1 to 2 required.
PRODUCT TYPE CODE	varies	1	N	1 to 5 required.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.15 Mastercard Purchasing Card

PAN must pass a MOD 10 check-digit test.

Card are embossed with the Primary Account Number and the Expiration Date.

3.15.1 Mastercard Purchasing Card Example

3.15.2 Mastercard Purchasing Track 1 Format

Table 3-25 Mastercard Purchasing Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3varies	16–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (caret)
CARDHOLDER NAME	varies	varies	A/N	Contains a maximum of 26 characters.
FIELD SEPARATOR	varies	1	A/N	^ (caret)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	A/N	Identifies the circumstances under which the card can be used.
DISCRETIONARY DATA	varies	22	A/N	Optional field.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.15.3 Mastercard Purchasing Track 2 Format

Table 3-26 Mastercard Purchasing Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2^{varies}	16–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	A/N	Identifies the circumstances under which the card can be used.
DISCRETIONARY DATA	varies	varies	A/N	Optional field.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.15.4 Mills Fleet Farm PLCC Track 1 Format

Table 3-27 Mills Fleet Farm PLCC Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1		"
START SENTINEL	2	1	A/N	% (percent sign)
FORMAT CODE	3	1		B
PRIMARY ACCOUNT NUMBER	4	16	N	Cardholder's PAN.
FIELD SEPARATOR	20	1	A/N	¬
CARDHOLDER NAME	21	26	A/N	Contains a maximum of 26 characters.
FIELD SEPARATOR	47	1	A/N	¬
EXPIRATION YEAR DATE	48	2	N	The year the card expires.
EXPIRATION MONTH DATE	50	2	N	The month the card expires.
SERVICE CODE	52	3	A/N	Identifies the circumstances under which the card can be used. • Mills Dual Card = 201 • PLCC = 701
PIN VERIFICATION	55	1		PIN Indicator (will be 0) Not used
PIN OFFSET	56	4		PIN Offset (will be 0) Not used
CARD VERIFICATION VALUE	60	11	A/N	CVV
END SENTINEL	71	1	A/N	? (question mark)

3.15.5 Mills Fleet Farm PLCC Track 2 Format

Table 3-28 Mills Fleet Farm PLCC Track 2 Format

Field Name	Position	Length	Format	Value/Description
	1	1		Space
START SENTINEL	2	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	3	16	N	Cardholder's PAN.
FIELD SEPARATOR	19	1	A/N	= (equal sign)
EXPIRATION YEAR DATE	20	2	N	The year the card expires.
EXPIRATION MONTH DATE	22	2	N	The month the card expires.
SERVICE CODE	24	3	A/N	Identifies the circumstances under which the card can be used. • Mills Dual Card = 201 • PLCC = 701
PIN VERIFICATION	27	1		PIN Indicator (will be 0) Not used
PIN OFFSET	28	4		PIN Offset (will be 0) Not used
CARD VERIFICATION VALUE	32	3	A/N	CVV
END SENTINEL	35	1	A/N	? (question mark)

3.16 Multi Service Track Data

3.16.1 Multi Service Swiped Track 2 Format

Table 3-29 Multi Service Swiped Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
ISO PREFIX	2	6	N	Refer to the *Heartland BIN Guide*.
ACCOUNT NUMBER	8	8	N	Cardholder's PAN.
FIELD SEPARATOR	16	1	A/N	= (equal)
CASH FLAG	17	1	N	
PO REQUIRED FLAG	18	1	N	
TWO DIGIT DAY OF ISSUANCE	19	2	N	
FIELD SEPARATOR	21	1	A/N	= (equal)
DATE OF ISSUANCE	22	4	N	YYMM
SERVICE RESTRICTIONS	26	1	N	
FUEL FLAG	27	1	N	
OIL FLAG	28	1	N	
PLUS AMOUNT ON CARD	29	3	N	
TYPE FLAG	32	1	N	
FILLER SPACE	33	5		
STRIPE VERSION NUMBER	38	1	N	
END SENTINEL	39	1	A/N	? (question mark)

3.17 PayPal Card

PayPal cards are now part of the Discover Network and follow the same track format as Discover. See *3.5 Discover Card, p. 38*.

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number and the Expiration Date.

3.18 Stored Value Solutions (SVS)

- PAN must pass MOD 10 check-digit test. (MOD 10 check on first 18 digits, 19th digit is the check digit.)
- Cards are embossed with the Account Number.

3.18.1 SVS Track 1 Format

Table 3-30 SVS Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	5–21	19	N	Cardholder's PAN.
FIELD SEPARATOR	22	1	A/N	^ (caret)
CARDHOLDER NAME	23–48	26^{max}	A/N	Contains a maximum of 26 characters.
FIELD SEPARATOR	49	1	A/N	^ (caret)
EXPIRATION DATE	50–53	4	N	The date the card expires in YYMM format.
SERVICE CODE	54–56	3	N	110
CVV DATA	57–59	3	A/N	Card Verification Value.
END SENTINEL	60	1	A/N	? (question mark)
LRC	61	1	A/N	Created by the encoding equipment.

3.18.2 SVS Track 2 Format

Table 3-31 SVS Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1–1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2–20	19	N	Cardholder's PAN.
FIELD SEPARATOR	21–21	1	A/N	= (equal sign)
EXPIRATION DATE	22–25	4	N	The date the card expires in YYMM format.
SERVICE CODE	26–28	3	N	110
CVV DATA	29–36	8	N	Card Verification Value.
END SENTINEL	37–37	1	A/N	? (question mark)
LRC	38–38	1	A/N	Created by encoding equipment.

3.19 UnionPay Card

All UnionPay issued cards follow the same track format as Discover. See *3.5 Discover Card, p. 38*.

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number and the Expiration Date.

3.20 ValueLink Card

PAN must pass MOD 10 check digit test. (MOD 10 check on first 18 digits, 19th digit is the check digit.)

Card are embossed with the Account Number. CLGC cards (Closed Loop Gift Cards) are embossed with 16 digits.

3.20.1 ValueLink Track 1 Format

Table 3-32 ValueLink Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3–20	13–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (caret)
CARDHOLDER NAME	varies	2–26	A/N	Contains a maximum of 26 characters.
SEPARATOR	varies	1	A/N	^ (caret)
CARD EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	
PVKI		1	N	PIN Verification Key Index.
PVV		4	N	PIN Verification Value.
DISCRETIONARY DATA	varies	varies	A/N	
VISA RESERVED	varies	11	A/N	
END SENTINEL	varies	1	A/N	
LRC	varies	1	A/N	Longitudinal Redundancy Check.

3.20.2 ValueLink Track 2 Format

Table 3-33 ValueLink Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	
PRIMARY ACCOUNT NUMBER	3–20	13–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	Usually = (equal)
CARD EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	
PVKI		1	N	PIN Verification Key Index.
PVV		4	N	PIN Verification Value.
DISCRETIONARY DATA	varies	8	A/N	
END SENTINEL	varies	1	A/N	
LRC	varies	1	A/N	Longitudinal Redundancy Check.

3.21 Visa Card

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number and the Expiration Date.

3.21.1 Visa Track 1 Format

Table 3-34 Visa Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3varies	13–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
CARDHOLDER NAME	varies	2–26	A/N	Contains a maximum of 26 characters.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	Identifies the circumstances under which the card can be used.
PIN VERIFICATION	varies	0 or 5	N	If used, this field is composed of two components.
PVKI		1		PIN Verification Key Index.
PVV		4		PIN Verification Value.
DISCRETIONARY DATA	varies	varies	A/N	
VISA RESERVED	varies	11[1]	A/N	PIN Verification. All 11 positions are required.
Filler		1–2		Zero-fill
CVV		3–5		Card Verification Value.
Filler		6–7		Zero-fill
ACI		8		Authorization Control Indicator.
Filler		9–11		Zero-fill
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

1. The length is always the last 11 positions of Track 1, excluding the END SENTINEL and LONGITUDINAL REDUNDANCY CHECK.

3.21.2 Visa Track 2 Format

Table 3-35 Visa Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2^{varies}	13–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	Identifies the circumstances under which the card can be used.
PIN VERIFICATION	varies	0 or 5	N	If used, this field is composed of two components.
PVKI		1	N	PIN Verification Key Index (PVKI).
PVV		4	N	PIN Verification Value (PVV).
DISCRETIONARY DATA	varies	varies	A/N	Contains the Card Verification Value.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

3.22 Visa Corporate or Business

For Track 1, see *Table 3-34 Visa Track 1 Format, p. 61*.

For Track 2, see *Table 3-35 Visa Track 2 Format, p. 62*.

3.23 Visa Purchasing

For Track 1, see *Table 3-34 Visa Track 1 Format, p. 61*.

For Track 2, see *Table 3-35 Visa Track 2 Format, p. 62*.

3.24 Visa Fleet Card Type

PAN must pass a MOD 10 check-digit test.

Cards are embossed with the Primary Account Number, Expiration Date, Company Name or generic Cardholder ID.

3.24.1 Visa Fleet Card Example

Figure 3-3 Visa Fleet Card: Driver Assigned Example

Figure 3-4 Visa Fleet Card: Vehicle Assigned Example

3.24.2 Visa Fleet Track 1 Format

Table 3-36 Visa Fleet Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	B
PRIMARY ACCOUNT NUMBER	3–20	13–19	N	Cardholder's PAN.
FIELD SEPARATOR	varies	1	A/N	^ (caret)
CARDHOLDER NAME	varies	2–26	A/N	Contains a maximum of 26 characters.
SEPARATOR	varies	1	A/N	^ (caret)
CARD EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	Identifies the circumstances under which the card can be used.
PIN VERIFICATION	varies	0 or 5	N	If used, this field is composed of two components.
PVKI		1	N	PIN Verification Key Index.
PVV		4	N	PIN Verification Value.
DISCRETIONARY DATA	varies	varies	A/N	
VISA RESERVED	varies	11	A/N	
FILLER		2	A/N	Zero-filled.
CVV		3	A/N	Card Verification Value.
FILLER		2	A/N	Zero-filled.
AUTHORIZATION CONTROL INDICATOR (ACI)		1	A/N	Zero or A to Z required.
RESERVED		1	A/N	0 (zero)
SERVICE ENHANCEMENT INDICATOR		1	A/N	• 0 = Fleet, No restriction (fuel, maintenance and non-fuel purchases) • 1 = Fleet (fuel and maintenance purchases only) • 2 = Fleet (fuel only) • 3–9 = Reserved

Table 3-36 Visa Fleet Track 1 Format (Continued)

Field Name	Position	Length	Format	Value/Description
SERVICE PROMPT		1	A/N	• 0 = Reserved (no prompt) • 1 = Generic Identification Number and ODOMETER[1] • 2 = VEHICLE ID and ODOMETER • 3 = DRIVER ID and ODOMETER • 4 = ODOMETER • 5 = No Prompt • 6 = Generic Identification Number[2] • 7–9 = Reserved (no prompt)
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by the encoding equipment.

1. SERVICE PROMPT 1: After prompt for an ID, cardholder enters 6-digit VEHICLE ID, DRIVER ID, or a generic identification number followed by Odometer.
2. SERVICE PROMPT 6: After prompt for an ID, cardholder enters 6-digit VEHICLE ID, DRIVER ID, or generic identification number.

3.24.3 Visa Fleet Track 2 Format

Table 3-37 Visa Fleet Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2varies	13–19	N	Cardholder's PAN.
SEPARATOR	varies	1	A/N	= (equal sign)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
SERVICE CODE	varies	3	N	Identifies the circumstances under which the card can be used.
PIN VERIFICATION	26 varies if used	0 or 5	N	If used, this field is composed of two components.
PVKI		1	N	PIN Verification Key Index.
PVV		4	N	PIN Verification Value.
DISCRETIONARY DATA	varies	varies	N	
CARD VERIFICATION VALUE (CVV)		3	N	Identifies the Card Verification Value.
ISSUER INFORMATION		varies	N	The length of this field depends on the length of PIN Verification and must occupy the third last position of the field. Visa Fleet cards are required to use the last three positions of this field to provide instructions for customized prompts. Refer to the *Heartland BIN Guide*.

Table 3-37 Visa Fleet Track 2 Format (Continued)

Field Name	Position	Length	Format	Value/Description
FLEET SERVICES		2	N	The third to last position from the END SENTINEL, valid value is zero. Service Enhancement Indicator. The value entered in this field must occupy the second last position of the field. • 0 = Fleet, No restriction (fuel, maintenance and non-fuel purchases) • 1 = Fleet (fuel and maintenance purchases only) • 2 = Fleet (fuel only) **Note:** The position of this field varies depending on the length of PIN Verification.
		1	N	Indicate the SERVICE PROMPT. • 0 = Reserved (no prompt) • 1 = Generic Identification Number and ODOMETER[1] • 2 = VEHICLE ID and ODOMETER • 3 = DRIVER ID and ODOMETER • 4 = ODOMETER • 5 = No Prompt • 6 = Generic Identification Number[2] • 7–9 = Reserved (no prompt)
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Value of 0 (zero) to F.

1. SERVICE PROMPT 1: After prompt for an ID, cardholder enters six-digit VEHICLE ID, DRIVER ID, or a generic identification number followed by Odometer.
2. SERVICE PROMPT 6: After prompt for an ID, cardholder enters six-digit VEHICLE ID, DRIVER ID, or generic identification number.

3.25 Voyager Fleet Card

PAN must pass two MOD 10 check-digit tests. The 13th position is the check-digit for the previous eight digits. The 19th position is the check-digit for the previous 18 digits.

Cards are embossed with the Account Number, ID Number, Restriction Code and Expiration Date.

3.25.1 Voyager Account Number Information

The following sections describe the method that can be used by a POS application to identify a Voyager Account Number.

Table 3-38 Voyager Fleet Account Number Information Method

Method	Description
Magnetic Track Identification	The Voyager account number is nineteen characters in length. The Voyager ISO is 7088. The Card's account number prefix (the first two digits following the ISO) begins with 85, 86, 88 or 89. **The thirteenth position of the Card's account number is the first check digit**. It is calculated on the previous eight digits. **Example:** Voyager account: 000**4** 00001 6 will have their first check digit calculated on the 85999 000. In this case the check digit is **4**. **The nineteenth position of the Card's account number is a second check digit**. It is calculated on the previous eighteen digits. **Example:** Voyager account: 0004 00001 **6** will have the second check digit calculated on the 7088 85999 0004 00001. In this case the check digit is **6**.
Embossed Identification	The Card's embossed account number is fifteen characters in length. The Card's account number prefix (first two positions of the embossed account number) begins with 85, 86, 88 or 89. **The ninth position of the Card's embossed account number is the first of two check digits**. It is calculated on the previous eight digits. **Example:** Voyager account number: 85999 000**4** 00001 6 will have the first check digit calculated on the 85999 000. In this case the check digit is **4**. **The fifteenth position of the Card's embossed account number is the second check digit.** It is calculated on the previous 14 digits plus an ISO of 7088 is added before the account number. The ISO is not embossed on the credit card. **Example:** Voyager embossed account number of: 85999 0004 00001 **6** will have the check digit calculated on the 7088 85999 0004 00001. In this case the check digit is **6**. Identification Number (optional, based on Product Restriction Code information). • Cardholder's Name. • Production Restriction Code (also located on magnetic strip). • Expiration Date.

3.25.2 Voyager Fleet Track 1 Format

Table 3-39 Voyager Fleet Track 1 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	% (percent sign)
FORMAT CODE	2	1	A/N	0 (zero)
PRIMARY ACCOUNT NUMBER	3–21	19	N	Cardholder's PAN.
FIELD SEPARATOR	22	1	A/N	^ (carat)
CARDHOLDER NAME	23–47	varies	A/N	Contains a maximum of 25 characters.
FIELD SEPARATOR	varies	1	A/N	^ (carat)
EXPIRATION DATE	varies	4	N	The date the card expires in YYMM format.
RESTRICTION CODE	varies	2	N	Code indicating the type of prompts that display for a customer transaction. • 00 = Do not prompt for ID Number or odometer. All items allowed. • 01 = Do not prompt for ID Number or odometer. Fuel only. • 10 = Prompt for ID Number. All items allowed. • 11 = Prompt for ID Number. Fuel only. • 20 = Prompt for odometer. All items allowed. • 21 = Prompt for odometer. Fuel only. • 30 = Prompt for ID Number and odometer. All items allowed. • 31 = Prompt for ID Number and odometer. Fuel only.
DISCRETIONARY DATA	varies	13	N	Contains a valid numeric value or be zero-filled.
END SENTINEL	varies	1	A/N	? (question mark)
LRC	varies	1	A/N	Created by encoding equipment.

3.25.3 Voyager Fleet Track 2 Format

Table 3-40 Voyager Fleet Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1		A/N	; (semicolon)
PRIMARY ACCOUNT NUMBER	2–20	19	N	Cardholder's PAN.
FIELD SEPARATOR	21	1	A/N	= (equal sign)
EXPIRATION DATE	22–25	4	N	The date the card expires in YYMM format.
RESTRICTION CODE	26–27	2	N	Code indicating the type of prompts that display for a customer transaction. • 00 = Do not prompt for ID Number or odometer. All items allowed. • 01 = Do not prompt for ID Number or odometer. Fuel only. • 10 = Prompt for ID Number. All items allowed. • 11 = Prompt for ID Number. Fuel only. • 20 = Prompt for odometer. All items allowed. • 21 = Prompt for odometer. Fuel only. • 30 = Prompt for ID Number and odometer. All items allowed. • 31 = Prompt for ID Number and odometer. Fuel only.
DISCRETIONARY DATA	28–38	11	N	Will contain a valid numeric value or be zero-filled.
END SENTINEL	39	1	A/N	? (question mark)
LRC	40	1	A/N	Created by encoding equipment.

3.26 WEX Fleet Card

Account Number is seven positions in length where the first six digits must pass MOD 10 check-digit test. The seventh digit is the check-digit.

Cards are embossed with the Account Number, ISO Number, Purchase Device Sequence Number, Expiration Date, Cardholder Name, Description and Restriction.

3.26.1 WEX Fleet Card Example

Figure 3-5 WEX Fleet Card Example

3.26.2 WEX GSA Fleet Cards

The following WEX GSA cards are to be treated just like any other WEX Fleet card.

- WEX Universal cards and WEX GSA cards have the same Track 2 layout.
- The card front for WEX Universal cards and WEX GSA cards differs, as the placement of the six-digit ISO of 690046, the 13-digit Account Number, and five-digit value for the Purchase Device Sequence Number varies by card type.
- WEX Universal cards display the 690046 ISO below the 13-digit Account Number, and label the five-digits Purchase Device Sequence Number as the PURCH. DEV. SEQ. NO.
- WEX GSA Fleet cards display the 690046 ISO above the 13-digit Account Number and place the five-digit Purchase Device Sequence Number after the 13-digit Account Number, with no distinct label.
- WEX Dept of Defense cards and Dept of Energy cards display the 690046 ISO above the 13-digit Account Number and label the five-digit Purchase Device Sequence Number as CARD NO.

Figure 3-6 WEX GSA Fleet

Figure 3-7 WEX Dept. of Defense Fleet

Figure 3-8 WEX Dept. of Energy Fleet

3.26.3 WEX Fleet Track 2 Format

Table 3-41 WEX Fleet Track 2 Format

Field Name	Position	Length	Format	Value/Description
START SENTINEL	1	1	A/N	; (semicolon)
ISO PREFIX	2	6	N	Refer to the *Heartland BIN Guide*.
PRIMARY ACCOUNT NUMBER	3–20	19	N	Cardholder's PAN.
FIELD SEPERATOR	21	1	A/N	= (equal sign)
EXPIRATION DATE	22–25	4	N	The date the card expires in YYMM format.
PROMPT TABLE KEY	26	1	N	Values are 0, 1, 2, 3, 4 or 5.
PURCHASE RESTRICTION	27–28	2	N	• 00 = Fuel Only • 01 = Unrestricted • 02 = Fuel and Auto (Includes Car Wash) • 04 = Fuel and Oil **Note:** Product restriction or validation is only performed by the POS when processing in offline mode. Product restriction or validation is never performed by the Host.
PURCHASE DEVICE SEQUENCE NUMBER	29–33	5	N	Distinct from the prompt Vehicle ID.
CAV1	34–37	4	N	Card Authentication Value.
POS PROMPTS	38	1	N	Refer to the *Heartland POS Integrator's Guide* for WEX Fleet Prompting Values.
END SENTINEL	39	1	A/N	? (question mark)
LRC	40	1	A/N	Created by encoding equipment.

3.26.4 WEX MOD 10 Calculation

WEX defines their Fleet number as:

- ISO – six numeric
- Client Id – four numeric
- Zeros – two numeric
- Account Number – six numeric
- Check Digit – one numeric

To calculate the Check Digit, follow these steps:

- Examine the six-digit Account Number, one digit at a time
- Result 1 = Multiply digit 1 by 1
- Result 2 = Multiply digit 2 by 2
- Result 3 = Multiply digit 3 by 1
- Result 4 = Multiply digit 4 by 2
- Result 5 = Multiply digit 5 by 1
- Result 6 = Multiply digit 6 by 2

If any of these Results (1 through 6) are > 9, then subtract 9 from that Result

The sum of all Results (1 through 6) = the Dividend

Divide the Dividend by 10 resulting in a Quotient and a Remainder

The Remainder = the MOD10-Value

If the MOD10-Value is not equal to **0**, compute MOD10-Value = 10 minus MOD10-Value

Move MOD10-Value to Check Digit

Chapter 4: E3 Processing Overview

4.1 Introduction

Heartland Secure™ is a comprehensive credit/debit card data security solution that combines three powerful technologies working in tandem to provide merchants with the highest level of protection available against card-present data fraud.

Offered to Heartland customers for no additional processing fees as part of Heartland's comprehensive solutions, Heartland Secure combines:

- EMV electronic chip card technology to prove that a consumer's card is genuine.
- Heartland's E3® end-to-end encryption technology, which immediately encrypts card data as it is acquired so that no one else can read it.
- Tokenization technology, which replaces card data with “tokens” that can be used for returns and repeat purchases, but are unusable by outsiders because they have no value.

This guide focuses on Heartland's E3 end-to-end encryption solution and contains integration information for POS systems. It serves as a companion to Heartland's host network specifications and the E3 device programmer's manuals. These documents should be referred to for more detailed information.

4.2 The E3® Solution

E3, an end-to-end encryption product by Heartland, is designed to protect credit and debit card data from the moment of card swipe and through the Heartland network — not just at certain points of the transaction flow.

E3 is based on Voltage Security's SecureData Payments product which provides a complete payment transaction protection framework, built on two breakthrough technologies encompassing encryption and key management: Voltage Format-Preserving Encryption (FPE) and Voltage Identity-Based Encryption (IBE).

With Voltage Format-Preserving Encryption (FPE), credit card numbers and other sensitive data are protected without the need to change the data format or structure. In addition, data properties are maintained, such as a checksum, and portions of the data can remain in the clear.

With Voltage Identity-Based Encryption (IBE), the complexity of key management through traditional Public Key Infrastructure (PKI) systems and symmetric key systems is eliminated — because encryption keys are securely generated on demand and not stored, POS devices are not subject to key injection and key rotation.

4.3 Encryption Data

4.3.1 Encrypted Track and PAN Data

Depending on the configuration of your E3-capable card acceptance device, the E3 encrypted Track and PAN data will be formatted using one of two Track Encryption Protocol (TEP) algorithms, TEP1 or TEP2. TEP1 is whole track encryption, while TEP2 is structure preserving encryption.

Example: The following data was produced by an E3-capable device using Heartland's Visa test card:

Table 4-1 PAN Encryption

Cleartext	4012002000060016
TEP2	4012002650330016
TEP1	+++++++BWmfv/HUA

Table 4-2 Track 1 Encryption

Cleartext	%B4012002000060016^VI TEST CREDIT^25121011803900000000396?
TEP2	B4012007060016^VI TEST CREDIT^2512101XlwD91O5qOg+7Ftv+nLu
TEP1	3FLr83Ed5tiHN3r2CpT3kIndkhtiHRt3mtKQsozJ2rFQM8GE0ha2X7K6t

Table 4-3 Track 2 Encryption

Cleartext	;4012002000060016=25121011803939600000?
TEP2	4012007060016=2512101e3vdC5QhAEZa7UAN
TEP1	AsbjXkDWaRqLV0o5U33jffZqiPg

For TEP2, the following is guaranteed:

- The leading six digits of the original PAN are maintained in the clear.
- The trailing four digits of the original PAN are maintained in the clear.
- The middle digits are used for the ciphertext value, which is guaranteed to consist solely of digits.
- The Luhn check value is preserved so that a PAN with a valid zero (0) result, creates ciphertext that also checks as valid.

For TEP1, the device will provide a separate masked or obfuscated representation of the track data for processing that requires the first six or last four digits of the PAN, cardholder name, expiration date, Luhn check results, etc.

4.3.2 Encrypted Card Security Code

The Card Security Code (CSC) printed on the back of the card, referred to as CAV2, CVC2, CVV2, or CID depending on the card brand, can be optionally encrypted.

The value to be encrypted is constructed as follows:

- Length [1 digit]
- Random Filler [x digits]
- CSC [3 or 4 digits]

Table 4-4 Encrypted CSC Steps

Step	Example Data
1. Obtain the CSC value (either 3 or 4 digits)	572
2. Generate a random 3-digit number	413
3. Construct the value to be encrypted	3413572
4. Encrypt the value	9037662

Note: The total length of the encrypted CSC will always be seven digits. Typically, the device will randomly generate 2 or 3 digits of filler to ensure the CSC is seven digits.

4.3.3 Encryption Transmission Block

The Encryption Transmission Block (ETB), sometimes referred to as a Key Transmission Block (KTB), contains the IBE encrypted version of the device's randomly generated FPE key that was used to encrypt the card data. The ETB must be sent in the authorization requests so that the host can decrypt the card data.

Heartland's ETB must be Base64 encoded, and for TEP1 and TEP2 it must be 276 bytes.

Example:

```
/wECAQEEAoFGAgEH3gcOTDT6jRZwb3NAc2VjdXJlZXhjaGFuZ2UubmV0tmpl5zBEIeyea
DRWB0IlbnWdMjK32V4QIJRoRIpu1Fm9w8fdoJt1gLt2jkkliD+0kvFOrhspWh4dsDYvSH
GgdgetU3pfAx+iBS38Wq2KvTOOlueGvXcGe0y4G/DFVgT7zBHm1YS7cseYLEtADtoSnhB
UjasCciO5ul9GhesvQo8Ah7NM8geDZdKN0QZZiLH8cmYhgHp8kamxSciDJHARUO9tFb+h
```

4.4 E3 Specific Requirements

4.4.1 Heartland Exchange

This section addresses specific requirements for E3 terminals using the Heartland Exchange Message Specification. All card types may be sent using E3 encryption.

4.4.1.1 Unique Transaction ID (UID)

Heartland's Unique Transaction ID (UID) is a software solution that eliminates the need for a POS application to store the account number or track data for subsequent processing such as Voids/Incrementals, and Batch Settlement. The UID is returned by the Heartland Exchange Host in the Authorization response messages. This application is not available on other Heartland Host platforms.

- **Voids/Incrementals:** The Account Data Source field will be 'Z' or 'z' to indicate that the UID is being used instead of track or Primary Account Number (PAN) data. The Customer Data field will contain the UID which is the Retrieval Reference Number (RRN) from the Authorization.
- **Batch Settlement:** The Primary Account Number field in the Batch Settlement Detail Record will be filled with all spaces to indicate that the UID is being used instead of PAN data. The Transaction Identifier field in the Batch Settlement Detail Record is the Transaction Identifier from the Authorization and it contains the UID.

4.4.1.2 Merchant ID Number (MID)

Merchant ID Number is a 12 character field that contains a unique number assigned by Heartland. If your E3 implementation encrypts the MID, then the E3 sub-encryption indicator in the Key Block Data field must indicate the MID is encrypted (**01** or **02** as appropriate).

4.4.1.3 Account Data Source

The Account Data Source field is used to indicate the source and format of the data contained in the Customer Data field. Refer to the Exchange Host Specification for a complete list of Account Data Source codes.

4.4.1.4 Customer Data

The Customer Data field contains the Key Block data and either the Cardholder Account data or the Unique Transaction ID. The Cardholder Account data may be either the encrypted Track 1, encrypted Track 2, or encrypted primary account number. The unique transaction ID is never encrypted. Refer to the Exchange Host Specification for the Customer Data format.

4.4.1.5 Retrieval Reference Number (RRN)

The Retrieval Reference Number field contains a value that uniquely identifies a transaction. The Retrieval Reference Number is sent in an authorization response. The POS then uses the RRN in voids and incrementals to identify the original transaction.

4.4.1.6 Transaction Identifier

The Transaction Identifier field contains the UID. The Transaction Identifier is sent in an authorization response.

4.4.1.7 Authorization Example

The following examples shows highlighted fields that are used in the POS message to Heartland messaging:

- Encrypted Track 1 Data
- Encrypted Track 2 Data
- KTB (Key Transmission Block)
- PAN (Primary Account Number)

Table 4-5 Authorization Examples

Request	Response
For Encrypted Card Swipes: The following request fields require specific handling: • **MID (Merchant ID Number)** – This field will be either the unencrypted, cleartext MID or the encrypted MID if supported. • **Account Data Source** – This field will indicate that either encrypted Track 1 or Track 2 data is being sent: – "h" = Encrypted Track 1 – "d" = Encrypted Track 2 • **Customer Data** – This field will be <Key Block Data><FS><Encrypted Track 1 or Track 2 Data>, where <Key Block Data> is "v" (Voltage encryption)+ "01", "02", or "03" as appropriate + KTB. **Example:** v03/wECAQECAoFGAgEH2ggJTHLeIBZwb3NAc2 VjdXJlZXhjaGFuZ2UubmV0aFLxu2XTNLs6jIk3Bakt bFZrdJ26dX85BjkkngQnmk+3tOhXRVILvASHnfmao0y l5z7KNBx6Na7ekL+hryGQ3oPOcOVkEzei83Clsc 9QSfQJWB9ysAynGc6btccnrfjwyJn70KJ1cqQrw 623ASSWm57Hov2fMtWmPpYpQRr54oAoXZY jUajd0sRXCn5XeD5BhpE/Wzd4Ayn+342BGUL 0N7hWKm<FS>V2uvVFzWkBTNzcX7vcrWTi4 jV9AtG2bLYJkCOi+OA2aY2OiRmw/0ZSQcH	The following response fields require specific handling: • RRN (Retrieval Reference Number) – This field will be used as the UID (Unique Transaction ID) for subsequent messages such as voids. • Transaction Identifier – This field will be used as the UID in the batch settlement detail record.

Table 4-5 Authorization Examples (Continued)

Request	Response
For Encrypted Manual Entry from E3 PIN Pad: The following request fields require specific handling: • Merchant ID Number – This field will be the unencrypted, cleartext MID. • Account Data Source – This field will indicate that an encrypted PAN is being sent: – n "x" = Encrypted, manually keyed PAN, Track 1 capable – n "t" = Encrypted, manually keyed PAN, Track 2 capable • Customer Data – This field will be <Key Block Data><FS><Encrypted Primary Acct Num><FS><Exp Date><FS>, where <Key Block Data> is "v" (Voltage encryption) + "03" (sub-encryption indicator that only PAN is encrypted, not MID) + KTB from the E3 PIN Pad. **Example:** v03/wECAQECAoFGAgEH2ggJTHLeIBZwb3NAc 2VjdXJlZXhjaGFuZ 2UubmV0aFLxu2XTNLs6jIk3Ba ktbFZrdJ26dX85BjkkngQnm k+3 tOhXRVILvASHnfmao0yl5z7 KNBx6Na7ekL+hryGQ3oPOcOVkE zei83Clsc9QSf QJWB9ysAynGc6btccnfrfjwyJn70KJ1 cqQrw623ASSWm57Hov2fMtWmPpYpQRr 54oAoXZYjUajd0sRXCOn5XeD5BhpE/Wzd4Ayn+3 42BGUL0N7hWKm<FS>+++++++X8zr5YaCZ<FS>1012	

Note:

- Refer to section Authorization Chapter in the Heartland Exchange specification for all other fields.
- UIDs are used to retrieve a transaction's account data for Voids, Incrementals, and Batch Settlement. This eliminates the need to store or send encrypted or unencrypted track, PAN, or KTB data once authorization has occurred.
- For refunds/returns, Purchase Return (Transaction Code **CR**) must be utilized so that the returned UID can be used for settlement.
- For voice authorizations, Online Forced Purchase (Transaction Code **5S**) must be utilized so that the returned UID can be used for settlement.

4.4.1.8 Void/Incremental Example

A Void is required to cancel a previously authorized transaction. Online Auth Void (Transaction Code **59**), PIN Debit: Purchase Void (Transaction Code **A3**), or PIN Debit: Purchase Return Void (Transaction Code **A4**) should be used depending on the type of the original authorization.

An Incremental Authorization is required in certain industries such as Hotel/Lodging when the final amount due is more than 15% higher than the originally authorized amount.

For Voids/Incremental Requests the fields below require specific handling:

- Merchant ID Number – This field will be the unencrypted, cleartext MID.
- Account Data Source – This field will indicate that the UID is being sent instead of track or PAN data:
  - "z" = Original authorization request contained encrypted track or PAN data.
- Customer Data – This field will be <Key Block Data><FS><UID>, where <Key Block Data> is just "v03" – the KTB is not required in this case since no encrypted data is being sent, and <UID> is the RRN from the original authorization response.

Note: Refer to the Heartland Exchange Specification for all other fields.

Void/Incremental Responses – No specific fields in the Exchange Host response require specific handling.

4.4.2 Settlements

Batch transactions consist of a number of record types and require both request and responses.

4.4.2.1 Header Record Field Requirements

- Merchant ID Number – This field will be the unencrypted, cleartext MID.
- Key Block – This field will be just "v03" – the KTB is not required in this case since no encrypted data is being sent.

4.4.2.2 Detail Record Fields Requirements

- Account Data Source – This field will be the same value as was used in the original authorization request.
- Primary Account Number – This field will be filled with 22 spaces to indicate that the UID will be used.
- Transaction Identifier – This field will be the Transaction Identifier from the original authorization response (it contains the UID).

4.4.2.3 Settlement Notes

UIDs must be used for settlement, all other record fields in both the request and responses follow those defined in the Exchange Host Specifications.

Note: The only alternative supported on Exchange for settling E3 encrypted transactions is to send the encrypted PANs in the detail records, but that option requires that all transactions in the batch share the same KTB.

4.4.3 POS 8583

This section addresses specific requirements for E3 terminals using the POS 8583 message specification. All card types may be sent using E3 encryption. All transactions utilizing E3 processing will include E3 data in DE 127: Forwarding Data.

These transactions require the following:

- E3 data must always appear in DE 127: Forwarding Data (using an Entry Tag value of **E3E**.)

Note: Then encrypted CVV and ETB are attached to the E3 Data Block, while the encrypted track data and/or encrypted PAN are placed in their normal position in the authorization message.

- An account number must be more than 13 characters, the encrypted account number data cannot exceed 19 characters.
- Encrypted Track 1 data will not exceed 79 bytes.
- Encrypted Track 2 data will not exceed 40 bytes.

Response codes specific to E3 transactions are:

- DE 39 = 952 (Failure for E3 terminals only – encryption error)
- DE 39 = 953 (Failure for E3 terminals only – too many queued / no connection)

Table 4-6 POS 8583 Data Fields

Field Name	Length	Value/Description
RECORD ID	2	E3
RECORD TYPE	3	001
KEY BLOCK DATA TYPE	1	v = Voltage
ENCRYPTED FIELD MATRIX	2	• 03 = CustomerData • 04 = CustomerData, Card Security Code
TEP TYPE	1	• 1 = TEP 1 • 2 = TEP 2
RESERVED	18	Blank-fill
CARD SECURITY CODE	7	Encrypted CVV data. Unencrypted bytes defined as: • 1 = Length of actual CVV data • 2–7 = CVV data, right-justified, random fill, numeric only
RESERVED	45	Blank-fill
ETB LLL	3	Length of ETB Block.
ETB BLOCK	Varies	ETB cannot exceed 276 bytes.

4.4.4 NTS

This section addresses specific requirements for E3 terminals processing on the NTS network platform. All card types may be sent via E3 encryption. All transactions using E3 processing append additional data items at the end of the record, which signals to the host that the transaction is E3 encrypted.

These transactions require the following:

- E3 data must always appear at the end of a transaction. The POS terminal will append a 0x1D at the end of the transaction followed by the E3 data. Refer to *Table 4-7 NTS Data Fields, p. 85*.

Note: Then encrypted CVV and ETB are attached to the E3 Data Block, while the encrypted track data and/or encrypted PAN are placed in their normal position in the authorization message.

- POS must send spaces in the CVN field. This encrypted CVN value will be in the E3 Data Block.
- An account number must not be less than 13 characters and the encrypted account number data will not exceed 19 characters.
- Encrypted Track 1 data will not exceed 79 bytes.
- Encrypted Track 2 data will not exceed 40 bytes.

Response codes specific to E3 transactions are:

- 52 (Failure for E3 terminals only – encryption error)
- 53 (Failure for E3 terminals only – too many queued / no connection)

Table below shows the data items that must be appended to the end of an E3 transaction.

Table 4-7 NTS Data Fields

Field Name	Length	Value/Description
FIELD SEPARATOR	1	0x1D Indicator for E3 transaction (Hex: Constant ASCII). Must be appended at end of E3 transaction.
RECORD ID	2	E3
RECORD TYPE	3	001
KEY BLOCK DATA TYPE	1	v = Voltage
ENCRYPTED FIELD MATRIX	2	• 03 = Customer Data • 04 = Customer Data, Card Security Code
TEP TYPE	1	• 1 = TEP 1 • 2 = TEP 2
RESERVED	18	Blank-fill
CARD SECURITY CODE	7	Encrypted CVV data. Unencrypted bytes defined as: • 1 = Length of actual CVV data • 2–7 = CVV data, right-justified, random fill numeric only
RESERVED	45	Blank-fill
ETB LLL	3	Length of ETB Block.
EBT BLOCK	Varies	ETB should not exceed 276 bytes.

4.4.5 Z01

This section addresses specific requirements for E3 terminals processing on the Z01 network platform. All card types may be sent via E3 encryption. All transactions using E3 processing will append additional data items at the end of the record, which will signal to the Host that the transaction is E3 encrypted.

These transactions require the following:

- E3 data must always appear at the end of a transaction. The POS terminal will append a 0x1D at the end of the transaction followed by the E3 data as specified in *Table 4-8 Z01 Data Fields, p. 87*.

Note: The encrypted CVV and ETB are attached to the E3 Data Block, while the encrypted track data and/or encrypted PAN are placed in their normal position in the authorization message.

- POS must send spaces in AVS RESULT AND CID RESULT. The encrypted values are in the E3 Data Block.
- An account number must not be less than 13 characters and the encrypted account number data will not exceed 19 characters.
- Encrypted Track 1 data will not include the field separator 0x1C.
- Encrypted Track 2 data will not exceed 37 bytes.

Response codes specific to E3 transactions are:

- URC = EG, SRC = 8 (Failure for E3 terminals only – encryption error)
- URC = EH, SRC = 8 (Failure for E3 terminals only – too many queued / no connection)

Note: E3 transactions are not supported for TDC batch uploads.

Table 4-8 Z01 Data Fields

Field Name	Length	Value/Description
FIELD SEPARATOR	1	0x1D. Indicator for E3 transaction (Hex: Constant ASCII). Must be appended at end of E3 transaction.
RECORD ID	2	E3
RECORD TYPE	3	001
KEY BLOCK DATA TYPE	1	v = Voltage
ENCRYPTED FIELD MATRIX	2	• 03 = Customer Data • 04 = Customer Data, Card Security Code
TEP TYPE	1	• 1 = TEP 1 • 2 = TEP 2
RESERVED	18	Blank-fill
CARD SECURITY CODE	7	Encrypted CVV data. Unencrypted bytes defined as: • 1 = Length of actual CVV data • 2–7 = CVV data, right-justified, random fill, numeric only
RESERVED	45	Blank-fill
ETB LLL	3	Length of ETB Block.
EBT BLOCK	Varies	ETB should not exceed 276 bytes.

4.5 E3 Hardware Devices

The following section describes two hardware devices that use E3 encryption technology that integrates with Heartland Hosts:

- E3 MSR Wedge (HPS-E3-M1)
- E3 PIN Pad (HPS-E3-P1)

4.5.1 E3 MSR Wedge (HPS-E3-M1)

- Hardware-encrypts card data upon swipe.
- Incorporates a Tamper-Resistant Security Module (TRSM) to physically protect data and encryption keys.
- Available with USB and RS232 connectors.

Figure 4-1 E3 MSR Wedge

4.5.2 E3 MSR Wedge Device Interface

Table 4-9 E3 MSR Wedge Operation Modes

Mode	Description
USB HID-KB	The POS system receives data from the E3 MSR Wedge as if sent from a standard USB keyboard. In this mode, you can see the output by opening a text editor such as Notepad and swiping a card. The output is in Format 2 per the programmer's manual.
USB HID-MSR	The POS system receives data from the E3 MSR Wedge via its native USB HID interface in Format 1. For this mode, an ActiveX control is available for web applications running on Internet Explorer and provides commands for obtaining the desired output components. Also, a command-line application is available that acquires and reformats the output as Format 2.
USB Virtual-COM or RS232	The POS system receives data from the E3 MSR Wedge via its native serial COM port interface, which outputs in Form 2. A virtual COM port driver is available for Windows. The RS232 wedge has a standard 9-PIN serial connector.

4.5.3 E3 MSR Wedge Example Output

See the following Format 2 example output from the E3 MSR Wedge:

```
<E1050711%B4012001000000016^VI TEST
CREDIT^2512000000000000000000000?|
ycO0LNhgiu4XH7J1Lqg8BY6Vc25F3ft3qoTEeqk3wrx7KGh8JSrEUfAAW
|+++++++8q0sLWCB5|11;4012001000000016=25120000000000000000?|
7YIC67MkijZle6TL5Tdw90jCQ3F|+++++++8q0sLWCB5|00|||
/wECAQECAoFGAgEH1AESTDT6jRZwb3NAc2VjdXJlZXhjaGFuZ2UubmV0aXGRuQf68kvJ3Sb
fATjjdctZlBnX2gFQ3chN7Fq2s22bTq/rTVzl7fLQ/j1CGGohcyB
vmmYxGs6ZLDyYL+8EWZFhhjQC7tIKaYMsdua4SxeYAg9wQGHczVI+tTKFXClWEQ8kCKZ6
zHkG5+jJZhjGpO2EWSe18DH3HiKMsDwM8DcA5l5b3GT+pc7XwwK8oEdU3gjOiRo4/fdPm
F/PPBxAET1zlPUq|>
```

4.6 E3 PIN Pad (HPS-E3-P1)

The E3 PIN Pad is compatible with standard PIN entry/encryption operations, but is also capable of functioning with MSR, Europay, Mastercard, and Visa (EMV) smart cards.

- Built-in MSR encrypts at the swipe and TRSM protects the data and keys.
- Hardware-encrypt manually-entered card numbers.
- Available with USB and RS232 connectors.

Figure 4-2 E3 PIN Pad

Table 4-10 E3 MSR Wedge Operation Modes

POS System	Direction	E3 PIN Pad
<STX>E1.3111219098025<ETX>[LRC]	→	"SWIPE CARD OR ENTER ACCOUNT #" is displayed on LCD.
	←	<ACK>
<STX>E2.030<ETX>[LRC]	→	
	←	<ACK>
	←	If card is swiped... <STX>E3.11%B4012000000000016^VI TEST CREDIT^2512000000000000000000?|V2uvVFzWkBTNzcX7vcrWTi4jV9AtG2bLYJkCOi+OA2aY2OiRmw/0ZSQcH|++++++++X8zr5YaCZ<FS>11;4012000000000016= 251 2000000000000000?|7QjTe2v1Qy1L84Q+n6zudfNOXf|+++++++X8zr5YaCZ<FS>00||<FS>/wECAQECAoFGAgEH2ggJTHLeIBZwb3NAc2VjdXJlZXhjaGFuZ2UubmV0aFLxu2XTNLs6jIk3Baktb FZrdJ26dX85Bjkkng Qnmk+3tOhXRVILvASHnfmao0yl5z7KNBx6Na7ekL+hry GQ3oPOcOVkEzei8 3Clsc9QSfQJWB9ysAynGc6btccn fr fjwyJn70KJ1cqQrw623ASSWm 57Hov2fMtWmPpYpQRr54 oAoXZYjUajd0sRXCOn5XeD5Bhp E/Wzd4Ayn+3 42BGUL0N7hWKm <ETX>[LRC] or If card number is manually entered... <STX>E4.114012000000000016 <FS> +++++++X8zr5YCZ <FS>/wECAQECAoFGAgEH2g gJTHLeIBZwb3NA2VjdXJlZXhj aGFuZ2UubmV0aFLxu2XTNLs6 jIk3Baktb FZrdJ26dX85Bjkkng Qnmk+3tOhXRVILvASHnfma o0yl5 z7KNBx6Na7ekL+hryGQ3 oPOcOVkEzei83Clsc9QSfQJW B9ysAynGc6btccnfrfjwyJn70KJ 1cqQrw623ASSWm57H ov2fM tWmPYpQRr54oAoXZYjUajd0 sRXCOn5XeD5BhpE /Wzd4Ayn +342BGUL0N7hWKm<ETX>[LRC]

4.6.1 E3 PIN Pad Device Interface

The POS system transmits and receives data to/from the E3 PIN Pad via its native serial COM port interface. For the USB PIN pad, a virtual COM port driver is available for Windows. The RS232 PIN pad has a standard 9-PIN serial connector.

All messages are framed using standard Visa protocols:

- <STX>Message<ETX>[LRC]
- <SI>Message<SO>[LRC]

4.6.1.1 E3 PIN Pad Requests

The following messages are sent to the PIN pad to request E3 encrypted card data via card swipe and/or manual entry:

- <STX>E1.[entry_flag] [disp_flag] [mask_flag] [min len] [max len] [prompt1] [prompt2]<FS>[prossing_prompt]<ETX>[LRC]
- <STX>E2.[timeout]<ETX>[LRC]

4.6.1.2 E3 PIN Pad Responses

The following messages are returned from the PIN pad with E3 encrypted card data via card swipe or manual entry:

- Card Swipe: <STX>E3.[trk1]<FS>[trk2]<FS>[trk3]<FS>[ktb]<ETX>[LRC]
- Manual Entry: <STX>E4.[result] [luhn] [obf]<FS>[enc]<FS>[ktb]<ETX>[LRC]

4.6.2 Ingenico iPP300 and iSC Touch Series PIN Pads

You must sign up for an account at the *Ingenico Developer Portal* and mention that you are working with Heartland. Retail Base Application (RBA) Integration Kits, Software Development Kits (SDKs), and integration documentation for these devices can be downloaded from their portal.

The E3 encryption settings are contained in a digitally signed SECURITY.PGZ files. Work with Heartland to ensure that the appropriate file is loaded to your devices prior to certification testing or production deployment.

4.6.3 Equinox L4000 and L5000 Series PIN Pads

You must sign up for an account at the *Equinox Developer Portal* and mention that you are working with Heartland. Software Development Kits (SDKs) and integration documentation for these devices can be downloaded from their portal.

The E3 encryption settings are contained in XML files which must be specified for all forms (screens) from which card data is obtained, and the forms must be digitally signed. Equinox can provide a development key to sign the forms for use on a development device, but for production devices the forms will either need to be signed by Heartland, Equinox, or another entity that has the appropriate signing tools. Work with Heartland to ensure that the appropriate forms have been signed and loaded to your devices prior to certification testing or production deployment.

Chapter 5: EMV Processing Overview

5.1 Introduction

In 1996, **E**uropay, **M**astercard, and **V**isa first published the "EMV" specifications for the use of chip cards for payment. EMV® is now a registered trademark of EMVCo, LLC, an organization jointly owned and operated by American Express, Discover, JCB, Mastercard, UnionPay, and Visa.

EMVCo manages, maintains, and enhances the EMV Integrated Circuit Card Specifications to help facilitate global interoperability and compatibility of payment system integrated circuit cards and acceptance devices. EMVCo maintains and extends specifications, provides testing methodology, and oversees the testing and approval process.

The EMV Specifications provide a global standard for credit and debit payment cards based on chip card technology. Payment chip cards contain an embedded microprocessor, a type of small computer that provides strong security features and other capabilities not possible with traditional magnetic stripe cards.

Chip cards are available in two forms, contact and contactless.

- For contact, the chip must come into physical contact with the chip reader for the payment transaction to occur.
- For contactless, the chip must come within sufficient proximity of the reader (less than 4 cm) for the payment transaction to occur. Some cards may support both contact and contactless interfaces, and non-card form factors such as mobile phones may also be used for contactless payment.

Heartland recommends that vendors become familiar with general EMV processing prior to initial implementation at Heartland. A good overview of EMV is available from EMVCo at: *http://www.emvco.com/best_practices.aspx?id=217*.

5.2 EMV Migration

5.2.1 Enhanced Security

EMV is designed to significantly improve consumer card payment security by providing features for reducing fraudulent transactions that result from counterfeit and lost and stolen cards. Due to increased credit card breaches, this enhanced security has become a significant necessity.

The key security features are:

Table 5-1 Key Security Features

Key Security Feature	Description
Card Authentication	The terminal can authenticate the legitimacy of the card by using a public-key infrastructure (PKI) and Rivest, Shamir, and Adleman (RSA) cryptography to validate signed data from the card. The issuer can authenticate the legitimacy of the card by validating a unique cryptogram generated by the card for each payment transaction. These features will help protect against counterfeit fraud.
Risk Management	EMV introduces localized parameters to define the conditions under which the issuer will permit the chip card to be used and force transactions online for authorization under certain conditions such as offline limits being exceeded.
Transaction Integrity	Payment data such as purchase and cashback amounts are part of the cryptogram generation and authentication processing, which will help ensure the integrity of this data across authorization, settlement, and clearing.
Cardholder Verification	More robust cardholder verification processes and methods such as online PIN (verified online by issuer) and offline PIN (verified offline by card) will help protect against lost and stolen fraud.

5.2.2 Card Brand Mandates

Effective April 2013, acquirer processors and sub-processor service providers are required to support merchant acceptance of EMV chip transactions.

5.2.3 Fraud Liability Shifts

Effective October 2015 (or October 2017 for automated fuel dispensers), a merchant that does not support EMV assumes liability for counterfeit card transactions.

There are two types of liability shifts:

Table 5-2 Liability Shifts

Liability Shift	Description
Chip Liability Shift	An issuer may charge back a counterfeit fraud transaction that occurred at a non-EMV POS terminal if the valid card issued was a chip card.
Chip/PIN Liability Shift	An issuer may charge back a lost or stolen fraud transaction that occurred at an EMV POS terminal that was not PIN-capable if the card involved was a PIN-preferring chip card. A PIN-preferring chip card is defined as an EMV chip card that has been personalized so that a PIN CVM option (online PIN or offline PIN) appears in the card's CVM list with a higher priority than the signature option.

5.2.4 PCI Audit Waivers

Effective October 2012, the card brands will waive PCI DSS compliance validation requirements if the merchant invests in contact and contactless chip payment terminals. For example, Visa's Technology Innovation Program (TIP) provides PCI audit relief to qualifying merchants (Level 1 and Level 2 merchants that process more than 1 million Visa transactions annually) when 75 percent of the merchant's Visa transactions originate at a dual-interface EMV chip-enabled terminal. Mastercard offers a similar program.

5.3 EMV Specifications

This document provides guidelines for EMV integration, but it does not contain all the EMV requirements. It should be used in conjunction with the following documents:

5.3.1 Contact Specifications

For EMV contact card acceptance, device manufacturers and payment application developers **must** adhere to the following specifications:

Table 5-3 Contact Specifications

Source	Specification
EMVCo	• EMV Specifications v4.3 (Nov 2011) – http://www.emvco.com/specifications.aspx?id=223 – Book 1: Application Independent ICC to Terminal Interface Requirements – Book 2: Security and Key Management – Book 3: Application Specification – Book 4: Cardholder, Attendant, and Acquirer Interface Requirements
Visa	• Transaction Acceptance Device Guide v3.1 (Nov 2016) • Integrated Circuit Card Specification v1.6 (Jan 2016)
Mastercard	• M/Chip Requirements for Contact and Contactless (Sep 2016)
American Express	• AEIPS Terminal Implementation Guide v4.3 (April 2015) • AEIPS Terminal Technical Manual v4.3 (April 2015)
Discover	• Contact D-PAS Acquirer Implementation Guide v3.2 (Jul 2016) • D-PAS Terminal Specification v1.0 (Jun 2009)

5.3.2 Contactless Specifications

For EMV contactless card acceptance, device manufacturers and payment application developers **must** adhere to the following specifications:

Table 5-4 Contactless Specifications

Source	Specification
EMVCo	• EMV Contactless Specifications v2.6 (May 2016) – http://www.emvco.com/specifications.aspx?id=21 – Book A: Architecture and General Requirements – Book B: Entry Point – Books C [C-1, C-2, C-3, C-4, C-5, C-6, C-7]: Kernel Specifications – Book D: Contactless Communication Protocol
Visa	• Transaction Acceptance Device Guide v3.1 (Nov 2016) • Contactless Payment Specification v2.1 (May 2009)
Mastercard	• M\Chip Requirements for Contact and Contactless (Sep 2016) • Contactless Reader Specification v3.1 (Jun 2015)
American Express	• Contactless NFC Terminal Implementation Guide v1.0 (Mar 2014) • Expresspay Terminal Specification v3.0 (Feb 2012)
Discover	• Contactless D-PAS Acquirer Implementation Guide v1.2 (Jul 2016) • Contactless D-PAS Terminal Application Specification v1.0 (May 2013)

5.3.3 Heartland Host Specifications

Information given in this document for each network platform is meant to be an overview only. The latest version of these Heartland platform specifications should be used for complete message requirements and formats:

Table 5-5 Heartland Host Specifications

Platform	Specification
Exchange	• Exchange Host Specifications
Portico	• Portico Developer Guide
NWS	• Z01 Specifications • POS 8583 Specifications • SpiDr Specifications Developer's Guide
VAPS	• Network Terminal Specifications (NTS) • POS 8583 Specifications • SpiDr Specifications Developer's Guide

5.4 EMV Online vs. Offline

In the magstripe world, the term "offline" is often associated with certain types of transactions that may occur when host communications are down, such as voice authorization, deferred authorization (i.e. store and forward), and forced acceptance (i.e. merchant/acquirer stand-in). Those same transactions can still occur in the EMV world as well, but there are several additional uses of the term "offline" for EMV.

5.4.1 Card Authentication

Table 5-6 Card Authentication

Online Card Authentication	vs.	Offline Card Authentication
The transaction is sent online to an issuer who authenticates the CVV in the track data for swiped transactions, or CVV2 on the back of the card for manually entered transactions.		The card may be authenticated offline by the terminal using a PKI and RSA cryptography to verify that certain static and/or dynamic data elements have been digitally signed by the legitimate card issuer.

5.4.2 Cardholder Verification

Table 5-7 Cardholder Verification

Online Cardholder Verification	vs.	Offline Cardholder Verification
The transaction is sent online to an issuer who verifies that the online PIN or AVS data is correct.		An offline PIN may be securely stored on the card, so the PIN entered on the PIN entry device may be sent to the card in plaintext or enciphered format to be validated by the card.

5.4.3 Authorization

Table 5-8 Authorization

Online Authorization	vs.	Offline Authorization
The transaction is sent online to an issuer who approves or declines the transaction.		Based on the amount of the transaction, and the risk management criteria established by the card and the terminal, a transaction may be approved or declined by the card on behalf of the issuer, either with or without attempt to go online to the issuer.

5.5 Full vs. Partial EMV Transactions and Flow

EMV POS solutions typically support both "full" EMV transactions and "partial" EMV transactions as follows:

Table 5-9 Full vs. Partial EMV Transactions and Flow

EMV Transaction	Description
Full EMV Transactions	Transactions such as Purchases and Pre-Authorizations where the full EMV transaction flow (i.e. the interaction between the card and terminal) is performed and the card participates in the authorization decision, whether online or offline.
Partial EMV Transactions	Transactions such as Returns and Reversals where the EMV transaction flow is only partially performed to the extent necessary to get the card data from the chip and the card does not participate in the authorization decision.

5.5.1 Full vs. Partial Transaction Flow

Table 5-10 Full vs. Partial Transaction Flow

EMV Transaction Step	Full EMV	Partial EMV	Notes
Card Acquisition	✓	✓	Card is inserted or tapped.
Application Selection	✓	✓	
Initiate Application Processing	✓	✓	
Read Application Data	✓	✓	
Offline Data Authentication	✓		
Processing Restrictions	✓		
Cardholder Verification	✓		
Terminal Risk Management	✓		
Terminal Action Analysis	✓	✓	For partial EMV transactions, the terminal requests an AAC at 1st GENERATE AC to terminate card usage.
Card Action Analysis	✓	✓	For partial EMV transactions, the card always returns an AAC.
Online Processing	✓		
Issuer Authentication	✓		
Completion	✓		
Issuer Script Processing	✓		
Card Removal	✓	✓	Prompt to remove card if it was inserted.

5.5.2 Full vs. Partial Credit Transactions

Table 5-11 Full vs. Partial Credit Transactions

EMV Transactions	Full EMV	Partial EMV	Notes
Bill Payment	✓		
Card Verify	✓		
Cash Advance	✓		
Incremental Authorization			No chip data should be sent.
Offline Decline Advice	✓		AAC received at 1st GENERATE AC or due to failed Issuer Authentication at 2nd GENERATE AC.
Offline Purchase Advice	✓	✓	Full for EMV offline approvals where TC received at 1st GENERATE AC or after failed host communications at 2nd GENERATE AC. Partial for voice authorizations if PAN obtained from chip.
Online Purchase	✓		ARQC received at 1st GENERATE AC.
Pre-Authorization	✓		
Pre-Auth Completion			No chip data should be sent.
Purchase Return		✓	To obtain PAN from chip if needed.
Reversal on Timeout			PAN and chip data from original authorization should be sent unless otherwise stated in the network specifications. (This is currently not applicable for the NTS platform.) **Note:** No EMV data will be returned in the response.
Void			PAN and chip data from original authorization should be sent. This should be the **final** chip data available from the original authorization. Typically, this would be from the 2nd GEN AC for contact and from the 1st GEN AC for contactless. **Note:** No EMV data will be returned in the response.

5.5.3 Full vs. Partial Debit Transactions

Table 5-12 Full vs. Partial Debit Transactions

EMV Transactions	Full EMV	Partial EMV	Notes
Offline Decline Advice	✓		AAC received at 1st GENERATE AC or due to failed Issuer Authentication at 2nd GENERATE AC.
Online Purchase	✓		ARQC received at 1st GENERATE AC.
Pre-Authorization	✓		
Pre-Auth Completion			No chip data should be sent.
Purchase Return	✓		ARQC or AAC received at 1st GENERATE AC.
Reversal on Timeout			PAN and chip data from original authorization should be sent. **Note:** No EMV data will be returned in the response.
Void			PAN and chip data from original authorization should be sent. This should be the **final** chip data available from the original authorization. Typically, this would be from the 2nd GEN AC for contact and from the 1st GEN AC for contactless. **Note:** No EMV data will be returned in the response for Void.

Chapter 6: EMV Development Overview

6.1 EMV Terminals

In order to develop an EMV POS solution, an approved EMV transaction acceptance device must be used. In this document all such devices, whether they are a countertop terminal, multi-function PIN pad, multi-lane signature capture device, automated fuel dispenser module, etc., will be referred as a 'terminal'.

6.1.1 Contact Devices

For EMV contact card acceptance, use any terminal if **all** of the following criteria apply:

- Contains an EMVCo Level 1 Contact approved Interface Module (IFM) evaluated against the EMV ICC Specifications, Book 1 v4.0 or later.
- Contains a Mastercard Terminal Quality Management (TQM) approved IFM.
- Is running an EMVCo Level 2 Contact approved application kernel evaluated against the EMV ICC Specifications v4.3 or later.
- Contains a PCI PTS 3.x or 4.x approved PIN Entry Device (PED) or Encrypting PIN Pad (EPP), if you plan to support PIN.

6.1.2 Contactless Devices

For EMV contactless card acceptance, use any terminal if **all** of the following criteria apply:

- Contains an EMVCo Level 1 Contactless approved Proximity Coupling Device (PCD) evaluated against the EMV Contactless Specifications, Book D v2.2 or later.
- Contains a Mastercard TQM approved PCD.
- Is running a Visa approved payWave application kernel evaluated against the Visa Contactless Payment Specification v2.1.1 or later.
- Is running a Mastercard approved Mastercard Contactless application kernel approved against the Mastercard Contactless Reader Specification v3.0.1 or later.
- Is running an American Express approved Expresspay application kernel evaluated against the Expresspay Terminal Specification v3.0 or later.
- Is running a Discover approved D-PAS application kernel evaluated against the Contactless D-PAS Terminal Payment Application v1.0 or later.
- Contains a PCI PTS 3.x or 4.x approved PED or EPP, if you plan to support PIN.

REQUIREMENT	An EMV POS Solution cannot be certified unless the EMVCo Level 1 and Level 2 Letters of Approval for your terminal(s) of choice are current and not about to expire.

6.1.3 Letters of Approval

The EMVCo and PCI approval numbers and/or Letters of Approval (LoAs) can be obtained from their respective websites:

- *http://www.emvco.com/approvals.aspx?id=83*
- *https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php*

The other approval numbers and/or LoAs can be obtained from the device supplier or manufacturer.

6.2 EMV Solutions

The type of EMV POS solution to be developed is an important consideration as this will determine the level of expertise needed, the amount of time it will take and whether a full EMV certification will be required.

6.2.1 Integrated

Integrated solutions typically involve an Electronic Cash Register (ECR) that is connected to a terminal containing the EMV kernel and providing all EMV functionality including card acquisition and PIN entry.

Table 6-1 Integrated Solutions

Integrated Solution	Description
Fully Integrated	The terminal provides the EMV functionality, but the ECR still handles card data and host communication. Therefore, it is in scope for PCI and full EMV certification.
Semi-Integrated	The terminal not only provides the EMV functionality, but also handles the host communication, so the ECR does not see the card data. Therefore, the ECR is not in scope for PCI or full EMV certification. Only a minimal EMV validation script must be run for semi-integrated solutions.

6.2.2 Standalone

Standalone solutions consist of a terminal that runs the POS software, contains the EMV kernel and provides all EMV functionality. PIN entry occurs on an internal or external PIN pad and if contactless is supported, the reader may be integrated into the terminal or be a separate device. A standalone solution is in scope for PCI and full EMV certification.

6.3 EMV Certifications

Magstripe swiped and key entered transactions will continue to be certified directly through Heartland per the existing processes already in place. However, EMV requires additional certifications. Each card brand has its own proprietary chip applications that run on EMV cards bearing their brand. For that reason, each card brand has its own certification requirements that must be met and submitted for approval.

6.3.1 Test Requirements

The card brand certification requirements must be met for each distinct POS configuration that will be deployed, which is defined by a unique combination of:

- The **kernel software**, which includes the Level 2 Contact Application Kernel and/or Level 2 Contactless Application Kernel (payWave, Mastercard Contactless, Expresspay, etc.).
- The **terminal application software**, which includes the payment application software and the terminal-to-acquirer communication software.
- The **specific terminal configuration**, which includes use of a particular EMVCo Level 2 approved kernel configuration for the specific Terminal Type, Terminal Capabilities and other relevant terminal parameter settings.
- The **complete connection path** from the terminal to the card brand.

The card brand certification requirements must be met when any of the following occurs:

- A particular POS configuration is deployed for the first time.
- A major upgrade is made to an already deployed POS configuration.
- The terminal hardware and software is upgraded and the change is major according to the EMVCo Type Approval Bulletin No. 11 (*http://www.emvco.com/approvals.aspx?id=108)*. **Note:** Replacing the IFM with another approved IFM is not considered a major change.
- A contact terminal is upgraded to support contactless transactions.
- The terminal application software is upgraded to support additional payment related functionality such as the partial approval, purchase with cash back, purchase with gratuity, cardholder application selection, etc.
- The Level 2 kernel configuration is modified.
- The terminal is upgraded to support an additional AID.
- The acquirer modifies its network in such a way that it affects the transaction message mapping between the POS and the acquirer host that interfaces with the card brand networks.
- The card brand requests it, for instance, in the scope of the ad-hoc resolution of a field interoperability issue.

REQUIREMENT	If an EMV POS Solution supports multiple kernel configurations, multiple certifications will be required, one for each kernel configuration that will be used in production.

6.3.2 Test Plans

The following card brand test plans must be executed for full EMV certifications:

6.3.2.1 Visa Smart Debit/Credit (VSDC) Testing

Table 6-2 VSDC Testing

Test Plan	Description
Acquirer Device Validation Toolkit (ADVT) User Guide	Test cases for EMV contact card acceptance.
Contactless Device Evaluation Toolkit (CDET) User Guide	Test cases for general contactless card acceptance.
Visa U.S. Debit ADVT-CDET Use Cases	Test cases for EMV contact and contactless debit card acceptance.

6.3.2.2 Mastercard Terminal Integration Process (M-TIP) Testing

Table 6-3 M-TIP Testing

Test Plan	Description
M-TIP 2.0 – M-TIP Subset	Test cases for EMV contact card acceptance.
M-TIP 2.0 – Contactless Subset 6	Test cases for EMV contactless card acceptance.
M-TIP 2.0 – Contactless Subset 8	Test cases for EMV contactless card acceptance.

6.3.2.3 AMEX Integrated Circuit Card Payment Specification (AEIPS) Testing

Table 6-4 AEIPS Testing

Test Plan	Description
Global AEIPS Terminal Test Plan	Test cases for EMV contact card acceptance.
AMEX Quick Chip Terminal Test Plan	Test cases for EMV Quick Chip contact card acceptance.
Global Expresspay EMV Terminal End-to-End Test Plan	Test cases for EMV contactless card acceptance.

6.3.2.4 Discover D-Payment Application Specification (D-PAS) Testing

Table 6-5 D-PAS Testing

Test Plan	Description
Contact D-PAS Acquirer-Terminal End-to-End Test Plan	Test cases for EMV contact card acceptance.
Contactless D-PAS Acquirer-Terminal End-to-End Test Plan	Test cases for EMV contactless card acceptance.

6.3.3 Test Tools

To successfully execute the test plans, you need the following:

1. The appropriate test cards.
2. A means of capturing, logging and validating the interaction between the terminal and cards.

One method to accomplish this is to order all of the required physical test cards from a company such as FIME, along with their Smartspy tools for logging the interaction. However, because there are hundreds of different test cases and test cards and the requirements often change for both, this approach is prohibitively impractical and expensive. Heartland recommends purchasing test tools instead.

Many EMV test tools are available on the market today that remove the need for physical test cards and rudimentary card spies. These tools emulate all the required test cards, facilitate execution of the test cases, capture the interaction between the terminal and the cards in a readable format, clearly indicate pass/fail results of the test cases and log the results in the format required for submission to the card brands.

You may use any test tool if it has been approved for use by a card brand for the purpose of meeting that brand's certification requirements. Each card brand maintains a list of approved test tools that have been verified to properly emulate the test cards and execute the test cases required for certification.

The following tools are approved by all four card brands for both contact and contactless EMV testing:

- ICC Solutions' **ICCSimTmat Test Manager**
- UL Transaction Security's **Collis Brand Test Tool**

You may choose to purchase either of these tools or any other tools approved for use by one or more card brands. Heartland uses the Collis Brand Test Tool for testing our internally developed applications. If you choose to purchase Collis, Heartland can apply knowledge and expertise of that tool toward facilitating your testing.

6.3.4 Test Environments

Heartland currently has two EMV test environments:

Table 6-6 Test Environments

Test Environment	Description
Pre-certification	This environment is used for executing the card brand test cases to ensure a 100% pass rate prior to moving to certification. This environment can also be used for generic EMV and non-EMV testing where certain dollar amounts trigger fixed responses from the host.
Certification	This environment is used for executing the card brand test cases for submission to the card brands for formal certification.

It is essential that you work with POS Integrations to insure you are pointed to the correct test environment based on the type of testing you are executing.

6.3.5 Test Process

You will need to work with our POS Integrations team to understand and follow their current certification procedures. The following is only a high-level overview of the process:

Table 6-7 Test Process

Test Process	Description
Certification Setup	A certification analyst will provide you with the appropriate certification request forms. Once those are returned and processed, the POS Integrations team will set up the required test accounts, point them to the appropriate environments, provide you with the corresponding credentials and provide test scripts as follows: • **Visa** – No script available. You must configure your test tool according to configuration being certified and it will specify test case applicability. • **Mastercard** – We provide a TSE file that contains your script and must be imported into your test tool. • **American Express** – We provide access to the AMEX Test System (ATS) which contains your script. • **Discover** – We provide a spreadsheet from UL that contains your script.
Card Brand Pre-Certification	Execute all card brand test cases in our pre-certification environment to ensure a 100% pass rate prior to moving to certification. Our certification analyst may request your terminal logs and transaction receipts if needed to help resolve issues.
Class B Certification	Execute the non-EMV test script provided by our certification analyst. The analysts will review the results and provide their analysis. Errors are corrected and test cases re-executed if necessary.

Table 6-7 Test Process (Continued)

Test Process	Description
Card Brand Certification	Execute all card brand test cases in our certification environment. The following actions must be completed depending on card brand: • **Visa** – Export XML file for upload to Chip Compliance Reporting Tool (CCRT). • **Mastercard** – Export TSEZ file containing terminal logs and validation, host logs and validation and receipts. • **American Express** – Complete user validations and upload terminal logs in ATS. • **Discover** – Indicate results and add comments as needed in provided spreadsheet.
Card Brand Submission	A certification analyst will ensure that all test cases have been completed then submit the results to the card brands for approval. The turnaround time for the card brands to review, approve and return a Letter of Approval is typically 10-15 business days.

REQUIREMENT	Your terminal(s) of choice must have EMVCo Level 2 approved kernel configurations that match each of the configurations specified in your certification request forms.

6.4 EMV Support

Our POS Integrations team is available from 9:00 AM to 5:00 PM Eastern to support EMV testing and can be reached at one of the following email addresses based on message spec:

- Exchange: *POSIntegrationExchange@e-hps.com*
- Portico: *POSIntegrationPortico@e-hps.com*
- POS 8583: *POSIntegration8583@e-hps.com*
- NTS: *POSIntegrationNTS@e-hps.com*
- Z01: *POSIntegrationZ01@e-hps.com*

This page intentionally left blank for duplex printing.

Chapter 7: EMV Terminal Interface

7.1 EMV Terminal to Card Communication

7.1.1 Application Protocol Data Units (APDUs)

The terminal talks to the Integrated Circuit Card (ICC) using Application Protocol Data Unit (APDU) command-response pairs, which have the following formats:

- Command APDU Format

Table 7-1 Command APDU Format

Code	Description	Length
CLA	Class of instruction	1
INS	Instruction code	1
P1	Instruction parameter 1	1
P2	Instruction parameter 2	1
Lc	Number of bytes present in command data field	0 or 1
Data	String of data bytes send in command (= Lc)	var.
Le	Maximum number of data bytes expected in data field of response	0 or 1

- Response APDU Format

Table 7-2 Response APDU Format

Code	Description	Length
Data	String of data bytes received in response	var. (= Lr)
SW1	Command processing status	1
SW2	Command processing qualifier	1

Where...

- **SW1 SW2** = '9000' (Success)
- **SW1 SW2** = '6xxx' (Failure)

7.1.2 Tag, Length, Value (TLV) Data Objects

Data objects are BER-TLV coded, as defined in ISO/IEC 8825:

- The **T**ag field consists of one or more consecutive bytes. It indicates a class, a type, and a number. EMV tags are coded on one or two bytes.
- The **L**ength field consists of one or more consecutive bytes that indicate the length of the following value field.
  - If bit 8 of the most significant byte of the length field is set to **0**, the length field consists of only one byte. Bits 7 to 1 code the number of bytes of the value field, for lengths from 1 to 127.
  - If bit 8 of the most significant byte of the length field is set to **1**, the subsequent bits 7 to 1 code the number of subsequent bytes in the length field. The subsequent bytes code an integer representing the number of bytes in the value field. Two bytes are necessary to express lengths from 128 to 255.
- The **V**alue field indicates the value of the data object. If L = 00, the value field is not present.

7.1.3 Kernel Application Programming Interface (API)

Your terminal will come with a Software Development Kit (SDK) that provides an extraction layer/library built on top of the EMVCo Level 2 contact approved kernel application that allows your payment application to run EMV transactions. Discussion of the specific functions/methods that are part of the SDKs provided by the device manufacturers is outside of the scope of this document, although the intent of this document is to provide the background needed to successfully utilize any API.

7.2 EMV Data Elements

7.2.1 Data Conventions

The following sections describe the TLV data objects that come from the terminal, card, and issuer. The Value column uses the following format conventions:

Table 7-3 Data Conventions

Value	Description
a	Alphabetic data elements contain a single character per byte. The permitted characters are alphabetic only (a to z and A to Z, upper and lower case).
an	Alphanumeric data elements contain a single character per byte. The permitted characters are alphabetic (a to z and A to Z, upper and lower case) and numeric (0 to 9).
ans	Alphanumeric Special data elements contain a single character per byte. The permitted characters and their coding are shown in the Common Character Set table in Annex B of Book 4. There is one exception: The permitted characters for Application Preferred Name are the non-control characters defined in the ISO/IEC 8859 part designated in the Issuer Code Table Index associated with the Application Preferred Name.
b	These data elements consist of either unsigned binary numbers or bit combinations that are defined elsewhere in the specification. **Binary example:** The Application Transaction Counter (ATC) is defined as "b" with a length of two bytes. An ATC value of 19 is stored as Hex '00 13'. **Bit combination example:** Processing Options Data Object List (PDOL) is defined as "b" with the format shown in Book 3, section 5.4.
cn	Compressed numeric data elements consist of two numeric digits (having values in the range Hex '0'–'9') per byte. These data elements are left justified and padded with trailing hexadecimal 'F's. **Example:** The Application Primary Account Number (PAN) is defined as "cn" with a length of up to ten bytes. A value of 1234567890123 may be stored in the Application PAN as Hex '12 34 56 78 90 12 3F FF' with a length of 8.
n	Numeric data elements consist of two numeric digits (having values in the range Hex '0'–'9') per byte. These digits are right justified and padded with leading hexadecimal zeroes. Other specifications sometimes refer to this data format as Binary Coded Decimal ("BCD") or unsigned packed. **Example:** Amount, Authorised (Numeric) is defined as "n 12" with a length of six bytes. A value of 12345 is stored in Amount, Authorised (Numeric) as Hex '00 00 00 01 23 45'.
var.	Variable data elements are variable length and may contain any bit combination. Additional information on the formats of specific variable data elements is available elsewhere.

7.2.2 Terminal Data

The following data comes from the terminal, payment application, or parameter management system:

Table 7-4 Terminal Data

<table>
<tr><th>Name</th><th>Tag</th><th>Length</th><th>Value</th><th colspan="9">Description</th></tr>
<tr><td rowspan="22">ADDITIONAL TERMINAL CAPABILITIES</td><td rowspan="22">9F40</td><td rowspan="22">5</td><td rowspan="22">b</td><td colspan="9">Indicates the data input and output capabilities of the terminal.</td></tr>
<tr><td colspan="9">Byte 1 – Transaction Type Capability</td></tr>
<tr><td>b8</td><td>b7</td><td>b6</td><td>b5</td><td>b4</td><td>b3</td><td>b2</td><td>b1</td><td>Meaning</td></tr>
<tr><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Cash</td></tr>
<tr><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Goods</td></tr>
<tr><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Services</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Cashback</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>Inquiry</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>Transfer</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>Payment</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>Administrative</td></tr>
<tr><td colspan="9">Byte 2 – Transaction Type Capability</td></tr>
<tr><td>b8</td><td>b7</td><td>b6</td><td>b5</td><td>b4</td><td>b3</td><td>b2</td><td>b1</td><td>Meaning</td></tr>
<tr><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Cash Deposit</td></tr>
<tr><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>RFU</td></tr>
</table>

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description								
ADDITIONAL TERMINAL CAPABILITIES (cont'd)	9F40	5	b	**Byte 3 – Terminal Data Input Capability**								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				1	x	x	x	x	x	x	x	Numeric keys
				x	1	x	x	x	x	x	x	Alphabetic and special character keys
				x	x	1	x	x	x	x	x	Command keys
				x	x	x	1	x	x	x	x	Function keys
				x	x	x	x	0	x	x	x	RFU
				x	x	x	x	x	0	x	x	RFU
				x	x	x	x	x	x	0	x	RFU
				x	x	x	x	x	x	x	0	RFU
				Byte 4 – Terminal Data Output Capability								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				1	x	x	x	x	x	x	x	Print, attendant
				x	1	x	x	x	x	x	x	Print, cardholder
				x	x	1	x	x	x	x	x	Display, attendant
				x	x	x	1	x	x	x	x	Display, cardholder
				x	x	x	x	0	x	x	x	RFU
				x	x	x	x	x	0	x	x	RFU
				x	x	x	x	x	x	1	x	Code table 10
				x	x	x	x	x	x	x	1	Code table 9

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description
ADDITIONAL TERMINAL CAPABILITIES (cont'd)	9F40	5	b	**Byte 5 – Terminal Data Output Capability**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Code table 8
x	1	x	x	x	x	x	x	Code table 7
x	x	1	x	x	x	x	x	Code table 6
x	x	x	1	x	x	x	x	Code table 5
x	x	x	x	1	x	x	x	Code table 4
x	x	x	x	x	1	x	x	Code table 3
x	x	x	x	x	x	1	x	Code table 2
x	x	x	x	x	x	x	1	Code table 1

AMOUNT, AUTHORISED (NUMERIC)	9F02	6	n 12	Authorized amount of the transaction (excluding adjustments).
AMOUNT, OTHER (NUMERIC)	9F03	6	n 12	Secondary amount associated with the transaction representing a cashback amount.
APPLICATION IDENTIFIER (AID) - TERMINAL	9F06	3	b	Identifies the application as described in ISO/IEC 7816-5. Consists of the Registered Application Provider Identifier (RID) + a Proprietary Application Identifier Extension (PIX).
APPLICATION SELECTION INDICATOR	—	At the discretion of the terminal. The data is not sent across the interface	See length	For an application in the ICC to be supported by an application in the terminal, the Application Selection Indicator indicates whether the associated AID in the terminal must match the AID in the card exactly, including the length of the AID, or only up to the length of the AID in the terminal. There is only one Application Selection Indicator per AID supported by the terminal.
APPLICATION VERSION NUMBER	9F09	2	b	Version number assigned by the payment system for the application.
AUTHORISATION RESPONSE CODE (ARC)	8A	2	an 2	Code that defines the disposition of a message. Terminal should set the value according to *Table 7-20 Online or Offline Disposition, p. 153*.

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description		
CARDHOLDER VERIFICATION METHOD (CVM) RESULTS	9F34	3	b	Indicates the results of the last CVM performed.		
				Byte 1	CVM Performed	Last CVM of the CVM List actually performed by the terminal: One-byte CVM Code of the CVM List as defined in Book 3 ('3F' if no CVM is performed).
				Byte 2	CVM Condition	One-byte CVM Condition Code of the CVM List as defined in Book 3 or '00' if no actual CVM was performed.
				Byte 3	CVM Result	Result of the (last) CVM performed as known by the terminal: • 0 = Unknown (for example, for signature) • 1 = Failed (for example, for offline PIN) • 2 = Successful (for example, for offline PIN) or set to '1' if no CVM Condition Code was satisfied or if the CVM Code was not recognized or not supported.
CERTIFICATION AUTHORITY PUBLIC KEY CHECK SUM	—	20	b	A check value calculated on the concatenation of all parts of the Certification Authority Public Key (RID, Certification Authority Public Key Index, Certification Authority Public Key Modulus, Certification Authority Public Key Exponent) using SHA-1.		
CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	—	1 or 3	b	Value of the exponent part of the Certification Authority Public Key.		
CERTIFICATION AUTHORITY PUBLIC KEY INDEX	9F22	1	b	Identifies the certification authority's public key in conjunction with the RID.		
CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	—	N_{CA} (up to 248)	b	Value of the modulus part of the Certification Authority Public Key.		
DEFAULT DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)	—	var.	b	DDOL to be used for constructing the INTERNAL AUTHENTICATE command if the DDOL in the card is not present.		
DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)	—	var.	b	TDOL to be used for generating the TC Hash Value if the TDOL in the card is not present.		
ENCIPHERED PERSONAL IDENTIFICATION NUMBER (PIN) DATA	—	8	b	Transaction PIN enciphered at the PIN pad for online verification or for offline verification if the PIN pad and IFD are not a single integrated device.		
INTERFACE DEVICE (IFD) SERIAL NUMBER	9F1E	8	an 8	Unique and permanent serial number assigned to the IFD by the manufacturer.		

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description		
ISSUER SCRIPT RESULTS	9F5B	var. (up to 20)	b	Indicates the result of the terminal script processing. **Note:** Bytes 1-5 are repeated for each Issuer Script processed by the terminal.		
				Byte 1	SCRIPT RESULT	Most significant nibble: Result of the Issuer Script processing performed by the terminal: • 0 = Script not performed 1 = Script processing failed 2 = Script processing successful Least significant nibble: Sequence number of the Script Command: • 0 = Not specified • 1 to E = Sequence number from 1 to 14 • F = Sequence number of 15 or above
				Byte 2–5	SCRIPT IDENTIFIER	Script Identifier of the Issuer Script received by the terminal, if available, zero filled if not. Mandatory if more than one Issuer Script was received by the terminal.
MAXIMUM TARGET PERCENTAGE TO BE USED FOR BIASED RANDOM SELECTION	—	1	n 2	Value used in terminal risk management for random transaction selection. This is the desired percentage of transactions "just below" the floor limit that will be selected to go online.		
POINT-OF-SERVICE (POS) ENTRY MODE	9F39	1	n 2	Indicates the method by which the PAN was entered, according to the first two digits of the ISO 8583:1987 POS Entry Mode.		
TARGET PERCENTAGE TO BE USED FOR RANDOM SELECTION	—	1	n 2	Value used in terminal risk management for random transaction selection. For transactions with amounts less than the Threshold Value for Biased Random Selection, the terminal shall generate a random number from 1 to 99, and if this number is less than or equal to this value, the transaction shall be selected to go online.		
TERMINAL ACTION CODE (TAC) – DEFAULT	FFC6	5	b	Specifies the acquirer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online.		
TERMINAL ACTION CODE (TAC) – DENIAL	FFC7	5	b	Specifies the acquirer's conditions that cause the denial of a transaction without attempt to go online.		
TERMINAL ACTION CODE (TAC) – ONLINE	FFC8	5	b	Specifies the acquirer's conditions that cause a transaction to be transmitted online.		

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description								
TERMINAL CAPABILITIES	9F33	3	b	Indicates the data input and output capabilities of the terminal.								
				Byte 1 – Card Data Input Capability								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				1	x	x	x	x	x	x	x	Manual key entry
				x	1	x	x	x	x	x	x	Magnetic stripe
				x	x	1	x	x	x	x	x	IC with contacts
				x	x	x	0	x	x	x	x	RFU
				x	x	x	x	0	x	x	x	RFU
				x	x	x	x	x	0	x	x	RFU
				x	x	x	x	x	x	0	x	RFU
				x	x	x	x	x	x	x	0	RFU
				Byte 2 – CVM Capability								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				1	x	x	x	x	x	x	x	Plaintext PIN for ICC verification
				x	1	x	x	x	x	x	x	Enciphered PIN for online verification
				x	x	1	x	x	x	x	x	Signature (paper)
				x	x	x	1	x	x	x	x	Enciphered PIN for offline verification
				x	x	x	x	1	x	x	x	No CVM Required
				x	x	x	x	x	0	x	x	RFU
				x	x	x	x	x	x	0	x	RFU
				x	x	x	x	x	x	x	0	RFU

Table 7-4 Terminal Data (Continued)

<table>
<tr><th>Name</th><th>Tag</th><th>Length</th><th>Value</th><th>Description</th></tr>
<tr><td>TERMINAL CAPABILITIES (cont'd)</td><td>9F33</td><td>3</td><td>b</td><td>
Byte 3 – Security Capability
<table>
<tr><th>b8</th><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>Meaning</th></tr>
<tr><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>SDA</td></tr>
<tr><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>DDA</td></tr>
<tr><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Card capture</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>CDA</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>RFU</td></tr>
</table>
</td></tr>
<tr><td>TERMINAL COUNTRY CODE</td><td>9F1A</td><td>2</td><td>n 3</td><td>Indicates the country of the terminal, represented according to ISO 3166.</td></tr>
<tr><td>TERMINAL FLOOR LIMIT</td><td>9F1B</td><td>4</td><td>b</td><td>Indicates the floor limit in the terminal in conjunction with the AID.
Indicates the amount above which an online authorization is required for contact transactions.</td></tr>
<tr><td>TERMINAL RISK MANAGEMENT DATA</td><td>9F1D</td><td>1–8</td><td>b</td><td>Application-specific value used by the card for risk management purposes.</td></tr>
<tr><td>TERMINAL TYPE</td><td>9F35</td><td>1</td><td>n 2</td><td>Indicates the environment of the terminal, its communications capability, and its operational control.
<table>
<tr><th rowspan="2">Environment</th><th colspan="3">Operational Control Provided by:</th></tr>
<tr><th>Financial Institution</th><th>Merchant</th><th>Cardholder</th></tr>
<tr><td>Attended</td><td></td><td></td><td></td></tr>
<tr><td>Online only</td><td>11</td><td>21</td><td></td></tr>
<tr><td>Online with offline capability</td><td>12</td><td>22</td><td></td></tr>
<tr><td>Offline only</td><td>13</td><td>23</td><td></td></tr>
<tr><td>Unattended</td><td></td><td></td><td></td></tr>
<tr><td>Online only</td><td>14</td><td>24</td><td>34</td></tr>
<tr><td>Online with offline capability</td><td>15</td><td>25</td><td>35</td></tr>
<tr><td>Offline only</td><td>16</td><td>26</td><td>36</td></tr>
</table>
</td></tr>
</table>

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description								
TERMINAL VERIFICATION RESULTS (TVR)	95	5	b	Status of the different functions as seen from the terminal.								
				Byte 1								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				1	x	x	x	x	x	x	x	Offline data authentication was not performed
				x	1	x	x	x	x	x	x	SDA failed
				x	x	1	x	x	x	x	x	ICC data missing
				x	x	x	1	x	x	x	x	Card appears on terminal exception file
				x	x	x	x	1	x	x	x	DDA failed
				x	x	x	x	x	1	x	x	CDA failed
				x	x	x	x	x	x	1	x	SDA selected
				x	x	x	x	x	x	x	0	RFU
				Byte 2								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				1	x	x	x	x	x	x	x	ICC and terminal have different application versions
				x	1	x	x	x	x	x	x	Expired application
				x	x	1	x	x	x	x	x	Application not yet effective
				x	x	x	1	x	x	x	x	Requested service not allowed for card product
				x	x	x	x	1	x	x	x	New card
				x	x	x	x	x	0	x	x	RFU
				x	x	x	x	x	x	0	x	RFU
				x	x	x	x	x	x	x	0	RFU

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description								
TERMINAL VERIFICATION RESULTS (TVR) (cont'd)	95	5	b	**Byte 3**								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				1	x	x	x	x	x	x	x	Cardholder verification was not successful
				x	1	x	x	x	x	x	x	Unrecognized CVM
				x	x	1	x	x	x	x	x	PIN Try Limit exceeded
				x	x	x	1	x	x	x	x	PIN entry required and PIN pad not present or not working
				x	x	x	x	1	x	x	x	PIN entry required, PIN pad present, but PIN was not entered
				x	x	x	x	x	1	x	x	Online PIN entered
				x	x	x	x	x	x	0	x	RFU
				x	x	x	x	x	x	x	0	RFU
				Byte 4								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				1	x	x	x	x	x	x	x	Transaction exceeds floor limit
				x	1	x	x	x	x	x	x	Lower consecutive offline limit exceeded
				x	x	1	x	x	x	x	x	Upper consecutive offline limit exceeded
				x	x	x	1	x	x	x	x	Transaction selected randomly for online processing
				x	x	x	x	1	x	x	x	Merchant forced transaction online
				x	x	x	x	x	0	x	x	RFU
				x	x	x	x	x	x	0	x	RFU
				x	x	x	x	x	x	x	0	RFU

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description
TERMINAL VERIFICATION RESULTS (TVR) (cont'd)	95	5	b	**Byte 5 – Terminal Data Output Capability**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Default TDOL used
x	1	x	x	x	x	x	x	Issuer authentication failed
x	x	1	x	x	x	x	x	Script processing failed
x	x	x	1	x	x	x	x	Code table 5
x	x	x	x	1	x	x	x	Code table 4
x	x	x	x	x	1	x	x	Code table 3
x	x	x	x	x	x	1	x	Code table 2
x	x	x	x	x	x	x	1	Code table 1

THRESHOLD VALUE FOR BIASED RANDOM SELECTION	—	4	b	Value used in terminal risk management for random transaction selection. Transactions with amounts less than this value will be subject to selection at random without further regard for the value of the transaction. Transactions with amounts equal to or greater than this value but less than the floor limit will be subject to selection with bias toward sending higher value transaction online more frequently (biased random selection).
TRANSACTION CURRENCY CODE	5F2A	2	n 3	Indicates the currency code of the transaction according to ISO 4217.
TRANSACTION CURRENCY EXPONENT	5F36	1	n 1	Indicates the implied position of the decimal point from the right of the transaction amount represented according to ISO 4217.
TRANSACTION DATE	9A	3	n 6 YYMMDD	Local date that the transaction was authorized.

Table 7-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description
TRANSACTION REFERENCE CURRENCY CODE	9F3C	2	n 3	Code defining the common currency used by the terminal in case the Transaction Currency Code is different from the Application Currency Code.
TRANSACTION REFERENCE CURRENCY CONVERSION	—	4	n 8	Factor used in the conversion from the Transaction Currency Code to the Transaction Reference Currency Code.
TRANSACTION REFERENCE CURRENCY EXPONENT	9F3D	1	n 1	Indicates the implied position of the decimal point from the right of the transaction amount, with the Transaction Reference Currency Code represented according to ISO 4217.
TRANSACTION TYPE	9C	1	n 2	Indicates the type of financial transaction, represented by the first two digits of the ISO 8583:1987 Processing Code. • 00 = Purchase or Card Verify • 09 = Purchase with Cashback • 20 = Purchase Return • 30 = Balance Inquiry
UNPREDICTABLE NUMBER	9F37	1	b	Value to provide variability and uniqueness to the generation of a cryptogram.

7.2.3 Card Data

The following data comes from the ICC:

Table 7-5 Card Data

Name	Tag	Length	Value	Description
APPLICATION CRYPTOGRAM	9F26	8	b	Cryptogram returned by the ICC in response of the GENERATE AC command.
APPLICATION CURRENCY CODE	9F42	2	n 3	Indicates the currency in which the account is managed according to ISO 4217.
APPLICATION CURRENCY EXPONENT	9F44	1	n 1	Indicates the implied position of the decimal point from the right of the amount represented according to ISO 4217.
APPLICATION DISCRETIONARY DATA	9F05	1–32	b	Issuer or payment system specified data relating to the application.
APPLICATION EFFECTIVE DATE	5F25	3	n6 YYMMDD	Date from which the application may be used.
APPLICATION EXPIRATION DATE	5F24	3	n6 YYMMDD	Date after which application expires.
APPLICATION FILE LOCATOR (AFL)	94	var. up to 252	var.	Indicates the location (SFI, range of records) of the AEFs related to a given application.
APPLICATION DEDICATED FILE (ADF) NAME	4F	5–16	b	Identifies the application as described in ISO/IEC 7816-5.
APPLICATION INTERCHANGE PROFILE	82	2	b	Indicates the capabilities of the card to support specific functions in the application.

Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	1	x	x	x	x	x	x	SDA supported
x	x	1	x	x	x	x	x	DDA supported
x	x	x	1	x	x	x	x	Cardholder verification is supported
x	x	x	x	1	x	x	x	Terminal risk management is to be performed
x	x	x	x	x	1	x	x	Issuer authentication is supported
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	1	CDA supported

Table 7-5 Card Data

Name	Tag	Length	Value	Description								
APPLICATION INTERCHANGE PROFILE (cont'd)	82	2	b	**Byte 2**								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				0	x	x	x	x	x	x	x	Reserved for use by the EMV Contactless Specifications
				x	0	x	x	x	x	x	x	RFU
				x	x	0	x	x	x	x	x	RFU
				x	x	x	0	x	x	x	x	RFU
				x	x	x	x	0	x	x	x	RFU
				x	x	x	x	x	0	x	x	RFU
				x	x	x	x	x	x	0	x	RFU
				x	x	x	x	x	x	x	0	RFU
APPLICATION LABEL	50	1–16	ans with the special character limited to space	Mnemonic associated with the AID according to ISO/IEC 7816-5.								
APPLICATION PREFERRED NAME	9F12	1–16	ans	Preferred mnemonic associated with the AID.								
APPLICATION PRIMARY ACCOUNT NUMBER (PAN)	5A	var. up to 10	cn var. up to 19	Valid cardholder account number.								
APPLICATION PRIMARY ACCOUNT NUMBER (PAN) SEQUENCE NUMBER	5F34	1	n 2	Identifies and differentiates cards with the same PAN.								
APPLICATION PRIORITY INDICATOR	87	1	b	Indicates the priority of a given application or group of applications in a directory.								
APPLICATION REFERENCE CURRENCY	9F3B	2–8	n 3	1-4 currency codes used between the terminal and the ICC when the Transaction Currency Code is different from the Application Currency Code; each code is 3 digits according to ISO 4217.								
APPLICATION REFERENCE CURRENCY EXPONENT	9F43	1–4	n 1	Indicates the implied position of the decimal point from the right of the amount, for each of the 1-4 reference currencies represented according to ISO 4217.								
APPLICATION TRANSACTION COUNTER (ATC)	9F36	2	b	Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC).								

Table 7-5 Card Data

<table>
<tr><th>Name</th><th>Tag</th><th>Length</th><th>Value</th><th>Description</th></tr>
<tr><td>APPLICATION USAGE CONTROL</td><td>9F07</td><td>2</td><td>b</td><td>Indicates issuer's specified restrictions on the geographic usage and services allowed for the application.
Byte 1
<table>
<tr><th>b8</th><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>Meaning</th></tr>
<tr><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Valid for domestic cash transactions</td></tr>
<tr><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Valid for international cash transactions</td></tr>
<tr><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Valid for domestic goods</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Valid for international goods</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>Valid for domestic services</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>x</td><td>Valid for international services</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>x</td><td>Valid at ATMs</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>1</td><td>Valid at terminals other than ATMs</td></tr>
</table>
Byte 2
<table>
<tr><th>b8</th><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>Meaning</th></tr>
<tr><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Domestic cashback allowed</td></tr>
<tr><td>x</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>International cashback allowed</td></tr>
<tr><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>x</td><td>RFU</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>0</td><td>RFU</td></tr>
</table></td></tr>
<tr><td>APPLICATION VERSION NUMBER</td><td>9F08</td><td>2</td><td>b</td><td>Version number assigned by the payment system for the application.</td></tr>
<tr><td>CARD RISK MANAGEMENT DATA OBJECT LIST 1 (CDOL1)</td><td>8C</td><td>var. up to 252</td><td>b</td><td>List of data objects (tag and length) to be passed to the ICC in the first GENERATE AC command.</td></tr>
<tr><td>CARD RISK MANAGEMENT DATA OBJECT LIST 2 (CDOL2)</td><td>8D</td><td>var. up to 252</td><td>b</td><td>List of data objects (tag and length) to be passed to the ICC in the second GENERATE AC command.</td></tr>
<tr><td>CARDHOLDER NAME</td><td>5F20</td><td>2–26</td><td>ans</td><td>Indicates cardholder name according to ISO 7813.</td></tr>
</table>

Table 7-5 Card Data

Name	Tag	Length	Value	Description								
CARDHOLDER NAME EXTENDED	9F0B	27–45	ans	Indicates the whole cardholder name when greater than 26 characters using the same coding convention as in ISO 7813.								
CARDHOLDER VERIFICATION METHOD (CVM) LIST	8E	10–252	b	Identifies a method of verification of the cardholder supported by the application.								
				CV Rule Byte 1								
				b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				0								RFU
					0							Fail cardholder verification if this CVM is unsuccessful
					1							Apply succeeding CV Rule if this CVM is unsuccessful
						0	0	0	0	0	0	Fail CVM processing
						0	0	0	0	0	1	Plaintext PIN verification performed by ICC
						0	0	0	0	1	0	Enciphered PIN verified online
						0	0	0	0	1	1	Plaintext PIN verification performed by ICC and signature (paper)
						0	0	0	1	0	0	Enciphered PIN verification performed by ICC
						0	0	0	1	0	1	Enciphered PIN verification performed by ICC and signature (paper)
						0	x	x	x	x	x	Values in the range 000110–011101 reserved for future use by this specification
						0	1	1	1	1	0	Signature (paper)
						0	1	1	1	1	1	No CVM required
						1	0	x	x	x	x	Values in the range 100000–101111 reserved for use by the individual payment systems
						1	1	x	x	x	x	Values in the range 110000–111110 reserved for use by the issuer
						1	1	1	1	1	1	This value is not available for use

Table 7-5 Card Data

Name	Tag	Length	Value	Description
CARDHOLDER VERIFICATION METHOD (CVM) LIST (cont'd)	8E	10–252	b	**CV Rule Byte 2**
				Value: Message
				00: Always
				01: If unattended cash
				02: If not unattended cash and not manual cash and not purchase with cashback
				03: If terminal supports the CVM
				04: If manual cash
				05: If purchase with cashback
				06: If transaction is in the application currency and is under X value
				07: If transaction is in the application currency and is over X value
				08: If transaction is in the application currency and is under Y value
				09: If transaction is in the application currency and is over Y value
				0A–7F: RFU
				80–FF: Reserved for card brands
CERTIFICATION AUTHORITY PUBLIC KEY INDEX	8F	1	b	Identifies the certification authority's public key in conjunction with the RID.
CRYPTOGRAM INFORMATION DATA	9F27	1	b	Indicates the type of cryptogram and the actions to be performed by the terminal.
DEDICATED FILE (DF) NAME	84	5–16	b	Identifies the name of the DF as described in ISO/IEC 7816-4.
DIRECTORY DEFINITION FILE (DDF) NAME	9D	5–16	b	Identifies the name of a DF associated with a directory.
DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)	9F49	var. up to 252	b	List of data objects (tag and length) to be passed to the ICC in the INTERNAL AUTHENTICATE command.
FILE CONTROL INFORMATION (FCI) TEMPLATE	6F	var. up to 252	var.	Identifies the FCI template according to ISO/IEC 7816-4.
ICC DYNAMIC NUMBER	9F4C	2–8	b	Time-variant number generated by the ICC, to be captured by the terminal.
INTEGRATED CIRCUIT CARD (ICC) PIN ENCIPHERMENT PUBLIC KEY CERTIFICATE	9F2D	N_I	b	ICC PIN Encipherment Public Key certified by the issuer.

Table 7-5 Card Data

Name	Tag	Length	Value	Description
INTEGRATED CIRCUIT CARD (ICC) PIN ENCIPHERMENT PUBLIC KEY EXPONENT	9F2E	1 or 3	b	ICC PIN Encipherment Public Key Exponent used for PIN Encipherment.
INTEGRATED CIRCUIT CARD (ICC) PIN ENCIPHERMENT PUBLIC KEY REMAINDER	9F2F	$N_{PE} - N_I + 42$	b	Remaining digits of the ICC PIN Encipherment Public Key Modulus.
INTEGRATED CIRCUIT CARD (ICC) PUBLIC KEY CERTIFICATE	9F46	N_I	b	ICC Public Key certified by the issuer.
INTEGRATED CIRCUIT CARD (ICC) PUBLIC KEY EXPONENT	9F47	1 to 3	b	ICC Public Key Exponent used for the verification of the Signed Dynamic Application Data.
INTEGRATED CIRCUIT CARD (ICC) PUBLIC KEY REMAINDER	9F48	$N_{IC} - N_I + 42$	b	Remaining digits of the ICC Public Key Modulus.
ISSUER ACTION CODE (IAC) – DEFAULT	9F0D	5	b	Specifies the issuer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online.
ISSUER ACTION CODE (IAC) – DENIAL	9F0E	5	b	Specifies the issuer's conditions that cause the denial of a transaction without attempt to go online.
ISSUER ACTION CODE (IAC) – ONLINE	9F0F	5	b	Specifies the issuer's conditions that cause a transaction to be transmitted online.
ISSUER APPLICATION DATA	9F10	var. up to 32	b	Contains proprietary application data for transmission to the issuer in an online transaction.
ISSUER CODE TABLE INDEX	9F11	1	n 2	Indicates the code table according to ISO/IEC 8859 for displaying the Application Preferred Name.
ISSUER COUNTRY CODE	5F28	2	n 3	Indicates the country of the issuer according to ISO 3166.
ISSUER PUBLIC KEY CERTIFICATE	90	N_{CA}	b	Issuer public key certified by a certification authority.
ISSUER PUBLIC KEY EXPONENT	9F32	1 to 3	b	Issuer public key exponent used for the verification of the Signed Static Application Data and the ICC Public Key Certificate.
ISSUER PUBLIC KEY REMAINDER	92	$N_I - N_{CA} + 36$	b	Remaining digits of the Issuer Public Key Modulus.
LANGUAGE PREFERENCE	5F2D	2–8	an 2	1–4 languages stored in order of preference, each represented by 2 alphabetical characters according to ISO 639.
LAST ONLINE APPLICATION TRANSACTION COUNTER (ATC) REGISTER	9F13	2	b	ATC value of the last transaction that went online.

Table 7-5 Card Data

Name	Tag	Length	Value	Description
LOWER CONSECUTIVE OFFLINE LIMIT	9F14	1	b	Issuer-specified preference for the maximum number of consecutive offline transactions for this ICC application allowed in a terminal with online capability.
PERSONAL IDENTIFICATION NUMBER (PIN) TRY COUNTER	9F17	1	b	Number of PIN tries remaining.
PROCESSING OPTIONS DATA OBJECT LIST (PDOL)	9F38	var.	b	Contains a list of terminal resident data objects (tags and lengths) needed by the ICC in processing the GET PROCESSING OPTIONS command.
SERVICE CODE	5F30	2	n 3	Service code as defined in ISO/IEC 7813 for Track 1 and Track 2.
SHORT FILE IDENTIFIER (SFI)	88	1	b	Identifies the AEF referenced in commands related to a given ADF or DDF. It is a binary data object having a value in the range 1 to 30 and with the three high order bits set to zero.
SIGNED DYNAMIC APPLICATION DATA	9F4B	N_{IC}	b	Digital signature on critical application parameters for DDA or CDA.
SIGNED STATIC APPLICATION DATA	93	N_I	b	Digital signature on critical application parameters for SDA.
STATIC DATA AUTHENTICATION TAG LIST	9F4A	var.	—	List of tags of primitive data objects defined in this specification whose value fields are to be included in the Signed Static or Dynamic Application Data.
TRACK 1 DISCRETIONARY DATA	9F1F	var.	ans	Discretionary part of Track 1 according to ISO/IEC 7813.
TRACK 2 DISCRETIONARY DATA	9F20	var.	cn	Discretionary part of Track 2 according to ISO/IEC 7813.
TRACK 2 EQUIVALENT DATA	57	var. up to 19	b n, var. up to 19 b n 4 n 3 n, var. b	Contains the data elements of Track 2 according to ISO/IEC 7813, excluding start sentinel, end sentinel, and Longitudinal Redundancy Check (LRC), as follows: • Primary Account Number • Field Separator (Hex 'D') • Expiration Date (YYMM) • Service Code • Discretionary Data (defined by individual payment systems) • Pad with one Hex 'F' if needed to unsure whole bytes
TRANSACTION CERTIFICATION DATA OBJECT LIST (TDOL)	97	var. up to 252	b	List of data objects (tag and length) to be used by the terminal in generating the TC Hash Value.
UPPER CONSECUTIVE OFFLINE LIMIT	9F23	1	b	Issuer-specified preference for the maximum number of consecutive offline transactions for this ICC application allowed in a terminal without online capability.

7.2.4 Issuer Data

The following data comes from the issuer:

Table 7-6 Issuer Data

Name	Tag	Length	Value	Description
AUTHORIZATION RESPONSE CRYPTOGRAM (ARPC)	—	4 or 8	b	Cryptogram generated by the issuer and used by the card to verify that the response came from the issuer.
CARD STATUS UPDATE (CSU)	—	4	b	Contains data sent to the ICC to indicate whether the issuer approves or declines the transaction, and to initiate actions specified by the issuer. Transmitted to the card in Issuer Authentication Data.
ISSUER AUTHENTICATION DATA	91	8-16	b	Data sent to the ICC for online issuer authentication.
ISSUER SCRIPT COMMAND	86	var. up to 261	b	Contains a command for transmission to the ICC.
ISSUER SCRIPT IDENTIFIER	9F18	4	b	Identification of the Issuer Script.
ISSUER SCRIPT TEMPLATE 1	71	var.	b	Contains proprietary issuer data for transmission to the ICC before the second GENERATE AC command.
ISSUER SCRIPT TEMPLATE 2	72	var.	b	Contains proprietary issuer data for transmission to the ICC after the second GENERATE AC command.
PROPRIETARY AUTHENTICATION DATA	—	var. up to 8	b	Contains issuer data for transmission to the card in the Issuer Authentication Data of an online transaction.

7.3 Contact Transaction Flow

The EMV transaction flow for contact EMV cards consists of up to 13 steps, each of which consist of a set of interactions between the card, terminal, and/or issuer. See *Figure 7-1*.

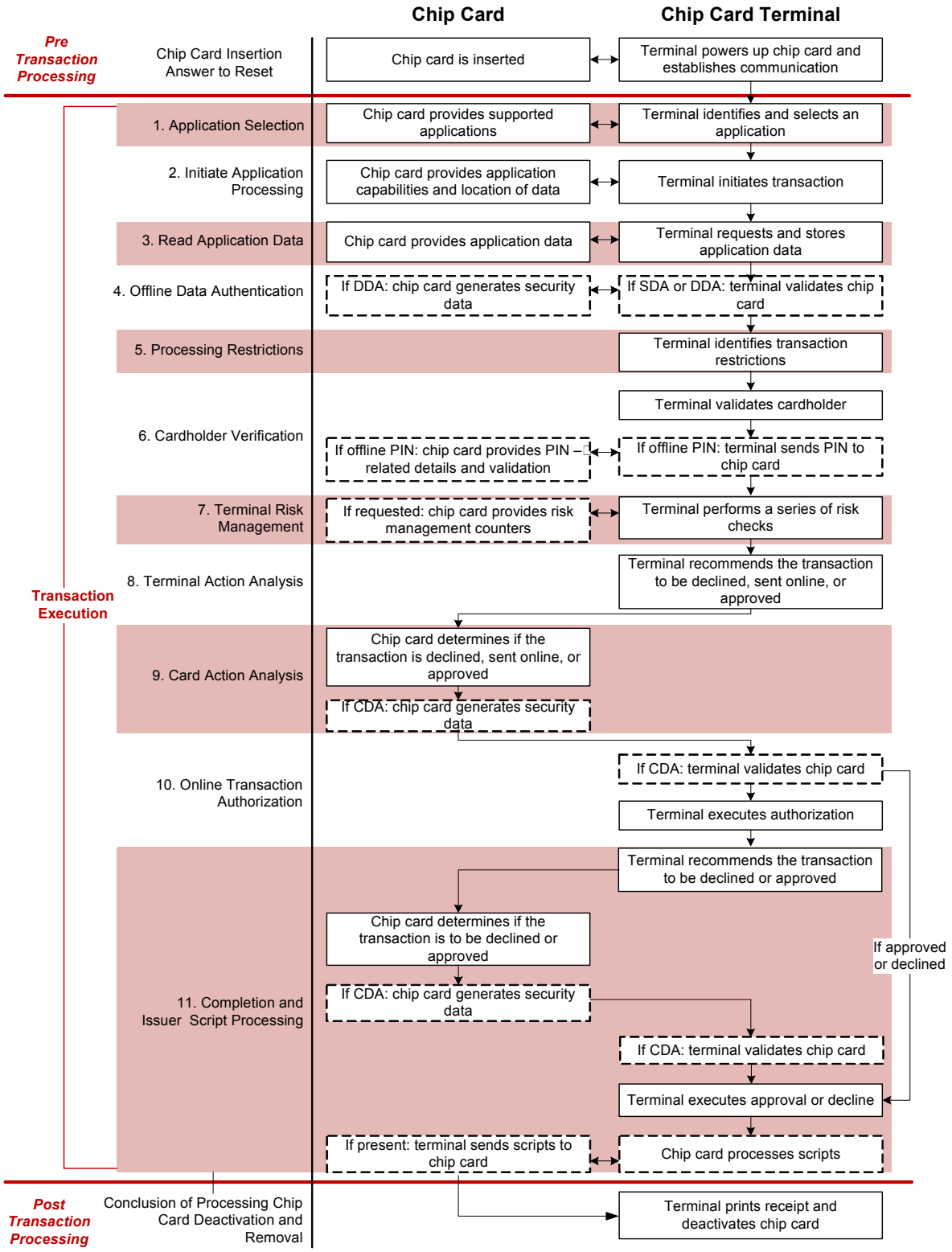

Figure 7-1 Contact Transaction Flow

7.3.1 Tender Processing

For EMV transactions, the transaction amount requiring authorization must be known prior to card entry and the Amount, Authorised (Tag 9F02) that is used for cryptogram generation must be set to this amount. This amount would include the base amount plus any of the following additional amounts:

Table 7-7 Tender Processing

Additional Amounts	Description
Cashback	If cashback is allowed and entered, Amount, Other (Tag 9F03) must be set to the cashback amount and this amount must be included in Amount, Authorised (Tag 9F02).
Surcharges	Any surcharges (e.g. taxes, fees, etc.) that are applied must be included in Amount, Authorised (Tag 9F02).
Tips	For pay-at-the-counter and pay-at-the-table environments, where the cardholder has access to the PIN pad, it is recommended that the tip amount be specified prior to card entry and be included in Amount, Authorised (Tag 9F02). The cardholder would be handed the PIN pad and they would enter their tip, confirm the total, insert/tap their card, enter their PIN if prompted, and wait for transaction completion before removing their card and handing back the PIN pad. For table service environments, the cardholder may still write in their tip later on the receipt and sign for authorization, in which case the Amount, Authorised (Tag 9F02) would not include the tip amount.

There are circumstances where the final amount requiring authorization may be adjusted after setting Amount, Authorised (Tag 9F02) and after the cryptogram has been generated, such as subtracting items from the sale amount that are not allowed for purchase with certain types of cards. In this case, it is acceptable that the final authorization amount specified elsewhere in the host messaging does not match the amount specified in Tag 9F02.

REQUIREMENT	The Amount, Authorised (Tag 9F02) must be set to the transaction amount known at the time of card acquisition and is used for cryptogram generation. This amount must not be changed even if the final amount submitted for authorization is different due to adjustments that may have been applied after cryptogram generation.

7.3.2 Card Acquisition

7.3.2.1 Card Swipe

Merchants have not been mandated to accept EMV cards nor have issuers been mandated to issue EMV cards, so the full migration to EMV may not be completed for several years or decades. Therefore, EMV chip cards will continue to have magnetic stripes into the foreseeable future so that they can continue to be used at magstripe only terminals.

If a card is swiped on an EMV terminal, the terminal software **must** parse the three-digit service code from the Track 1 or Track 2 data and examine the first digit. If the first digit of the service code is a **2** or a **6** indicating that the card is a chip card, the terminal must not normally allow the transaction to be processed using the magstripe data, but rather must prompt the merchant or customer to insert or tap the card instead.

An appropriate message such as "SWIPE NOT ALLOWED FOR CHIP CARD – INSERT CARD" should be displayed on the terminal.

REQUIREMENT	EMV solutions must continue to support magnetic stripe transactions, but must force chip usage if the service code in the Track 2 data is '2xx' or '6xx'.

7.3.2.2 Fallback Processing

When a chip card is presented, the card should normally be inserted or tapped and if swiped, the terminal should prompt to insert the card as described above. However, there are circumstances where the chip cannot be used and the magnetic stripe may be used instead. This is referred to as "fallback" and it is allowed in the following scenarios:

Table 7-8 Fallback Processing

Card Brand	Fallback Scenarios
Visa and Mastercard	Unable to read chip due to chip or chip reader failure. Empty candidate list due to no mutually supported AIDs.
Discover	Unable to read chip due to chip or chip reader failure.
AMEX	Unable to read chip due to chip or chip reader failure. Empty candidate list due to no mutually supported AIDs. **Note:** AMEX recommends allowing 3 attempts to read the chip before completing the transaction as fallback.

Note: If a chip cannot be read and a fallback magstripe authorization request is then sent, it must contain the same track data that was read to determine if the card was a chip.

Fallback is **not** allowed in the following scenarios:

- The transaction is declined by the card or the issuer.
- The fallback transaction cannot be online-authorized.
- The card is blocked.
- All applicable AIDs on the chip are blocked.
- The card is withdrawn before the transaction is completed.
- The transaction is canceled or times out before completion.

When waiting for a fallback card swipe:

- If an EMV card is inserted or tapped, fallback processing must be canceled, and the transaction must be processed as an EMV transaction.
- If the swiped card does not have a service code of '2xx' or '6xx', fallback processing must be canceled, and the transaction must be processed as a regular magstripe transaction with no fallback indicator.
- If the swiped card has a PAN that falls into a BIN/IIN range for Discover, Diners Club, JCB, or UnionPay, and it is a fallback scenario due to unknown AID, fallback processing must be canceled, and the transaction must be processed as a regular magstripe transaction with no fallback indicator.

REQUIREMENT	For fallback transactions, EMV solutions must set the appropriate fallback indicators in the authorization request message and must otherwise process the transaction as a standard magnetic stripe transaction.

7.3.3 Application Selection

EMV chip cards are capable of running multiple payment applications. For example, a single EMV card could be used to make payments from three different credit accounts, two different debit accounts, two different gift card accounts, and one loyalty account.

Application Identifiers (AIDs) are used to identify and select the application to use, and the terminal must be loaded with a list of supported AIDs. AIDs consist of three components:

Table 7-9 Application Selection

Component	Description
Registered Application Identifier (RID)	Each card brand has one or more RIDs **Example:** A000000003 is Visa's RID.
Proprietary Application Identifier Extension (PIX)	Each card brand has one or more PIXs to represent a particular payment application type. **Example:** 1010 is Visa's PIX for their global credit/debit application.
Issuer Suffix	Trailing digits that may be added by the issuer, and must be added if there are multiple applications on the card that share the same RID and PIX. **Example:** A000000003101001 for a Visa credit account. A000000003101002 for a Visa debit account on the same card.

The terminal selects the appropriate application to use for the current transaction as follows:

1. The terminal builds a candidate list of mutually supported applications using one of two methods:

Table 7-10 Supported Application Methods

Method	Description
Payment System Environment (PSE) Method	The terminal sends a SELECT command to the card requesting a file name of "1PAY.SYS.DDF01", and if the card supports PSE it will return a directory of supported applications.
List of AIDs Method	It is recommended that the terminal always try the PSE method first to increase transaction speed. If the card does not support PSE, the terminal sends a SELECT command to the card for each AID supported by the terminal to determine if the card also supports the AID.

2. If there is more than one mutually supported application in the candidate list, the terminal either automatically selects an application from the list based on predetermined preference or displays the list to the cardholder for selection. If displaying the candidate list:
   - Display the list in the order specified by the issuer in the Application Priority Indicator (Tag 87) if present, otherwise display in the order received from the card.
   - Display the Application Preferred Name (Tag 9F12) if present and if the Issuer Code Table Index (Tag 9F11) is present and supported by the terminal.
   - Display the Application Label (Tag 50) if present and the Application Preferred Name is not present or cannot be displayed.
   - Display a default application name assigned by the EMV POS Solution if the Application Preferred Name and Application Label are not present or cannot be displayed.
3. If the terminal automatically selects an application, or if there is only one mutually supported application in the candidate list, and the Application Priority Indicator (Tag 87) returned by the card indicates that use of the application must be confirmed, the terminal must prompt the cardholder for confirmation.
4. The terminal sends a final SELECT command to the card to indicate the selected application.
5. The card returns the Processing Options Data Object List (PDOL) for the selected application.

REQUIREMENT	Partial selection must be supported for all AIDs. This ensures that all supported applications are available for selection even if they contain an issuer assigned suffix at the end of the AID.

7.3.3.1 Available AIDs

The AIDs that may be available for selection on U.S.-issued cards include the following:

Table 7-11 Available AIDs

	Name	AID	Description
Global Credit/Debit	American Express	A00000002501	Used for global credit transactions routed to American Express on the credit rails.
	Discover/Diners	A0000001523010	Used for global credit and signature debit transactions routed to Discover on the credit rails.
	Discover Zip	A0000003241010	Used for global legacy contactless magnetic stripe mode credit transactions routed to Discover on the credit rails.
	JCB	A0000000651010	Used for global credit transactions routed to Discover on the credit rails.
	Mastercard	A0000000041010	Used for global credit and signature debit transactions routed to Mastercard on the credit rails.
	Visa	A0000000031010	Used for global credit and signature debit transactions routed to Visa on the credit rails.
	Visa Electron	A0000000032010	Used for global credit and signature debit transactions routed to Visa on the credit rails.
	UnionPay Credit	A000000333010102	Used for U.S., Mexico, Puerto Rico and The Bahamas credit and signature debit transactions routed to Discover on the credit rails.
	UnionPay Quasi Credit	A000000333010103	Used for U.S., Mexico, Puerto Rico and The Bahamas credit and signature debit transactions routed to Discover on the credit rails.
Global PIN Debit	Mastercard Maestro	A0000000043060	Used for global PIN debit transactions routed to Mastercard on the PIN debit rails.
	Visa Interlink	A0000000033010	Used for global PIN debit transactions routed to Visa on the PIN debit rails.
	UnionPay Debit	A000000333010101	Used for U.S., Mexico, Puerto Rico and The Bahamas PIN debit transactions routed to PULSE on the PIN debit rails. Can also be used for signature debit transactions routed to Discover on credit rails.

Table 7-11 Available AIDs (Continued)

	Name	AID	Description
U.S. Common Debit	Debit Network Alliance (DNA) Shared Debit	A0000006200620	Used for U.S. PIN debit transactions routed to any participating U.S. debit network on the PIN debit rails. **Note: Not supported at this time.**
	Discover U.S. Common Debit	A0000001524010	Used for U.S. PIN debit transactions routed to any participating U.S. debit network on the PIN debit rails. Can also be used for signature debit transactions routed to Discover on the credit rails.
	Mastercard U.S. Maestro	A0000000042203	Used for U.S. PIN debit transactions routed to any participating U.S. debit network on the PIN debit rails. Can also be used for signature debit transactions routed to Mastercard on the credit rails.
	Visa U.S. Common Debit	A0000000980840	Used for U.S. PIN debit transactions routed to any participating U.S. debit network on the PIN debit rails. Can also be used for signature debit transactions routed to Visa on the credit rails.
	UnionPay U.S. Common Debit	A000000333010108	Used for U.S. PIN debit transactions routed to any participating U.S. debit network on the PIN debit rails. Can also be used for signature debit transactions routed to Discover on the credit rails.

Note: The standard credit AIDs for Mastercard and Visa support their fleet, business, corporate, consumer cards, etc.

7.3.3.2 Debit AIDs

The presence of **both** of the following data elements identifies the AID as relating to a debit or prepaid program:

- ISSUER COUNTRY CODE (two digit alpha) (Tag 5F55) with a value **5553** ("US")
- ISSUER IDENTIFICATION NUMBER (IIN) (Tag 42)

If two or more AIDs have the same IIN, the terminal may assume they access the same underlying funding account and can eliminate all but one of the AIDs with the same IIN from the candidate list. Which AIDs are eliminated in this case should be configurable. For example, a merchant might specify their preference such that U.S. Common Debit AIDs will always remain in the candidate list if present.

If two or more AIDs with different IINs or no specified IINs still remain in the candidate list after eliminating AIDs with duplicate IINs, the EMV POS Solution must display the list to the cardholder for selection as described in the *7.3.3 Application Selection, p. 139*.

7.3.4 Initiate Application Processing

Once an application has been selected, the terminal begins processing an EMV transaction with the card as follows:

1. The terminal sets all the bits in the Transaction Status Information (TSI) and Terminal Verification Results (TVR) to **0**.
2. The terminal sends a GET PROCESSING OPTIONS command to the card to let it know that the processing of a new transaction is beginning and to provide the card with the terminal-related data requested by the card in the PDOL.
3. The card returns the Application Interchange Profile (AIP) and the Application File Locater (AFL).
   - The AIP specifies the functions supported by the card, such as offline data authentication, cardholder verification, issuer authentication, etc.
   - The AFL specifies the location of all the data that is relevant to the current transaction that should be read by the terminal.

7.3.5 Read Application Data

Once the application processing has begun and the terminal has received the AFL from the card, it sends READ RECORD commands to the card to retrieve all of the TLV data objects specified in the AFL.

If the following sensitive cardholder data is read from the card, it must **not** be included in authorization request messages sent to the host:

- 57 – Track 2 Equivalent Data
- 5A – Application PAN
- 5F20 – Cardholder Name
- 5F24 – Application Expiration Date
- 99 – Transaction PIN Data
- 9F0B – Cardholder Name Extended
- 9F1F – Track 1 Discretionary Data
- 9F20 – Track 2 Discretionary Data

REQUIREMENT	Sensitive cardholder data objects must not be sent to the host in authorization or settlement messages even if received from the card and terminal.

7.3.6 Offline Data Authentication

Once all of the application data has been read, if both the card and the terminal support Offline Data Authentication, the terminal authenticates the legitimacy of the card.

Based on the AIP received from the card and the capabilities of the terminal, the most secure mutually supported card authentication method is performed. The available methods from least to most secure are as follows:

Table 7-12 Offline Data Authentication

Authentication Method	Description
Static Data Authentication (SDA)	The terminal uses a PKI and public key cryptography to authenticate the digital signature of static data retrieved from the card.
Dynamic Data Authentication (DDA)	The terminal uses a PKI and public key cryptography to authenticate the digital signature of dynamic data retrieved from the card.
Combined DDA / Application Cryptogram Generation (CDA)	The terminal uses a PKI and public key cryptography to authenticate the digital signature of dynamic data retrieved from the card which includes the application cryptogram.

Bits in the Terminal Verification Results (TVR) are set based on the outcome of the Offline Data Authentication step.

7.3.7 Processing Restrictions

Once the card has been legitimized, the terminal determines the degree of compatibility with the card by performing the following checks:

Table 7-13 Processing Restrictions

Restriction	Description
Application Version Number	Is the version of the card application supported by terminal?
Application Usage Control	Is the card allowed for the transaction, e.g. is a domestic, international, or cashback transaction allowed?
Application Effective/Expiration Dates	Is the card application not yet effective or already expired?

Bits in the TVR are set based on the outcome of the Processing Restrictions step.

7.3.8 Cardholder Verification

Once the processing restrictions have been analyzed, the terminal processes the Cardholder Verification Method (CVM) list returned by the card and attempts to perform the first CVM in the list that is also supported by the terminal. The following CVMs are supported by EMV cards:

Table 7-14 Cardholder Verification

Verification Method	Description
Signature	This method prompts the cardholder to provide a signature that must match the signature on the back of the card.
Online Enciphered PIN	This method requires the cardholder to enter a PIN that is encrypted at the PIN entry device before being sent to Heartland (and subsequently out to the issuer) for validation.
Offline Enciphered PIN	This method requires the cardholder to enter a PIN that is encrypted at the PIN entry device before being sent to the chip card for validation.
Offline Enciphered PIN and Signature	This method requires the cardholder to enter a PIN that is encrypted at the PIN entry device before being sent to the chip card for validation, and that the cardholder provide a signature that must match the signature on the back of the card.
Offline Plaintext PIN	This method requires the cardholder to enter a PIN that is not encrypted before being sent to the chip card for validation.
Offline Plaintext PIN and Signature	This method requires the cardholder to enter a PIN that is not encrypted before being sent to the chip card for validation, and that the cardholder provide a signature that must match the signature on the back of the card.
No CVM Required	This method requires no checks to verify the cardholder.

Bits in the TVR are set based on the outcome of the Cardholder Verification step.

REQUIREMENT	The U.S. Common Debit AIDs support Online PIN and No CVM. If Online PIN is obtained, the transaction **must** be sent as a PIN debit transaction. If the CVM result is No CVM due to PIN bypass, the transaction **must** be sent as a credit (i.e. signature debit) transaction, and a signature must be obtained unless the transaction qualifies as a no signature required transaction.

7.3.8.1 PIN Support

From a security and fraud liability standpoint, it is typically in the best interest of the merchant and cardholder that PIN be prompted and entered if the card is a PIN-preferring card, but there are circumstances under which PIN entry may be avoided or skipped:

Table 7-15 PIN Support

PIN Support	Description
PIN Disablement	If PIN entry is not feasible because the merchant does not have a customer facing PIN pad, then all the PIN CVMs should be disabled on the terminal so that it does not prompt for PIN. In order to deploy this "No PIN" kernel configuration, it would need to have EMVCo Level 2 approval, and it would have to be certified with the card brands. If this functionality is supported, PIN entry is typically enabled/disabled via parameter setting.
PIN Entry Bypass	This is the EMVCo defined process where the terminal prompts for PIN, but at the direction of the merchant or cardholder the PIN is bypassed and not entered. In this case, the 'PIN entry required, PIN pad present, but PIN was not entered' bit in the TVR is set to 1, which the Issuer may consider when making its authorization decision. If this functionality is supported, PIN bypass is typically enabled/disabled via parameter setting. **Note:** Support of PIN bypass is a requirement for Visa debit cards only. It must be supported either through a credit/debit button, application selection, or by allowing the customer a method to bypass entry of the PIN.
PIN Prompt Bypass	This is typically used for small ticket VEPS/QPS transactions where no CVM is required. The terminal must have a selectable kernel where it can automatically switch to a "No CVM" configuration if the amount is under the limit. If this functionality is supported, the CVM required limit is typically specified per card brand or AID via parameter settings. PIN Prompt Bypass could also be invoked at the direction of the merchant or cardholder by pressing a "Credit" or "Signature" button on the terminal.

7.3.9 Terminal Risk Management

Once the cardholder has been verified, the terminal performs the following steps to protect the acquirer, issuer, and system from fraud:

Table 7-16 Terminal Risk Management

Risk Management	Description
Floor limit Checking	Transactions over the floor limit should be sent to host for online authorization.
Random transaction Selection	A certain percentage of transactions under the floor limit (which are normally eligible for offline authorization by terminal and card) should be randomly selected to go online.
Velocity Checking	After a certain number of consecutive offline transactions are performed using a particular card, the next transaction using that card should go online.

Bits in the TVR are set based on the outcome of the Terminal Risk Management step.

7.3.10 Terminal Action Analysis

Once the terminal has completed the previous 4 steps and has set the appropriate bits in the TVR accordingly, the terminal makes the initial decision as to the disposition of the transaction based on a bit-by-bit comparison of the TVR with the Terminal Action Codes (TACs) and Issuer Action Codes (IACs), and sends a GENERATE APPLICATION CRYPTOGRAM (AC) command to card accordingly:

Table 7-17 Terminal Action Analysis

Scenario	Terminal Action
For each bit in the TVR set to 1,	
If the corresponding bit in the IAC-Denial or TAC-Denial is set to 1,	It indicates that the issuer or acquirer wishes the transaction to be rejected offline without attempt to go online. The terminal requests an Application Authorization Cryptogram (AAC) in this case.
If the corresponding bit in the IAC-Online or TAC-Online is set to 1,	It indicates that the issuer or acquirer wishes the transaction to be completed online. The terminal requests an Authorization Request Cryptogram (ARQC) in this case.
If the corresponding bit in the IAC-Default or TAC-Default is set to 1,	It indicates that the issuer or acquirer wishes the transaction to be rejected offline if it might have been approved online but the terminal is for any reason unable to process the transaction online. The terminal requests an AAC in this case.
If there are no corresponding bits in the TVR set to 1,	The terminal may request an ARQC or Transaction Certificate (TC) depending on the other circumstances of the transaction.

7.3.11 Card Action Analysis

Once the terminal has made its initial decision, the card makes the final decision as to the disposition of the transaction based on the issuer's proprietary card risk management criteria and responds to the GENERATE AC command accordingly:

- Returns a TC to approve the transaction offline. This option is not available to the card if the terminal has made a preliminary decision to reject the transaction or complete it online.
- Returns an ARQC to complete the transaction online. This option is not available to the card if the terminal has made a preliminary decision to reject the transaction.
- Returns an AAC to reject the transaction.

Note: If the card returns a TC or AAC cryptogram, the transaction is complete and the remaining steps are not performed. If the card returns a TC to approve the transaction offline, the terminal must ensure that the offline approval is sent to the host for settlement.

7.3.12 Online Processing

Once the card has made its final decision, the terminal goes online for processing if the card returns an ARQC cryptogram in response to the first GENERATE AC command.

Online processing is performed to ensure that the issuer can review and authorize or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer.

In general, online processing of EMV transactions is the same as online processing of magstripe transactions except for the addition of the ARQC cryptogram and other chip card data sent in the request, and the Authorization Response Cryptogram (ARPC), issuer scripts, and other chip card data that may be received in the response.

7.3.12.1 Offline Authorization (Optional, Not Used in U.S.)

Note: Offline approvals are currently not used by any issuers in the U.S. Heartland will accept the transaction in the U.S. but it is an optional feature, not required.

If the card returns an ARQC to go online but the issuer cannot be reached, the merchant may elect to inform that card that it cannot go online and ask for an offline approval. This is typically accomplished by setting the Authorisation Response Code to **Y3**, although there may some other way to indicate this desire based on your terminal's specific API/SDK. The terminal will perform the Completion step below.

If the card returns a TC cryptogram, the transaction is offline approved and the terminal must ensure that the offline approval is sent to the host for settlement. No additional store-and-forward or stand-in processing is required. If the card returns an AAC cryptogram, the transaction is not offline approved and the merchant may elect to proceed with the store-and forward or stand-in processing as described in the following sections.

7.3.12.2 Deferred Authorization (Store-and-Forward)

If the card returns an ARQC to go online but the issuer cannot be reached, the merchant may elect to store the transaction and submit it later for authorization. The merchant does so at their own risk as the transaction may be later declined, ask your merchants if they want to support this functionality.

It is recommended that the Offline Authorization step above be performed first to see if the card will approve offline. However, if the merchant does not support offline authorizations or if the card returns an AAC cryptogram indicating that it is unwilling to approve offline, the following store-and-forward process may be followed:

1. The terminal stores the transaction details including the original ARQC cryptogram and associated chip data.
2. Later, the terminal uploads its batch of authorization requests that include the ARQCs.
3. The acquirer submits the authorization requests, most of which are approved online.
4. Repeated attempts at authorization for declined transactions are permitted, but declined transactions must eventually be discarded.
5. The acquirer submits a clearing record for each approved transaction, using the ARQC for online approved transactions and the Authorisation Response Code returned in the authorization response.

7.3.12.3 Forced Acceptance (Stand-In)

If the card returns an ARQC to go online but the issuer cannot be reached, the merchant may elect to stand-in for the transaction and submit it for settlement. The merchant does so at their own risk as the transaction may not clear or may incur a chargeback due to no authorization, ask your merchants if they want to support this functionality.

It is recommended that the Offline Authorization step above be performed first to see if the card will approve offline. However, if the merchant does not support offline authorizations or if the card returns an AAC cryptogram indicating that it is unwilling to approve offline, the following stand-in process may be followed:

1. Check if the transaction amount is below the Stand-in Floor Limit for this card type. Proceed if the transaction amount is below the Stand-in Floor Limit; otherwise, do not stand-in.
2. Check if the card is domestic (i.e., U.S.-issued). This can be determined by ensuring that the Issuer Country Code (Tag 5F28) = **840**. International cards pose a higher risk and should not be approved via stand-in authorization. Proceed if card is domestic; otherwise, do not stand-in.
3. Apply the TVR Mask to the transaction's Terminal Verification Results (Tag 95) value. If any of the bits in the TVR match the corresponding bits in the TVR Mask, then a condition exists that indicates the transaction should not be approved via stand-in authorization. The recommended TVR Mask is "FC 50 FC 20 00" which means that if any of the following conditions exists, the transaction should not be approved via stand-in authorization:

Table 7-18 Terminal Verification Results

Byte	Bit	Value
1	8	Offline data authentication not performed
1	7	Offline SDA failed
1	6	ICC data missing
1	5	Card appears on terminal exception file
1	4	Offline DDA failed
1	3	Offline CDA failed
2	7	Expired applications
2	5	Requested service not allowed for card product
3	8	Cardholder verification was not successful
3	7	Unrecognized CVM
3	6	Offline PIN Try Limit exceeded
3	5	PIN entry required, PIN pad not present or not working

Table 7-18 Terminal Verification Results (Continued)

Byte	Bit	Value
3	4	Offline PIN required, PIN pad present, but PIN not entered
3	3	Online PIN entered
4	6	Upper consecutive offline limit exceeded

Proceed if a bitwise AND of the TVR and TVR Mask bits are all zero; otherwise, do not approve the transaction.

4. Use the TSI Mask and the transaction's Transaction Status Indicator (Tag 9B) value to check that the required EMV transaction steps were performed. If any of the bits in the TSI are zero in the corresponding bits of the TSI Mask, then a required EMV transaction step was not performed. The recommended TSI Mask is "E8 00" which means that the following transaction steps were performed:

Table 7-19 Transaction Status Indicator

Byte	Bit	Value
1	8	Offline data authentication was performed
1	7	Cardholder verification was performed
1	6	Card risk management was performed
1	4	Terminal risk management was performed

Proceed if a bitwise AND of the TSI and TSI Mask equals the TSI Mask; otherwise, do not approve the transaction.

5. If all of the above steps pass, approve the transaction and submit it for settlement; otherwise, decline the transaction and/or proceed with Voice Authorization.

7.3.13 Issuer Authentication

The authorization response message from the issuer may contain Issuer Authentication Data (Tag 91), which contains the ARPC.

If the Issuer Authentication Data is received in the authorization response message and the AIP indicates that card supports issuer authentication, the Issuer Authentication Data is sent to card in the EXTERNAL AUTHENTICATE command.

Bits in the TVR are set based on outcome of issuer authentication.

7.3.14 Issuer-to-Card Script Processing

The issuer may provide command scripts to be delivered to the card by the terminal to perform functions that are not necessarily relevant to the current transaction but are important for continued functioning of the card application.

Multiple scripts may be provided with an authorization response and each may contain any number of Issuer Script Commands.

Two separate script tags are available for use by the issuer.

- Issuer scripts with Tag 71 are processed prior to issuing the final GENERATE AC command.
- Issuer scripts with Tag 72 are processed after issuing the final GENERATE AC command.

Bits in the TVR are set based on outcome of issuer-to-card script processing and Issuer Script Results are made available for sending for reversals or settlement.

REQUIREMENT	If issuer scripts are received in the host response, they must be processed whether the transaction was approved or declined.

7.3.15 Completion

Whether the terminal receives an authorization response message as a result of online processing or whether it receives an approval or rejection for a transaction that was unable to go online based on TAC/IAC-Default, it completes the transaction by requesting either a TC (if an approval was obtained), or an AAC (if the issuer's instruction is to reject the transaction) from the card by a second GENERATE AC command.

The Authorisation Response Code (Tag 8A) should be set by the terminal based on the following requirements:

For American Express:

- If Issuer Authentication Data (Tag 91) is received in the authorization response message, the terminal **must** set Tag 8A to the exact value of the last two bytes of Tag 91, even if that value is not included in *Table 7-20*.
- If Tag 91 is not received in the authorization response message, the terminal must set Tag 8A to the appropriate value in *Table 7-20*.

For all other card brands:

- The terminal must set Tag 8A to the appropriate value in Table 7-20 below, without regard to Tag 91.

Table 7-20 Online or Offline Disposition

Disposition	ASCII	Hex	Notes
Online approved	"00"	'3030'	Should be sent to card at 2nd GENERATE AC if the host response code indicates any approval, including partial approvals or card verifications.
Online declined	"05"	'3035'	Should be sent to card at 2nd GENERATE AC if the host response code indicates any decline, i.e. anything that is not an approval. Also used if a partial approval from the host is rejected at the terminal.
Offline approved	"Y1"	'5931'	Should be sent to host in offline approval advice if the card approves offline at 1st GENERATE AC before attempt to go online.
Offline declined	"Z1"	'5A31'	Should be sent to host in offline decline advice if card declines offline at 1st GENERATE AC before attempt to go online, or at 2nd GENERATE AC due to bad ARPC cryptogram.
Unable to go online, offline approved	"Y3"	'5933'	Should be sent to card at 2nd GENERATE AC to request offline approval after failed attempt to go online. Should be sent to host in offline approval advice if the card approves offline at 2nd GENERATE AC.
Unable to go online, offline declined	"Z3"	'5A33'	Should be sent to host in offline decline advice if the card declines offline at 2nd GENERATE AC after failed attempt to go online and the transaction is not eligible for store-and-forward or stand-in processing.

The card will respond to the 2nd GENERATE AC command as follows:

- If a TC was requested, the card returns either a TC or an AAC.
- If an AAC was requested, the card returns an AAC.

REQUIREMENT	The Authorisation Response Code (Tag 8A) is not returned by the issuer or card brands, and thus is not included in the authorization response message from the host. The terminal must set Tag 8A based on the disposition of the transaction, whether online or offline.

7.3.16 Card Removal

When the transaction flow is complete, the cardholder should be prompted to remove their card before receipts are printed. It is recommended that the terminal also beep at regular intervals until the card is removed as an audible reminder to the cardholder to remove their card.

REQUIREMENT	If the card is removed prematurely before transaction flow completion, the transaction must be canceled, and if the transaction was approved online a reversal must be sent.

7.4 Contactless Transaction Flow

The major difference between EMV contactless transactions and EMV contact transactions is transaction speed. The information transmitted between the chip card and POS terminal is done in a more succinct manner and many of the transaction flow steps are performed either before or after the card leaves the proximity of the reader. See *Figure 7-2*.

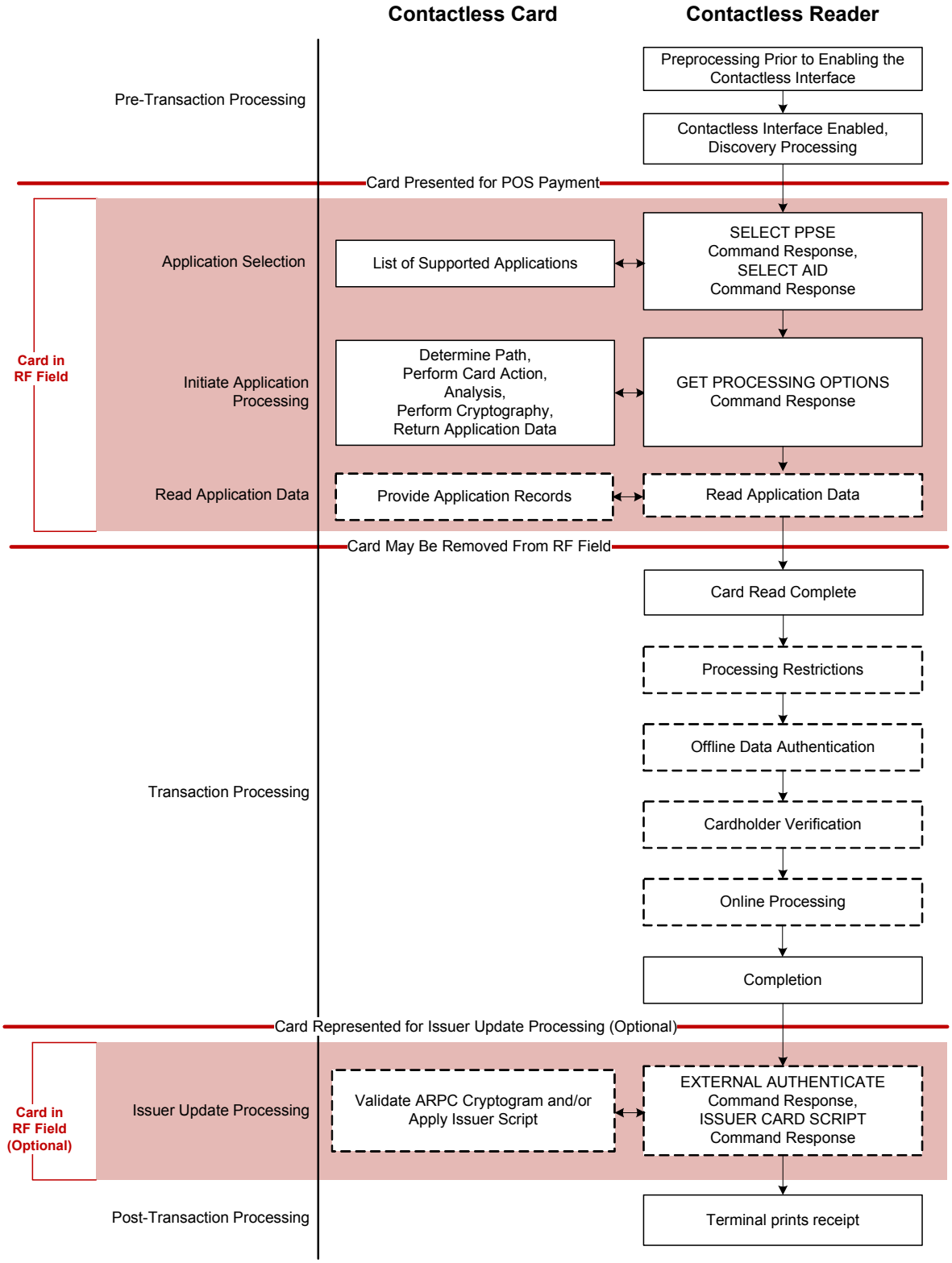

Figure 7-2 Contactless Transaction Flow

The focus of the following sections is to highlight some of the specific differences from the contact EMV flow. A summary of the differences is as follows:

Table 7-21 Contact EMV Flow Differences

Step Name	Description
Application Selection	The highest priority mutually supported application is automatically selected by the contactless card reader.
Initiate Application Processing	This step includes the Terminal Risk Management, Terminal Action Analysis, and Card Action Analysis processing.
Read Application Data	The chip card may be removed from the proximity of the reader after this step.
Cardholder Verification	The offline enciphered/plaintext PIN CVMs are not supported for contactless transactions.
Issuer Update Processing	This is an optional step that encompasses the Issuer Authentication and Issuer-to-Card Script processing, and would require re-presentment of the card into the proximity of the reader. This is currently not supported.

7.4.1 Pre-Processing

To minimize the duration in which the card must remain within the reader's radio frequency (RF) field, the reader may obtain the transaction amount and perform some risk management checks prior to prompting for card presentment. This pre-processing is performed prior to powering on the contactless interface.

7.4.2 Discovery Processing

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

7.4.3 Application Selection

Similar to contact EMV, but the terminal builds a candidate list of mutually supported applications using the mandatory Proximity Payment System Environment (PPSE) method, whereby the terminal sends a SELECT command to the card and the card returns a directory of supported applications. The List of AIDs method is not used for contactless.

If there is more than one mutually supported application in the candidate list, the terminal automatically selects an application from the list based on predetermined preference, which may be to choose the application of highest priority according the Application Priority Indicator (Tag 87) returned by the card.

7.4.4 Initiate Application Processing

This step includes:

- *Path Determination*
- *Terminal Risk Management*
- *Terminal Action Analysis*
- *Card Action Analysis*

7.4.4.1 Path Determination

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

7.4.4.2 Terminal Risk Management

Similar to contact EMV, but only floor limit checking is performed for contactless transactions. Random transaction selection and velocity checking is not performed for contactless transactions.

7.4.4.3 Terminal Action Analysis

Same as contact EMV, except that the TACs and IACs may be different for contactless.

7.4.4.4 Card Action Analysis

Same as contact EMV.

7.4.5 Read Application Data

Same as contact EMV.

7.4.6 Card Read Complete

The card may be removed from the reader's RF field at this point. The reader determines whether all mandatory data elements for the transaction were returned by the card, and terminates the transaction if they were not.

All of the remaining steps are performed after the card has left the proximity of the reader.

7.4.7 Processing Restrictions

Same as contact EMV.

7.4.8 Offline Data Authentication

Similar to contact EMV, but with some variances. For example, Visa uses Fast Dynamic Data Authentication (fDDA) and Mastercard does not support SDA or DDA for contactless.

7.4.9 Cardholder Verification

Similar to the CVMs supported for contact EMV cards, with the exception that offline PIN is not supported. Contactless transactions may also occur with a new CVM that indicates the cardholder was validated by the mobile device (for instance, fingerprint scan or password that is required to unlock a phone).

Each card brand has a different term for this new CVM:

Table 7-22 Card Verification

Card Brand	Description
Visa	Consumer Device CVM
Mastercard	Consumer Device CVM (CDCVM)
American Express	Mobile CVM
Discover	Confirmation Code (Mobile) CVM

7.4.10 Online Processing

Same as contact EMV.

7.4.11 Completion

Similar to contact EMV, except that there is no request for a TC or AAC after online processing since the card has already been removed from the proximity of the reader.

7.4.12 Issuer Update Processing

This optional step to validate the ARPC cryptogram and apply issuer scripts to the card would require re-presentment of the card into the proximity of the reader and is not currently supported by most cards or readers.

7.5 EMV Receipts

7.5.1 Approval Receipts

In addition to the magstripe receipt requirements, the following additional items must be included on EMV receipts:

Table 7-23 Receipt Requirements

Receipt Item	Description
APPLICATION NAME	Use Application Preferred Name (Tag 9F12) if available and printer supports the corresponding character set as specified in Issuer Code Table Index (Tag 9F11), else use Application Label (Tag 50).
APPLICATION IDENTIFIER (AID)	Use Tag 4F if available, else Tag 84 if available, else Tag 9F06.
APPLICATION CRYPTOGRAM TYPE	Use "ARQC", "TC", or "AAC" based on the final cryptogram generated for the transaction.
APPLICATION CRYPTOGRAM	Contents of Tag 9F26 for the final cryptogram generated for the transaction.
CARDHOLDER VERIFICATION METHOD (CVM)	Based on the CVM Results (Tag 9F34), either print a signature line, "PIN VERIFIED", and/or "NO SIGNATURE REQUIRED". If the CVM Results indicate a failure, or "No CVM Required" when that was not the expected result, a signature line should be printed.
CARD ENTRY METHOD	Use "INSERT", "TAP", "SWIPE", "MANUAL", or equivalent text based on the source of the card data.

Figure 7-3 EMV Receipt Example

7.5.2 Decline Receipts

There are no card brand requirements to print decline receipts and no requirements for EMV information that should be included on such receipts. Heartland has an Offline Decline Advice message for capturing EMV decline data, so a detailed decline receipt is unnecessary.

If you choose to print decline receipts, then, in addition to the information required on approval receipts, it is recommended that the following tags be printed if available:

- TERMINAL VERIFICATION RESULTS (Tag 95)
- CVM RESULTS (Tag 9F34)
- ISSUER ACTION CODE (IAC) – DENIAL (Tag 9F0E)
- ISSUER APPLICATION DATA (Tag 9F10)

Chapter 8: EMV Parameter Interface

8.1 Introduction

A table-driven EMV Parameter Data Load (EMV PDL) is available and required for all terminals processing EMV transactions. These tables consist of various terminal capabilities, supported applications and keys used for processing EMV. The Heartland network will maintain five Tables of EMV PDL information:

Table 8-1 EMV PDL Tables

Table-ID	Description
Table-ID 10	EMV Table-ID Versions and Flags for Data Tables
Table-ID 30	Terminal Data
Table-ID 40	Contact Card Data
Table-ID 50	Contactless Card Data
Table-ID 60	Public Key Data

The network will relay to the POS which table data it needs to download by sending Table Versions and Flags to it in Table-ID 10.

Note: A Table Version of ### and Flag of @ indicate that the table is not applicable to the POS terminal and that the table must not be requested by the POS terminal.

The EMV PDL system was designed to maintain a specific set of data for each EMV card acceptance device based on the particular certified configuration of that device being utilized by the merchant. The data set is linked to the following identifiers:

Table 8-2 Platform Identifiers to EMV PDL System

Platform	Merchant/Company ID	Location/Unit ID	Terminal/Device ID
Exchange/Portico	12-digit Merchant ID Number	N/A	4-digit Terminal Number
NWS	4-char Company ID	15-char Terminal Location ID	4-char Unique Device ID
POS 8583	DE 41	DE 42	DE 62~IID
VAPS	4-digit Company Number	11-digit Unit Number	2-digit Terminal ID

In practice, a merchant location could have multiple devices that are the same and are using the same certified configuration, so it is not necessary to request an EMV PDL for each of these devices.

For example, a site may be able to set up one PDL for the inside terminals and one PDL for the outside terminals and the POS controller/aggregator could pull those two PDLs from the host and subsequently push the data out to all the devices as appropriate.

Different pumps, different card readers, different kernels, etc. do not necessarily require multiple configurations. Multiple configurations are only needed if there are differences in any of the following:

- Terminal Type
- Terminal Capabilities
- Merchant Category Code
- Accepted Transaction Types (Credit and/or Debit)
- Accepted Card Types (Visa, Mastercard, AMEX, and/or Discover)
- Supported Interfaces (Contact and/or Contactless)

The approach for sending EMV PDLs to each device or groups of devices must be managed by the customer working with Heartland.

The POS can optionally override the value received in the EMV PDL for the following parameters:

- EMV PDL TERMINAL FLOOR LIMIT: This is the maximum value allowed by the card brand for the AID. The POS may use any amount that is less than or equal to this value, including $0 if the POS does not support offline authorizations or if the merchant does not want to support offline authorizations.
- EMV PDL THRESHOLD VALUE FOR BIASED RANDOM SELECTION: This is the minimum value allowed by the card brand for the AID. The POS may use any amount that is greater than or equal to this value.
- EMV PDL TARGET PERCENTAGE TO BE USED FOR RANDOM SELECTION: This is the minimum value allowed by the card brand for the AID. The POS may use any percentage that is greater than or equal to this value.
- EMV PDL MAXIMUM TARGET PERCENTAGE TO BE USED FOR BIASED RANDOM SELECTION: This is the minimum value allowed by the card brand for the AID. The POS may use any percentage that is greater than or equal to this value.
- EMV PDL TERMINAL CONTACTLESS FLOOR LIMIT: This is the maximum value allowed by the card brand for the AID. The POS may use any amount that is less than or equal to this value, including $0 if the POS does not support offline authorizations or if the merchant does not want to support offline authorizations. It is recommended that a $0 floor limit is used for contactless transactions.
- EMV PDL TERMINAL CVM REQUIRED LIMIT: This is the maximum value allowed by the card brand for the AID. The POS may use any amount that is less than or equal to this value, including $0 if the merchant does not support No CVM processing for low value transactions.

- EMV PDL TERMINAL CONTACTLESS TRANSACTION LIMIT: This is the minimum value allowed by the card brand for the AID. The POS may use any amount that is greater than or equal to this value.

If the POS receives parameters which are not applicable to the merchant or at the particular merchant location, the POS should ignore those parameters and not load them to the EMV terminal. For example:

- If parameters are received for AMEX, but the location does not accept AMEX cards, those parameters should be ignored.
- If parameters are received for PIN debit, but the location does not accept PIN debit at all, or does not accept EMV PIN debit specifically, those parameters should be ignored.
- If parameters are received for contactless, but the location does not support contactless at all, or does not accept EMV contactless specifically, those parameters should be ignored.

8.2 Exchange

EMV Parameter Download Notification is indicated when Group III Version 090 contains a value of **Y**. After the EMV Parameter Download Notification is received by the POS Terminal, an EMV Parameter Download request should be sent after the current batch is closed. The EMV Parameter Download Notification Request (Transaction Code = EP) with Group III Version 091 containing the following values:

- PDL-EMV Parameter Type = 06
- PDL-EMV Table ID field = 10
- PDL-EMV Card Type = space-filled
- PDL-EMV Parameter Version = 001
- PDL-EMV Block Sequence Number = 00

The response for Table-ID 10 will contain the latest version number and the download flag for Table-ID 30, 40, 50 and 60.

8.3 POS 8583

The EMV Parameter Download Notification is sent in a response message in DE 48.12 (Administratively Directed Task) with a value of **3**. After the EMV Parameter Download Notification is received by the POS Terminal, an EMV Parameter Download request should be sent after the current batch is closed. The EMV Parameter Download Request (MTI = 1300, DE 24 = 304, DE 25 = 3718, DE 72.1 = EPDL) including the following values:

- PDL-EMV Parameter Type = 06
- PDL-EMV Table ID field = 10
- PDL-EMV Card Type = space-filled
- PDL-EMV Parameter Version = 001
- PDL-EMV Block Sequence Number = 00

The response for Table-ID 10 will contain the latest version number and the download flag for Table-ID 30, 40, 50 and 60.

8.4 NTS

- Terminal will receive notification of a pending EMV PDL via a value of **3** in the PENDING REQUEST INDICATOR field of a Host authorization response.
- Terminal must send a MESSAGE CODE **21**, with an EMV PDL PARAMETER TYPE of **06** to request EMV download information.
- Terminal must send a MESSAGE CODE **21**, with an EMV PDL PARAMETER TYPE of **07** to confirm receipt of each complete EMV table.

8.5 Z01

- Terminal will receive notification of a pending EMV PDL via a value of **E** in the MULTIPLE INQUIRY FLAG of a Host authorization response (**Z01 06** and **Z01 14** response maps only).
- Terminal must send an EMV PDL Request format with RESPONSE FORMAT CODE of **E1**, REQUEST FORMAT CODE of **E1**, TRANSACTION TYPE **80** and EMV PDL PARAMETER TYPE of **06** to request EMV download information.
- Terminal must send an EMV PDL Request format with RESPONSE FORMAT CODE of **E1**, REQUEST FORMAT CODE of **E1**, TRANSACTION TYPE **80** and EMV PDL PARAMETER TYPE of **07** to confirm receipt of each complete EMV table.

8.6 Portico

EMV Parameter Download Notification is indicated in the response Header of the following Portico Transaction Services. The notification will be included in the response Header once per day until the download is confirmed or the download flag is reset in the parameter download system.

- CreditAdditionalAuth
- CreditAccountVerify
- CreditIncrementalAuth
- DebitSale
- CreditAuth
- CreditSale

Parameter Downloads may be retrieved and confirmed through the Portico "ParameterDownload" service. See the Portico SDK for additional information.

8.7 SpiDr

A POS terminal performs an EMV Parameter Data Load after receiving notification, DE 48~12 Administratively Directed Task, in a response message.

The EMV Parameter Data Load request is sent after a batch close in a file download request message (MTI = 1300, DE 24 = 304, DE 25 = 3718) with the following values:

- PDL-EMV Parameter Type = 06
- PDL-EMV Table ID field = 10
- PDL-EMV Card Type = space-filled
- PDL-EMV Parameter Version = space-filled
- PDL-EMV Block Sequence Number = 00

The response for table 10 will contain the latest version number and the download flag for tables 30, 40, 50 and 60.

- A PDL-EMV Table ID Flag value of **Y** will direct the POS to request the data for that table in a subsequent PDL request.
- A PDL-EMV Table ID Flag value of **N** indicates that the table is utilized by the POS terminal, but there is no new data to download at this time.

The POS terminal sends a request for each Table-ID with a Flag value of **Y** using the indicated PDL-EMV Table Version and PDL-EMV Card Type values.

Some of the tables must be downloaded in multiple blocks, and the POS must keep track of the Block Sequence Number it needs and increment it appropriately until all blocks are successfully received. When the POS receives a PDL-EMV End-Of-Table Flag of **Y**, it sends a PDL-EMV Parameter Type of **07** to confirm receipt of that table.

Use the SpiDr transaction type PDL.

Chapter 9: EMV Quick Chip Processing Overview

9.1 Introduction

This chapter introduces modifications to the EMV standard process for contact and contactless chip transactions. All other standard EMV processing in *Chapter 5: EMV Processing Overview*, *Chapter 6: EMV Development Overview*, *Chapter 7: EMV Terminal Interface*, *Chapter 8: EMV Parameter Interface* applies and should be used in conjunction with this chapter.

The requirements in this chapter are valid for all of the accelerated methods of processing EMV transactions listed below:

- Visa Quick Chip
- Mastercard M/Chip Fast
- Discover Quick Chip
- American Express Quick Chip

All of these methods will be referred to collectively in this specification as 'quick chip processing'.

9.2 Quick Chip Processing Definition

Quick chip processing allows for early removal of the chip card from the terminal, while still relying on standard EMV processing between the card and terminal. The need for EMV processing to wait for the final transaction amount, authorization response, and post-authorization processing (such as script processing and issuer authentication) is eliminated. When the card generates an online cryptogram response, it is transmitted to the terminal as usual. The chip card is then notified that card removal can occur, with appropriate prompts.

Features and benefits of this processing include the following:

- Reduces the amount of time the card is inserted in terminal as part of critical processing path, by eliminating dependencies.
- EMV level of security for online authorizations, including the cryptogram, remains the same as standard EMV.
- The cardholder experience is improved by reducing wait time on card removal. The risk of cards being left in the terminal is reduced.
- Integrates with both Global and U.S. Common Debit AID processing.
- All cardholder verification methods are supported.

9.3 Impact to Existing EMV Kernel and Host Software

Quick chip processing has no impact on the EMV kernel or the EMVCo Level 2 approval of the kernel. The timing of when the payment application invokes EMV processing may change, but all necessary EMV processes will be performed. Quick chip is a modification to the payment application around the EMV kernel that reduces the time the card remains in the terminal by allowing a contact chip transaction to mimic much of what takes place today on contactless chip transactions.

Note: Quick chip has no impact to host network messaging and there are no host changes to be implemented.

9.4 Comparison of Standard EMV and Quick Chip Processes

Table 9-1 Comparison of Standard EMV and Quick Chip Processes

Chip Processing Steps	Standard EMV	QuickChip
Application Selection	✓	✓
Initiate Application Processing	✓	✓
Read Application Data	✓	✓
Offline Data Authentication	✓	✓
Processing Restrictions	✓	✓
Cardholder Verification	✓	✓
Terminal Risk Management	✓	✓
Terminal Action Analysis	✓	✓
Card Action Analysis	✓	✓
Online Authorization	✓	✓
Completion	✓	✓
Post-Authorization Card Processing	✓	

With standard EMV processing the following factors can make the transactions slower than magnetic stripe transactions and increase the perception to the cardholder that the transaction is slow:

- The chip terminal waits for the final amount before completing cardholder verification method processing and requesting data for online authorization from the card.
- The card remains in the reader until the authorization response is received.

These factors are eliminated with quick chip processing.

9.5 Online Processing Overview

Quick chip transactions **must** be authorized online. This allows the card to be removed before the online response is returned, while the merchant uses the issuer's online response to determine whether the transaction is approved or declined. The cardholder can insert the card at any time during the check-out process, just like a magnetic stripe.

Note: Offline decline advice messages would only be generated for Quick Chip processing for 1st GEN AC declines. This advice is needed to research why the card is offline declining the transaction.

Offline decline advice messages would not be applicable at 2nd GEN AC after host communications error due to an invalid ARPC cryptogram. At this point the card is not in the reader.

The online processing steps are:

Table 9-2 Online Processing

	Process
1.	The terminal may activate the reader as soon as the scanning of goods starts. If the final amount is not known yet, the terminal includes a pre-determined amount in the activation request. The pre-determined amount is a non-zero amount. The merchant may select any non-zero value but $1 is not recommended. **Note:** Due to common use of $1 as the amount for petroleum pre-authorizations, Heartland does not recommend the use of $1 as the estimated amount for quick chip implementations. A non $1 amount will allow simpler identification of quick chip enabled terminals.
2.	Depending on the acceptance environment, the terminal may be configured to select a pre-determined amount that does not exceed the Cardholder Verification Method (CVM) limit (if the terminal is configured to perform No CVM processing and to submit the transaction without PIN or signature).
3.	The cardholder is invited to insert their card. The pre-determined amount of the transaction is not shown to the cardholder.
4.	Application selection, transaction initiation and reading of the card data is performed as per traditional EMV (through the Select, Get Processing Options and Read Record commands). Faster EMV supports standard application selection processes, whether Cardholder Selection, Application Priority Selection, or customized application selection.
5.	If supported by the card and the terminal, offline data authentication is performed as per traditional EMV. (This may involve additional commands, such as Internal Authenticate.)

Table 9-2 Online Processing (Continued)

	Process
6.	If the transaction amount exceeds the CVM limit and if PIN is the selected CVM, the cardholder is invited to enter the PIN. a) If offline PIN is the selected CVM, the cardholder is informed of the result (through the Verify PIN command and potentially the Get Challenge command for encrypted offline PIN). b) If online PIN is the selected CVM, the PIN is encrypted into a PIN block. c) If signature is the selected CVM, it is not captured at this point but at the end of the transaction following receipt of the issuer approval.
7.	The reader requests an online cryptogram (ARQC) from the card.
8.	Unless the transaction is terminated when the online cryptogram is requested (i.e., AAC returned), the reader receives an ARQC from the card and returns the ARQC together with the other chip data to the terminal.
9.	The terminal stores the ARQC and the associated chip data for the later authorization request.
10.	The reader completes EMV processing by sending a second Generate AC command with an Authorization Response Code 'Unable to go online, offline declined' (value 'Z3') to request an AAC, and upon receipt of the card's response, informs the terminal that the EMV processing is completed. (In this scenario, requesting a "decline" cryptogram is used only to complete EMV processing, and does not determine transaction disposition. Disposition is determined by the issuer response.) The cardholder is prompted to remove their card.
11.	When the final transaction amount is known, the terminal sends an authorization request to the issuer with: • the final amount in the host specific transaction amount field, • the ARQC and chip data in EMV data field, and • if applicable, the online PIN block. The transaction amount in EMV data field (with Tag 9F02) is the amount used to generate the ARQC. In this example, the pre-determined amount. The authorization request amount (host specific transaction amount field) may vary from the cryptogram amount (EMV data field Tag 9F02).
12.	The payment process is completed according to the issuer response (approve or decline) and the cardholder is informed of the outcome. If the transaction is approved and signature was the chosen CVM, the signature can be captured on a sales receipt or signature capture device. If chip data is received in the authorization response, the terminal should ignore the data.

9.6 Quick Chip Processing Flow

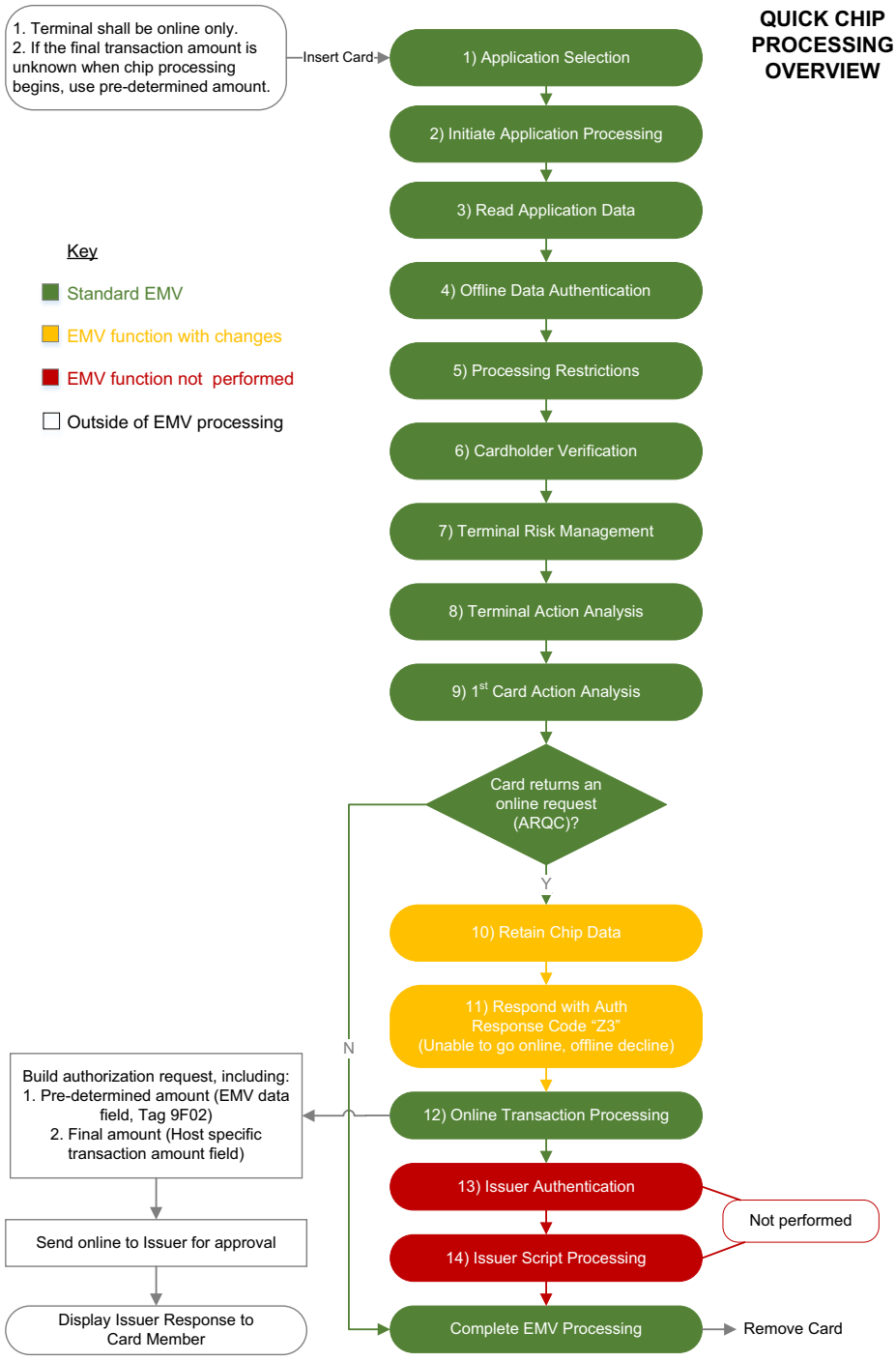

Figure 9-1 Quick Chip Processing Flow

9.7 Floor Limit

A $0 dollar floor limit must be used for quick chip processing for all AIDs. This in combination with the TAC-Online Transaction Exceeds Floor Limit (Byte 4, bit 8) = 1 will result in the EMV kernel requesting an Authorization Request Cryptogram (ARQC) from the chip card.

Note: If a non-$0 dollar floor limit is received in the EMV PDL for any AIDs, it must be overridden by the POS with a $0 dollar floor limit for quick chip processing.

9.8 Amounts – Final or Pre-Determined

The payment application does not need to wait for the final amount to be known before the EMV processing can take place between the card and terminal. Send either the final amount (if known), or a pre-determined amount to the EMV kernel.

- If the final amount of the transaction is known, send it to the EMV kernel in Tag 9F02 (Amount, Authorised).
- If the final amount is not known, a merchant may select a pre-determined amount above $0 dollars to use for quick chip processing. Using a $0 dollar amount is not valid.

9.9 Cashback Processing

Cashback functionality is the same as it is for standard EMV transactions.

Note: The terminal may wait until the Application Usage Control (AUC) has been read from the card to check whether cashback is allowed by the issuer before offering cashback as an option to the cardholder. If the cardholder has already indicated they want to sign for a debit transaction (by choosing "credit" instead of "debit"), they should not be offered cashback.

The terminal can prompt for Online PIN when needed (for a cashback transaction), even if the CVM List processing does not result in the Online PIN being requested as a CVM. In order to ensure the PIN-related indicators are set correctly in the Terminal Verification Results (TVR) before cryptogram generation, the prompt for Online PIN entry must be performed before completion of the Cardholder Verification phase of the transaction.

If cashback is offered, the cashback amount must be requested from the cardholder prior to requesting the first Application Cryptogram from the card. The cashback amount is sent to the EMV kernel in Tag 9F03 (Amount, Other) and is included in the amount sent to the EMV kernel in Tag 9F02 (Amount, Authorised).

- If the final amount of the transaction is known, send it (including the cashback amount) in the EMV kernel in Tag 9F02 (Amount, Authorised).

- If the final amount is not yet known, send the sum of the pre-determined amount plus the cashback amount to the EMV kernel in Tag 9F02 (Amount, Authorised).

9.10 CVM List

Follow the standard CVM list (Signature, Online PIN, Offline PIN, and No CVM) as cardholder verification methods.

For implementations that initiate chip processing when the final amount is not yet known and PIN is the chosen CVM for a transaction, do not display the amount on the PIN entry device.

When signature is the selected CVM, defer printing/displaying the signature panel until the authorization response is received, like standard chip transactions.

9.11 No Signature Required Processing

Quick chip is compatible with No Signature Required processing, and can be implemented in several ways depending on the merchant preference and risk tolerance.

Merchants utilizing quick chip and No Signature Required processing should note the following with regard to use of pre-determined or final amount:

- If the final amount is known before EMV processing begins, then standard No Signature Required processing should be performed if the final amount is less than or equal to the No Signature Required limit.
- If the final amount is not known before EMV processing begins, and a pre-determined amount is used that is **less than or equal to** the No Signature Required limit:
  - If the POS invokes a "No CVM Only" selectable kernel configuration so that the CVM Results of the standard EMV cardholder verification processing is "No CVM Required", then neither PIN or signature will be prompted. The merchant may be liable for lost/stolen chargebacks if the card is PIN preferring.
  - If the POS does not invoke a selectable kernel configuration, and the CVM Results are "Signature", then signature should not be prompted if the final amount is less than or equal to the No Signature Required Limit. If the CVM Results are "PIN", then PIN will be prompted.
- If the final amount is not known before EMV processing being, and a pre-determined amount is used that is **greater than** the No Signature Required limit, and the CVM Results are "Signature", then signature should not be prompted if the final amount is less than or equal to the No Signature Required Limit. If the CVM Results are "PIN", then PIN will be prompted.

Appendices

This Appendix contains the following:

Appendix A: Industry Codes

A.1 Conexxus Product Codes

Note: While this section lists all of the available Conexxus Product Codes, specific Fleet cards may only use a subset. Refer to the specific fleet provider's section for their accepted Product Code list. These codes are subject to change without notice.

Conexxus Product Codes have the following ranges:

- 001–099 apply to purchases of dispensed motor fuels and additives.
- 100–149 apply to purchases of vehicle products / services.
- 150–174 apply to purchases of aviation fuels.
- 175–224 apply to purchases of aviation products and services.
- 225–249 apply to purchases of marine fuels.
- 250–299 apply to purchases of marine products and services.
- 300–399 apply to purchases of other dispensed fuel and metered products.
- 400–599 apply to purchases of merchandise.
- 600–624 apply to purchase of packaged fuels.
- 625–649 are reserved for Conexxus future use.
- 650–699 apply to purchase of vehicle products/services (continued).
- 800–899 are reserved for proprietary use.
- 700–799 are reserved for Conexxus future use.
- 800–899 are reserved for proprietary use.
- 900–949 apply to negative transactions.
- 950–999 apply to administrative.

Table A-1 Conexxus Product Codes

Product Code	Description
000	Not Used
001–099	Dispensed Motor Fuels and Additives
001	Unleaded Regular
002	Unleaded Plus
003	Unleaded Super
004	Unleaded 4
005	Unleaded 5
006	<Deprecated> Unleaded Methanol (5.7% blend)
007	<Deprecated> Unleaded Plus Methanol (5.7% blend)
008	<Deprecated> Super Unleaded Methanol (5.7% blend)
009	<Deprecated> Unleaded Methanol (7.7% blend)

Table A-1 Conexxus Product Codes

Product Code	Description
010	<Deprecated> Unleaded Plus Methanol (7.7% blend)
011	Unleaded Ethanol (5.7% blend)
012	Unleaded Plus Ethanol (5.7% blend)
013	Unleaded Super Ethanol (5.7% blend)
014	Unleaded Ethanol (7.7% blend)
015	Unleaded Plus Ethanol (7.7% blend)
016	<Deprecated> Methanol / Leaded
017	<Deprecated> Ethanol / Leaded
018	<Deprecated> Leaded
019	Regular Diesel #2
020	Premium Diesel #2
021	Regular Diesel #1
022	Compressed Natural Gas
023	Liquid Propane Gas
024	Liquid Natural Gas
025	<Deprecated> M-85
026	E-85
027	Unleaded - Reformulated 1
028	Unleaded - Reformulated 2
029	Unleaded - Reformulated 3
030	Unleaded - Reformulated 4
031	Unleaded - Reformulated 5
032	<Deprecated> Diesel Off-Road (#1 and #2 Non-Taxable)
033	<Deprecated> Diesel Off-Road (Non-Taxable)
034	Biodiesel Blend Off-Road (Non-Taxable)
035	<Deprecated> Biodiesel Blend Off-Road (Non-Taxable)
036	Racing Fuel
037	<Deprecated> Super Unleaded Methanol (7.7% Blend)
038	<Deprecated> Unleaded Methanol (10% Blend)
039	<Deprecated> Unleaded Plus Methanol (10% Blend)
040	<Deprecated> Super Unleaded Methanol (10% Blend)
041	Super Unleaded Ethanol (7.7% Blend)
042	Unleaded Ethanol (10% Blend)
043	Unleaded Plus Ethanol (10% Blend)

Table A-1 Conexxus Product Codes

Product Code	Description
044	Super Unleaded Ethanol (10% Blend)
045	B2 Diesel Blend 2% Biodiesel
046	B5 Diesel Blend 5% Biodiesel
047	B10 Diesel Blend 10% Biodiesel
048	B11 Diesel Blend 11% Biodiesel
049	B15 Diesel Blend 15% Biodiesel
050	B20 Diesel Blend 20% Biodiesel
051	B100 Diesel Blend 100% Biodiesel
052	<Deprecated> Ultra Low Sulfur #1
053	<Deprecated> Ultra Low Sulfur #2
054	<Deprecated> Ultra Low Sulfur Premium Diesel #2
055	<Deprecated> Ultra Low Sulfur Biodiesel Blend 2%
056	<Deprecated> Ultra Low Sulfur Biodiesel Blend 5%
057	<Deprecated> Ultra Low Sulfur Biodiesel Blend 10%
058	<Deprecated> Ultra Low Sulfur Biodiesel Blend 11%
059	<Deprecated> Ultra Low Sulfur Biodiesel Blend 15%
060	<Deprecated> Ultra Low Sulfur Biodiesel Blend 20%
061	<Deprecated> Ultra Low Sulfur Biodiesel Blend 100%
062	DEF (Diesel Exhaust Fluid)
063	Premium Diesel #1
064	Unleaded Ethanol (15% Blend)
065	Unleaded Plus Ethanol (15% Blend)
066	Super Unleaded Ethanol (15% Blend)
067	Premium Diesel Blend <20% Biodiesel
068	Premium Diesel Blend >= 20% Biodiesel
069	B75 Diesel Blend 75% Biodiesel
070	B99 Diesel Blend 99% Biodiesel
071–098	Undefined Fuel–Reserved for Proprietary Use
099	Miscellaneous Fuel
100–149	Vehicle Products / Services
100	General Automotive Merchandise
101	Motor Oil
102	Car Wash
103	Oil Change

Table A-1 Conexxus Product Codes

Product Code	Description
104	Oil Filter
105	Work Order
106	Anti-Freeze
107	Washer Fluid
108	Brake Fluid
109	Tires
110	Federal Excise Tax (Tires)
111	Tire Rotation
112	Batteries
113	Lube
114	Inspection
115	Labor
116	Towing
117	Road Service
118	Vehicle Accessories
119	Vehicle Parts
120	Preventative Maintenance
121	Air Conditioning Service
122	Engine Service
123	Transmission Service
124	Brake Service
125	Exhaust Service
126	Body Work
127	Vehicle Glass
128	Synthetic Oil
129	Lamps
130	Wipers
131	Hoses
132	Tire-related (Wheel Balance Valve Stem)
133	Repairs
134	Service Package
135	Vehicle Parking
136	Truck Tank Cleaning
137	Other Lubricants

Table A-1 Conexxus Product Codes

Product Code	Description
138	Vehicle Fuel Additives/Treatment (Injected)
139	Vehicle Rental
140	Air Filter
141	Vehicle Prep
142	Fuel System
143–148	Undefined Vehicle Product/Services–Reserved for Proprietary Use
149	Miscellaneous Vehicle Products / Services
150–174	Aviation Fuels
150	Jet Fuel
151	Aviation Fuel Regular
152	Aviation Fuel Premium
153	Aviation Fuel JP8
154	Aviation Fuel 4
155	Aviation Fuel 5
156–167	Undefined Aviation Fuel–Reserved for Conexxus Future Use
168–173	Undefined Aviation Fuel–Reserved for Proprietary Use
174	Miscellaneous Aviation Fuel
175–224	Aviation Products / Services
175	Storage
176	Aircraft Ground Handling
177	Aircraft Ground Power Unit
178	Aircraft Labor
179	Aircraft Work Order
180	Aircraft Maintenance
181	Aircraft Service
182	Transportation
183	De-icing
184	Ramp Fees
185	Catering
186	Hangar Fee
187	Landing Fee
188	Call Out Fee
189	Aircraft Rental
190	Instruction Fee

Table A-1 Conexxus Product Codes

Product Code	Description
191	Flight Plans / Weather Brief
192	Charter Fee
193	Communication Fee
194	Aircraft Cleaning
195	Cargo Handling
196	Aircraft Accessories
197	Pilot Supplies
198	Aircraft Parking Fees
199	Aircraft Tie Down Fees
200	Aircraft Sanitation Fees
201	Aircraft Fuel Additive
202	AC Parts
203	Oxygen
204	De-fuel
205	Re-service
206	Static Dissipater Additive
207	Corrosion Inhibitor
208	Airport Fees
209	Overtime Fees
210	IT/Bladder
211	Ground Equipment Service Fees
212	Secure Fees
213	Flow Fee
214–215	Undefined Aviation–Reserved for Conexxus Future Use
216–223	Undefined Aviation–Reserved for Proprietary Use
224	Miscellaneous Aviation Products/Services
225–249	Marine Fuels
225	Marine Fuel 1
226	Marine Fuel 2
227	Marine Fuel 3
228	Marine Fuel 4
229	Marine Fuel 5
230	Marine - Other
231–242	Undefined Marine Fuel–Reserved for Conexxus Future Use

Table A-1 Conexxus Product Codes

Product Code	Description
243–248	Undefined Marine Fuel–Reserved for Proprietary Use
249	Miscellaneous Marine Fuel
250–299	Marine Products / Services
250	Marine Service
251	Marine Labor
252	Marine Work Order
253	Launch Fee
254	Slip Rental
255–280	Undefined Marine Services–Reserved for Conexxus Future Use
281–298	Undefined Marine Services–Reserved for Proprietary Use
299	Miscellaneous Marine Products/Services
300–399	Other Dispensed Fuels and Metered Products
300	Kerosene–Low Sulfur
301	White Gas
302	Heating Oil
303	<Deprecated> Bottled Propane
304	Other Fuel (Non-Taxable)
305	Kerosene–Ultra Low Sulfur
306	Kerosene–Low Sulfur (Non-Taxable)
307	Kerosene–Ultra Low Sulfur (Non-Taxable)
308	EVC-1–Level 1 charge = 110v 15 amp
309	EVC-2–Level 2 charge = 240v 15-40 amp
310	EVC-3–Level 3 charge = 480v 3 phase charge
311	Biodiesel Blend 2% Off-Road
312	Biodiesel Blend 5% Off-Road
313	Biodiesel Blend 10% Off-Road
314	Biodiesel Blend 11% Off-Road
315	Biodiesel Blend 15% Off-Road
316	Biodiesel Blend 20% Off-Road
317	Diesel #1 Off-Road
318	Diesel #2 Off-Road
319	Diesel #1 Premium Off-Road
320	Diesel #2 Premium Off-Road
321	Additive Dosage

Table A-1 Conexxus Product Codes

Product Code	Description
322	Unleaded Ethanol Blends E16-E84
323	Low Octane Unleaded
324	Blended Diesel (#1 and #2)
325	Off-Road Unleaded Regular (Non-Taxable)
326	Off-Road Unleaded Plus (Non-Taxable)
327	Off-Road Unleaded Super (Non-Taxable)
328	Off-Road Unleaded 4 (Non-Taxable)
329	Off-Road Unleaded 5 (Non-Taxable)
330	Recreational Fuel (90 Octane)
331	Hydrogen H35
332	Hydrogen H70
333–380	Undefined Other Fuel–Reserved for Conexxus Future Use
381–398	Undefined Other Fuel–Reserved for Proprietary Use
399	Miscellaneous Other Fuel
400–599	Merchandise
400	General Merchandise
401	General Ice
402–409	General Undefined–Reserved for Conexxus Future Use
410	General Tobacco
411	Cigarettes
412	Tobacco - Other
413–417	Undefined Tobacco–Reserved for Conexxus Future Use
418–419	Undefined Tobacco–Reserved for Proprietary Use
420	General Packaged Beverage
421	Packaged Beverages (non-alcoholic)
422	Packaged Juice
423	Other Packaged Beverages
424–427	Undefined Packaged Beverages–Reserved for Conexxus Future Use
428–429	Undefined Packaged Beverages–Reserved for Proprietary Use
430	General Dispensed Beverage
431	Hot Dispensed Beverages
432	Cold Dispensed Beverages
433	Frozen Dispensed Beverages
434	Other Dispensed Beverages

Table A-1 Conexxus Product Codes

Product Code	Description
435–437	Undefined Dispensed Beverages–Reserved for Conexxus Future Use
438–439	Undefined Dispensed Beverages–Reserved for Proprietary Future
440	General Snacks
441	Salty Snacks
442	Alternative Snacks
443	Sweet Snacks - Packaged
444–447	Undefined Snacks–Reserved for Conexxus Future Use
448–449	Undefined Snacks–Reserved for Proprietary Use
450	General Candy
451–457	Undefined Candy–Reserved for Conexxus Future Use
458–459	Undefined Candy–Reserved for Proprietary Use
460	General Dairy
461	Fluid Milk Products
462	Packaged Ice Cream/Novelties
463	Other Dairy
464–467	Undefined Dairy–Reserved for Conexxus Future Use
468–469	Undefined Dairy–Reserved for Proprietary Use
470	General Grocery
471	Groceries - Edible
472	Groceries - Non-Edible
473	Groceries - Perishable
474	Bread - Packaged
475	Frozen Foods
476–477	Undefined Grocery–Reserved for Conexxus Future Use
478–479	Undefined Grocery–Reserved for Proprietary Use
480	General Alcohol
481	Beer - Alcoholic
482	Beer - Non-Alcoholic
483	Wine
484	Liquor
485–487	Undefined Alcohol–Reserved for Conexxus Future Use
488–489	Undefined Alcohol–Reserved for Proprietary Use
490	General Deli
491	Packaged Sandwiches/Deli Products

Table A-1 Conexxus Product Codes

Product Code	Description
492	Prepared Foods
493	Deli Items
494–497	Undefined Deli–Reserved for Conexxus Future Use
498–499	Undefined Deli–Reserved for Proprietary Use
500	General Foodservice
501–507	Undefined Foodservice–Reserved for Conexxus Future Use
08–509	Undefined Foodservice–Reserved for Proprietary Use
510	General Lottery
511	Lottery - Instant
512	Lottery - Online
513	Lottery - Other
514–517	Undefined Lottery–Reserved for Conexxus Future Use
518–519	Undefined Lottery–Reserved for Proprietary Use
520	General Money Order
521	Money Order - Vendor Payment
522	Money Order - Payroll Check
523	Money Order - Gift Certificate
524	Money Order - Refund Check
525	Money Order - Official Check
526	Money Order - Rebate Check
527	Money Order - Dividend Check
528	Money Order - Utility Check
529	Undefined Money Order–Reserved for Conexxus Future Use
530	General Store Service
531	Home Delivery
532	Prepaid Cards - Purchase
533	Prepaid Cards - Activation/Recharge
534	Membership/Loyalty
535–537	Undefined Store Services–Reserved for Conexxus Future Use
538–539	Undefined Store Services–Reserved for Proprietary Use
540	General Health & Beauty Care
541–547	Undefined Health & Beauty Care–Reserved for Conexxus Future Use
548–549	Undefined Health & Beauty Care–Proprietary Use
550	General Publications

Table A-1 Conexxus Product Codes

Product Code	Description
551–557	Undefined General Publications– Reserved for Conexxus Future Use
558–559	Undefined General Publications Reserved for Proprietary Use
558–559	Undefined General Publications Reserved for Proprietary Use
560–590	Prepaid and Bill Pay (Secondary Network)
560	PIN Activate Prepaid Card
561	PIN Return Prepaid Card
562	Enable Device/Handset Unlock
563	Disable Device/Handset Lock
564	3rd Party Prepaid Card Activate
565	3rd Party Prepaid Card Reload
566	Financial Prepaid Card Activate
567	Financial Prepaid Card Reload
568	Proprietary Prepaid Card Activate
569	Proprietary Prepaid Card Reload
570	General Purpose Activate
71	General Purpose Reload
572	Real Time Recharge
573	Wireless Real Time Recharge
574	Single Payee Bill Pay
575	Multiple Payee Bill Pay
576–583	Undefined Prepaid and Bill Pay–Reserved for Conexxus Future Use
584–590	Undefined Prepaid and Bill Pay–Reserved for Proprietary Use
591–599	Undefined Merchandise–Reserved Proprietary Use
600–624	Packaged Fuels
600	DEF (Diesel Exhaust Fluid)
601	B99
602	B100
603	Additive
604	Kerosene
605	Propane
606–612	Undefined Packaged Fuels–Reserved for Conexxus Future Use
613–623	Undefined Packaged Fuels–Reserved for Proprietary Use
624	Miscellaneous Packaged Fuels

Table A-1 Conexxus Product Codes

Product Code	Description
625–649	Reserved for Conexxus Future Use
650–699	Vehicle Products/Services (Continued)
650	Scales
651	Shower
652	Tire Repair
653	Lodging
654	Wash Out
655	Trailer Wash
656	RV Dump Fee
657	EV Charging Fee
658–689	Undefined Vehicle Product/Services–Reserved for Conexxus Use
690–699	Undefined Vehicle Product/Services–Reserved for Proprietary Use
700–799	Reserved for Conexxus Future Use
800–899	Reserved for Proprietary Use
900–949	Negative Transactions
900	Discount 1
901	Discount 2
902	Discount 3
903	Discount 4
904	Discount 5
905	Coupon 1
906	Coupon 2
907	Coupon 3
908	Coupon 4
909	Coupon 5
910	Lottery Pay Out - Instant
911	Lottery Pay Out - Online
912	Lottery Pay Out - Other
913	Split Tender
914	Tax Discount/Forgiven
915–940	Undefined Negative–Reserved for Conexxus Future Use
941–948	Undefined Negative–Reserved for Proprietary Use
949	Miscellaneous Negative Administrative

Table A-1 Conexxus Product Codes

Product Code	Description
950–999	Administrative
950	Tax 1
951	Tax 2
952	Tax 3
953	Tax 4
954	Tax 5
955	Cash Back
956	Cash Back Fee
957	Fee 1
958	Fee 2
959	Fee 3
960	Fee 4
961	Fee 5
962	Miscellaneous Aviation Tax
963	GST/HST (Canadian)/VAT 1
964	PST/QST (Canadian) VAT 2
965	SWT Rate (Canadian)
966	Tax 6
967	Tax 7
968	Tax 8
969	Jet Federal Excise Tax
970	AvGas Federal Excise Tax
971–990	Undefined Administrative–Reserved for Conexxus Future Use
991–998	Undefined Administrative–Reserved for Proprietary Use
999	Miscellaneous Administrative

A.2 Mastercard Purchasing Product Codes

Mastercard Purchasing Product Codes have the following ranges:

- 001–029 apply to purchases for motor fuels for cars, trucks, and vans.
- 030–099 apply to purchases for automotive repairs, goods purchased from convenience stores, and other miscellaneous purchases.
- 100–149 apply to purchase aviation fuels.
- 150–199 apply to purchase marine fuels.
- 200–299 apply to purchases other fuels.
- 300–349 apply to purchases aviation repairs and services.
- 350–399 apply to purchase marine and boat repair/other.
- 400–999 undefined.

This section includes the following product codes:

- *A.2.1 Mastercard Purchasing Fuel Product Codes, p. 191*
- *A.2.2 Mastercard Purchasing Non-Fuel Product Codes, p. 193*

A.2.1 Mastercard Purchasing Fuel Product Codes

Table A-2 Mastercard Purchasing Fuel Product Codes

Product Codes	Description
000	Not Used
001	Unleaded Regular (86 or 87 Octane)
002	Unleaded Mid Grade (88 or 89 Octane)
003	Unleaded Premium (90 or 91 Octane)
004	Unleaded Super (92–94 Octane)
005	Methanol Unleaded Regular (86 or 87 Octane)
006	Methanol Unleaded Mid Grade (88 or 89 Octane)
007	Methanol Unleaded Premium (90 or 91 Octane)
008	Methanol Unleaded Super (92 or 94 Octane)
009	Methanol Regular Leaded
011	Regular Leaded Gasoline
012	Diesel
013	Diesel Premium
014	Kerosene
015	LPG

Table A-2 Mastercard Purchasing Fuel Product Codes (Continued)

Product Codes	Description
016	Compressed Natural Gas
017	M85 (Methanol 85%)
018	E85 (Ethanol 85%)
019	Ethanol Unleaded Regular (86 or 87 Octane)
020	Ethanol Unleaded Mid Grade (88 or 89 Octane)
021	Ethanol Unleaded Premium (90 or 91 Octane)
022	Ethanol Unleaded Super (92 or 94 Octane)
023	Ethanol Regular Leaded
024	Unleaded Reformulated (86 or 87 Octane)
025	Unleaded Mid Grade Reformulated (88 or 89 Octane)
026	Dyed Diesel
027	Gasohol
028	Biodiesel
029	Ultralow Sulfer Diesel (ULSD)
100	Aviation 100 Octane
101	Jet Fuel
102	Aviation Fuel
150	Marine Fuel
200	Miscellaneous Fuel
201	Liquid Natural Gas
202	White Gas
203	Racing Fuel

A.2.2 Mastercard Purchasing Non-Fuel Product Codes

Table A-3 Mastercard Purchasing Non-Fuel Product Codes

Product Codes	Description
030	Motor Oil
031	Oil Change
032	Engine Service
033	Transmission Service
034	Brake Service
035	Solvent
036	Brake Fluid
037	Miscellaneous Parts
038	Miscellaneous Labor
039	Miscellaneous Repairs
040	TBA (Tires, Batteries, Accessories)
041	Tires
042	Batteries
043	Automotive Accessories
044	Automotive Glass
045	Car Wash
046	Towing
070	Cigarettes/Tobacco
078	Health/Beauty Aid
079	Miscellaneous Food/Grocery
080	Soda
081	Beer/Wine
082	Milk/Juice
083	Restaurant
089	Miscellaneous Beverage
099	Miscellaneous Other
300	Aviation Maintenance
301	De-icing
302	APU or Aircraft Jump Start
303	Aviation Catering
304	Tie down or Hangar
305	Landing Fee

Table A-3 Mastercard Purchasing Non-Fuel Product Codes (Continued)

Product Codes	Description
306	Ramp Fee
307	Call Out Fee
308	Plane Rental
309	Instruction Fee
310	Miscellaneous Aviation
311	Flight Planning/Weather Fees
312	Charter Fees
313	Ground Handling
314	Communications Fees
315	Aircraft Cleaning
316	Cargo Handling
317	Aviation Accessories
350	Boat Service

A.3 Mastercard Fleet Product Codes

This section includes the following product codes:

A.3.1 Mastercard Fleet Fuel Product Codes

Table A-4 Mastercard Fleet Fuel Product Codes

Product Code	Description
00	Not Used
01	Unleaded Regular (86 or 87 Octane)
02	Unleaded Mid Grade (88 or 89 Octane)
03	Unleaded Premium (90 or 91 Octane)
04	Unleaded Super (92–94 Octane)
05	Methanol Unleaded Regular (86 or 87 Octane)
06	Methanol Unleaded Mid Grade (88 or 89 Octane)
07	Methanol Unleaded Premium (90 or 91 Octane)
08	Methanol Unleaded Super (92 or 94 Octane)
09	Methanol Regular Leaded
11	Regular Leaded Gasoline
12	Diesel
13	Diesel Premium
14	Kerosene
15	LPG
16	Compressed Natural Gas
17	M85 (Methanol 85%)
18	E85 (Ethanol 85%)
19	Ethanol Unleaded Regular (86 or 87 Octane)
20	Ethanol Unleaded Mid Grade (88 or 89 Octane)
21	Ethanol Unleaded Premium (90 or 91 Octane)
22	Ethanol Unleaded Super (92 or 94 Octane)
23	Ethanol Regular Leaded
24	Unleaded Reformulated (86 or 87 Octane)
25	Unleaded Mid Grade Reformulated (88 or 89 Octane)
26	Dyed Diesel

Table A-4 Mastercard Fleet Fuel Product Codes (Continued)

Product Code	Description
27	Gasohol
28	Biodiesel
29	Ultralow Sulfer Diesel (ULSD)

A.3.2 Mastercard Fleet Non-Fuel Product Codes

Table A-5 Mastercard Fleet Non-Fuel Product Codes

Product Code	Description
30	Motor Oil
31	Oil Change
32	Engine Service
33	Transmission Service
34	Brake Service
35	Solvent
36	Brake Fluid
37	Miscellaneous Parts
38	Miscellaneous Labor
39	Miscellaneous Repairs
40	TBA (Tires, Batteries, Accessories)
41	Tires
42	Batteries
43	Automotive Accessories
44	Automotive Glass
45	Car Wash
46	Towing
70	Cigarettes/Tobacco
78	Health/Beauty Aid
79	Miscellaneous Food/Grocery
80	Soda
81	Beer/Wine
82	Milk/Juice
83	Restaurant
89	Miscellaneous Beverage
99	Miscellaneous Other

A.4 Heartland Product Codes for Visa Fleet Processing

The following Heartland product codes are to be used when processing Visa Fleet transactions for NTS, Z01 and POS 8583. These codes are converted by Heartland to the Visa Fleet product codes contained in Visa's Implementation Guide.

- Codes numbered 00–29 apply to fuel purchases for motor vehicles.
- Codes numbered 30–99 apply to purchases for automotive repairs, goods purchased from convenience stores, and other miscellaneous purchases.

This section includes the following product codes:

- *A.4.1 Fuel Product Codes, p. 197*
- *A.4.2 Non-Fuel Product Codes, p. 199*

A.4.1 Fuel Product Codes

Table A-6 Fuel Product Codes

Fuel Product Code	Description
00	Other
01	Unleaded Regular – 86
02	Unleaded Regular – 87
03	Unleaded Mid Grade – 88
04	Unleaded Mid Grade – 89
05	Unleaded Premium – 90
06	Unleaded Premium – 91
07	Unleaded Super – 92
08	Unleaded Super – 93
09	Unleaded Super – 94
10	RESERVED
11	Regular Leaded
12	Diesel
13	Diesel Premium
14	Kerosene
15	LPG
16	Gasohol
17	CNG
18	Methanol – 85
19	Methanol – 10

Table A-6 Fuel Product Codes

Fuel Product Code	Description
20	Methanol – 7
21	Methanol – 5
22	Ethanol – 85
23	Ethanol – 10
24	Ethanol – 7
25	Ethanol – 5
26	Jet Fuel
27	Aviation Fuel
28	Off-Road diesel
29	Marine

A.4.2 Non-Fuel Product Codes

Table A-7 Non-Fuel Product Codes

Non-Fuel Product Code	Description
30	Motor Oil
31	Oil Change
32	Engine Service
33	Transmission Service
34	Brake Service
35–38	Unassigned Repair Values
39	Miscellaneous Repairs
40	Tires, Batteries, and Accessories
41	Tires
42	Batteries
43	Automotive Accessories
44	Automotive Glass
45	Car Wash
46–69	Unassigned Automotive Products and Services
70	Cigarettes and Tobacco
71–77	Unassigned Food and Grocery Items
78	Health and Beauty Aids
79	Miscellaneous Grocery
80	Soda
81	Beer and Wine
82	Milk and Juice
83–89	Unassigned Beverage Items
90	Miscellaneous
91–99	Unassigned

A.5 Voyager Product Codes

This section includes the following product codes:

A.5.1 Voyager Fuel Product Codes

Table A-8 Voyager Fuel Product Codes

Product Code	Description
01	UNLEADED
02	UNLEADED PLUS
03	FUTURE USE
04	SUPER UNLEADED
05	DIESEL
06	AVIATION
07	JET FUEL
08	MARINE
50	PROPANE
51	NATURAL GAS
52	METHANOL
53	ETHANOL
54	KEROSENE
55	10% GASOHOL
56	7.7% GASOHOL
57	5.7% GASOHOL
58	WHITE GAS
59	COMPR NAT GAS(CNG)
60	DUAL PROPANE/UNLDED
61	WIDE NOZZLE UNLEADED
62	SPECIAL MTR FUEL LPG
63	OTHER FUEL
64	M 85
65	DIESEL WITHOUT TAX
66	E 85
67	LIQUIFIED NATURAL GAS

Table A-8 Voyager Fuel Product Codes

Product Code	Description
68	UNLEADED WITHOUT TAX
D0 (zero)	BIO DIESEL
D1	5.7% UNLEADED BLEND
D2	7.7% UNLEADED BLEND
D3	10% UNLEADED BLEND
D4	5.7% UNLD PLUS BLEND
D5	7.7% UNLD PLUS BLEND
D6	10% UNLD PLUS BLEND
D7	5.7% UNLD SUPER BLND
D8	7.7% UNLD SUPER BLND
D9	10% UNLD SUPER BLND

A.5.2 Voyager Non-Fuel Product Codes

Table A-9 Voyager Non-Fuel Product Codes

Product Code	Description
09	OIL
10	ACCESSORIES
11	COOLING SYSTEM
12	CHARGING SYSTEM
13	FLUIDS
14	FOOD
15	TIRE AND TUBE
16	TUBES
17	AVIONICS
18	OIL FILTER AND SERV
19	PARTS
20	REPAIRS
21	SERVICE
22	STORAGE
23	TIRES
24	TIRES AND TUBE REPAIR
25	LABOR
26	FEDERAL EX TAX TIRE

Table A-9 Voyager Non-Fuel Product Codes

Product Code	Description
27	WASH JOB
28	WASH AND LUBE
29	WASH AND POLISH
30	MAINTENANCE
31	LUBE
32	STATE INSPECTION
33	MISCELLANEOUS
34	SALES TAX
35	LOCATION DISCOUNT
36	PARTICIPANT DISCOUNT
37	AIR FILTERS
38	AUTO/MAN TRANS SERV
39	AIR CONDITION SERV
40	FUEL INJECT CLEAN SV
41	RADIATOR SERVICE
42	TIRE ROTATION
43	WIPER BLADE
44	BELTS-SERVICE&REPLACEMENT
45	FULL SERVICE OIL CHANGE
46	FRONT/REAR DIFF SERVICE
47	BREATHERS/PCV VALVES
48	AUTOMOTIVE GLASS
49	FUEL ADDITIVES
70	TOW
71	FLAT
72	NON-CONTRACTED SERV
73	BATTERY
74	GAS/ROADSIDE SERVICE
75	STALLED
76	LOCKOUT
77	NO SERVICE RENDERED
78	AMBULANCE
79	OTHER
80	AVIATION MAINTENANCE

Table A-9 Voyager Non-Fuel Product Codes

Product Code	Description
81	DE-ICING
82	APU OR AIRCRAFT JUMP SEAT
83	AVIATION CATERING
84	TIEDOWN OR HANGER
85	LANDING FEE
86	RAMP FEE
87	CALL OUT FEE
88	PLANE RENTAL
89	INSTRUCTIONAL FEE
90	MISCELLANEOUS AVIATION
91	FLIGHT PLANNING FEE
92	WEATHER FEE
93	CHARTER FEES
94	GROUND HANDLING
95	COMMUNICATION FEES
96	AIRCRAFT CLEANING
97	CARGO HANDLING
98	AVIATION ACCESSORIES
99	FUTURE USE
M0	CAB, CLIMATE CNTL & AERO
M1	AIR COND, HEATING & VENTI
M2	CAR & SHEET METAL
M3	INSTRUMENTS, GAUGE, WARNI
M4	AERODYNAMIC DEVICES
M5	CHASSIS GROUP
M6	AXLES - NON DRIVEN, FRONT
M7	AXLES - NON DRIVEN, REAR
M8	BRAKES
M9	FRAME
N0	STEERING
N1	SUSPENSION
N2	WHEELS RIMS HUBS & BEARIN
N3	AUTO/MANU CHASSIS LUBRICA
N4	DRIVE TRAIN GROUP

Table A-9 Voyager Non-Fuel Product Codes

Product Code	Description
N5	AXLES-DRIVEN, FRONT STEER
N6	AXLES-DRIVEN, REAR
N7	CLUTCH
N8	DRIVE SHAFTS
N9	TRANSFER CASE
O0	TRANSMISSION-MAIN, MANUAL
O1	TRANSMISSION-MAIN, AUTO
O2	AUXILIARY TRANSMISSION
O3	AUX SEC-MAIN TRANS, MANU
O4	ELECTRICAL GROUP
O5	CRANKING SYSTEM
O6	IGNITION SYSTEM
O7	LIGHTING SYSTEM
O8	MULTI-FUNC ELECT DEVICES
O9	ENGINE/MOTOR SYSTEMS
P0	AIR INTAKE SYSTEM
P1	EXHAUST SYSTEM
P2	FUEL SYSTEM
P3	POWER PLANT
P4	ELECTRIC PROPULSION SYSTE
P5	MUL SYS(40-46) FILTER KIT
P6	EXPANDABLE ITEMS
P7	HORNS & SIGNAL ALARMS
P8	CARGO HANDLING RESTRAINT
P9	POWER TAKE OFF
Q0	SPARE WHEEL MOUNTING
Q1	WINCH
Q2	VEHICLE COUPLING SYSTEM
Q3	SPECIAL APPLICATIONS GRP
Q4	TERMINAL EQUIPMNT-SYS & A
Q5	CONSTRU EQUIP-CHASSIS MOU
Q6	SATELLITE COMM SYSTEM
Q7	HYDRAULIC SYSTEMS - S APP
Q8	BODIES AND VESSELS GROUP

Table A-9 Voyager Non-Fuel Product Codes

Product Code	Description
Q9	BODY
R0	REAL WALL & DOOR
R1	TANK VESSEL-INNER SHELL
R2	TANK VESSEL-OUTER JACKET
R3	MANHOLES
R4	RINGS & BOLSTERS
R5	TRAILER FRAME & SUPPORT
R6	TRIM & MISC HARDWARE
R7	SAFTY DEVICES
R8	HEATING & REFRIGERATION G
R9	HEATING UNIT
S0	MECHANICAL REFRIG UNIT
S1	NITROGEN REFRIG UNIT
S2	HOLDOVER PLATE REFRIGERAT
S3	BULK PRODUCT TRANSFER SYS
S4	BLOWERS, CONVEYORS & VIBR
S5	COMPRESSOR-BULK PROD SYS
S6	ENGINE (AUXILIARY)
S7	LINES TUBES HOSES & ATTIN
S8	MANIFOLD
S9	POWER SHAFT-POWER TAKE OF
T0	PUMP-PRODUCT TRANSFER
T1	VALVES & CONTROLS-BULK PR
T2	SAFETY DEVICES,INSTRU & G
T3	RE-REFINED OIL
T4	DISPOSAL/WASTE FEE
T5	EMISSION TEST FEE
T6	TRANSMISSION
T7	DO NOT USE – REVERSE TRANS
T8	AUTO PAINT
T9	RADIO MAINT
U1	ALIGNMENT
U2	PREV MAINT
V1	KEY CHAINS

Table A-9 Voyager Non-Fuel Product Codes

Product Code	Description
V2	ACCOUNT SET UP
V3	ELECTRONIC FILE
V4	OVERNIGHT CARD
V5	CUSTOMIZED REPORT
V6	FLEET COMMANDER
V7	CUSTOMIZED QUERY
V8	MEDIA FEE
V9	BILLING REPRINT
VA	CARD REISSUE
VB	MOCHA ONLINE
W2	AUTO SIDE GLASS
W3	AUTO BACK GLASS
WI	AUTO WINDSHIELD GLASS

A.6 WEX Supported Conexxus Product Codes

Table A-10 WEX Supported Conexxus Product Codes

Product Code	Conexxus Description	WEX Description
001	Unleaded Regular	Unleaded
002	Unleaded Plus	Unleaded Plus
003	Unleaded Super	Super Unleaded
004	Unleaded 4	N/A
005	Unleaded 5	N/A
006	Gas / Methanol 1	Unleaded 5.7 methanol blend
007	Gas / Methanol 2	Unleaded Plus 5.7% methanol blend
008	Gas / Methanol 3	Super Unleaded 5.7% methanol blend
009	Gas / Methanol 4	Unleaded 7.7% methanol blend
010	Gas / Methanol 5	Unleaded Plus 7.7% methanol blend
011	Gas / Ethanol 1	Unleaded 5.7 ethanol blend
012	Gas / Ethanol 2	Unleaded Plus 5.7% ethanol blend
013	Gas / Ethanol 3	Super Unleaded 5.7% ethanol blend
014	Gas / Ethanol 4	Unleaded 7.7% ethanol blend
015	Gas / Ethanol 5	Unleaded Plus 7.7% ethanol blend
016	Methanol / Leaded	Methanol / Leaded
017	Ethanol / Leaded	Ethanol / Leaded
018	Leaded	Leaded
019	Regular Diesel #2	Regular Diesel (Taxed)
020	Premium Diesel #2	Premium Diesel (Taxed)
021	Diesel #1	N/A
022	Compressed Natural Gas	Compressed Natural Gas
023	Liquid Propane Gas	Liquid Propane Gas
024	Liquid Natural Gas	Liquid Natural Gas
025	M-85	M-85
026	E-85	E-85
027	Unleaded - Reformulated 1	N/A
028	Unleaded - Reformulated 2	N/A
029	Unleaded - Reformulated 3	N/A
030	Unleaded - Reformulated 4	N/A
031	Unleaded - Reformulated 5	N/A

Table A-10 WEX Supported Conexxus Product Codes (Continued)

Product Code	Conexxus Description	WEX Description
032	Diesel 1 Off-Road (#1 and #2 Non-Taxable)	Diesel Off Road / Farm Fuel
033	Ultra Low Sulfur Diesel Off-Road (Non-Taxable)	Diesel Refrigerator Fuel
034	Biodiesel Blend Off-Road (Non-Taxable)	N/A
035	Ultra Low Sulfur Biodiesel Blend Off-Road (Non-Taxable)	Other Farm Fuel or Refrigerator Fuel
036	Racing Fuel	Racing Fuel
037	Super Unleaded Methanol	Super Unleaded 7.7% methanol blend
038	Unleaded Methanol	Unleaded 10% methanol blend
039	Undefined Plus Methanol	Unleaded Plus 10% methanol blend
040	Super Unleaded Methanol	Super Unleaded 10% methanol blend
041	Super Unleaded Ethanol	Super Unleaded 7.7% ethanol blend
042	Unleaded Ethanol	Unleaded 10% ethanol blend
043	Unleaded Plus Ethanol	Unleaded Plus 10% ethanol blend
044	Super Unleaded Ethanol	Super Unleaded 10% ethanol blend
045	B2 Diesel Blend 2% Biodiesel	
046	B5 Diesel Blend 5% Biodiesel	
047	B10 Diesel Blend 10% Biodiesel	
048	B11 Diesel Blend 11% Biodiesel	
049	B15 Diesel Blend 15% Biodiesel	
050	B20 Diesel Blend 20% Biodiesel	
051	B100 Diesel Blend 100% Biodiesel	
052	Ultra Low Sulfur #1	
053	Ultra Low Sulfur #2	
054	Ultra Low Sulfur Premium Diesel #2	
055	Ultra Low Sulfur Biodiesel Blend 2%	
056	Ultra Low Sulfur Biodiesel Blend 5%	
057	Ultra Low Sulfur Biodiesel Blend 10%	
058	Ultra Low Sulfur Biodiesel Blend 11%	
059	Ultra Low Sulfur Biodiesel Blend 15%	
060	Ultra Low Sulfur Biodiesel Blend 20%	
061	Ultra Low Sulfur Biodiesel Blend 100%	
062	Diesel Exhaust Fluid	
063–070	Undefined Fuel – Reserved for Conexxus Future Use	

Table A-10 WEX Supported Conexxus Product Codes (Continued)

Product Code	Conexxus Description	WEX Description
071	Auth Only	Fuel, grade unknown at Auth
072	Auth Only	Diesel, grade unknown at Auth
073	Auth Only	Alt. Fuel grade unknown at Auth
074	Auth Only	Multi Fuel, grade unknown at Auth
075	Auth Only	Multi Product, product unknown at Auth
076–098	Undefined Fuel, reserved for Proprietary	Undefined Fuel, reserved for Proprietary
099	Miscellaneous Fuel	Miscellaneous Fuel
100	General Automotive Merchandise	General Automotive Merchandise
101	Motor Oil	Motor Oil
102	Car Wash	Car Wash
103	Oil Change	Oil Change
104	Oil Filter	Oil Filter
105	Work Order	Work Order
106	Anti-Freeze	Anti-Freeze
107	Washer Fluid	Washer Fluid
108	Brake Fluid	Brake Fluid
109	Tires	Tires
110	Federal Excise Tax (Tires)	Federal Excise Tax (Tires)
111	Tire Rotation	Tire Rotation
112	Batteries	Batteries
113	Lube	Lube
114	Inspection	Inspection
115	Labor	Labor
116	Towing	Towing
117	Road Service	Road Service
118	Auto Accessories	Auto Accessories
119	Auto Parts	Auto Parts
120	Preventive Maintenance	Preventive Maintenance
121	Air Conditioning Service	Air Conditioning Service
122	Engine Service	Engine Service
123	Transmission Service	Transmission Service
124	Brake Service	Brake Service
125	Exhaust Service	Exhaust Service
126	Body Work	Body Work

Table A-10 WEX Supported Conexxus Product Codes (Continued)

Product Code	Conexxus Description	WEX Description
127	Automotive Glass	Automotive Glass
128	Synthetic Motor Oil	
129	Undefined Parts / Service	Lamps
130	Undefined Parts / Service	Wipers
131	Undefined Parts / Service	Hoses
132	Undefined Parts / Service	Tire related, Wheel Balance, Valve Stem
133	Undefined Parts / Service	Repairs or Service
134	Undefined Parts / Service	Service Package
135	Automotive Parking	Automotive Parking
136	Truck Tank Cleaning	Truck Tank Cleaning
137	Other Lubricants	Other Lubricants
138	Automotive Fuel Additives / Treatment (injected)	
139	Vehicle Rental	Car Rental
140	Air Filter	Filters
141	Vehicle Prep	Auto Detail
142	Fuel System	Service Package
143–148	Undefined Parts / Service	
149	Misc. Parts and Service	Front End, Shocks & Springs, Flush & Fill, or Automotive Detailing
150	Jet Fuel Regular	Jet Fuel A
151	Jet Fuel Premium	Jet Fuel A with Additives
152	Jet Fuel JP8	Jet Fuel B turbo
153	Aviation Fuel 3	Jet Fuel JP8
154	Aviation Fuel 4	Aviation Gas 100LL
155	Aviation Fuel 5	Aviation Gas 80LL
156–173	Undefined Aviation Fuel	
174	Miscellaneous Aviation Fuel	Miscellaneous Aviation Fuel
175	Storage	Storage
176	Aircraft Ground Handling	Aircraft Ground Handling
177	Aircraft Ground Power Unit	Aircraft Ground Power Unit
178	Aircraft Labor	Aircraft Labor
179	Aircraft Work Order	Aircraft Work Order
180	Aircraft Maintenance	Aircraft Maintenance

Table A-10 WEX Supported Conexxus Product Codes (Continued)

Product Code	Conexxus Description	WEX Description
181	Aircraft Service	Aircraft Service
182	Transportation	Transportation
183	De-icing	De-icing
184	Ramp Fees	Ramp Fees
185	Catering	Catering
186	Hangar Fee	Hangar Fee
187	Landing Fee	Landing Fee
188	Call Out Fee	Call Out Fee
189	Aircraft Rental	Aircraft Rental
190	Instruction Fee	Instruction Fee
191	Flight Plans / Weather Brief	Flight Plans / Weather Brief
192	Charter Fee	Charter Fee
193	Communication Fee	Communication Fee
194	Aircraft Cleaning	Aircraft Cleaning
195	Cargo Handling	Cargo Handling
196	Aircraft Accessories	Aircraft Accessories
197	Undefined Aviation	Pilot Supplies
198	Undefined Aviation	Aircraft Parking Fees
199	Undefined Aviation	Aircraft Tie down Fees
200	Undefined Aviation	Aircraft Sanitation Fees
201	Undefined Aviation	Aviation Fuel Additive
202–223	Undefined Aviation	Undefined Aviation
224	Miscellaneous Aviation	Airline Fee, APT Airport Fees, or Miscellaneous Aviation
225	Marine Fuel 1	Marine Fuel 1
226	Marine Fuel 2	Marine Fuel 2
227	Marine Fuel 3	Marine Fuel 3
228	Marine Fuel 4	Marine Fuel 4
229	Marine Fuel 5	Marine Fuel 5
230	Marine - Other	Marine - Other
231–248	Undefended Marine Fuel	Unidentified Marine Fuel
249	Miscellaneous Marine Fuel	Miscellaneous Marine Fuel
250	Marine Service	Marine Service
251	Marine Labor	Marine Labor

Table A-10 WEX Supported Conexxus Product Codes (Continued)

Product Code	Conexxus Description	WEX Description
252	Marine Work Order	Marine Work Order
253	Launch Fee	Launch Fee
254	Slip Rental	Slip Rental
255–298	Undefined Marine Services	Undefined Marine Services
299	Miscellaneous Marine Service	Miscellaneous Marine Service
300	Kerosene – Low Sulfur	Kerosene
301	White Gas	White Gas
302	Heating Oil	Heating Oil
303	Bottled Propane	Bottled Propane
304	Other Fuel (Non-Taxable)	Other Fuel (Non-Taxable)
305	Kerosene – Ultra Low Sulfur	
306	Kerosene – Low Sulfur (non-taxable)	
307	Kerosene – Ultra Low Sulfur (non-taxable)	
308–398	Undefined Other Fuel	Undefined Other Fuel
399	Miscellaneous Other Fuel	Miscellaneous Other Fuel
400	General Merchandise	General Merchandise
401	General Ice	General Ice
402–409	General Undefined	General Unidentified
410	General Tobacco	General Tobacco
411	Cigarettes	Cigarettes
412	Tobacco - Other	Tobacco - Other
413–419	Undefined Tobacco	Unidentified Tobacco
420	General Packaged Beverage	General Packaged Beverage
421	Packaged Beverages (non-alcoholic)	Packaged Beverages (non-alcoholic)
422	Juice	Juice
423	Other Packaged Beverages	Other Packaged Beverages
424–429	Undefended Packaged Beverage	Undefended Packaged Beverage
430	General Dispensed Beverage	General Dispensed Beverage
431	Hot Dispensed Beverage	Hot Dispensed Beverage
432	Cold Dispensed Beverage	Cold Dispensed Beverage
433	Frozen Dispensed Beverage	Frozen Dispensed Beverage
434	Other Dispensed Beverage	Other Dispensed Beverage
435–439	Undefined Dispensed Beverage	Undefined Dispensed Beverage
440	General Snacks	General Snacks

Table A-10 WEX Supported Conexxus Product Codes (Continued)

Product Code	Conexxus Description	WEX Description
441	Salty Snacks	Salty Snacks
442	Alternative Snacks	Alternative Snacks
443	Sweet Snacks - Packaged	Sweet Snacks - Packaged
444–449	Undefined Snacks	Undefined Snacks
450	General Candy	General Candy
451–459	Undefined Candy	Undefined Candy
460	General Dairy	General Dairy
461	Fluid Milk Products	Fluid Milk Products
462	Packaged Ice Cream/Novelties	Packaged Ice Cream/Novelties
463	Other Dairy	Other Dairy
464–469	Undefined Dairy	Undefined Dairy
470	General Grocery	General Grocery
471	Groceries - Edible	Groceries - Edible
472	Groceries - Non-Edible	Groceries - Non-Edible
473	Groceries - Perishable	Groceries - Perishable
474	Bread - Packaged	Bread - Packaged
475	Frozen Foods	Frozen Foods
476–479	Undefined Grocery	Undefined Grocery
480	General Alcohol	General Alcohol
481	Beer - Alcohol	Beer - Alcohol
482	Beer - Non-Alcoholic	Beer - Non-Alcoholic
483	Wine	Wine
484	Liquor	Liquor
485–489	Undefined Alcohol	Undefined Alcohol
490	General Deli	General Deli
491	Packaged Sandwiches/Deli Products	Packaged Sandwiches/Deli Products
492	Prepared Foods	Prepared Foods
493	Deli Items	Deli Items
494–499	Undefined Deli	Undefined Deli
500	General Food Service	General Food Service
501–509	Undefined Food Service	
510	General Lottery	General Lottery
511	Lottery - Instant	Lottery - Instant
512	Lottery - Online	Lottery - Online

Table A-10 WEX Supported Conexxus Product Codes (Continued)

Product Code	Conexxus Description	WEX Description
513	Lottery - Other	Lottery - Other
514–519	Undefined Lottery	Undefined Lottery
520	General Money Order	General Money Order
521	Money Order - Vendor Payment	Money Order - Vendor Payment
522	Money Order - Payroll Check	Money Order - Payroll Check
523	Money Order - Gift Certificate	Money Order - Gift Certificate
524	Money Order - Refund Check	Money Order - Refund Check
525	Money Order - Official Check	Money Order - Official Check
526	Money Order - Rebate Check	Money Order - Rebate Check
527	Money Order - Dividend Check	Money Order - Dividend Check
528	Money Order - Utility Check	Money Order - Utility Check
529	Undefined Money Order	Undefined Money Order
530	General Store Services	General Store Services
531	Home Delivery	Home Delivery
532	Prepaid Cards - Purchase	Prepaid Cards - Purchase
533	Prepaid Cards - Activation/Recharge	Prepaid Cards - Activation/Recharge
534–539	Undefined Store Services	
540	General Health & Beauty Care	General Health & Beauty Care
541–549	Undefined Health & Beauty Care	
550	General Publications	General Publications
551–559	Undefined Publications	
560–599	Undefined Merchandise	Undefined Merchandise
600–799	Reserved for Future Use	
800	Reserved for Proprietary Use	WEX use only. Management Control Card Approved
801	Reserved for Proprietary Use	WEX use only. Replacement Card Fee (WEX generated; used for some Partner Billed Cobrands)
802	Reserved for Proprietary Use	WEX use only. Tax Exempt (WEX generated; used to populate OFFIS Trnx Detail).
803	Reserved for Proprietary Use	Environmental Disposal Fee
804	Reserved for Proprietary Use	Car Rental
805–899	Reserved - Proprietary Use	Reserved - Proprietary Use
900	Discount 1	Discount Fuel
901	Discount 2	Discount Non-Fuel

Table A-10 WEX Supported Conexxus Product Codes (Continued)

Product Code	Conexxus Description	WEX Description
902	Discount 3	Discount 3
903	Discount 4	Discount 4
904	Discount 5	Discount 5
905	Coupon 1	Coupon Fuel
906	Coupon 2	Coupon Non-Fuel
907	Coupon 3	Coupon 3
908	Coupon 4	Coupon 4
909	Coupon 5	Coupon 5
910	Lottery Pay Out - Instant	Lottery Pay Out - Instant
911	Lottery Pay Out - Online	Lottery Pay Out - Online
912	Lottery Pay Out - Other	Lottery Pay Out - Other
913	Auth Only	Split Tender
914–948	Undefined Negative	Undefined Negative
949	Miscellaneous Negative Administration	Miscellaneous Negative Administration
950	Tax 1	Sales Tax Non-Fuel
951	Tax 2	Federal Excise Tax (Non-Fuel)
952	Tax 3	StateTax (Aviation Only)
953	Tax 4	Federal Excise Tax (Aviation Only)
954	Tax 5	Miscellaneous Fuel Tax (Aviation Only)
957	Fee 1	Fee 1
958	Fee 2	Fee 2
959	Fee 3	Fee 3
960	Fee 4	Fee 4
961	Fee 5	Fee 5
962	Miscellaneous Aviation Tax	Miscellaneous Aviation Tax (Aviation Only)
963	GST/HST (Canadian) / VAT 1	GST/HST (Canadian) VAT 1
964	PST/QST (Canadian) / VAT 2	PST/QST (Canadian) VAT 2
965	SWT Rate (Canadian)	SWT Rate (Canadian)
966–998	Unidentified Administrative	Unidentified Administrative
999	Miscellaneous Administrative	Miscellaneous Administrative

Appendix B: Receipt Requirements

B.1 General Receipt Requirements

The following are industry requirements for all cards:

- Merchant Name and Location (city, state, and zip)
- Transaction Date and Time
- Account Number must be masked (no spaces), print last four digits
- Total Transaction Amount
- Surcharge or Fee, if charged
- Transaction Payment Type (Visa, Mastercard, AMEX, etc.)
- Transaction Receipt Type (Sale, Refund, Cash disbursement, etc.)
- Quantity and Description of goods or service returned or refunded.
- Authorization Code (same as Approval Number, Authorization Number, Authorization ID Response, and Approval Code)
- Signature line on the merchant copy, including return receipts (unless eligible for the No Signature Required Program or from an unattended terminal)
- Language to be printed under the signature line, such as "I agree to pay above amount according to card issuer agreement."
- Store Return Policy (near to the signature line)
- Remaining Balance (must be printed for face-to-face transactions when present in the authorization response)
- Wording indicating: Merchant Copy or Cardholder Copy

Note: The Expiration Date **must never** be printed.

B.2 Additional Receipt Requirements by Card Types

The following table lists additional requirements for specific card types. There may be other notations within the spec regarding receipts for these card types, for cards not listed in this section, or for private label cards. Additional receipt requirements may also be client-specified.

Table B-1 Additional Receipt Requirements by Card Types

Card Type	Additional Receipt Requirements
Centego	• System Trace Audit Number (STAN) • Activation receipt must indicate that the card has been activated and include the card balance.
Contact and Contactless Chip Card	• See section *7.5 EMV Receipts, p. 160*.
Discover	• Cash Over Amount • Cardholder Name as it appears on the card, if present, and signature required
EBT	• System Trace Audit Number (STAN) • Purchase Type (Food Stamp or Cash Benefit) • Debit Authorizer • Cash Back Amount • Product Description • Ledger Balance (only if not zero) **Note:** If multiple balances are returned to the POS, they should be printed.
eCommerce	• Merchant Online Address • Unique Transaction Identification Number • Purchaser Name • Description of merchandise or service
FleetCor	• Odometer • Vehicle Card Number (last four or six digits) • Items purchased, including: quantity, gallons, product description, price-per-gallon • Receipt text if returned in the response message (must be printed at the bottom of the receipt) **Note:** The Identification Number, Driver Number and Driver ID **must never** be printed.
Fleet One	• Odometer • Items purchased, including: quantity, gallons, product description • Price-per-gallon is optional **Note:** The Driver ID and PIN Number **must never** be printed.

Table B-1 Additional Receipt Requirements by Card Types (Continued)

Card Type	Additional Receipt Requirements
Heartland Gift Card	• For an **inside sale**, the remaining balance sent back to the terminal (in the HOST-RESP-AREA) must be printed on the receipt, as well as being displayed at the terminal. • For an **outside sale**, the remaining balance printed on the receipt is calculated by subtracting the completed purchase from the balance sent back in the HOST-RESP-AREA. • The format of the receipt must follow guidelines set forth by the customer.
Mastercard Fleet	• Customer Name, if available • Items purchased, including: quantity, gallons, product description, price-per-gallon **Note:** The Driver Number and ID Number **must never** be printed.
PayPal	• Print "PayPal" on the receipt.
PIN Debit	• Account Type • Cash Back Amount • Network Name/Network Verbiage
Stored Value Systems (SVS)	• System Trace Audit Number (STAN) • Activation receipt must indicate that the card has been activated and include the card balance
ValueLink	• System Trace Audit Number (STAN) • Activation receipt must indicate that the card has been activated and include the card balance
Visa	Effective April 22, 2017, merchants must provide cardholders with a receipt only in the following circumstances: • Transactions initiated by the merchant without reference to the cardholder, such as recurring and installment transactions. • When the receipt is required to make a refund, or when there are restrictive conditions of sale. • In all other transactions, when the cardholder requests it merchants must make a paper receipt available to cardholder, but may provide an electronic receipt at cardholder request. **Note:** A merchant may provide an electronic receipt without offering a paper receipt for e-commerce transactions and transactions at contactless-only terminals and for low-value, unattended, cardholder-activated transactions in all regions. An exclusion to this rule is automated fuel dispensers and ATMs, where the merchant or acquirer must offer a receipt to the cardholder for all transactions. In addition, effective April 22, 2017, Visa reduced the required period for merchants to retain receipts from 13 months to 120 days for transactions that require a fulfillment.
Visa Fleet	• Items purchased, including: quantity, gallons, product description, price-per-gallon • Odometer **Note:** The Driver ID, Driver Number and Vehicle ID **must never** be printed.

Table B-1 Additional Receipt Requirements by Card Types (Continued)

Card Type	Additional Receipt Requirements
Visa ReadyLink	• Load amount authorized • Load card service fee, if applicable **Note:** If a Load transaction is unsuccessful, must indicate the reason the transaction failed. No response from the Host is a valid reason.
Voyager Fleet	• Expiration Date • Invoice Number • Odometer must be printed on the receipt if prompted **Note:** The Driver/Vehicle Identification Number or PIN Number **must never** be printed.
WEX Fleet	• Account Number (masked with the first six digits and last four digits) • Approval Code • Expiration Date is optional • Fuel or Product Description (for non-fuel items, tax may be required) • Site Name • Physical Site Address, including: city, state/province and zip/postal code • Heartland Unit/Store Number • Heartland Terminal ID • Product Description (tax may be required for non-fuel items) • Price per unit of measure by Product Code • Quantity for each Product Code • Total amount by Product Code • Retrieval Reference Number • Vehicle Card Number / Purchase Device Sequence Number • Odometer (do not print any other prompt values)

Appendix C: State Codes / Region Codes

Non-alpha terminals use the numeric state code value.

Table C-1 State Codes

State	Numeric Value	Alpha Value
Alabama	01	AL
Alaska	02	AK
Arizona	04	AZ
Arkansas	05	AR
California	06	CA
Colorado	08	CO
Connecticut	09	CT
Delaware	10	DE
District of Columbia	11	DC
Florida	12	FL
Georgia	13	GA
Hawaii	15	HI
Idaho	16	ID
Illinois	17	IL
Indiana	18	IN
Iowa	19	IA
Kansas	20	KS
Kentucky	21	KY
Louisiana	22	LA
Maine	23	ME
Maryland	24	MD
Massachusetts	25	MA
Michigan	26	MI
Minnesota	27	MN
Mississippi	28	MS
Missouri	29	MO
Montana	30	MT
Nebraska	31	NE
Nevada	32	NV

Table C-1 State Codes (Continued)

State	Numeric Value	Alpha Value
New Hampshire	33	NH
New Jersey	34	NJ
New Mexico	35	NM
New York	36	NY
North Carolina	37	NC
North Dakota	38	ND
Ohio	39	OH
Oklahoma	40	OK
Oregon	41	OR
Pennsylvania	42	PA
Rhode Island	44	RI
South Carolina	45	SC
South Dakota	46	SD
Tennessee	47	TN
Texas	48	TX
Utah	49	UT
Vermont	50	VT
Virginia	51	VA
Washington	53	WA
West Virginia	54	WV
Wisconsin	55	WI
Wyoming	56	WY
Other US Related Codes		
American Samoa	60	AS
Guam	66	GU
Military	99	MM
Northern Mariana Island	80	MP
Puerto Rico	72	PR
Virgin Islands	78	VI

FIPS 10-4 is the source for the numeric code (n2). ISO 3166-2:1998 is the source for the alphabetic code (a2) and the description.

Table C-2 Region Codes: Canada (Province Codes)

Alpha Value (a2)	Numeric Value (n2)	Description
AB	01	Alberta
BC	02	British Columbia
MB	03	Manitoba
NB	04	New Brunswick
NF	05	Newfoundland
NS	07	Nova Scotia
NT	06	Northwest Territories
NU	13	Nunavut
ON	08	Ontario
PE	09	Prince Edward Island
QC	10	Quebec
SK	11	Saskatchewan
YT	12	Yukon Territory

Appendix D: EMV Field Definitions

This section provides a detailed definition of EMV Data fields passed between the terminal and the host when processing EMV transactions. The components of each field consist of the tag, length, and value (TLV) subfields and a field separator. The TLV fields may be in any order.

Note: Usage conditions are provided for each field (conditional, mandatory, etc.).

For all fields: If the field is received from the reader, the POS must send it to Heartland even if its usage is notated as conditional.

Differences in TLV Transmission to Host

The format of these fields is dependent upon the network platform you use (8583, Exchange, Portico, NTS, Z01, SpiDr).

Example: How do you send Amount, Authorised of $1234.56 to the host?

The TLV would be 9F0206000000123456 (hex). See the binary and ASCII Hex examples below:

Binary Example

Table D-1 POS 8583: Binary Example

Format	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
hex	9F	02	06	00	00	00	12	34	56
decimal	159	2	6	0	0	0	22	52	86
binary	10011111	00000010	00000110	00000000	00000000	00000000	00010010	00110100	01010110

ASCII Hex Example

Table D-2 Exchange, Portico, NTS, Z01, SpiDr: ASCII Hex Example

Format	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
char	'9'	'F'	'0'	'2'	'0'	'6'	'0'	'0'	'0'
hex	39	46	30	32	30	36	30	30	30
decimal	57	70	48	50	48	54	48	48	48
Format	**Byte 10**	**Byte 11**	**Byte 12**	**Byte 13**	**Byte 14**	**Byte 15**	**Byte 16**	**Byte 17**	**Byte 18**
char	'0'	'0'	'0'	'1'	'2'	'3'	'4'	'5'	'6'
hex	30	30	30	31	32	33	34	35	36
decimal	48	48	48	49	50	51	52	53	54

These are general definitions only. Refer to the network platform specifications for full usage requirements of these fields.

D.1 Additional Terminal Capabilities

Table D-3 Additional Terminal Capabilities

Tag:	9F40
Description:	This field contains the POS terminal input and output capabilities.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	5
ASCII Hex Length:	10
Example Value:	0111 0000 0000 0000 1111 0000 1011 0000 0000 0001 (binary)
Example TLV:	9F40057000F0B001 (hex)

D.2 Amount, Authorised (Numeric)

Table D-4 Amount, Authorised (Numeric)

Tag	9F02
Description:	The Amount, Authorised (Numeric) contains the authorized amount of the transaction. In the Authorization request message this is the amount known and sent to the card when calculating the Application Cryptogram. This amount may not always match the authorization amount specified elsewhere in the messaging outside of the DE55 EMV tag data if the amount was adjusted after cryptogram generation. It must contain numeric right-justified data with leading zeros. If the transaction includes a cashback amount, this field includes the purchase amount plus the cashback amount.
Source:	POS Terminal
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	n 12
Binary Length:	6
ASCII Hex Length:	12
Example Value:	12345 (decimal)
Example TLV:	9F0206000000012345 (hex)

D.3 Amount, Other (Numeric)

Table D-5 Amount, Other (Numeric)

Tag:	9F03
Description:	This field contains the cashback amount used by the chip card when calculating the Application Cryptogram. It must contain numeric right-justified data with leading zeros. If the transaction does not include a cashback amount, the Amount, Other (Numeric) field must be all zeros.
Source:	POS Terminal
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	n 12
Binary Length:	6
ASCII Hex Length:	12
Example Value:	123456 (numeric)
Example TLV:	9F03060000004000 (hex)

D.4 Application Cryptogram

Table D-6 Application Cryptogram

Tag:	9F26
Description:	This field contains the cryptogram returned by the chip card in response to the Generate AC command. There are four types of Application Cryptogram: • **ARQC (Authorization Request Cryptogram):** Used in Online processing. This is a cryptogram requested by the POS and generated by the Chip Card at the end of the first round of Card Action Analysis step for transactions requiring online authorization. It is included in the authorization request or full financial request sent to the Issuer and it allows the Issuer to verify the validity of the Chip Card and message. When validated by the Issuer, the ARQC confirms that the Chip Card has not been copied or changed. • **TC (Transaction Certificate):** A type of cryptogram generated by the card for online and offline transactions to indicate that the transaction was completed and approved by the chip card. • **AAC (Application Authentication Cryptogram):** A type of cryptogram generated by the Chip Card when a transaction is declined (at the end of offline or online declined transaction) to indicate the card declined the transaction.

Table D-6 Application Cryptogram (Continued)

Description (cont'd)	• **ARPC (Authorization Response Cryptogram):** Used in Online processing. A cryptogram generated **by the Issuer** in response to an ARQC. It is sent in the authorization response back to the acquirer Host to the POS. The POS sends this cryptogram back to the Chip Card with a response code accepting or declining the transaction. The Chip Card's receipt and validation of the ARPC confirms approval response from the Issuer and ensures that it is communicating with the valid Issuer. This cryptogram is also typically used to allow the Chip Card to reset counters.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	8
ASCII Hex Length:	16
Example Value:	0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111 0001 (binary)
Example TLV:	9F2608123456789ABCDEF1 (hex)

D.5 Application Dedicated File (ADF) Name

Table D-7 Application Dedicated File (ADF) Name

Tag:	4F
Description:	This field is used to address an application in the chip card. An ADF Name consists of a registered application provider identifier (RID) of five bytes, which is issued by the ISO/IEC 7816-5 registration authority. This is followed by a proprietary application identifier extension (PIX), which enables the application provider to differentiate between the different applications offered. The ADF Name is obtained during the application selection process. Previous versions of the EMVCo specifications refer to this tag as Application Identifier (AID) – ICC.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	5 to 16
ASCII Hex Length:	10 to 32
Example Value:	1010 0000 0000 0000 0000 0000 0000 0000 0000 0011 0001 0000 0001 0000 (binary)
Example TLV:	4F07A0000000031010 (hex)

D.6 Application Identifier (AID) – Terminal

Table D-8 Application Identifier (AID) – Terminal

Tag:	9F06
Description:	This field is used to address an application in the chip card. An AID consists of a registered application provider identifier (RID) of five bytes, which is issued by the ISO/IEC 7816-5 registration authority. This is followed by a proprietary application identifier extension (PIX) which enables the application provider to differentiate between the different applications offered. The AID is obtained during the application selection process.
Source:	POS Terminal
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	5 to 16
ASCII Hex Length:	10 to 32
Example Value:	1010 0000 0000 0000 0000 0000 0000 0000 0000 0011 0001 0000 0001 0000 (binary)
Example TLV:	9F0607A0000000031010 (hex)

D.7 Application Interchange Profile

Table D-9 Application Interchange Profile

Tag:	82
Description:	This field indicates the capabilities of the chip card to support specific functions in the application.
Source:	Chip Card
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	2
ASCII Hex Length:	4
Example Value:	0111 1100 0000 0000 (binary)
Example TLV:	82027C00 (hex)

D.8 Application Label

Table D-10 Application Label

Tag:	50
Description:	The Application Label is the mnemonic associated with the AID according to ISO/IEC 7816-5.
Source:	Chip Card
Usage:	Conditional
Format:	ans
Binary Length:	1 to 16
ASCII Hex Length:	2 to 32
Example Value:	Credit
Example TLV:	5006437265646974 (hex)

D.9 Application Preferred Name

Table D-11 Application Preferred Name

Tag:	9F12
Description:	The Application Preferred Name is the mnemonic associated with the AID.
Source:	Chip Card
Usage:	Conditional
Format:	ans
Binary Length:	1 to 16
ASCII Hex Length:	2 to 32
Example Value:	Credit
Example TLV:	9F1206437265646974 (hex)

D.10 Application Primary Account Number (PAN) Sequence Number

Table D-12 Application Primary Account Number Sequence Number

Tag:	5F34
Description:	This field contains a value maintained and supplied by the chip card. It identifies the card when multiple chip cards are associated with a single account number.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	n 2
Binary Length:	1
ASCII Hex Length:	2
Example Value:	2 (numeric)
Example TLV:	5F340102 (hex)

D.11 Application Transaction Counter (ATC)

Table D-13 Application Transaction Counter (ATC)

Tag:	9F36
Description:	This field contains the counter value maintained by the chip card. The chip card increments this value for each transaction (including failed transactions).
Source:	Chip Card
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	2
ASCII Hex Length:	4
Example Value:	0001 0010 0011 0100 (binary)
Example TLV:	9F36021234 (hex)

D.12 Application Usage Control

Table D-14 Application Usage Control

Tag:	9F07
Description:	This field indicates the Issuer's specified restrictions on the geographic usage and services allowed for the chip card application.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	2
ASCII Hex Length:	4
Example Value:	1111 1111 0000 0000 (binary)
Example TLV:	9F0702FF00 (hex)

D.13 Application Version Number (ICC)

Table D-15 Application Version Number (ICC)

Tag:	9F08
Description:	This field is the version number of the chip card application.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	2
ASCII Hex Length:	4
Example Value:	0000 1000 1010 0001 (binary)
Example TLV:	9F080208C1 (hex)

D.14 Application Version Number (Terminal)

Table D-16 Application Version Number (Terminal)

Tag:	9F09
Description:	The four-character numeric Application Version Number (Terminal) is the version number of the POS terminal payment application.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	2
ASCII Hex Length:	4
Example Value:	0001 0000 0000 0001 (binary)
Example TLV:	9F09021001 (hex)

D.15 Authorisation Response Code

Table D-17 Authorisation Response Code

Tag:	8A
Description:	The two-character Authorisation Response Code (Tag 8A) defines the disposition of an authorization request. For online transactions, the terminal should generate the value as follows: • 00 = Online approved. Should be sent to card at 2nd GENERATE AC if the host response code indicates any approval, including partial approvals or card verifications. • 05 = Online declined. Should be sent to card at 2nd GENERATE AC if the host response code indicates any decline, i.e. anything that is not an approval. Also used if a partial approval from the host is rejected at the terminal. For offline transactions, the terminal should generate the value as follows: • Y1 = Offline approved. Should be sent to host in offline approval advice if the card approves offline at 1st GENERATE AC before attempt to go online. • Z1 = Offline declined. Should be sent to host in offline decline advice if card declines offline at 1st GENERATE AC before attempt to go online, or at 2nd GENERATE AC due to bad ARPC cryptogram. • Y3 = Unable to go online, offline approved. Should be sent to card at 2nd GENERATE AC to request offline approval after failed attempt to go online. Should be sent to host in offline approval advice if the card approves offline at 2nd GENERATE AC. • Z3 = Unable to go online, offline declined. Should be sent to host in offline decline advice if the card declines offline at 2nd GENERATE AC and the transaction is not eligible for store-and-forward or stand-in processing.

Table D-17 Authorisation Response Code (Continued)

Description (cont'd):	**Note:** For American Express, the value of Tag 8A must be created by using the last two bytes received in (Tag 91) Issuer Authentication Data, if received in the authorization response.
Source:	POS Terminal
Usage:	Optional: Mandatory for offline decline advice transactions and offline approvals.
Format:	an 2
Binary Length:	2
ASCII Hex Length:	4
Example Value:	00 (alphanumeric)
Example TLV:	8A023030 (hex)

D.16 Cardholder Verification Method (CVM) Results

Table D-18 Cardholder Verification Method (CVM) Results

Tag:	9F34
Description:	This field indicates the results of the last CVM performed.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions when the result of the last CVM performed is available.
Format:	b
Binary Length:	3
ASCII Hex Length:	6
Example Value:	1010 0100 0000 0000 0000 0010 (binary)
Example TLV:	9F3403A40002 (hex)

D.17 Cryptogram Information Data (CID)

Table D-19 Cryptogram Information Data (CID)

Tag:	9F27
Description:	This field indicates the type of cryptogram generated (TC, ARQC, or AAC), why the cryptogram was generated, and actions that the chip card instructed the POS terminal to perform.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	1
ASCII Hex Length:	2
Example Value:	1000 0000 (binary)
Example TLV:	9F270180 (hex)

D.18 Customer Exclusive Data

Table D-20 Customer Exclusive Data

Tag:	9F7C
Description:	This field contains issuer proprietary data for transmission to the issuer.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contactless transactions if available.
Format:	b
Binary Length:	1 to 32
ASCII Hex Length:	2 to 64
Example Value:	0001 0010 0011 0100 0101 0110 0111 1000 (binary)
Example TLV:	9F7C0412345678 (hex)

D.19 Dedicated File Name

Table D-21 Dedicated File Name

Tag:	84
Description:	This field identifies the name of the Dedicated File as described in ISO/IEC 7816-4.
Source:	Chip Card
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	5 to 16
ASCII Hex Length:	10 to 32
Example Value:	1010 0000 0000 0000 0000 0000 0000 0000 0000 0011 0001 0000 0001 0000 (binary)
Example TLV:	8407A0000000031010 (hex)

D.20 Form Factor Indicator (FFI)

Table D-22 Form Factor Indicator

Tag:	9F6E
Description:	This field indicates the form factor of the consumer payment device and the type of contactless interface over which the transaction was conducted. The Form Factor Indicator is both an implementation and issuer option.
Source:	Chip Card
Usage:	Conditional: Mandatory for Mastercard MSD contactless only. If available, send for any EMV contactless transactions.
Format:	b
Binary Length:	4
ASCII Hex Length:	8
Example Value:	0000 0001 0000 0010 0000 0011 0000 0100 (binary)
Example TLV:	9F6E0401020304 (hex)

D.21 ICC Dynamic Number

Table D-23 ICC Dynamic Number

Tag:	9F4C
Description:	This field is a time-variant numerical value generated by the chip card.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contactless transactions.
Format:	b
Binary Length:	2 to 8
ASCII Hex Length:	4 to 16
Example Value:	0001 0010 0011 0100 0101 0110 0111 0100 (binary)
Example TLV:	9F4C0412345678 (hex)

D.22 Interface Device (IFD) Serial Number

Table D-24 Interface Device (IFD) Serial Number

Tag:	9F1E
Description:	This field contains a unique and permanent identification number assigned to the IFD by the manufacturer.
Source:	POS Terminal (from the chip card reader)
Usage:	Conditional: Mandatory for EMV contact transactions if available.
Format:	an 8
Binary Length:	8
ASCII Hex Length:	16
Example Value:	SERIAL12 (alphanumeric)
Example TLV:	9F1E0853455249414C3132 (hex)

D.23 Issuer Action Code – Default

Table D-25 Issuer Action Code – Default

Tag:	9F0D
Description:	This field specifies the issuer's conditions that cause a transaction to be rejected when the POS terminal is unable to process the transaction online (even when the transaction has already been approved online).
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact transactions.
Format:	b
Binary Length:	5
ASCII Hex Length:	10
Example Value:	1111 0000 0100 0000 0000 0000 1000 1000 0000 0000 (binary)
Example TLV:	9F0D05F040008800 (hex)

D.24 Issuer Action Code – Denial

Table D-26 Issuer Action Code – Denial

Tag:	9F0E
Description:	This field specifies the issuer's conditions that cause the denial of a transaction without an attempt to go online.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact transactions.
Format:	b
Binary Length:	5
ASCII Hex Length:	10
Example Value:	1111 1100 1111 1000 1111 1100 1111 1000 1111 0000 (binary)
Example TLV:	9F0E05FCF8FCF8F0 (hex)

D.25 Issuer Action Code – Online

Table D-27 Issuer Action Code – Online

Tag:	9F0F
Description:	This field specifies the issuer's conditions that cause a transaction to be transmitted online.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact transactions.
Format:	b
Binary Length:	5
ASCII Hex Length:	10
Example Value:	1111 1100 1111 1000 1111 1100 1111 1000 1111 0000 (binary)
Example TLV:	9F0F05FCF8FCF8F0 (hex)

D.26 Issuer Application Data

Table D-28 Issuer Application Data

Tag:	9F10
Description:	This field contains proprietary application data for transmission to the issuer.
Source:	Chip Card
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	1 to 32
ASCII Hex Length:	up to 64
Example Value:	0000 0001 0000 1010 0000 0011 0110 0000 0000 0000 0000 0000 (binary)
Example TLV:	9F1006010A03600000 (hex)

D.27 Issuer Authentication Data

Table D-29 Issuer Authentication Data

Tag:	91
Description:	This field contains data delivered to the chip card including the ARPC cryptogram for online issuer authentication. The data is in the format required by the card.
Source:	Issuer
Usage:	Optional: May be returned in the authorization response message.
Format:	b
Binary Length:	8 to 16
ASCII Hex Length:	16 to 32
Example Value:	0010 0010 0110 0011 1100 1100 0001 1100 0010 1110 1001 1100 0100 0100 0010 0000 0000 0001 0011 (binary)
Example TLV:	91102263BCC1C2D9C4420013 (hex)

D.28 Issuer Country Code

Table D-30 Issuer Country Code

Tag:	5F28
Description:	This field indicates the country of the issuer according to ISO 3166.
Source:	Chip Card
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	n 3
Binary Length:	2
ASCII Hex Length:	4
Example Value:	840 (numeric)
Example TLV:	5F28020840 (hex)

D.29 Issuer Script Results

Table D-31 Issuer Script Results

Tag:	9F5B
Description:	This field contains the results of the card issuer script update to the chip card.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact transactions when an issuer script was returned in the authorization response message.
Format:	b
Binary Length:	varies
ASCII Hex Length:	up to 40
Example Value:	0010 0000 0000 0000 0000 0000 0000 0000 0000 0000 (binary)
Example TLV:	9F5B052000000000 (hex)

D.30 Issuer Script Template 1 & 2

Table D-32 Issuer Script Template 1 & 2

Tag:	71 or 72
Description:	The Issuer Script Template 1 contains proprietary issuer data for transmission to the chip card before the second GENERATE AC command. The Issuer Script Template 2 contains proprietary issuer data for transmission to the chip card after the second GENERATE AC command.
Source:	Issuer
Usage:	Conditional: Mandatory for EMV contact transactions when received in the response message.
Format:	b
Binary Length:	1 to 127
ASCII Hex Length:	2 to 254
Example Value:	1001 1111 0001 1000 0000 0100 0001 0000 0000 0000 0000 0000 0000 0000 1000 0110 0000 1101 1000 0100 0001 1000 0000 0000 0000 0000 0000 1000 0001 0110 0010 1100 11110 0001 0111 1000 0101 1111 1100 1111 0001 1010 0110 1000 (binary)
Example TLV:	72169F180410000000860D8418000008162CE1785FCF1A68 (hex)

D.31 POS Entry Mode

Table D-33 POS Entry Mode

Tag:	9F39
Description:	This field indicates the method by which the PAN was entered, according to the first two digits of the ISO 8583:1987 POS Entry Mode.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contactless transactions.
Format:	n 2
Binary Length:	1
ASCII Hex Length:	2
Example Value:	00 (numeric)
Example TLV:	9F390100 (hex)

D.32 Terminal Action Code – Default

Table D-34 Terminal Action Code – Default

Tag:	FFC6 (HPS proprietary tag identifier)
Description:	This field specifies the acquirer's conditions that cause a transaction to be rejected when the POS terminal is unable to process the transaction online (even when the transaction has already been approved online).
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact transactions declined offline.
Format:	b
Binary Length:	5
ASCII Hex Length:	10
Example Value:	0000 0101 1111 1110 0101 0000 1011 1100 1010 0000 0000 0000 (binary)
Example TLV:	FFC605FE50BCA000 (hex)

D.33 Terminal Action Code – Denial

Table D-35 Terminal Action Code – Denial

Tag:	FFC7 (HPS proprietary tag identifier)
Description:	This field specifies the acquirer's conditions that cause the denial of a transaction without an attempt to go online.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact transactions declined offline.
Format:	b
Binary Length:	5
ASCII Hex Length:	10
Example Value:	0000 0101 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 (binary)
Example TLV:	FFC7050000000000 (hex)

D.34 Terminal Action Code – Online

Table D-36 Terminal Action Code – Online

Tag:	FFC8 (HPS proprietary tag identifier)
Description:	This field specifies the acquirer's conditions that cause a transaction to be transmitted online.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact transactions declined offline.
Format:	b
Binary Length:	5
ASCII Hex Length:	10
Example Value:	0000 0101 1111 1110 0101 0000 1011 1100 1111 1000 0000 0000 (binary)
Example TLV:	FFC805FE50BCF800 (hex)

D.35 Terminal Capabilities

Table D-37 Terminal Capabilities

Tag:	9F33
Description:	This field indicates the card data input, the cardholder verification method (CVM), and the security capabilities supported by the POS terminal.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	3
ASCII Hex Length:	6
Example Value:	0000 0001 0000 0001 0000 0001 (binary)
Example TLV:	9F3303010101 (hex)

D.36 Terminal Country Code

Table D-38 Terminal Country Code

Tag:	9F1A
Description:	This field indicates the country of the terminal, represented according to ISO 3166.
Source:	POS Terminal
Usage:	Mandatory for EMV contact, EMV contactless transactions.
Format:	n 3
Binary Length:	2
ASCII Hex Length:	3
Example Value:	840 (numeric)
Example TLV:	9F1A020840 (hex)

D.37 Terminal Type

Table D-39 Terminal Type

Tag:	9F35
Description:	The two-character numeric Terminal Type indicates the environment of the POS terminal, its communications capability, and its operational control.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	n 2
Binary Length:	1
ASCII Hex Length:	2
Example Value:	22 (numeric)
Example TLV:	9F350122 (hex)

D.38 Terminal Verification Results (TVR)

Table D-40 Terminal Verification Results (TVR)

Tag:	95
Description:	This field contains a series of indicators set by the POS terminal recording both offline and online processing results.
Source:	POS Terminal
Usage:	Mandatory for chip card transactions (contact and contactless)
Format:	b
Binary Length:	5
ASCII Hex Length:	10
Example Value:	0000 0000 0000 0000 0000 0100 1000 0000 0000 0000 (binary)
Example TLV:	95050000048000 (hex)

D.39 Third Party Data

.

Table D-41 Third Party Data

Tag:	9F6E
Description:	The Third Party Data contains proprietary data from a third party.
Source:	Issuer
Usage:	Mandatory for Mastercard contactless transactions if available.
Format:	b
Binary Length:	5 to 32
ASCII Hex Length:	10 to 64
Example Value:	0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 (binary)
Example TLV:	9F6E05123456789A (hex)

D.40 Transaction Currency Code

Table D-42 Transaction Currency Code

Tag:	5F2A
Description:	This field contains the currency code of the transaction according to ISO 4217.
Source:	POS Terminal
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	n 3
Binary Length:	2
ASCII Hex Length:	4
Example Value:	840 (numeric)
Example TLV:	5F2A020840 (hex)

D.41 Transaction Date

Table D-43 Transaction Data

Tag:	9A
Description:	This field contains the local date used to generate the cryptogram.
Source:	POS Terminal
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	n 6 (YYMMDD)
Binary Length:	3
ASCII Hex Length:	6
Example Value:	121231 (numeric)
Example TLV:	9A03121231 (hex)

D.42 Transaction Sequence Counter

Table D-44 Transaction Sequence Counter

Tag:	9F41
Description:	This field uniquely identifies each transaction on a POS terminal. The Transaction Sequence Counter value subfield is right-justified with leading zeros.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	n 4 to 8
Binary Length:	2 to 4
ASCII Hex Length:	4 to 8
Example Value:	435 (numeric)
Example TLV:	9F410400000435 (hex)

D.43 Transaction Status Information

Table D-45 Transaction Status Information

Tag:	9B
Description:	This field contains the functions performed in the transaction.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	2
ASCII Hex Length:	4
Example Value:	0100 1000 0000 0000 (binary)
Example TLV:	9B024800 (hex)

D.44 Transaction Time

Table D-46 Transaction Time

Tag:	9F21
Description:	This subfield contains the local time that the transaction was authorized.
Source:	POS Terminal
Usage:	Conditional: Mandatory for EMV contact and EMV contactless transactions.
Format:	n 6 (HHMMSS)
Binary Length:	3
ASCII Hex Length:	6
Example Value:	123456 (numeric)
Example TLV:	9F2103123456 (hex)

D.45 Transaction Type

Table D-47 Transaction Type

Tag:	9C
Description:	This field indicates the type of financial transaction as represented by the first two digits of the ISO 8583:1987 Processing Code.
Source:	POS Terminal
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	n 2
Binary Length:	1
ASCII Hex Length:	2
Example Value:	00 (numeric)
Example TLV:	9C0100 (hex)

D.46 Unpredictable Number

Table D-48 Unpredictable Number

Tag:	9F37
Description:	This field is randomly generated by the POS Terminal and is used to provide variability and uniqueness to the cryptogram.
Source:	POS Terminal
Usage:	Mandatory for EMV contact and EMV contactless transactions.
Format:	b
Binary Length:	4
ASCII Hex Length:	8
Example Value:	0001 0010 0011 0100 0101 0110 0111 1000 (binary)
Example TLV:	9F370412345678 (hex)

Appendix E: EMV PDL Data Examples

The following example does not include any host specific "wrapper", but rather only depicts the exchange of the actual EMV PDL data between the POS and the host.

Note: This is example data only that should not be used for certification or in production.

Table E-1 EMV PDL Data Examples

POS		⇔	Host	
Table 10 Request (Versions and Flags)		⇨		
Field	**Value**			
EMV PDL PARAMETER TYPE	06			
EMV PDL TABLE ID	10			
EMV PDL CARD TYPE	<2 spaces>			
EMV PDL PARAMETER VERSION	001			
EMV PDL BLOCK SEQUENCE NUMBER	00			
		⇦	**Table 10 Response (Versions and Flags)**	
			Field	**Value**
			EMV PDL PARAMETER VERSION	001
			EMV PDL BLOCK SEQUENCE NUMBER	00
			EMV PDL TABLE ID	10
			EMV PDL CARD TYPE	<2 spaces>
			EMV PDL END-OF-TABLE FLAG	Y
			EMV PDL ENABLED	Y
			EMV PDL TABLE ID 30 VERSION	001
			EMV PDL TABLE ID 30 FLAG	Y
			EMV PDL NUMBER OF CARD TYPES	04

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		Visa	
		EMV PDL CARD TYPE	01
		EMV PDL TABLE ID 40 VERSION	001
		EMV PDL TABLE ID 40 FLAG	Y
		EMV PDL TABLE ID 50 VERSION	001
		EMV PDL TABLE ID 50 FLAG	Y
		EMV PDL TABLE ID 60 VERSION	001
		EMV PDL TABLE ID 60 FLAG	Y
		Mastercard	
		EMV PDL CARD TYPE	02
		EMV PDL TABLE ID 40 VERSION	001
		EMV PDL TABLE ID 40 FLAG	Y
		EMV PDL TABLE ID 50 VERSION	001
		EMV PDL TABLE ID 50 FLAG	Y
		EMV PDL TABLE ID 60 VERSION	001
		EMV PDL TABLE ID 60 FLAG	Y
		American Express	
		EMV PDL CARD TYPE	03
		EMV PDL TABLE ID 40 VERSION	001
		EMV PDL TABLE ID 40 FLAG	Y
		EMV PDL TABLE ID 50 VERSION	001
		EMV PDL TABLE ID 50 FLAG	Y
		EMV PDL TABLE ID 60 VERSION	001
		EMV PDL TABLE ID 60 FLAG	Y
		Discover	
		EMV PDL CARD TYPE	04
		EMV PDL TABLE ID 40 VERSION	001
		EMV PDL TABLE ID 40 FLAG	Y
		EMV PDL TABLE ID 50 VERSION	001
		EMV PDL TABLE ID 50 FLAG	Y
		EMV PDL TABLE ID 60 VERSION	001
		EMV PDL TABLE ID 60 FLAG	Y

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th>Host</th></tr>
<tr><td colspan="2">Table 10 Confirmation Request
(Versions and Flags)</td><td rowspan="6">⇨</td><td rowspan="6"></td></tr>
<tr><td>Field</td><td>Value</td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>10</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td><2 spaces></td></tr>
<tr><td>EMV PDL PARAMETER VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td colspan="2" rowspan="6"></td><td rowspan="6">⇦</td><td colspan="2">Table 10 Confirmation Response
(Versions and Flags)</td></tr>
<tr><td>Field</td><td>Value</td></tr>
<tr><td>EMV PDL PARAMETER VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>10</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td><2 spaces></td></tr>
<tr><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
<tr><td colspan="2">Table 30 Request
(Terminal Data)</td><td rowspan="6">⇨</td><td rowspan="6"></td></tr>
<tr><td>Field</td><td>Value</td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>06</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>30</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td><2 spaces></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td rowspan="14"></td><td rowspan="14">⇦</td><td colspan="2">Table 30 Response
(Terminal Data)</td></tr>
<tr><td>Field</td><td>Value</td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>30</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td><2 spaces></td></tr>
<tr><td>EMV PDL END-OF-TABLE FLAG</td><td>Y</td></tr>
<tr><td>EMV PDL TABLE DATA BLOCK LENGTH</td><td>023</td></tr>
<tr><td>EMV PDL TERMINAL TYPE</td><td>22</td></tr>
<tr><td>EMV PDL ADDITIONAL TERMINAL CAPABILITIES</td><td>F000F0A001</td></tr>
<tr><td>EMV PDL TERMINAL COUNTRY CODE</td><td>840</td></tr>
<tr><td>EMV PDL TRANSACTION CURRENCY CODE</td><td>840</td></tr>
<tr><td>EMV PDL TRANSACTION CURRENCY EXPONENT</td><td>2</td></tr>
<tr><td>EMV PDL TRANSACTION REFERENCE CURRENCY CODE</td><td>840</td></tr>
<tr><td>EMV PDL TRANSACTION REFERENCE CURRENCY EXPONENT</td><td>2</td></tr>
<tr><td colspan="2">Table 30 Confirmation Request
(Terminal Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>30</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td><2 spaces></td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th>Host</th></tr>
<tr><td></td><td>⇦</td><td>
<table>
<tr><th colspan="2">Table 30 Confirmation Response
(Terminal Data)</th></tr>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>30</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td><2 spaces></td></tr>
<tr><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table>
</td></tr>
<tr><td>
<table>
<tr><th colspan="2">Table 40 Request
(Visa Contact Card Data)</th></tr>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>06</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>40</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>01</td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td></tr>
</table>
</td><td>⇨</td><td></td></tr>
<tr><td></td><td>⇦</td><td>
<table>
<tr><th colspan="2">Table 40 Response
(Visa Contact Card Data)</th></tr>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>40</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>01</td></tr>
<tr><td>EMV PDL END-OF-TABLE FLAG</td><td>Y</td></tr>
<tr><td>EMV PDL TABLE DATA BLOCK LENGTH</td><td>374</td></tr>
<tr><td>EMV PDL AID COUNT</td><td>02</td></tr>
<tr><th colspan="2">Visa Credit/Debit</th></tr>
<tr><td>EMV PDL APPLICATION IDENTIFIER (AID)</td><td>A0000000031010 + <18 spaces></td></tr>
<tr><td>EMV PDL APPLICATION SELECTION INDICATOR</td><td>1</td></tr>
<tr><td>EMV PDL APPLICATION VERSION NUMBER</td><td>0096</td></tr>
</table>
</td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		EMV PDL APPLICATION COUNTRY CODE	<3 spaces>
		EMV PDL TRANSACTION TYPES	8000
		EMV PDL TERMINAL CAPABILIITES	E0B8C8
		EMV PDL TERMINAL FLOOR LIMIT	000000000000
		EMV PDL THRESHOLD VALUE FOR BIASED RANDOM SELECTION	000000000000
		EMV PDL TARGET PERCENTAGE TO BE USED FOR RANDOM SELECTION	00
		EMV PDL MAXIMUM TARGET PERCENTAGE TO BE USED FOR BIASED RANDOM SELECTION	00
		EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL	0010000000
		EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE	DC4004F800
		EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT	DC4000A800
		EMV PDL TERMINAL RISK MANAGEMENT DATA	<16 spaces>
		EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)	<32 spaces>
		EMV PDL DEFAULT DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)	9F3704 + <26 spaces>
		Visa Electron	
		EMV PDL APPLICATION IDENTIFIER (AID)	A0000000032010 + <18 spaces>
		EMV PDL APPLICATION SELECTION INDICATOR	1
		EMV PDL APPLICATION VERSION NUMBER	0096
		EMV PDL APPLICATION COUNTRY CODE	<3 spaces>
		EMV PDL TRANSACTION TYPES	8000
		EMV PDL TERMINAL CAPABILIITES	E0B8C8
		EMV PDL TERMINAL FLOOR LIMIT	000000000000
		EMV PDL THRESHOLD VALUE FOR BIASED RANDOM SELECTION	000000000000

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL TARGET PERCENTAGE TO BE USED FOR RANDOM SELECTION</td><td>00</td></tr>
<tr><td></td><td></td><td>EMV PDL MAXIMUM TARGET PERCENTAGE TO BE USED FOR BIASED RANDOM SELECTION</td><td>00</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL</td><td>0010000000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE</td><td>DC4004F800</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT</td><td>DC4000A800</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td><16 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)</td><td><32 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)</td><td>9F3704
+ <26 spaces></td></tr>
<tr><td colspan="2">Table 40 Confirmation Request
(Visa Contact Card Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>40</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>01</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 40 Confirmation Response
(Visa Contact Card Data)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID</td><td>40</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE</td><td>01</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host

Table 40 Request (Mastercard Contact Card Data)

Field	Value
EMV PDL PARAMETER TYPE	06
EMV PDL TABLE ID	40
EMV PDL CARD TYPE	02
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01

⇨

⇦

Table 40 Response (Mastercard Contact Card Data)

Field	Value
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01
EMV PDL TABLE ID	40
EMV PDL CARD TYPE	02
EMV PDL END-OF-TABLE FLAG	Y
EMV PDL TABLE DATA BLOCK LENGTH	188
EMV PDL AID COUNT	01
Mastercard Credit/Debit	
EMV PDL APPLICATION IDENTIFIER (AID)	A0000000041010 + <18 spaces>
EMV PDL APPLICATION SELECTION INDICATOR	1
EMV PDL APPLICATION VERSION NUMBER	0002
EMV PDL APPLICATION COUNTRY CODE	<3 spaces>
EMV PDL TRANSACTION TYPES	8000
EMV PDL TERMINAL CAPABILIITES	E0F8C8
EMV PDL TERMINAL FLOOR LIMIT	000000020000
EMV PDL THRESHOLD VALUE FOR BIASED RANDOM SELECTION	000000000000
EMV PDL TARGET PERCENTAGE TO BE USED FOR RANDOM SELECTION	00

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL MAXIMUM TARGET PERCENTAGE TO BE USED FOR BIASED RANDOM SELECTION</td><td>00</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL</td><td>0000000000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE</td><td>FC50BCF800</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT</td><td>FC50BCA000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td><16 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)</td><td><32 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)</td><td>9F3704 + <26 spaces></td></tr>
<tr><td colspan="2">Table 40 Confirmation Request (Mastercard Contact Card Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>40</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>02</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td>⇦</td><td colspan="2">Table 40 Confirmation Response (Mastercard Contact Card Data)</td></tr>
<tr><td></td><td></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL TABLE ID</td><td>40</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL CARD TYPE</td><td>02</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th colspan="2">POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td colspan="2">Table 40 Request
(American Express Contact Card Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>06</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>40</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>03</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 40 Response
(American Express Contact Card Data)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID</td><td>40</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE</td><td>03</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL END-OF-TABLE FLAG</td><td>Y</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE DATA BLOCK LENGTH</td><td>188</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL AID COUNT</td><td>01</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2">American Express Credit/Debit</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL APPLICATION IDENTIFIER (AID)</td><td>A00000002501 + <20 spaces></td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL APPLICATION SELECTION INDICATOR</td><td>1</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL APPLICATION VERSION NUMBER</td><td>0001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL APPLICATION COUNTRY CODE</td><td><3 spaces></td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TRANSACTION TYPES</td><td>8000</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TERMINAL CAPABILIITES</td><td>E0B8C8</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TERMINAL FLOOR LIMIT</td><td>000000000000</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL THRESHOLD VALUE FOR BIASED RANDOM SELECTION</td><td>000000000000</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TARGET PERCENTAGE TO BE USED FOR RANDOM SELECTION</td><td>00</td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL MAXIMUM TARGET PERCENTAGE TO BE USED FOR BIASED RANDOM SELECTION</td><td>00</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL</td><td>0000000000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE</td><td>C800000000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT</td><td>C800000000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td><16 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)</td><td><32 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)</td><td>9F3704
+ <26 spaces></td></tr>
<tr><td colspan="2">Table 40 Confirmation Request
(American Express Contact Card Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>40</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>03</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 40 Confirmation Response
(American Express Contact Card Data)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID</td><td>40</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE</td><td>03</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host
Table 40 Request (Discover Contact Card Data)	⇨	
Field / **Value**		
EMV PDL PARAMETER TYPE: 06		
EMV PDL TABLE ID: 40		
EMV PDL CARD TYPE: 04		
EMV PDL TABLE VERSION: 001		
EMV PDL BLOCK SEQUENCE NUMBER: 01		
	⇦	**Table 40 Response (Discover Contact Card Data)**
		Field / **Value**
		EMV PDL TABLE VERSION: 001
		EMV PDL BLOCK SEQUENCE NUMBER: 01
		EMV PDL TABLE ID: 40
		EMV PDL CARD TYPE: 04
		EMV PDL END-OF-TABLE FLAG: Y
		EMV PDL TABLE DATA BLOCK LENGTH: 188
		EMV PDL AID COUNT: 01
		Discover Credit/Debit
		EMV PDL APPLICATION IDENTIFIER (AID): A0000001523010 + <18 spaces>
		EMV PDL APPLICATION SELECTION INDICATOR: 1
		EMV PDL APPLICATION VERSION NUMBER: 0001
		EMV PDL APPLICATION COUNTRY CODE: <3 spaces>
		EMV PDL TRANSACTION TYPES: 8000
		EMV PDL TERMINAL CAPABILIITES: E0F8C8
		EMV PDL TERMINAL FLOOR LIMIT: 000000030000
		EMV PDL THRESHOLD VALUE FOR BIASED RANDOM SELECTION: 000000000000
		EMV PDL TARGET PERCENTAGE TO BE USED FOR RANDOM SELECTION: 00

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL MAXIMUM TARGET PERCENTAGE TO BE USED FOR BIASED RANDOM SELECTION</td><td>00</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL</td><td>0010000000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE</td><td>FCE09CF800</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT</td><td>DC00002000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td><16 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)</td><td><32 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)</td><td>9F3704 + <26 spaces></td></tr>
<tr><td colspan="2">Table 40 Confirmation Request (Discover Contact Card Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>40</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>04</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 40 Confirmation Response (Discover Contact Card Data)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID</td><td>40</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE</td><td>04</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host
Table 50 Request (Visa Contactless Card Data)	⇨	
Field / **Value**		
EMV PDL PARAMETER TYPE: 06		
EMV PDL TABLE ID: 50		
EMV PDL CARD TYPE: 01		
EMV PDL TABLE VERSION: 001		
EMV PDL BLOCK SEQUENCE NUMBER: 01		
	⇦	**Table 50 Response (Visa Contactless Card Data)**
		Field / **Value**
		EMV PDL TABLE VERSION: 001
		EMV PDL BLOCK SEQUENCE NUMBER: 01
		EMV PDL TABLE ID: 50
		EMV PDL CARD TYPE: 01
		EMV PDL END-OF-TABLE FLAG: Y
		EMV PDL TABLE DATA BLOCK LENGTH: 350
		EMV PDL AID COUNT: 02
		Visa Credit/Debit
		EMV PDL APPLICATION IDENTIFIER (AID): A0000000031010 + <18 spaces>
		EMV PDL APPLICATION SELECTION INDICATOR: 1
		EMV PDL APPLICATION VERSION NUMBER: 0096
		EMV PDL CONTACTLESS MAGSTRIPE APPLICATION VERSION NUMBER: 0001
		EMV PDL APPLICATION COUNTRY CODE: <3 spaces>
		EMV PDL TRANSACTION TYPES: 8000
		EMV PDL TERMINAL CAPABILIITES: E028C8
		EMV PDL TERMINAL CONTACTLESS FLOOR LIMIT: 000000000000
		EMV PDL TERMINAL CVM REQUIRED LIMIT: 000000005000

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		EMV PDL TERMINAL CONTACTLESS TRANSACTION LIMIT	999999999999
		EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL	0010000000
		EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE	DC4004F800
		EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT	DC4000A800
		EMV PDL TERMINAL TRANSACTION QUALIFIERS (TTQ)	B2004000
		EMV PDL TERMINAL RISK MANAGEMENT DATA	<16 spaces>
		EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)	<32 spaces>
		Visa Electron	
		EMV PDL APPLICATION IDENTIFIER (AID)	A0000000031010 + <18 spaces>
		EMV PDL APPLICATION SELECTION INDICATOR	1
		EMV PDL APPLICATION VERSION NUMBER	0096
		EMV PDL CONTACTLESS MAGSTRIPE APPLICATION VERSION NUMBER	0001
		EMV PDL APPLICATION COUNTRY CODE	<3 spaces>
		EMV PDL TRANSACTION TYPES	8000
		EMV PDL TERMINAL CAPABILIITES	E028C8
		EMV PDL TERMINAL CONTACTLESS FLOOR LIMIT	000000000000
		EMV PDL TERMINAL CVM REQUIRED LIMIT	000000005000
		EMV PDL TERMINAL CONTACTLESS TRANSACTION LIMIT	999999999999
		EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL	0010000000
		EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE	DC4004F800
		EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT	DC4000A800

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL TRANSACTION QUALIFIERS (TTQ)</td><td>B2004000</td></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td><16 spaces></td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)</td><td><32 spaces></td></tr>
<tr><td colspan="2">Table 50 Confirmation Request
(Visa Contactless Card Data)
<table><tr><th>Field</th><th>Value</th></tr><tr><td>EMV PDL PARAMETER TYPE</td><td>07</td></tr><tr><td>EMV PDL TABLE ID</td><td>50</td></tr><tr><td>EMV PDL CARD TYPE</td><td>01</td></tr><tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr><tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr></table></td><td>⇨</td><td colspan="2"></td></tr>
<tr><td></td><td>⇦</td><td colspan="2">Table 50 Confirmation Response
(Visa Contactless Card Data)
<table><tr><th>Field</th><th>Value</th></tr><tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr><tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr><tr><td>EMV PDL TABLE ID</td><td>50</td></tr><tr><td>EMV PDL CARD TYPE</td><td>01</td></tr><tr><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr></table></td></tr>
<tr><td colspan="2">Table 50 Request
(Mastercard Contactless Card Data)
<table><tr><th>Field</th><th>Value</th></tr><tr><td>EMV PDL PARAMETER TYPE</td><td>06</td></tr><tr><td>EMV PDL TABLE ID</td><td>50</td></tr><tr><td>EMV PDL CARD TYPE</td><td>02</td></tr><tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr><tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td></tr></table></td><td>⇨</td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
	⇦	**Table 50 Response (Mastercard Contactless Card Data)**	
		Field	**Value**
		EMV PDL TABLE VERSION	001
		EMV PDL BLOCK SEQUENCE NUMBER	01
		EMV PDL TABLE ID	50
		EMV PDL CARD TYPE	02
		EMV PDL END-OF-TABLE FLAG	Y
		EMV PDL TABLE DATA BLOCK LENGTH	176
		EMV PDL AID COUNT	01
		Mastercard Credit/Debit	
		EMV PDL APPLICATION IDENTIFIER (AID)	A0000000041010 + <18 spaces>
		EMV PDL APPLICATION SELECTION INDICATOR	1
		EMV PDL APPLICATION VERSION NUMBER	0002
		EMV PDL CONTACTLESS MAGSTRIPE APPLICATION VERSION NUMBER	0001
		EMV PDL APPLICATION COUNTRY CODE	<3 spaces>
		EMV PDL TRANSACTION TYPES	8000
		EMV PDL TERMINAL CAPABILIITES	E068C8
		EMV PDL TERMINAL CONTACTLESS FLOOR LIMIT	000000020000
		EMV PDL TERMINAL CVM REQUIRED LIMIT	000000005000
		EMV PDL TERMINAL CONTACTLESS TRANSACTION LIMIT	999999999999
		EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL	0000000000
		EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE	FC509C8800
		EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT	FC509C8800
		EMV PDL TERMINAL TRANSACTION QUALIFIERS (TTQ)	B6000000

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td>6CF8000000000000</td></tr>
<tr><td></td><td></td><td>EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)</td><td><32 spaces></td></tr>
<tr><td colspan="2">Table 50 Confirmation Request
(Mastercard Contactless Card Data)
Field / Value
EMV PDL PARAMETER TYPE: 07
EMV PDL TABLE ID: 50
EMV PDL CARD TYPE: 02
EMV PDL TABLE VERSION: 001
EMV PDL BLOCK SEQUENCE NUMBER: 00</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 50 Confirmation Response
(Mastercard Contactless Card Data)
Field / Value
EMV PDL PARAMETER VERSION: 001
EMV PDL BLOCK SEQUENCE NUMBER: 00
EMV PDL TABLE ID: 50
EMV PDL CARD TYPE: 02
EMV PDL CONFIRMATION FLAG: Y</td></tr>
<tr><td colspan="2">Table 50 Request
(American Express Contactless Card Data)
Field / Value
EMV PDL PARAMETER TYPE: 06
EMV PDL TABLE ID: 50
EMV PDL CARD TYPE: 03
EMV PDL TABLE VERSION: 001
EMV PDL BLOCK SEQUENCE NUMBER: 01</td><td>⇨</td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
	⇦	**Table 50 Response (American Express Contactless Card Data)**	
		Field	**Value**
		EMV PDL TABLE VERSION	001
		EMV PDL BLOCK SEQUENCE NUMBER	01
		EMV PDL TABLE ID	50
		EMV PDL CARD TYPE	03
		EMV PDL END-OF-TABLE FLAG	Y
		EMV PDL TABLE DATA BLOCK LENGTH	176
		EMV PDL AID COUNT	01
		American Express Credit/Debit	
		EMV PDL APPLICATION IDENTIFIER (AID)	A00000002501 + <20 spaces>
		EMV PDL APPLICATION SELECTION INDICATOR	1
		EMV PDL APPLICATION VERSION NUMBER	0001
		EMV PDL CONTACTLESS MAGSTRIPE APPLICATION VERSION NUMBER	0001
		EMV PDL APPLICATION COUNTRY CODE	<3 spaces>
		EMV PDL TRANSACTION TYPES	8000
		EMV PDL TERMINAL CAPABILIITES	E0E8C8
		EMV PDL TERMINAL CONTACTLESS FLOOR LIMIT	000000000000
		EMV PDL TERMINAL CVM REQUIRED LIMIT	000000005000
		EMV PDL TERMINAL CONTACTLESS TRANSACTION LIMIT	999999999999
		EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL	0000000000
		EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE	C400000000
		EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT	DC50840000
		EMV PDL TERMINAL TRANSACTION CAPABILIITES	D8F00000

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th colspan="2">POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td><16 spaces></td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)</td><td><32 spaces></td></tr>
<tr><td colspan="2">Table 50 Confirmation Request
(American Express Contactless Card Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>50</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>03</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 50 Confirmation Response
(American Express Contactless Card Data)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID</td><td>50</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE</td><td>03</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
<tr><td colspan="2">Table 50 Request
(Discover Contactless Card Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>06</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>50</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>04</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td><td></td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
	⇦	**Table 50 Response (Discover Contactless Card Data)**	
		Field	**Value**
		EMV PDL TABLE VERSION	001
		EMV PDL BLOCK SEQUENCE NUMBER	01
		EMV PDL TABLE ID	50
		EMV PDL CARD TYPE	04
		EMV PDL END-OF-TABLE FLAG	Y
		EMV PDL TABLE DATA BLOCK LENGTH	176
		EMV PDL AID COUNT	01
		Discover Credit/Debit	
		EMV PDL APPLICATION IDENTIFIER (AID)	A0000003241010 + <18 spaces>
		EMV PDL APPLICATION SELECTION INDICATOR	1
		EMV PDL APPLICATION VERSION NUMBER	0001
		EMV PDL CONTACTLESS MAGSTRIPE APPLICATION VERSION NUMBER	0001
		EMV PDL APPLICATION COUNTRY CODE	<3 spaces>
		EMV PDL TRANSACTION TYPES	8000
		EMV PDL TERMINAL CAPABILIITES	E068C8
		EMV PDL TERMINAL CONTACTLESS FLOOR LIMIT	000000000000
		EMV PDL TERMINAL CVM REQUIRED LIMIT	000000005000
		EMV PDL TERMINAL CONTACTLESS TRANSACTION LIMIT	999999999999
		EMV PDL TERMINAL ACTION CODE (TAC) - DENIAL	0010000000
		EMV PDL TERMINAL ACTION CODE (TAC) - ONLINE	FCE09CF800
		EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT	DC00002000
		EMV PDL TERMINAL TRANSACTION QUALIFIERS (TTQ)	96000000

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th colspan="2">POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td><16 spaces></td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)</td><td><32 spaces></td></tr>
<tr><td colspan="2">Table 50 Confirmation Request
(Discover Contactless Card Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>50</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>04</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 50 Confirmation Response
(Discover Contactless Card Data)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID</td><td>50</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE</td><td>04</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
<tr><td colspan="2">Table 60 Request
(Visa Public Key Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>06</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>01</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td><td></td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
	⇦	**Table 60 Response (Visa Public Key Data)**	
		Field	**Value**
		EMV PDL TABLE VERSION	001
		EMV PDL BLOCK SEQUENCE NUMBER	01
		EMV PDL TABLE ID	60
		EMV PDL CARD TYPE	01
		EMV PDL END-OF-TABLE FLAG	N
		EMV PDL TABLE DATA BLOCK LENGTH	875
		EMV PDL KEY COUNT	04
		Visa 1024-Bit Key (Expired)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000003
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	01
		EMV PDL KEY STATUS	E
		VISA 1152-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000003
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	07
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0288

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	A89F25A56FA6DA258C8CA8B40427D927B4A1EB4D7EA326BBB12F97DED70AE5E4480FC9C5E8A972177110A1CC318D06D2F8F5C4844AC5FA79A4DC470BB11ED635699C17081B90F1B984F12E92C1C529276D8AF8EC7F28492097D8CD5BECEA16FE4088F6CFAB4A1B42328A1B996F9278B0B7E3311CA5EF856C2F888474B83612A82E4E00D0CD4069A6783140433D50725F
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	B4BC56CC4E88324932CBC643D6898F6FE593B172
		Visa 1408-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000003
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	08
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0352

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	D9FD6ED75D51D 0E30664BD15702 3EAA1FFA871E4D A65672B863D255 E81E137A51DE4F 72BCC9E44ACE1 2127F87E263D3A F9DD9CF35CA4A 7B01E907000BA8 5D24954C2FCA30 74825DDD4C0C8 F186CB020F683E 02F2DEAD396913 3F06F7845166AC EB57CA0FC26034 45469811D293BF EFBAFAB57631B3 DD91E796BF850A 25012F1AE38F05 AA5C4D6D03B1D C2E56861278593 8BBC9B3CD3A91 0C1DA55A5A9218 ACE0F7A2128775 2682F15832A678 D6E1ED0B
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	20D213126955DE 205ADC2FD2822B D22DE21CF9A8
		Visa 1984-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000003
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	09
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0496
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	9D912248DE0A4E 39C1A7DDE3F6D 2588992C1A4095 AFBD1824D1BA7 4847F2BC4926D2 EFD904B4B54954 CD1

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host
Table 60 Request (Visa Public Key Data Continued)	⇨	
Field / **Value**		
EMV PDL PARAMETER TYPE: 06		
EMV PDL TABLE ID: 60		
EMV PDL CARD TYPE: 01		
EMV PDL TABLE VERSION: 001		
EMV PDL BLOCK SEQUENCE NUMBER: 02		
	⇦	**Table 60 Response (Visa Public Key Data Continued)**
		Field / **Value**
		EMV PDL TABLE VERSION: 001
		EMV PDL BLOCK SEQUENCE NUMBER: 02
		EMV PDL TABLE ID: 60
		EMV PDL CARD TYPE: 01
		EMV PDL END-OF-TABLE FLAG: Y
		EMV PDL TABLE DATA BLOCK LENGTH: 453

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS</td><td>89A54C5D117965
4F8F9B0D2AB5F0
357EB642FEDA95
D3912C6576945F
AB897E7062CAA4
4A4AA06B8FE6E3
DBA18AF6AE3738
E30429EE9BE034
27C9D64F695FA8
CAB4BFE376853E
A34AD1D76BFCA
D15908C077FFE6
DC5521ECEF5D2
78A96E26F57359
FFAEDA19434B93
7F1AD999DC5C4
1EB11935B44C18
100E857F431A4A
5A6BB65114F174
C2D7B59FDF237
D6BB1DD0916E6
44D709DED56481
477C75D95CDD6
8254615F7740EC
07F330AC5D67BC
D75BF23D28A140
826C026DBDE971
A37CD3EF9B8DF
644AC385010501
EFC6509D7A41</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT</td><td>03</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM</td><td>1FF80A40173F52
D7D27E0F26A146
A1C8CCB29046</td></tr>
<tr><td colspan="2">Table 60 Confirmation Request
(Visa Public Key Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>01</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host
	⇦	**Table 60 Confirmation Response (Visa Public Key Data)**

Field	Value
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	00
EMV PDL TABLE ID	60
EMV PDL CARD TYPE	01
EMV PDL CONFIRMATION FLAG	Y

⇨

Table 60 Request (Mastercard Public Key Data)

Field	Value
EMV PDL PARAMETER TYPE	06
EMV PDL TABLE ID	60
EMV PDL CARD TYPE	02
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01

⇦

Table 60 Response (Mastercard Public Key Data)

Field	Value
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01
EMV PDL TABLE ID	60
EMV PDL CARD TYPE	02
EMV PDL END-OF-TABLE FLAG	N
EMV PDL TABLE DATA BLOCK LENGTH	875
EMV PDL KEY COUNT	03

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		Mastercard 1152-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000003
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	04
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0288
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	A6DA428387A502D7DDFB7A74D3F412BE762627197B25435B7A81716A700157DDD06F7CC99D6CA28C2470527E2C03616B9C59217357C2674F583B3BA5C7DCF2838692D023E3562420B4615C439CA97C44DC9A249CFCE7B3BFB22F68228C3AF13329AA4A613CF8DD853502373D62E49AB256D2BC17120E54AEDCED6D96A4287ACC5C04677D4A5A320DB8BEE2F775E5FEC5
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	381A035DA58B482EE2AF75F4C3F2CA469BA4AA6C

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		Mastercard 1408-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000004
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	05
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0352
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	B8048ABC30C90 D976336543E3FD 7091C8FE4800DF 820ED55E7E9481 3ED00555B573FE CA3D84AF6131A6 51D66CFF4284FB 13B635EDD0EE40 176D8BF04B7FD1 C7BACF9AC7327 DFAA8AA72D10D B3B8E70B2DDD8 11CB4196525EA3 86ACC33C0D9D4 575916469C4E4F 53E8E1C912CC61 8CB22DDE7C356 8E90022E6BBA77 0202E4522A2DD6 23D180E215BD1D 1507FE3DC90CA3 10D27B3EFCCD8 F83DE3052CAD1 E48938C68D095A AC91B5F37E28BB 49EC7ED597
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	EBFA0D5D06D8C E702DA3EAE8907 01D45E274C845

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		Mastercard 1984-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000004
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	06
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0496
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	CB26FC830B4378 5B2BCE37C81ED 334622F9622F4C 89AAE641046B23 53433883F307FB7 C974162DA72F7A 4EC75D9D657336
Table 60 Request (Mastercard Public Key Data Continued)	⇨		
Field / **Value**			
EMV PDL PARAMETER TYPE: 06			
EMV PDL TABLE ID: 60			
EMV PDL CARD TYPE: 01			
EMV PDL TABLE VERSION: 001			
EMV PDL BLOCK SEQUENCE NUMBER: 02			
	⇦	**Table 60 Response (Mastercard Public Key Data Continued)**	
		Field	**Value**
		EMV PDL TABLE VERSION	001
		EMV PDL BLOCK SEQUENCE NUMBER	02
		EMV PDL TABLE ID	60
		EMV PDL CARD TYPE	01
		EMV PDL END-OF-TABLE FLAG	Y
		EMV PDL TABLE DATA BLOCK LENGTH	440

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS</td><td>865B8D3023D3D6
45667625C9A07A
6B7A137CF0C641
98AE38FC238006
FB2603F41F4F3B
B9DA1347270F2F
5D8C606E420958
C5F7D50A71DE30
142F70DE468889
B5E3A08695B938
A50FC980393A9C
BCE44AD2D64F6
30BB33AD3F5F5F
D495D31F37818C
1D94071342E07F
1BEC2194F6035B
A5DED3936500EB
82DFDA6E8AFB6
55B1EF3D0D7EB
F86B66DD9F29F6
B1D324FE8B26C
E38AB2013DD13F
611E7A594D675C
4432350EA244CC
34F3873CBA0659
2987A1D7E852AD
C22EF5A2EE2813
2031E48F74037E
3B34AB747F</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT</td><td>03</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM</td><td>F910A1504D5FFB
793D94F3B50076
5E1ABCAD72D9</td></tr>
<tr><td colspan="2">Table 60 Confirmation Request (Mastercard Public Key Data)
<table><tr><th>Field</th><th>Value</th></tr><tr><td>EMV PDL PARAMETER TYPE</td><td>07</td></tr><tr><td>EMV PDL TABLE ID</td><td>60</td></tr><tr><td>EMV PDL CARD TYPE</td><td>02</td></tr><tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr><tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr></table></td><td>⇨</td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host
	⇦	**Table 60 Confirmation Response (Mastercard Public Key Data)**

Field	Value
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	00
EMV PDL TABLE ID	60
EMV PDL CARD TYPE	02
EMV PDL CONFIRMATION FLAG	Y

⇨

Table 60 Request (American Express Public Key Data)

Field	Value
EMV PDL PARAMETER TYPE	06
EMV PDL TABLE ID	60
EMV PDL CARD TYPE	03
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01

⇦

Table 60 Response (American Express Public Key Data)

Field	Value
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01
EMV PDL TABLE ID	60
EMV PDL CARD TYPE	03
EMV PDL END-OF-TABLE FLAG	N
EMV PDL TABLE DATA BLOCK LENGTH	875
EMV PDL KEY COUNT	04
American Express 1024-Bit Key (Expired)	
EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000025
EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	03
EMV PDL KEY STATUS	E

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		American Express 1152-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000025
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	0E
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0288
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	AA94A8C6DAD24F9BA56A27C09B01020819568B81A026BE9FD0A3416CA9A71166ED5084ED91CED47DD457DB7E6CBCD53E560BC5DF48ABC380993B6D549F5196CFA77DFB20A0296188E969A2772E8C4141665F8BB2516BA2C7B5FC91F8DA04E8D512EB0F6411516FB86FC021CE7E969DA94D33937909A53A57F907C40C22009DA7532CB3BE509AE173B39AD6A01BA5BB85
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	A7266ABAE64B42A3668851191D49856E17F8FBCD
		American Express 1408-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000025
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	0F
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0352

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	C8D5AC27A5E1F B89978C7C6479A F993AB3800EB24 3996FBB2AE26B6 7B23AC482C4B74 6005A51AFA7D2D 83E894F591A235 7B30F85B85627F F15DA12290F70F 05766552BA11AD 34B7109FA49DE2 9DCB0109670875 A17EA95549E923 47B948AA1F0457 56DE56B707E386 3E59A6CBE99C12 72EF65FB66CBB4 CFF070F36029DD 76218B21242645B 51CA752AF37E70 BE1A84FF31079D C0048E928883EC 4FADD497A71938 5C2BBBEBC5A66 AA5E5655D18034 EC5
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	A73472B3AB5574 93A9BC2179CC80 14053B12BAB4
		American Express 1984-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000025
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	10
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0496
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	CF98DFEDB3D37 27965EE77977233 55E0751C81D2D3 DF4D18EBAB9FB 9D49F38C8C4A82 6B99DC9DEA3F0 104

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host
Table 60 Request (American Express Public Key Data Continued)	⇨	
Field / **Value**		
EMV PDL PARAMETER TYPE: 06		
EMV PDL TABLE ID: 60		
EMV PDL CARD TYPE: 03		
EMV PDL TABLE VERSION: 001		
EMV PDL BLOCK SEQUENCE NUMBER: 02		
	⇦	**Table 60 Response (American Express Public Key Data Continued)**
		Field / **Value**
		EMV PDL TABLE VERSION: 001
		EMV PDL BLOCK SEQUENCE NUMBER: 02
		EMV PDL TABLE ID: 60
		EMV PDL CARD TYPE: 03
		EMV PDL END-OF-TABLE FLAG: Y
		EMV PDL TABLE DATA BLOCK LENGTH: 453

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS</td><td>3D4BF22AC3550E
2962A59639B1332
156422F788B9C1
6D40135EFD1BA9
4147750575E636B
6EBC618734C91C
1D1BF3EDC2A46
A43901668E0FFC
136774080E88804
4F6A1E65DC9AA
A8928DACBEB0D
B55EA3514686C6
A732CEF55EE27
CF877F110652694
A0E3484C855D88
2AE191674E25C2
96205BBB599455
176FDD7BBC549
F27BA5FE35336F
7E29E68D783973
199436633C67EE
5A680F05160ED1
2D1665EC83D199
7F10FD05BBDBF
9433E8F797AEE3
E9F02A34228ACE
927ABE62B8B928
1AD08D3DF5C73
79685045D7BA5F
CDE58637</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT</td><td>03</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM</td><td>C729CF2FD26239
4ABC4CC1735065
02446AA9B9FD</td></tr>
<tr><td colspan="2">Table 60 Confirmation Request
(American Express Public Key Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>03</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th>Host</th></tr>
<tr><td></td><td>⇦</td><td>Table 60 Confirmation Response
(American Express Public Key Data)
<table>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>03</td></tr>
<tr><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table></td></tr>
<tr><td>Table 60 Request
(Discover Public Key Data)
<table>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>06</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>04</td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td></tr>
</table></td><td>⇨</td><td></td></tr>
<tr><td></td><td>⇦</td><td>Table 60 Response
(Discover Public Key Data)
<table>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>04</td></tr>
<tr><td>EMV PDL END-OF-TABLE FLAG</td><td>N</td></tr>
<tr><td>EMV PDL TABLE DATA BLOCK LENGTH</td><td>875</td></tr>
<tr><td>EMV PDL KEY COUNT</td><td>04</td></tr>
</table></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		Discover 1024-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000152
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	01
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0256
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	8D1727AB9DC852 453193EA0810B1 10F2A3FD304BE2 58338AC2650FA2 A040FA10301EA5 3DF18FD9F40F55 C44FE0EE7C7223 BC649B8F932892 5707776CB86F3A C37D1B22300D00 83B49350E09ABB 4B62A96363B01E 4180E158EADDD 6878E85A6C9D56 509BF68F0400AF FBC441DDCCDAF 9163C4AACEB2C 3E1EC13699D23C DA9D3AD
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	E0C2C1EA411DB 24EC3E76A9403F 0B7B6F406F398
		Discover 1152-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000152
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	03
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0288

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	BF321241BDBF3585FFF2ACB89772EBD18F2C872159EAA4BC179FB03A1B850A1A758FA2C6849F48D4C4FF47E02A575FC13E8EB77AC37135030C5600369B5567D3A7AAF02015115E987E6BE566B4B4CC03A4E2B16CD9051667C2CD0EEF4D76D27A6F745E8BBEB45498ED8C30E2616DB4DBDA4BAF8D71990CDC22A8A387ACB21DD88E2CC27962B31FBD786BBB55F9E0B041
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	CA1E9099327F0B786D8583EC2F27E57189503A57

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td rowspan="6"></td><td rowspan="6"></td><td colspan="2">Discover 1408-Bit Key (Active)</td></tr>
<tr><td>EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)</td><td>A000000152</td></tr>
<tr><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX</td><td>04</td></tr>
<tr><td>EMV PDL KEY STATUS</td><td>A</td></tr>
<tr><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH</td><td>0352</td></tr>
<tr><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS</td><td>8EEEC0D6D3857FD558285E49B623B109E6774E06E9476FE1B2FB273685B5A235E955810ADDB5CDCC2CB6E1A97A07089D7FDE0A548BDC622145CA2DE3C73D6B14F284B3DC1FA056FC0FB2818BCD7C852F0C97963169F01483CE1A63F0BF899D412A</td></tr>
<tr><td colspan="2">Table 60 Request
(Discover Public Key Data Continued)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>06</td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>04</td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>02</td><td colspan="2"></td></tr>
</table>

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
	⇦	**Table 60 Response (Discover Public Key Data Continued)**	
		Field	**Value**
		EMV PDL TABLE VERSION	001
		EMV PDL BLOCK SEQUENCE NUMBER	02
		EMV PDL TABLE ID	60
		EMV PDL CARD TYPE	04
		EMV PDL END-OF-TABLE FLAG	Y
		EMV PDL TABLE DATA BLOCK LENGTH	755
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	B67C5BBDC8B4F 6FB9ABB57E9512 5363DBD8F5EBA A9B74ADB932020 50341833DEE8E3 8D28BD175C83A6 EA720C262682BE ABEA8E955FE67 BD9C2EFF7CB9A 9F45DD5BDA4A1 EEFB148BC44FF F68D9329FD
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	17F971CAF6B708 E5B9165331FBA9 1593D0C0BF66

Table E-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		Discover 1984-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000152
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	05
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0496
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	E1200E9F4428EB 71A526D6BB44C9 57F18F27B20BAC E978061CCEF235 32DBEBFAF654A1 49701C14E6A2A7 C2ECAC4C92135 BE3E9258331DDB 0967C3D1D375B9 96F25B77811CCC C06A153B4CE699 0A51A0258EA843 7EDBEB701CB1F 335993E3F48458 BC1194BAD29BF6 83D5F3ECB984E3 1B7B9D2F6D947B 39DEDE0279EE45 B47F2F3D4EEEF9 3F9261F8F5A571 AFBFB569C15037 0A78F6683D687C B677777B2E7ABE FCFC8F5F935017 36997E8310EE0F D87AFAC5DA772 BA277F88B44459 FCA563555017CD 0D66771437F8B6 608AA1A665F88D 846403E4C41AFE EDB9729C2B2511 CFE228B50C1B15 2B2A60BBF61D89 13E086210023A3 AA499E423
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03

Table E-1 EMV PDL Data Examples (Continued)

<table>
<tr><th colspan="2">POS</th><th>⇔</th><th colspan="2">Host</th></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM</td><td>12BCD407B6E627 A750FDF629EE8C 2C9CC7BA636A</td></tr>
<tr><td colspan="2">Table 60 Confirmation Request (Discover Public Key Data)</td><td>⇨</td><td colspan="2"></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>04</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td colspan="2"></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 60 Confirmation Response (Discover Public Key Data)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID</td><td>60</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE</td><td>04</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table>

Appendix F: Glossary

Note: Shaded glossary terms are EMV related.

Table F-1 Glossary

Term	Definition
3-D Secure™	Three-Domain Secure™ (merchant, acquirer, issuer). A Visa-approved Authentication Method that is the global authentication standard for Electronic Commerce Transactions.
ABA Transit Number	See *American Bankers Association Transit Number*.
AC	See *Application Cryptogram (AC)*.
ACC	See *Application Authentication Cryptogram (AAC)*.
ACH	See *Automated Clearing House (ACH)*.
ACI	See *Authorization Characteristics Indicator (ACI)*.
Acquirer	A company that enters into contractual relationships with merchants, therefore allowing the merchant to accept credit/debit cards. Heartland is an acquirer.
Acquiring Financial Institution	An acquiring financial institution contracts with the bank and the merchants to enable credit card transaction. Also known as an Acquirer.
Acquiring Host	The processing system which communicates with the card acceptor or a communications network processor and is responsible for receiving the data relating to a transaction and obtaining an approval or denial for the transaction. The system maintains reconciliation totals for all financial transactions.
Action Codes	There are 2 sets of action codes: • **TACs** (Terminal Actions Codes held in the POS terminal) and • **IACs** (Issuer Action Codes read from the Chip Card). Each of these sets of action codes contain 3 codes which are compared to the TVR: • **Denial** action codes are used to determine if the transaction should be declined. • **Online** action codes are used to determine if the transaction required online authorization, and in the event that the terminal is unable to go online. • **Default** action codes are used to determine if the transaction should be declined.
Activation	Changing the state of a fixed denomination account from "inactive" to "active", enabling the prepaid card for use.
Activation and Initial Load	Changing the state of a stored value/prepaid account from "inactive" to "active", enabling the card for use, and requesting the loading of a variable amount to the account.
Address Verification Service (AVS)	A service supported by Visa, Mastercard, Discover and American Express that verifies the cardholder's billing address against the address on file with the issuer. AVS is designed to minimize fraud in non-face-to-face transactions (card not present, internet, mail/phone order).

Table F-1 Glossary

Term	Definition
Advice Message	A message that notifies a party of an action that has been taken and does not require further approval, but does require a response from the receiver.
AFD	See *Automated Fuel Dispenser (AFD)*.
Age Verification	A security process used to verify a consumer's age. Age verification is typically used by liquor and tobacco outlets, bars and casinos.
Agents	Those who sell bankcard services to merchants on behalf of ISOs, acquirers and processors. Also known as merchant level salespeople (MLSs) and independent sales agents (ISAs), most agents are independent contractors. Others are paid employees of ISOs, acquirers and processors.
AID	See *Application Identifier (AID)*.
AIP	See *Application Interchange Profile (AIP)*
American Bankers Association Transit Number	The ABA Transit Number, known as the routing transit number (RTN), is a nine-digit bank code used in the United States. It appears on the bottom of negotiable instruments, such as checks identifying the financial institution on which it was drawn.
American National Standards Institute (ANSI)	Governing institute that establishes guidelines for business practices.
American Standard Code for Information Interchange (ASCII)	ASCII is a character-encoding scheme based on the ordering of the English alphabet. ASCII codes represent text for computers, communications equipment, and other devices that use text.
Annual Percentage Rate	The percentage rate charged for a credit card (or other loan) for a whole year. It is the finance charge, expressed as an annual rate.
Annual Percentage Rate (APR)	The percentage rate charged for a credit card (or other loan) for a whole year. It is the finance charge, expressed as an annual rate.
ANSI	See *American National Standards Institute (ANSI)*.
Application Authentication Cryptogram (AAC)	A type of cryptogram generated by the Chip Card when a transaction is declined (at the end of offline or online declined transaction) to indicate the card declined the transaction. Other types of cryptograms are ARQC, TC, ARPC, AAR.
Application Cryptogram (AC)	This is a generic term to describe an application cryptogram. It is generated from data elements contained in either the online authorization request to the Issuer, or the final financial transaction required for clearing and settlement. There are four types of Application Cryptograms: • ARQC • TC • AAC • ARPC

Table F-1 Glossary

Term	Definition
Application Identifier (AID)	Names of applications supported by the POS. The POS obtains the DF names from the Card by issuing SELECT and READ RECORD commands. The POS AIDs are compared with the Chip Card DF Names to find a **mutually** supported application. *POS and Chip Card can support multiple AIDs. The AID structure is an ISO entity defined in the ISO7816 standard and is made up of two elements: • The **RID** (Registered Identification Provider Identifier) is five (5) bytes and identifies the scheme. (See RID for more detailed explanation). • The **PIX** (Proprietary Application Identification Extension) is a variable length field from 0 to 11 bytes long and is used to identify the different applications offered. Each brand under a specific scheme normally have a unique PIX. Example of two AIDs for Visa: • RID: A000000003 PIX: 1010 AID: A0000000031010 PRODUCT: Visa Credit or Debit • RID: A000000003 PIX: 1020 AID: A0000000032010 PRODUCT: Visa Electron
Application Interchange Profile (AIP)	List of security functions that reside on the Chip Card. The AIP indicates which functions are supported by the Card and which should be applied to the current transaction.Types of security functions residing on the card may include: • SDA • DDA • CDA • Terminal Risk Management • Cardholder Verification • Issuer Authentication. See SDA, DDA, CDA, and other functions for further details.
Application Version Number (ICC)	This data element indicates the version of the application on the Chip Card. It is specified by the Payment System and used in Application Version Number checking by the POS.
Application Version Number (Terminal)	This data element indicates the version of the application on the POS device. It is specified by the Payment System and used in Application Version Number checking by the POS.

Table F-1 Glossary

Term	Definition
Approved Scanning Vendor (ASV)	The PCI Security Standards Council maintains a structured process for security solution providers to become Approved Scanning Vendors (ASVs), as well as to be re-approved each year. The five founding members of the Council recognize the ASVs certified by the PCI Security Standards Council as being qualified to validate adherence to the PCI DSS by performing vulnerability scans of Internet facing environments of merchants and service providers. The major requirement of the process is a rigorous remote test conducted by each vendor on the PCI Security Standards Council's test infrastructure, which simulates the network of a typical security scan customer. The Council has set up the test infrastructure in such a way as to deliberately introduce vulnerabilities and misconfigurations for the vendor to identify and report as part of the compliance testing process.
ARPC (Authorization Response Cryptogram)	Used in Online processing. A cryptogram generated **by the Issuer** in response to an ARQC. It is sent in the authorization response back to the acquirer Host to the POS. The POS sends this cryptogram back to the Chip Card with a response code accepting or declining the transaction. The Chip Card's receipt and validation of the ARPC confirms approval response from the Issuer and ensures that it is communicating with the valid Issuer. This cryptogram is also typically used to allow the Chip Card to reset counters.
ARQC (Authorization Request Cryptogram)	Used in Online processing. This is a cryptogram requested by the POS and generated by the Chip Card at the end of the first round of Card Action Analysis step for transactions requiring online authorization. It is included in the authorization request or full financial request (B2) sent to the Issuer and it allows the Issuer to verify the validity of the Chip Card and message. When validated by the Issuer, the ARQC confirms that the Chip Card has not been copied or changed.
ASCII	See *American Standard Code for Information Interchange (ASCII)*.
ASV	See *Approved Scanning Vendor (ASV)*.
Attended POS	An attended POS device, meaning a person representing the merchant, accepts the payment. This can also be called a MAT, attended POS, and face-to-face transaction.
Auth Only	Authorization Only. Host Processing Mode whereby a POS utilizes the Heartland network to obtain online authorizations only. It then captures offline transactions such as sales captures, returns, and voids and settles with an acquirer other than Heartland.
Authorization	A process where a merchant issues a request to an authorization center to obtain an approval for a cardholder transaction for a specific amount. This process verifies that a credit or debit card has sufficient funds available to cover the amount of the transaction. This process also reserves the specified amount and ensures the card is authentic and not reported lost or stolen. This authorization request is usually submitted through a point-of-sale device. The merchant may also obtain authorizations by telephoning the authorization center.
Authorization Characteristics Indicator (ACI)	A value determined by VISA based on the data included with the authorization request. It is returned with the electronic authorization response.

Table F-1 Glossary

Term	Definition
Authorization Code	A code that a credit card issuing bank returns to the POS indicating an approval of the request transaction.
Authorization Request	A request sent to a financial institution to determine if a credit or debit card has sufficient funds to cover the amount of the transaction.
Authorization Response	A response to an authorization request indicating a financial institution's approval or disapproval of a transaction.
Auto-Substantiation	This transaction is applied to either a Credit Authorization or Credit Sale Transaction. Amount types included in this transaction are healthcare, prescription, vision/optical, clinic or other qualified medical and dental amounts.
Automated Clearing House (ACH)	An electronic payment network most commonly associated with payroll direct deposit and recurring payments. The ACH can also be used to clear electronic checks and other demand deposit account (DDA) transactions.
Automated Fuel Dispenser (AFD)	A pump at a service station or truck stop that is operated by the cardholder to obtain credit for pumping fuel. The pump contains a card reader. Also called an ICR, CRIND, or CAT.
AVS	See *Address Verification Service (AVS)*.
Balance Inquiry	Requesting the balance of an account to provide to the cardholder at the POS.
Bank Card Direct (BCD)	A service offered by Heartland Prepaid Services.
Bank Identification Number (BIN)	The primary account number found on credit cards and bank cards. It is a six-digit number, maintained by the American Bankers Association that identifies the bank and type of card. The first number identifies the card type. For example: • AMEX = 3 • Visa = 4 • Mastercard = 5 • Discover = 6 Also known as Issuer Identification Number (IIN).
Bank Routing Number	See *Routing Transit Number (RTN)*.
Bankcard	In general, a bankcard refers to a plastic card issued by a bank and used to access funds from an account.
Batch	Based on pre-determined criteria, the terminal will submit the batch transaction that has taken place since the last successful batch.
Batch Close	The process of sending batch information to the Host processor for clearing and settlement (the cardholders are charged and the merchant is paid).
BCD	See *Bank Card Direct (BCD)*.
BER-TLV Format	TLV is a data format that uses a label (tag) to uniquely identify the field. The tag is followed by the length, then the actual value of the field.
BIN	See *Bank Identification Number (BIN)*.
CA	See *Certificate Authority (CA)*.
CAPN	See *Card Acceptance Processing Network (CAPN)*.

Table F-1 Glossary

Term	Definition
Card Acceptance Processing Network (CAPN)	A set of requirements mandated by American Express to ensure processing of AMEX transactions according to their security standards. CAPN enhances POS security, supports expanded amounts, and adds a transaction life cycle identifier for all AMEX transactions.
Card Acceptor	The facility at which a purchase is made and a payment transaction is initiated. Also known as a merchant.
Card Acceptor Business Program Code (CAB Program Code)	Formerly MCC (Merchant Category Code) is a numerical representation of the type of business in which the card acceptor (merchant) engages. Mastercard assigns these codes.
Card Authentication	Chip Cards are authenticated during the payment transaction, protecting against counterfeit cards. Transactions require an authentic card validated either online by the Issuer using a dynamic cryptogram or offline with the Terminal using one of the following authentication methods: • **SDA** (Static Data Authentication) • **DDA** (Dynamic Data Authentication) • **CDA** (Combined DDA with application cryptogram generation)
Card Data Object List (CDOL1)	A list of data objects (tags and lengths) that are personalized on the Chip Card to make a decision on whether to approve or decline a transaction. They are read from the Card by the POS and used for the generation of the first cryptogram. The POS will send the values of these data objects together with the first Generate AC Command.
Card Data Object List (CDOL2)	A list of data objects (tags and lengths) that are personalized on the Chip Card to make a decision on whether to approve or decline a transaction. They are read from the Card by the POS and used for the generation of the final cryptogram. The POS will send the values of these data objects together with the second Generate AC Command.
Card Identifier	See *Card Verification Number (CVN)*.
Card Issuing Bank	A financial institution that issues payment cards such as credit/debit cards.
Card Not Present (CNP)	Card transactions (Internet or MOTO/eCommerce purchases, for example) for which the customer's card is not physically handled by the merchant. Interchange is set higher on these transactions because there is a higher risk of fraud.
Card Reader IN Dispenser (CRIND)	A term used primarily by Gilbarco referring to their brand of ICR.
Card Validation Code (CVC)	This is a 3 digit code value. See *Card Validation Code (CVC)*.

Table F-1 Glossary

Term	Definition
Card Verification Number (CVN)	This is a 3 or 4 digit number that appears on either the front or back of a credit card. It is not included in the magnetic stripe data. It is provided as a fraud deterrent to ensure the card is physically present when a POS transaction is initiated. These codes are only required at authorization time. The following terms are used by various card issuers: • CVV2 and CVC2 (3 digits) used by Visa and Mastercard account numbers. • CID (3 digits) used by Discover account numbers. • CID (4 digits) used by American Express account numbers.
Card Verification Value (CVV)	An authentication procedure established by credit card companies to reduce fraud for internet transactions. It consists of requiring a card holder to enter the CVV number in at transaction time to verify that the card is on hand. The CVV code is a security feature for "card not present" transactions (e.g., Internet transactions), and now appears on most (but not all) major credit and debit cards. This new feature is a 3 or 4 digit code which provides a cryptographic check of the information embossed on the card. The CVV code is not part of the card number itself.
Cardholder	A customer doing business with a merchant using a payment card.
Cardholder Authentication Verification Value (CAVV)	A unique value transmitted by an issuer (or Visa on behalf of an issuer) in response to an authorization request message.
Cardholder Verification	This verification validates that the person using the Chip Card is the true cardholder and the Card has not been lost or stolen. The Chip Card contains a list of cardholder verification methods (CVM) it supports, and the conditions under which they should be applied. The POS must navigate through this list and attempt the first method it finds for which the condition is met. If a method fails, the POS must check whether additional methods are allowed. For example, a list might contain the following: • Signature • Online enciphered PIN • Offline enciphered PIN • Offline enciphered PIN and signature • Offline plaintext PIN • Offline plaintext PIN and signature • No CVM required
Cash Advance	A transaction that dispenses cash against a cardholder's account using rules specific to a client/merchant.
Cash Back	This is a service offered to retail customers whereby an amount is added to the total purchase price of a transaction the customer receives that amount in cash along with the purchase.
Cash Out	To remove the remaining cash funds available on the stored value card leaving the card with a balance of zero for the cash account.
CAT	See *Customer Activated Terminal (CAT)*.

Table F-1 Glossary

Term	Definition
CAVV	See *Cardholder Authentication Verification Value (CAVV)*.
CDA (Combined DDA/Application Cryptogram Generation)	Used in Offline processing. One of the three methods of Offline Data Authentication. This applies the same requirements of DDA with an additional step during Chip Card analysis so it is the most secure option. It offers protection against counterfeit and skimming and protects against man-in-the-middle attacks. The Chip Card generates a dynamic signature using card private key, in addition to the application cryptogram, to prove that the Chip Card authenticated during DDA was the same card that provided the application cryptogram.
Certificate	The public key and identity of an entity together with some other information, rendered unforgeable by signing with the private key of the certification authority which issued that certificate.
Certificate Authority (CA)	Trusted third party that establishes a proof that links a public key (used by a merchant) and other relevant information to its owner. The CA issues, revokes and expires certificates. It is responsible for ensuring that the identity of the user requesting the certificate is legitimate.
Chargeback	A procedure where a cardholder or card issuer is disputing all or part of the amount of a credit or debit card transaction. A chargeback is therefore the act of taking back funds from a merchant for a disputed or improper transaction.
Check Reader	A device used to scan images of checks, according to legal specifications, for electronic clearing and settlement. Also known as check scanner.
Chip Card	A Chip Card (also known as a Smart Card or ICC) is simply a plastic card containing an integrated circuit. It is used to perform EMV transactions on a POS and is instrumental in reducing fraud. It is usually powered by a reader and relies on a reader to function. Chip cards may be contact or contactless.A reader recognizes a Chip Card by the first digit of its Service Code, with one of the following values: • 2 = International cards • 6 = Domestic cards
CID	See *Cryptogram Information Data (CID)*.
Client	A company that has contracted to use the services provided by Heartland.
Commercial Cards	Credit cards issued to businesses for travel, entertainment and other business expenses.
Consumer	See *Cardholder*.
Contact Chip Card	With a contact Chip Card, the embedded chip must come into physical contact with the chip reader for the payment transaction to occur. The Chip Card must remain in contact with the reader for the duration of the transaction. The terminal provides power to the chip to enable the chip to process.

Table F-1 Glossary

Term	Definition
Contactless Card	These cards are also known as Proximity cards or NFC cards. These cards communicate with a reader through a RFID (radio frequency interface device) by waving or tapping the card on the designated area on the terminal. With a contactless Chip Card, the embedded chip must come within sufficient proximity of the reader (a maximum of 4cm) for information to flow between the chip and the acceptance terminal.The terminal provides power to the chip to enable the chip to process but the card does not have to remain in the device through the end of the transaction. This minimizes the amount of time the card must be held within proximity of a reader.Transmission of information is faster between the Card and the Terminal with contactless. And, additional steps may be performed after the card has left the proximity of the reader. The contactless card has an embedded RF antenna. It has longer life and higher reliability than a contact card. This contactless card method is the foundation for acceptance of mobile payments.
Coordinated Universal Time	The time scale used as the basis of a coordinated dissemination of standard frequencies and time signals. UTC is formerly known as Greenwich Mean Time (GMT).
Corporate Cards	See *Commercial Cards*.
Counter-top POS	A category of POS devices that typically fits on a counter for use.
CPS	See Custom Payment Services.
CRIND	See Card Reader IN Dispenser.
Cryptogram	A numeric value that is the result of data elements entered into an algorithm. The result of this operation 'hides' the data and produces a 'digital signature' that can be used to verify the origin and integrity of the data by either a Chip Card or an Issuer. For EMV, a cryptogram is generated by the Chip Card in response to a Generate AC command and by the Issuer in the authorization response message.
Cryptogram Information Data (CID)	A bit that is set by the Chip Card after Card Risk Management. It indicates the action to be performed by the POS. There are 3 types of actions indicated by the CID: • **AAC** is generated whenever a card declines a transaction. • **ARQC** is generated whenever a card requests online authorization. • **TC** is generated whenever a card approves a transaction. In addition, the card may also return a reason or advice code (e.g. service not allowed, or issuer authentication failed) to allow the terminal to perform any additional processing that may be required.
Customer	See Cardholder.
Customer Activated Terminal (CAT)	An unattended POS, which includes kiosks and fuel dispensers. Similar to AFD, ICR, & CRIND. Also known as Cardholder Activated Terminal.

Table F-1 Glossary

Term	Definition
Customer Payment Services	Visa's regulations for the information that must be submitted with each transaction. Transactions must meet CPS criteria in order to qualify for lowest transaction-processing fees available. This is similar to Mastercard's Merit system.
CVC	See *CVC* or *CVN*.
CVN	See *CVN*.
CVV	See *CVV*.
CVV2	This is a 3 digit code used by Visa. See *CVV*.
Data Element	The identification of a data element based on the relative position of the data element within the message.
DDA (Dynamic Authentication Data)	An authentication technique used in offline chip transactions. This technique calculates a cryptogram for each transaction that is unique to the card and transaction. DDA protects against modification counterfeiting, cloning, and skimming.
DE	See Data Element.
Demand Deposit Account (DDA)	A merchant's checking account that is credited or debited with their deposits, fees and adjustments (also referred to as Direct Deposit Account).
Derived Unique Key Per Transaction (DUKPT)	Reference standard X9.24, Retail Key Management for this definition. It is a key management technique in which for every transaction a unique key is used, which is derived from a fixed key. If a derived key is compromised, future and past transaction data are still protected since the next or prior keys cannot be easily determined.
Discover	Common name for DFS Services LLC.
Discretionary Data	An optional field where client data can be included within a transaction.
DSS	Data Security Standard. See *Payment Card Industry Data Security Standard (PCI-DSS)*.
Dual Interface Card	A chip card that has contact and contactless interfaces. The card can be tapped or inserted into the POS device to initiate a transaction.
DUKPT	See *Derived Unique Key Per Transaction (DUKPT)*.
E-PIN	Electronic PIN.
E3™	Heartland End-to-End Encryption. New technology offered by Heartland to allow encryption of card data from initial swipe or input at the POS through arrival at the Issuer. This system not only removes intrusion threats but it also greatly reduces the scope for PCI audits on the associated merchant POS software.
EBT	See *Electronic Benefits Transfer*.
EFT	Electronic Funds Transfer. A way of performing financial transactions electronically. The Pulse and Star networks are examples of EFT systems.

Table F-1 Glossary

Term	Definition
Electronic Benefits Transfer	EBT is an electronic system in the United States that allows state governments to provide financial and material benefits to authorized recipients via a plastic debit card. Common benefits provided via EBT are typically sorted into two general categories: • Food Stamp • Cash Benefits
Electronic PIN	E-PIN.
Electronic PIN Delivery	A service provided by Heartland Prepaid Services.
EMV Terminal or Reader	Also known as a Chip device. This is any point of sale device that is able to process chip transactions.
EMVCo	Europay International, Mastercard International and Visa International. EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including POS terminals and ATMs. EMVCo establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, Mastercard and Visa.
Encryption	A method of protecting data. Encryption transforms readable information using an algorithm (called a cipher) and makes it unintelligible to anyone except those who possess a key that converts the information back into readable form. See also end-to-end data encryption.
End-to-End Encryption	E3™. Refers to the Heartland process of converting card data to seemingly unreadable text from the moment it gets entered at the POS and through to the final authorization.
EPD	See *Electronic PIN Delivery*.
Face-to-Face Transactions	Transactions in which both the cardholder and the card are present at the point of sale.
Fallback	If a Chip-Card-capable POS is unable to read the data from the Chip Card, or if for Visa, Mastercard and AMEX, there are no mutually supported applications between the Card and the POS, the POS will 'fallback' to a magnetic stripe or manually keyed transaction. The resulting magnetic stripe or manually keyed transaction must be submitted to the Issuer for authorization online.
Financial Transaction	A message that either notifies the Host of the completion of a previously authorized payment transaction or that requests the approval and completion of the payment transaction by the Host causing the reconciliation totals to be increased.
Flexible Spending Accounts	A tax-advantaged financial account that can be set up through an employer in the United States. An FSA allows an employee to set aside a portion of his or her earnings to pay for qualified expenses as established in the cafeteria plan, most commonly for medical expenses or purchases.
Floor Limit	The payment amount above which credit and debit card transactions must be authorized. This amount is specified in each merchant's processing agreement.
FSA	See *Flexible Spending Accounts*.

Table F-1 Glossary

Term	Definition
General Services Administration	Visa Purchasing Card that is issued to federal government agencies by an Issuer contracted with the General Services Administration.
Global Trade Identification Number	The GTIN is an umbrella term used to describe the entire family of EAN/UCC data structures for trade item (products and services) identification. GTIN is a term only. It does not change existing standards. The UCC-12 code does not go away. The definition and information obtained from the Uniform Code Council, Inc. Refer to the organization's website at *www.uc-council.org* for more information.
Gratuity	This is an adjustment to a transaction for a tip.
GSA	See *General Services Administration*.
GTIN	See *Global Trade Identification Number*.
HDC	See *Host Data Capture*.
Health Reimbursement Arrangement	HRAs are Internal Revenue Service sanctioned programs that allow an employer to set aside funds to reimburse medical expenses paid by participating employees. Using an HRA yields tax advantages to offset health care costs for both employees as well as an employer.
Host Data Capture	Host Processing Mode whereby a POS utilizes the Heartland network to authorize, capture and adjust transactions. The POS maintains a batch which it reconciles with the Host. The Host will settle the batch on behalf of the POS.
HRA	See *Health Reimbursement Arrangement*.
IAC	See *Issuer Action Code (IAC)*.
ICC	Another name for a Chip Card or Chip application.
ICR	See *Island Card Reader (ICR)*.
IEEE	See *Institute of Electrical and Electronics Engineers*.
IIAS	See *Inventory Information Approval System*.
IIN	See *Bank Identification Number (BIN)*.
Incremental Authorization	Unique authorization for the Lodging Industry. Occurs when an authorization is adjusted above a threshold amount.
Independent Sales Agent (ISA)	See *Agents*.
Information Security and Compliance (ISC)	ISC program used by Discover to implement and maintain efficient data security requirements and procedures. PCI is now used as a standard.
Inside POS	See *Attended POS*.
Institute of Electrical and Electronics Engineers	The IEEE is a non-profit professional association dedicated to advancing technological innovation related to electricity.
Integrated POS	A category of POS devices that typically combine several Point of Service locations in such industries as Retail, Parking, and Petroleum.
Integrated Services Digital Network	A set of standards for digital transmission over ordinary telephone copper wire as well as over other media. ISDN requires adapters at both ends of the transmission so an access provider also needs an ISDN adapter.

Table F-1 Glossary

Term	Definition
Interchange	The process by which all parties involved in a credit card transaction (processors, acquirers, and issuers) manages the processing, clearing and settlement of credit card transactions.
Interchange Fees	Fees paid by the acquirer (Heartland) to the card issuing bank to compensate for transaction-related costs.
International Organization for Standardization (ISO)	Founded in 1946, ISO is an international organization composed of national standards bodies from over 75 countries. ANSI is a member of ISO. ISO has defined a number of important computer standards. Also an organization registered with Visa and sponsored by an acquiring bank to sell Visa card acceptance services. Can refer to an organization that works with and does business under the name of such a registered ISO. ISOs may also service merchant accounts once they are registered, dependent upon the contract with the acquirer. Mastercard uses the term "member service provider" to describe ISOs. However, it is common within the payments industry to use the term "ISO" when referring to independent sales organizations registered with either or both card brands.
International Telecommunication Union	An international organization within which governments and the private sector coordinate global telecom networks and services.
Inventory Information Approval System	This system identifies the qualified healthcare products being purchased by the cardholder at the point of sale. This system must be used for merchants utilizing auto-substantiation.
IP Address	Internet Protocol Address. A unique number assigned to any computer or printer that uses internet protocol.
ISC	See *Information Security and Compliance (ISC)*.
ISDN	See *Integrated Services Digital Network*.
Island Card Reader (ICR)	An ICR is an unattended device that accepts payment cards, typically used with fuel pumps at gasoline stations. Also known as AFD, CAT, CRINDS, DCR, and pay-at-the-pump.
ISO	See *International Organization for Standardization (ISO)*.
Issuer	A company that enters into contractual relationships with consumers and/or businesses through the issuance of plastic credit/debit cards. An issuer is also known as a "card issuing center." Examples of issuers are Bank of America and Citi-Bank.
Issuer Action Code (IAC)	Issuer-configured conditions or rules stored on the Chip Card. As a result of previous Chip & POS processing steps, the IACs are used by the POS, along with analysis of the TVR (Terminal Verification Results), to determine the action to be taken.Three types of codes are: • **IAC Default:** Specifies the Issuer's conditions (or rules) that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online. • **IAC Denial**: Specifies the Issuer's conditions (or rules) that cause the denial of a transaction without attempt to go online. • **IAC Online:** Specifies the Issuer's conditions (or rules) that cause a transaction to be transmitted online.

Table F-1 Glossary

Term	Definition
Issuer Authentication	EMVCO: Validation of the issuer by the Chip Card to ensure the integrity of the authorization response. If the auth response contains an ARPC (Authorization Response Cryptogram), the Terminal sends the cryptogram to the Chip Card. The Card then performs Issuer Authentication by validating the response cryptogram to verify that the response came from the genuine Issuer. This process prevents criminals from circumventing the Chip Card's security features by simulating online processing and fraudulently approving a transaction to reset counters and indicators. If this step fails, subsequent transactions for the Chip Card will be sent online for authorization until Issuer Authentication is successful.
Issuer Script	This is a string of commands sent to the chip card from an issuer in a transaction response. The issuer can update securely the contents that are stored on chip cards without reissuing the cards, such as changing the cardholder's PIN, disabling the card, enabling a card, or changing authorization controls for the card. The terminal must send each of these commands unaltered to the Card.
Issuing Bank	A federally insured financial institution that issues credit and debit cards. This is the cardholder's financial institution.
Issuing Host	The processing system that acts under the authority of the card issuer to receive a transaction and to approve funds to be given to the card acceptor or to guarantee checks.
ITU	See *International Telecommunication Union*.
Japan Credit Bureau (JCB)	An independent card company originally established in Japan. JCB International Credit Card Company, Ltd. was established in Los Angeles in 1988 to issue credit cards as well.
Key Data	Data related to a security key. Reference standard X9.24, Retail Key Management.
Key Serial Number (KSN)	Used in PIN encryption/decryption.
Level of Issuance (LOI)	Series Number.
LLVAR	L is for length (LLL = 3 bytes). The field is parsed as 3 bytes of length and remaining of bytes as text content.
Load Amount	The amount of value that is added to the account. See Activation and Reload.
Load Value	To deposit funds into a cash account. See Activation and Replenish.
Local Pump Limit	This is the dollar amount that the POS has set for an ICR. The Pump will not exceed this amount regardless of the approved amount of the transaction. The customer can initiate another transaction if more fuel is desired.
Longitudinal Redundancy Check (LRC)	The LRC is used as an error checking method by both Host and terminal to validate that the data was received without error.
LUHN Formula	The LUHN formula, also known as the MOD-10 Checksum, is used to generate and/or validate and verify the accuracy of account numbers.
Maestro	Maestro is a multi-national debit card service owned by Mastercard.
Magnetic Ink Character Recognition	Used on checks and includes the ABA number, account number, check sequence number, and special characters.
Magnetic Strip Reader	The device that a payment card is swiped through as the Track Data is read.

Table F-1 Glossary

Term	Definition
Magnetic Stripe	A strip of magnetic material on the back of credit cards which contains data identifying the cardholder, such as account number and cardholder name.
Manual Entry (Key Entered)	Card information is entered manually, or key-entered into a terminal, usually because the magnetic stripe could not be read or the card is not present at the time of sale (i.e., a mail/phone order merchant).
MAT	Manually Attended Terminal. See *Inside POS*.
MCC	See *Merchant Category Code*.
Member Service Provider	See *International Organization for Standardization (ISO)*.
Merchant	Describes the business relationship where a cardholder interacts with the client.
Merchant Bank	A banking or financial institution that provides merchant services.
Merchant Category Code	Usually a four digit number that identifies the type of business in which a merchant is engaged by the type of goods or services it provides. Visa and Mastercard have specific numbers for each type of merchant business.
Merchant Discount Fee	A fee charged to a merchant for card processing services. This fee is usually represented in a percent format (example 2.25%). This merchant discount fee is used to determine part of a merchant's monthly processing charge.
Merchant Identification Number	A number assigned by an acquirer to identify each merchant for the purpose of reporting, processing and billing. All Heartland merchant numbers begin with a 65. All Heartland merchant numbers are 15 digits in length.
Merchant Service Fee	A fee assessed to a merchant for Heartland's value-add services such as the Merchant Center, 24/7 customer support and local servicing by Heartland Relationship Managers.
Merchant Services Provider	Handles the setup with the Front-End and Back-End Processors by Heartland.
Message	A set of data elements used to exchange information between a POS application and the Heartland system.
MICR	See *Magnetic Ink Character Recognition*.
MID	See *Merchant Service Fee*.
MIME	See *Multipurpose Internet Mail Extensions*.
MOD-10 Checksum	Modulus 10 Checksum. The "modulus 10" or mod 10" algorithm, also known as the Luhn formula, is a simple checksum formula used to validate a variety of identification numbers, such as credit card numbers.
MOTO/eCommerce	Mail Order/Telephone Order. A category of card-not-present transactions involving purchases made through mail order or telesales companies. In this type of transaction, the merchant typically has a card terminal and manually keys in required card information for transmission to the appropriate authorization network. Interchange rates for these transactions are among the highest.
MPLS	See *Multiprotocol Label Switching*.
MSP	See *Merchant Services Provider*.
MSR	See *Magnetic Strip Reader*.

Table F-1 Glossary

Term	Definition
Multiprotocol Label Switching	A mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. It can encapsulate packets of various network protocols. MPLS is a highly scalable, protocol agnostic, data-carrying mechanism. Packet-forwarding decisions are made solely on the contents of the MPLS label, without the need to examine the packet itself. This allows creation of end-to-end circuits across any type of transport medium, using any protocol.
Multipurpose Internet Mail Extensions	An Internet standard that extends the format of email to support: Text in character sets other than ASCII Non-text attachments Message bodies with multiple parts Header information in non-ASCII character sets.
NACS	National Association of Convenience Stores. See *Petroleum Convenience Alliance for Technology Standards (PCATS)*.
NDA	Non-Disclosure Agreement. A confidentiality agreement signed by a customer and delivered to Heartland. Completion of NDA is required before receiving Heartland SDK, documentation and specifications.
NFC (Near Field Communication)	Wireless communication that allows data to be exchanged between devices (such as smart phones or mobile phones) that are centimeters apart. NFC-enabled mobile phones incorporate smart chips (called secure elements) that allow the phones to securely store payment and consumer account information.
NTS	Network Terminal Specification. Heartland proprietary transaction format (VAPS).
NWS	Heartland Host processing system supporting the Z01 and the POS 8583 specifications.
Offline Approval	A transaction that is approved at the point of transaction between the Chip Card and POS only, without an authorization response from the Issuer.
Offline Data Authentication	This is a method the POS uses to authenticate a Chip Card using public-key cryptography. This authentication check protects against counterfeit and skimming.There are three methods of authentication that may be used: • SDA • DDA • CDA The method chosen is determined by the Issuer depending upon Chip Card capability. Only one method of offline data authentication is performed during a transaction.
Offline Decline	A transaction that is declined at the point of transaction between the Chip Card and POS only without interaction with the Host and Issuer (no authorization response from the Issuer).
Offline Enciphered PIN	A card verification method (CVM). In this method, the PIN is entered at the POS device. The POS encrypts the entered PIN before sending it to the Chip Card (using public key encryption). The Chip Card decrypts PIN and compares with the reference PIN in its memory. This method assists with prevention of counterfeit and skimming through the use of cryptography. Terminals that support Offline Enciphered PIN must also support the less secure Offline Plaintext PIN method.

Table F-1 Glossary

Term	Definition
Offline PIN Verification	The process whereby a cardholder-entered PIN is passed to the Chip Card for comparison to a PIN value stored secretly on the Card. This method assists with detection of a lost or stolen card.
Offline Plaintext PIN	A card verification method (CVM). The cardholder enters a PIN at the entry device. The entry device does not encrypt the PIN before sending it to the Chip Card. This is commonly used by cards that cannot support the more secure Offline Enciphered PIN method. Terminals that support Offline Plaintext PIN must also support Offline Enciphered PIN method.
Online Card Authentication	Used in Online processing. When Chip Card and Terminal agree to send a transaction online, the Chip Card generates a cryptogram, the ARQC (Authorization Request Cryptogram). The Issuer may respond with an ARPC (Authorization Response Cryptogram).
Open-to-Buy (OTB)	An inquiry transaction used to request the unused credit amount available for the account at the time of the transaction. The OTB is the amount of credit left on an account. For example, before a purchase, a customer has $500.00 OTB. The customer purchases $200.00 worth of products. After the sale, the OTB returned in the response will be $300.00.
Owning Host	Owning Host refers to one of several instances of the VAPS application suite that "owns" a particular terminal. These instances are geographically separated across the country. Any of these Hosts can initiate the authorization of a financial request (1200) with the issuer, but the Owning Host is the only Host that can process the capture or collect for that transaction.
PA-DSS	See *Payment Application Data Security Standard (PA-DSS)*.
PAN	See *Primary Account Number*.
PAPB	See *Payment Application Best Practices*.
Partial Authorization	A process to complete a transaction if the full amount requested is not approved but a partial portion of the requested amount is approved. A merchant must be set up for this capability. If a merchant is set up for this capability, the Issuer response will contain the full amount requested or a lesser or partial amount authorized.
Pay at the Pump (PATP)	The ability to use a payment card at a self-service island for the petroleum industry. See ICR, AFD, CAT, or CRIND.
Payment Application Best Practices	PCI SSC took over management of PABP and renamed to PA-DSS. See *PA-DSS*.
Payment Application Data Security Standard (PA-DSS)	Established to help software vendors and others develop secure payment applications that do not store prohibited data and to ensure their compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to PA-DSS requirements.
Payment Card Industry (PCI)	The PCI denotes the debit, credit, prepaid, and POS cards and associated businesses. The term is sometimes more specifically used to refer to the Payment Card Industry Security Standards Council (PCI SSC) an independent council originally formed with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standards.

Table F-1 Glossary

Term	Definition
Payment Card Industry Compliance Acceleration Program (PCI CAP)	Under the CAP plan, acquirers are required to validate Level 1 and Level 2 merchant compliance with PIN security. This means that Level 1 and Level 2 merchants must not use payment devices such as PIN pads, and encourages the use of unique encryption keys for every device. For Level 3 and Level 4 merchants, acquirers must establish a thorough compliance program for those merchants. According to Visa, as of November 1, 2007, acquirers whose transactions qualify for lower interchange rates available in the Visa and Interlink tiers must ensure that the merchants generating the transactions are PCI compliant in order to receive this benefit.
Payment Card Industry Data Security Standard (PCI-DSS)	The Payment Card Industry Data Security Standard is a worldwide information security standards assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.
Payment System Environment (PSE)	This is a method that could be used by the Terminal for application selection. PSE is optional but highly recommended to enhance the performance of the transaction. HPS recommends this method if it is supported by the Chip Card.
PCATS	See *Petroleum Convenience Alliance for Technology Standards (PCATS)*.
PCI	See *Payment Card Industry (PCI)*.
PCI CAP	See *Payment Card Industry Compliance Acceleration Program (PCI CAP)*.
PCI-DSS	See *Payment Card Industry Data Security Standard (PCI-DSS)*.
PED	See *PIN Entry Device*.
Peripheral	Any device that attaches to a computer and is controlled by its processor.
Personal Identification Number (PIN)	A PIN is used to help ensure that the cardholder is really the cardholder. It is typically a four digit number that is not found anywhere on the card or in track data.
Petroleum Convenience Alliance for Technology Standards (PCATS)	PCATS is an organization devoted to the development, maintenance, and implementation of standards for the convenience store and petroleum industries.
Piggyback Transaction	A Piggyback transaction allows the Capture from a previous Pre-authorization to be sent when the next transaction is sent to the Host. This helps to reduce the number of transactions sent reducing the cost to the merchant. Some transactions cannot be piggybacked. Fleet cards are not supported as part of a Piggyback transaction.
PIN	See *Personal Identification Number (PIN)*.

Table F-1 Glossary

Term	Definition
PIN (Personal Identification Number)	For EMV, a secret number between 4 and 12 digits, known only by the Cardholder. It may be used during Cardholder Verification to confirm that the user of the card is the cardholder. The methods of PIN verification supported by EMV are: • Offline Plaintext PIN • Offline Enciphered PIN • Online Enciphered PIN For EMV processing, when either online or offline PIN is changed, they must be synchronized.
PIN Debit	A debit card transaction authorized by the cardholder using a PIN.
PIN Entry Device	PCI PED requirements were established to protect against fraud by ensuring the security of devices that process financial data. Approval is granted for devices that have been evaluated by an approved laboratory and determined to be compliant with PCI Security Requirements.
PIN Pad	Numeric key pad a consumer uses to enter a PIN when paying with a debit card.
PL	See *Private Label*.
PLR	See *Private Label Retail*.
Point of Purchase (POP)	See POS.
POS	Point of Sale or Point of Service. The hardware and software used to collect and transmit non-cash payments for goods and/or services. The device where retail sales occur and payment transactions are initiated.
POS 8583	A Heartland transaction format based on ISO 8583.
POS System	Point of Sale System or Point of Service System. The system that processes the transaction messages at a point of service. The system may handle other non-transaction functions also.
PPSE (Proximity Payment System Environment)	This contains a directory of all the **contactless** payment applications that exist on the ICC. PPSE is mandatory in all contactless implementations.
Pre-Authorization	A pre-authorization is a request for approval of an estimated purchase amount before the exact amount is known.
Prepaid Card	A card representing a proxy for a stored value/prepaid account where value resides that the consumer can use for the purchase of specific goods or services provided by a prepaid product's service provider.
Primary Account Number	The account number that appears on the face of payment cards.
Private Key	That key of an entity's asymmetric key pair that should only be used by that entity. In the case of a digital signature scheme, the private key defines the signature function.
Private Label	Private Label products or services are typically those manufactured or provided by one company for offer under another company's brand. Private Label Payment Cards tend to be exclusive to one merchant or company and can include special features, such as a loyalty program.
Private Label Retail	Acronym for Heartland Retail's Private Label system.

Table F-1 Glossary

Term	Definition
Processor	An acquirer (such as Heartland) or an acquirer's agent that provides authorization, clearing or settlement services for merchants.
Programmable Read-Only Memory (PROM)	Programmable Read-Only Memory. A form of digital memory where the setting of each bit is locked. Such PROMs are used to store programs permanently. The key difference from a strict ROM is that the programming is applied after the device is constructed.
Proprietary Cards	See *Private Label*.
Proximity Entry	This transaction occurs when a card is read by a proximity reader to capture the card information stored on the magnetic strip or chip.
Public Key	This is the public component of an asymmetric key pair. The public key is usually publicly exposed and available to users (not secret). A certificate to prove its origin often accompanies it. All card brands utilize public keys and it is used for contact and contactless.It is used to counter act any cryptographic operation that is done by the Private Key. The Public Key has a mathematical link to the Private Key which makes them a key pair.
Purchase	This term represents both a sale transaction and an Authorization/Force Draft Capture transaction pair.
Quick Reference Guide (QRG)	A document or chart, used as a guide, to give a merchant quick reference to terminal operation procedures, such as batch settlement, offline/force entries, returns, etc.
Quick Service Restaurant (QSR)	A specific type of restaurant characterized by fast-food cuisine and by mini-meal table service.
Random Selection	An EMV online-capable POS function that allows for the selection of transactions for online processing. Part of the Terminal Risk Management function.
RDC	See Remote Deposit Capture.
Real Time Clearing	RTC is used only with Visa transactions, and is an online transaction based clearing system for Petroleum Merchant Codes 5541 and 5542 only.
Recharge	See Replenish.
Reconciliation	The process of confirming the accuracy of partial or final totals by comparing totals from different systems.
Reference Account	The account is part of an application transaction as one criterion for assessing the suitability for granting the application for a new account.
Referral Messages	A "call" or "call center" response for an authorization. See also *Voice Authorization*.
Registered Application Provider Identifier (RID)	This is part of the AID, 5 bytes in length, used to identify the scheme (e.g. Visa, Mastercard, etc). Functions of this field: • Identifies the payment brand/application • Certification Authority Public Key Index (1 byte) – unique per RID • It is received from the Chip Card and is a pointer to the offline Public keys required for the transaction.
Reload	To load an amount of funds into a stored value/prepaid account.

Table F-1 Glossary

Term	Definition
Remote Deposit Capture	A check deposit process whereby paper checks are converted into digital images for electronic clearing and settlement, through either electronic check or ACH systems.
Replenish	To deposit funds into either the cash or credit account.
Request	A message directing or instructing the receiver to perform a specified action and respond with the results of the action.
Response	A message that provides the results of an action requested by the sender.
Response Codes	Codes returned from the Issuer down to the POS. Codes verify that a particular transaction was accepted or reflect why it was declined.
Retransmits Message	A message that retransmits the same information as a prior message.
Retrieval	A request for a legible copy of a sales slip and/or other documentation relating to a credit or debit card transaction. This is the process or stage before a disputed transaction becomes a chargeback.
Reversal	A system initiated transaction request to cancel or reverse a recently completed transaction.
Reversal Transaction	A message that cancels the specified financial transaction that was previously reported as complete, causing the reconciliation totals to be decreased.
RFID	Radio Frequency Identification or Radio Frequency Input Device. Radio-frequency identification (RFID) is the use of an RFID tag applied to or incorporated into a product for the purpose of identification using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader.
RID	See *Registered Application Provider Identifier (RID)*.
Routing Transit Number (RTN)	A routing transit number is a nine-digit bank code, used in the United States, which appears on the bottom of negotiable instruments such as checks identifying the financial institution on which is was drawn.
RTC	See *Real Time Clearing*.
Script Commands (Issuer Scripts)	Issuers can return script commands to Chip Cards in online responses. Scripts can block chips, and change Chip Card offline limits. Scripts may not be relevant to the current transaction but are important for the continued functioning of the ICC. A script may contain commands not known to the terminal, but the terminal must deliver each command to the ICC individually.
SDA	See *Static Data Authentication (SDA)*.
Service Code	The 3-digit code that follows the expiration date on the card's Track 2 magnetic stripe. In EMV it is used to identify the technology supported of the payment card being swiped. Values supported by HPS are as follows for the first digit: • 2 = International (EMV Chip, debit or credit) • 6 = National use only (EMV Chip, debit or credit)
Service Fee	See *Merchant Service Fee*.
Session	A series of messages exchanged between the POS application and the Heartland system during a single communication connection.

Table F-1 Glossary

Term	Definition
Settlement	The process of transferring funds for sales and credits between acquirers and issuers, including the final debiting of a cardholder's account and the crediting of a merchant's account.
SIC	See *Merchant Category Code*.
Signature Debit	A Visa Debit or Debit Mastercard transaction authorized by a cardholder's signature.
Spectrum	A Heartland proprietary POS Transaction Format.
Split Tender	Split tender processing allows the total amount of a particular transaction to be split over two different methods of payment (electronic or non-electronic).
SSL	Secure Sockets Layer. A protocol for transmitting data over the internet. SSL uses a cryptographic system to provide safety and privacy of data.
STAN	System Trace Audit Number. Also known as the transaction sequence number.
Stand-In	The process of providing authorization services on behalf of an Issuer. If allowed, a processing network or POS may act as a stand-in for the authorizer to approve transactions.
State Withholding Tax Rate (SWT Rate)	The state withholding tax rate that is imposed for this transaction. The rates can vary by state.
Static Data Authentication (SDA)	One of the three methods of Offline Data Authentication. SDA authenticates SAD (static data) put on the card by the Issuer has not changed since the original personalization of the card. This is a Terminal function. Each Chip Card is personalized with an Issuer public key certificate and static signed application data composed of data elements personalized onto the card and signed with Issuer private key. The POS validates this cryptographic signature/value. During SDA processing, the Chip Card is passive and the Terminal is active. The Chip Card provides the data to be validated but the POS carries out all the computation. This protects against some types of counterfeit fraud, ensuring that the data has not been fraudulently altered since original chip card personalization. This does not protect against skimming. Each terminal should be able to store 6 certification authority public keys per Registered Application Provider Identifier (RID).
SVS	Stored Value Solutions.
Swiped Entry	A transaction where a card is swiped (or passed) through a magnetic card reader or chip reader to capture card information stored on the magnetic strip or chip.
System/Device	A single hardware unit (device) or a group of units (system) that present messages to a Host processing system.
TAG Format	This is the format method used to exchange information with the EMV Chip and the POS Terminal. Each Tag is assigned a Tag Number denoting the type of information it contains.
Tamper Resistant Security Module	Key encryption.

Table F-1 Glossary

Term	Definition
Taxpayer Identification Number (TIN)	An identification number assigned to taxpayers by the IRS. The TIN for individuals is their social security number. The TIN for businesses is the employer identification number.
TDC	See *Terminal Data Capture*.
TDES	See *Triple Data Encryption System*.
Terminal	See *POS System*.
Terminal Action Codes (TAC)	A set of action codes stored on the POS terminal for AIDs it supports. As a result of previous Chip & POS processing steps, these are used by the POS, along with analysis of the TVR, to determine the action to be taken. Three types of codes are: • **TAC Default:** Specifies the acquirer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online. • **TAC Denial:** Specifies the acquirer's conditions that cause the denial of a transaction without an attempt to go online. • **TAC Online:** Specifies the acquirer's conditions that cause a transaction to be transmitted online.
Terminal Based Terminal	A system where the merchant's transactions are stored within the terminals memory. The terminal stores the transactions until the merchant closes the batch.
Terminal Data Capture	The terminal captures all transactions and forwards transaction detail to the Heartland Host via a batch upload transaction. The terminal captures all other credit card transactions offline without contacting the Host.
Terminal Identification Number	A number assigned to the physical terminal device to identify its attributes to the processor. Each terminal within a merchant location has a separate TID.
Terminal Risk Management	This step performs various checks to protect the Issuer, acquirer, and system from fraud. Checks include the following: • Floor Limit • Random Selection • Velocity Checking The results of these checks are stored by the Terminal in the TVR for later use. **Note:** The terminal may randomly select some transactions for online processing.
Third Party Processors	An independent processor that is contracted with by a Bank or Processor to conduct a part of transaction processing.
TID	See *Terminal Identification Number*.
TIN	See *Taxpayer Identification Number (TIN)*.
TPP	See *Third Party Processors*.
Track Data	Track Data is the information encoded within the magnetic strip on the back of a credit card which is read by the electronic reader within the terminal or point-of-sale (POS) system.
Transaction	A set of messages to complete a processing action.

Table F-1 Glossary

Term	Definition
Transaction Certificate (TC)	Indicates the data input and output capabilities of the POS, such as: • methods supported for entering information from the card into the POS • methods (CVM) for verifying the identity of the cardholder • methods for authenticating the card and whether or not the POS has the ability to capture a card
Transaction Fee	A fee charged to a merchant each time a transaction is processed, which dials into the authorization system, such as a sale or authorization only.
Triple Data Encryption System	In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm. It is so named because it applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.
TRSM	See *Tamper Resistant Security Module*.
TSYS	Total System Services. Vital. Back-end processor.
TVR (Terminal Verification Result)	The TVR is an EMV Tag containing the status of several different EMV checks and functions performed by the PINPad, Kernel, or the POS. It consists of a series of indicators used to record the results of offline processing between the Chip and the POS (e.g. card is expired, cardholder verification has failed, or online floor limits have been exceeded). The POS compares the TVR values with the IACs (on the Card) and TACs (on the POS) to determine if the transaction should be approved, declined, or sent online to the Issuer. Upon that determination the POS requests a cryptogram from the Chip Card (TC, ARQC or AAC).
UAT	See *User Acceptance Test (UAT)*.
Unload Value	See *Cash Out*.
User Acceptance Test (UAT)	Testing for business users to attempt to make a system fail, taking into account the type of organization it will functioning in. It is checking and verifying the system in the context of the business environment it will operate in.
UTC	See *Coordinated Universal Time*.
Value Added Reseller	A company that adds features or services to an existing product and resells it (usually to end-users) as an integrated product or complete turn-key solution.
ValueLink	ValueLink is a prepaid or stored value card and is a funds-valued card issued to a cardholder by a merchant.
VAPS	Value Added Payment System. Proprietary Heartland Host processing system supporting the NTS and the POS 8583 specifications.
VAR	See *Value Added Reseller*.
VDDF	Variable Discretionary Data Field. See *Discretionary Data*.
Version	May refer to a document version or software version. Each time a new document or software revision is released, a revision version number is incremented.
VisaNet Integrated Payment (VIP)	Visa's main transaction processing system.

Table F-1 Glossary

Term	Definition
VisaNet Processors (VNP)	An entity that is directly connected to Visa through a VisaNet Extended Access Server (VEAS).
Voice Authorization	An authorization center operated either by issuers or by processors on behalf of issuers. It is used to respond to requests for authorizations for purchases from merchants who do not have terminals, or whose terminals are not functioning properly, or for transactions for which special assistance is required.
Void	An attendant initiated transaction request to cancel a recently completed transaction.
VSAT	Very Small Aperture Terminal. The hardware and software located at a merchant's location that allows POS communications via satellite.
Z01	A Heartland Proprietary POS Transaction Format.
Zero Balance	See *Cash Out*.