EMV Integrator's Guide

Version 15.2
October 2015

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. ALL SUCH WARRANTIES ARE EXPRESSLY DISCLAIMED.

HEARTLAND PAYMENT SYSTEMS SHALL NOT 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 PAYMENT SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. HEARTLAND PAYMENT SYSTEMS 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 HEARTLAND PAYMENT SYSTEMS INFORMATION. UNDER ANY CIRCUMSTANCES, RECIPIENT SHALL NOT DISCLOSE THIS DOCUMENT OR THE SYSTEM DESCRIBED HEREIN TO ANY THIRD PARTY WITHOUT PRIOR WRITTEN CONSENT OF A DULY AUTHORIZED REPRESENTATIVE OF HEARTLAND PAYMENT SYSTEMS. 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 ACKNOWLEDGEMENT 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 PRODUCTS OR SERVICES OF HEARTLAND PAYMENT SYSTEMS OR OF THIRD PARTIES ARE OWNED BY HEARTLAND PAYMENT SYSTEMS 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 Payment Systems contact.

Release Notes

Version 15.2 Release Notes

Version	Release Date	Revisions
1.0	07/15/2014	New document.
1.1	07/31/2014	Clarification updates.
1.2	11/21/2014	Portico updates.
1.2.1	12/19/2014	Removed references regarding preliminary and subject to change.
15.1.1	06/02/2014	Identified corrections and clarification updates.
15.2	10/30/2015	Restructured and applied updates.

Table of Contents

List of Tables

List of Figures

Chapter 1: Overview

1.1 Introduction

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

- Host Network transaction services
- Bank Card, 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 an overview of integrating EMV chip card technology on a POS system and interfacing to Heartland Payment Systems payment processing systems.

1.3 Audience

This document is intended for integrators who wish to develop EMV-capable POS solutions and interface them with Heartland's hosts for payment processing. It provides guidelines and recommendations for that effort.

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 Bank Card Companies (VISA, MasterCard, Discover, American Express, and JCB).

In order to comply with the mandates set by the bank card companies, Heartland Payment Systems:

- 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; Discover, including JCB, UnionPay, Carte Blanche, 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 Heartland 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: EMV Processing Overview

2.1 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*.

2.2 EMV Migration

2.2.1 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 2-1 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.

2.2.2 Card Brand Mandates

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

2.2.3 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 2-2 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.

2.2.4 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.

2.3 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:

2.3.1 Contact Specifications

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

Table 2-3 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 v3.0 (May 2015) • Integrated Circuit Card Specification v1.5 (May 2009)
MasterCard	• U.S. Market Terminal Requirements (April 2014)
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 v3.0 (Jan 2015) • D-PAS Terminal Specification v1.0 (Jun 2009)

2.3.2 Contactless Specifications

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

Table 2-4 Contactless Specifications

Source	Specification
EMVCo	• EMV Contactless Specifications v2.5 (Mar 2015) – 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 v3.0 (May 2015) • Contactless Payment Specification v2.1 (May 2009)
MasterCard	• U.S. Market Terminal Requirements (Apr 2014) • 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)

Table 2-4 Contactless Specifications

Source	Specification
Discover	• Contactless D-PAS Acquirer Implementation Guide v1.0 • Contactless D-PAS Terminal Application Specification v1.0

2.3.3 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 2-5 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

2.4 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.

2.4.1 Card Authentication

Table 2-6 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.

2.4.2 Cardholder Verification

Table 2-7 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.

2.4.3 Authorization

Table 2-8 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.

2.5 Full vs. Partial EMV Transactions and Flow

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

Table 2-9 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.

2.5.1 Full vs. Partial Transaction Flow

Table 2-10 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.

2.5.2 Full vs. Partial Credit Transactions

Table 2-11 Full vs. Partial Credit Transactions

EMV Transactions	Full EMV	Partial EMV	Notes
Online Purchase	✓		ARQC received at 1st 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.
Pre-Authorization	✓		
Incremental Authorization			No chip data should be sent.
Completion			No chip data should be sent.
Cash Advance	✓		
Bill Payment	✓		
Card Verify	✓		
Purchase Return		✓	To obtain PAN from chip if needed.
Void			PAN and chip data from original authorization should be sent.
Reversal on Timeout			PAN and chip data from original authorization should be sent.
Offline Decline Advice	✓		AAC received at 1st GENERATE AC or due to failed Issuer Authentication at 2nd GENERATE AC.

2.5.3 Full vs. Partial Debit Transactions

Table 2-12 Full vs. Partial Debit Transactions

EMV Transactions	Full EMV	Partial EMV	Notes
Online Purchase	✓		ARQC received at 1st GENERATE AC.
Purchase Return	✓		ARQC received at 1st GENERATE AC.
Void			PAN and chip data from original authorization should be sent.
Reversal on Timeout			PAN and chip data from original authorization should be sent.
Offline Decline Advice	✓		AAC received at 1st GENERATE AC or due to failed Issuer Authentication at 2nd GENERATE AC.

Chapter 3: EMV Development Overview

3.1 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'.

3.1.1 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 2.x, 3.x or 4.x approved PIN Entry Device (PED) or Encrypting PIN Pad (EPP), if you plan to support PIN.

3.1.2 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 v2.1 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 PayPass application kernel approved against the MasterCard Contactless Reader Specification v3.0.3 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 2.x, 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.

3.1.3 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.

3.2 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.

3.2.1 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 3-1 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.

3.2.2 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.

3.3 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.

3.3.1 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, PayPass, 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.

3.3.2 Test Plans

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

- *VISA Smart Debit/Credit (VSDC) Testing*
- *MasterCard Terminal Integration Process (M-TIP) Testing*
- *American Express Integrated Circuit Card Payment Specification (AEIPS) Testing*
- *Discover D-Payment Application Specification (D-PAS) Testing*

3.3.2.1 VISA Smart Debit/Credit (VSDC) Testing

Table 3-2 VSDC Testing

Test Plan	Description
Acquirer Device Validation Toolkit (ADVT) User Guide v6.1	Up to 32 test cases for EMV contact card acceptance.
qVSDC Device Module Test Cases v2.1	Up to 89 test cases for EMV contactless card acceptance. ***Required*** for stand-alone contactless readers. ***Optional*** for dual-interface (contact and contactless) integrated readers.
Contactless Device Evaluation Toolkit (CDET) User Guide v2.1	Up to 15 test cases for general contactless card acceptance.

3.3.2.2 MasterCard Terminal Integration Process (M-TIP) Testing

Table 3-3 M-TIP Testing

Test Plan	Description
M-TIP 2.0 Build 215 – M-TIP Subset	Up to 175 test cases for EMV contact card acceptance.
M-TIP 2.0 Build 215 – Field Interoperability Subset	Up to 89 test cases for EMV contact card acceptance.
M-TIP 2.0 Build 215 – Contactless Subset 6	Up to 23 test cases for EMV contactless card acceptance.
M-TIP 2.0 Build 215 – Contactless Subset 8	Up to 268 test cases for EMV contactless card acceptance.

3.3.2.3 American Express Integrated Circuit Card Payment Specification (AEIPS) Testing

Table 3-4 AEIPS Testing

Test Plan	Description
Global AEIPS Terminal Test Plan v6.0	Up to 34 test cases for EMV contact card acceptance.
Global Expresspay EMV Terminal End-to-End Test Plan v1.5	Up to 25 test cases for EMV contactless card acceptance.

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

Table 3-5 D-PAS Testing

Test Plan	Description
Contact D-PAS Acquirer-Terminal End-to-End Test Plan v1.3	Up to 52 test cases for EMV contact card acceptance.
Contactless D-PAS Acquirer-Terminal End-to-End Test Plan v1.2	Up to 33 test cases for EMV contactless card acceptance.

3.3.3 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.

3.3.4 Test Environments

Heartland currently has two EMV test environments:

Table 3-6 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.

3.3.5 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 3-7 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 3-7 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.

3.4 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 *EMVDevSupport@e-hps.com*.

Chapter 4: EMV Terminal Interface

4.1 EMV Terminal to Card Communication

4.1.1 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 4-1 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 4-2 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)

4.1.2 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.

4.1.3 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.

4.2 EMV Data Elements

4.2.1 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 4-3 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 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.

4.2.2 Terminal Data

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

Table 4-4 Terminal Data

Name	Tag	Length	Value	Description
ADDITIONAL TERMINAL CAPABILITIES	'9F40'	5	b	Indicates the data input and output capabilities of the terminal.

Byte 1 – Transaction Type Capability

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cash
x	1	x	x	x	x	x	x	Goods
x	x	1	x	x	x	x	x	Services
x	x	x	1	x	x	x	x	Cashback
x	x	x	x	1	x	x	x	Inquiry
x	x	x	x	x	1	x	x	Transfer
x	x	x	x	x	x	1	x	Payment
x	x	x	x	x	x	x	1	Administrative

Byte 2 – Transaction Type Capability

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cash Deposit
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

Table 4-4 Terminal Data (Continued)

<table>
<tr><th>Name</th><th>Tag</th><th>Length</th><th>Value</th><th>Description</th></tr>
<tr><td colspan="4"></td><td>
Byte 3 – Terminal Data Input 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>Numeric keys</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>Alphabetic and special character keys</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>Command keys</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>Function keys</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>
Byte 4 – Terminal Data Output 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>Print, attendant</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>Print, cardholder</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>Display, attendant</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>Display, cardholder</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>1</td><td>x</td><td>Code table 10</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>Code table 9</td></tr>
</table>
Byte 5 – Terminal Data Output 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>Code table 8</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>Code table 7</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>Code table 6</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>Code table 5</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>Code table 4</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>Code table 3</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>Code table 2</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>Code table 1</td></tr>
</table>
</td></tr>
<tr><td>AMOUNT, AUTHORIZED (NUMERIC)</td><td>‘9F02’</td><td>6</td><td>n 12</td><td>Authorized amount of the transaction (excluding adjustments).</td></tr>
</table>

Table 4-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description		
AMOUNT, OTHER (NUMERIC)	'9F03'	6	n 12	Secondary amount associated with the transaction representing a cashback amount.		
APPLICATION IDENTIFIER (AID) - TERMINAL	'9F33'	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. For online transactions, the terminal should generate the value as follows:		
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.

Table 4-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description
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 4-4 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.		
				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.		

Table 4-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description
TERMINAL ACTION CODE (TAC) – ONLINE	'FFC8'	5	b	Specifies the acquirer's conditions that cause a transaction to be transmitted online.
TERMINAL CAPABILITIES	'9F40'	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

Byte 3 – Security Capability

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	SDA
x	1	x	x	x	x	x	x	DDA
x	x	1	x	x	x	x	x	Card capture
x	x	x	0	x	x	x	x	RFU
x	x	x	x	1	x	x	x	CDA
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU

Table 4-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description
				x x x x x x x 0 RFU
TERMINAL COUNTRY CODE	'9F1A'	2	n 3	Indicates the country of the terminal, represented according to ISO 3166.
TERMINAL FLOOR LIMIT	'9F1B'	4	b	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.
TERMINAL RISK MANAGEMENT DATA	'9F1D'	1-8	b	Application-specific value used by the card for risk management purposes.
TERMINAL TYPE	'9F35'	1	n 2	Indicates the environment of the terminal, its communications capability, and its operational control.

Environment	Operational Control Provided by:		
	Financial Institution	Merchant	Cardholder
Attended • Online only	11	21	–
• Online with offline capability	12	22	–
• Offline only	13	23	–
Unattended • Online only	14	24	34
• Online with offline capability	15	25	35
• Offline only	16	26	36

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

Table 4-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description								
				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
				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

Table 4-4 Terminal Data (Continued)

<table>
<tr><th>Name</th><th>Tag</th><th>Length</th><th>Value</th><th>Description</th></tr>
<tr><td colspan="4"></td><td>
Byte 4
<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>Transaction exceeds floor limit</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>Lower consecutive offline limit exceeded</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>Upper consecutive offline limit exceeded</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>Transaction selected randomly for online processing</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>Merchant forced transaction online</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>
Byte 5 – Terminal Data Output 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>Default TDOL used</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>Issuer authentication failed</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>Script processing failed</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>Code table 5</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>Code table 4</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>Code table 3</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>Code table 2</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>Code table 1</td></tr>
</table>
</td></tr>
<tr><td>THRESHOLD VALUE FOR BIASED RANDOM SELECTION</td><td>—</td><td>4</td><td>b</td><td>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).</td></tr>
<tr><td>TRANSACTION CURRENCY CODE</td><td>‘5F2A’</td><td>2</td><td>n 3</td><td>Indicates the currency code of the transaction according to ISO 4217.</td></tr>
<tr><td>TRANSACTION CURRENCY EXPONENT</td><td>‘5F36’</td><td>1</td><td>n 1</td><td>Indicates the implied position of the decimal point from the right of the transaction amount represented according to ISO 4217.</td></tr>
</table>

Table 4-4 Terminal Data (Continued)

Name	Tag	Length	Value	Description
TRANSACTION DATE	'9A'	3	n 6 YYMMDD	Local date that the transaction was authorized.
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.

4.2.3 Card Data

The following data comes from the ICC:

Table 4-5 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 4-5 Card Data

<table>
<tr><th>Name</th><th>Tag</th><th>Length</th><th>Value</th><th colspan="9">Description</th></tr>
<tr><td colspan="4" rowspan="10"></td><td colspan="9">Byte 2</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>0</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Reserved for use by the EMV Contactless Specifications</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>
<tr><td>APPLICATION LABEL</td><td>‘50’</td><td>1–16</td><td>ans with the special character limited to space</td><td colspan="9">Mnemonic associated with the AID according to ISO/IEC 7816-5.</td></tr>
<tr><td>APPLICATION PREFERRED NAME</td><td>‘9F12’</td><td>1–16</td><td>ans</td><td colspan="9">Preferred mnemonic associated with the AID.</td></tr>
<tr><td>APPLICATION PRIMARY ACCOUNT NUMBER (PAN)</td><td>‘5A’</td><td>var. up to 10</td><td>cn var. up to 19</td><td colspan="9">Valid cardholder account number.</td></tr>
<tr><td>APPLICATION PRIMARY ACCOUNT NUMBER (PAN) SEQUENCE NUMBER</td><td>‘5F34’</td><td>1</td><td>n 2</td><td colspan="9">Identifies and differentiates cards with the same PAN.</td></tr>
<tr><td>APPLICATION PRIORITY INDICATOR</td><td>‘87’</td><td>1</td><td>b</td><td colspan="9">Indicates the priority of a given application or group of applications in a directory.</td></tr>
<tr><td>APPLICATION REFERENCE CURRENCY</td><td>‘9F3B’</td><td>2–8</td><td>n 3</td><td colspan="9">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.</td></tr>
<tr><td>APPLICATION REFERENCE CURRENCY EXPONENT</td><td>‘9F43’</td><td>1–4</td><td>n 1</td><td colspan="9">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.</td></tr>
</table>

Table 4-5 Card Data

<table>
<tr><th>Name</th><th>Tag</th><th>Length</th><th>Value</th><th>Description</th></tr>
<tr><td>APPLICATION TRANSACTION COUNTER (ATC)</td><td>'9F36'</td><td>2</td><td>b</td><td>Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC).</td></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.</td></tr>
<tr><td colspan="4"></td><td>
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>
</table>

Table 4-5 Card Data

Name	Tag	Length	Value	Description
CARD RISK MANAGEMENT DATA OBJECT LIST 2 (CDOL2)	'8D'	var. up to 252	b	List of data objects (tag and length) to be passed to the ICC in the second GENERATE AC command.
CARDHOLDER NAME	'5F20'	2–26	ans	Indicates cardholder name according to ISO 7813.
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

Table 4-5 Card Data

<table>
<tr><th>Name</th><th>Tag</th><th>Length</th><th>Value</th><th>Description</th></tr>
<tr><td colspan="4"></td><td>
<table>
<tr><td></td><td></td><td>1</td><td>1</td><td>x</td><td>x</td><td>x</td><td>x</td><td>Values in the range 110000-111110 reserved for use by the issuer</td></tr>
<tr><td></td><td></td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>This value is not available for use</td></tr>
</table>
CV Rule Byte 2
<table>
<tr><th>Value</th><th>Message</th></tr>
<tr><td>‘00’</td><td>Always</td></tr>
<tr><td>‘01’</td><td>If unattended cash</td></tr>
<tr><td>‘02’</td><td>If not unattended cash and not manual cash and not purchase with cashback</td></tr>
<tr><td>‘03’</td><td>If terminal supports the CVM</td></tr>
<tr><td>‘04’</td><td>If manual cash</td></tr>
<tr><td>‘05’</td><td>If purchase with cashback</td></tr>
<tr><td>‘06’</td><td>If transaction is in the application currency and is under X value</td></tr>
<tr><td>‘07’</td><td>If transaction is in the application currency and is over X value</td></tr>
<tr><td>‘08’</td><td>If transaction is in the application currency and is under Y value</td></tr>
<tr><td>‘09’</td><td>If transaction is in the application currency and is over Y value</td></tr>
<tr><td>‘0A’-‘7F’</td><td>RFU</td></tr>
<tr><td>‘80’-‘FF’</td><td>Reserved for card brands</td></tr>
</table>
</td></tr>
<tr><td>CERTIFICATION AUTHORITY PUBLIC KEY INDEX</td><td>‘8F’</td><td>1</td><td>b</td><td>Identifies the certification authority’s public key in conjunction with the RID.</td></tr>
<tr><td>CRYPTOGRAM INFORMATION DATA</td><td>‘9F27’</td><td>1</td><td>b</td><td>Indicates the type of cryptogram and the actions to be performed by the terminal.</td></tr>
<tr><td>DEDICATED FILE (DF) NAME</td><td>‘84’</td><td>5–16</td><td>b</td><td>Identifies the name of the DF as described in ISO/IEC 7816-4.</td></tr>
<tr><td>DIRECTORY DEFINITION FILE (DDF) NAME</td><td>‘9D’</td><td>5–16</td><td>b</td><td>Identifies the name of a DF associated with a directory.</td></tr>
<tr><td>DYNAMIC DATA AUTHENTICATION DATA OBJECT LIST (DDOL)</td><td>‘9F49’</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 INTERNAL AUTHENTICATE command.</td></tr>
<tr><td>FILE CONTROL INFORMATION (FCI) TEMPLATE</td><td>‘6F’</td><td>var. up to 252</td><td>var.</td><td>Identifies the FCI template according to ISO/IEC 7816-4.</td></tr>
<tr><td>ICC DYNAMIC NUMBER</td><td>‘9F4C’</td><td>2–8</td><td>b</td><td>Time-variant number generated by the ICC, to be captured by the terminal.</td></tr>
</table>

Table 4-5 Card Data

Name	Tag	Length	Value	Description
INTEGRATED CIRCUIT CARD (ICC) PIN ENCIPHERMENT PUBLIC KEY CERTIFICATE	'9F2D'	N_I	b	ICC PIN Encipherment Public Key certified by the issuer.
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.

Table 4-5 Card Data

Name	Tag	Length	Value	Description
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.
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.

Table 4-5 Card Data

Name	Tag	Length	Value	Description
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.

4.2.4 Issuer Data

The following data comes from the issuer:

Table 4-6 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.

4.3 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 4-1*.

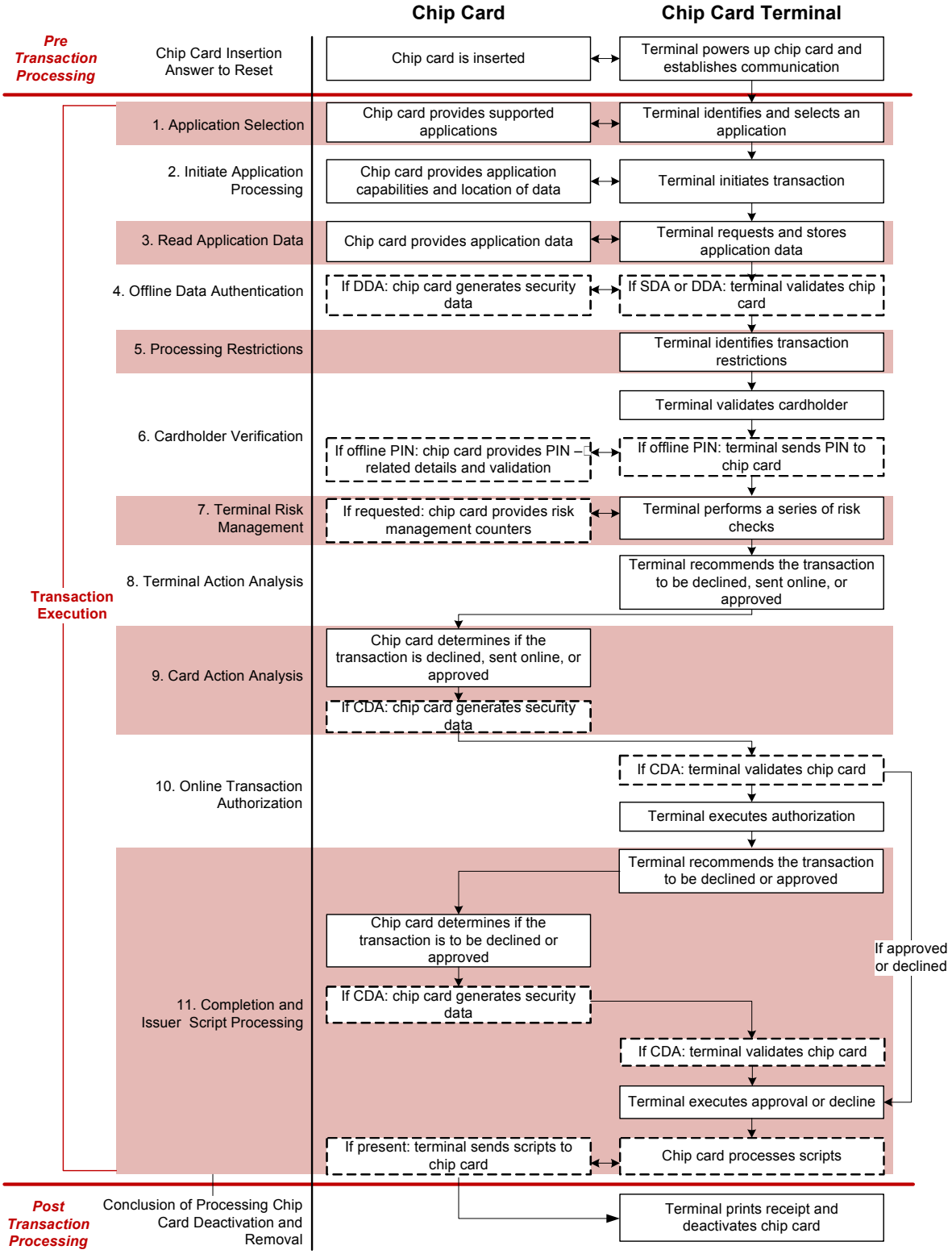

Figure 4-1 Contact Transaction Flow

4.3.1 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 4-7 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, Authorized (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, Authorized (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, Authorized (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.

4.3.2 Card Acquisition

4.3.2.1 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 3-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'.

4.3.2.2 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 there are two scenarios under which it is allowed:

Table 4-8 Fallback Processing

Fallback Scenario	Description
Technical Fallback	Unable to read chip card due to chip or chip reader failure.
Non-Technical Fallback	Empty application selection candidate list due to no mutually supported AIDs.

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.

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.

4.3.3 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 4-9 Application Selection

Component	Description
Registered Application Identifier (RID)	Each card brand has one or more RIDs (e.g. 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 (e.g. 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 (e.g. A000000003101001 for a VISA credit account and 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 4-10 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.

4.3.3.1 Available AIDs

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

	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.
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.
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. **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. **Not supported for PIN debit at this time**.
	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.

4.3.3.2 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 (2 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 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 the cardholder for selection as described in the Application Selection section above.

4.3.4 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 Locator (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.

4.3.5 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.

4.3.6 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 4-11 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.

4.3.7 Processing Restrictions

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

Table 4-12 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.

4.3.8 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 4-13 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.

4.3.8.1 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 4-14 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.
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.

4.3.9 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 4-15 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.

4.3.10 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 4-16 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.

4.3.11 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.

4.3.12 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.

4.3.12.1 Offline Authorization

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 below.

4.3.12.2 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 authorization response code returned in the authorization response.

4.3.12.3 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:

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

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.

4.3.13 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.

4.3.14 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.

4.3.15 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 Authorization Response Code (Tag '8A') should be set by the terminal based on the online or offline disposition as follows:

Table 4-17 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.

Table 4-17 Online or Offline Disposition (Continued)

Disposition	ASCII	Hex	Notes
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.

4.3.16 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.

4.4 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 4-2*.

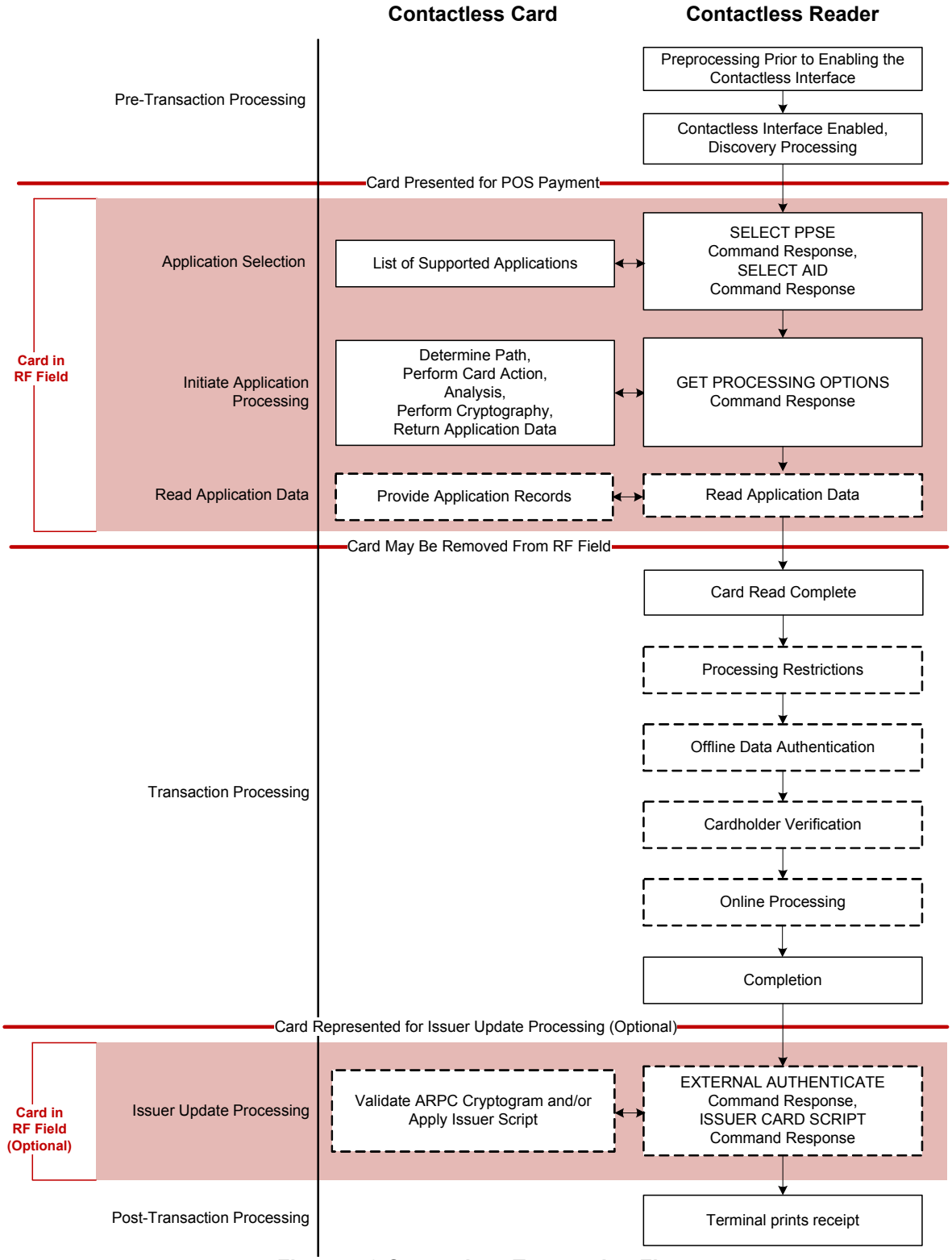

Figure 4-2 Contactless Transaction Flow

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 4-18 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.

4.4.1 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.

4.4.2 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.

4.4.3 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.

4.4.4 Initiate Application Processing

This step includes:

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

4.4.4.1 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.

4.4.4.2 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.

4.4.4.3 Terminal Action Analysis

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

4.4.4.4 Card Action Analysis

Same as contact EMV.

4.4.5 Read Application Data

Same as contact EMV.

4.4.6 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.

4.4.7 Processing Restrictions

Same as contact EMV.

4.4.8 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.

4.4.9 Cardholder Verification

Similar to contact EMV, but the offline enciphered/plaintext CVMs are not supported for contactless. In addition, contactless includes support for a new CVM which occurs on a separate device such as a mobile phone that is used to emulate a contactless card.

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

Table 4-19 Card Verification

Card Brand	Description
VISA	Consumer Device CVM
MasterCard	On Device CVM
American Express	Mobile CVM
Discover	Confirmation Code (Mobile) CVM

4.4.10 Online Processing

Same as contact EMV.

4.4.11 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.

4.4.12 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.

4.5 EMV Receipts

4.5.1 Approval Receipts

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

Table 4-20 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 4-3 EMV Receipt Example

4.5.2 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 5: EMV Parameter Interface

5.1 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 5-1 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:

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
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.

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

5.2 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.

5.3 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.

5.4 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 20, with an EMV PDL PARAMETER TYPE of **06** to request EMV download information.
- Terminal must send a MESSAGE CODE 20, with an EMV PDL PARAMETER TYPE of **07** to confirm receipt of each complete EMV table.

5.5 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.

5.6 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.

5.7 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.

Appendix

Appendix A: 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 A-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 A-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 A-1 EMV PDL Data Examples (Continued)

<table>
<tr><th colspan="2">POS</th><th>⇔</th><th>Host</th></tr>
<tr><td colspan="2">Table 10 Confirmation Request
(Versions and Flags)</td><td>⇨</td><td></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td></td><td></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>10</td><td></td><td></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td><2 spaces></td><td></td><td></td></tr>
<tr><td>EMV PDL PARAMETER VERSION</td><td>001</td><td></td><td></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td>Table 10 Confirmation Response
(Versions and Flags)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field / Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL PARAMETER VERSION: 001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER: 00</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID: 10</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE: <2 spaces></td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG: Y</td></tr>
<tr><td colspan="2">Table 30 Request
(Terminal Data)</td><td>⇨</td><td></td></tr>
<tr><td>Field</td><td>Value</td><td></td><td></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>06</td><td></td><td></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>30</td><td></td><td></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td><2 spaces></td><td></td><td></td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td><td></td><td></td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>01</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>⇦</td><td>Table 30 Response
(Terminal Data)</td></tr>
<tr><td colspan="2"></td><td></td><td>Field / Value</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE VERSION: 001</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER: 01</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE ID: 30</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE: <2 spaces></td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL END-OF-TABLE FLAG: Y</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TABLE DATA BLOCK LENGTH: 023</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TERMINAL TYPE: 22</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL ADDITIONAL TERMINAL CAPABILITIES: F000F0A001</td></tr>
</table>

Table A-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 COUNTRY CODE</td><td>840</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TRANSACTION CURRENCY CODE</td><td>840</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TRANSACTION CURRENCY EXPONENT</td><td>2</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TRANSACTION REFERENCE CURRENCY CODE</td><td>840</td></tr>
<tr><td colspan="2"></td><td></td><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>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 30 Confirmation Response
(Terminal 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>30</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CARD TYPE</td><td><2 spaces></td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
<tr><td colspan="2">Table 40 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>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>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 A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
	⇦	**Table 40 Response (VISA 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	01
		EMV PDL END-OF-TABLE FLAG	Y
		EMV PDL TABLE DATA BLOCK LENGTH	374
		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 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>

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		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
		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>
Table 40 Confirmation Request (VISA Contact Card Data)	⇨		
Field	**Value**		
EMV PDL PARAMETER TYPE	07		
EMV PDL TABLE ID	40		
EMV PDL CARD TYPE	01		
EMV PDL TABLE VERSION	001		
EMV PDL BLOCK SEQUENCE NUMBER	00		

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host
	⇦	**Table 40 Confirmation Response (VISA Contact Card Data)**

Field	Value
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	00
EMV PDL TABLE ID	40
EMV PDL CARD TYPE	01
EMV PDL CONFIRMATION FLAG	Y

⇨

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

Table A-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 THRESHOLD VALUE FOR BIASED RANDOM SELECTION</td><td>000000000000</td></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>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 colspan="2"></td><td>⇦</td><td colspan="2">Table 40 Confirmation Response
(MasterCard 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>02</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table>

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host

Table 40 Request (American Express Contact Card Data)

Field	Value
EMV PDL PARAMETER TYPE	06
EMV PDL TABLE ID	40
EMV PDL CARD TYPE	03
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01

⇨

⇦

Table 40 Response (American Express 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	03
EMV PDL END-OF-TABLE FLAG	Y
EMV PDL TABLE DATA BLOCK LENGTH	188
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 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	0000000000

Table A-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 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>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 colspan="2"></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td colspan="2"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>40</td><td colspan="2"></td></tr>
<tr><td>EMV PDL CARD TYPE</td><td>03</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>00</td><td colspan="2"></td></tr>
<tr><td></td><td>⇦</td><td colspan="2">Table 40 Confirmation Response
(American Express Contact Card Data)</td></tr>
<tr><td></td><td></td><td>Field</td><td>Value</td></tr>
<tr><td></td><td></td><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td></td><td></td><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>00</td></tr>
<tr><td></td><td></td><td>EMV PDL TABLE ID</td><td>40</td></tr>
<tr><td></td><td></td><td>EMV PDL CARD TYPE</td><td>03</td></tr>
<tr><td></td><td></td><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
<tr><td>Table 40 Request
(Discover Contact Card Data)</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>40</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>01</td><td colspan="2"></td></tr>
</table>

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
	⇦	**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
		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	FCE09CF800
		EMV PDL TERMINAL ACTION CODE (TAC) - DEFAULT	DC00002000
		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>

Table A-1 EMV PDL Data Examples (Continued)

POS ⇔ **Host**

Table 40 Confirmation Request (Discover Contact Card Data) ⇨

Field	Value
EMV PDL PARAMETER TYPE	07
EMV PDL TABLE ID	40
EMV PDL CARD TYPE	04
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	00

⇦ **Table 40 Confirmation Response (Discover Contact Card Data)**

Field	Value
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	00
EMV PDL TABLE ID	40
EMV PDL CARD TYPE	04
EMV PDL CONFIRMATION FLAG	Y

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

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		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
		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

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		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
		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>
Table 50 Confirmation Request (VISA Contactless Card Data)	⇨		
Field / **Value**			
EMV PDL PARAMETER TYPE / 07			
EMV PDL TABLE ID / 50			
EMV PDL CARD TYPE / 01			
EMV PDL TABLE VERSION / 001			
EMV PDL BLOCK SEQUENCE NUMBER / 00			
	⇦	**Table 50 Confirmation Response (VISA Contactless Card Data)**	
		Field	**Value**
		EMV PDL TABLE VERSION	001
		EMV PDL BLOCK SEQUENCE NUMBER	00
		EMV PDL TABLE ID	50
		EMV PDL CARD TYPE	01
		EMV PDL CONFIRMATION FLAG	Y

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host

Table 50 Request (MasterCard Contactless Card Data) ⇨

Field	Value
EMV PDL PARAMETER TYPE	06
EMV PDL TABLE ID	50
EMV PDL CARD TYPE	02
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01

⇦ **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

Table A-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 ACTION CODE (TAC) - DEFAULT</td><td>FC509C8800</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TERMINAL TRANSACTION QUALIFIERS (TTQ)</td><td>B6000000</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL TERMINAL RISK MANAGEMENT DATA</td><td>6CF8000000000000</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
(MasterCard 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>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 colspan="2"></td><td>⇦</td><td colspan="2">Table 50 Confirmation Response
(MasterCard 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 PARAMETER 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>02</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
(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>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>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>
</table>

Table A-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
		EMV PDL TERMINAL RISK MANAGEMENT DATA	<16 spaces>
		EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)	<32 spaces>

Table A-1 EMV PDL Data Examples (Continued)

POS ⇔ **Host**

Table 50 Confirmation Request (American Express Contactless Card Data) ⇨

Field	Value
EMV PDL PARAMETER TYPE	07
EMV PDL TABLE ID	50
EMV PDL CARD TYPE	03
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	00

⇦ **Table 50 Confirmation Response (American Express Contactless Card Data)**

Field	Value
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	00
EMV PDL TABLE ID	50
EMV PDL CARD TYPE	03
EMV PDL CONFIRMATION FLAG	Y

Table 50 Request (Discover Contactless Card Data) ⇨

Field	Value
EMV PDL PARAMETER TYPE	06
EMV PDL TABLE ID	50
EMV PDL CARD TYPE	04
EMV PDL TABLE VERSION	001
EMV PDL BLOCK SEQUENCE NUMBER	01

⇦ **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

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		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
		EMV PDL TERMINAL RISK MANAGEMENT DATA	<16 spaces>
		EMV PDL DEFAULT TRANSACTION CERTIFICATE DATA OBJECT LIST (TDOL)	<32 spaces>
Table 50 Confirmation Request (Discover Contactless Card Data)	⇨		
Field / **Value**			
EMV PDL PARAMETER TYPE / 07			
EMV PDL TABLE ID / 50			
EMV PDL CARD TYPE / 04			
EMV PDL TABLE VERSION / 001			
EMV PDL BLOCK SEQUENCE NUMBER / 00			

Table A-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th>Host</th></tr>
<tr><td></td><td>⇦</td><td>Table 50 Confirmation Response
(Discover 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>04</td></tr>
<tr><td>EMV PDL CONFIRMATION FLAG</td><td>Y</td></tr>
</table></td></tr>
<tr><td>Table 60 Request
(VISA 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>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 60 Response
(VISA 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>01</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 A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		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
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	A89F25A56FA6DA258C8CA8B40427D927B4A1EB4D7EA326BBB12F97DED70AE5E4480FC9C5E8A972177110A1CC318D06D2F8F5C4844AC5FA79A4DC470BB11ED635699C17081B90F1B984F12E92C1C529276D8AF8EC7F28492097D8CD5BECEA16FE4088F6CFAB4A1B42328A1B996F9278B0B7E3311CA5EF856C2F888474B83612A82E4E00D0CD4069A6783140433D50725F
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	B4BC56CC4E88324932CBC643D6898F6FE593B172

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		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
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	D9FD6ED75D51D0 E30664BD157023E AA1FFA871E4DA65 672B863D255E81E 137A51DE4F72BCC 9E44ACE12127F87 E263D3AF9DD9CF 35CA4A7B01E9070 00BA85D24954C2F CA3074825DDD4C 0C8F186CB020F68 3E02F2DEAD39691 33F06F7845166AC EB57CA0FC260344 5469811D293BFEF BAFAB57631B3DD9 1E796BF850A2501 2F1AE38F05AA5C4 D6D03B1DC2E5686 12785938BBC9B3C D3A910C1DA55A5 A9218ACE0F7A212 87752682F15832A6 78D6E1ED0B
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	20D213126955DE2 05ADC2FD2822BD 22DE21CF9A8

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		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	9D912248DE0A4E39C1A7DDE3F6D2588992C1A4095AFBD1824D1BA74847F2BC4926D2EFD904B4B54954CD1
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 A-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 MODULUS</td><td>89A54C5D1179654
F8F9B0D2AB5F035
7EB642FEDA95D39
12C6576945FAB89
7E7062CAA44A4AA
06B8FE6E3DBA18A
F6AE3738E30429E
E9BE03427C9D64F
695FA8CAB4BFE37
6853EA34AD1D76B
FCAD15908C077FF
E6DC5521ECEF5D
278A96E26F57359F
FAEDA19434B937F
1AD999DC5C41EB
11935B44C18100E8
57F431A4A5A6BB6
5114F174C2D7B59
FDF237D6BB1DD0
916E644D709DED5
6481477C75D95CD
D68254615F7740E
C07F330AC5D67B
CD75BF23D28A140
826C026DBDE971A
37CD3EF9B8DF644
AC385010501EFC6
509D7A41</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT</td><td>03</td></tr>
<tr><td colspan="2"></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM</td><td>1FF80A40173F52D
7D27E0F26A146A1
C8CCB29046</td></tr>
<tr><td colspan="2">Table 60 Confirmation Request
(VISA Public Key Data)</td><td>⇨</td><td colspan="2" rowspan="6"></td></tr>
<tr><th>Field</th><th>Value</th><td></td></tr>
<tr><td>EMV PDL PARAMETER TYPE</td><td>07</td><td rowspan="5"></td></tr>
<tr><td>EMV PDL TABLE ID</td><td>60</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>

Table A-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 A-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	A6DA428387A502D 7DDFB7A74D3F412 BE762627197B2543 5B7A81716A700157 DDD06F7CC99D6C A28C2470527E2C0 3616B9C59217357 C2674F583B3BA5C 7DCF2838692D023 E3562420B4615C4 39CA97C44DC9A24 9CFCE7B3BFB22F 68228C3AF13329A A4A613CF8DD8535 02373D62E49AB25 6D2BC17120E54AE DCED6D96A4287A CC5C04677D4A5A3 20DB8BEE2F775E5 FEC5
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	381A035DA58B482 EE2AF75F4C3F2C A469BA4AA6C

Table A-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	B8048ABC30C90D976336543E3FD7091C8FE4800DF820ED55E7E94813ED00555B573FECA3D84AF6131A651D66CFF4284FB13B635EDD0EE40176D8BF04B7FD1C7BACF9AC7327DFAA8AA72D10DB3B8E70B2DDD811CB4196525EA386ACC33C0D9D4575916469C4E4F53E8E1C912CC618CB22DDE7C3568E90022E6BBA770202E4522A2DD623D180E215BD1D1507FE3DC90CA310D27B3EFCCD8F83DE3052CAD1E48938C68D095AAC91B5F37E28BB49EC7ED597
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	EBFA0D5D06D8CE702DA3EAE890701D45E274C845

Table A-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 colspan="2">MasterCard 1984-Bit Key (Active)</td></tr>
<tr><td></td><td></td><td>EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)</td><td>A000000004</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX</td><td>06</td></tr>
<tr><td></td><td></td><td>EMV PDL KEY STATUS</td><td>A</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH</td><td>0496</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS</td><td>CB26FC830B43785 B2BCE37C81ED33 4622F9622F4C89A AE641046B2353433 883F307FB7C9741 62DA72F7A4EC75D 9D657336</td></tr>
<tr><td colspan="2">Table 60 Request
(MasterCard Public Key Data Continued)</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>02</td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td>⇦</td><td colspan="2">Table 60 Response
(MasterCard Public Key Data Continued)</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>02</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL TABLE ID</td><td>60</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL CARD TYPE</td><td>01</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL END-OF-TABLE FLAG</td><td>Y</td></tr>
<tr><td></td><td></td><td></td><td>EMV PDL TABLE DATA BLOCK LENGTH</td><td>440</td></tr>
</table>

Table A-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>865B8D3023D3D64
5667625C9A07A6B
7A137CF0C64198A
E38FC238006FB26
03F41F4F3BB9DA1
347270F2F5D8C60
6E420958C5F7D50
A71DE30142F70DE
468889B5E3A08695
B938A50FC980393
A9CBCE44AD2D64
F630BB33AD3F5F5
FD495D31F37818C
1D94071342E07F1
BEC2194F6035BA5
DED3936500EB82D
FDA6E8AFB655B1
EF3D0D7EBF86B66
DD9F29F6B1D324F
E8B26CE38AB2013
DD13F611E7A594D
675C4432350EA24
4CC34F3873CBA06
592987A1D7E852A
DC22EF5A2EE2813
2031E48F74037E3
B34AB747F</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>F910A1504D5FFB7
93D94F3B500765E
1ABCAD72D9</td></tr>
<tr><td colspan="2">Table 60 Confirmation Request
(MasterCard 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>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>
</table>

Table A-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 A-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 A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	C8D5AC27A5E1FB 89978C7C6479AF9 93AB3800EB24399 6FBB2AE26B67B23 AC482C4B746005A 51AFA7D2D83E894 F591A2357B30F85 B85627FF15DA122 90F70F05766552BA 11AD34B7109FA49 DE29DCB01096708 75A17EA95549E92 347B948AA1F0457 56DE56B707E3863 E59A6CBE99C1272 EF65FB66CBB4CF F070F36029DD762 18B21242645B51C A752AF37E70BE1A 84FF31079DC0048 E928883EC4FADD4 97A719385C2BBBE BC5A66AA5E5655D 18034EC5
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	A73472B3AB55749 3A9BC2179CC8014 053B12BAB4
		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	CF98DFEDB3D372 7965EE7797723355 E0751C81D2D3DF4 D18EBAB9FB9D49 F38C8C4A826B99D C9DEA3F0104

Table A-1 EMV PDL Data Examples (Continued)

<table>
<tr><th>POS</th><th>⇔</th><th>Host</th></tr>
<tr><td>
Table 60 Request
(American Express Public Key Data Continued)
<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>03</td></tr>
<tr><td>EMV PDL TABLE VERSION</td><td>001</td></tr>
<tr><td>EMV PDL BLOCK SEQUENCE NUMBER</td><td>02</td></tr>
</table>
</td><td>⇨</td><td></td></tr>
<tr><td></td><td>⇦</td><td>
Table 60 Response
(American Express Public Key Data Continued)
<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>02</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 END-OF-TABLE FLAG</td><td>Y</td></tr>
<tr><td>EMV PDL TABLE DATA BLOCK LENGTH</td><td>453</td></tr>
<tr><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS</td><td>3D4BF22AC3550E2
962A59639B133215
6422F788B9C16D4
0135EFD1BA94147
750575E636B6EBC
618734C91C1D1BF
3EDC2A46A439016
68E0FFC13677408
0E888044F6A1E65
DC9AAA8928DACB
EB0DB55EA351468
6C6A732CEF55EE2
7CF877F110652694
A0E3484C855D882
AE191674E25C296
205BBB599455176
FDD7BBC549F27B
A5FE35336F7E29E
68D7839731994366
33C67EE5A680F05
160ED12D1665EC8
3D1997F10FD05BB
DBF9433E8F797AE
E3E9F02A34228AC
E927ABE62B8B928
1AD08D3DF5C7379
685045D7BA5FCDE
58637</td></tr>
</table>
</td></tr>
</table>

Table A-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 EXPONENT</td><td>03</td></tr>
<tr><td></td><td></td><td>EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM</td><td>C729CF2FD262394 ABC4CC173506502 446AA9B9FD</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>
<tr><td colspan="2"></td><td>⇦</td><td colspan="2">Table 60 Confirmation Response
(American Express 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>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 60 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>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>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 A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
	⇦	**Table 60 Response (Discover 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	04
		EMV PDL END-OF-TABLE FLAG	N
		EMV PDL TABLE DATA BLOCK LENGTH	875
		EMV PDL KEY COUNT	04
		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	8D1727AB9DC852453193EA0810B110F2A3FD304BE258338AC2650FA2A040FA10301EA53DF18FD9F40F55C44FE0EE7C7223BC649B8F9328925707776CB86F3AC37D1B22300D0083B49350E09ABB4B62A96363B01E4180E158EADDD6878E85A6C9D56509BF68F0400AFFBC441DDCCDAF9163C4AACEB2C3E1EC13699D23CDA9D3AD
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	E0C2C1EA411DB24EC3E76A9403F0B7B6F406F398

Table A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		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
		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 A-1 EMV PDL Data Examples (Continued)

POS	⇔	Host	
		Discover 1408-Bit Key (Active)	
		EMV PDL REGISTERED APPLICATION PROVIDER IDENTIFIER (RID)	A000000152
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY INDEX	04
		EMV PDL KEY STATUS	A
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS LENGTH	0352
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY MODULUS	8EEEC0D6D3857F D558285E49B623B 109E6774E06E9476 FE1B2FB273685B5 A235E955810ADDB 5CDCC2CB6E1A97 A07089D7FDE0A54 8BDC622145CA2D E3C73D6B14F284B 3DC1FA056FC0FB2 818BCD7C852F0C9 7963169F01483CE1 A63F0BF899D412A
Table 60 Request (Discover Public Key Data Continued)	⇨		
Field	**Value**		
EMV PDL PARAMETER TYPE	06		
EMV PDL TABLE ID	60		
EMV PDL CARD TYPE	04		
EMV PDL TABLE VERSION	001		
EMV PDL BLOCK SEQUENCE NUMBER	02		

Table A-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	B67C5BBDC8B4F6 FB9ABB57E951253 63DBD8F5EBAA9B 74ADB9320205034 1833DEE8E38D28B D175C83A6EA720C 262682BEABEA8E9 55FE67BD9C2EFF7 CB9A9F45DD5BDA 4A1EEFB148BC44F FF68D9329FD
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	17F971CAF6B708E 5B9165331FBA915 93D0C0BF66

Table A-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	E1200E9F4428EB71A526D6BB44C957F18F27B20BACE978061CCEF23532DBEBFAF654A149701C14E6A2A7C2ECAC4C92135BE3E9258331DDB0967C3D1D375B996F25B77811CCCC06A153B4CE6990A51A0258EA8437EDBEB701CB1F335993E3F48458BC1194BAD29BF683D5F3ECB984E31B7B9D2F6D947B39DEDE0279EE45B47F2F3D4EEEF93F9261F8F5A571AFBFB569C150370A78F6683D687CB677777B2E7ABEFCFC8F5F93501736997E8310EE0FD87AFAC5DA772BA277F88B44459FCA563555017CD0D66771437F8B6608AA1A665F88D846403E4C41AFEEDB9729C2B2511CFE228B50C1B152B2A60BBF61D8913E086210023A3AA499E423
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY EXPONENT	03
		EMV PDL CERTIFICATION AUTHORITY PUBLIC KEY CHECKSUM	12BCD407B6E627A750FDF629EE8C2C9CC7BA636A

Table A-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 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>