EMV®
Contactless Specifications for Payment Systems

Book C-6

Kernel 6 Specification

Version 2.6
February 2016

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Legal Notice

Unless the user has an applicable separate agreement with EMVCo or with the applicable payment system, any and all uses of these Specifications is subject to the terms and conditions of the EMVCo Terms of Use agreement available at www.emvco.com and the following supplemental terms and conditions.

Except as otherwise may be expressly provided in a separate agreement with EMVCo, the license granted in the EMVCo Terms of Use specifically excludes (a) the right to disclose, distribute or publicly display these Specifications or otherwise make these Specifications available to any third party, and (b) the right to make, use, sell, offer for sale, or import any software or hardware that practices, in whole or in part, these Specifications. Further, EMVCo does not grant any right to use the Kernel Specifications to develop contactless payment applications designed for use on a Card (or components of such applications). As used in these supplemental terms and conditions, the term “Card” means a proximity integrated circuit card or other device containing an integrated circuit chip designed to facilitate contactless payment transactions. Additionally, a Card may include a contact interface and/or magnetic stripe used to facilitate payment transactions. To use the Specifications to develop contactless payment applications designed for use on a Card (or components of such applications), please contact the applicable payment system. To use the Specifications to develop or manufacture products, or in any other manner not provided in the EMVCo Terms of Use, please contact EMVCo.

These Specifications are provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THESE SPECIFICATIONS.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to the Specifications. EMVCo undertakes no responsibility to determine whether any implementation of these Specifications may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of these Specifications should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, the Specifications may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement these Specifications is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with these Specifications.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Contents

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figures

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Tables

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

[This page is intentionally left blank.]

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

1 Introduction

This *EMV Contactless Specifications for Payment Systems, Book C-6, Kernel 6 Specification* (this Specification) addresses the requirements applicable to Kernel 6, including the:

- Kernel 6 Approach,
- Terminal Transaction Processing Steps, and
- Application Protocol Data Unit (APDU) Commands.

Baseline functionalities are addressed in [EMV Book B], which should be read as a companion document and is hereby incorporated into this specification by reference. These baseline functionalities include, but are not limited to:

- Preliminary Transaction Processing (i.e., Pre-Processing),
- Protocol Activation,
- Combination Selection,
- Kernel Activation,
- Outcome Processing, and
- Data Element Processing.

1.1 Scope

This Specification describes one of several Kernels defined for use with Entry Point.

1.2 Audience

This Specification is intended for use by system designers in payment systems and financial institution staff responsible for implementing financial applications.

Note: Throughout this Specification, Contactless Cards and Mobile Devices are referenced as Contactless Cards unless Contactless and Mobile Devices must be addressed separately.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

1.3 Volumes of Contactless Specifications

This Specification is part of an EMVCo ten-volume set, including:

- Book A: Architecture and General Requirements [EMV Book A]
- Book B: Entry Point Specification [EMV Book B]
- Book C-1: Kernel 1 Specification
- Book C-2: Kernel 2 Specification
- Book C-3: Kernel 3 Specification
- Book C-4: Kernel 4 Specification
- Book C-5: Kernel 5 Specification
- Book C-6: Kernel 6 Specification
- Book C-7: Kernel 7 Specification
- Book D: Contactless Communication Protocol [EMV Book D]

1.4 Reference Specifications

In addition to the volumes cited in section 1.3, the following specifications and standards contain provisions that are referenced in this Specification. The latest version shall apply unless a publication date is explicitly stated.

If any provision or definition in this Specification differs from those in the listed specifications and standards, the provision or definition herein shall take precedence.

Abbreviation	Title
[EMV Book 1]	EMV Integrated Circuit Card Specifications for Payment Systems. Book 1 - Application Independent ICC to Terminal Interface Requirements.
[EMV Book 2]	EMV Integrated Circuit Card Specifications for Payment Systems. Book 2 - Security and Key Management.
[EMV Book 3]	EMV Integrated Circuit Card Specifications for Payment Systems. Book 3 - Application Specification.
[EMV Book 4]	EMV Integrated Circuit Card Specifications for Payment Systems. Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements.
[ISO/IEC 639-1]	Codes for the representation of names of languages – Part 1: Alpha-2 Code.
[ISO/IEC 3166-1]	Codes for the representation of names of countries and their subdivisions Part 1 Country Codes.
[ISO/IEC 4217]	Codes for the representation of currencies and funds.
[ISO/IEC 7810]	Information technology – Identification cards – Physical characteristics.
[ISO/IEC 7813]	Information technology – Identification cards – Financial transaction cards.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Abbreviation	Title
[ISO/IEC 7816-4]	Information technology – Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange.
[ISO/IEC 7816-5]	Identification cards – Integrated circuit cards – Part 5: Registration of application providers.
[ISO/IEC 8583-1]	Financial transaction card originated messages – Interchange message specifications – Part 1: Messages, data elements and code values.
[ISO/IEC 8825-1]	Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
[ISO/IEC 8859-1]	Information Technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1.
[ISO/IEC 9797-1]	Information technology – Security techniques - Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.
[ISO/IEC 10116]	Information technology – Security techniques - modes of operation for an n-bit block cipher.
[ISO/IEC 13239]	Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures.
[ISO/IEC 14443-1]	Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics.
[ISO/IEC 14443-2]	Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface.
[ISO/IEC 14443-3]	Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anti-collision.
[ISO/IEC 14443-4]	Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol.

1.5 Overview

This volume includes the following chapters and annexes:

- **Chapter 1:** contains general information regarding this Specification.
- **Chapter 2:** provides a high-level description of the Kernel 6 approach, including configurations of the supported modes, transaction processing flows, terminal and configuration requirements and options, and supported APDU commands.
- **Chapter 3:** specifies detailed transaction processing flows for Kernel 6.
- **Chapter 4:** lists and describes the APDU commands used by Kernel 6.
- **Annex A:** is a glossary of terms and abbreviations used in this specification.
- **Annex B:** contains Kernel 6 Transaction Parameters and Outcomes.
- **Annex C:** lists data elements required for offline only, online only, and offline / online transactions.
- **Annex D:** is a dictionary of data elements for Kernel 6.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

- **Annex E:** specifies the Track Data for MS Mode and Legacy MS Mode Transactions.

1.6 Data Conventions

The data conventions included in Table 1-1 are used throughout this Specification.

Table 1-1: Data Conventions

Convention	Description
'…'	Single quotation marks surround a decimal or hexadecimal digit. For example '3A' or '9901'
[…]	Squared brackets surround a reference document. For example: [EMV Book A].
A	Alphanumeric
b	Binary
n	Numeric
Var	Variable length

For data elements that have multiple bytes, the first byte or byte 1 is the leftmost byte, while the last byte is the rightmost byte.

1.7 Terminology

The terminology used in this specification is presented in Table 1-2.

Table 1-2: Terminology

Term	Definition
Shall, must, or required	Denotes a mandatory requirement
Should	Denotes a recommendation
May or optional	Denotes an optional feature

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

2 Overview of Kernel 6 Approach

A high-level description of the Kernel 6 approach is provided in the following sections:

- 2.1: Configuration of Supported Modes
- 2.2: Transaction Processing Flows
- 2.3: Configuration, Functionality, and APDU Command Support

2.1 Configuration of Supported Modes

The Kernel 6 approach supports three principle configurations: EMV Mode, Magnetic Stripe Mode (MS Mode), and Legacy MS Mode or both EMV and MS Modes. EMV Mode allows the processing of transactions offline or online (based on Terminal capabilities), while MS Mode and Legacy MS Mode only support transactions completed online with:

- **EMV Mode** – Functioning as an operating mode that relies on an infrastructure created via data elements and configuration settings in a chip application, and
- **MS Mode and Legacy MS Mode** – Functioning as an operating mode based on the use of Track 1 and Track 2 equivalent data.

Access to a particular configuration is enabled by a designated Application Identifier (AID) assigned to EMV Mode and MS Mode ('A0000001523010') and another specified for Legacy MS Mode ('A0000003241010').

2.1.1 EMV Mode (Offline or Online Transactions)

EMV Mode conforms to the EMV requirements supporting offline and online capabilities including the functionalities and commands for:

- Selecting the application, initializing transaction processing, and reading records to obtain the application data items,
- Performing Cardholder Verification and Offline Data Authentication (ODA) for offline transactions,
- Enabling Processing Restrictions, Terminal Action Analysis, Online Processing, and Issuer Update Processing for online transactions, and
- Supporting security parameters, including an optimized cryptographic process that enables the generation of an Application Cryptogram (AC) or Combined Dynamic Data Authentication / Application Cryptogram Generation (CDA) using the Unpredictable Number (UN) provided by the reader in the Processing Data Objects List (PDOL).

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Unlike ***contact*** EMV-based transactions, the reader performs certain checks before the card enters the Radio Frequency (RF) field as specified in [EMV Book B] and after the card has left the RF field. Additional information regarding EMV Mode is provided in Section 3 of this Specification.

2.1.2 MS Mode or Legacy MS Mode (Online Only Transactions)

MS Mode and Legacy Zip Mode use Track 1 and Track 2 equivalent data, which contain the same fields as that of a magnetic stripe card. In addition, MS Mode and Legacy Mode support the inclusion of a Dynamic Card Verification Value (DCVV) in Track 1 and Track 2.

Both Track 1 and Track 2 shall be coded according to [ISO/IEC7813].

2.2 Transaction Processing Flows

Transaction Processing Flows for the MS and Legacy MS Modes and EMV Mode are provided in the following sections.

2.2.1 MS Mode and Legacy MS Mode Processing Flow (Online Only Processing)

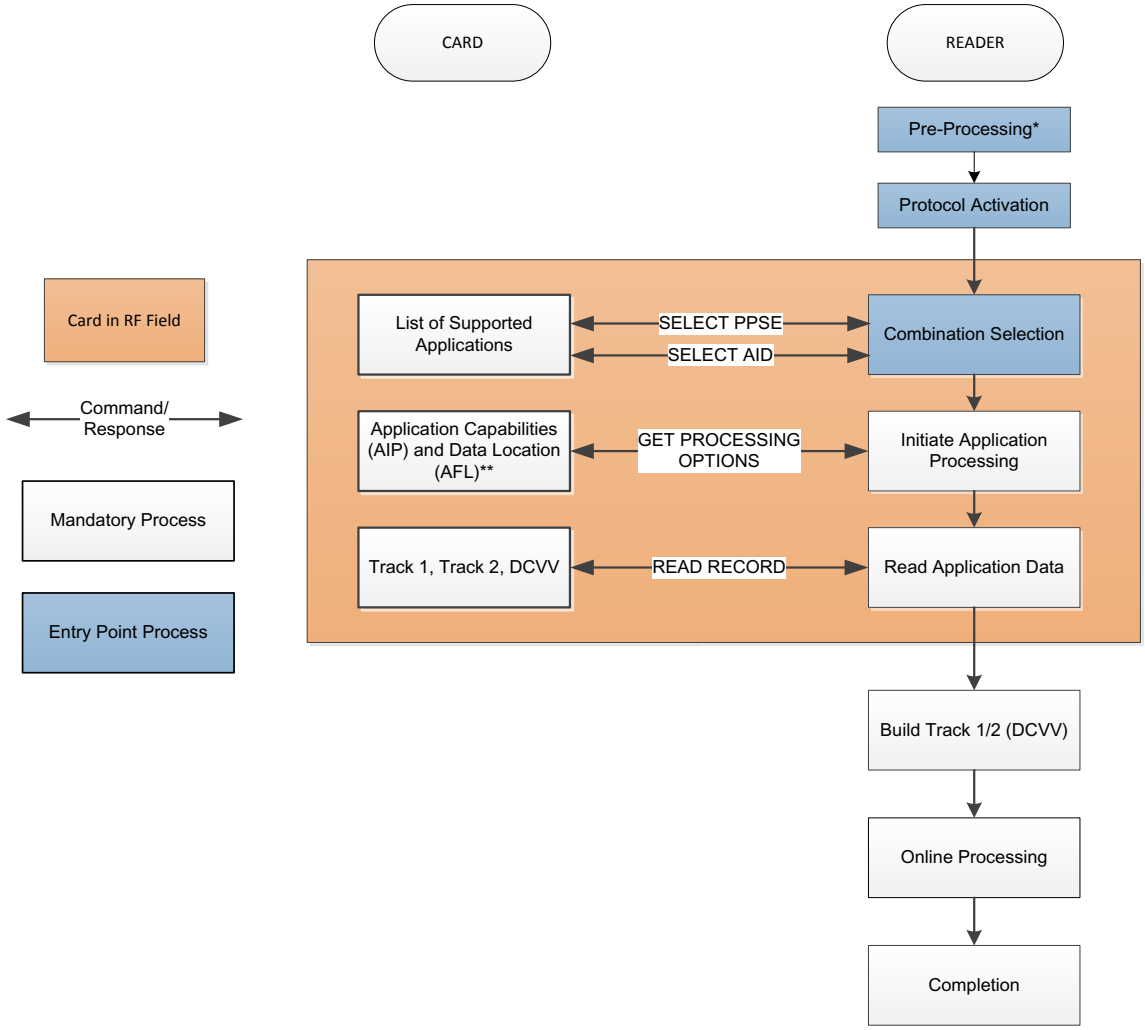
MS Mode and Legacy MS Mode offer enhanced magnetic stripe payment services using Track 1 and Track 2 equivalent data retrieved from the Contactless Card over the contactless interface.

Unlike a magnetic stripe card, both MS Mode and Legacy MS Mode have the ability to generate a DCVV. If supported, the DCVV is integrated into the build of the Track 1 data and Track 2 data to be transmitted to the Issuer in an Authorization Request.

The Authorization Request is sent via online messages defined by the payment scheme for Outcome Processing. Both DCVV-supported and Non-DCVV-supported configurations, which are described in detail in Annex E, provide data for online messages and clearing records. The MS Mode and Legacy MS Mode transaction flow is illustrated in Figure 2-1.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 2-1: Magnetic Stripe Mode and Legacy MS Mode - Transaction Flow



Notes:

*Pre-processing may be optional at Legacy MS Contactless Readers.

**Transaction-Specific Application Data are provided in Table 4-3.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

2.2.2 EMV Mode Processing Flow

The Kernel will initiate the transaction in EMV Mode, when the mode is supported by both the card and the Kernel and the transaction passes the required PDOL checks.

Terminal entry point shall perform the pre-processing and combination selection prior to the activation of the contactless interface of the reader and before the cardholder is invited to present a Contactless Card. Because the interaction (i.e., the command-response) between the card and the Terminal can only occur when the card is in the RF field, the process requires adaptations to permit the:

- Reduction of the number of commands and adjustment of the transaction flow for both the first and second presentment processes,
- Definition of data elements taking into account events relevant for contactless transactions,
- Usage of Entry Point as defined for [EMV Book B], to select the application and activate the corresponding Contactless Kernel 6,
- Generation of a CDA Cryptogram for an offline transaction or an Application Cryptogram for an online transaction during the transaction initiation,
- Execution of Terminal Risk Management before the card is placed in the field and after the card is removed from the field, and
- If required, execution of cardholder verification after the card is removed from the field.

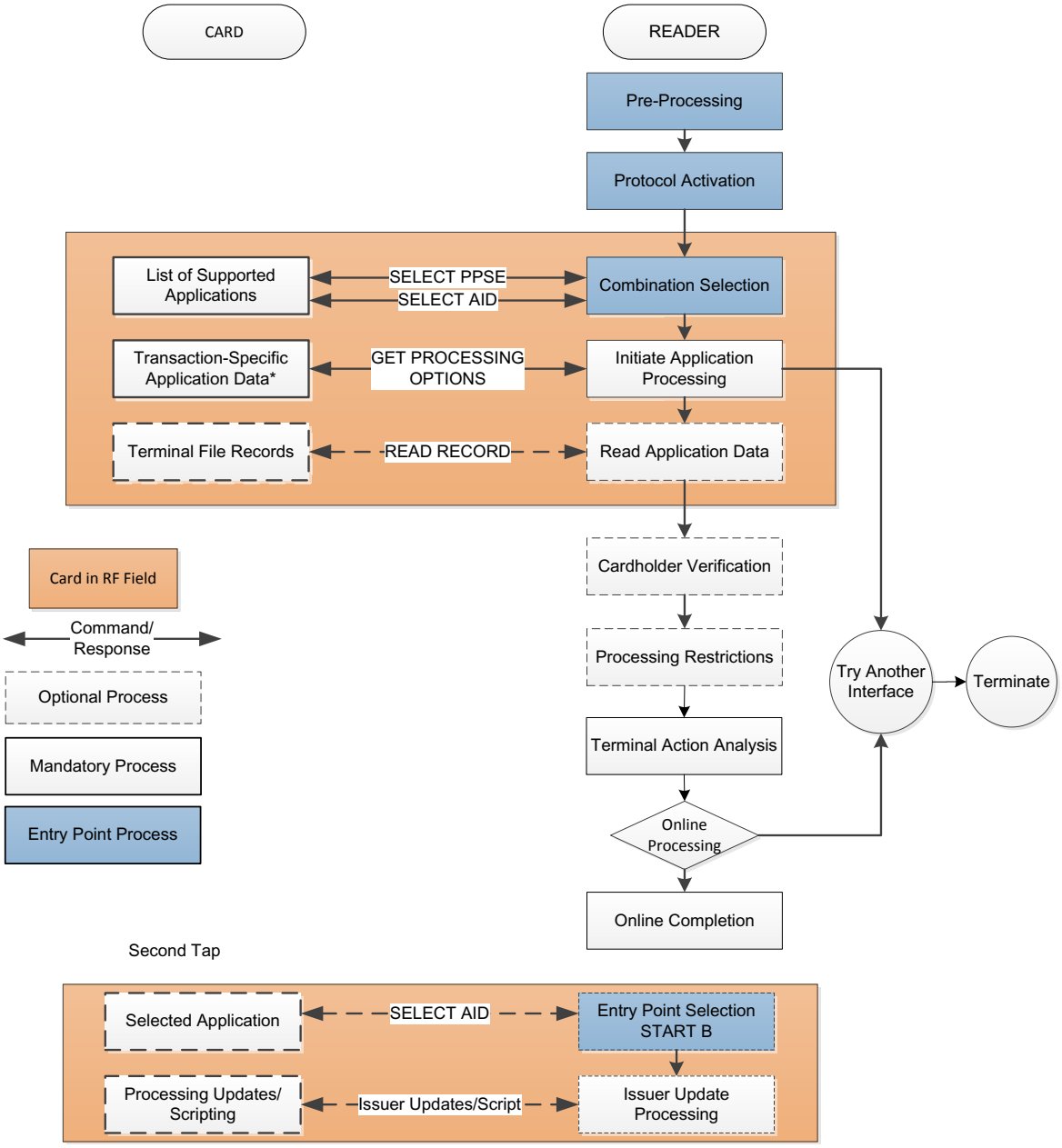
Issuers may allow a Contactless Card to be presented a second time (via a second presentment) for updating application data. The need for a second presentment is determined by the contactless reader by checking for the presence of Issuer scripts included in the authorization request response. The reader shall store the fields that are required for a second presentment in transient memory as specified in [EMV Book B]. Entry Point uses this transient memory to select the Combination used in the previous Final Combination Selection to deliver the Issuer Update Processing commands.

The EMV Mode configuration uses the Outcome parameters defined in Annex B and provides data for online messages and clearing records.

Figure 2-2 and Figure 2-3 illustrate EMV Mode online and offline transaction flows.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

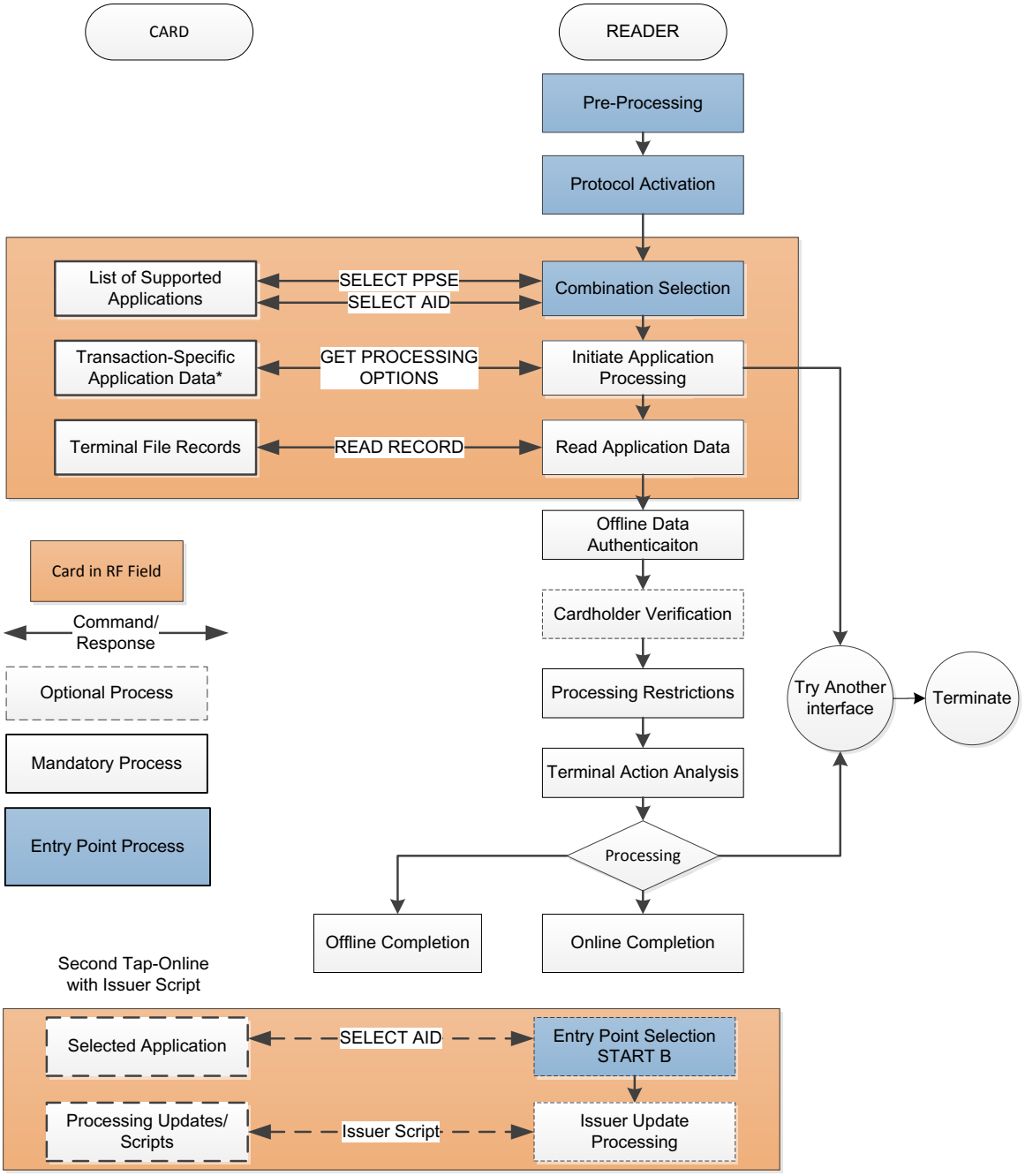
Figure 2-2: Kernel 6 Contactless Transaction Flow - Online EMV Mode



*Transaction-Specific Application Data are provided in Table 4-4.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 2-3: Kernel 6 Contactless Transaction Flow - Offline EMV Mode



*Transaction-Specific Application Data are provided in Table 4-3.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

2.3 Configuration, Functionality, and APDU Command Support

Section Summary:

2.3.1 POS System Configuration Options

The POS System Configuration options are used by the Kernel and must be set as described in [EMV Book A] and [EMV Book B]. In addition, the following configuration options are specific to Kernel 6.

1. **Acceptance Environment:** Reader will be enabled to support one of the following modes:
   - EMV Mode,
   - Mag-stripe Mode (MS Mode or Legacy MS Mode), or
   - Both EMV Mode and MS Mode.
2. **Kernel AID:** Discover AIDs will be configured to be used with Kernel 6.

2.3.2 Functionality

Specific Contactless functionalities are included in Table 2-1 and classified based on the following definitions:

- **Mandatory:** This functionality must be present and must conform to the behavior described in this Specification.
- **Conditional:** The presence of the functionality is dependent on another function.
- **Acquirer Option:** This functionality must be present in the Terminal application but the Acquirer may choose not to use the function.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Table 2-1: Contactless Functionality

Function	Kernel 6 Terminal Support	Notes
Entry Point Processing based on [EMV Book B]	Mandatory	The Terminal shall support Entry Point processing as defined in [EMV Book B]
Combination Selection Post Processing	Mandatory	See Section 3.1: Combination Selection Post Processing
Initiate Application Processing	Mandatory	If a data requested by the PDOL is not present in the Terminal, then the Terminal shall set the value to zeroes.
Cardholder Verification Method (CVM) • Online PIN • Signature • Consumer Device CVM • No CVM	Conditional	Mandatory for EMV Mode transactions except as determined by the payment system.
Read Application Data • EMV Data in Terminal File records, identified by Short File Identifier (SFI) and record number	Conditional	Mandatory for Offline capable EMV Mode readers and MS and Legacy MS Mode readers
Offline Data Authentication (ODA) • CDA	Conditional	Mandatory for Offline capable readers (must be performed before Termination Action Analysis)

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Function	Kernel 6 Terminal Support	Notes
Processing Restrictions • Application Expiration Date • Application Effective Date • Application Version Number • Application Usage Control* • Exception List	Mandatory	*Conditional - Mandatory for offline transactions
Terminal Action Analysis	Mandatory	
Online Processing	Conditional	Mandatory for Offline capable EMV Mode readers and MS & Legacy MS Mode readers
Completion • Offline • Online	Mandatory	
Issuer Update Processing • Application Block • Application Unblock • Put Data • Update Record	Mandatory	

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

2.3.3 APDU Command Support

The APDU commands included in Table 2-2 are designated as “Mandatory”, “Optional”, or “Not supported” by the Contactless Kernel 6 Terminal based on the following definitions:

- **Mandatory**: The command must be supported.
- **Not supported**: The command is not supported.

Table 2-2: APDU Command Support

Command	Kernel 6 Support
APPLICATION BLOCK	Mandatory[1]
APPLICATION UNBLOCK	Mandatory[1]
CARD BLOCK	Not supported
EXTERNAL AUTHENTICATE	Not Supported
GENERATE APPLICATION CRYPTOGRAM (AC)	Not Supported
GET CHALLENGE	Not Supported
GET DATA	Mandatory
GET PROCESSING OPTIONS	Mandatory
INTERNAL AUTHENTICATE	Not Supported
PIN CHANGE / UNBLOCK	Not Supported
PUT DATA	Mandatory[1]
READ RECORD	Mandatory
SELECT	Mandatory
UPDATE RECORD	Mandatory[1]

Notes: 1 = Terminal to only pass supported Issuer Script commands to card.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

3 Terminal Transaction Processing Steps

This section addresses the Kernel 6 transaction processing requirements, including process flows, in the following sections:

- 3.1: Combination Selection Post Processing
- 3.2: Initiate Application Processing
- 3.3: Read Application Data
- 3.4: Offline Data Authentication (ODA)
- 3.5: Cardholder Verification
- 3.6: Processing Restrictions
- 3.7: Terminal Action Analysis
- 3.8: Online Processing
- 3.9: Completion
- 3.10: Issuer Update Processing

Details on each APDU command referenced in this section are provided in Section 4, and additional information regarding Outcomes and Outcome Parameters are included in Annex B.

3.1 Combination Selection Post Processing

The transaction starts in the Kernel at the handover from Entry Point, which has performed:

- **EMV Mode**: Pre-Processing, Protocol Activation, Combination Selection, and Kernel Activation), or
- **Mag-stripe (MS Mode or Legacy MS Mode)**: Pre-Processing, Protocol Activation, Combination Selection, and Kernel Activation.

After Kernel Activation, the selected Kernel must check the response sent by the card to the SELECT command. The operations to be performed to validate the answer sent by the card are described in the following sections:

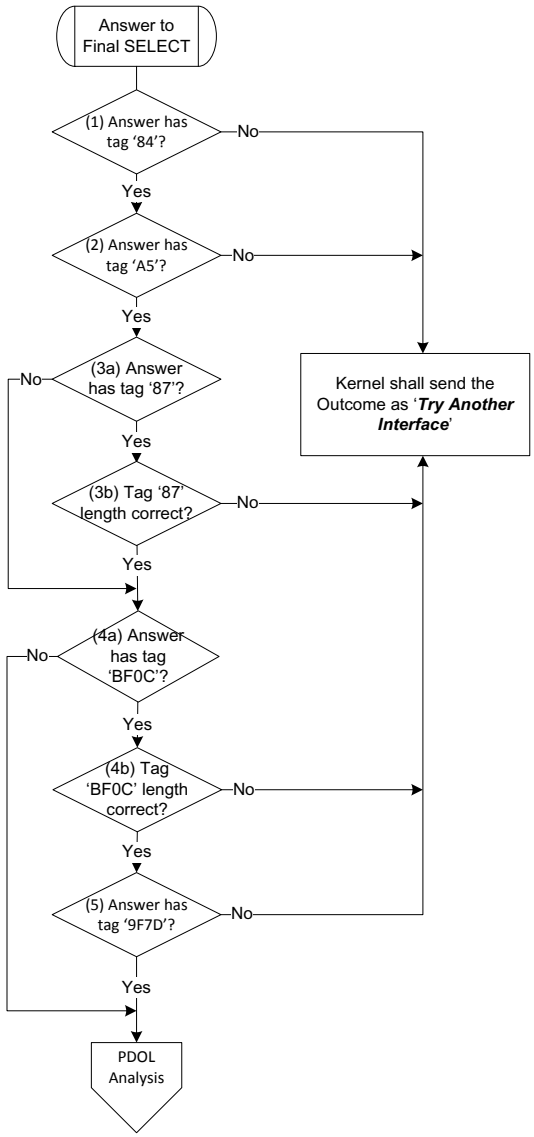
- 3.1.1: MS Mode and Legacy MS Mode:
  - Figure 3-1: Processing Flow (Format Analysis)
  - Figure 3-2: Processing Flow (PDOL Mandatory Check)

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

- 3.1.2: EMV Mode:
  - Figure 3-3: Processing Flow (Format Analysis)
  - Figure 3-4: Processing Flow (PDOL Mandatory Check)
  - Figure 3-5: Processing Flow (PDOL Optional Check)
  - Figure 3-6: Processing Flow (Optional Check)

3.1.1 MS Mode and Legacy MS Mode

Figure 3-1: MS and Legacy Modes Selection - Processing Flow (Format Analysis)

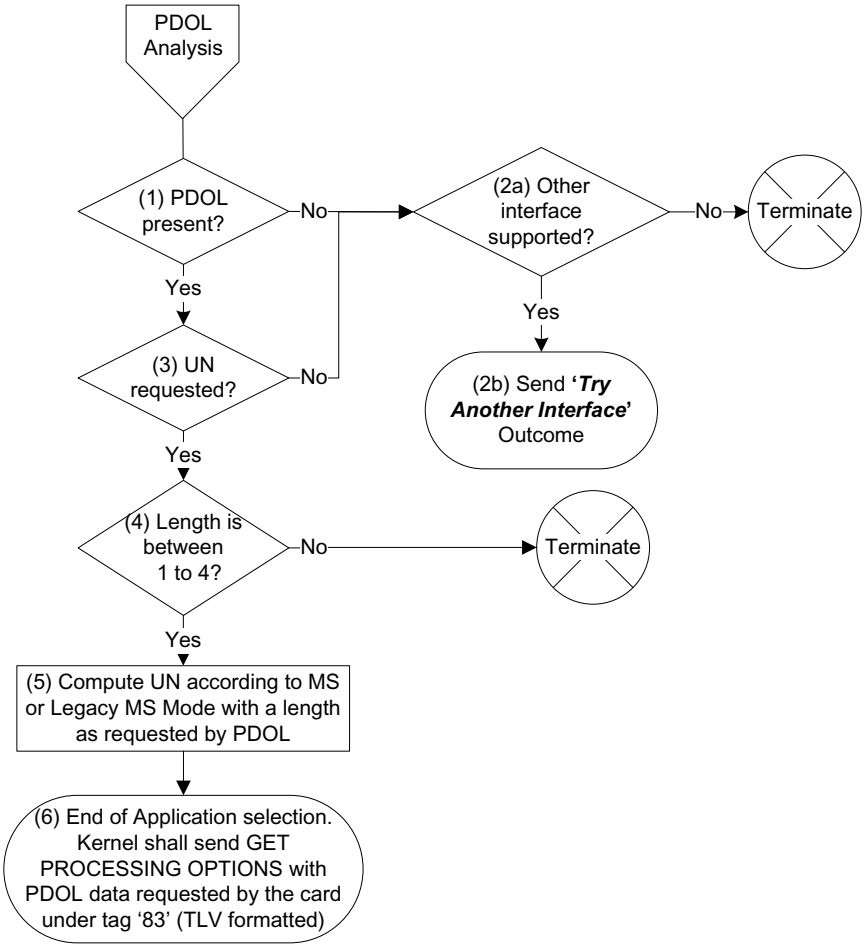


© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

#	Description
1	The Kernel shall check if Dedicated File (DF) name (tag '84') of the application is provided by the card. If the tag is not present, the Kernel shall send the Outcome as '***Try Another Interface***' to prompt the user to use another interface (if one is supported).
2	Kernel shall check if File Control Information (FCI) Proprietary Template (tag 'A5') is present. If the tag is not present, the Kernel shall send the Outcome as '***Try Another Interface***' to prompt the user to use another interface (if one is supported).
3a	Kernel shall check if Application Priority Indicator (tag '87') is present in the answer provided by the card and is under tag 'A5'. • If the Application Priority Indicator (tag '87') is present, go to step 3b. • ELSE go to step 4a. **Note:** If the tag is not under the tag 'A5', the Kernel shall end the transaction with '***End Application***' Outcome.
3b	Kernel shall check if the length of tag '87' is correct. • If the length is not correct, the Kernel shall send the Outcome as '***Try Another Interface***' to prompt the user to use another interface (if one is supported). • ELSE go to Step 4a.
4a	Kernel shall check if FCI Issuer Discretionary Data (tag 'BF0C') is present in the answer and is under the tag 'A5'. • If FCI Issuer Discretionary Data tag (tag 'BF0C') is not present, the process will skip to the PDOL Analysis, • ELSE go to Step 4b. **Note:** If the 'BF0C' tag is not under the tag 'A5', Kernel shall end the transaction with '***End Application***' Outcome.
4b	Tag BF0C shall be present if any of the subfields are present. The length of BF0C is checked based on the other fields present under it and it should be correctly TLV formatted. • If the format is not correct, the Kernel shall send the Outcome as '***Try Another Interface***' to prompt the user to use another interface (if one is supported). • ELSE go to step 5.
5	Kernel shall check if the "Discover® Network RF Contactless Payment Application Version Number" (tag '9F7D') is present in the answer and under tag 'BF0C'. • If tag '9F7D' is not present, the Kernel shall send the Outcome as '***Try Another Interface***' to prompt the user to use another interface (if one is supported). • ELSE perform PDOL Analysis.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-2: MS Modes Selection - Processing Flow (PDOL Mandatory Check)



#	Description
1	The Kernel shall check if PDOL is requested by the application. If… / Then… Yes / Go to step 3. No / Go to step 2a.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>2a</td><td>If PDOL is not present, the Kernel shall check if another interface is supported.

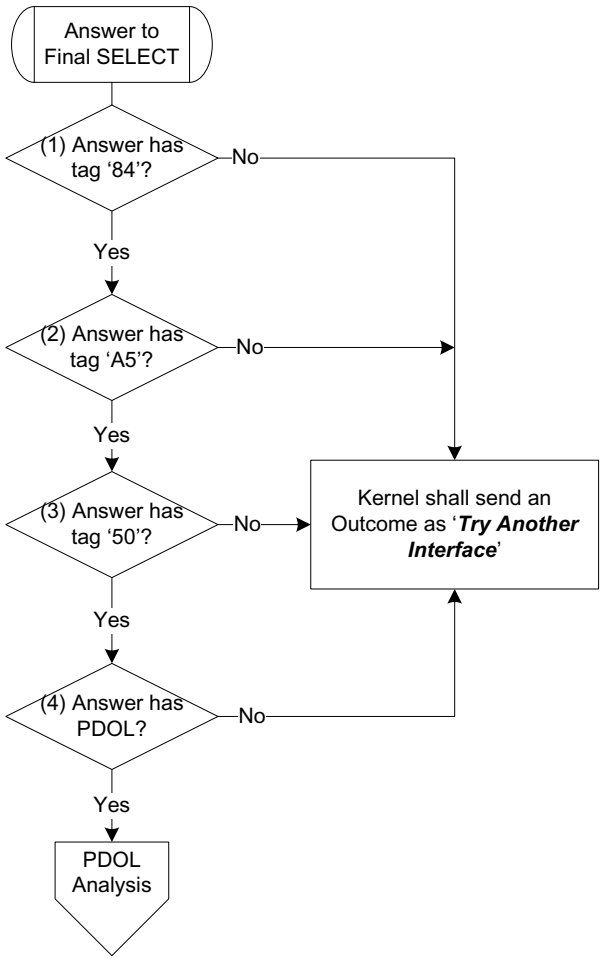
<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 2b.</td></tr><tr><td>No</td><td>Terminate the Transaction with ‘End Application’ (for Processing Error) Outcome.</td></tr></table></td></tr>
<tr><td>2b</td><td>If another interface is supported, the Kernel shall send the Outcome as ‘Try Another Interface’ to prompt the user to use another interface.</td></tr>
<tr><td>3</td><td>Kernel shall verify if an Unpredictable Number (UN) (tag ‘9F37’) is requested.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 4.</td></tr><tr><td>No</td><td>Go to step 2a.</td></tr></table></td></tr>
<tr><td>4</td><td>Kernel shall check if the length of UN requested by the application is between 1 to 4.
If the length has a different size, Kernel shall end the transaction with ‘End Application’ (for Processing Error) Outcome.
ELSE go to step 5.</td></tr>
<tr><td>5</td><td>Kernel shall compute a numeric UN for Legacy MS or MS Mode and pass it within the length requested by the PDOL.</td></tr>
<tr><td>6</td><td>Kernel shall end the selection process and shall send the GET PROCESSING OPTIONS with the PDOL data requested by the card under tag 83 (TLV formatted).</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

3.1.2 EMV Mode (Figures 3-3 to 3-7)

Figure 3-3: EMV Mode Selection - Processing Flow (Format Analysis)



#	Description
1	The Kernel shall begin the checks on the response received for the final SELECT command. The Kernel shall check if DF name (tag '84') of the application is provided by the card. If the tag is not present, the Kernel shall send the Outcome as '***Try Another Interface***' to request the use of another interface (if one is supported).
2	Kernel shall check if FCI Proprietary Template (tag 'A5') is present. If the tag is not present, the Kernel shall send the outcome as '***Try Another Interface***' to request the use of another interface (if one is supported).
3	Kernel shall check if Application Label (tag '50') is present in the answer provided by the card and is under tag 'A5'. If the tag is not present as specified, the Kernel shall send the Outcome as '***Try Another Interface***' to request the use of another interface (if one is supported).

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

#	Description
4	Kernel shall check if Processing Options Data Object List (PDOL) (tag '9F38') is present in the answer provided by the card and is under tag 'A5'. • If tag '9F38' is not present as specified, the Kernel shall send the Outcome as '***Try Another Interface***' to request the use of another interface (if one is supported) to the Entry Point. • If tag '9F38' is present as specified, the Kernel shall perform a PDOL analysis.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

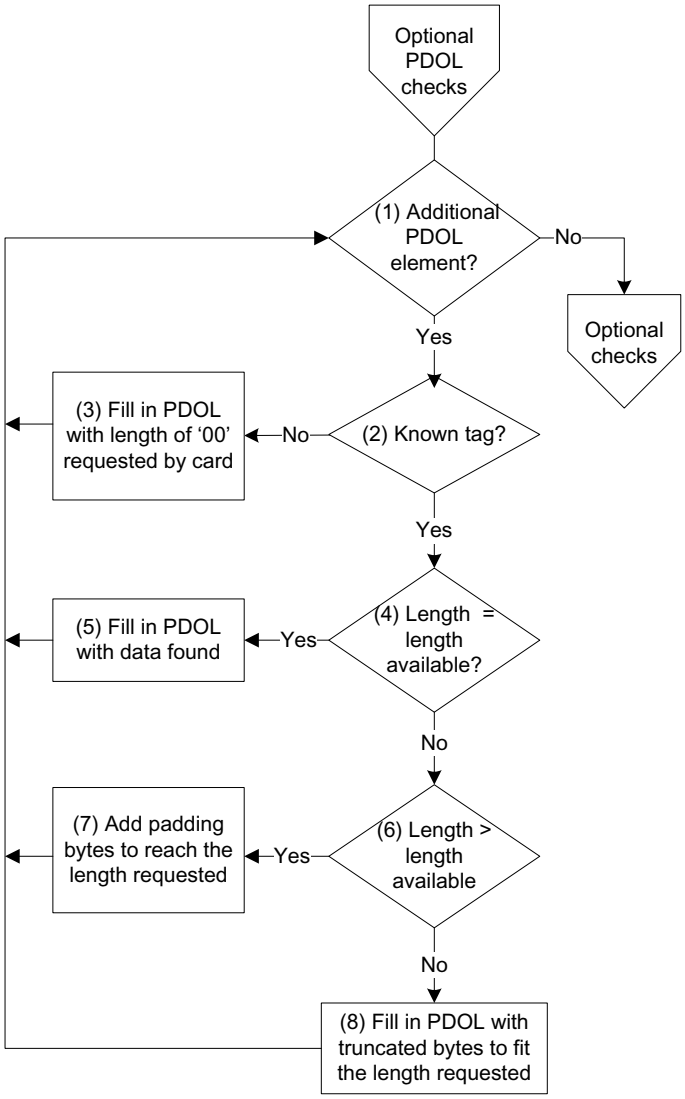
Figure 3-4: EMV Mode Selection - Processing Flow (PDOL Mandatory Check)

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

#	Description
1	Kernel shall check if the card requests a TTQ (tag '9F66') with a length of 4 bytes. If the TTQ is not requested or the TTQ length is different from 4, then the Kernel shall go to step 9.
2	Kernel shall check if the card requests Amount Authorized (tag '9F02') with a length of 6 bytes. If Amount Authorized is not requested or the Amount Authorized length is not equal to 6, then the Kernel shall go to step 9.
3	Kernel shall check if the card requests Amount Other (tag '9F03') with a length of 6 bytes. If Amount Others is not requested or the Amount Others length is not equal to 6, then the Kernel shall go to step 9.
4	Kernel shall check if the card requests Terminal Country Code (tag '9F1A') with a length of 2 bytes. If Terminal Country Code is not requested or the Terminal Country Code length is not equal to 2, then the Kernel shall go to step 9.
5	Kernel shall check if the card requests Transaction Currency Code (tag '5F2A') with a length of 2 bytes. If the transaction Currency Code is not requested or the Transaction Currency Code length is not equal to 2, then the Kernel shall go to step 9.
6	Kernel shall check if the card requests Transaction Date (tag '9A') with a length of 3 bytes. If the Transaction Date is not requested or the Transaction Date length is not equal to 3, then the Kernel shall go to step 9.
7	Kernel shall check if the card requests Transaction Type (tag '9C') with a length of 1 byte. If the Transaction Type is not requested or the Transaction Type length is not equal to 1, then the Kernel shall go to step 9.
8	a. Kernel shall check if the card requests Unpredictable Number (UN) (tag '9F37'). If not present, the Kernel shall go to step 9. b. Kernel shall check if MS Mode (TTQ B1b8 = 1) is enabled and tag 9F7D is present in card response. If yes, the Transaction will process in MS Mode (go to 8c) else it continues in EMV Mode. (Go to 8d) c. Kernel will check for UN length of '01' byte or '04'bytes. If yes, the Transaction will perform optional PDOL checks. If no, go to step 9. d. Kernel will check for UN length of '04' bytes. If yes, the Transaction will perform optional PDOL checks. If no, go to step 9. Note: If the UN is not requested or the UN length is not correct, then the Kernel shall go to step 9.
9	The Kernel shall send the Outcome as '***Select Next'***.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-5: EMV Mode Selection - Processing Flow (PDOL Optional Check)



#	Description
1	Kernel shall check if the PDOL requested by the card contains additional data to be sent with the GET PROCESSING OPTION. If… / Then… Yes / Go to step 2. No / Go to Figure 3-6 to perform optional checks.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>2</td><td>Kernel verifies if the data element requested by the card is a Discover D-PAS tag or EMV tag.

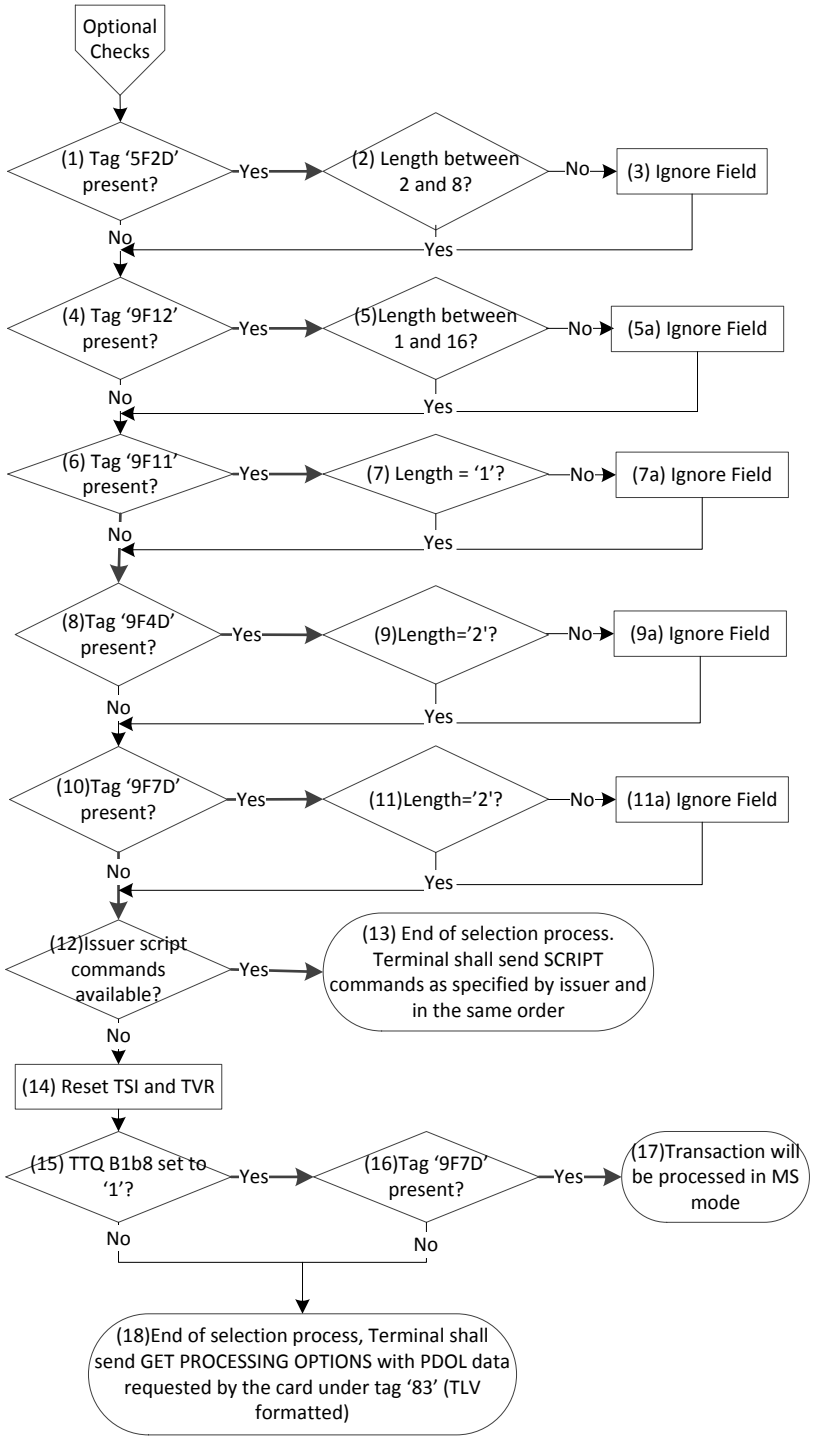
<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 4.</td></tr><tr><td>No</td><td>Go to step 3.</td></tr></table></td></tr>
<tr><td>3</td><td>If the requested data is unknown by the Kernel, the Kernel shall add the number of ‘00’ bytes requested by the card to data that will be sent to the card.
Then, go to step 1.</td></tr>
<tr><td>4</td><td>Kernel shall check If the length requested by the card concerning the known element is equal to the length available in the Kernel.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 5.</td></tr><tr><td>No</td><td>Go to step 6.</td></tr></table></td></tr>
<tr><td>5</td><td>Kernel inserts requested data into the PDOL that will be sent to the card.
Then, go to step 1.</td></tr>
<tr><td>6</td><td>Kernel checks if the length requested by the PDOL entry is greater than the length of available data inside the Kernel.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 7.</td></tr><tr><td>No</td><td>Go to step 8.</td></tr></table></td></tr>
<tr><td>7</td><td>Kernel shall add padding bytes (as per [EMV Book 3] Section 5.4 padding rules) to reach the size requested by the card and add the result to the PDOL that will be sent to the card.
Then, go to step 1.</td></tr>
<tr><td>8</td><td>If the length of data requested by the card in the PDOL entry is lower than the length of available data inside the Kernel, the Kernel shall include truncated bytes to match the requested length (as per [EMV Book 3] Section 5.4).
Then, go to step 1.</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-6: EMV Mode Selection - Processing Flow (Optional Check)



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall check if the card has returned Language Preference (tag ‘5F2D’). If data is not present, the Kernel shall continue the optional checks.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 2.</td></tr><tr><td>No</td><td>Go to step 4.</td></tr></table></td></tr>
<tr><td>2</td><td>Kernel verifies if Language Preference (tag ‘5F2D’) length is coded between 2 and 8 bytes and is a multiple of 2.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 4.</td></tr><tr><td>No</td><td>Go to step 3.</td></tr></table></td></tr>
<tr><td>3</td><td>If the length returned by the card is not the expected one, the Kernel shall ignore the field and continue the optional checks.</td></tr>
<tr><td>4</td><td>Kernel shall check if Application Preferred Name (tag ‘9F12’) is sent by the card. If data is not present, the Kernel shall continue the optional checks (Step 6).</td></tr>
<tr><td>5</td><td>Kernel verifies if the Application Preferred Name (tag ‘9F12’) length is between 1 and 16 bytes.
If the length returned by the card is not the expected one, the Kernel shall ignore the field (Step 5a) and continue the optional checks (Step 6).</td></tr>
<tr><td>6</td><td>Kernel shall check if Issuer Code Table Index (tag ‘9F11’) is sent by the card. If data is not present, the Kernel shall continue the optional checks (Step 8).</td></tr>
<tr><td>7</td><td>Kernel verifies if Issuer Code Table Index (tag ‘9F11’) length is 1 byte.
If the length returned by the card is not the expected one, the Kernel shall ignore the field (Step 7a) and continue the optional checks (Step 8).</td></tr>
<tr><td>8</td><td>Kernel shall check if Log Entry (tag ‘9F4D’) is sent by the card. If data is not present, the Kernel shall continue the optional checks (Step 10).</td></tr>
<tr><td>9</td><td>Kernel verifies if Log Entry (tag ‘9F4D’) length is 2 bytes.
If the length returned by the card is not the expected one, the Kernel shall ignore the field (Step 9a) and continue the optional checks (Step 10).</td></tr>
<tr><td>10</td><td>Kernel shall verify if the Contactless Payment Application Version Number (tag ‘9F7D’) is present. If data is not present, the Kernel shall continue the optional checks (Step 12).</td></tr>
<tr><td>11</td><td>Kernel verifies if the Contactless Payment Application Version Number (tag ‘9F7D’) length is 2 bytes.
If the length returned by the card is not the expected one, the Kernel shall ignore the field (Step 11a) and continue the optional checks (Step 12).</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>12</td><td>Kernel shall verify if it receives Issuer script commands sent by Issuer.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 13.</td></tr><tr><td>No</td><td>Go to step 14.</td></tr></table></td></tr>
<tr><td>13</td><td>Kernel shall end the selection process and shall send script commands received from Issuer in the same order as received from Issuer.</td></tr>
<tr><td>14</td><td>New transaction is being processed. All information concerning the previous transaction (TVR and TSI) shall be reset.</td></tr>
<tr><td>15</td><td>Kernel shall check if it supports MS Mode (TTQ B1b8 =1).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 16.</td></tr><tr><td>No</td><td>Go to step 18.</td></tr></table></td></tr>
<tr><td>16</td><td>Kernel that supports MS Mode shall check if the card wishes to process the transaction in Legacy or MS Mode by verifying if tag ‘9F7D’ is present in the File Control Information (FCI).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 17.</td></tr><tr><td>No</td><td>Go to step 18.</td></tr></table></td></tr>
<tr><td>17</td><td>The transaction will be performed via MS Mode using a GPO command configured for MS or Legacy MS Mode processing.</td></tr>
<tr><td>18</td><td>The transaction will be performed via a GPO command configured for EMV Mode processing.</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

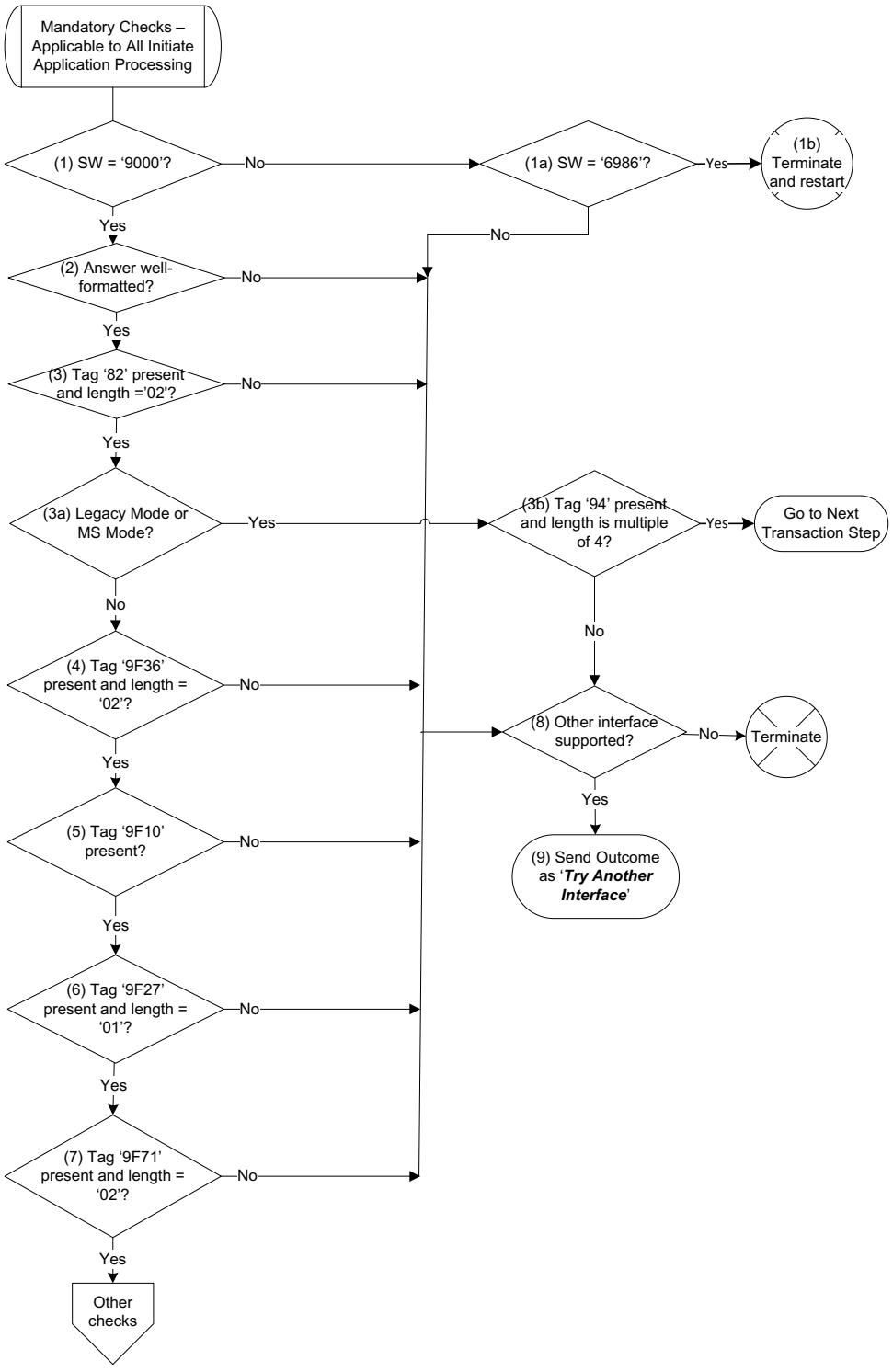
3.2 Initiate Application Processing

At the Initiate Application Processing stage, the Kernel indicates to the card that a new transaction is beginning by sending the GET PROCESSING OPTIONS command as described in this section.

As part of this step, the Kernel will only check if the answer to the command is well formatted and will analyze data later during the Terminal Action Analysis step. Different checks must be performed depending on the type of transaction being processed. The diagrams included in this section show the checks performed by the Kernel when it receives the response to the GET PROCESSING OPTIONS command.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-7: Initiate Application Processing (Mandatory Data Checks: All Transactions)



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall verify that the command has been successfully processed by the card (by confirming that the Status Word is set to ’9000’).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 2.</td></tr><tr><td>No</td><td>Go to step 8.</td></tr></table></td></tr>
<tr><td>1a</td><td>Kernel shall check if the card application returns status words SW ‘6986’.
• If status word is not equal to ‘6986’, the Terminal shall go to step 10.
• ELSE go to step 1b.

Note that the SW ‘6986’ response only applies to Mobile transactions and occurs when a passcode is not entered and verified.</td></tr>
<tr><td>1b</td><td>Kernel shall send the outcome “Try Again” to allow the entry of a Confirmation Code of the Mobile device.</td></tr>
<tr><td>2</td><td>Kernel shall check if the answer returned by the card is formatted according to [EMV Book 3]. If no, go to step 8.</td></tr>
<tr><td>3</td><td>Kernel shall check if Tag 82 is present.

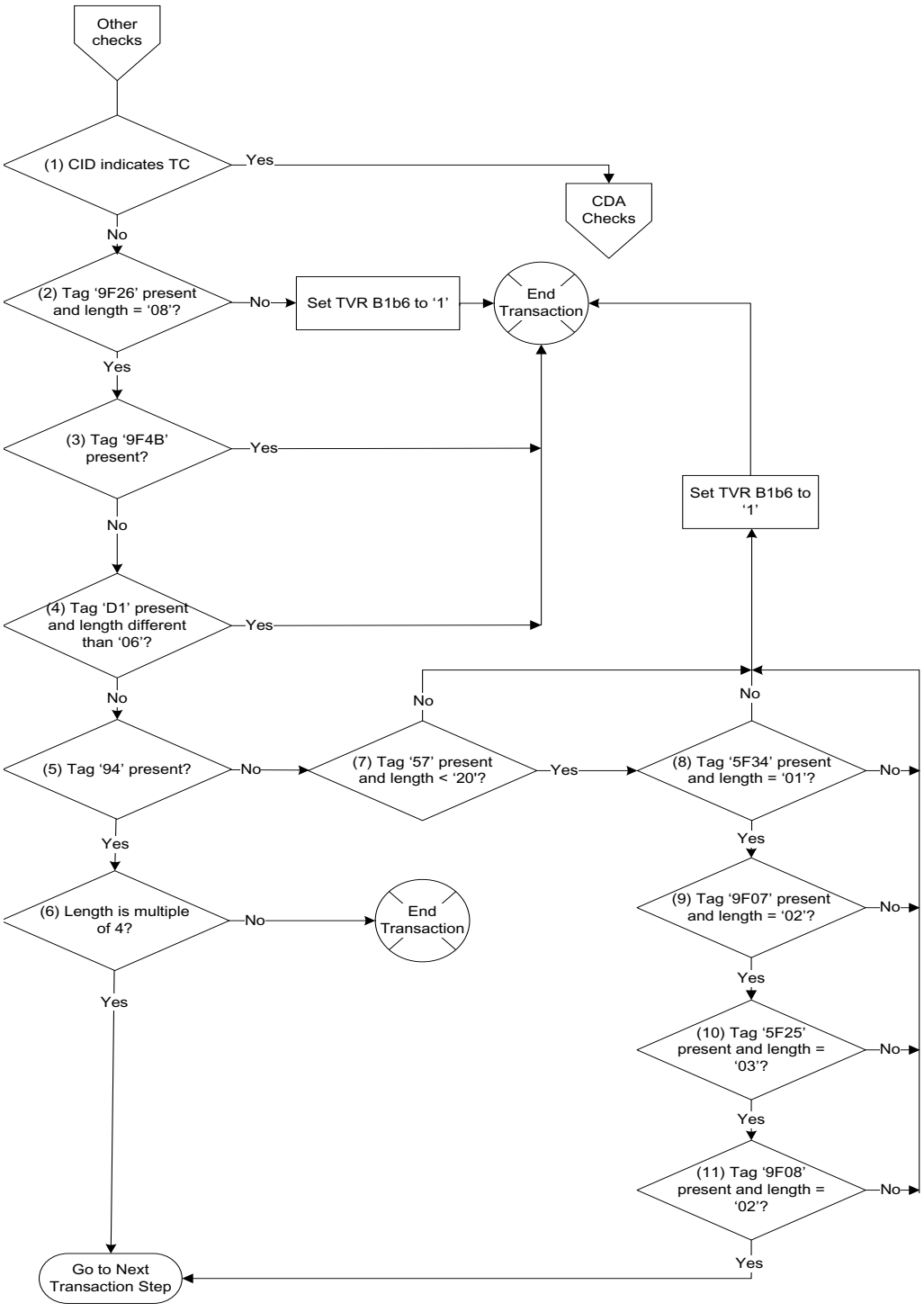
<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 3a.</td></tr><tr><td>No</td><td>Go to step 8.</td></tr></table></td></tr>
<tr><td>3a</td><td>Kernel shall check if the transaction being performed is with Legacy Mode or MS Mode.
• If Yes, go to step 3b.
• If No, go to step 4.</td></tr>
<tr><td>3b</td><td>Kernel shall check if “Application File Locator” (AFL) (tag ‘94’) is present in the answer from the card and the associated length is a multiple of 4.
• If Yes, proceed to next transaction step command.
• If no, go to step 8.</td></tr>
<tr><td>4</td><td>Kernel shall check if the ATC (tag ‘9F36’) is present and coded on two bytes. If no, go to step 8.</td></tr>
<tr><td>5</td><td>Kernel shall check if application has returned Issuer Application Data (tag ‘9F10’) to GET PROCESSING OPTIONS. If no, go to step 8.</td></tr>
<tr><td>6</td><td>Kernel shall verify that Cryptogram Information Data (CID) (tag ‘9F27’) is present as the answer to GET PROCESSING OPTIONS command and is coded on one byte. If no, go to step 8.</td></tr>
<tr><td>7</td><td>Kernel shall check that the application returns Card Processing</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

#	Description
	Requirement (CPR) (tag '9F71') coded on two bytes. If no, go to step 8.
8	Kernel shall check if it supports another interface. • If Terminal does not support another interface, the Terminal shall terminate the transaction with '***End* Application**' (for Processing Error) Outcome. • ELSE go to step 9.
9	If another interface is supported by the Terminal, the Kernel shall provide the Outcome '***Try Another Interface***' to Entry Point.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-8: Initiate Application Processing (Checks for Online and Decline Decision - No CDA)



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall check if the card has returned Cryptogram Information Data (CID) indicating that it is TC.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Complete CDA checks.</td></tr><tr><td>No</td><td>Go to step 2.</td></tr></table></td></tr>
<tr><td>2</td><td>Kernel shall verify that an AC (tag ‘9F26’) is provided by the card and is coded on 8 bytes. If the AC is not present or is not 8 bytes long, the Kernel shall set TVR B1b6 to ‘1’ (ICC Data missing) and end the transaction with ‘End Application’ (for Processing Error) Outcome to Entry Point.</td></tr>
<tr><td>3</td><td>Kernel shall check if Signed Dynamic Application Data (SDAD) (tag ‘9F4B’) is returned by the application. If SDAD is present in the answer, the Kernel shall end the transaction with ‘End Application’ (for Processing Error) Outcome to Entry Point.</td></tr>
<tr><td>4</td><td>Kernel shall verify that Offline Balance (tag ‘D1’) is present in the answer from the card and has a length that is different than 6 bytes. If Offline balance is present and has a length different than ‘06’, the Kernel shall return the transaction with ‘End Application’ (for Processing Error) Outcome to Entry Point.</td></tr>
<tr><td>5</td><td>Kernel shall check if Application File Locator (AFL) (tag ‘94’) is returned by the card.

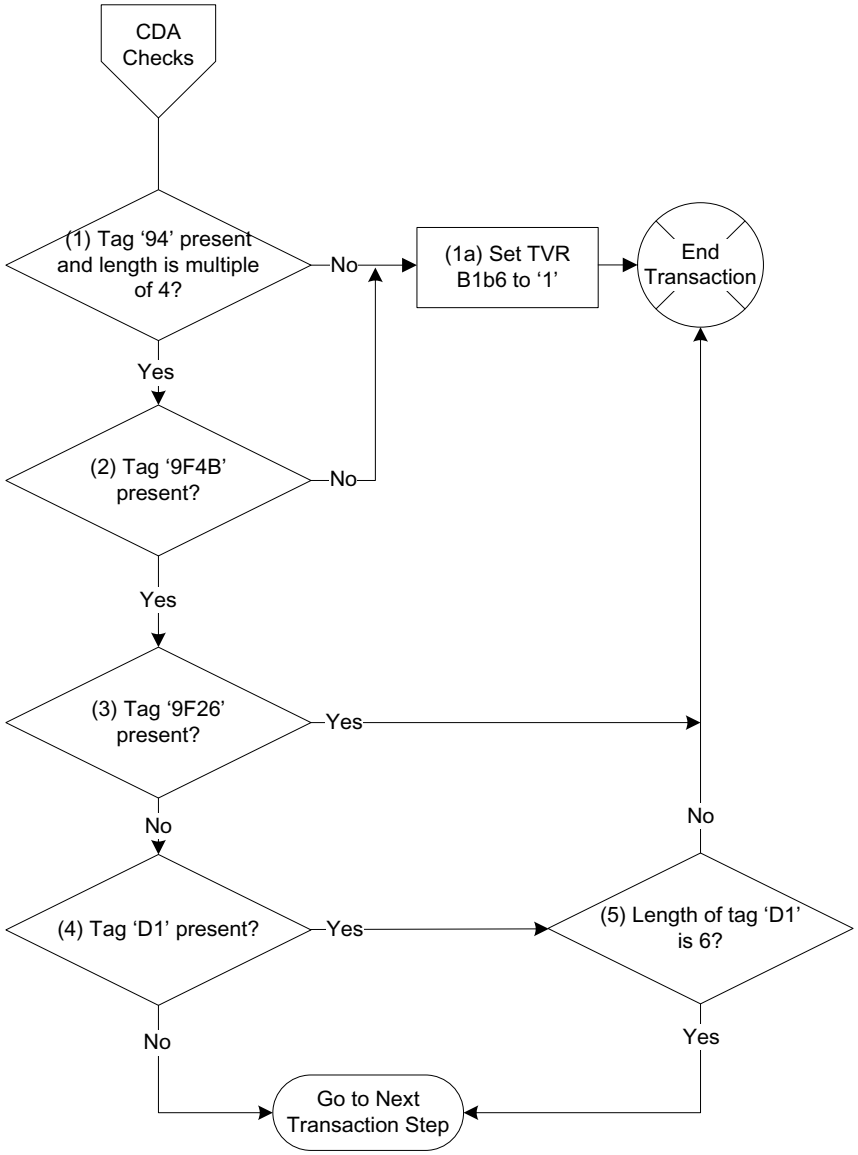
<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 6.</td></tr><tr><td>No</td><td>Go to step 7.</td></tr></table></td></tr>
<tr><td>6</td><td>Kernel shall check if the AFL is coded on a multiple of 4 bytes.
If AFL does not have a length that is a multiple of 4 bytes, the Kernel shall end the transaction with ‘End Application’ (for Processing Error) Outcome.
ELSE go to the next transaction process step.</td></tr>
<tr><td>7</td><td>If AFL (tag ‘94’) is not present in the answer of the GET PROCESSING OPTIONS command, the Kernel shall verify that the answer from the card contains Track 2 Equivalent Data (tag ‘57’) at a length of less than 20 bytes.
If neither Track 2 Equivalent Data (at a length less than 20 bytes) nor the AFL is present in the answer, the Terminal shall set TVR B1b6 to ‘1’ (ICC Data missing) and end the transaction.
ELSE go to step 8.</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

#	Description
8	Kernel shall verify that the answer from the card contains PAN Sequence Number (tag '5F34') at a length equal to '01'. • If no, set TVR B1b6 to '1' (ICC data missing) and end the transaction with '***End Application***' (for Processing Error) Outcome. • ELSE go to step 9.
9	Kernel shall verify that the answer from the card contains Application Usage Control (tag '9F07') at a length equal to '02'. • If no, set TVR B1b6 to '1' (ICC data missing) and end the transaction with '***End Application***' (for Processing Error) Outcome. • ELSE go to step 10.
10	Kernel shall verify that the answer from the card contains Application Effective Date (tag '5F25') at a length equal to '03'. • If no, set TVR B1b6 to '1' (ICC data missing) and end the transaction with '***End Application***' (for Processing Error) Outcome. • ELSE go to step 11.
11	Kernel shall ensure that the answer from the card contains Application Version Number (tag '9F08') at a length equal to '02'. • If no, set TVR B1b6 to '1' (ICC data missing) and end the transaction with '***End Application***' (for Processing Error) Outcome. • ELSE go to the next transaction process step.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-9: Initiate Application Processing (Checks for CDA)



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall check if Application File Locator (AFL) (tag ‘94’) is present in the answer from the card and the associated length is a multiple of 4 bytes.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 2.</td></tr><tr><td>No</td><td>Go to step 1a.</td></tr></table></td></tr>
<tr><td>1a</td><td>If AFL is not present or its length is not multiple of 4, the Kernel shall set TVR B1b6 to ‘1’ (ICC data missing) and end the transaction with ‘End Application’ (for Processing Error) Outcome.</td></tr>
<tr><td>2</td><td>Kernel shall verify that Signed Dynamic Application Data (SDAD) (tag ‘9F4B’) is present.
If data is not present, the Kernel shall set TVR B1b6 to ‘1’ (ICC data missing) and end the transaction.
Note: The verification of the SDAD (length, decipherment, data control) occurs later in the transaction (during ODA).</td></tr>
<tr><td>3</td><td>Kernel shall check if Application Cryptogram (AC) (tag ‘9F26’) is returned in the answer to GET PROCESSING OPTIONS.
• If data is present, the Kernel shall end the transaction.
• ELSE go to step 4.</td></tr>
<tr><td>4</td><td>Kernel shall verify if Offline Balance (tag ‘D1’) is present in the answer to GET PROCESSING OPTIONS command.
• If data is not present, the Kernel shall end Initiate Application processing and start to perform the next transaction process step.
• ELSE go to step 5.</td></tr>
<tr><td>5</td><td>Kernel shall check If the length of Offline Balance has a length of 6 bytes.
• If the length is not 6, the Kernel shall end the transaction with ‘End Application’ (for Processing Error) Outcome.
• ELSE the Kernel shall end Initiate Application processing and start to perform the next transaction process step.</td></tr>
</table>

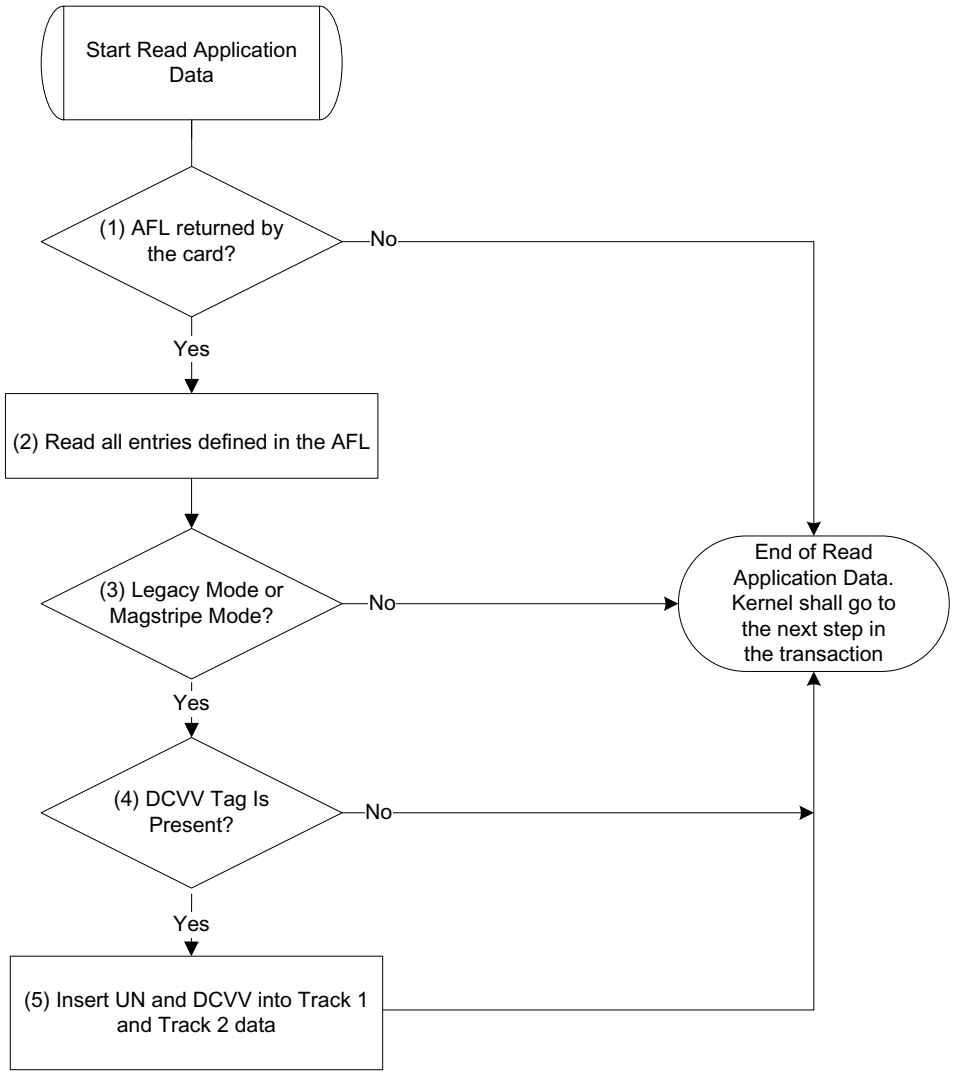
© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

3.3 Read Application Data

The terminal shall perform Read Application Data if the card returns an AFL to the GET PROCESSING OPTIONS command and data is well-formatted (i.e., the length related to AFL shall be a multiple of 4 bytes). The aim is to read all records as referenced in the AFL file identified as the Short File Indicator (SFI).

The Read Application Data process is illustrated in Figure 3-10.

Figure 3-10: Read Application Data Process



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Terminal shall check if an AFL has been returned in response to the GPO command. (This can be completed by setting an internal flag when verifying the GET PROCESSING OPTIONS command or by another mechanism.)

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 2.</td></tr><tr><td>No</td><td>End Read Application. Go to the next transaction step.</td></tr></table></td></tr>
<tr><td>2</td><td>Terminal shall read all entries included in the AFL. Data read shall be stored in transient memory.</td></tr>
<tr><td>3</td><td>Check if the transaction is being performed via Legacy MS Mode or MS Mode.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 4.</td></tr><tr><td>No</td><td>End Read Application. Go to the next transaction step.</td></tr></table></td></tr>
<tr><td>4</td><td>Check if the Dynamic Card Verification Value (DCVV) tag ‘‘9F7E’ is present. [Note: The tag applies to Legacy MS Mode or MS Mode.]

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 5.</td></tr><tr><td>No</td><td>End Read Application. Go to the next transaction step.</td></tr></table></td></tr>
<tr><td>5</td><td>Insert the Unpredictable Number (UN) and DCVV in the correct locations of Track 1 and Track 2 as described in Annex E.
End Read Application. Go to the next transaction step.</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

3.4 Offline Data Authentication (ODA) for Offline Transactions

Offline Data Authentication (ODA) is performed by the Kernel after the Read Application Data step is completed, *only if the transaction is processed offline and the application has returned a SDAD in response to the GET PROCESSING OPTIONS command*. The kernel executes the ODA process to authenticate the Contactless Card (i.e., to verify that the card being used is genuine).

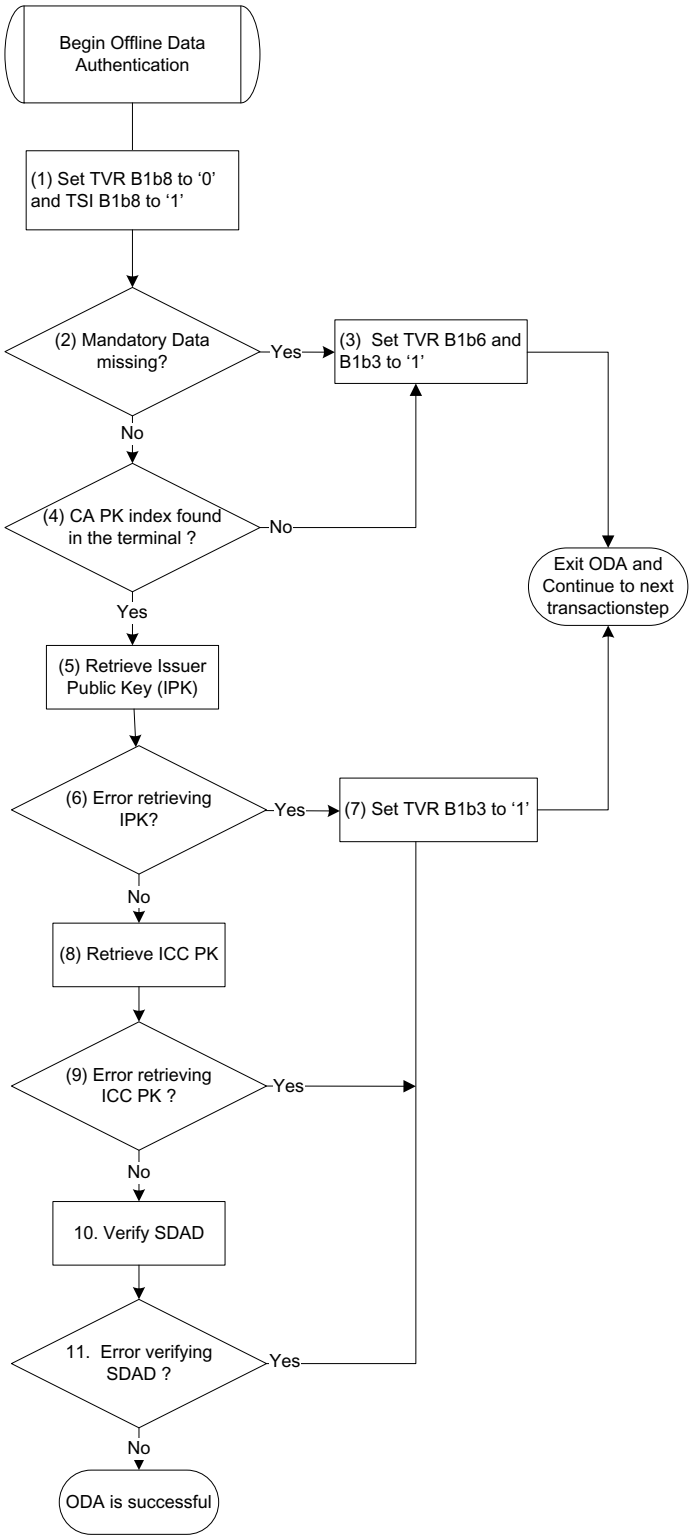
Detailed information regarding the ODA process is provided in [EMV Book 2]. During the execution of the process, the Kernel shall:

- Retrieve the CA Public Key - associated with the CA Public Key Index (tag '8F).
- Retrieve the Issuer Public Key - based on data read during the Read Application Data step.
- Retrieve the ICC Public Key - based on data read during Read Application Data step.
- Verify Signed Dynamic Application Data (SDAD tag '9F4B') - in the GPO data returned by the card to the Kernel.

Upon completion of the process, the Kernel shall set TVR B1b8 to '0' (Offline data authentication was performed). If ODA fails, then the Kernel will set TVR B1b3 to '1'(CDA failed).

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-11: Offline Data Authentication (Global Overview)



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall set TVR B1b8 to ‘0’ (Offline data authentication was performed) and TSI B1b8 to ‘1’ (Offline data authentication was performed).</td></tr>
<tr><td>2</td><td><table><tr><td>If the mandatory values are...</td><td>Then…</td></tr><tr><td>Missing</td><td>Go to step 3.</td></tr><tr><td>Present</td><td>Go to step 4.</td></tr></table></td></tr>
<tr><td>3</td><td>Kernel shall set TVR B1b6 to ‘1’ (ICC Data missing) and B1b3 to ‘1’ (CDA failed).
Exit ODA and continue to the next transaction step.</td></tr>
<tr><td>4</td><td>Kernel shall verify that the Certificate Authority Public Key Index (CA PKI) is present in the terminal.<table><tr><td>If CA PKI is...</td><td>Then…</td></tr><tr><td>Missing</td><td>Go to step 3.</td></tr><tr><td>Present</td><td>Go to step 5.</td></tr></table></td></tr>
<tr><td>5</td><td>The Kernel shall attempt to retrieve the Issuer Public Key (IPK) from the card.</td></tr>
<tr><td>6</td><td><table><tr><td>If the IPK is...</td><td>Then…</td></tr><tr><td>Not retrievable</td><td>Go to step 7.</td></tr><tr><td>Retrievable</td><td>Go to step 8.</td></tr></table></td></tr>
<tr><td>7</td><td>Kernel shall set TVR B1b3 to ‘1’ (‘CDA failed’).
Exit ODA and continue to the next transaction step.</td></tr>
<tr><td>8</td><td>The Kernel shall attempt to retrieve the ICC PK from the card.</td></tr>
<tr><td>9</td><td><table><tr><td>If the ICC PK is...</td><td>Then…</td></tr><tr><td>Not retrievable</td><td>Go to step 7.</td></tr><tr><td>Retrievable</td><td>Go to step 10.</td></tr></table></td></tr>
<tr><td>10</td><td>Kernel shall verify the signed SDAD as described in the Section 3.4.1.</td></tr>
<tr><td>11</td><td><table><tr><td>If the SDAD is...</td><td>Then…</td></tr><tr><td>Not verified</td><td>Go to step 7.</td></tr><tr><td>Verified</td><td>ODA successful. Go to the next transaction step.</td></tr></table></td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

3.4.1 Signed Dynamic Application Data

Verifying Signed Dynamic Application Data shall only be performed if the Certificate Authority Public Key, Issuer Public Key and ICC Public Key are retrieved successfully. The aim is to authenticate the card.

To complete this authentication, the Kernel shall perform following checks:

- Verify the SDAD size: the SDAD shall have the same length as the ICC Public Key Modulus (if not, CDA is considered as failing).
- Apply the RSA algorithm on SDAD data using the ICC Public Key. Deciphered data shall be formatted as specified in [EMV Book 2].
- Check the following elements on deciphered data:
  - Recovered Data Header set to '6A'.
  - Recovered Data Trailer set 'BC'.
  - Signed Data Format set to '05'.

- Verify that ICC Dynamic Data are present and formatted as follows:
  - ICC Dynamic Data shall be present in deciphered data starting at byte 5, and the length of ICC Dynamic Data is given by byte 4 of deciphered data with:
    - ICC Dynamic Number Length = 1 B
    - ICC Dynamic Number = 2-8 b
    - Cryptogram Information Data (CID) = 1 B
    - Transaction Certificate or ARQC = 8 B
    - Transaction Data Hash Code = 20
  - Verify that the CID found in deciphered data is the same as the one returned in GET PROCESSING OPTIONS under tag '9F27'
  - Create the Hash Result: Kernel shall compute the hash applying the Hash Indicator Algorithm to the following data in the order presented: from the Hash Algorithm Indicator to the pad pattern followed by the Unpredictable Number sent by the Kernel.
  - Perform a comparison between the Hash Result recovered from deciphered data and Hash Result previously computed. If they do not match, the Kernel shall consider that CDA verification is failing, update the TVR, and skip the remainder of the CDA process.
  - Create Transaction Data Hash Code: Kernel shall concatenate the following elements: PDOL values (sent by the Kernel) and TLV data returned by the card to GPO command in the order they are returned, with the exception of the Signed Dynamic Application Data.
  - Perform a comparison between the Transaction Data Hash Code computed by the Kernel and Transaction Data Hash Code recovered from deciphered data. If they do not match, the Kernel shall consider that CDA verification is failing, update the TVR, and shall skip the remainder of the CDA process.

If no issues have been found, CDA verification was successful, and the Kernel will update the TVR accordingly.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

3.5 Cardholder Verification

The Kernel may perform Cardholder verification based on the reader configuration and card request. The CVMs supported by the Kernel are:

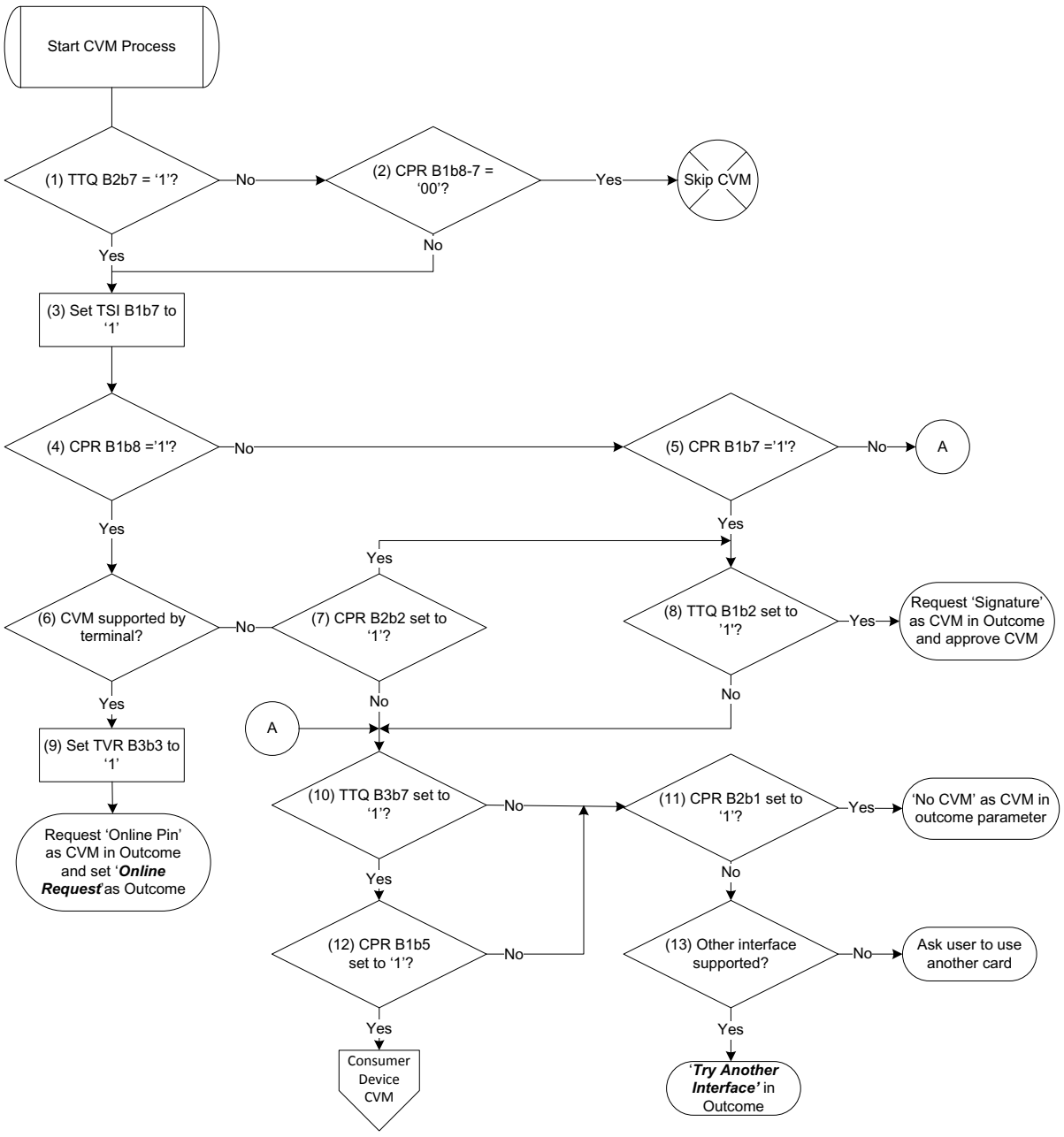
- Online PIN,
- Signature,
- No CVM, and
- For mobile only: Consumer Device CVM (CD CVM) - a CVM performed on, and validated by, the consumer's payment device, independent of the reader.

The following flow diagrams describe the CVM processing steps for:

- Online PIN, Signature, and No CVM in Figure 3-12: Cardholder Verification Method Process (Online PIN, Signature, and No CVM), and
- CD CVM: Figure 3-13.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-12: Cardholder Verification Method Process (Online PIN, Signature, and No CVM)



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall check if the Terminal has requested the Kernel to process a CVM (TTQ B2b7 = 1 CVM Required).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 3.</td></tr><tr><td>No</td><td>Go to step 2.</td></tr></table></td></tr>
<tr><td>2</td><td>Kernel shall verify if the card has not requested the Terminal to process an Online or Signature CVM (CPR B1b8-7 = ‘00’ – bit 8 Online PIN required, bit 7 Signature required).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>The Kernel shall end the CVM process, and go to the next transaction step.</td></tr><tr><td>No</td><td>Go to step 3.</td></tr></table></td></tr>
<tr><td>3</td><td>CVM will be performed. The Kernel shall update the TSI (B1b7 = 1 Cardholder verification was performed).</td></tr>
<tr><td>4</td><td>Kernel shall check if the card requests an Online PIN verification (CPR B1b8 = 1 Online PIN required).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 6.</td></tr><tr><td>No</td><td>Go to step 5.</td></tr></table></td></tr>
<tr><td>5</td><td>Kernel shall verify if the card has requested a signature (CPR B1b7 = 1 Signature required).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 8.</td></tr><tr><td>No</td><td>Go to step 10.</td></tr></table></td></tr>
<tr><td>6</td><td>Kernel shall verify that it supports Online PIN (TTQ B1b3 =1 Online PIN supported).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 9.</td></tr><tr><td>No</td><td>Go to step 7.</td></tr></table></td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>7</td><td>Kernel shall verify if the card supports fallback to signature (CPR B2b2 = 1 CVM Fallback to Signature allowed).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 8.</td></tr><tr><td>No</td><td>Go to step 10</td></tr></table></td></tr>
<tr><td>8</td><td>Kernel shall check if it supports Signature as CVM (TTQ B1b2 =1 Signature supported).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>The Kernel shall request ‘Obtain Signature’ in the CVM Outcome parameter and request cardholder to sign a receipt.</td></tr><tr><td>No</td><td>Go to step 10</td></tr></table></td></tr>
<tr><td>9</td><td>When processing the Online PIN as CVM method, the Kernel shall update TVR B3b3 to ‘1’ (Online PIN entered).
Kernel shall request ‘Online PIN’ as the CVM outcome parameter and set Online Request as Outcome.</td></tr>
<tr><td>10</td><td>Online PIN and signature are not requested. The Kernel shall check if it supports Confirmation Code. (TTQ B3b7 = 1 Consumer Device CVM (CD CVM) supported).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 12.</td></tr><tr><td>No</td><td>Go to step 11.</td></tr></table></td></tr>
<tr><td>11</td><td>Online PIN, signature and confirmation code are not allowed. The Kernel shall check if the card allows No CVM.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>The Kernel shall request ‘No CVM’ in the CVM outcome parameter and approve the CVM.
(End Card Verification Method process. Go to the next transaction step in the process.)</td></tr><tr><td>No</td><td>Go to step 13.</td></tr></table></td></tr>
<tr><td>12</td><td>Kernel shall check if a Confirmation Code has been performed (mobile implementation) (CPR B1b5 = 1 Consumer Device CVM Performed).

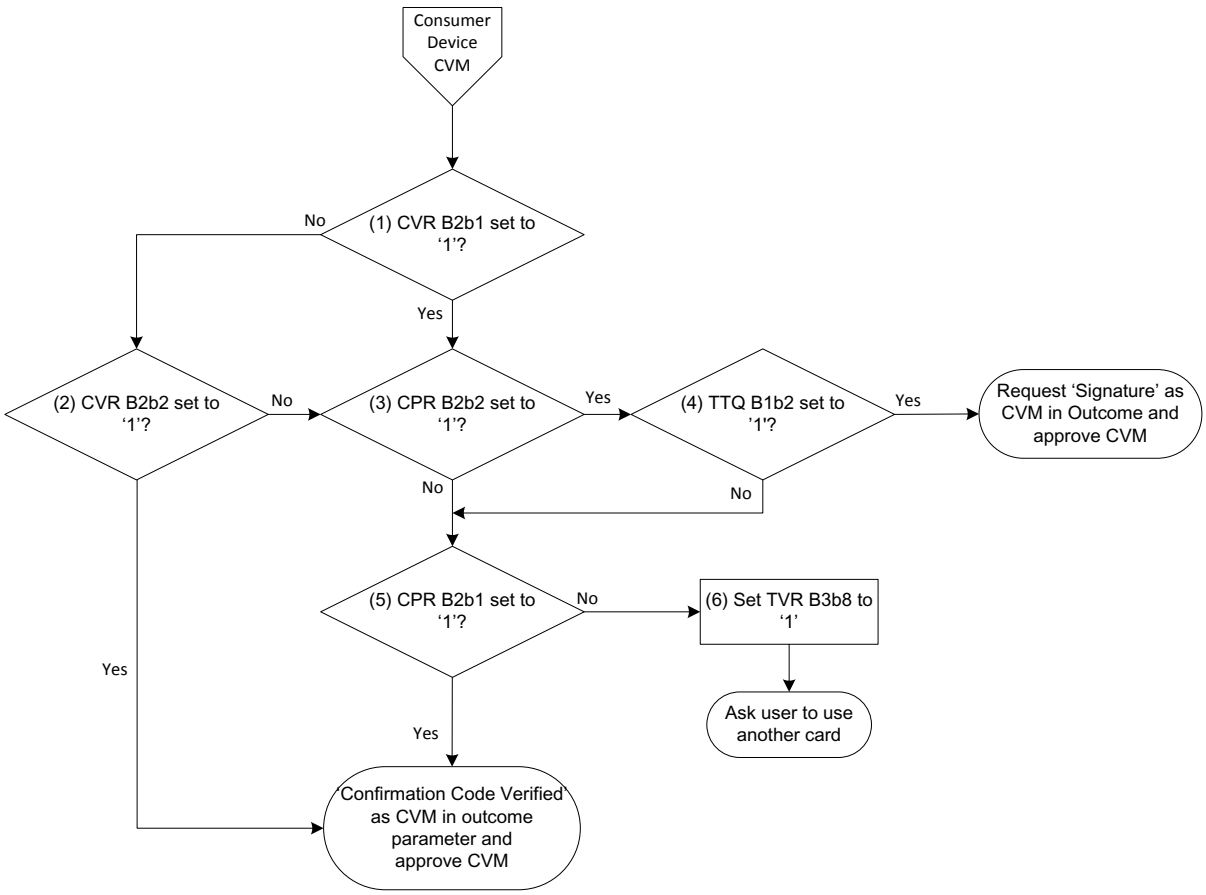
<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Process CD CVM.
(End Card Verification Method process. Go to the next transaction</td></tr></table></td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

#	Description
	<table><tr><td></td><td>step.).</td></tr><tr><td>No</td><td>Go to step 11.</td></tr></table>
13	Kernel shall check if the terminal supports another interface. • If the Kernel does not support another interface, the Kernel shall ask for another card and sends '***End Application***' (for Processing Error) Outcome. • ELSE the Kernel shall send '***Try Another Interface***' as Outcome.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-13: Cardholder Verification Method Process: Consumer Device CVM (CD CVM – Mobile Only)



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall check if the confirmation code CVR B2b1 = 1 (Confirmation Code Verification performed and failed).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>No</td><td>Go to step 2.</td></tr><tr><td>Yes</td><td>Go to step 3.</td></tr></table></td></tr>
<tr><td>2</td><td>Kernel shall check if confirmation code has been entered and successfully verified [CVR B2b2 = 1 Confirmation Code Verification performed).<table><tr><td>If…</td><td>Then…</td></tr><tr><td>No</td><td>Go to step 3.</td></tr><tr><td>Yes</td><td>Approve the CVM with ‘Confirmation Code Verified’ in the CVM Outcome parameter.
(End Card Verification Method process. Go to the next transaction step.).</td></tr></table></td></tr>
<tr><td>3</td><td>Kernel shall check if the card allows the processing of the signature (CPR B2b2 = 1 CVM Fallback to Signature allowed).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 4.</td></tr><tr><td>No</td><td>Go to step 5.</td></tr></table></td></tr>
<tr><td>4</td><td>Kernel shall check if signature is supported (TTQ B1b2 =1).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Kernel shall prompt the user to sign the receipt.
(End Card Verification Method process. Go to the next transaction step.)</td></tr><tr><td>No</td><td>Go to step 5.</td></tr></table></td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>5</td><td>Kernel shall check if the card allows “No CVM” (CPR B2b1 = 1 CVM Fallback to No CVM allowed).
<table>
<tr><td>If…</td><td>Then…</td></tr>
<tr><td>Yes</td><td>The kernel shall allow ‘No CVM’ as the CVM outcome parameter and approve the CVM.
(End Card Verification Method process. Go to the next transaction step.).</td></tr>
<tr><td>No</td><td>Go to step 6.</td></tr>
</table></td></tr>
<tr><td>6</td><td>Kernel shall indicate that CVM has failed by setting TVR B3b8 to ‘1’ (Cardholder verification was not successful) and shall ask cardholder to use another card.
Send ‘End Application’ (for Processing Error) as the Outcome.
(End Card Verification Method process. Go to the next transaction step.).</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

3.6 Processing Restrictions

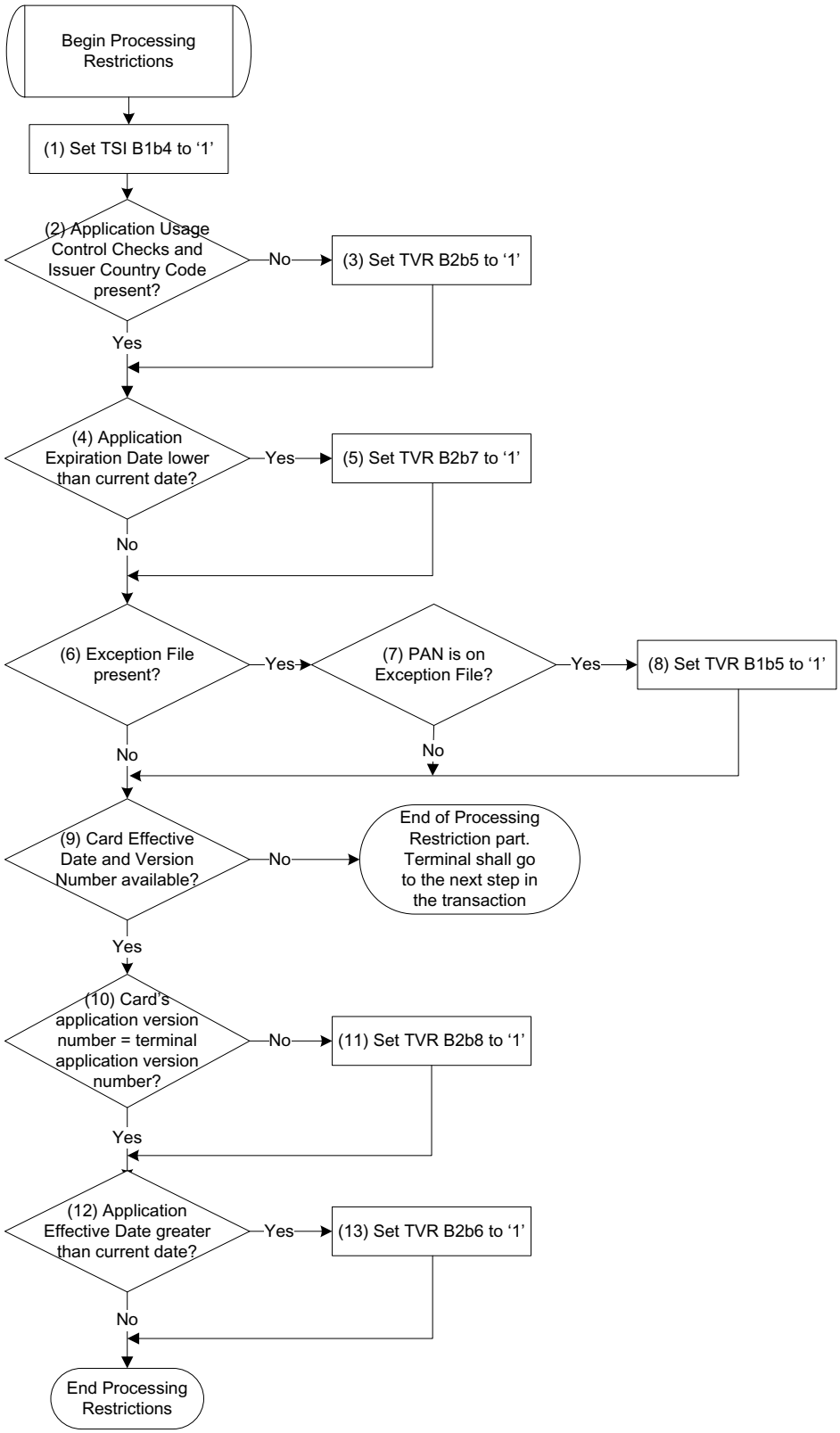
The processing restrictions function must be performed by the Kernel using the data elements retrieved from the card, as described in [EMV Book 3]. The following checks must be performed by the Kernel (based on the data provided during the completion of the READ RECORD command):

- **Application Expiration Date:** The Terminal shall extract the Expiration Date present in the Track 2 Equivalent Data and compare that value with the date of the transaction. If the date of the transaction is greater than the expiration date found in the Track 2 Equivalent Data, the Terminal shall set the TVR B2b7 to '1' (Expired application).
- **Application Effective Date:** The Terminal shall check if the application effective date is greater than the current date. If the application effective date is greater than the current date, the Terminal shall set TVR B2b6 to '1' (Application not yet effective).
- **Application Version Number:** The Terminal shall compare its application version number against the one read in the card. If they do not match, the Terminal shall set the TVR B2b8 to '1' (ICC and Terminal have different application versions).
- **Application Usage Control:** The terminal shall check for restrictions limiting the application geographically or relative to certain types of transactions. If the usage conditions are not met, the Kernel shall set the TVR B2b5 to '1' (Requested service not allowed for card product).
- **Exception File:** The Terminal shall have an internal file that references a special PAN (for example, it can be a blacklist PAN to indicate which PANs shall generate a decline transaction). If a Terminal has this type of file, it shall check that the PAN read is not present in this file. If present, the Terminal shall to set TVR B1b5 to '1' (Card appears on Terminal exception file). [There is no requirement in this specification for an Exception File; however, it is recognized that some terminals may have this capability.]

Figure 3-14 describes how the Processing Restriction step shall be performed.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-14: Processing Restriction Process



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall set the TSI B1b4 to ‘1’ (Terminal risk management was performed).</td></tr>
<tr><td>2</td><td>Kernel shall check if the Application Usage Control (AUC) and Issuer Country Code checks are present.*

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 4.</td></tr><tr><td>No</td><td>Go to step 3.</td></tr></table>
*Note: If yes, the Kernel shall complete the AUC check as described in [EMV4.2-3].
For online transactions, if either the AUC or Issuer Country Code is not present, the AUC check is skipped. For offline transactions, the AUC check is mandatory, as these two fields are read from the file records.</td></tr>
<tr><td>3</td><td>Kernel shall set TVR B2b5 to ‘1’ (Requested service not allowed for card product).</td></tr>
<tr><td>4</td><td>Kernel shall determine if the card’s application has expired.*

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 5.</td></tr><tr><td>No</td><td>Go to step 6.</td></tr></table>
1. *Note: there are two ways to retrieve the Application Expiration Date, including via the: “Track 2 Equivalent Data”.
2. Application Expiry date (tag ‘5F24’), if provided by the card. (This should match the date in the track data.)</td></tr>
<tr><td>5</td><td>If the application has expired, the Terminal shall set TVR B2b7 to ‘1’ (Expired application).</td></tr>
<tr><td>6</td><td>Kernel shall check if it embeds an exception file that contains a list of PAN(s).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 7.</td></tr><tr><td>No</td><td>Go to step 9.</td></tr></table></td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>7</td><td>Kernel shall verify if the PAN returned by the card is found inside the exception file.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 8.</td></tr><tr><td>No</td><td>Go to step 9.</td></tr></table></td></tr>
<tr><td>8</td><td>Kernel shall set TVR B1b5 to ‘1’ (Card appears on Terminal exception file).</td></tr>
<tr><td>9</td><td>Kernel shall determine if the card’s Application Effective Date (tag ‘5F25’) and Application Version Number (tag ‘9F08’) are available.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 10.</td></tr><tr><td>No</td><td>End the Processing Restriction check. Go to the next transaction step.</td></tr></table></td></tr>
<tr><td>10</td><td>Kernel shall check if the card’s Application Version Number (tag ‘9F08’) matches the Terminal’s Application Version Number (9F09’’).

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 12.</td></tr><tr><td>No</td><td>Go to step 11</td></tr></table>
Note: The card’s Application Version Number shall be present in one record under tag ‘9F08’.</td></tr>
<tr><td>11</td><td>Kernel shall update TVR B2b8 to ‘1’ (ICC and Terminal have different application versions).</td></tr>
<tr><td>12</td><td>Kernel shall check if the Application Effective Date (tag ‘5F25’) returned by the card is older than current date.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 13.</td></tr><tr><td>No</td><td>End the Processing Restriction Process.</td></tr></table>
Note: Application Effective Date shall be present in one record under tag ‘5F25’</td></tr>
<tr><td>13</td><td>Kernel shall set TVR B2b6 to ‘1’ (Application not yet effective) and exit the processing restrictions step.</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

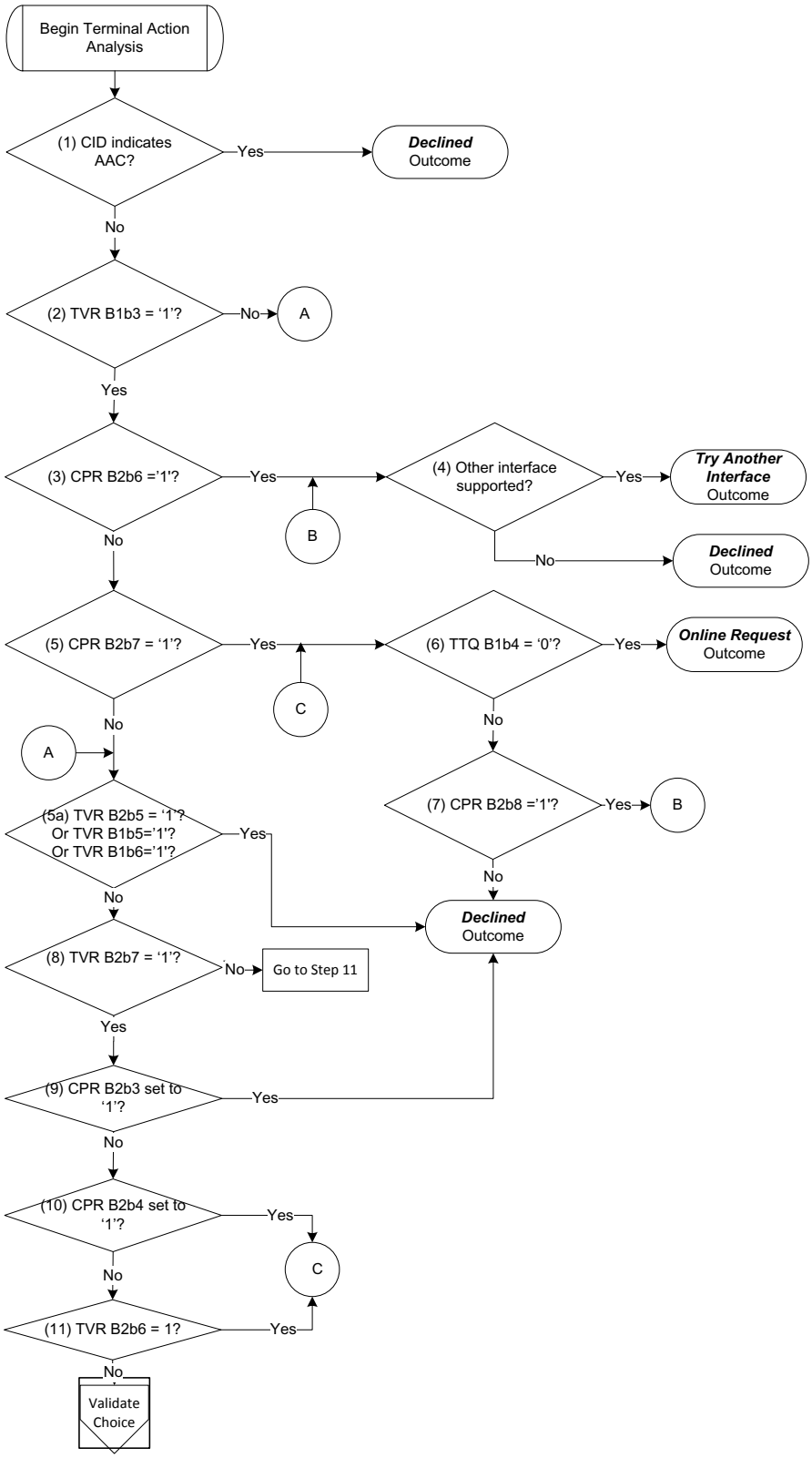
3.7 Terminal Action Analysis

Terminal Action Analysis is a mandatory step performed by the Kernel. The objective of this step is to complete additional checks on the Kernel side to make a final decision concerning the current transaction.

The Kernel shall not perform this step if the decision taken by the card is to decline the transaction. The Kernel shall check if some TVR bits are set and then (if they are set) shall determine the card recommendations. The following diagrams show the Terminal Action Analysis to be performed.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-15: Terminal Action Analysis Process



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall check if the card returns a decline transaction response based on the CID setting [i.e., CID B1b8-7 to '00' (00 = AAC)].
<table>
<tr><td>If…</td><td>Then…</td></tr>
<tr><td>Yes</td><td>Decline the transaction and send the Outcome as 'Declined'.</td></tr>
<tr><td>No</td><td>Go to step 2.</td></tr>
</table></td></tr>
<tr><td>2</td><td>Kernel shall check if CDA has failed [TVR B1b3 = '1' (CDA failed)].
<table>
<tr><td>If…</td><td>Then…</td></tr>
<tr><td>Yes</td><td>Go to step 3.</td></tr>
<tr><td>No</td><td>Go to step 5a.</td></tr>
</table>
Note: When the Kernel processes the TVR, the following applies:
If CDA has not been processed or CDA is successful, the Kernel shall skip the card's recommendation and go to step 5a.
If CDA is failing, go to step 3.</td></tr>
<tr><td>3</td><td>Kernel shall perform a CPR check to determine if the card allows a switch to another interface or decline of the transaction if CDA is failing [CPR B2b6 = '1' (Decline/switch other interface if CDA failed).
<table>
<tr><td>If…</td><td>Then…</td></tr>
<tr><td>Yes</td><td>Go to step 4.</td></tr>
<tr><td>No</td><td>Go to step 5.</td></tr>
</table></td></tr>
<tr><td>4</td><td>Kernel shall verify if it supports another interface that can process the transaction.
If the Terminal has another interface, it shall send the 'Try Another Interface' Outcome. (End the Terminal Action Analysis. Go to the next transaction step.)
ELSE it shall decline the transaction and send the Outcome as 'Declined' (End the Terminal Action Analysis. Go to the next transaction step.)</td></tr>
<tr><td>5</td><td>Kernel shall go online for authorization if CDA is failing [CPR B2b7 = '1' (Process online if CDA failed)].
<table>
<tr><td>If…</td><td>Then…</td></tr>
<tr><td>Yes</td><td>Go to step 6.</td></tr>
<tr><td>No</td><td>Go to step 5a.</td></tr>
</table></td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

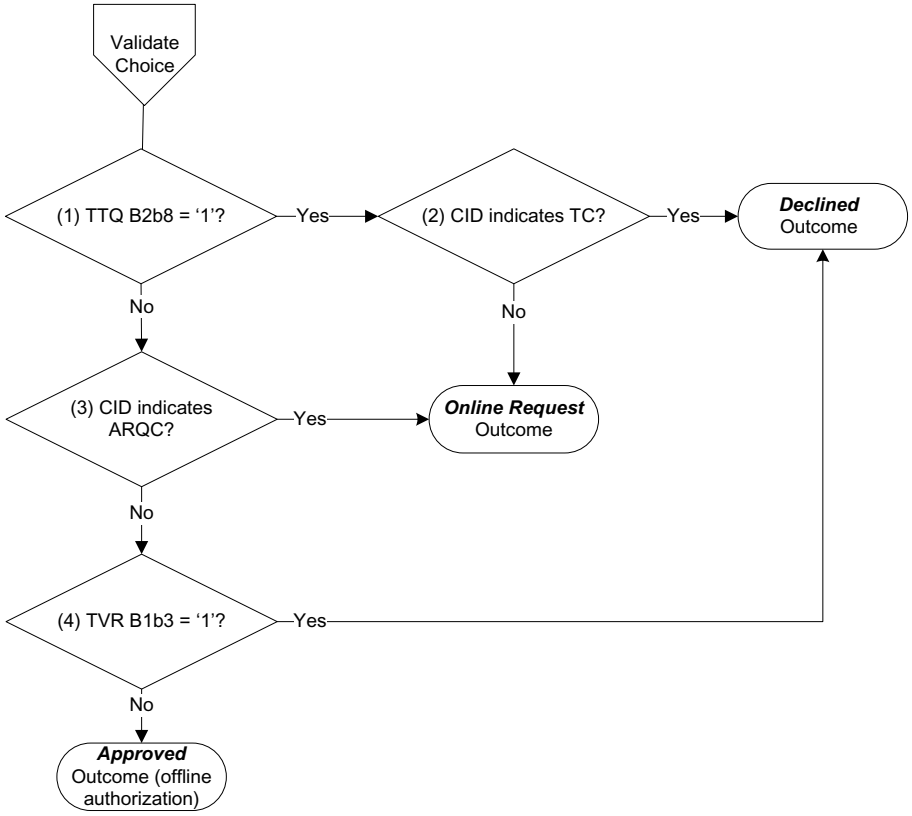
#	Description
5a	Kernel shall check if: • Application usage is not allowed [TVR B2b5 = '1' (Requested service not allowed for card product)], or • The card appears in the exception file [TVR B1b5 = '1' (Card appears on Terminal exception file)], or • ICC data missing bit is set [TVR B1b6 = '1' (ICC Data missing)]. • If any one of the foregoing conditions is true, the Kernel shall decline the transaction with '***Declined***' Outcome (End the Terminal Action Analysis). **ELSE** go to step 8.
6	Kernel shall check if it is configured to go online for authorization (TTQ B1b4 ='0' Offline-only Reader). • If Terminal is able to go online [TTQ B1b4 ='0' (Not Offline-only Reader)], then it shall process the online authorization with the Outcome as '***Online Request***'. (End the Terminal Action Analysis. Go to the next transaction step.) • ELSE it will to step 7.
7	Kernel shall check if the card allows a switch to another interface, if the Terminal is not able to go online [CPR B2b8 = '1' (Switch other interface if unable to process online)]. • If the card does not allow a switch to another interface, the Kernel shall decline the transaction with '***Declined***' Outcome. (End the Terminal Action Analysis. Go to the next transaction step). • If allowed to switch to another interface with '***Try Another Interface***' Outcome, the Terminal shall go to step 4.
8	Kernel shall check if the application has expired (TVR B2b7 Expired application). • If not expired, the Kernel shall go to step 11. • If expired, go to step 9.
9	Kernel shall check if it should decline the transaction when application has expired: • If CPR B2b3 is set to '1' (Decline if card expired), the Kernel shall decline the transaction with '***Declined***' Outcome (End the Terminal Action Analysis). • ELSE, go to step 10.
10	Kernel shall check if it should process the transaction online when application has expired [CPR B2b4 = '1' (Process online if card expired)]. • If CPR B2b4 is set, the Kernel shall go to step 6. • If it is not set, go to Step 11.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

#	Description
11	Kernel shall check if TVR B2b6 is set to '1' (Application is not yet effective). • If yes, the Kernel shall try to process transaction online or request another interface by going to Step 6 • Else, Kernel shall go to the second part of Terminal Action Analysis.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-16: Terminal Action Analysis Process (Validate Choice)



#	Description
1	Kernel shall verify if an online cryptogram is required [TTQ B2b8 = '1' (Online Cryptogram required)]. If… / Then… Yes / Go to step 2. No / Go to step 3.
2	Kernel shall verify if the CID indicates TC based on the CID setting [i.e., CID B1b8-7 to '01' (01 = TC)]. • If the card has approved the transaction when the Kernel asked to go online (i.e., the CID indicates TC), the Kernel shall send a '***Declined***' Outcome (End the Terminal Action Analysis). • ELSE, it shall process the online authorization with '***Online Request***' Outcome (End the Terminal Action Analysis).

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

#	Description
3	Kernel shall verify which action the card wants to complete. • If the card requests an online authorization (i.e., CID indicates ARQC) based on the CID setting [i.e., CID B1b8-7 to '10' (10 = ARQC)], the Kernel shall process the transaction online with '***Online Request***' Outcome (End the Terminal Action Analysis). • Else, go to step 4.
4	If the transaction is not sent online and the CDA check is not equal to '1` [(TVR B1b3 = '0' (CDA did not fail)], the Kernel shall approve the transaction offline with '***Approved***' Outcome, (End the Terminal Action Analysis). Else the Kernel shall decline the transaction '***Declined***' Outcome.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

3.8 Online Processing

Online processing is performed if:

- It is supported by the reader and warranted based on the results of the prior steps, or
- The transaction is being completed in MS Mode or Legacy Mode.

The Online Processing step consists of sending the transaction data to the Issuer, who will then decide whether to approve or decline the transaction and then send that decision back to the reader. This enables the Issuer to complete further analyses of the transaction relative to the Cardholder's account and any other criteria specific to the Issuer.

If the Reader is configured with TTQ B3b8 = '1' (Issuer Update Processing supported) and the card is configured with CPR B2b5 = '1' (Issuer Update Processing supported), the Kernel shall process the Outcome as '***Online Request (for Two Presentments)'***.

3.9 Completion

Completion is the last step of the transaction unless script processing is required. Upon completion, the Kernel communicates an Outcome to Entry Point, and provides parameter values based on the associated Outcome and transaction mode as specified in [EMV Book A]. The final completion decision may consist of one of the following:

- **Offline declined**: The transaction has been declined. The Kernel shall notify the user and log information regarding the transaction with a '***Declined***' Outcome, or the Kernel may ask the user to present a new card or to switch to another interface by sending a '***Try Another Interface***' Outcome.

- **Offline approved**: The transaction has been approved without sending the transaction online for authorization, and the Kernel shall return the Outcome as '***Approved***' to notify the user. The Terminal shall log transaction information for clearing (that may occur at a later time).

- **Online approved**: The transaction has been processed online, and the Issuer approved the transaction. Information concerning the transaction may be logged; however, this is not mandatory as the Issuer has already obtained all of the information required for clearing. The Kernel notifies the user that the transaction has been approved online with an '***Approved***' Outcome.

- **Online declined**: The transaction has been processed online, and the Issuer declined the transaction. Information concerning the transaction may be logged; however, this is not mandatory because no clearing is required. The Kernel notifies the user that the transaction has been online declined with a '***Declined***' Outcome.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

- **Switch to another interface**: The transaction cannot be processed using the contactless interface but may be processed via a magnetic stripe or contact interface. The Kernel notifies the user to use another interface by sending a '***Try Another Interface***' Outcome. **Select Next**: The Kernel has determined that the selected Combination is unsuitable, and the next Combination (if any) should be tried.

- **Try Again**: The Kernel requires that the device be presented again; this may be a result of an error, such as tearing, that could resolve if the transaction is attempted again.

- **End Application**: The Kernel experienced an application error, such as missing data that will not resolve if the transaction is attempted again with the same selected Contactless Card application.

Refer to Annex B for all the Transaction Outcomes by the Kernel with their Outcome parameters.

3.10 Issuer Update Processing

Issuer Update Processing is an optional step that shall be processed only if the Kernel receives Issuer script processing commands. Issuer scripts may be processed irrespective of whether an online transaction is approved or declined. This requires both card and reader to support the second presentment of a card after an Issuer responds to an online request. If the Issuer responds with a script command in the online authorization response message, the Kernel will request the cardholder to present the card again. Once the card is presented, the Kernel sends the SELECT command using the same combination as used for the first presentment. If a different card is presented, then either it will not be successfully selected by the Kernel, or the Issuer script update will fail.

Issuer script commands are received in the authorization responses in Tags '71' or '72'. For Kernel 6, only one template tag '71' or '72' is allowed in one transaction. Each individual script command within tag '71' or '72' is encapsulated within tag '86'.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

The aim of Issuer Updates Processing is to transmit Issuer script commands to the card and check the answer returned by the card as follows:

- SW = ’9000’: Kernel has successfully processed the command. The Kernel shall send the next script command (if a new script command has to be sent to the card).
- SW = ’6982’: Kernel shall update TVR B5b7 to ‘1’ (Issuer authentication failed) and TVR B5b6 to ‘1’ (Script processing failed before final GENERATE AC).Other SWs: Kernel shall update TVR B5b6 to ‘1’ (Script processing failed before final GENERATE AC).

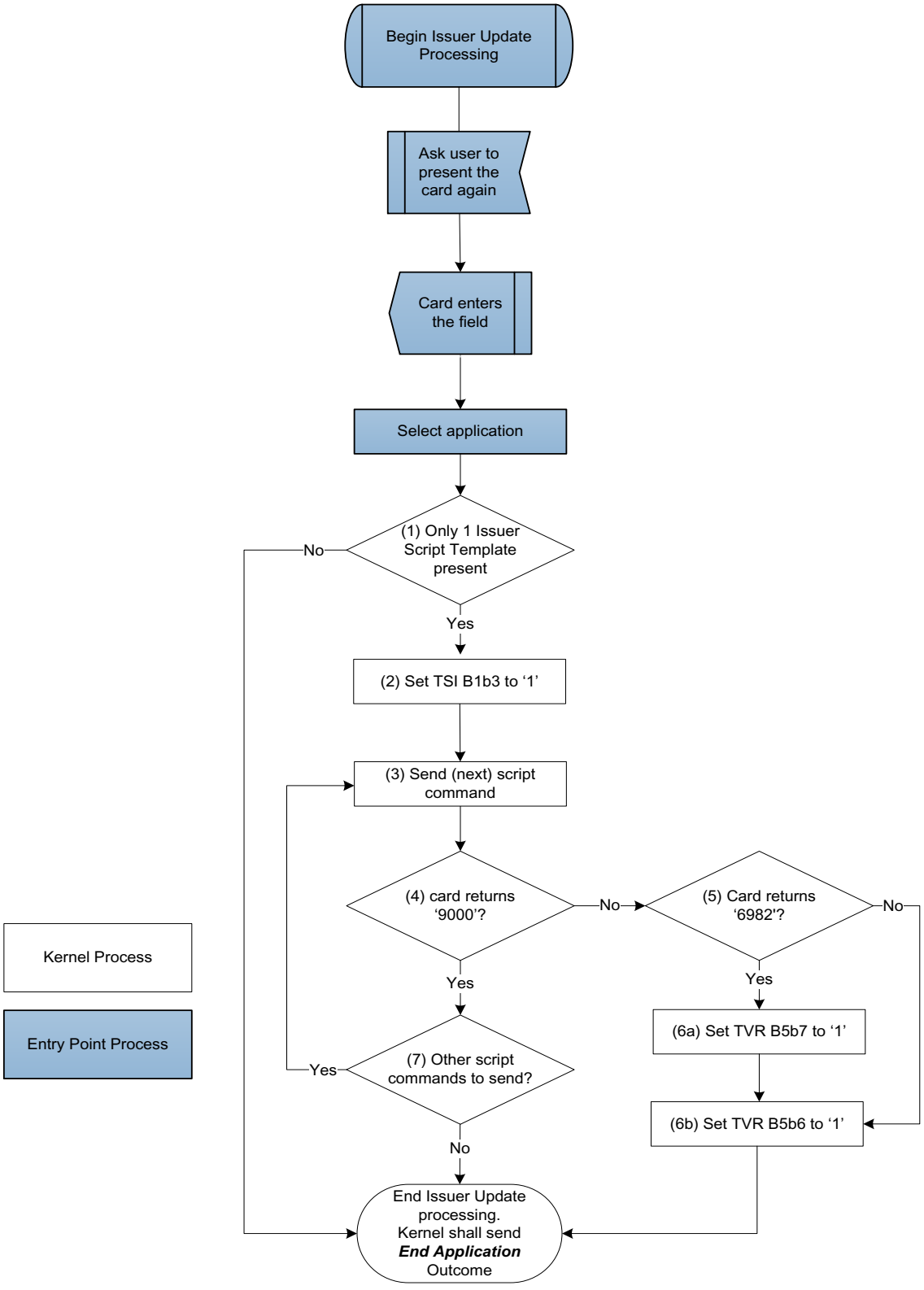
Each time that the Kernel receives Issuer script commands to be transmitted to the card, the Kernel has to update:

- TSI B1b5 to ‘1’ (Issuer authentication was performed), and
- TSI B1b3 to ‘1’ (Script processing was performed).

Processing is ended when the card generates an error message or no additional scripts must be sent to the card. After completing Issuer Update Processing, the Kernel shall provide an ‘***End Application***’ Outcome. The POS system will indicate to the cardholder the transaction Outcome based on the Issuer authorization response, regardless of the results of Issuer Update Processing. At that point, the Kernel shall send the TVR and TSI to the Issuer to communicate the status of the script commands sent to the card. The following diagram illustrates the Issuer update process.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Figure 3-17: Issuer Update Process



© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

<table>
<tr><th>#</th><th>Description</th></tr>
<tr><td>1</td><td>Kernel shall check if only one Issuer Script template is present.

<table><tr><td>If…</td><td>Then…</td></tr><tr><td>Yes</td><td>Go to step 2.</td></tr><tr><td>No</td><td>End the transaction. The Kernel shall send the TSI and TVR to the Issuer.</td></tr></table></td></tr>
<tr><td>2</td><td>Kernel shall update TSI B1b3 to ‘1’ (Script processing was performed) to indicate that Issuer scripts commands are being sent to the card.</td></tr>
<tr><td>3</td><td>Kernel shall send the script command (next available) received from Issuer.</td></tr>
<tr><td>4</td><td>Kernel shall verify the status word returned by the card.

<table><tr><td>If the card…</td><td>Then…</td></tr><tr><td>Returns ‘9000’</td><td>Go to step 7.</td></tr><tr><td>Does not return ‘9000’</td><td>Go to step 5.</td></tr></table></td></tr>
<tr><td>5</td><td>Kernel shall verify the status word returned by the card.

<table><tr><td>If the card…</td><td>Then…</td></tr><tr><td>Returns ‘6982’</td><td>Go to step 6a.</td></tr><tr><td>Does not return ‘6982’</td><td>Go to step 6b.</td></tr></table></td></tr>
<tr><td>6a</td><td>There is an error with the MAC verification. Kernel shall update TVR B5b7 to ‘1’ (Issuer authentication failed).</td></tr>
<tr><td>6b</td><td>Kernel shall update TVR B5b6 to ‘1’ (Script processing failed before final GENERATE AC).
The Kernel shall end Issuer script processing with ‘End Application’ Outcome.</td></tr>
<tr><td>7</td><td>The Kernel shall check if another script command needs to be sent to the card.
• If a script command is available, the Kernel shall go to step 3.
• ELSE, the Kernel shall end the Issuer script processing with ‘End Application’ Outcome.</td></tr>
</table>

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

[This page is intentionally left blank.]

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

4 Application Protocol Data Unit (APDU) Command Description

4.1 Summary

This section describes the APDU commands that the Terminal must be able to send to the card. Each command sent by the Terminal must be correctly formatted as specified in [ISO/IEC 7816-4]. Status bytes descriptions are included in [EMV Book 3].

When the card returns the answer to the command, the Terminal must always first check the SW of the answer and abort the transaction if the SW does not indicate normal processing (i.e., SW = ’9000’ or ’61XX’).

Table 4-1: List of APDU Commands Used by This Kernel

Command	CLA	INS	P1	P2	Lc	Data	Le
SELECT	‘00’	‘A4’	‘04’	‘00’ First or only occurrence ’02’ Next occurrence	’05’-‘10’	AID	‘00’
GET PROCESSING OPTIONS	‘80’	‘A8’	‘00’	‘00’	Var.	Data elements specified in PDOL Tag '83' || Length || Concatenation of the BER-TLV value of the data elements specified in Processing Options Data Object List (PDOL) No PDOL: '8300'	‘00’
READ RECORD	‘00’	‘B2’	Record Number	Reference Control Parameter	Not Present	Not Present	‘00’

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Command	CLA	INS	P1	P2	Lc	Data	Le
GET DATA	'80'	'CA'	Tag		Not Present	Not Present	'00'
							Length of TLV field
UPDATE RECORD	'84'	'DC'	Record Number	Reference Control Parameter	Var.	Record Data Object + 8 Bytes for MAC	Not Present
PUT DATA	'84'	'DA'	Tag		Var.	Tagged Data Object + 8 bytes for MAC	Not Present
APPLICATION BLOCK	'84'	'1E'	'00'	'00'	'08'	MAC	Not Present
APPLICATION UNBLOCK	'84'	'18'	'00'	'00'	'08'	MAC	Not Present

4.2 SELECT

The SELECT command is issued to activate and select an application in the card. The SELECT command conforms to the requirements specified in [EMV Book 1].

4.3 GET PROCESSING OPTIONS

The GET PROCESSING OPTIONS (GPO) command is used to inform the Contactless Card that the processing of a new transaction is beginning. The command is sent by the kernel to the card with the information requested in the PDOL.

The GET PROCESSING OPTIONS command conforms to the requirements specified in [EMV Book 3] and the Kernel-specific requirements described in the following sections.

4.3.1 Data Field Returned in the Response Message

The data field returned in the GPO response message shall be coded according to EMV format 2 for MS, Legacy, and EMV Modes. This format requires a constructed BER-TLV data object with template '77' as shown in the following table.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Table 4-2: GET PROCESSING OPTIONS Response Data Objects

Tag	Length	Data Object 1	Data Object 2	Data Object ....
'77'		Application Interchange Profile (AIP) (Primitive or constructed BER-TLV data object number 1)	Application File Locator (AFL) (Primitive or constructed BER-TLV data object number 2)	... (Primitive or constructed BER TLV data object number ...)

The value field shall consist of several BER-TLV coded objects that shall always include the mandatory data specified in Table 4-3 (for Legacy MS Mode and MS Mode) and Table 4-4 (for EMV Mode).

If any of these mandatory data elements are missing, the Terminal shall terminate the transaction.

Table 4-3: GET PROCESSING OPTIONS Response Data Field for Legacy and MS Modes

Tag Description	Tag	Presence
Application Interchange Profile (AIP)	'82'	Mandatory
Application File Locator (AFL)	'94'	Mandatory

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Table 4-4: GET PROCESSING OPTIONS Response Data Field for Contactless EMV Mode

Data Element	Tag	Length	C6 Kernel		
			Online Processing (ARQC, no CDA)	**Decline Processing (AAC, no CDA)**	**Offline-capable Processing (TC or AAC with CDA)**
Application Interchange Profile (AIP)	'82'	2 bytes	Mandatory	Mandatory	Mandatory
Application File Locator (AFL)	'94'	Var.	Optional (set in CL-ACO B2b8)	Optional (set in CL-ACO B2b8)	Mandatory
Application Cryptogram	'9F26'	8 bytes	Mandatory	Mandatory	Not Present
Signed Dynamic Application Data	'9F4B'	N_{IC} bytes	Not present	Not Present	Mandatory
Application Transaction Counter (ATC)	'9F36'	2 bytes	Mandatory	Mandatory	Mandatory
Issuer Application Data (IAD)	'9F10'	Var. up to 32 bytes	Mandatory	Mandatory	Mandatory
Cryptogram Information Data (CID)	'9F27'	1 byte	Mandatory	Mandatory	Mandatory
Track 2 Equivalent Data	'57'	Var. up to 19 bytes	Conditional (Not Present if AFL is present)	Conditional (Not Present if AFL is present)	Not present
Application Usage Control (AUC)	'9F07'	2 bytes	Conditional (Not Present if AFL is present)	Conditional (Not Present if AFL is present)	Not present
Issuer Country Code	'5F28'	2 bytes	Conditional (Not Present if AFL present)	Conditional (Not Present if AFL present)	Not Present

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Data Element	Tag	Length	C6 Kernel		
			Online Processing (ARQC, no CDA)	**Decline Processing (AAC, no CDA)**	**Offline-capable Processing (TC or AAC with CDA)**
PAN Sequence Number (PSN)	'5F34'	1 byte	Conditional (Not Present if AFL is present)	Conditional (Not Present if AFL is present)	Not present
Card Processing Requirements (CPR)	'9F71'	2 bytes	Mandatory	Mandatory	Mandatory
Offline Balance	'D1'	6 bytes	Optional	Not present	Optional
Application Effective Date	'5F25'	3 bytes	Conditional (Not Present if AFL is present)	Conditional (Not Present if AFL is present)	Not present
Application Version Number	'9F08'	2 bytes	Conditional (Not Present if AFL is present)	Conditional (Not Present if AFL is present)	Not present

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

4.4 READ RECORD

The READ RECORD command shall be issued by the Kernel to retrieve data stored in one record. The data present in the record depends on how the application has been personalized.

The command is performed when the AFL was returned by the card during Initiate Application Processing via the GET PROCESSING OPTION. The Kernel shall then send the command according to information in the AFL. The Terminal shall store the data read in temporary memory. Some Terminals (such as ATMs for example) are also able to read the log record.

Refer to [EMV Book 3] for additional information, including the Command format and Response message format.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

4.5 GET DATA

This command shall be issued by the Terminal to retrieve a primitive data object that is not encapsulated in a record within the current application. The Terminal shall store the data value in temporary memory.

Refer to [EMV Book 3] for additional details, including the Command format and Response message format.

4.6 PUT DATA

This command shall be issued by the Terminal on Issuer request. The aim is to update some primitive data objects. The command can only be sent during Issuer update processing (meaning during second presentment). The full command is sent by Issuer to the Terminal.

4.6.1 Command Format

The PUT DATA command is coded as specified in Table 4-5.

Table 4-5: PUT DATA Command Format

Code	Value
CLA	'84'
INS	'DA'
P1	MSB byte of the primitive data object to be updated (set to ‘00’ if tag is one byte long)
P2	LSB byte of the primitive data object to be updated
Lc	Var. (length of data field including the MAC)
Data	New data value and MAC (MAC is 8-bytes long)
Le	Not present

4.6.2 Data Field Returned in the Response Message

No data are returned by the card. The Terminal shall check that card returns ’9000’ to this command.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

4.7 UPDATE RECORD

The UPDATE RECORD command is an Issuer script command that writes new values into the Elementary File (EF) Record identified by an SFI. This command shall be issued by the Terminal on Issuer request. The aim is to update one record content.

For a Contactless Card transaction, the command can only be sent during Issuer update processing (meaning during second presentment). The full command is sent by Issuer to the Terminal.

4.7.1 Command Format

The UPDATE RECORD command is coded as specified in the table below:

Table 4-6: UPDATE RECORD Command Format

Code	Value
CLA	'84'
INS	'DC'
P1	Record Number
P2	Reference Control Parameter
Lc	Var. (length of data field including the MAC)
Data	New data value and MAC (MAC is 8-bytes long)
Le	Not present

The reference control parameter shall be coded as follows

Table 4-7: Reference Control Parameter

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x				SFI
					1	0	0	P1 is a record number

4.7.2 Data Field Returned in the Response Message

No data are returned by the card. The Terminal shall check that the card returns ’9000’ to this command.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

4.8 APPLICATION BLOCK

This is a script command provided by the Issuer to the Terminal to invalidate the application. The Terminal shall send the command as provided by the Issuer. The command shall be coded as specified in [EMV Book 2] using Secure Messaging for Integrity and Authentication Format 2.

Refer to [EMV Book 3] for additional details, including the Command format and Response message format.

4.9 APPLICATION UNBLOCK

This is a script command provided by the Issuer to the Terminal to unblock the application. The Terminal sends the command as provided by the Issuer. The command shall be coded as specified in [EMV Book 3] using Secure Messaging for Integrity and Authentication Format 2.

Refer to [EMV Book 3] for additional details, including the Command format and Response message format.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

[This page is intentionally left blank.]

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Annex A Glossary

This annex provides a glossary of terms and abbreviations used in this specification.

Term	Definition
AAC	Application Authentication Cryptogram. An Application Cryptogram generated by the card when declining a transaction.
AC	Application Cryptogram. For contactless transactions: A cryptogram generated by the card in response to a GET PROCESSING OPTIONS command.
ADF	Application Definition File. Identifies the application (AID) as described in [ISO/IEC 7816-5].).
AEF	Application Elementary File. See [EMV Book 3].
AFL	Application File Locator. Indicates the location (SFI, range of records) of the AEFs related to a given application.
AID	Application Identifier. Identifies the application as described in ISO/IEC 7816-5.
AIP	Application Interchange Profile. Indicates the capabilities of the card to support specific functions in the application.
APDU	Application Protocol Data Unit. The Data Unit used to exchange information between the Terminal via a Command APDU (C-APDU) and card via a Response APDU (R-APDU) as defined in [ISO/IEC 7816-4].
API	Application Priority Indicator. Indicates the priority of a given application or group of applications in a directory.
Application Effective Date	Date from which the application may be used.
Application Expiration Date	Date after which the application expires.
Application Label	Mnemonic associated with the AID according to ISO/IEC 7816-5
Application Version Number	Version number assigned by the payment system for the application.
ATC	Application Transaction Counter. Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC).
AUC	Application Usage Control. Indicates the Issuer's specified restrictions on the geographic usage and services allowed for the application.
BER-TLV	Basic Encoding Rules – Tag Length Value. A set of encoding rules for a data object. As defined in ISO/IEC 8825-1, a BER-TLV data element consists of the following three consecutive components: • Tag field (T) indicates a class, a type, and a number. • Length field (L) indicates the length of the field. • Value field (V) indicates the value of the data object. (Note that if L = '00', the value field is not present.)
CA PKI	Certificate Authority Public Key Index. Identifies the certification authority's public key in conjunction with the RID.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Term	Definition
CDA	Combined Dynamic Data Authentication / Application Cryptogram Generation. A form of offline dynamic data authentication.
CID	Cryptogram Information Data. Indicates the type of cryptogram and the actions to be performed by the Terminal.
CL-ACO	Contactless Application Configuration Options. A Contactless D-PAS proprietary data element that contains a list of the card supported functions and the AIP.
Combination	Apply the following:

For:	The combination of:
• a card	• an ADF Name • a Kernel Identifier
• a reader	• an AID • a Kernel ID
• the Candidate List for final selection	• an ADF Name • a Kernel ID • the Application Priority Indicator (if present) • the Extended Selection (if present)

CPR	Card Processing Requirement. Data element that indicates the card requirements for processing the transaction to the reader.
CRM-CACs	Card Risk Management-Card Action Codes. Designated by Issuers and used during the Card Action Analysis to determine the level of risk associated with a transaction.
CVM-CACs	Card Verification Method-Card Action Codes. Designated by Issuers and used during the Card Action Analysis to determine the type of Card Verification to be applied to the transaction.
Data Element Processing	Addresses Requirements regarding the Presence of Data, Rules for Padding, and Order of Data Elements as specified in [EMV Book B).
DCVV	Dynamic Card Verification Value. The dynamic CVV value generated by a card during a contactless magnetic stripe transaction.
DDF	Directory Definition File (DDF). Issuer discretionary part of the directory according to ISO/IED 7816-5.
DF Name	Dedicated File Name. Identifies the name of the DF as described in ISO.IEC 7816-4.
EMV Mode	An operating mode of the POS System that indicates that this particular acceptance environment and acceptance rules supports chip infrastructure. Typically used in conjunction with the term “transaction” (i.e., EMV Mode transaction) to indicate contactless payment utilizing a full chip infrastructure carrying EMV minimum data.
Entry Point	Within these specifications, Entry Point is software in the POS System that is responsible for the following: • Performing pre-processing, • Discovery and selection of a contactless application that is supported by

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Term	Definition
	both the card and the reader, • Activation of the appropriate Kernel, and • Handling of Outcomes returned by the Kernel, including passing selected Outcomes to the reader. Under exception conditions, Entry Point may return an Outcome to the reader as a result of its own processing.
Exception File	A file listing cards and associated applications.
FCI Issuer Discretionary Data	File Control Information (FCI) Issuer Discretionary Data. Issuer discretionary part of the FCI.
FCI	File Control Information
IAD	Issuer Application Data. Contains proprietary application data for transmission to the Issuer in an online Transaction.
ICC	Integrated Circuit Card. A card with an embedded chip that communicates with a point of interaction (terminal).
IDD	Issuer Discretionary Data. Issuer-specified data relating to the application that is part of the Issuer Application Data.
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
Kernel	The set of functions required to be present on every terminal implementing a specific interpreter. The kernel contains device drivers, interface routines, security and control functions, and the software for translating from the virtual machine language to the language used by the real machine. In other words, the kernel is the implementation of the virtual machine on a specific real machine.
Kernel Activation:	The activation of the selected Kernel via Entry Point to enable the beginning of Kernel processing.
Kernel Identifier	Identifier to distinguish between different kernels that may be indicated by the card.
Legacy MS Mode	Legacy Magnetic Stripe Mode. A payment solution that uses Track 1 and Track 2 equivalent data and Radio-Frequency communication to enable the performance of transactions via contactless technology.
MS Mode	Magnetic Stripe Mode. An operating mode of the POS System that indicates that this particular acceptance environment and acceptance rules supports mag-stripe infrastructure. Typically used in conjunction with the term “transaction” (i.e., MS Mode transaction) to indicate contactless payment based on Track 1 and Track 2 Data obtained from the card.
ODA	Offline Data Authentication.
PAN	Primary Account Number.
PAN Sequence Number	Primary Account Number Sequence Number. Identifies and differentiates cards with the same PAN.
PDOL	Processing Data Objects List. Contains a list of terminal resident data objects (tags and lengths) needed by the ICC in processing the GET PROCESSING OPTIONS command.
Protocol Activation	Activation of the contactless interface.
Radio Frequency	RF

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Term	Definition
RID	Registered Application Provider Identifier. Part of an AID as defined in [ISO/IEC 7816-4] and obtained as specified in [ISO/IEC 7816-5]. The RID is unique to an application provider and consists of the 5 most significant bytes of the AID.
SDAD	Signed Dynamic Application Data. Digital signature on critical application parameters for DDA or CDA.
SFI	Short File Identifier. Identifies the AEF referenced in commands related to a given ADF or DDF. The SFI is a binary data object having a value in the range 1 to 30 and with the three high order bits set to 0.
Starting Points	

	Start at:	Activation
Start A	Pre-Processing	Start at Pre-Processing; activated by the reader when Autorun is 'No'. This is typical for a new transaction with a variable amount in an EMV Mode acceptance environment.
Start B	Protocol Activation	Activated in any of the following cases: • Activated by the reader when Autorun is 'Yes'; this is typical for a new transaction with a fixed amount in an MS Mode acceptance environment, or • Activated by the reader to handle Issuer responses after an ***Online Request*** or ***End Application*** Outcome with parameter Start = B, or • Handled internally by Entry Point for an error situation, or • Handled internally by Entry Point for a ***Try Again*** Outcome
Start C	Combination Selection	Handled internally by Entry Point for a ***Select Next*** Outcome.
Start D	Kernel Activation	Activated by the reader to handle Issuer responses after an Online Request Outcome with parameter Start = D.

TC	Transaction Certificate. An Application Cryptogram generated by the card when approving a transaction.
TTQ	Terminal Transaction Qualifiers. Indicates the requirements for online and CVM processing as a result of Entry Point processing. The scope of this tag is limited to Entry Point. Kernels may use this tag for different purposes.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Term	Definition
Track 2 Equivalent Data	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, and • Discretionary Data (defined by individual payment systems). Pad with one Hex 'F; if needed to ensure whole bytes.
Triple DES (3DES)	Triple Data Encryption Standard.
TVR	Terminal Verification Results. Status of the different functions as seen from the terminal
UN	Unpredictable Number. Value to provide variability and uniqueness to the generation of a cryptogram.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Annex B Kernel 6 Transaction Outcome and Parameter Settings

An Outcome is the primary instruction from the Kernel or Entry Point on how processing should be continued. When a Kernel provides an Outcome, control is passed back to Entry Point which handles certain parameters immediately, then either processes the Outcome or forwards it to the reader as a Final Outcome.

Refer to [EMV Book A] for description of all the Outcome parameters, their values and User Interface standard Display messages.

B.1. Approved

The kernel has determined that the transaction is approved, either through offline processing or after reactivation following an online response.

Outcome	Outcome Parameter	Value
Approved	Start	N/A
	Online Response Data	N/A
	CVM	As described in Section 3.5 Cardholder Verification
	UI Request on Outcome Present	Yes Message Identifier: as applicable '03' (Approved) '1A' (Approved – Please Sign) Status: Card Read Successfully [Value Qualifier: Balance] [Value: Offline Balance (from Tag 'D1')] [Currency Code: Transaction Currency Code] Note: Balance is displayed only if 'D1' is returned by card
	UI Request on Restart Present	No
	Data Record Present	Yes The minimum data requirements for clearing records are specified in Annex B.10.
	Discretionary Data Present	No
	Alternate Interface Preference	N/A
	Receipt	Yes or N/A as required
	Field Off Request	N/A
	Removal Timeout	Zero

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

B.2. Online Request

The kernel requests online authorization.

Outcome	Outcome Parameter	Value
Online Request	Start	N/A
	Online Response Data	N/A
	CVM	As described in Section 3.5 Cardholder Verification
	UI Request on Outcome Present	Yes Message Identifier: '1B' (Authorizing, Please Wait) Status: Card Read Successfully [Value: Offline Balance (from Tag 'D1')] [Currency Code: Transaction Currency Code] Note: Balance is displayed only if 'D1' is returned by card
	UI Request on Restart Present	No
	Data Record Present	Yes The minimum data requirements for online authorization are specified in Annex B.10.
	Discretionary Data Present	No
	Alternate Interface Preference	N/A
	Receipt	Yes or N/A as required
	Field Off Request	N/A
	Removal Timeout	Zero

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

B.3. Online Request (for Two Presentments)

The kernel has determined that the transaction must be sent online and that the card can be re-presented.

Outcome	Outcome Parameter	Value
Online Request (for Two Presentments)	Start	B
	Online Response Data	EMV data
	CVM	As described in Section 3.5 Cardholder Verification
	UI Request on Outcome Present	Yes Message Identifier: as applicable: '1B' (Authorizing, Please Wait) [Value: Offline Balance (from Tag 'D1')] [Currency Code: Transaction Currency Code] Note: Balance is displayed only if 'D1' is returned by card
	UI Request on Restart Present	Message Identifier: '21' (Present Card Again) Status: Ready to Read
	Data Record Present	Yes The minimum data requirements for online authorization are specified in Annex B.10.
	Discretionary Data Present	No
	Alternate Interface Preference	N/A
	Receipt	Yes or N/A as required
	Field Off Request	N/A
	Removal Timeout	Zero

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

B.4. Declined

The kernel has determined that the transaction is declined, either through offline processing or after reactivation following an online response.

Outcome	Outcome Parameter	Value
Declined	Start	N/A
	Online Response Data	N/A
	CVM	N/A
	UI Request on Outcome Present	Yes Message Identifier: '07' (Not Authorized) Status: Card Read Successfully [Value Qualifier: Balance] [Value: Offline Balance (from Tag 'D1')] [Currency Code: Transaction Currency Code] Note: Balance is displayed only if 'D1' is returned by card
	UI Request on Restart Present	No
	Data Record Present	Yes The minimum data requirements for declined transactions are specified in Annex B.10.
	Discretionary Data Present	No
	Alternate Interface Preference	N/A
	Receipt	Yes or N/A as required
	Field Off Request	N/A
	Removal Timeout	Zero

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

B.5. Try Another Interface

The kernel (or Entry Point) has determined that the transaction cannot be completed over the contactless interface and another interface such as contact chip or mag-stripe should be attempted.

Outcome	Outcome Parameter	Value
Try Another Interface	Start	N/A
	Online Response Data	N/A
	CVM	N/A
	UI Request on Outcome Present	Yes Message Identifier: '18' (Please insert or swipe card) Status: Ready to Read
	UI Request on Restart Present	No
	Data Record Present	No
	Discretionary Data Present	Yes or No
	Alternate Interface Preference	Contact Chip or Mag-Stripe
	Receipt	N/A
	Field Off Request	N/A
	Removal Timeout	Zero

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

B.6. End Application

Outcome	Outcome Parameter	Value
End Application (for Termination of First presentment or following an Online Request with 'Two presentment' or unrecoverable error)	Start	N/A
	Online Response Data	N/A
	CVM	N/A
	UI Request on Outcome Present	No
	UI Request on Restart Present	No
	Data Record Present	No
	Discretionary Data Present	No
	Alternate Interface Preference	N/A
	Receipt	N/A
	Field Off Request	N/A
	Removal Timeout	Zero

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

B.7. End Application (for Processing Error)

Outcome	Outcome Parameter	Value
End Application (for Processing Error: Conditions for use of contactless not satisfied)	Start	N/A
	Online Response Data	N/A
	CVM	N/A
	UI Request on Outcome Present	Yes Message Identifier:'1C' (Insert, swipe or try another card) Status: Processing Error
	UI Request on Restart Present	No
	Data Record Present	No
	Discretionary Data Present	No
	Alternate Interface Preference	N/A
	Receipt	N/A
	Field Off Request	N/A
	Removal Timeout	Zero

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

B.8. Try Again (Entry of a Confirmation Code on Mobile)

Outcome	Outcome Parameter	Value
End Application (for Processing Error: Conditions for use of contactless not satisfied)	Start	B
	Online Response Data	N/A
	CVM	N/A
	UI Request on Outcome Present	Yes Message Identifier:‘20’ (See Phone for Instructions) Status: Processing Error Hold Time: 13
	UI Request on Restart Present	Yes Status: Ready to Read
	Data Record Present	No
	Discretionary Data Present	No
	Alternate Interface Preference	N/A
	Receipt	N/A
	Field Off Request	13
	Removal Timeout	Zero

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

B.9. Select Next

The kernel has determined that the selected combination is unsuitable and the next combination (if any) should be tried. In practice, this is handled directly by Entry Point and only the UI Request parameter settings are relevant.

Outcome	Outcome Parameter	Value
Select Next	Start	C
	Online Response Data	N/A
	CVM	N/A
	UI Request on Outcome Present	No
	UI Request on Restart Present	No
	Data Record Present	No
	Discretionary Data Present	No
	Alternate Interface Preference	N/A
	Receipt	N/A
	Field Off Request	N/A
	Removal Timeout	Zero

B.10. Data Record Outcome Parameter

This section describes the minimum data elements to be present in the Data record Outcome parameter depending on the Transaction Mode (i.e., EMV Mode, MS Mode or Legacy MS Mode) and the Transaction Outcome (Approved, Online request or Declined). Depending on the outcome, the Kernel will make appropriate data records available to enable the clearing and/or authorization of the transaction.

In

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Table 4-8, data elements mentioned as ‘M’ are mandatory elements that need to be present in the data record for the given Transaction Mode and Outcome and data elements mentioned as ‘C’ are conditional elements that need to be present if they are provided by the Card or POS or Kernel.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Table 4-8: Minimum Data Elements Returned in Transaction Data Record Outcome Parameter

Date Element	Tag	Source	Approved & Online request (EMV Mode)	Online request MS Mode & Legacy MS Mode	Declined (All Transactions)
Amount, Authorized	'9F02'	POS	M	M	M
Amount, Other	'9F03'	POS	C	C	C
Application Cryptogram (AC)	'9F26'	Card	M	-	-
Application Identifier (AID)	'9F06'	POS	C	-	-
Application Interchange Profile (AIP)	'82'	Card	M	-	-
Application PAN Sequence Number	'5F34'	Card	C	-	-
Application Transaction Counter (ATC)	'9F36'	Card	M	-	-
Application Usage Control	'9F07'	Card	C	-	-
Cardholder Name	'5F20'	Card	C	-	-
Cryptogram Information Data	'9F27'	Card	C	-	-
Dedicated File Name	'84'	Card	C	-	-
Issuer Application Data (IAD)	'9F10'	Card	M	-	-
Terminal Application Version Number	'9F09'	POS	C	-	-
Terminal Capabilities	'9F33'	POS	M	M	M

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Date Element	Tag	Source	Approved & Online request (EMV Mode)	Online request MS Mode & Legacy MS Mode	Declined (All Transactions)
Terminal Country Code	'9F1A'	POS	M	M	M
Terminal Type	'9F35'	POS	M	M	M
Terminal Verification Results (TVR)	'95'	Kernel 6	M	-	-
Track 1 Discretionary Data	'9F1F'	Card	C	-	-
Track 1/2 Data		Card	-	M	-
Track 2 Equivalent Data	'57'	Card	C	-	-
Transaction Date	'9A'	POS	M	M	M
Transaction Type	'9C'	POS	M	M	M
Unpredictable Number	'9F37'	POS	M	-	-

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Annex C Terminal Configuration: Data Elements

This section describes the parameters to be set in the Terminal for each available combination (i.e., offline only, online only, and offline / online capable) based on the following definitions:

- **Mandatory:** Always required,
- **Conditional:** Dependent on the configuration, or
- **Optional:** May be present.

C.1. Offline Only Terminals

The following table lists data elements that must be present in Terminals that are offline capable only.

Table 4-9: Offline Only Terminals

Data Element	Tag	Presence
Amount, Authorized	‘9F02’	Mandatory
Amount, Other	‘9F03’	Conditional
Application Identifier	‘9F06’	Mandatory
Application Version Number	‘9F09’	Mandatory
Certificate Authority Public Key Checksum	Proprietary	Mandatory
Certificate Authority Public Key Exponent	Proprietary	Mandatory
Certificate Authority Public Key Index	’9F22’	Mandatory
Certificate Authority Public Key Modulus	Proprietary	Mandatory
Extended Selection Support flag	Proprietary	Optional
Interface Device (IFD) Serial Number	‘9F1E’	Mandatory
Merchant Category Code	‘9F15’	Optional
Reader Contactless CVM limit	Proprietary	Conditional
Reader Contactless Floor limit	Proprietary	Optional
Reader Contactless Transaction limit	Proprietary	Optional
Status Check Support flag	Proprietary	Optional
Terminal Country Code	‘9F1A’	Mandatory
Terminal Floor Limit	‘9F1B’	Optional
Terminal Transaction Qualifier	‘9F66’	Mandatory
Transaction Currency Code	‘5F2A’	Mandatory
Transaction Date	‘9A’	Mandatory

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Data Element	Tag	Presence
Transaction Status Information	‘9B’	Mandatory
Transaction Type	‘9C’	Mandatory
Transaction Verification Results	‘95’	Mandatory
Unpredictable Number	‘9F37’	Mandatory
Value Added Tax 1	‘DF71’	Optional
Value Added Tax 2	‘DF72’	Optional
Zero Amount Allowed flag	Proprietary	Optional

C.2. Online Only Terminals

The following table lists data elements that must be present in Terminals that are online capable only.

Table 4-10: Online Only Terminals

Data Element	Tag	Presence
Amount, Authorized	‘9F02’	Mandatory
Amount, Other	‘9F03’	Conditional
Application Identifier	‘9F06’	Mandatory
Application Version Number	‘9F09’	Mandatory
Certificate Authority Public Key Checksum	Proprietary	Not present
Certificate Authority Public Key Exponent	Proprietary	Not present
Certificate Authority Public Key Index	’9F22’	Not present
Certificate Authority Public Key Modulus	Proprietary	Not present
Extended Selection Support flag	Proprietary	Optional
Interface Device (IFD) Serial Number	‘9F1E’	Mandatory
Merchant Category Code	‘9F15’	Optional
Reader Contactless CVM limit	Proprietary	Conditional
Reader Contactless Floor limit	Proprietary	Optional
Reader Contactless Transaction limit	Proprietary	Optional
Status Check Support flag	Proprietary	Optional
Terminal Country Code	‘9F1A’	Mandatory
Terminal Floor Limit	‘9F1B’	Optional
Terminal Transaction Qualifier	‘9F66’	Mandatory
Transaction Currency Code	‘5F2A’	Mandatory
Transaction Date	‘9A’	Mandatory

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Data Element	Tag	Presence
Transaction Status Information	'9B'	Mandatory
Transaction Type	'9C'	Mandatory
Transaction Verification Result	'95'	Mandatory
Unpredictable Number	'9F37'	Mandatory
Value Added Tax 1	'DF71'	Optional
Value Added Tax 2	'DF72'	Optional
Zero Amount Allowed flag	Proprietary	Optional

C.3. Offline / Online Terminals

The following table lists data elements that must be present in Terminals that are offline and online capable.

Table 4-11: Online and Offline Terminals

Data Element	Tag	Presence
Amount, Authorized	'9F02'	Mandatory
Amount, Other	'9F03'	Conditional
Application Identifier	'9F06'	Mandatory
Application Version Number	'9F09'	Mandatory
Certificate Authority Public Key Checksum	Proprietary	Mandatory
Certificate Authority Public Key Exponent	Proprietary	Mandatory
Certificate Authority Public Key Index	'9F22'	Mandatory
Certificate Authority Public Key Modulus	Proprietary	Mandatory
Extended Selection Support flag	Proprietary	Optional
Interface Device (IFD) Serial Number	'9F1E'	Mandatory
Merchant Category Code	'9F15'	Optional
Reader Contactless CVM limit	Proprietary	Conditional
Reader Contactless Floor limit	Proprietary	Optional
Reader Contactless Transaction limit	Proprietary	Optional
Status Check Support flag	Proprietary	Optional
Terminal Country Code	'9F1A'	Mandatory
Terminal Floor Limit	'9F1B'	Optional
Terminal Transaction Qualifiers	'9F66'	Mandatory
Transaction Currency Code	'5F2A'	Mandatory
Transaction Date	'9A'	Mandatory

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Data Element	Tag	Presence
Transaction Status Information	'9B'	Mandatory
Transaction Type	'9C'	Mandatory
Transaction Verification Results	'95'	Mandatory
Unpredictable Number	'9F37'	Mandatory
Value Added Tax 1	'DF71'	Optional
Value Added Tax 2	'DF72'	Optional
Zero Amount Allowed flag	Proprietary	Optional

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Annex D Data Elements Dictionary

This section focuses on the data elements required for the Kernel 6 Card application.

General Note: Reserved for Future Use

If a bit is specified as Reserved for Future Use (RFU), it must be:

- Set as specified or to 0 if no indication is provided or ignored, unless explicitly stated otherwise, and
- Excluded from any data field whose value is dependent on multiple bytes or bits.

D.1. Card Processing Requirements (tag '9F71')

This is a Contactless Kernel 6 application proprietary data element used by the card to communicate the card processing requirements for the transaction and the card capabilities to the reader.

Format: Binary, 2 bytes

Table 4-12: Card Processing Requirement (CPR) Encoding

BYTE 1: Transient Data		
Bit	**Value**	**Meaning**
b8	1	Online PIN required
b7	1	Signature required
b6	1	RFU
b5	1	Consumer Device CVM Performed
b4	0	RFU
b3	0	RFU
b2	0	RFU
b1	0	RFU
BYTE 2: Permanent Data		
Bit	**Value**	**Meaning**
b8	1	Switch other interface if unable to process online
b7	1	Process online if CDA failed
b6	1	Decline/switch to other interface if CDA failed

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

b5	1	Issuer Update Processing supported
b4	1	Process online if card expired
b3	1	Decline if card expired
b2	1	CVM Fallback to Signature allowed
b1	1	CVM Fallback to No CVM allowed

D.2. Cryptogram Information Data (CID, tag '9F27')

The CID indicates the type of cryptogram (TC, ARQC, or AAC) returned by the card and the actions to be performed by the reader.

Format: Binary, 1 byte

Table 4-13: Cryptogram Information Data (CID) Encoding

BYTE 1		
Bit	**Value**	**Meaning**
b8-7	XX	00 = AAC 01 = TC 10 = ARQC 11 = RFU
b6-5	00	00 = Payment System-specific cryptogram
b4	0	0 = No advice required 1 = Advice required
b3-1	000	No information given

D.3. Cryptogram Version Number (CVN)

Cryptogram version number indicates the version of the algorithm used by the card to generate an Application Cryptogram (TC, ARQC, or AAC). The value of CVN is sent to the Issuer as part of the Issuer Application Data. The card that supports Kernel 6 can have may be:

- '15'. CVN 15 is the default CVN and indicates that Issuer Application Data is included in the cryptogram generation, or
- '16'. CVN 16 is available as an option in the Contactless Application Configuration Options (CL-ACO). It indicates that the CVR is included in the cryptogram generation.

Format: Binary, 1 byte

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

D.4. Contactless Card Verification Results (tag '9F53')

This Contactless Kernel 6 application proprietary data element is used to inform the Issuer about the transaction context, the card decision, and the exceptions conditions that occurred during the current and previous transactions.

The Contactless CVR is used with Card Risk Management-Card Action Codes (CRM-CACs) and Card Verification Method-Card Action Code (CVM-CACs) during Card Action Analysis. This data element allows the Contactless application to determine the acceptable risk for processing the:

- Transaction over the contactless interface,
- Transaction offline, or
- Transaction with no cardholder verification.

The Contactless CVR is transmitted to the Issuer as part of Issuer Application Data (tag '9F10').

Format: Binary, 8 bytes

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Table 4-14: Contactless Card Verification Results (CL CVR) Encoding

BYTE 1: Information for Issuer (Card Decision)		
Bit	**Value**	**Meaning**
b8	1	Online PIN Required
b7	1	Signature Required
b6-5	XX	00 = AAC 01 = TC 10 = ARQC 11 = RFU
b4	1	RFU
b3-1	XXX	Script Counter indicating the number of the script processed during previous contact or contactless transaction
BYTE 2: Compared with CRM-CAC and CVM-CAC		
Bit	**Value**	**Meaning**
b8	1	Online cryptogram required (if not required, then reader is offline-capable and supports CDA)
b7	1	Transaction Type required to be processed online with online PIN CVM (e.g., purchase with cash-back, prepaid top-up, etc.)
b6	1	Transaction Type required to be processed offline without any CVM (e.g., refund transaction, prepaid, ticketing, offline balance inquiry, etc.)
b5	1	Domestic Transaction (based on Contactless-ACO setting)
b4	1	International Transaction
b3	1	PIN Try Limit exceeded (Dual-Interface implementation only)
b2	1	Confirmation Code Verification performed
b1	1	Confirmation Code Verification performed and failed

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

BYTE 3: CVM Related Actions		
Bit	**Value**	**Meaning**
b8	1	CVM Required
b7	0	RFU
b6	1	Consecutive CVM Transaction limit 1 exceeded (CVM-Cons 1)
b5	1	Consecutive CVM Transaction limit 2 exceeded (CVM-Cons 2)
b4	1	Cumulative CVM Transaction Amount limit 1 exceeded (CVM-Cum 1)
b3	1	Cumulative CVM Transaction Amount limit 2 exceeded (CVM-Cum 2)
b2	1	CVM Single Transaction Amount limit 1 exceeded (CVM-STA 1)
b1	1	CVM Single Transaction Amount limit 2 exceeded (CVM-STA 2)
BYTE 4: CRM Related Actions		
Bit	**Value**	**Meaning**
b8	1	CDA failed during previous contactless transaction
b7	1	Last contactless transaction not completed
b6	1	'Go on-line next transaction' was set by contact or contactless application
b5	1	Issuer Authentication failed during previous contact or contactless transaction
b4	1	Script failed on previous contact or contactless transaction
b3	1	Invalid PDOL check
b2	1	PDOL forced online (during GPO)
b1	1	PDOL forced decline (during GPO)
BYTE 5: CRM Related Actions		
Bit	**Value**	**Meaning**
b8	1	Consecutive Contactless Transaction limit exceeded (CL-Cons)
b7	1	Cumulative Contactless Transaction limit exceeded (CL-Cum)
b6	1	Single Contactless Transaction Amount limit exceeded (CL-STA)
b5	1	Lower Consecutive Offline Transaction limit exceeded (LCOL)
b4	1	Upper Consecutive Offline Transaction limit exceeded (UCOL)
b3	1	Lower Cumulative Offline Transaction Amount limit exceeded (LCOA)
b2	1	Upper Cumulative Offline Transaction Amount limit exceeded (UCOA)
b1	1	Single Transaction Amount limit exceeded (STA)

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

BYTE 6: Information for Issuer		
Bit	**Value**	**Meaning**
b8-5	XXXX	ID of PDOL-Decline or PDOL-Online check that forced the transaction to be declined or to go online (Only valid if CL -CVR B4b1 or B4b2 is set)
b4-1	XXXX	Transaction profile identifier (0000 by default)
BYTE 7: TTQ information for Issuer		
Bit	**Value**	**Meaning**
b8	1	Contact chip supported
b7	1	Offline-only reader
b6	1	Online PIN supported
b5	1	Signature supported
b4	1	Issuer Update Processing supported
b3	0	RFU
b2	0	RFU
b1	0	RFU
BYTE 8: RFU		
Bit	**Value**	**Meaning**
b8-1	'XX'	RFU

D.5. Contactless-Application Configuration Options (CL-ACO) tag 'C0'

The Contactless-Application Configuration Options (CL-ACO) is a proprietary data element that contains a list of the card supported functions and the Application Interchange Profile (AIP).

This data element provides the Issuer with the option to:

- Select cryptographic options,
- Configure access rights, and
- Activate or de-activate functions in the application.

Format: Binary, 2 bytes

Table 4-15: Contactless Application Configuration Options (CL-ACO) Encoding

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

BYTE 1		
Bit	**Value**	**Meaning**
b8	1	MS Mode is the preferred contactless mode using EMV Mode
b7	1	DCVV supported
b6	1	PTC checking not supported (Dual-Interface implementation only)[1]
b5	1	Confirmation Code supported (Mobile implementation only)
b4	1	Prepaid Product
b3	0	RFU
b2	1	Transaction Logging supported: Log all transactions
b1	1	Domestic transaction ('1' based on Country Code, '0' based on Currency Code)
BYTE 2		
Bit	**Value**	**Meaning**
b8	1	AFL inclusion for online transaction
b7	1	CVN for Application Cryptogram: where: '0' = CVN set to 15 (Include Issuer Application Data in data input for Application Cryptogram) '1' = CVN set to 16 (Include only CVR in data input for Application Cryptogram)
b6	1	Use of Issuer Discretionary Data (IDD)/ Issuer Application Data Object List (IADOL) in Issuer Application Data
b5	1	Enable Issuer Defined Data Tags (IDDT)
b4	1	Activate / Enable all predefined PDOL Checks
b3	1	Mobile Only: Passcode Verification required for non-matching currency[1] 0 = Do not verify, 1 = Always verify
b2	1	GET DATA only after GPO
b1	1	Separate Key pair used for CDA computation over contactless interface

[1]: If set to 1, Passcode Verification must be performed if the transaction Currency Code does not match the CRM Currency Code or one of the Secondary Currency Codes.

D.6. Extended Selection Support Flag

This is an optional internal data.

Format: Terminal vendor specific

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

D.7. Offline Balance

This is a Kernel 6 proprietary data element specifying the remaining amount of offline spending available for the application/transaction profile. The value of Offline Balance may be obtained from the application using the GET DATA command, if allowed by the card configuration: Offline balance = UCOA – COA. If the Offline balance cannot be calculated or is a negative value, then the card shall return a value of '0'.

Format: Numeric, 6 bytes.

D.8. Reader Contactless CVM Limit

This data sets the CVM limit for a particular Combination based on the amount of the transaction. If the amount of the transactions is greater than or equal to this limit, the terminal will ask the card to perform Cardholder Verification.

Format: Numeric, 6 bytes.

D.9. Reader Contactless Floor Limit

This data sets the floor limit for a particular Combination. If the amount of the transactions is greater than this limit, the terminal will send the transaction online for processing.

Format: Numeric, 6 bytes.

D.10. Reader Contactless Transaction Limit

This data sets the reader transaction limit for a particular Combination. If the amount of the transactions is greater than or equal to this limit, the terminal will not process the transaction and inform the merchant to use a contact interface.

Format: Numeric, 6 bytes.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

D.11. Terminal Transaction Qualifier (TTQ, tag '9F66')

Terminal Transaction Qualifiers (TTQs) are online and CVM processing options that may be supported by the Terminal during Entry Point processing. Detailed definitions of TTQs are provided in Table 4-16.

Format: Binary, 4 bytes (as specified in (EMV BOOK B)

Table 4-16: Terminal Transaction Qualifiers (TTQ) Encoding

BYTE 1: Reader Capabilities		
Bit	**Name**	**Meaning**
b8	Mag stripe mode supported	0 = Not supported, 1 = Supported
b7	0	RFU
b6	EMV mode supported	0 = Not supported, 1 = Supported
b5	EMV contact chip supported[1]	0 = Not supported, 1 = Supported
b4	Offline-only Contactless Reader	0 = Online capable, 1 = Offline Only
b3	Online PIN supported	0 = Not supported, 1 = Supported
b2	Signature supported	0 = Not supported, 1 = Supported
b1	0	RFU Note: Readers compliant with [EMV CTL: BOOK B, v2.1] must set TTQ B1b1 to '0'.
BYTE 2: Reader CVM Requirements		
Bit	**Value**	**Meaning**
b8	Online cryptogram required[2]	0 = Not required, 1 = Required
b7	CVM required[2]	0 = Not required, 1 = Required
b6	(Contact Chip) Offline PIN supported[1]	0 = Not supported, 1 = Supported
b5	0	RFU
b4	0	RFU
b3	0	RFU
b2	0	RFU
b1	0	RFU

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

BYTE 3: Reader Additional Capabilities		
Bit	**Value**	**Meaning**
b8	Issuer Update Processing supported	0 = Not supported, 1 = Supported
b7	Consumer Device CVM supported	0 = Not supported, 1 = Supported
b6	0	RFU
b5	0	RFU
b4	Consumer Device CVM required	0 = Not supported, 1 = Supported
b3	0	RFU
b2	0	RFU
b1	0	RFU
Byte 4		
Bit	**Value**	**Meaning**
b8	1	RFU
b7	1	RFU
b6	1	RFU
b5	1	RFU
b4	1	RFU
b3	1	RFU
b2	1	RFU
b1	1	RFU

[1] This bit shall be set to '1' if the Terminal has a contact interface. Otherwise, it shall be set to '0' if the Terminal is a contactless only Terminal.

[2] This bit is set dynamically based on the pre-processing result.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

D.12. Terminal Verification Result (TVR, tag '95')

The TVR is a bitmap that shows the result of some functions processed by the Terminal. The Terminal Verification Result is coded according to Annex C5 of [EMV Book 2].

Format: Binary, 5 bytes.

Table 4-17: Terminal Verification Result (TVR) Encoding

BYTE 1								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	-	-	-	-	-	-	-	Offline data authentication was not performed
-	1	-	-	-	-	-	-	SDA Failed[1]
-	-	1	-	-	-	-	-	ICC Data missing
-	-	-	1	-	-	-	-	Card appears on Terminal exception file
-	-	-	-	1	-	-	-	DDA failed[1]
-	-	-	-	-	1	-	-	CDA failed
-	-	-	-	-	-	0	-	RFU
-	-	-	-	-	-	-	0	RFU
BYTE 2								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	-	-	-	-	-	-	-	ICC and Terminal have different application versions
-	1	-	-	-	-	-	-	Expired application
-	-	1	-	-	-	-	-	Application not yet effective
-	-	-	1	-	-	-	-	Requested service not allowed for card product
-	-	-	-	1	-	-	-	New card
-	-	-	-	-	0	-	-	RFU
-	-	-	-	-	-	0	-	RFU
-	-	-	-	-	-	-	0	RFU

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

BYTE 3								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	-	-	-	-	-	-	-	Cardholder verification was not successful
-	1	-	-	-	-	-	-	Unrecognized CVM
-	-	1	-	-	-	-	-	PIN Try Limit exceeded
-	-	-	1	-	-	-	-	PIN entry required and PIN pad not present or not working[1]
-	-	-	-	1	-	-	-	PIN entry required, PIN pad present, but PIN was not entered[1]
-	-	-	-	-	1	-	-	Online PIN entered
-	-	-	-	-	-	0	-	RFU
-	-	-	-	-	-	-	0	RFU
BYTE 4								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	-	-	-	-	-	-	-	Transaction exceeds floor limit
-	1	-	-	-	-	-	-	Lower Consecutive offline limit exceeded[1]
-	-	1	-	-	-	-	-	Upper Consecutive offline limit exceeded[1]
-	-	-	1	-	-	-	-	Transaction selected randomly for online processing
-	-	-	-	1	-	-	-	Merchant forced transaction online[1]
-	-	-	-	-	0	-	-	RFU
-	-	-	-	-	-	0	-	RFU
-	-	-	-	-	-	-	0	RFU

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

BYTE 5								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	-	-	-	-	-	-	-	Default TDOL used[1]
-	1	-	-	-	-	-	-	Issuer Authentication failed
-	-	1	-	-	-	-	-	Script processing failed before final GENERATE AC[1]
-	-	-	1	-	-	-	-	Script processing failed after final GENERATE AC[1]
-	-	-	-	0	-	-	-	RFU
-	-	-	-	-	0	-	-	RFU
-	-	-	-	-	-	0	-	RFU
-	-	-	-	-	-	-	0	RFU

Note [1]: These bits are only present for compatibility with contact TVR and should be set to '0' or ignored by Issuer.

D.13. Transaction Certificate (TC)

This data may be returned by the card in response to the GET PROCESSING OPTIONS command, when the card approves the transaction offline. The value is part of Signed Dynamic Application Data (SDAD). For more information, refer to [EMV Book 3 and 4].

Format: Binary, 8 bytes.

D.14. Transaction Status Information (TSI, tag '9B')

This data indicates which operation(s) have been performed during the current transaction. For more information, refer to [EMV Book 3].

Format: Binary, 2 bytes.

D.15. Zero Amount Allowed Flag

This is an optional internal data.

Format: Terminal vendor specific

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

[This page is intentionally left blank.]

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.

Annex E Track Data for MS Mode and Legacy MS Mode Transactions

The card returns both Track 1 Data and Track 2 Data to the reader in response to the READ RECORD command for MS Mode and Legacy MS Mode transactions. If the DCVV functionality is enabled in the card, the card returns DCVV in the READ RECORD response data. If no DCVV data is received, the Track 1 and Track 2 data is not altered by the Kernel.

If the DCVV functionality is enabled, then Track 1 and Track 2 need to contain the DCVV and UN. The Kernel shall update Track 1 and Track 2 with UN and DCVV values as described in Sections E.1 and E.2.

E.1. Track 1 Data with DCVV

With ‘Start Sentinel’ being in position 1 of Track 1, the Kernel shall:

- Insert 3 digit numeric DCVV data received in READ RECORD response in positions 59-61.
- Insert 2 digit numeric UN data from the terminal generated UN sent in PDOL to card (least significant digits of the UN) in positions 65-66.

E.1. Track 2 Data with DCVV

With ‘Start Sentinel’ being in position 1 of Track 2, the Kernel shall:

- Insert 3 digit numeric DCVV data received in READ RECORD response in positions 31-33.
- Insert 2 digit numeric UN data from the terminal generated UN sent in PDOL to card (least significant digits of the UN) in positions 37-38.

© 2011-2016 EMVCo, LLC. All rights reserved. Reproduction, distribution and other use of this document is permitted only pursuant to the EMVCo Terms of Use agreement found at www.emvco.com, as supplemented by the Legal Notice on Page ii of this document, or such other separate agreement that the user may have with EMVCo or the applicable payment system. EMV® is a registered trademark or trademark of EMVCo, LLC in the United States and other countries.