EMV®*
ContactlessSpecifications for Payment Systems

Book C-1

Kernel 1 Specification

Version 2.6
February 2016

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.

Contents

Figures

Tables

Requirements

1 Introduction

This chapter contains information that helps the reader understand and use this specification.

1.1 Scope

This document, the *EMV ContactlessSpecifications for Payment Systems, Kernel 1 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.

1.3 Volumes of the Contactless Specifications

This specification is part of a ten-volume set:

Book A: Architecture and General Requirements

Book B: Entry Point Specification

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*Specification

1.4 Reference Materials

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.

[EMV 4.3] *EMV Integrated Circuit Card Specifications for Payment Systems*, Version 4.3, November 2011, including:

- *[EMV 4.3 Book 1]* *EMV Integrated Circuit Card Specifications for Payment Systems*, Book 1, Application Independent ICC to Terminal Interface Requirements
- *[EMV 4.3 Book 2]* *EMV Integrated Circuit Card Specifications for Payment Systems*, Book 2, Security and Key Management
- *[EMV 4.3 Book 3]* *EMV Integrated Circuit Card Specifications for Payment Systems*, Book 3, Application Specification
- *[EMV 4.3 Book 4]* *EMV Integrated Circuit Card Specifications for Payment Systems*, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements

1.5 Overview

This volume includes the following chapters and annexes:

Chapter 1contains general information that helps the reader understand and use this specification.

Chapter 2provides an overview of the Kernel 1 approach.

Chapter 3 specifies transaction processing for Kernel 1.

Annex Adefines Kernel 1 data elements and lists data elements that are mandatory for Kernel 1 processing, those required for offline approved transactions, and those required for online requested transactions.

Annex B is a glossary of terms and abbreviations used in this specification.

2 Overview of the Kernel 1 Approach

The Kernel 1 approach supports both offline and online transactions.

- Offline transactions use fDDA for offline authentication. From the card perspective, this is regular EMV DDA.The reader completes the signature verification process after the card has left the field. Mag-stripe data is delivered for the clearing records.
- Online transactions use regular EMV based cryptogram generation and deliver chip data for the online authorisation request and for clearing records.

For online transactions, Kernel 1 provides CVM support using the EMV CVM List approach including the options: No CVM, Signature, and Online PIN. Offline transactions do not require CVM. Offline PIN is not supported.

Before Kernel 1 can process transactions, configuration parameters must be set relating to the reader/terminal capabilities, acceptance environment, and AID selected.

For online only environments or for cross border transactions, all transactions are processed online.

For offline capable environments, the choice between offline or online processing is determined by a reader risk management process that includes the Entry Point checking of floor limits and thepresence or absence of data from the card:

- If the VLP Issuer Authorisation Code is present in the records read by the reader and no floor limit is exceeded, then the processing is done offline.
- If the VLP Issuer Authorisation Code is absent or at least one floor limit is exceeded,then the processing is done online.

2.1 Online or Offline Transactions and CVM

The decision as to whether a transaction is conducted online or offline and with or without a CVM depends on a hierarchy of the three transaction amount limits defined in *Book B: Entry PointSpecification*:

- Reader Contactless Transaction Limit, which is greater than:
- Reader CVM Required Limit, which is greater than:
- Reader Contactless Floor Limit

Transactions with an amount greater than or equal to the Reader Contactless Transaction Limit will not be conducted over the contactless interface. This decision is handled by Entry Point, not Kernel 1.

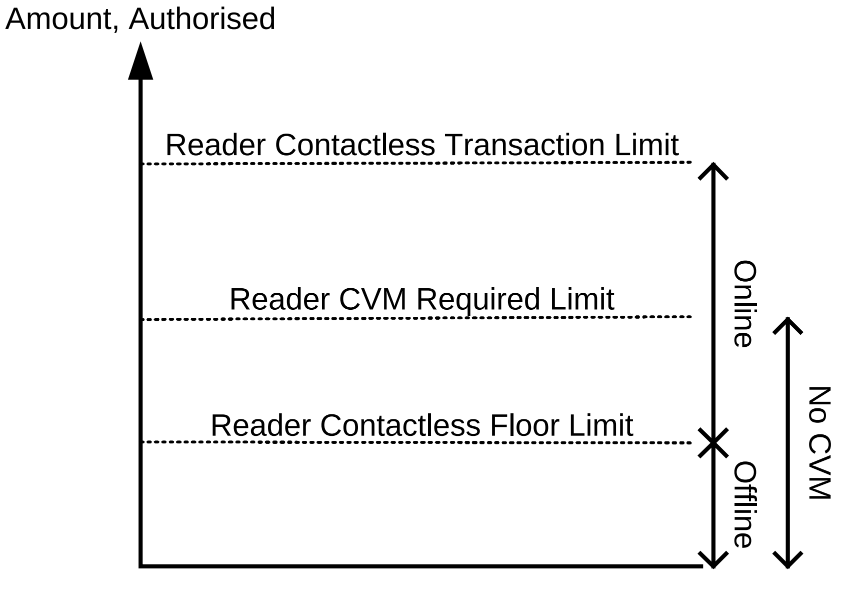
For transactions with an amount greater than or equal to the Reader CVM Required Limit (but no greater than the Reader Contactless Transaction limit), the kernel will request a CVM with an ***Online Request*** Outcome. The CVM may be online PIN or signature.

Transactions with an amount greater than the Reader Contactless Floor Limit (but no greater than the Reader CVM Required Limit) will be conducted online, without a CVM.

Transactions with an amount no greater than the Reader Contactless Floor Limit will be conducted offline. These transactions do not require a CVM.

Figure 2-1 shows the hierarchy.

Figure 2-1: Online, Offline,and CVM TransactionLimit Hierarchy


Amount, Authorised
Reader Contactless Transaction Limit
Online
Reader CVM Required Limit
No CVM
Reader Contactless Floor Limit
Offline

2.2 High Level Transaction Flow

Kernel 1 transactions follow a simplified EMV transaction flow truncated after the first GENERATE AC command. The main difference between the offline and online transactions is that for offline transactions the first GENERATE AC isnot performed, whilst for online transactions, INTERNAL AUTHENTICATEis not performed.

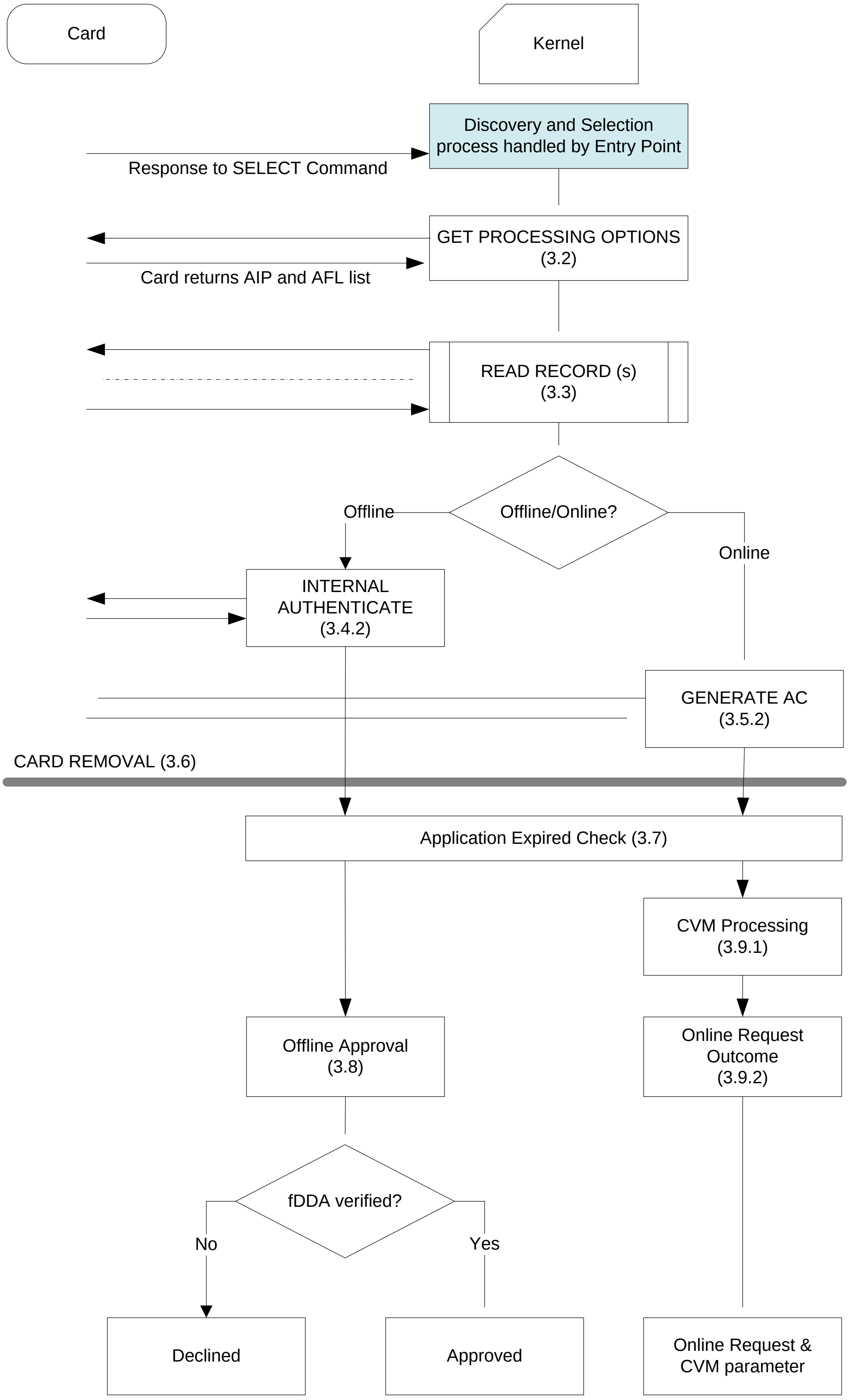
Kernel 1 uses the EMV commands listed in Table 2-1.

Table 2-1: EMV Commands

EMV Commands	Offline	Online
Application Selection	✓	✓
GET PROCESSING OPTIONS	✓	✓
READ RECORD	✓	✓
INTERNAL AUTHENTICATE	✓	–
GENERATE AC	–	✓

Figure 2-2illustrates the high level transaction flow. The numbers in parenthesis indicate the section detailing the requirements.

Figure 2-2: High-Level Transaction Flow


Card
Kernel
Discovery and Selection process handled by Entry Point
Response to SELECT Command
GET PROCESSING OPTIONS (3.2)
Card returns AIP and AFL list
READ RECORD (s) (3.3)
Offline
Offline/Online?
Online
INTERNAL AUTHENTICATE (3.4.2)
GENERATE AC (3.5.2)
CARD REMOVAL (3.6)
Application Expired Check (3.7)
CVM Processing (3.9.1)
Offline Approval (3.8)
Online Request Outcome (3.9.2)
fDDA verified?
No
Yes
Declined
Approved
Online Request & CVM parameter

2.3 Transaction Processing

This section outlines Kernel 1 transaction processing.

When started by Entry Point, the kernel uses the PDOL returned in the SELECT response to construct the command data for a GPOcommand. The VLP Terminal Support Indicator value is used to indicate the reader/kernels online preference.

Using the AFL returned in the GPO response, the kernel reads the indicated records. Cards using Kernel 1 will return different AFLs for online and offline transactions and thus the kernel will only read data appropriate for the expected processing.

At this point the kernel has the necessary reader and card data to choose whether the remaining processing will be offline or online.

If the result is for offline processing, the kernel will use the DDOL from the records to construct and send an INTERNAL AUTHENTICATE command. Otherwise the result is for online and the kernel will use the CDOL1 from the records to construct and send a GENERATE AC command.

Once the response from either command has been received, the kernel indicates to the cardholder that the card can be removed from the field. The kernel then checks that the application has not expired.

For offline transactions, the kernel recovers the ICC Public Key via the ICC Certificate and Issuer Certificate obtained from the records and uses it to verify the signature returned in the INTERNAL AUTHENTICATE response. The result determines the Outcome to be either ***Approved*** or ***End Application***.

Otherwise, for online transactions, the kernel evaluates the need for CVM processing and indicates any required CVM in the ***Online Request*** Outcome.

3 Detailed Transaction Processing

This chapter provides detailed transaction processing requirements for Kernel 1 including information related to EMV functions.

3.1 Configuration and Transaction Parameters

Table 3-1 lists the configuration and transaction data elements and flags that must be availablebefore Kernel 1 processing can start.

A data elementor flag may be set:

- per reader (e.g. Terminal Country Code), or
- variable per the AID selected to run on Kernel 1 (e.g. CVM Capabilities), or
- dynamic per transaction (e.g. Amount, Authorised and Unpredictable Number).

Table 3-1: Initial ConfigurationParameters

Parameter	Tag	M/C/O	Description	Defined By	Varies By
Terminal Country Code	'9F1A'	M	May be requested in PDOL or CDOL1.	EMV	Reader
Transaction Currency Code	'5F2A'	M	May be requested in PDOL or CDOL1.	EMV	Reader
VLP Terminal Support Indicator	'9F7A'	C	If present: • '00' = Online only solution supported • '01' = Offline/online solution supported If absent: • Online only solution supported May be requested in PDOL	Kernel 1 See section A.1	AID
CVM Capabilities Flags: • Online PIN Support • Signature Support		C	If CVM is supported, these flags indicate support for Online PIN and/or Signature.		AID
Amount,Authorised	'9F02'	M	May be requested in CDOL1.	EMV	Transaction
Transaction Date	'9A'	M	May be requested in CDOL1.	EMV	Transaction
Transaction Type	'9C'	M	Should be '00' to indicate a purchase transaction. May be requested in CDOL1.	EMV	Transaction
Unpredictable Number	'9F37'	M	May be requested in CDOL1.	EMV	Transaction
Reader Contactless Floor Limit Exceeded[1]		M	Used in Kernel 1 processing.	Entry Point; see *Book B*	Transaction
Reader CVM Required Limit Exceeded[1]		M	Used in Kernel 1 processing.	Entry Point; see *Book B*	Transaction

[1] This is an Entry Point Pre-Processing Indicator, which is set based on configuration data for a combination using Kernel 1.

3.2 GET PROCESSING OPTIONS Command

The PDOL provided by the card in response to the SELECT command contains a list of tags that the card requests from the reader. The reader provides the card with the PDOL-related data elements when issuing the GPO command to the card.

Requirement – PDOL Processing	
3.2.1.1	The kernel shall process the PDOL and construct the command data for the GET PROCESSING OPTIONS command, taking the following requirements into account:
3.2.1.2	**If** the 'Reader Contactless Floor Limit Exceeded' indicator is 1 **and** the VLP Terminal Support Indicator is requested in the PDOL, **then**the value of the VLP Terminal Support Indicator(Tag '9F7A') in the command data shall be set to '00'. This is an indication (if submitted as PDOL data) that an online transaction is the only choice.[2]
3.2.1.3	**If** no PDOL was returned in the response to the SELECT command, **then** the kernel shall construct the command data for the GET PROCESSING OPTIONS command with a value of '8300'.

Requirement – GPO Command	
3.2.1.4	The kernel shall support the GET PROCESSING OPTIONS command and response as defined in *[EMV 4.3 Book 3]*.

The Application Interchange Profile (AIP) and Application File Locator (AFL) returned by the cards in response to the GPO command contain information on the card configuration and data records to be read. The AIP is not used by Kernel 1.

[2] Note that if the 'Reader Contactless Floor Limit Exceeded' indicator is 0, then the value of VLP Terminal Support Indicator in the command data is as configured in the reader.

3.3 READ RECORD Command

The reader uses the Application File Locator (AFL) to determine which records to request from the card. The reader does not need to process any data at this point, except to determine if the transaction should be processed online or offline. Further processing of data should be completed after the contactless card has been removed from the reader, in particular completion of offline data authentication.

Requirement – Reading Records

3.3.1.1 The kernel shall read the records indicated in the AFL using the READ RECORD command and response as defined in *[EMV 4.3 Book 3]*.

Requirement – Determination of offline/online

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

- the VLP Terminal Support Indicator indicates offline support,
- **and**the 'Reader Contactless Floor Limit Exceeded'indicator is 0,
- **and** the VLP Issuer Authorisation Code ('9F74') is present in the data read from SFI 11, Record 1,

then the kernel shall prepare to process the transaction offline (section 3.4).

Elsethe kernel shall prepare to process the transaction online (section 3.5).

3.4 Offline Processing

If the transaction is to be processed offline, the reader will request the card to return a dynamic signature by sending an INTERNAL AUTHENTICATE command with the data requested in the DDOL obtained during READ RECORDprocessing. The DDOL will normally only require the Unpredictable Number.

Validation of the signature will normally occur after the card is no longer required in the field.

3.4.1 DDOL Processing

Requirement – DDOL Processing	
3.4.1.1	The kernel shall process the DDOL, if present, and construct the command data for the INTERNAL AUTHENTICATE command.
3.4.1.2	**If** no DDOL was found in the records, **then** the kernel shall construct the command data for the INTERNAL AUTHENTICATE command using only the Unpredictable Number (Tag '9F37').

3.4.2 INTERNAL AUTHENTICATE Command

Requirement – INTERNAL AUTHENTICATE	
3.4.2.1	The kernel shall request the card to generate a signature using the INTERNAL AUTHENTICATE command and shall obtain the response as defined in *[EMV 4.3 Book 3]*.

On receipt of the response, kernel processing will continue with Card Removal (section 3.6).

3.5 Online Processing

If the transaction is to be processed online, the reader will request the card to return an Application Request Cryptogram (ARQC) by sending a GENERATE AC command with the data requested in the CDOL1 obtained during READ RECORD processing. The CDOL1 will normally require the Amount, Authorised; Amount, Other; Terminal Country Code; TVR; Transaction Currency Code; Transaction Date; Transaction Type; andUnpredictable Number. As for any DOL processing, data elements which are unknown to the reader (such as Amount, Other) will be zero filled.

Completion of online processing will normally occur after the card is no longer required in the field.

3.5.1 CDOL1 Processing

Requirement – CDOL1 Processing	
3.5.1.1	The kernel shall process the CDOL1 and construct the command data for the GENERATE AC command.The value of the Terminal Verification Results (Tag '95') in the command data shall be set to '00 00 00 00 00'.

3.5.2 GENERATE AC Command

Requirement – GENERATE AC	
3.5.2.1	The kernel shall request the card to generate an ARQC using the GENERATE APPLICATION CRYPTOGRAM command and shall obtain the response as defined in *[EMV 4.3 Book 3]*.
3.5.2.2	**If** the cryptogram returned is not an ARQC, **then** the terminal shall end the application as defined in section 3.10.3.

On receipt of the response, kernel processing will continue with Card Removal (section 3.6).

3.6 Card Removal

Once all records have been read and the signature or cryptogram has been generated, then the card is no longer required in the field and the indication is given to the cardholder that the card can be removed.

Requirement – Card Removal

3.6.1.1 The kernel shall send a User Interface Request with the following parameters:

- Message Identifier:'17' (“Card Read OK”)
- Status: Card Read Successfully

This will result in an indication to the cardholder that the card can be removed from the field.

3.7 Application Expired Check

Requirement – Application Expired Check

3.7.1.1 The kernel shall compare the Transaction Date (Tag '9A') with the Application Expiration Date (Tag '5F24').

Ifthe value of Transaction Date is greater than the value of Application Expiration Date,
then the application has expired and the kernel shall end the application as defined in section 3.10.3.

For transactions conducted offline, the kernel processing continues with Offline Approval (section 3.8) and for those conducted online, the kernel processing continues with Online Completion (section 3.9).

3.8 Offline Approval

The kernel verifies the signature returned in the INTERNAL AUTHENTICATE response and determines the Outcome and the associated parameters. Verification of the signature includes recovery of the Issuer and card public keys from the certificates contained in the data records.

Requirement – Signature Verification

3.8.1.1 The kernel shall verify the signature as defined for DDA in *[EMV 4.3 Book 2]*.

If any step of signature verification fails,
thenthe kernel shall end the application as defined in section 3.10.3.

Requirement – Offline Outcome

3.8.1.2 The kernel shall prepare the data record for an offline clearing record (section A.3) and make it available to the POS system.

Requirement – Offline Outcome

3.8.1.3 The kernel shall provide an ***Approved*** Outcome with the following parameters:

Approved:

- **Start:**N/A
- **Online Response Data:**N/A
- **CVM:** No CVM
- **UI Request on Outcome Present:** Yes
    - Message Identifier:'03' ("Approved")
- **UI Request on Restart Present:** No
- **Data Record Present:**Yes

  The minimum data requirements for EMV mode clearing records are specified in Annex A.3.
- **Discretionary Data Present:** No
- **Alternate Interface Preference:**N/A
- **Receipt:**N/A
- **Field Off Request:**N/A
- **Removal Timeout:**Zero

3.9 Online Completion

The kernel evaluates the need for CVM processing and determines the Outcome and associated parameters. The data for an online authorisation is prepared and made available to the POS system.

3.9.1 CVM Processing

If a CVM is required according to the ‘Reader CVM Required Limit Exceeded’ indicator, the kernel evaluates the CVM list contained in the data records and determines the appropriate CVM parameter setting for the Outcome. Kernel 1 CVM processing is a simplified version of CVM list processing defined in *[EMV 4.3 Book 3]* using only the CVM Code.

Requirement – CVM Required Check	
3.9.1.1	**If** the ‘Reader CVM Required Limit Exceeded’ indicator is 1, **then**the kernel shall evaluate the CVM List obtained from the data records. **Else**processing shall continue with ***Online Request*** Outcome (section 3.9.2).

Requirement – CVM Evaluation	
3.9.1.2	The kernel shall examine the CVM Codes in the CVM List (Tag '8E') in sequential order, comparing the CVM Capabilities flags (Online PIN Support and Signature Support) with the CVM Code values for ‘Enciphered PIN verified online’ and ‘Signature (paper)’, as defined in *[EMV 4.3 Book 3]*, Table 39. The first positive comparison in the list determines the CVM requirement for the transaction.
3.9.1.3	**If** no match is found in the comparison described in requirement 3.9.1.2, **then** the kernel shall end the application as defined in section 3.10.3.

3.9.2 Online Request Outcome

The Outcome is set for ***Online Request*** with the parameters indicating the CVM requirement (if any). The data for an online authorisation is made available.

Requirement – Online Request Outcome

3.9.2.1 The kernel shall prepare the data record for an online authorisation request (section A.4) and make it available to the POS system.

3.9.2.2 The kernel shall provide an ***Online Request*** Outcome with the following parameters:

Online Request:

- **Start:**N/A
- **Online Response Data:**N/A
- **CVM:** as defined in requirement 3.9.1.2
- **UI Request on Outcome Present:** No
- **UI Request on Restart Present:** No
- **Data Record Present:**Yes

  The minimum data requirements for EMV modeonline authorisation messages are specified in Annex A.4.
- **Discretionary Data Present:** No
- **Alternate Interface Preference:**N/A
- **Receipt:**N/A
- **Field Off Request:**N/A
- **Removal Timeout:**Zero

3.10 Error Handling and End Application

3.10.1 Processing Errors

Requirement – Processing Errors

3.10.1.1 **If** the status bytes returned in the response to any command are any value other than '9000',
thenthe kernel shall end the application as defined in section 3.10.3.

3.10.2 CommunicationErrors

Requirement – Communication Errors

3.10.2.1 **If** the kernel is informed of a contactless communications error,
thenthe kernel shall provide a ***Try Again*** Outcome with the following parameters:

Try Again:

- **Start:** B
- **Online Response Data:**N/A
- **CVM:**N/A
- **UI Request on Outcome Present:** Yes
  - Message Identifier:'15' (“Present Card”)
  - Status: Readyto Read
- **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

3.10.3 End Application

Requirement – End Application

3.10.3.1 The kernel shall provide an ***End Application*** Outcome with the following parameters:

End Application:

- **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

Annex A Data Elements

This annex defines the following categories of data elements:

A.1 Kernel 1 Data Elements

Table A-1: Kernel 1 Data Elements

Name (Format; Tag; Length)	Requirement	Description	Values
VLP Issuer Authorisation Code F: a T: '9F74' L: 6	Conditional If offline transaction supported	If present indicates offline approval from card	As personalised on the card by the Issuer
VLP Terminal Support Indicator F: n 1 T: '9F7A' L: 1	Conditional If offline transaction supported	If present indicates offline and/or online support. If absent indicates online only support	'00' = online only solution supported '01' = offline/online solution supported

A.2 Mandatory Data Elements for Processing

The following data elements are mandatory for Kernel 1 processing:

- Card Risk Management Data Object List 1 (CDOL1) – Tag '8C'
- Application Expiration Date – Tag '5F24'

A.3 Data Elements for Offline Approved Transactions

Table A-2 lists the minimum data elements in the data record for an offline approved transaction.

Table A-2: Minimum Data Elements for Offline Approved Transactions

Data Element Name	Tag #	M/C	Source
Track 2 Equivalent Data	'57'	M	Card
VLP Issuer Authorisation Code	'9F74'	M	Card
Cardholder Name	'5F20'	C[3]	Card
Track 1 Discretionary Data	'9F1F'	C[3]	Card

[3] If present on the card.

A.4 Data Elements for Online Requested Transactions

Table A-3 lists the minimum data elements in the data record for an online requested transaction.

Table A-3: Minimum Data Elements for Online Requested Transactions

Data Element Name	Tag #	M/C/O	Source/Value
Amount, Authorised	'9F02'	M	Entry Point (see *Book B*)
Amount, Other	'9F03'	M	Always '00 00 00 00 00 00'
Terminal Country Code	'9F1A'	M	Reader
Terminal Verification Results (TVR)	'95'	M	Always '00 00 00 00 00'
Transaction Currency Code	'5F2A'	M	Transaction
Transaction Date	'9A'	M	Transaction
Transaction Type	'9C'	M	Always '00'
Unpredictable Number (UN)	'9F37'	M	Reader (see *Book A*)
Application PAN Sequence Number	'5F34'	C[4]	Card
Application Interchange Profile (AIP)	'82'	M	Card
Application Transaction Counter (ATC)	'9F36'	M	Card
Application Cryptogram (AC)	'9F26'	M	Card
Cryptogram Information Data (CID)	'9F27'	M	Card
Issuer Application Data (IAD)	'9F10'	M	Card
Track 2 Equivalent Data	'57'	M	Card
Cardholder Name	'5F20'	C[4]	Card
Track 1 Discretionary Data	'9F1F'	O	Card

[4] If present on the card.

Annex B Glossary

This is a glossary of terms and abbreviations used in this specification. For descriptions of data elements, see Annex A.

a	Alphabetic
AAC	Application Authentication Cryptogram
AC	Application Cryptogram
Acquirer	A financial institution that signs a merchant (or disburses currency to a cardholder in a cash disbursement) and directly or indirectly enters the resulting transaction into interchange.
AFL	Application File Locator
AID	Application Identifier
AIP	Application Interchange Profile
Application Cryptogram	Cryptogram returned by the card; one of the following cryptogram types: AAC Application Authentication Cryptogram ARQC Authorisation Request Cryptogram TC Transaction Certificate
Approved	A Final Outcome
ARQC	Authorisation Request Cryptogram
ATC	Application Transaction Counter
C	Conditional
Card	As used in these specifications, a consumer device supporting contactless transactions.
Cardholder	An individual to whom a card is issued or who is authorised to use that card.

Cardholder Verification Method (CVM)

A method used to confirm the identity of a cardholder.

CDOL

Card Risk Management Data Object List

CID

Cryptogram Information Data

Combination

Any of 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)

Contactless card

See “Card”.

CVM

Cardholder Verification Method

DDA

Dynamic Data Authentication

DDOL

Dynamic Data Authentication Data Object List

Declined

A Final Outcome

DOL

Data Object List

EMV®

A global standard for credit and debit payment cards based on chip card technology. The EMV Integrated Circuit Card Specifications for Payment Systems are developed and maintained by EMVCo.

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 utilising a full chip infrastructure carrying EMV minimum data.

EMVCo EMVCo LLC is the organisation of payment systems that manages, maintains, and enhances the EMV specifications. EMVCo is currently operated by American Express, Discover, JCB, MasterCard, UnionPay and Visa.

End Application A Final Outcome

Extended Selection An option in which Entry Point appends the value indicated by the Extended Selection data element (Tag '9F29') to the ADF name in the SELECT command.

F Format

Fast DDA Leverages DDA as defined in *[EMV 4.3]* specifications. Used in EMV mode transactions to allow the reader to issue READ RECORD commands to obtain Dynamic Data Authentication (DDA) related data from the card and perform the DDA calculations after the card has left the field.

fDDA Fast DDA

Final Outcome Result provided to the reader as a result of Entry Point processing the Outcome from the kernel, or provided directly by Entry Point under exception conditions.

GPO GET PROCESSING OPTIONS command

IAD Issuer Application Data

ICC Integrated Circuit Card

Issuer A financial institution that issues contactless cards or contactless payment applications that reside in consumer devices.

Kernel	The kernel contains interface routines, security and control functions, and logicto manage a set of commands and responses to retrieve the necessary data from a card to complete a transaction. The kernel processing covers the interaction with the card between the Final Combination Selection (excluded) and the Outcome Processing (excluded).
Kernel ID	Identifier to distinguish between different kernels that may be supported by the reader.
Kernel Identifier	Identifier to distinguish between different kernels that may be indicated by the card.
L	Length
M	Mandatory
n	Numeric
N/A	Not Applicable; a possible value for several Outcome and Final Outcome parameters
O	Optional
Online PIN	A method of PIN verification where the PIN entered by the cardholder into the terminal PIN pad is encrypted and included in the online authorisation request message sent to the issuer.
Online Request	A Final Outcome
Outcome	Result from the kernel processing, provided to Entry Point, or under exception conditions, result of Entry Point processing. In either case, a primary value with a parameter set.
PAN	Primary Account Number
PDOL	Processing Options Data Object List
PICC	Proximity IC Card
PIN	Personal Identification Number
POS	Point of Sale
Reader	A component of the POS System; described in detail in *Book A*

Select Next	An Outcome
SFI	Short File Identifier
T	Tag
TC	Transaction Certificate
Terminal	A component of the POS System; described in detail in *Book A*
Transaction	The reader-card interaction between the first presentment of the card and the decision on whether the transaction is approved or declined. If the transaction is authorised online, this may involve multiple presentments of the card on the reader.
Try Again	An Outcome
Try Another Interface	A Final Outcome
TVR	Terminal Verification Results
UN	Unpredictable Number
VLP	Visa Low-Value Payment

*** END OF DOCUMENT ***