EMV®
Contactless Specifications for Payment Systems

Book C-5

Kernel 5 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 Contactless Specifications for Payment Systems, Kernel 5 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 multi-volume set:

Book A: Architecture and General Requirements

Book B: Entry Point Specification

Book C-n: Kernel Specifications

Book D: Contactless Communication Protocol

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]	*EMV Integrated Circuit Card Specifications for Payment Systems*, including:

[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

1.5 Overview

This volume includes the following chapters and annexes:

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

Chapter 2 provides an overview of the Kernel 5 approach, including implementation/acquirer options and a high level transaction flow description.

Chapter 3 specifies transaction processing for Kernel 5.

Chapter 4 lists and describes the APDU commands used by Kernel 5.

Annex A defines data elements that are specific to Kernel 5

Annex B is a dictionary of data elements used by Kernel 5 during the transaction processing.

Annex C lists data elements that are required in the transaction record for approved, declined, and online requested transactions.

Annex D defines the default Terminal Action Codes used by Kernel 5.

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

1.6 Conventions

Table 1-1: Conventions used for data format

Convention	Meaning
a	Alphabetic
an	Alphanumeric
ans	Alphanumeric Special
b	Binary
cn	Compressed Numeric
n	Numeric
n y	Numeric value of y digits (Example n 12 means 12 digits numeric value)
YYMMDD	Year, Month, Day
x	Numeric value in decimal
‘x’	Numeric value in hexadecimal
“abc”	Data string
Var.	Variable value

For data elements which have multiple bytes in this specification, the first byte or byte 1 is the leftmost byte, while the last byte is the rightmost byte.

1.7 Terminology

Table 1-2: Terminology

Terminology	Meaning
Shall, must, “is mandatory”	Denotes a mandatory requirement
Should, may, can, “is optional”	Denotes an optional requirement
if test_condition **then** action_true **else** action_false	Denotes a conditional test action, action_true is performed when test_condition result is true, action_false is performed when test_condition result is false
and	Logical AND which connects two conditional tests
or	Logical OR which connects two conditional tests
=	Logical comparison of two values
N/A	Not applicable

2 Overview of the Kernel 5 Approach

This section is a high-level description of Kernel 5 features, capabilities, and processes. Further details about the Transaction Flow and its implementation can be found in Section 3.

Vendors should check requirements of payment systems for each market deployed.

Please contact icsupport@info.jcb.co.jp for detailed JCB terminal requirements.

2.1 Three Transaction Modes

Kernel 5 is designed for acceptance of contactless cards in both Chip grade and Magstripe grade environments.

For every implementation, Kernel 5 must always support Magstripe Mode, while support of EMV Mode and/or Legacy Mode is optional.

2.1.1 EMV Mode

EMV Mode is designed for chip grade payment infrastructures.

The support of EMV Mode is optional, both on the card side (Issuer) and on the Kernel side (Acquirer). The card will select to conduct the transaction in EMV Mode when both the card and the Kernel support it.

The EMV Mode has many similarities with the transaction flow designed for contact EMV chips and defined in *[EMV]*. It is however simplified and adapted for contactless ergonomics. Here are the main features:

- **Online/offline capability:** EMV Mode transactions can be completed either online or offline. When completed online, the card is normally not informed about the final transaction outcome.
- **Offline Data Authentication:** The kernel shall support CDA when EMV Mode is supported and at least one of the conditions below is fulfilled:
    - the Kernel is offline-capable;
    - the Kernel is installed in a transit reader (where Cardholder Verification is bypassed);
    - the Kernel accepts On-Device CVM verification.

  Other data authentication methods (SDA, DDA) are not supported.

- **Online Data Authentication:** An ARQC cryptogram is generated by the card and verified by the Issuer host system.
- **Cardholder Verification:** The card determines the CVM requirement based on issuer preference and acquirer requirement and the Kernel performs the selected CVM.

2.1.2 Magstripe Mode

Magstripe Mode is designed for magstripe grade payment infrastructures.

The support of Magstripe Mode is mandatory. Here are the main features:

- **Online/offline capability:** Other than exceptional cases where the transaction can be declined offline, Magstripe Mode transactions are always authorised online. The card is not informed about the Issuer's decision.
- **Offline Data Authentication:** N/A
- **Online Data Authentication:** Issuer verifies the Card Authentication Value (CAV) included in the Track 2 Equivalent Data provided by the card. Depending on the option chosen by the Issuer, this value may be static or dynamic.
- **Cardholder Verification:** The card determines the CVM requirement based on issuer preference and acquirer requirement and the Kernel performs the selected CVM.If the card does not indicate any CVM requirement, the reader may apply its own CVM policy.

2.1.3 Legacy Mode

Legacy Mode is available for chip grade acquirers to satisfy specific market requirements. Please refer to payment system rules for further details. Here are the main features:

- **Online/offline capability:** Legacy Mode transactions are always authorised online. The card is not informed about the final transaction outcome.
- **Offline Data Authentication:** N/A
- **Online Data Authentication:** An ARQC cryptogram is generated by the card and verified by the Issuer host system
- **Cardholder Verification:** If the amount exceeds the CVM Required Limit, the Kernel analyses the CVM List from the card to determine the CVM requirement.

2.2 Transaction Processing

The transaction processing is summarised below.

1. Entry Point activates the Kernel to process the transaction. The reader provides transaction data and the relevant configuration parameters to the Kernel.
    a. Based on the card response to the SELECT (DF Name) command, the Kernel can determine whether it is a legacy card or not.
2. The Kernel sends the GET PROCESSING OPTIONS command to the card to initialise the card application.
    a. Card returns the Application Interchange Profile (AIP) and the Application File Locator (AFL).
    b. For non-legacy cards, the card response enables to detect whether the card has selected the EMV or the Magstripe Mode.
3. The Kernel reads the card data as indicated by the AFL.
4. The Kernel performs Terminal Risk Management, which consists of several verifications:
    a. Contactless Limit Check
    b. CVM Limit Check
    c. Floor Limit Check (EMV Mode only)
    d. Random Transaction Selection (EMV Mode only)
    e. Exception File Check (option only applying to EMV Mode)

    These verifications update the Terminal Verification Results (TVR).
5. The Kernel performs Processing Restrictions, which consists of several verifications:
    a. Application Usage Control (EMV Mode only)
    b. Application Expiration Date (EMV/Legacy Mode only)
    c. Application Effective Date (EMV/Legacy Mode only)

    These verifications update the Terminal Verification Results (TVR).
6. Based on the TVR value, as well as Terminal Action Codes (TAC) and Issuer Action Codes (IAC), the Kernel computes the first transaction outcome.
    a. If the outcome is a Decline, the transaction is declined offline and the Kernel provides a Declined Outcome to the Entry Point.

b. In the case of Legacy Mode and Magstripe Mode, unless the payment application declines the transaction, then the outcome is Online Authorisation.

7. The Kernel then completes the transaction in the following steps:

a) If the transaction is in EMV Mode:

- The Kernel issues a GENERATE AC command including Combined Data Authentication (CDA) request when supported.
- If the card approves or sends the transaction for authorisation (TC/ARQC), the card response includes a CDA signature (if requested by the Kernel) as well as the decision of the card regarding the Cardholder Verification Method (CVM) to be applied.
- The Kernel verifies the CDA signature (if any) and if valid, executes the card decision (TC/ARQC) and CVM policy.The Kernel then provides an Approved or Online Request Outcome corresponding to the decision for this transaction to the Entry Point.

b) If the transaction is in Magstripe Mode:

- The Kernel issues a GET MAGSTRIPE DATA command.
- The card returns the Track 2 Data (containing the card CVM policy in its discretionary data).
- The Kernel executes the card CVM policy and provides (when applicable) an Online Request to the Entry Point for this transaction for online authorisation.

c) If the transaction is in Legacy Mode:

- The Kernel issues a GENERATE AC command requesting an online authorisation (ARQC) without CDA.
- The card returns the ARQC cryptogram.
- If the CVM Required Limit is exceeded, the Kernel analyses the CVM list from the card to find an appropriate method.
- The Kernel provides an Online Request Outcome to the Entry Point for this transaction for online authorisation.

8. Optionally, if the transaction is in EMV Mode and the Transaction Outcome is Online Request, the reader may reactivate the Kernel when the online response from the Issuer contains any information. At this point, the card may still be in the field (e.g. “present-and-hold”) or requested to be presented again (e.g. “two presentments”).

- For “present-and-hold”: when returning the ARQC cryptogram, the card informs simultaneously the Kernel that it must be maintained in the contactless field during the online authorisation. After receiving the online response, Issuer Scripts and/or Issuer Authentication Data can be transmitted to the card.
- For “two presentments”: when returning the ARQC cryptogram, the card informs simultaneously the Kernel that it supports a second presentment. After receiving the online response, the cardholder is asked by Entry Point to present the card again, and Issuer Scripts and/or Issuer Authentication Data can be transmitted to the card.

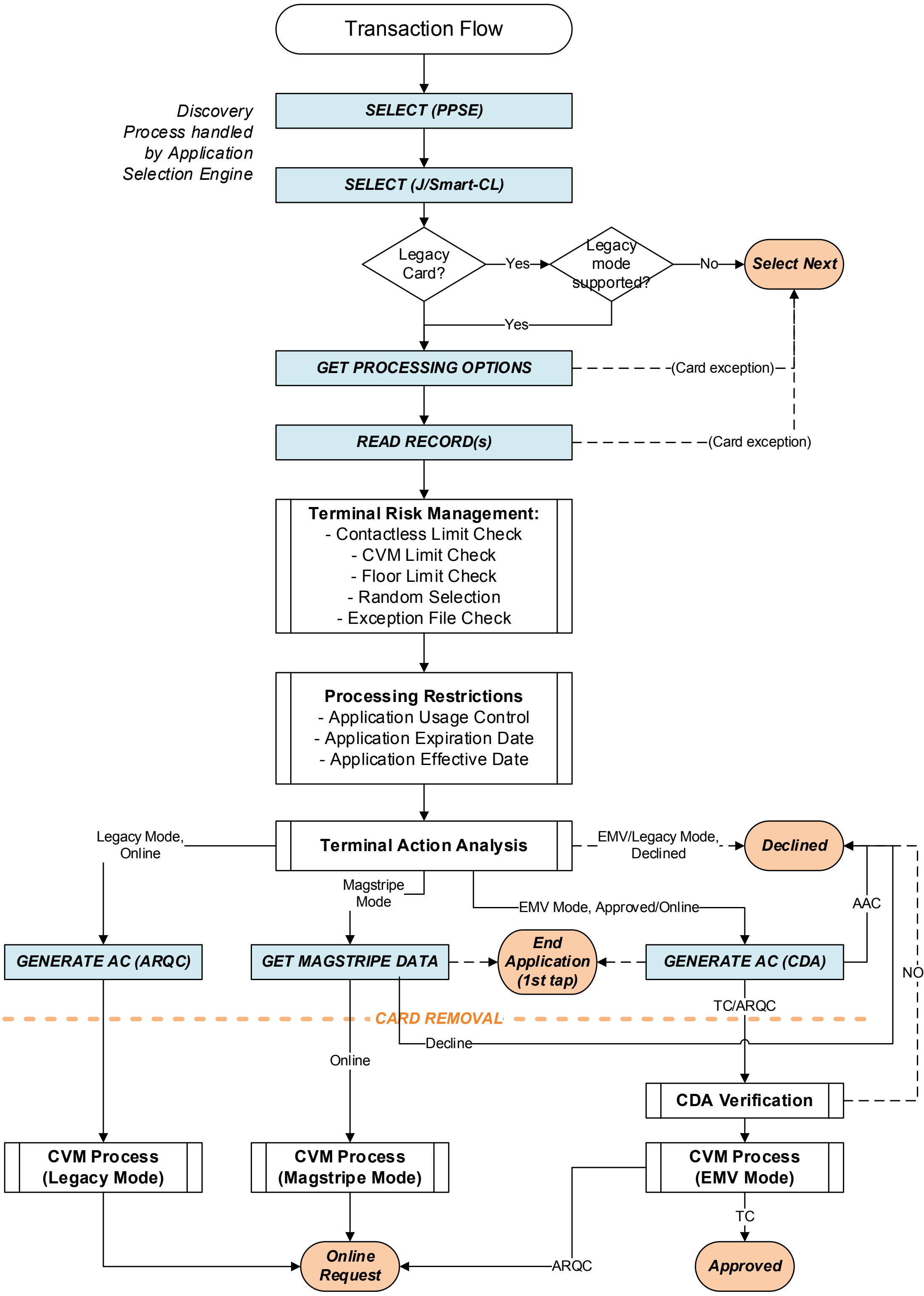
2.3 High Level Transaction Flow

Figure 2-1 below illustrates the high level transaction flow of Kernel 5.

The purpose is to provide a summarised overview of the normal Kernel 5 processing and is not prescriptive. Note that specific processes like Transaction Recovery or Issuer Update are not represented in this figure which features only a nominal transaction flow.

Details about each step of the transaction can be found in Section 3.

Figure 2-1: High-Level Sample Transaction Flow



2.4 Implementation Options and Acquirer Options

2.4.1 Implementation Options

The provider of Kernel 5 will choose whether to support or not the following options in the Kernel 5 implementation:

- **EMV Mode:**
    - This implementation option enables support of Transaction Mode that processes chip data.
    - Kernel 5 implementations aimed at being deployed in Chip grade markets must support it.
    - Kernel 5 implementations dedicated to Magstripe grade markets need not support this implementation option.
- **Legacy Mode:**
    - This implementation option enables support of Transaction Mode that processes chip data, namely Legacy Mode.
    - Kernel 5 implementations dedicated to Magstripe grade markets may not support this implementation option.
    - Legacy mode implementation may be required to satisfy specific market requirements.
- **Offline Data Authentication**
    - This implementation option enables support of CDA to authenticate the card. It can be supported only if EMV Mode is supported.
    - Kernel 5 implementations for offline-capable readers, transit readers, or readers accepting One-Device CVM must support this option.
- **Exception File Check:**
    - This implementation option enables Kernel 5 to check during the transaction whether the card appears in the Acquirer Exception File.
    - Exception File Check option can be supported only if EMV Mode is supported.
    - The exact implementation of this option is left at the discretion of the implementer. It may, for instance, take advantage of the Data Exchange mechanism described in Book A.

- **Issuer Update**
    - This implementation option enables to convey EMV data (Issuer Authentication Data and/or Issuer Scripts, optionally present in the Authorisation Response Message) to the contactless card, upon completion of the Authorisation process.
    - An Issuer Update may be transmitted to the card in one of two forms: either as a single presentment of the card (i.e. card remains in the contactless field while the authorisation process is ongoing), or as a second presentment of the card after the authorisation. Readers supporting Issuer Update must support both ergonomics, as the choice is indicated by the card.
    - Issuer Update option can be supported only if EMV Mode is supported.

2.4.2 Acquirer Options

In addition to the Implementation Options – which define the features for a specific Kernel 5 implementation, the Acquirer may also choose to support from these implemented features for deployment. The Acquirer Options are defined below:

Acquirer Options are parameterised in the Combination Options parameter (see Annex A.3) or in the static Terminal Interchange Profile (see Annex A.7) for each supported Reader Combination.

- **EMV Mode**
    - This option enables the EMV Mode flow for the associated Reader Combination
    - The option is available only if EMV Mode is supported as implementation option
- **Legacy Mode**
    - This option enables the Legacy Mode flow for the associated Reader Combination
    - The option is available only if Legacy Mode is supported as implementation option
- **Offline Data Authentication**
    - This option activates CDA for EMV Mode. *The option shall be activated if **any** of the conditions below is true:*
        - the reader is offline-capable
        - the reader is a transit reader as configured in the Terminal Interchange Profile (see Section A.7)

        - the reader accepts "On-Device CVM" as a Cardholder Verification Method in the Terminal Interchange Profile (see Section A.7)
    - The option is available only if Offline Data Authentication (implementation option) and EMV Mode (acquirer option) are supported.
- **Exception File Check**
    - This option activates the Acquirer Exception File Check during the transaction
    - The option is available only if Exception File Check (implementation option) and EMV Mode (acquirer option) are supported.
- **Random Transaction Selection**
    - This option activates Random Transaction Selection during Terminal Risk Management
    - The option is available only if EMV Mode is supported as implementation option
- **Issuer Update**
    - This option enables to convey EMV data (Issuer Authentication Data and/or Issuer Scripts, optionally present in the Authorisation Response Message) to the contactless card, upon completion of the Authorisation process.
    - The option is available only if Issuer Update (implementation option) and EMV Mode (acquirer option) are supported.

3 Transaction Processing

This chapter provides detailed transaction processing requirements for Kernel 5 including information related to EMV functions.

3.1 Kernel Activation

When activated, Kernel 5 requires certain data elements to be available in order to process the transaction.

A data element or flag may be:

- **Static (Configuration parameter)**: The value of this data is persistent from one transaction to the next (See Table 3-1). Updates of the values are exceptional and always outside the scope of Kernel 5 processing. A static data element may be set:
    - per POS System (e.g. Terminal Country Code), or
    - per RID (e.g. CAPK key), or
    - per AID (e.g. static Terminal Interchange Profile)
- **Dynamic (Transaction parameter):** Per transaction, e.g. Amount, Authorised (Numeric) and Unpredictable Number (See Table 3-2).

Requirement – Static Configuration Parameters

3.1.1.1 When the Kernel is activated, the reader shall provide to the Kernel the Configuration Data (see Table 3-1) associated with the selected Combination.

Requirement – Dynamic Transaction Parameters

3.1.1.2 When the Kernel is activated, the reader shall provide to the Kernel:

- The Dynamic Transaction Parameters (see Table 3-2);
- FCI received from the card as per section 3.4 in *[EMV CL Book B]* (when applicable).

Table 3-1: Static Configuration Parameters

Name	Description	Varies by	Presence[1]	Format	Specified	Tag	Length (bytes)
Combination Options	Defines some acquirer options for the combination, e.g. modes supported	AID	M	b	Kernel 5 See A.3	-	2
Contactless Floor Limit	Used in Kernel 5 Terminal Risk Management (EMV Mode only). Present if the Combination supports Floor Limit Check or Random Transaction Selection.	AID	C	n12	Kernel 5	-	6
Contactless Transaction Limit	Used in Kernel 5 Terminal Risk Management	AID	O	n12	Kernel 5	-	6
CVM Required Limit	Used in Kernel 5 Terminal Risk Management	AID	O	n12	Kernel 5	-	6
Maximum Target Percentage to be Used for Biased Random Selection	Present if the Combination supports Random Transaction Selection (EMV Mode only)	AID	C	n2	EMV	-	1
Removal Timeout	Present if the Combination supports Issuer Update as Acquirer Option (EMV Mode only). In case of Online Request with “Present and Hold” outcome, this parameter corresponds to the time after which cardholder is asked to remove the card. Value is given in units of 100ms.	AID	C	n4	Kernel	-	2

[1] M = mandatory ; C = conditional ; O = optional

Name	Description	Varies by	Presence[1]	Format	Specified	Tag	Length (bytes)
Target Percentage to be Used for Biased Random Selection	Present if the Combination supports Random Transaction Selection (EMV Mode only)	AID	C	n2	EMV	-	1
Terminal Action Code - Default	Used in Kernel 5 Terminal Action Analysis (EMV Mode only)	AID	O	b	EMV	-	5
Terminal Action Code - Denial	Used in Kernel 5 Terminal Action Analysis	AID	O	b	EMV	-	5
Terminal Action Code - Online	Used in Kernel 5 Terminal Action Analysis (EMV Mode only)	AID	O	b	EMV	-	5
Terminal Interchange Profile (static)	Defines the Cardholder Verification Methods and other reader capabilities (online capability, contact EMV capability) for the Combination	AID	M	b	Kernel 5 See A.5	-	3
Threshold Value for Biased Random Selection	Present if the Combination supports Random Transaction Selection (EMV Mode only)	AID	C	n12	EMV	-	6
Acquirer Identifier	Uniquely identifies the acquirer within each payment system	POS	M	n 6-11	EMV	‘9F01’	6
Merchant Category Code	Classifies the type of business being done by the merchant, represented according to ISO 8583:1993 for Card Acceptor Business Code	POS	O	n 4	EMV	'9F15'	2
Merchant Name and Location	Indicates the name and location of the merchant	POS	M	ans	EMV	'9F4E'	var.
Terminal Country Code	Indicates the country of the terminal, represented according to ISO 3166. Requested in CDOL1.	POS	M	n3	EMV	'9F1A'	2

Name	Description	Varies by	Presence[1]	Format	Specified	Tag	Length (bytes)
Terminal Type	Indicates the environment of the terminal, its communications capability, and its operational control	POS	M	n 2	EMV	'9F35'	1
Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217. Requested in CDOL1.	POS	M	n 3	EMV	'5F2A'	2
Transaction Currency Exponent	Indicates the implied position of the decimal point from the right of the transaction amount represented according to ISO 4217. Required to determine if Status Check is requested.	POS	M	n 1	EMV	‘5F36’	1
Certification Authority Public Key	Present (up to 6 different instances) if Offline Data Authentication is supported for at least one of the Combinations with this RID (EMV Mode only). Each CA Public Key in the list is composed of the following mandatory fields: - CAPK Index (b, 1 byte) - CAPK Modulus (b, max. 248 bytes) - CAPK Exponent (b, 1 or 3 bytes) - CAPK SHA-1 Checksum (b, 20 bytes)	RID	C	b	EMV	-	var.

Table 3-2: Dynamic Transaction Parameters

Name	Description	Presence[2]	Format	Specified	Tag	Length (bytes)
Amount, Authorised (Numeric)	Authorised amount of the transaction. Requested in CDOL1.	M	n12	EMV	'9F02'	6
Amount, Other (Numeric)	Secondary amount associated with the transaction representing a cashback amount. Requested in CDOL1.	M	n12	EMV	'9F03'	6
Authorisation Response Code (ARC)	Code that defines the disposition of a message. ARC must be present if the Kernel is restarted after an Online Request Outcome.	C	an2	EMV	‘8A’	2
Issuer Authentication Data	Data sent to the card for online issuer authentication	O	b	EMV	‘91’	8-16
Issuer Script Template 1	Contains proprietary issuer data for transmission to the card before the second GENERATE AC command. **Several occurrences of this data element may be present.**	O	b	EMV	‘71’	Var. max. 128
Issuer Script Template 2	Contains proprietary issuer data for transmission to the dard after the second GENERATE AC command. **Several occurrences of this data element may be present.**	O	b	EMV	‘72’	Var. max. 128
Transaction Date	Local date that the transaction was authorised. Requested in CDOL1.	M	n6	EMV	'9A'	3
Transaction Time	Local time that the transaction was authorised. Possibly requested in CDOL1.	M	n6	EMV	‘9F21’	3

[2] M = mandatory ; C = conditional ; O = optional

Name	Description	Presence[2]	Format	Specified	Tag	Length (bytes)
Transaction Type	Indicates the type of financial transaction, represented by the first two digits of the ISO 8583:1987 Processing Code. Requested in CDOL1. Possible values are: - '00' for a purchase transaction - ‘01’ for a cash advance transaction - ‘09’ for a purchase with cashback - ‘20’ for a refund transaction	M	n2	EMV	'9C'	1
Unpredictable Number	Value to provide variability and uniqueness to the generation of a cryptogram. Requested in CDOL1.	M	b	EMV	'9F37'	4

3.2 Transaction Initialisation

During Transaction Initialisation, Kernel 5 initialises internal variables and performs verifications.

Requirement – Recovering from Torn EMV Transaction

3.2.1.1 **If** the Kernel internal variable '*Recovering from Torn EMV Transaction*' has value TRUE,

Then the Kernel shall proceed with Torn Transaction Recovery as described in section 3.14.

Otherwise the Kernel shall proceed with Requirement 3.2.1.2.

Requirement – Transaction continuation

3.2.1.2 **If** Authorisation Response Code (tag '8A') is present in the Dynamic Transaction Parameters (see Table 3-2),

Then the Kernel shall proceed with Requirement 3.2.1.3.

Otherwise the Kernel shall proceed with Requirement3.2.1.4.

3.2.1.3 **If** any of the following is present in the Dynamic Transaction Parameters (see Table 3-2),

- Issuer Authentication Data ('91')
- At least one occurrence of Issuer Script Template 1 ('71')
- At least one occurrence of Issuer Script Template 2 ('72')

Then the Kernel shall restore transaction data from Online Transaction Context and proceed with Issuer Update Processing, as described in section 3.11.

Otherwise the Kernel shall provide an **End Application** outcome as described in section 3.13.7.

Requirement – SELECT response analysis

3.2.1.4 **If** the FCI is absent,
Or if the FCI is not parsed correctly (see table 45 in *[EMV Book 1]*),
Or if the PDOL data element is absent, or present but empty
Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.13.10.

Requirement – Variable Initialisation

3.2.1.5 The Kernel shall reset the following data elements:

- Terminal Verification Results (Tag '95') to '00 00 00 00 00'
- Terminal Compatibility Indicator (Tag '9F52') to '01', indicating that Magstripe Mode is supported

3.2.1.6 The Kernel shall reset the following internal variables:

- *Online Transaction Context*
- Transaction Mode to 'Undefined Mode'

Requirement – Terminal Compatibility Indicator

3.2.1.7 **If** the Kernel supports EMV Mode (Implementation Option)
And the Combination Options Byte 1 Bit 2 is set to 1b ('EMV Mode Supported') for the selected Combination,
Then bit 2 ('EMV Mode Supported') shall be set to '1' in Terminal Compatibility Indicator (Tag '9F52').

Requirement – Terminal Interchange Profile

3.2.1.8 The Kernel shall initialise a dynamic Terminal Interchange Profile (Tag ’9F53’) from the value of the static Terminal Interchange Profile (static configuration parameter – no tag) and perform the following:

- Clear Byte 1 Bit 8 ("CVM required by reader").
- **If** Issuer Update is *not* supported as an implementation option,
  Then clear Byte 2 Bit 8 (‘Issuer Update supported’).

Note: The dynamic Terminal Interchange Profile (Tag ‘9F53’) is updated by the Kernel during subsequent processing.

At that stage, the Kernel will detect whether the presented card is a legacy card, and if so, enure that it has the capability to process such cards.

Requirement – Legacy Mode Detection

3.2.1.9 **If** the PDOL contains Terminal Compatibility Indicator (Tag ’9F52’),
Then the Kernel shall proceed with section 3.3: Initiate Application Processing.

Otherwise the card is a legacy card and the Kernel shall proceed with Requirement 3.2.1.10.

3.2.1.10 **If** Kernel 5 supports Legacy Mode (Implementation Option)
And the Combination Options indicates ‘Legacy Mode Supported’ for this AID,
Then the Kernel shall set Transaction Mode to ‘Legacy Mode’ and proceed with section 3.3: Initiate Application Processing**.**

Otherwise the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.13.10.

3.3 Initiate Application Processing

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 and GPO Command

3.3.1.1 The Kernel shall process the PDOL and send the command data for the GET PROCESSING OPTIONS as described in *[EMV Book 3]*.

3.3.1.2 **If** the PDOL requires a data element that is not recognised by the Kernel (not referenced in Annex B),
Then the Kernel shall fill in the corresponding PDOL related data with zeroes.

The Application Interchange Profile (AIP) and Application File Locator (AFL) returned by the card in response to the GPO command contain information on the card configuration and data records to be read. The card response may use either Format 1 or Format 2, as described in *[EMV Book 3]*.

If the card chooses Magstripe Mode for the transaction, then AFL (Tag '94') may be absent; however, for an EMV Mode or Legacy Mode transaction, the card is expected to return the AFL (Tag '94') in the GPO response.

The Kernel detects the mode selected by the card (EMV / magstripe) and in the case of EMV Mode, the Kernel also ensures that the card supports CDA. Other AIP bits are not analysed by the Kernel.

Requirement – GPO Response Analysis

3.3.1.3 **If** the AIP (Tag '82') is absent from the GET PROCESSING OPTIONS response,
Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.13.10.

Requirement – GPO Response Analysis

3.3.1.4 **If** the Transaction Mode is equal to 'Undefined Mode',
Then

> **If** the AIP (Tag '82') returned by the card has Byte 2 Bit 8 set to '1' ('EMV Mode Selected'),
> **Then** the Kernel shall set Transaction Mode to 'EMV Mode'.
> **Else** the Kernel shall set the Transaction Mode to 'Magstripe Mode'.

3.3.1.5 **If** the AFL (Tag '94') is absent from the data returned to the GET PROCESSING OPTIONS response
And the Transaction Mode is 'EMV Mode' or 'Legacy Mode',
Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.13.10.

3.3.1.6 **If** the AFL (Tag '94') is present in the GET PROCESSING OPTIONS RESPONSE
And its value is incorrectly formatted (e.g. not multiple of 4 bytes, invalid SFI value...),
Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.13.10.

3.3.1.7 **If any** of the conditions below is true:

- the Transaction Mode is equal to 'Magstripe Mode'
- the Transaction Mode is equal to 'Legacy Mode'
- the Transaction Mode is equal to 'EMV Mode' and Offline Data Authentication (implementation or acquirer option) is not supported
- the Transaction Mode is equal to 'EMV Mode' and the AIP (Tag '82') indicates that CDA is not supported (Byte 1bit 1 is '0')

Then the Kernel shall set TVR Byte 1 bit 8 ('Offline Data Authentication was not performed') to '1'.

3.4 Read Application Data

The Kernel uses the AFL to determine which records to request from the card. The Kernel does not need to process any data at this point, except to determine if all the mandatory data elements are present.

Requirement – Reading Records

3.4.1.1 **If** the AFL has been provided by the card, the Kernel shall read the records indicated in the AFL using the READ RECORD command and process the response as defined in *[EMV Book 3]*.

At that point, the Kernel needs to determine if all mandatory data elements are present.

Requirement – Presence of Mandatory Data Elements

3.4.1.2 **If** the Transaction Mode is 'EMV Mode' or 'Legacy Mode'
And any of the following mandatory Data Elements is absent from the card:

- CDOL1 (Tag '8C')
- Track2 Equivalent Data (Tag '57')
- Application Expiration Date (Tag '5F24')

Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.13.10.

As CDA is the mandatory Data Authentication Method supported by the Kernel in 'EMV Mode', the Kernel shall ensure that all the appropriate data elements are present.

3.4.1.3 **If** the Transaction Mode is ‘EMV Mode’
And Offline Data Authentication is supported (implementation and acquirer option)
And the AIP (Tag ‘82’) indicates that CDA is supported (Byte 1bit 1 is ‘1’)
And any of the following Data Elements is absent from the card:

- Certification Authority Public Key Index (Tag ‘8F’)
- Issuer Public Key Certificate (Tag ‘90’)
- Issuer Public Key Exponent (Tag ‘9F32’)
- ICC Public Key Certificate (Tag ‘9F46’)
- ICC Public Key Exponent (Tag ‘9F47’)
- Issuer Public Key Remainder (Tag ‘92’), when required (based on the sizes of tags ‘90’ and ‘9F46’, when both are present)

Then the Kernel shall set TVR Byte 1 bit 6 (‘ICC Data Missing’) and Byte 1 bit 3 (‘CDA Failed’) to ‘1’.

3.4.1.4 **If** the Transaction Mode is ‘EMV Mode’
And Offline Data Authentication is supported (implementation and acquirer option)
And the Certification Authority Public Key corresponding to the CAPK index (Tag ‘8F’) provided by the card is not present in the Kernel configuration data,
Then the Kernel shall set TVR Byte 1 bit 3 (‘CDA Failed’) to ‘1’.

(Note: the kernel recovers the ICC public key later during the transaction to optimise the performance).

3.5 Terminal Risk Management

Terminal Risk Management consists of verifications that compare the transaction amount with reader-based limits, and take appropriate action if the limit is exceeded. The Acquirer’s Exception List may also be checked.

Terminal Risk Management is mandatory and always performed.

3.5.1 Contactless Limit Check

Requirement – Contactless Limit Check

3.5.1.1 **If** the Contactless Transaction Limit is present
And the value of Amount, Authorised (Numeric) (Tag ‘9F02’) is greater than or equal to this limit,
Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.13.10.

3.5.2 CVM Required Limit Check

Requirement – CVM Required Limit Check

3.5.2.1 **If** the CVM Required Limit is present
And the Transaction Type corresponds to a Purchase or Cash-Advance transaction (i.e. value is ‘00’, ‘01’ or ‘09’)
And the value of Amount, Authorised (Numeric) (Tag ‘9F02’) is greater than or equal to this limit,
Then the Kernel shall indicate ‘CVM Required by Reader’ (Byte 1, bit 8) in the dynamic Terminal Interchange Profile (Tag ’9F53’).

3.5.3 Floor Limit Check

Requirement – Floor Limit Check

3.5.3.1 **If any** of the conditions below is true:

- The Transaction Mode is 'Magstripe Mode'
- The Transaction Mode is 'Legacy Mode'
- The Terminal Type (Tag '9F35') indicates that the reader is online-only (value = 'x1' or 'x4')
- The Amount, Authorised is a single unit of currency[3] **and** the Combination Options Byte 1 Bit 7 is set to 1b ('Status Check Supported')

Then the Kernel shall set TVR Byte 4 bit 8 ('Transaction exceeds Floor Limit') to '1'.

3.5.3.2 **If** the Transaction Mode is 'EMV Mode'
And the Contactless Floor Limit is present
And the value of Amount, Authorised (Numeric) (Tag '9F02') is greater than or equal to this limit,
Then the Kernel shall set TVR Byte 4 bit 8 ('Transaction exceeds Floor Limit') to '1'.

3.5.4 Random Transaction Selection

Requirement – Random Transaction Selection

3.5.4.1 **If** the Transaction Mode is 'EMV Mode'
And the Combination Options indicate that 'Random Transaction Selection supported'
And the TVR Byte 4 bit 8 has value '0' (Floor Limit not exceeded),
Then the Kernel shall perform Random Transaction Selection as described in *[EMV Book 3]*.

[3] The Amount corresponding to a single unit of currency is obtained as $10^{\text{Transaction Currency Exponent}}$. E.g. for USD, where Transaction Currency Exponent = 2, a single unit of currency (1.00 USD) is coded as '000000000100'.

The Transaction Currency Exponent is a Kernel configuration parameter.

Requirement – Random Transaction Selection

3.5.4.2 **If** the transaction is randomly selected for online authorisation, **Then** the Kernel shall set TVR Byte 4 bit 5 ('Transaction selected randomly for online processing') to '1'.

3.5.5 Exception File Check

Exception file check is both an Implementation Option as well as an Acquirer Option.

When applicable, the exact implementation of this check is left at the discretion of the implementer. It may, for instance, take advantage of the Data Exchange mechanism described in *Book A.*

Requirement – Exception File Check

3.5.5.1 **If** all the conditions below are true:

- the Transaction Mode is 'EMV Mode'
- Exception File Check is supported (Implementation Option)
- the Combination Options (Acquirer Options) indicate that 'Exception File Check required'

Then the Kernel shall perform Exception File Check as described in *[EMV Book 4]*.

3.5.5.2 **If** the card number (PAN) has been found in the Exception File, **Then** the Kernel shall set TVR Byte 1 bit 5 ('Card appears on terminal exception file') to '1'.

3.6 Processing Restrictions

3.6.1 Application Usage Control Check

Requirement – Application Usage Control	
3.6.1.1	**If** the Transaction Mode is 'EMV Mode' **And** the Application Usage Control (Tag '9F07') has been provided by the card, **Then** the Kernel shall perform Application Usage Control as described in *[EMV Book 3]*.
3.6.1.2	**If** the result from Application Usage Control Check indicates that the transaction is not allowed, **Then** the Kernel shall set TVR Byte 2 bit 5 ('Requested Service Not Allowed for Card Product') to '1'.

3.6.2 Application Expiration Date Check

Requirement – Application Expiration Date	
3.6.2.1	**If** the Transaction Mode is 'EMV Mode' or 'Legacy Mode', **Then** the Kernel shall perform Application Expiration Date Check as described in *[EMV Book 3]*.
3.6.2.2	**If** the card application has expired, **Then** the Kernel shall set TVR Byte 2 bit 7 ('Expired Application') to '1'.

3.6.3 Application Effective Date Check

Requirement – Application Effective Date	
3.6.3.1	**If** the Transaction Mode is 'EMV Mode' or 'Legacy Mode' **And** the Application Effective Date (Tag '5F25') has been provided by the card, **Then** the Kernel shall perform Application Effective Date Check as described in *[EMV Book 3]*.
3.6.3.2	**If** the card application is not yet effective, **Then** the Kernel shall set TVR Byte 2 bit 6 ('Application Not Yet Effective') to '1'.

3.7 Terminal Action Analysis

Requirements – Terminal Action Analysis	
3.7.1.1	**If** the Transaction Type indicates a Refund ('20'), **Then** the Kernel shall decline the transaction (i.e. Terminal Action Analysis results in decline) and continue with Requirement 3.7.1.5 ("Terminal Action Analysis Completion"). **Else** the Kernel shall continue with Requirement 3.7.1.2.
3.7.1.2	**Issuer Action Code (IAC) Values:** **If** the Transaction Mode is 'EMV Mode' **Then** the Kernel shall use the Issuer Action Code values provided by the card for Terminal Action Analysis. **Otherwise** for 'Legacy Mode', 'Magstripe Mode', or no IAC values are provided by card, the Kernel shall use the following default IAC values: • IAC-Decline: 00 00 00 00 00 • IAC-Online: FF FF FF FF FF • IAC-Default: FF FF FF FF FF
3.7.1.3	**Terminal Action Code (TAC) Values:** **If** Terminal Action Code values (Decline, Online, Default) are parameterised as part of the Kernel configuration data, **then** the Kernel shall use the parameterised Terminal Action Code values. **Otherwise** the Kernel shall use the default TAC values as defined in Annex D, Table D-1.

Requirements – Terminal Action Analysis

3.7.1.4 **Terminal Action Analysis**

The Kernel shall perform Terminal Action Analysis as described in *[EMV Book 3]*, using:

- Terminal Verification Results (TVR)
- TAC/IAC-Decline
- TAC/IAC-Online: If the Terminal Type (Tag '9F35') indicates that the reader is online-capable ('x1', 'x2', 'x4' or 'x5')
- TAC/IAC-Default: If the Terminal Type (Tag '9F35') indicates that the reader is offline-only ('x3' or 'x6')

Requirement – Terminal Action Analysis Completion

3.7.1.5 **If** Transaction Mode is 'Magstripe Mode'
Then the Kernel shall proceed to completion as described in Section 3.9.

Else ('EMV Mode', 'Legacy Mode'):

> **If** the result of the Terminal Action Analysis is to decline the transaction
> **Then** the Kernel shall decline the transaction as described in Section 3.13.5.
>
> **Otherwise** the Kernel shall proceed to completion as described in:
>
> - Section 3.8 if Transaction Mode is 'EMV Mode'
> - Section 3.10 if Transaction Mode is 'Legacy Mode'

3.8 Completion – EMV Mode

When the transaction is processed in 'EMV Mode' the Kernel will request the card to generate a cryptogram corresponding to the decision taken during Terminal Action Analysis, by issuing a GENERATE AC command. A CDA signature is systematically requested if Offline Data Authentication is supported by the Kernel (implementation and acquirer option).

If the CDA signature is valid, the Kernel will apply the decision of the card with regards to the transaction outcome and the CVM to be performed.

3.8.1 GENERATE AC Command

The CDOL1 used to prepare the GENERATE AC command is obtained during READ RECORD processing.

Requirement – CDOL1 Processing

3.8.1.1 The Kernel shall process the CDOL1 and construct the command data for the GENERATE AC command, as described in *[EMV Book 3]*.

3.8.1.2 **If** the CDOL1 requests a Data Object that is not recognised by the Kernel (not referenced in Annex B),
Then the Kernel shall fill in the corresponding CDOL1 related data with zeroes.

Requirement – GENERATE AC

3.8.1.3 The Kernel shall request the card to generate a cryptogram using the GENERATE APPLICATION CRYPTOGRAM command as defined in Section 4.2 and *[EMV Book 3]*.

The type of cryptogram (TC or ARQC) requested by the Kernel in the Reference Control Parameter (parameter P1) shall correspond to the result of the Terminal Action Analysis.

Requirement – GENERATE AC

3.8.1.4 **If** Offline Data Authentication is supported (implementation and acquirer option)
And the AIP (Tag '82') indicates that CDA is supported (Byte 1bit 1 is '1'),

Then the Kernel shall request a CDA Signature in the Reference Control Parameter (bit 5 is set to '1').

At this stage the Kernel needs to analyse the GENERATE AC response.

Requirement – GENERATE AC Response Analysis

3.8.1.5 **If** the Status Word returned by the card is equal to **'6986'**,
Then the Kernel shall terminate the transaction with an ***End Application (with restart, On-device CVM)*** Outcome as defined in section 3.13.9.

This Status Word indicates that the CVM shall be performed on the cardholder device prior to attempting the transaction (e.g. a Confirmation Code shall be entered on the mobile device).

3.8.1.6 **If** the Status Word returned by the card is equal to **'6984'**,
Then the Kernel shall terminate the transaction with a ***Try Another Interface*** Outcome as defined in section 3.13.6.

This Status Word indicates that the card is a dual-interface card that prefers to conduct the transaction using the contact interface.

3.8.1.7 **If** the Status Word returned by the card is different from '6984', '6986' and '9000',
Then the Kernel shall terminate the transaction with a ***Select Next*** Outcome as defined in section 3.13.10.

Requirement – GENERATE AC Response Analysis

3.8.1.8 The Kernel shall parse the response to the GENERATE AC and ensure that it is correctly formatted and the card has provided all mandatory data elements. The mandatory data elements depend on the transaction context. They are listed in Table 4-3, Table 4-4 and Table 4-5.

If the response to the GENERATE AC command is not parsed correctly,
Or if a mandatory data element is missing,
Or if the format of a returned data element is incorrect,
Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.8.1.9 **If** the Cryptogram Information Data (Tag '9F27') indicates an AAC,
Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.8.1.10 The Kernel shall analyse the type of cryptogram returned from the card for consistency with the requested type of cryptogram.

If the Kernel requested ARQC, but the CID indicates a TC,
Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.8.1.11 **If** Offline Data Authentication is supported (implementation and acquirer option)
And the AIP (Tag '82') indicates that CDA is supported (Byte 1bit 1 is '1')
And the Signed Dynamic Application Data (Tag '9F4B') is absent from the card response,
Then the Kernel shall decline the transaction as defined in section 3.13.5.

Once the response has been received, if the card is no longer required in the field, and if the CDA verification is to be performed, the indication is given to the cardholder that the card can be removed.

Requirement – Card Removal

3.8.1.12 **If** Signed Dynamic Application Data (Tag ‘9F4B’) is present in the card response,

And one of the following conditions is True:

- the Issuer Update Parameter (Tag ‘9F60’) is absent from the card response, **or** has a value = ‘02’ (“Second Presentment”),
- Issuer Update is not supported by the Kernel (Implementation Option or Acquirer Options)

Then 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.

3.8.2 Offline Data Authentication

The Kernel verifies the CDA signature returned in the GENERATE AC 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 – CDA Signature Verification

3.8.2.1 **If** the card has returned a Signed Dynamic Application Data (tag ‘9F4B’),
Then the Kernel shall verify the signature as defined for CDA in *[EMV Book 2] ,* including the retrieval of ICC Public Key.[4]

If any step of signature verification fails,
Then the Kernel shall decline the transaction as defined in section 3.13.5.

[4] When an optional data object that is required to support offline data authentication is missing, the kernel shall set the ‘ICC data missing’ indicator in the Terminal Verification Results (TVR) to 1.

3.8.3 CVM Processing

When Transaction Mode is ‘EMV Mode’, the Kernel is required to check the consistency of the CVM decision (“Cardholder Verification Status”) that has been provided by the card with the GENERATE AC response, and to apply this decision.

This Cardholder Verification Status, authenticated by the CDA signature, is computed by the card based on its internal card risk management parameters, and based on the transaction context as communicated by the Kernel in the CDOL1 related data.

Requirement – CVM Evaluation

3.8.3.1 The Kernel shall examine the *Cardholder Verification Status* (Tag ’9F50’) returned by the card in the GENERATE AC response to determine the card CVM requirement for the transaction:

- ‘00’: No CVM
- ‘10’: Obtain Signature
- ‘20’: Online PIN
- ‘3x’: Confirmation Code Verified
- Other: Not Applicable (no CVM preference)[5]

[5] If the amount exceeds the CVM Required Limit and the card does not indicate any CVM requirement (CVS indicates no CVM preference), the reader may apply its own CVM policy.

Requirement – CVM Consistency Check

3.8.3.2 **If** the *Terminal Interchange Profile (dynamic)* indicates 'CVM Required by Reader' (byte 1 bit 8 = '1')
And the *Cardholder Verification Status* indicates No CVM ('00')
Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.8.3.3 **If** the *Cardholder Verification Status* has any value among '10', '20' or '3x' (Signature, Online PIN, or On-Device CVM)
And the corresponding CVM is not supported in the *Terminal Interchange Profile (dynamic)*
Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.8.4 Transaction Outcome

The Outcome is set for ***Approved*** or ***Online Request***, as per the card decision, with the parameters indicating the CVM requirement (if any). The data elements for an EMV clearing record or an online authorisation are made available to the reader.

Requirement – Transaction Outcome

3.8.4.1 **If** the Cryptogram Information Data (Tag '9F27') indicates a TC,
Then the Kernel shall provide an ***Approved*** Outcome as defined in section 3.13.1.

3.8.4.2 **If** the Cryptogram Information Data (Tag '9F27') indicates an ARQC,
And any of the conditions below is true:

- Issuer Update is NOT supported (as implementation option , or as acquirer option in static TIP, byte 2 bit 8)
- the Issuer Update Parameter (Tag '9F60') is absent or has value '00'

then the Kernel shall provide an ***Online Request*** Outcome as defined in section 3.13.2.

Requirement – Transaction Outcome

3.8.4.3 **If** the Cryptogram Information Data (Tag ‘9F27’) indicates an ARQC,
And Issuer Update is supported (both as implementation option and as acquirer option in static TIP, byte 2 bit 8)
And the Issuer Update Parameter (Tag ‘9F60’) is present with value value ‘01’
Then the Kernel shall provide an ***Online Request*** Outcome (“**Present and Hold**”) as defined in section 3.13.4.

3.8.4.4 **If** the Cryptogram Information Data (Tag ‘9F27’) indicates an ARQC,
And Issuer Update is supported (both as implementation option and as acquirer option in static TIP, byte 2 bit 8)
And the Issuer Update Parameter (Tag ‘9F60’) is present with value value ‘02’
Then the Kernel shall provide an ***Online Request*** Outcome (“**Two Presentments**”) as defined in section 3.13.3.

3.8.4.5 The CVM parameter in the Approved or Online Request Outcome shall be set to the result of CVM Processing as specified in section 3.8.3.

3.8.4.6 The Message Identifier parameter in the ***Approved*** or ***Online Request*** Outcome (UI Request on Outcome Present) shall take the following value:

```
If Outcome = Approved

Then
    If CVM = Obtain Signature
    Then Message Identifier = ‘1A’ (“Approved, please sign”)
    Else Message Identifier = ‘03’ (“Approved”)

Else (Outcome = Online Request)
    If CVM = Online PIN
    Then Message Identifier = ‘09’ (“Please enter your PIN”)
    Else Message Identifier = ‘1B’ (“Authorising, please wait”)
```

3.8.4.7 **If** the Kernel provides an ***Online Request “Present and Hold” or “Two Presentments”*** outcome as per Requirements 3.8.4.3 or 3.8.4.4,

Requirement – Transaction Outcome

Then the following information shall be retained as the *Online Transaction Context* (for subsequent Kernel activation to perform Issuer Update Processing):

- EMV Data Record provided as part of the outcome (see Annex C)
- CVM Parameter provided as part of the outcome
- CDOL2 data element (when provided by the card)

3.9 Completion – Magstripe Mode

When the transaction is processed in 'Magstripe Mode', the Kernel provides the transaction context to the card and in return requests the card to provide the Track 2 Equivalent Data. The card returns the Track 2 Equivalent Data when it considers that the transaction can be authorised online.

The Track 2 Equivalent Data will also contain the instructions from the card regarding the Cardholder Verification Method to be applied. The Kernel provides these instructions to the Reader in the Transaction Outcome.

3.9.1 GET MAGSTRIPE DATA Command

Normally, the card should be personalised with the Magstripe Data Object List (MDOL Tag '9F5C') and the MDOL is read by the Kernel during Read Application Data processing. The MDOL is then used to prepare the GET MAGSTRIPE DATA command. However, if the MDOL is absent, then the Kernel shall use a default MDOL value that is parameterised as part of Kernel configuration data.

Requirement – MDOL Processing

3.9.1.1 **If** the Kernel has not obtained MDOL (Tag '9F5C') as part of Read Application Data,
Then the Kernel shall use the following Default MDOL value:

• '9F02'	Amount, Authorised (Numeric),	6 bytes;
• '9F1A'	Terminal Country Code,	2 bytes;
• '5F2A'	Transaction Currency Code,	2 bytes;
• '9A'	Transaction Date,	3 bytes;
• '9C'	Transaction Type,	1 byte;
• '9F53'	Dynamic Terminal Interchange Profile,	3 bytes;
• '9F4E'	Merchant Name and Location,	20 bytes;

3.9.1.2 The Kernel shall process the MDOL and construct the command data (MDOL related data) for the GET MAGSTRIPE DATA command, using the standard DOL preparation rules described in *[EMV Book 3]*.

Requirement – MDOL Processing

3.9.1.3 **If** the MDOL requests a data element that is not recognised by the Kernel (not referenced in Annex B),
Then the Kernel shall fill in the corresponding MDOL related data with zeroes.

The Kernel issues a GET MAGSTRIPE DATA command in order to retrieve the image of financial Track 2 Magstripe. The card analyses the transaction context provided by the Kernel and decides whether the transaction can be sent online for authorisation (normal behaviour), or whether the transaction shall be declined. The card also determines the CVM to be applied for the transaction.

Requirement – GET MAGSTRIPE DATA command

3.9.1.4 The Kernel shall request the card to provide the Track2 Equivalent Data (Tag ‘57’) using the GET MAGSTRIPE DATA command as defined in Section 4.4.

The type of decision (online or decline) requested by the Kernel in the Reference Control Parameter (parameter P1) shall correspond to the result of the Terminal Action Analysis.

At that stage the Kernel needs to analyse the GET MAGSTRIPE DATA response.

Requirement – GET MAGSTRIPE DATA Response Analysis

3.9.1.5 **If** the Status Word returned by the card is equal to **‘6986’**,
Then the Kernel shall terminate the transaction with an ***End Application (with restart, On-device CVM)*** Outcome as defined in section 3.13.9.

This Status Word indicates that the CVM shall be executed on the cardholder device prior to attempting the transaction (e.g. a Confirmation Code shall be entered on the mobile device).

3.9.1.6 **If** the Status Word returned by the card is different from ‘6300’, ‘6986’ and ‘9000’,
Then the Kernel shall terminate the transaction with a ***Select Next*** Outcome as defined in section 3.13.10.

Requirement – GET MAGSTRIPE DATA Response Analysis	
3.9.1.7	The Kernel shall ensure that the card has provided Track2 Equivalent Data (Tag '57') in response to the GET MAGSTRIPE DATA. **If** Track2 Equivalent Data is missing or is incorrectly formatted, **Then** the Kernel shall terminate the transaction with a ***Select Next*** Outcome as defined in section 3.13.10.
3.9.1.8	**If** the Status Word returned by the card is equal to **'6300'**, **Then** the Kernel shall decline the transaction as defined in section 3.13.5. This Status Word indicates that the card refuses the Magstripe Mode transaction.

3.9.2 CVM Processing

When Transaction Mode is 'Magstripe Mode' and the card has requested an online authorisation, the Kernel is required to apply the CVM decision that is provided by the card inside the Track 2 Equivalent Data.

Requirement – CVM Evaluation

3.9.2.1 The Kernel shall extract the rightmost significant digit from Track2 Equivalent Data (Tag ‘57’) provided by the card.

> *Note: a significant digit is defined as a nibble with a decimal value (‘0’ to ‘9’), and thus excludes padding value ‘F’, usually present to ensure whole bytes.*
>
> *An example is given below:*
>
> 1234567890123456D1612201123451230000**0**F

The Kernel shall examine the rightmost significant digit (i.e. the CVM decision digit) to determine the CVM decision for this transaction:

‘0’:	Not Applicable (no CVM preference)
‘1’:	No CVM
‘2’:	Obtain Signature
‘3’:	Online PIN
‘4’:	Confirmation Code Verified
‘5-9’:	Not Applicable (no CVM preference)

Requirement – CVM Consistency Check

3.9.2.2 **If** the *Terminal Interchange Profile (dynamic)* indicates ‘CVM Required by Reader’ (byte 1 bit 8 = ‘1’)
And the CVM decision digit indicates No CVM (‘1’)
Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.9.2.3 **If** the CVM decision digit has any value among ‘2’, ‘3’ or ‘4’ (Signature, Online PIN, or On-Device CVM)
And the corresponding CVM is not supported in the *Terminal Interchange Profile (dynamic)*
Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.9.3 Transaction Outcome

The Outcome is set for ***Online Request***, with the parameters indicating the CVM requirement (if any). The data elements for a Magstripe online authorisation are made available to the Reader.

Requirement – Transaction Outcome

3.9.3.1 The Kernel shall provide an ***Online Request*** Outcome as defined in section 3.13.2.

3.9.3.2 The CVM parameter in the ***Online Request*** Outcome shall be the result of CVM Processing as specified in section 3.9.2.

3.9.3.3 The Message Identifier parameter in the ***Online Request*** Outcome (UI Request on Outcome Present) shall take the following value:

If CVM = Online PIN,
Then Message Identifier = ‘09’ (“Please enter your PIN”),
Else Message Identifier = ‘1B’ (“Authorising, please wait”)

3.10 Completion – Legacy Mode

If the transaction is to be processed as per 'Legacy Mode', the Kernel will request the card to return an Authorisation Request Cryptogram (ARQC) by sending a GENERATE AC command with the data requested in the CDOL1 obtained during READ RECORD processing. No CDA signature is required.

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

3.10.1 GENERATE AC Command

The CDOL1 used to prepare the GENERATE AC command is obtained during READ RECORD processing.

Requirement – CDOL1 Processing	
3.10.1.1	The Kernel shall process the CDOL1 and construct the command data for the GENERATE AC command, as described in *[EMV Book 3]*.
3.10.1.2	**If** the CDOL1 requests a data element that is not recognised by the Kernel (i.e. not referenced in Annex B), **Then** the Kernel shall fill in the corresponding CDOL1 related data with zeroes.

Requirement – GENERATE AC	
3.10.1.3	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 Book 3]*.
3.10.1.4	**If** the Status Word returned by the card is different from '9000', **Then** the Kernel shall terminate the transaction with a ***Select Next*** Outcome as defined in section 3.13.10.

Requirement – GENERATE AC

3.10.1.5 The Kernel shall ensure that the card response is correctly formatted (see section 4.2).

If the response to the GENERATE AC command is not parsed correctly,
Or if a mandatory data element is missing,
Or if the format of a returned data element is incorrect,

Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.10.1.6 **If** the Cryptogram Information Data (Tag '9F27') does not indicate an ARQC,
Then the terminal shall decline the transaction as defined in section 3.13.5.

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.

3.10.2 CVM Processing

If a CVM is required according to the result of CVM Required Limit Check, the Kernel evaluates the CVM list contained in the data records and determines the appropriate CVM parameter setting for the Outcome. Kernel 5 CVM processing is a simplified version of CVM list processing defined in *[EMV Book 3]* using only the CVM Code. The CVM Condition byte is not evaluated.

Requirement – CVM Required Check

3.10.2.1 **If** the 'CVM required by reader' indicator is set to 1 in the dynamic Terminal Interchange Profile (Tag '9F53'),
Then the Kernel shall evaluate the CVM List obtained from the data records.

Otherwise processing shall continue with ***Online Request*** Outcome (section 3.10.3), with CVM parameter set to "No CVM".

Requirement – CVM Evaluation

3.10.2.2 **If** the CVM List is absent from the card,
Then the Kernel shall assume the CVM to be Not Applicable (no CVM preference).

3.10.2.3 **If** the CVM List is provided by the card,
Then the Kernel shall examine the CVM Codes in the CVM List (Tag '8E') in sequential order, comparing the static Terminal Interchange Profile flags (‘Signature supported’ and ‘Online PIN supported’) with the CVM Code values for ‘Enciphered PIN verified online’ and ‘Signature (paper)’, as defined in *[EMV Book 3]*, Table 39.

The first positive comparison in the list shall determine the CVM requirement for the transaction.

3.10.2.4 **If** no match is found after processing requirement 3.10.2.3,
Then the Kernel shall decline the transaction as defined in section 3.13.5.

3.10.3 Online Request Outcome

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

Requirement – Online Request Outcome

3.10.3.1 The Kernel shall complete the transaction with an ***Online Request*** Outcome as defined in section 3.13.2.

3.10.3.2 The CVM parameter in the ***Online Request*** Outcome shall be the result of CVM Processing as specified in section 3.10.2.

3.10.3.3 The Message Identifier parameter in the ***Online Request*** Outcome (UI Request on Outcome Present) shall take the following value:

If CVM = Online PIN
Then Message Identifier = ‘09’ (“Please enter your PIN”)
Else Message Identifier = ‘1B’ (“Authorising, please wait”)

3.11 Issuer Update Processing

Issuer Update enables the Issuer to take advantage of a transaction authorisation message to perform remote maintenance operations on the card – typically Issuer Authentication enabling counter reset, or Issuer Scripts enabling updating card parameters.

The card must either be maintained in the RF field for the duration of the authorisation request, or be represented to the reader when the online response is received.

This section is performed when the Kernel is restarted after an Online Authorisation to execute Issuer Update, provided that all the conditions below are fulfilled:

- The Kernel supports Issuer Update (implementation option)
- The selected Combination supports Issuer Update (acquirer option)
- The card has returned an ARQC in answer to the first GENERATE AC command, with an Issuer Update Parameter requesting “Present-and-hold” (‘01’) or “Two Presentment” (‘02’) behaviour
- The Authorisation Response message contains Issuer Authentication Data (Tag ‘91’) and/or Issuer Script(s) (Templates ‘71’ and/or ‘72’)

When activated again to process Issuer Update, the Kernel restores the *Online Transaction Context* for the ongoing transaction that was retained before the online authorisation request.

3.11.1 Issuer Update Initialisation

Requirement – SELECT response analysis

3.11.1.1 **If** the FCI has been provided by the reader as part of the Dynamic Transaction Parameters (case of “Two Presentment”)

And the FCI is not parsed correctly (see table 45 in *[EMV Book 1]*),

Then the Kernel shall complete the transaction by returning an ***End Application*** Outcome as defined in Section 3.13.7.

3.11.2 Critical Script Processing

This requirement is performed when the Dynamic Transaction Parameters provided to the Kernel (see Table 3-2) contain at least one occurrence of Issuer Script Template 1 (tag '71'):

Requirement – Critical Script Processing

3.11.2.1 The Kernel shall process each occurrence of Issuer Script Template '71' sequencially, in the order provided by the terminal as part of the Dynamic Transaction Parameters. Each occurrence is processed as follows:

- The Kernel shall ensure that the Issuer Script Template can be parsed correctly, according to the format described in *[EMV Book 3]*, Section 10.10.

  If the parsing is incorrect

  Then the Kernel shall:

  - set TVR[6] Byte 5 bit 6 to '1' ('Script processing failed before final GENERATE AC'),
  - proceed with the next '71' tag occurrence, if any.

- The Kernel shall deliver each command to the card as a command APDU in the sequence in which it appears in the Issuer Script.

  If the card returns an error SW to any script command (SW1 ≠ '90', '62' and '63')

  Then the Kernel shall:

  - terminate the delivery of commands from this Issuer Script,
  - set TVR Byte 5, bit 6 to '1' ('Script processing failed before final GENERATE AC'),
  - proceed with the next '71' tag occurrence, if any.

[6] TVR is restored from *Online Transaction Context* and updated.

Note: the processing of Issuer Script is identical to the processing described for contact EMV kernels in *[EMV],* except that the Kernel does not generate the Transaction Status Information (TSI) nor Issuer Script Results. In particular, the following sections apply:

- *[EMV Book 3]*, Sections 10.10 and Annex E
- *[EMV Book 4]*, Sections 6.3.9 and 12.2.4

Requirement – Critical Script Processing Completion

3.11.2.2 Once all occurrences of Issuer Script Template '71' have been processed:

If the Dynamic Transaction Parameters provide neither Issuer Authentication Data (tag '91') nor Issuer Script Template 2 (tag '72')

Then the Kernel shall complete the transaction by returning an ***End Application*** Outcome as defined in Section 3.13.7.

Else the Kernel proceeds with Section 3.11.3.

Note: when the reader receives from the Kernel an ***End Application*** outcome following an Online restart, the terminal determines the transaction disposition according to the Authorisation Response Code provided by the Issuer (see Book A, Table 6-4 for the processing of the *End Application* outcome following an Online Request).

3.11.3 Second GENERATE AC Command

The requirements in this section are executed if Issuer Authentication Data (tag '91') or at least one occurrence of Issuer Script Template 2 (tag '72') is/are made available to the Kernel upon restart.

Requirement – CDOL2 Processing

3.11.3.1 The Kernel shall retrieve the CDOL2 value from the *Online Transaction Context* saved during the first part of the transaction.

If the CDOL2 is absent from the *Online Transaction Context* (i.e. the card has not provided any CDOL2 value)

Then the Kernel shall return an ***End Application*** Outcome as described in Section 3.13.7.

3.11.3.2 The Kernel shall process the CDOL2 and construct the command data for the GENERATE AC command, as described in *[EMV Book 3]*.

3.11.3.3 **If** the CDOL2 requests a Data Object that is not recognised by the Kernel (not referenced in Annex B)
then the Kernel shall fill in the corresponding CDOL2 related data with zeroes.

Requirement – GENERATE AC

3.11.3.4 The Kernel shall request the card to generate a cryptogram using the GENERATE APPLICATION CRYPTOGRAM command as defined in Section 4.2 and *[EMV Book 3]*.

The type of cryptogram (TC or AAC) requested by the Kernel in the Reference Control Parameter (parameter P1) depends on the Authorisation Response Code (ARC, tag ‘8A’) provided by the terminal:

> **If** the ARC value corresponds to an Approval (“00”, “10”, “11”) or a Referral (“01”, “02”),
> **Then** an approval (TC) shall be requested;
> **Else** a decline (AAC) shall be requested.

3.11.3.5 The Kernel shall *not* request any CDA Signature in the Reference Control Parameter (bit 5 is set to ‘0’).

At this stage the Kernel needs to analyse the GENERATE AC response.

Requirement – GENERATE AC Response Analysis	
3.11.3.6	**If** the Status Word returned by the card is different from '9000' **Then** the Kernel shall return an ***End Application*** Outcome as described in Section 3.13.7.
3.11.3.7	**If** the response to the GENERATE AC command is not parsed correctly, **Or** if a mandatory data element is missing (see Table 4-6), **Or** if the format of a returned data element is incorrect, **Then** the Kernel shall return a ***Declined*** Outcome as defined in section 3.13.7.

3.11.4 Transaction Outcome

The Outcome is set for ***Approved*** or ***Declined***, as per the card decision to the second GENERATE AC command, with the parameters indicating the CVM requirement (if any). The data elements for an EMV clearing record are made available to the reader.

Requirement – Transaction Outcome	
3.11.4.1	**If** the Cryptogram Information Data (Tag '9F27') returned to the second GENERATE AC indicates an AAC **Then** the Kernel shall prepare a ***Declined*** Outcome as defined in section 3.13.5.
3.11.4.2	**If** the Cryptogram Information Data (Tag '9F27') returned to the second GENERATE AC indicates a TC, **Then** the Kernel shall prepare an ***Approved*** Outcome as defined in section 3.13.1.
3.11.4.3	The Kernel shall retrieve the CVM parameter from the *Online Transaction Context*. **If** the value retrieved is equal to Online PIN **Then** the CVM parameter in the ***Approved*** Outcome shall be set to Not Applicable **Else** the CVM parameter in the ***Approved*** Outcome is equal to the value in the *Online Transaction Context*.

Requirement – Transaction Outcome

3.11.4.4 The Message Identifier parameter in the ***Approved*** Outcome (UI Request on Outcome Present) shall take the following value:

If CVM = Obtain Signature
Then Message Identifier = ‘1A’ (“Approved, please sign”)
Else Message Identifier = ‘03’ (“Approved”)

3.11.4.5 The EMV Data Record (see Annex C) provided with the Approved Outcome is populated as follows:

- Cryptogram Information Data (‘9F27’), ATC (‘9F36’), Application Cryptogram, Issuer Application Data (‘9F10’) are the values returned by the card to the second GENERATE AC command
- TVR (‘95’) is the value updated during Issuer Update Processing
- Other data elements are recovered from the *Online Transaction Context.*

3.11.4.6 **If** the Dynamic Transaction Parameters provide at least one occurrence of Issuer Script Template 2 (tag ‘72’)

Then the Kernel shall proceed with Section 3.11.5

Else the Kernel shall return the prepared Transaction Outcome.

3.11.5 Non-critical Script Processing

The Requirement below is executed when the Dynamic Transaction Parameters provided to the Kernel (see Table 3-2) for restart contain at least one occurrence of Issuer Script Template 2 (tag ‘72’):

Requirement – Non-critical Script Processing

3.11.5.1 The Kernel shall process each occurrence of Issuer Script Template ‘72’ sequencially, in the order provided by the terminal as part of the Dynamic Transaction Parameters. Each occurrence is processed as follows:

- The Kernel shall ensure that the Issuer Script Template can be parsed correctly, according to the format described in *[EMV Book 3]*, Section 10.10.

  If the parsing is incorrect

  Then the Kernel shall:

  - update TVR Byte 5 bit 5 to ‘1’ (‘Script processing failed after final GENERATE AC’) in the Transaction Outcome
  - proceed with the next ‘72’ tag occurrence, if any.

- The Kernel shall deliver each command to the card as a command APDU in the sequence in which it appears in the Issuer Script.

  If the card returns an error SW to any script command (SW1 ≠ ’90’, ‘62’ and ‘63’)

  Then the Kernel shall:

  - terminate the delivery of commands from this Issuer Script,
  - update TVR Byte 5, bit 5 to ‘1’ (‘Script processing failed after final GENERATE AC’) in the Transaction Outcome
  - proceed with the next ‘72’ tag occurrence, if any.

Requirement – Non-critical Script Processing Completion

3.11.5.2 Once all occurrences of Issuer Script Template ‘72’ have been processed, the Kernel shall complete the transaction by returning the Transaction Outcome prepared in Section 3.11.4.

3.12 Error Handling

3.12.1 Processing Errors

Unless otherwise specified in the relevant transaction paragraph above, the requirements in this section apply.

Processing errors for Completion (all modes) and Issuer Update are subject to specific processing; please refer to the relevant sections (3.8 to 3.11).

Requirements – Processing Errors - Default

3.12.1.1 **If** the status bytes returned in the response to any command are different from '9000' or other acceptable values as defined in section 4,
Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as defined in section 3.13.10.

3.12.1.2 **If** the response to a command is not parsed correctly as defined for the command in section 4,
Or if a mandatory data element is missing,
Or if the format of a returned data element is incorrect,
Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as defined in section 3.13.10.

This rule includes (but is not limited to) the data format errors listed in *[EMV Book 3]* Section 7.5.

3.12.2 Communication Errors

Requirement – Communication Errors – General

3.12.2.1 **If** a Transmission, Protocol, or Timeout error as defined in Book D is reported to the Kernel,
Then the Kernel shall terminate the transaction and provide an ***End Application (with restart – Communication errors)*** Outcome as described in section 3.13.8.

Requirement – Communication Errors – First GENERATE AC

3.12.2.2 **If** a Transmission, Protocol, or Timeout error as defined in Book D is reported to the Kernel during the first GENERATE APPLICATION CRYPTOGRAM command of a transaction in EMV Mode,
Then the Kernel shall prepare the *Recovery Context* as follows:

- Set indicator *'Recovering from Torn EMV Transaction'* to value TRUE;
- Store the card Track 2 Equivalent Data value (Tag '57') into variable *'Torn Track 2 Data'*;
- **If** CDA has been requested by the Kernel, concatenate in this order and store in variable '*Torn CDA Hash Data Buffer*'
  - o The values of the data elements specified by, and in the order they appear in the PDOL, and sent by the Kernel in the GET PROCESSING OPTIONS command
  - o The values of the data elements specified by, and in the order they appear in the CDOL1, and sent by the Kernel in the GENERATE AC command

3.12.2.3 The Reader shall retain the Recovery Context and make it available to the Kernel for the next Kernel Activation.

The Kernel shall terminate the transaction and provide an ***End Application (with restart – Communication errors)*** Outcome as described in section 3.13.8.

Requirement – Communication Errors – Issuer Updates

3.12.2.4 **If** a Transmission, Protocol, or Timeout error as defined in Book D is reported to the kernel while executing:

- o critical Issuer Script commands (see Section 3.11.2)
- o the second GENERATE AC command (see Section 3.11.3)

Then the Kernel shall return an ***End Application*** Outcome as defined in Section 3.13.7.

Requirement – Communication Errors – Issuer Updates

3.12.2.5 **If** a Transmission, Protocol, or Timeout error as defined in Book D is reported to the Kernel while executing non-critical Issuer Script commands (see Section 3.11.5),

Then the Kernel shall return the Transaction Outcome as previously determined in Section 3.11.4 after the second GENERATE AC command.

3.12.3 Transaction Cancellation

The Kernel may receive at any time a transaction cancellation order initiated by the Merchant (attended terminal) or by the Cardholder (unattended terminal).

Requirement – Transaction cancellation by Reader

3.12.3.1 The Kernel shall be capable of receiving a cancellation order from the reader at any time during transaction processing.

3.12.3.2 **If** a cancellation order is received from the reader
Then the Kernel shall:
- clear all internal Kernel variables
- terminate the transaction and provide an ***End Application*** Outcome as defined in section 3.13.7.

3.13 Transaction Outcomes

3.13.1 Approved

Requirement – Approved Outcome

3.13.1.1 The Kernel shall make available to the POS system the data elements necessary for an offline clearing record (cf. Annex C).

Requirement – Approved Outcome

3.13.1.2 The Kernel shall provide an ***Approved*** Outcome with the following parameters:

Approved:

- **Start:** N/A
- **Online Response Data:** N/A
- **CVM:** No CVM/ Obtain Signature/ Confirmation Code Verified/ Online PIN, as applicable
- **UI Request on Outcome Present:** Yes

  Message Identifier: as applicable
  '03' (“Approved”)
  '1A' (“Approved – Please Sign”)

  Status: Card Read Successfully

  [Value Qualifier: “Balance”][7]

  [Value: Offline Balance (Tag ‘9F5F’) returned by card]

  [Currency Code: Transaction Currency Code]
- **UI Request on Restart Present:** No
- **Data Record Present:** Yes

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

[7] Parameters in brackets ***[ ]*** are provided only if the card has returned the Offline Balance (Tag ‘9F5F’) in the GENERATE AC response (EMV Mode only)

3.13.2 Online Request

Requirement – Online Request Outcome	
3.13.2.1	The Kernel shall prepare the data record for an online request record (cf. Annex C) and make it available to the POS system.

Requirement – Online Request Outcome

3.13.2.2 The Kernel shall provide an ***Online Request*** Outcome with the following parameters:

Online Request:

- **Start:** N/A
- **Online Response Data:** N/A
- **CVM:** No CVM/ Obtain Signature/ Confirmation Code Verified/ Online PIN, as applicable
- **UI Request on Outcome Present:** Yes

  Message Identifier: as applicable:
  '1B' ("Authorising, Please Wait")
  '09' ("Please enter your PIN")

  Status: Card Read Successfully

  [*Value Qualifier: "Balance"****]***[8]

  [*Value: Offline Balance (Tag '9F5F') returned by card* ***]***

  [*Currency Code: Transaction Currency Code****]***

- **UI Request on Restart Present:** No
- **Data Record Present:** Yes

  The minimum data requirements for online authorisation records are specified in Annex C. Data requirements depend on the Transaction Mode.

- **Discretionary Data Present:** No
- **Alternate Interface Preference:** N/A
- **Receipt:** N/A
- **Field Off Request:** N/A
- **Removal Timeout:** Zero

[8] Parameters in brackets ***[ ]*** are provided only if the card has returned the Offline Balance (Tag '9F5F') in the GENERATE AC response (EMV Mode only)

3.13.3 Online Request (“Two Presentments”)

Requirement – Online Request Outcome (“Two Presentments”)

3.13.3.1 The Kernel shall prepare the data record for an online request record (cf. Annex C) and make it available to the POS system.

Requirement – Online Request Outcome ("Two Presentments")

3.13.3.2 The Kernel shall provide an ***Online Request*** Outcome with the following parameters:

Online Request:

- **Start:** B
- **Online Response Data:** EMV Data
- **CVM:** No CVM/ Obtain Signature/ Confirmation Code Verified/ Online PIN, as applicable
- **UI Request on Outcome Present:** Yes

  Message Identifier: as applicable:
  '1B' ("Authorising, Please Wait")
  '09' ("Please enter your PIN")

  Status: Card Read Successfully

  [Value Qualifier: "Balance"][9]

  [Value: Offline Balance (Tag '9F5F') returned by card]

  [Currency Code: Transaction Currency Code]
- **UI Request on Restart Present:** Yes

  Message Identifier: '21' ("Present Card Again")
  Status: Ready to Read
- **Data Record Present:** Yes

  The minimum data requirements for online authorisation records are specified in Annex C. Data requirements depend on the Transaction Mode.
- **Discretionary Data Present:** No
- **Alternate Interface Preference:** N/A
- **Receipt:** N/A
- **Field Off Request:** N/A
- **Removal Timeout:** Zero

[9] Parameters in brackets ***[ ]*** are provided only if the card has returned the Offline Balance (Tag '9F5F') in the GENERATE AC response (EMV Mode only)

3.13.4 Online Request ("Present and Hold")

Requirement – Online Request Outcome ("Present and Hold")	
3.13.4.1	The Kernel shall prepare the data record for an online request record (cf. Annex C) and make it available to the POS system.

Requirement – Online Request Outcome ("Present and Hold")

3.13.4.2 The Kernel shall provide an ***Online Request*** Outcome with the following parameters:

Online Request:

- **Start:** D
- **Online Response Data:** Any
- **CVM:** No CVM/ Obtain Signature/ Confirmation Code Verified, as applicable / Online PIN
- **UI Request on Outcome Present:** Yes

  Message Identifier: as applicable:
  '1B' ("Authorising, Please Wait")
  '09' ("Please enter your PIN")

  Status: Processing

  [*Value Qualifier: "Balance"****]***[10]

  [*Value: Offline Balance (Tag '9F5F') returned by card* ***]***

  [*Currency Code: Transaction Currency Code****]***
- **UI Request on Restart Present:** Yes

  Message Identifier: '16' ("Processing")
  Status: Processing
- **Data Record Present:** Yes

  The minimum data requirements for online authorisation records are specified in Annex C. Data requirements depend on the Transaction Mode.
- **Discretionary Data Present:** No
- **Alternate Interface Preference:** N/A
- **Receipt:** N/A
- **Field Off Request:** N/A
- **Removal Timeout:** Removal Timeout (static Kernel configuration parameter, see Table 3-1)

[10] Parameters in brackets ***[ ]*** are provided only if the card has returned the Offline Balance (Tag '9F5F') in the GENERATE AC response (EMV Mode only)

3.13.5 Declined

Requirement – Declined Outcome

3.13.5.1 The Kernel shall provide a ***Declined*** Outcome with the following parameters:

Declined:

- **Start:** N/A
- **Online Response Data:** N/A
- **CVM:** N/A
- **UI Request on Outcome Present:** Yes

  Message Identifier: '07' ("Not Authorised")

  Status: Card Read Successfully

  [Value Qualifier: "Balance"][11]

  [Value: Offline Balance (Tag '9F5F') returned by card]

  [Currency Code: Transaction Currency Code]
- **UI Request on Restart Present:** No
- **Data Record Present:** Yes

  The minimum data requirements for records associated to a *Declined* Outcome are specified in Annex C.
- **Discretionary Data Present:** No
- **Alternate Interface Preference:** N/A
- **Receipt:** N/A
- **Field Off Request:** N/A
- **Removal Timeout:** Zero

[11] Parameters in brackets ***[ ]*** are provided only if the card has returned the Offline Balance (Tag '9F5F') in the GENERATE AC response (EMV Mode only)

3.13.6 Try Another Interface

Requirement – Try Another Interface Outcome

3.13.6.1 The Kernel shall provide a ***Try Another Interface*** Outcome with the following parameters:

Try Another Interface :

- **Start:** N/A
- **Online Response Data:** N/A
- **CVM:** N/A
- **UI Request on Outcome Present:** Yes

  Message Identifier: '1D' ("Please insert card")

  Status: Ready to Read
- **UI Request on Restart Present:** No
- **Data Record Present:** No
- **Discretionary Data Present:** No
- **Alternate Interface Preference:** Contact Chip
- **Receipt:** N/A
- **Field Off Request:** N/A
- **Removal Timeout:** Zero

3.13.7 End Application

Requirement – End Application

3.13.7.1 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:** 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

Notes:

- When this Outcome is returned as a first Final Outcome (e.g. transaction cancellation by reader), the POS System determines the transaction disposition as “Terminated” and advises the cardholder of the situation.
- When this Outcome is returned as a second Final Outcome (i.e. following an Online Restart “present and hold” or “two presentments”), the POS System determines the final transaction disposition based on the online authorisation response from the Issuer, and indicates the final transaction disposition to the cardholder.

See *Book A*, Section 6.3 for further details.

3.13.8 End Application (with restart – communication error)

Requirement – Communication Errors

3.13.8.1 **If** the Kernel is informed of a contactless communication error, **Then** the Kernel shall provide an ***End Application*** Outcome with the following parameters:

End Application:

- **Start:** B
- **Online Response Data:** N/A
- **CVM:** N/A
- **UI Request on Outcome Present:** Yes

  Message Identifier: '21' ("Present Card Again")

  Status: Processing Error

  Hold Time: 13
- **UI Request on Restart Present:** Yes

  Message Identifier: '21' ("Present Card Again")
- Status: Ready to Read**Data Record Present:** No
- **Discretionary Data Present:** No
- **Alternate Interface Preference:** N/A
- **Receipt:** N/A
- **Field Off Request:** N/A
- **Removal Timeout:** Zero

3.13.9 End Application (with restart - On-Device CVM)

Requirement – On-Device CVM to be Performed

3.13.9.1 **If** the Kernel is informed that the transaction shall be reattempted to allow entry of a Confirmation Code into a mobile device,
Then the Kernel shall provide an ***End Application*** Outcome with the following parameters:

End Application:

- **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

  Message Identifier: '21' (“Present Card Again”)

  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

3.13.10 Select Next

Requirement – Select Next

3.13.10.1 The Kernel shall provide a ***Select Next*** Outcome with the following parameters:

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

3.14 Torn Transaction Recovery

When a transaction performed in EMV mode is torn during the execution of the first GENERATE AC command, it may be preferable to have the card repeat its last GENERATE AC response (when available), instead of relaunching a new transaction.This method reduces the impact of tearing on the cards, especially when the card supports an offline stored value.

This section describes the sequence of requirements to follow in order to recover from a torn transaction in EMV Mode.

The torn transaction recovery is successful when the same card is re-presented after the torn transaction, and the card accepts the recovery (ECHO command).

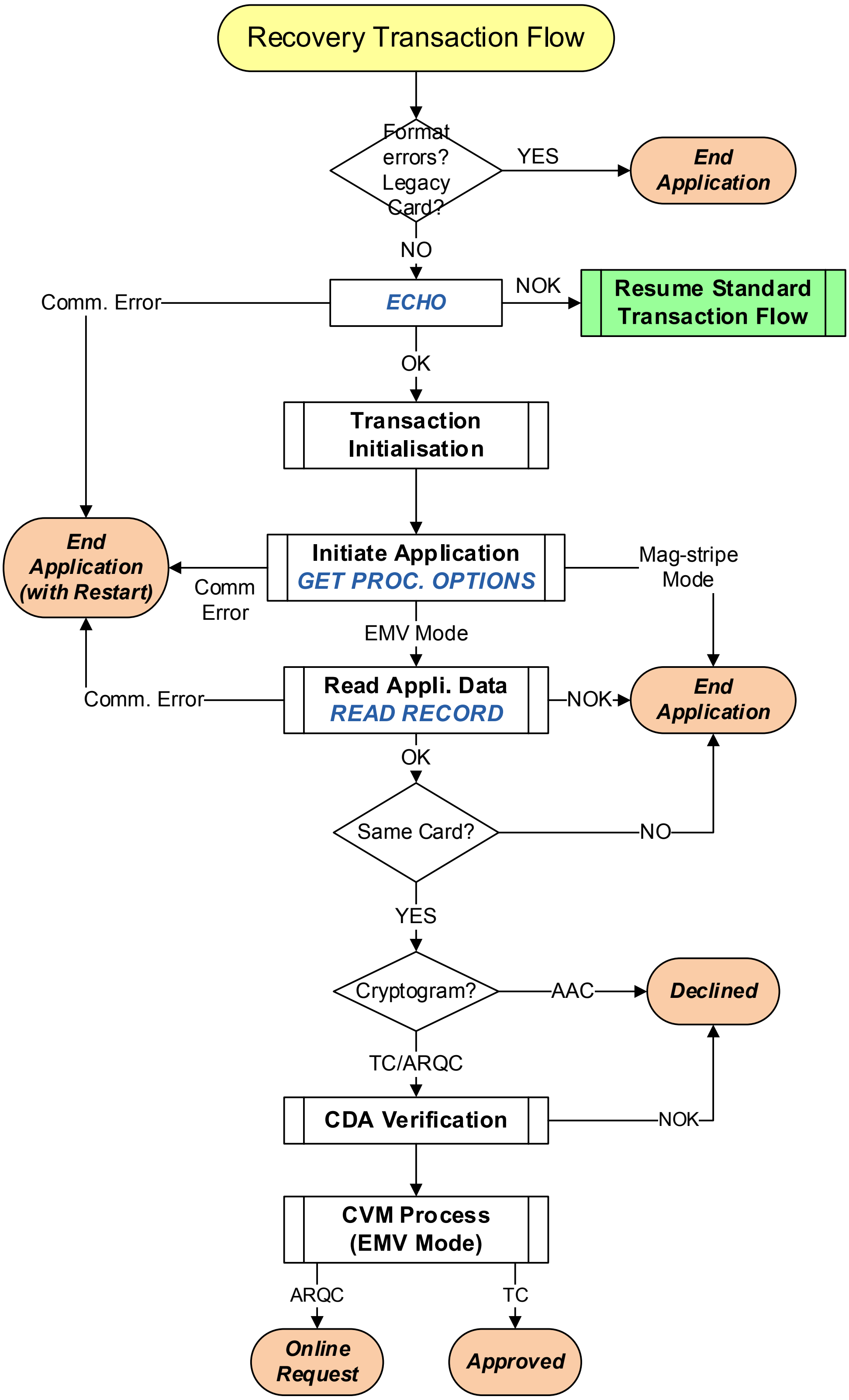
If the Kernel detects by any means that a different card is presented, the transaction is abandoned.

If the card is unable to process the ECHO command (function is deactivated, or transaction tearing has occurred before the card could save the transaction context), the Kernel resumes a regular transaction flow.

Payment applications on the card are designed to process the ECHO command only once. If another communication error occurs during the transaction recovery flow, cardholder is prompted to present the card again for a regular transaction flow.

Figure 3-1 provides an overview of the recovery transaction flow as well as the links to the standard transaction flow.

Figure 3-1 – Overview of the Recovery Transaction Flow



3.14.1 SELECT Response Analysis

If the card SELECT response does not parse correctly, or the Kernel recognised the card as a legacy card, this indicates that the represented card is not the same as in the first presentment. The recovery transaction is rejected:

Requirement – SELECT Response Analysis

3.14.1.1 **If** the FCI is absent,
Or if the FCI is not parsed correctly (see table 45 in *[EMV Book 1]*),
Or if the PDOL data element is absent, or present but empty
Then the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an ***End Application*** Outcome as described in Section 3.13.7.

3.14.1.2 **If** the card does not request the Terminal Compatibility Indicator (Tag '9F52') in the PDOL (legacy card)
Then the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an ***End Application*** Outcome as described in Section 3.13.7.

3.14.2 ECHO Command

Requirement – ECHO Command

3.14.2.1 The Kernel shall issue the ECHO command as described in section 4.1.

3.14.2.2 **If** the card returns a Status Word different from '9000'
Then the Kernel shall reset the Recovery Context as defined in section 3.14.7 and resume with a normal transaction flow from Requirement 3.2.1.5 onwards.

3.14.2.3 If a transmission, protocol, or timeout error is detected during processing of the ECHO command,
Then the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an End Application (with restart – Communication error) Outcome as described in Section 3.13.8.

3.14.3 Transaction Initialisation

Requirement – Transaction Initialisation	
3.14.3.1	The Kernel shall initialise the transaction data by applying Requirements 3.2.1.5 through 3.2.1.8.

3.14.4 Initiate Application Processing

Requirement – Initiate Application	
3.14.4.1	The Kernel shall initiate the application as described in section 3.3. Note: the SW returned in case of successful processing during a recovery transaction (warning SW=6200) differs from the SW returned for a regular transaction (SW=9000).
3.14.4.2	**If** a transmission, protocol, or timeout error is detected in the GET PROCESSING OPTIONS response, **Then** the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an ***End Application (with restart – Communication error)*** Outcome as described in Section 3.13.8.
3.14.4.3	**If** the result of Initiate Application (as per section 3.3) is a ***Select Next*** outcome, **Then** the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an ***End Application*** Outcome as described in Section 3.13.7.

If the AIP indicates that the card has selected the Magstripe Mode, recovery of the previously torn EMV transaction is impossible. This indicates that the cardholder has probably changed the faulty card for another one. The recovery transaction is rejected.

Requirement – Magstripe Mode Filtering	
3.14.4.4	**If** the Transaction Mode is set to 'Magstripe Mode' **Then** the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an ***End Application*** Outcome as described in Section 3.13.7.

3.14.5 Read Application Data

Requirement – Read Application Data	
3.14.5.1	The Kernel shall read the application data as described in section 3.4.
3.14.5.2	**If** a transmission, protocol or timeout error is detected in any of the READ RECORD response, **Then** the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an ***End Application (with restart – Communication error)*** Outcome as described in Section 3.13.8.
3.14.5.3	**If** the result of Read Application Data (as per section 3.4) is a ***Select Next*** outcome, **Then** the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an ***End Application*** Outcome as described in Section 3.13.7.

Transaction Recovery can occur only if the card presented for the first – torn – transaction is the same as the card presented for recovery. Thus the Kernel compares the card account data from both transactions.

Requirement – Account Data Verification

3.14.5.4 The Kernel shall compare the Track 2 Equivalent Data value (Tag '57') retrieved during 3.14.5.1 with the *'Torn Track 2 Data'* from the Recovery Context.

If the value of Track 2 Equivalent Data is not equal to the value of 'Torn Track 2 Data'
Then the Kernel shall reset the Recovery Context as defined in section 3.14.7 and provide an ***End Application*** Outcome as described in Section 3.13.7.

3.14.6 Transaction Recovery Completion

Requirement – Transaction Recovery Completion

3.14.6.1 The Kernel shall reset the Recovery Context as defined in section 3.14.7.

3.14.6.2 The Kernel shall proceed with CDA verification (when dynamic signature is returned) and transaction completion, from Requirement 3.8.1.8 onwards, with the following adjustments:

- the response to the GENERATE APPLICATION CRYPTOGRAM command is replaced by the response to the ECHO command
- verification of the CDA signature (requirement 3.8.2.1): the Transaction Data Hash Code is created by the concatenation in this order of:
  - the *'Torn CDA Hash Data Buffer'*
  - the tags, lengths, and values of the data elements returned by the card in the response to the ECHO command in the order they are returned - with the exception of the Signed Dynamic Application Data.

3.14.7 Reset Recovery Context

Requirement – Reset Recovery Context

3.14.7.1 The Kernel shall reset the Recovery Context as follows:

- reset the internal indicator *'Recovering from Torn EMV Transaction'* to value 'FALSE'
- reset the *'Torn Track 2 Data'* value (to zeroes)
- reset the *'Torn CDA Hash Data Buffer'* value (to zeroes)

4 APDU command description

This section describes the APDU command-response pairs that are used by the Kernel during the transaction flow. These commands are summarized in below:

Table 4-1: List of APDU commands used by the Kernel

CLA	INS	Meaning	Requirement
‘80’	‘DF’	ECHO	Conditional – if EMV Mode is supported as an implementation option
‘80’	‘AE’	GENERATE APPLICATION CRYPTOGRAM	Conditional – if EMV Mode and/or Legacy Mode is supported as an implementation option
‘80’	‘D0’	GET MAGSTRIPE DATA	Mandatory
‘80’	‘A8’	GET PROCESSING OPTIONS	Mandatory
‘00’	‘B2’	READ RECORD	Mandatory
‘00’	‘A4’	SELECT	Mandatory

4.1 ECHO

Definition and Scope

The ECHO command is used by the Kernel to retrieve the latest GENERATE APPLICATION CRYPTOGRAM response produced by the card.

It is used when the Kernel attempts to recover from a torn transaction in EMV Mode.

Command Message

The ECHO command message is coded as shown in Table 4-2:

Table 4-2: ECHO Command Message

Code	Value
CLA	‘80’
INS	‘DF’
P1	‘00’
P2	‘00’
Lc	Not present
Data	Not present
Le	‘00’

Data Field Sent in the Command Message

The data field of the command message is not present.

Data Field Returned in the Response Message

In case of successful execution of the command, the response data is identical to the response data generated by the card during the latest GENERATE APPLICATION CRYPTOGRAM command.

Further details can be found in Section 4.2.

Processing State Returned in the Response Message

- '9000' indicates a successful execution of the command.

- ‘6985’ may indicate any of the following reasons:
    - The command is not supported by the card,
    - No recovery response is available from the card
    - The ECHO command has already been played once for this transaction, and cannot be replayed any longer

4.2 First GENERATE APPLICATION CRYPTOGRAM

Definition and Scope

The GENERATE APPLICATION CRYPTOGRAM command is used to complete a transaction executed in EMV Mode or in Legacy Mode.

To a great extent, it inherits its scope and format from the same command defined in *[EMV Book 3].*

Command Message

The GENERATE APPLICATION CRYPTOGRAM command is coded as described in *[EMV Book 3]* Section 6.5.5.

Data Field Sent in the Command Message

As described in *[EMV Book 3]*, the command data consists of the CDOL1 related data. For further details, please refer to *[EMV Book 3]* Section 5.4.

Data Field Returned in the Response Message

The response data is formatted as described in *[EMV Book 3]* Section 6.5.5, with the following additional specificities:

- **Legacy Mode**: Response data is returned as per Format 1 (the data object returned in the response message is a primitive data object with tag equal to '80')
- **EMV Mode**: Response data is returned as per Format 2 (the data object returned in the response message is a constructed data object with tag equal to '77'.). The data elements present in the response depend on the type of cryptogram returned by the card.

Table 4-3: EMV Mode - Data Objects Included in Response to First GENERATE AC for [TC returned] or [ARQC returned, CDA requested]

Tag	Length	Description	Presence
'9F27'	1	Cryptogram Information Data	M
'9F36'	2	Application Transaction Counter	M
'9F4B'	N_{IC}	Signed Dynamic Application Data	M

Tag	Length	Description	Presence
‘9F50’	1	Cardholder Verification Status	M
'9F10'	Var. up to 32	Issuer Application Data	O
‘9F5F’	6	Offline Balance	O
‘9F60’	1	Issuer Update Parameter	O

Table 4-4: EMV Mode - Data Objects Included in Response to First GENERATE AC for [ARQC returned, CDA not requested]

Tag	Length	Description	Presence
'9F27'	1	Cryptogram Information Data	M
'9F36'	2	Application Transaction Counter	M
'9F26'	8	Application Cryptogram (ARQC)	M
‘9F50’	1	Cardholder Verification Status	M
'9F10'	Var. up to 32	Issuer Application Data	O
‘9F5F’	6	Offline Balance	O
‘9F60’	1	Issuer Update Parameter	O

Table 4-5: EMV Mode - Data Objects Included in Response to First GENERATE AC for [AAC returned]

Tag	Length	Description	Presence
'9F27'	1	Cryptogram Information Data	M
'9F36'	2	Application Transaction Counter	M
'9F26'	8	Application Cryptogram (AAC)	M
'9F10'	Var. up to 32	Issuer Application Data	O
‘9F5F’	6	Offline Balance	O

Processing State Returned in the Response Message

- '9000' indicates a successful execution of the command.
- ‘6984’ indicates that the card prefers to conduct the transaction using the contact chip interface
- ‘6985’ indicates that the conditions of use are not satisfied.
- ‘6986’ indicates that On-device Cardholder Verification is required (e.g. PIN code shall be entered on mobile device)
- ‘6A80’ indicates that the command is badly formatted.

4.3 Second GENERATE APPLICATION CRYPTOGRAM

Definition and Scope

The Second GENERATE APPLICATION CRYPTOGRAM command may be required during Issuer Update Processing for a transaction executed in EMV Mode.

To a great extent, it inherits its scope and format from the same command defined in *[EMV Book 3].*

Command Message

The GENERATE APPLICATION CRYPTOGRAM command is coded as described in *[EMV Book 3]* Section 6.5.5.

Data Field Sent in the Command Message

As described in *[EMV Book 3]*, the command data consists of the CDOL2 related data. For further details, please refer to *[EMV Book 3]* Section 5.4.

Data Field Returned in the Response Message

Response data is returned as per Format 2 (the data object returned in the response message is a constructed data object with tag equal to '77'.). The data elements present in the response depend on the type of cryptogram returned by the card.

Table 4-6: Data Objects Included in Response to Second GENERATE AC

Tag	Length	Description	Presence
'9F27'	1	Cryptogram Information Data	M
'9F36'	2	Application Transaction Counter	M
'9F26'	8	Application Cryptogram (TC/AAC)	M
'9F10'	Var. up to 32	Issuer Application Data	O
‘9F5F’	6	Offline Balance	O

Processing State Returned in the Response Message

- '9000' indicates a successful execution of the command.
- ‘6985’ indicates that the conditions of use are not satisfied.
- ‘6A80’ indicates that the command is badly formatted.

4.4 GET MAGSTRIPE DATA

Definition and Scope

The GET MAGSTRIPE DATA command is used to complete a transaction executed in Magstripe Mode.

The Kernel transmits the transaction context in the input data. The card analyses the transaction context, and returns the contents of Track 2 if it accepts to perform a transaction in Magstripe Mode.

The Track 2 information returned by the card may be a dynamic data element. In this case, the returned information also includes the decision of the card with regards to the Cardholder Verification Method to apply for the transaction.

Command Message

The GET MAGSTRIPE DATA command message is coded as shown inTable 4-7:

Table 4-7: GET MAGSTRIPE DATA Command Message

Code	Value
CLA	‘80’
INS	‘D0’
P1	‘80’: Online Requested ‘00’: Decline Requested
P2	‘00’
Lc	Var.
Data	Transaction-related data (MDOL-related data)
Le	‘00’

Data Field Sent in the Command Message

The command data consists of the Magstripe Data Object List (MDOL) related data.

For further details, please refer to *[EMV Book 3]* Section 5.4.

Data Field Returned in the Response Message

The response data is formatted as described in *[EMV Book 3]* Section 5.4, with the following additional specificities:

Table 4-8: Data Objects Included in Response to GET MAGSTRIPE DATA

Tag	Length	Description	Presence
'57'	Var. up to 19	Track 2 Equivalent Data	M

Processing State Returned in the Response Message

- '9000' indicates a successful execution of the command, card requests an online authorisation.
- ‘6300’ indicates a successful execution of the command, card declines the transaction. As this Status Word is a warning, the response data must be returned.
- ‘6985’ indicates that the conditions of use are not satisfied.
- ‘6986’ indicates that On-device Cardholder Verification is required (e.g. PIN code shall be entered on mobile device)
- ‘6A80’ indicates that the command is badly formatted.

4.5 GET PROCESSING OPTIONS

Definition and Scope

The GET PROCESSING OPTIONS command is used to initialise the transaction inside the card.

To a great extent, it inherits its scope and format from the same command defined in *[EMV Book 3].*

Command Message

See *[EMV Book 3]* Section 6.5.8.

Data Field Sent in the Command Message

See *[EMV Book 3]* Section 6.5.8.

Data Field Returned in the Response Message

The response data is formatted as described in *[EMV Book 3]* Section 6.5.8, with the following additional specificities:

- **Legacy Mode**: Response data is returned as per Format 1 (the data object returned in the response message is a primitive data object with tag equal to '80')
- **EMV Mode**: Response data is returned as per Format 2 (the data object returned in the response message is a constructed data object with tag equal to '77'.).
- **Magstripe Mode**: Response data is returned as per Format 2 (the data object returned in the response message is a constructed data object with tag equal to '77'.).

The data elements present in the response may depend on the Transaction Mode selected by the card, as can be seen from the Table 4-9 below.

The Kernel shall ignore data objects other than those described in this table that may be returned with Format 2.

Table 4-9: Data Objects Included in Response to GET PROCESSING OPTIONS

Tag (format 2 only)	Length	Description	Presence Legacy Mode	Presence EMV Mode	Presence Magstripe Mode
'82'	2	Application Interchange Profile (AIP)	M	M	M
'94'	Var.	Application File Locator (AFL)	M	M	O

Processing State Returned in the Response Message

- '9000' indicates a successful execution of the command during a normal transaction.
- ‘6200’ (warning) indicates a successful execution of the command during a torn transaction recovery.
- ‘6985’ indicates that the conditions of use are not satisfied.
- ‘6A80’ indicates that the command is badly formatted.

4.6 READ RECORD

Definition and Scope

See *[EMV Book 3]* Section 6.5.11.

Command Message

See *[EMV Book 3]* Section 6.5.11.

Data Field Sent in the Command Message

See *[EMV Book 3]* Section 6.5.11.

Data Field Returned in the Response Message

See *[EMV Book 3]* Section 6.5.11.

Processing State Returned in the Response Message

See *[EMV Book 3]* Section 6.5.11.

4.7 SELECT

Definition and Scope

See *[EMV Book 1]* Section 11.3.

Command Message

See *[EMV Book 1]* Section 11.3.

Data Field Sent in the Command Message

See *[EMV Book 1]* Section 11.3.

Data Field Returned in the Response Message

See *[EMV Book 1]* Section 11.3.

Processing State Returned in the Response Message

See *[EMV Book 1]* Section 11.3.

Annex A Coding of Data Elements Used in Transaction Flow

A.1 Application Interchange Profile (AIP)

Table A-1: Application Interchange Profile

AIP Byte 1 (Leftmost)

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

AIP Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								EMV Mode has been selected
0								Magstripe Mode has been selected
	1							OTA capable mobile device
		x	x	x	x	x	x	*Each bit RFU*

Note: cards using Legacy Mode have a value of zero for AIP Byte 2.

A.2 Cardholder Verification Status

Table A-2: Cardholder Verification Status

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								*RFU*
	0	0	0					No CVM required
	0	0	1					Signature (paper) is to be performed
	0	1	0					Enciphered PIN verified online is to be performed
	0	1	1					On-Device CVM has been successfully performed – method used is indicated in bits b4-b1
	1	0	0					*RFU*
	1	0	1					
	1	1	0					
	1	1	1					
				x	x	x	x	On-Device CVM performed: 0000b – No On-Device CVM performed 0001b – Confirmation Code entered on Mobile Device Other values - RFU

A.3 Combination Options

Table A-3: Combination Options

Combination Options Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								*RFU*
	1							Status Check supported
		1						Offline Data Authentication supported
			1					Exception File Check required[12]
				1				Random Transaction Selection supported
					0			*RFU*
						1		EMV Mode Supported[13]
							1	Legacy Mode Supported[14]

Combination Options Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	*Each bit RFU*

[12] Applies only if Exception File Check is supported as an Implementation Option

[13] Applies only if EMV Mode is supported as an Implementation Option

[14] Applies only if Legacy Mode is supported as an Implementation Option

A.4 CVM Results

Table A-4: CVM Results

CVM Results Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	CVM Performed: 00011111b – No CVM required 00111111b – No CVM performed 00011110b – Signature 00000010b – Online PIN 00000001b – Plaintext PIN verification performed by ICC or Confirmation Code entered on Mobile Device Other values – RFU

CVM Results Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	CVM Condition: 00000000b –always Other values – RFU

CVM Results Byte 3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	CVM Result: 00000000b –unknown 00000010b – successful Other values – RFU

Table A-5 shows the setting of CVM Results that correspond to each value of OUTCOME Parameter CVM.

Table A-5: Setting of CVM Results

OUTCOME Parameter CVM	CVM Results		
	Byte 1	Byte 2	Byte 3
No CVM	‘1F’ – No CVM required	‘00’	‘02’ – successful
Pbtain Signature	‘1E’ – Signature	‘00’	‘00’ –unknown
Online PIN	‘02’ – Online PIN	‘00’	‘00’ –unknown
Confirmation Code Verified	‘01’ – Plaintext PIN verification	‘00’	‘02’ – successful
N/A	‘3F’ – No CVM performed	‘00’	‘00’ –unknown

A.5 Issuer Update Parameter

Table A-6: Issuer Update Parameter

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x			*Each bit RFU*
						0	0	Issuer Update is not expected, card can be removed
						0	1	Issuer Update is expected, card shall be kept in RF field during authorisation process
						1	0	Issuer Update is expected, card shall be presented again if necessary after authorisation process
						1	1	*RFU*

A.6 Terminal Compatibility Indicator

Table A-7: Terminal Compatibility Indicator

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x			*Each bit RFU*
						1		EMV Mode Supported
							1	Magstripe Mode Supported

A.7 Terminal Interchange Profile (static/dynamic)

Table A-8: Terminal Interchange Profile

TIP Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								CVM required by reader / N/A[15]
	1							Signature supported
		1						Online PIN supported
			1					On-Device CVM supported
				0				*RFU*
					1			Reader is a Transit Reader
						1		EMV contact chip supported
							1	(Contact Chip) Offline PIN supported

TIP Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								Issuer Update supported[16]
	x	x	x	x	x	x	x	*Each bit* RFU

TIP Byte 3 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	*Each bit* RFU

[15] This bit is not applicable for the static Terminal Interchange Profile data element. It is dynamically set by Kernel 5 for the dynamic Terminal Interchange Profile data element.

[16] Applies only if Issuer Update is supported as an Implementation Option

Annex B Data Elements Dictionary

Table B-1: Data Elements Dictionary

Name	Description	Source	Presence	Format	Specified	Tag	Length
Acquirer Identifier	Uniquely identifies the acquirer within each payment system	Configuration (POS)	M	n 6-11	EMV	‘9F01’	6
Amount, Authorised (Numeric)	Authorised amount of the transaction. Requested in CDOL1.	POS	M	n 12	EMV	'9F02'	6
Amount, Other (Numeric)	Secondary amount associated with the transaction representing a cashback amount. Requested in CDOL1.	POS	M	n 12	EMV	'9F03'	6
Application Cryptogram (AC)	Cryptogram returned by the card in response of the GENERATE AC command	ICC	C	b	EMV	'9F26'	8
Application Currency Code	Indicates the currency in which the account is managed according to ISO 4217	ICC	O	n 3	EMV	‘9F42’	2
Application Effective Date	Date from which the application may be used	ICC	O	n 6	EMV	'5F25'	3
Application Expiration Date	Date after which application expires. It shall be present for EMV Mode and Legacy Mode.	ICC	C	n 6 YYMMDD	EMV	'5F24'	3
Application File Locator (AFL)	Indicates the location (SFI, range of records) of the AEFs related to a given application	ICC	C	var.	EMV	'94'	var. up to 252

Name	Description	Source	Presence	Format	Specified	Tag	Length
Application Interchange Profile (AIP)	Indicates the capabilities of the card to support specific functions in the application	ICC	M	b	Kernel 5 See A.1	'82'	2
Application Label	Mnemonic associated with the AID according to ISO/IEC 7816-5 (with the special character limited to space)	ICC	M	ans	EMV	'50'	1-16
Application Preferred Name	Preferred mnemonic associated with the AID	ICC	O	ans	EMV	'9F12'	1-16
Application Primary Account Number (PAN)	Valid cardholder account number	ICC	O	cn var. up to 19	EMV	'5A'	var. up to 10
Application Primary Account Number (PAN) Sequence Number	Identifies and differentiates cards with the same PAN	ICC	C	n 2	EMV	'5F34'	1
Application Priority Indicator	Indicates the priority of a given application or group of applications in a directory	ICC	O	b	EMV	‘87’	1
Application Transaction Counter (ATC)	Counter maintained by the application in the card (incrementing the ATC is managed by the card)	ICC	C	b	EMV	'9F36'	2
Application Usage Control	Indicates issuer‘s specified restrictions on the geographic usage and services allowed for the application	ICC	O	b	EMV	'9F07'	2
Authorisation Response Code	Code that defines the disposition of a message. ARC must be present if the Kernel is restarted after an Online Request Outcome.	Issuer	C	an2	EMV	‘8A’	2

Name	Description	Source	Presence	Format	Specified	Tag	Length
Card Risk Management Data Object List 1 (CDOL1)	List of data objects (tag and length) to be passed to the card in the first GENERATE AC command	ICC	M	b	EMV	'8C'	var. up to 252
Card Risk Management Data Object List 2 (CDOL2)	List of data objects (tag and length) to be passed to the card in the second GENERATE AC command	ICC	O	b	EMV	'8D'	var. up to 252
Cardholder Name	Indicates cardholder name according to ISO 7813	ICC	O	ans	EMV	'5F20'	2-26
Cardholder Verification Method (CVM) List	Identifies a method of verification of the cardholder supported by the application	ICC	C	b	EMV	'8E'	var. up to 252
Cardholder Verification Status	Indicates the CVM choice (already done or to be subsequently applied) for the transaction. Choice is made dynamically by card based on transaction context and card risk management configuration.	ICC	C	b	Kernel 5 See A.2	’9F50’	1
Certification Authority Public Key	Present (up to 5 different instances) if Offline Data Authentication is supported for at least one of the Combinations with this RID (EMV Mode only). Each CA Public Key in the list is composed of the following mandatory fields: - CAPK Index (b, 1 byte) - CAPK Modulus (b, max. 248 bytes) - CAPK Exponent (b, 1 or 3 bytes) - CAPK SHA-1 Checksum (b, 20 bytes)	Configuration (RID)	C	b	EMV	-	var.

Name	Description	Source	Presence	Format	Specified	Tag	Length
Certification Authority Public Key Index	Identifies the certification authority's public key in conjunction with the RID. Required for EMV Mode.	ICC	C	b	EMV	'8F'	1
Combination Options	Defines some acquirer options for the combination, e.g. modes supported	Configuration (AID)	M	b	Kernel 5 See A.3	-	2
Contactless Floor Limit	Used in Kernel 5 Terminal Risk Management (EMV Mode only). Present if the Combination supports Floor Limit Check or Random Transaction Selection.	Configuration (AID)	C	n 12	Kernel 5	-	6
Contactless Transaction Limit	Used in Kernel 5 Terminal Risk Management	Configuration (AID)	O	n 12	Kernel 5	-	6
Cryptogram Information Data (CID)	Indicates the type of cryptogram and the actions to be performed by the terminal after the GENERATE AC command	ICC	C	b	EMV	'9F27'	1
CVM Required Limit	Used in Kernel 5 Terminal Risk Management	Configuration (AID)	O	n 12	Kernel 5	-	6
CVM Results	Indicates the results of the last CVM performed	Kernel	M	b	EMV	'9F34'	3
Dedicated File (DF) Name	Identifies the name of the DF as described in ISO/IEC 7816-4	ICC	M	b	EMV	'84'	5-16
File Control Information (FCI) Issuer Discretionary Data	Issuer discretionary part of the FCI. This data element is mandatory for the PPSE application, and optional for the payment application.	ICC	C	var.	EMV	'BF0C'	var. up to 222
File Control Information (FCI) Proprietary Template	Identifies the data object proprietary to this specification in the FCI template according to ISO/IEC 7816-4	ICC	M	var.	EMV	'A5'	var.

Name	Description	Source	Presence	Format	Specified	Tag	Length
File Control Information (FCI) Template	Identifies the FCI template according to ISO/IEC 7816-4	ICC	M	var.	EMV	'6F'	var. up to 252
Integrated Circuit Card (ICC) Public Key Certificate	ICC Public Key certified by the issuer	ICC	C	b	EMV	'9F46'	NI
Integrated Circuit Card (ICC) Public Key Exponent	ICC Public Key Exponent used for the verification of the Signed Dynamic Application Data	ICC	C	b	EMV	'9F47'	1 to 3
Integrated Circuit Card (ICC) Public Key Remainder	Remaining digits of the ICC Public Key Modulus	ICC	C	b	EMV	'9F48'	NIC - NI + 42
Issuer Action Code - Default	Specifies the issuer‘s conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online	ICC	O	b	EMV	'9F0D'	5
Issuer Action Code - Denial	Specifies the issuer‘s conditions that cause the denial of a transaction without attempt to go online	ICC	O	b	EMV	'9F0E'	5
Issuer Action Code - Online	Specifies the issuer‘s conditions that cause a transaction to be transmitted online	ICC	O	b	EMV	'9F0F'	5
Issuer Application Data (IAD)	Contains proprietary application data for transmission to the issuer in an online transaction.	ICC	C	b	EMV	'9F10'	var. up to 32
Issuer Authentication Data	Data sent to the card for online issuer authentication.	Issuer	O	b	EMV	‘91’	8-16

Name	Description	Source	Presence	Format	Specified	Tag	Length
Issuer Code Table Index	Indicates the code table according to ISO/IEC 8859 for displaying the Application Preferred Name	ICC	C	n 2	EMV	'9F11'	1
Issuer Country Code	Indicates the country of the issuer according to ISO 3166	ICC	C	n 3	EMV	'5F28'	2
Issuer Public Key Certificate	Issuer public key certified by a certification authority	ICC	C	b	EMV	'90'	NCA
Issuer Public Key Exponent	Issuer public key exponent used for the verification of the Signed Static Application Data and the ICC Public Key Certificate	ICC	C	b	EMV	'9F32'	1 to 3
Issuer Public Key Remainder	Remaining digits of the Issuer Public Key Modulus	ICC	C	b	EMV	'92'	NI - NCA + 36
Issuer Script Command	Contains a command for transmission to the card	Issuer	O	b	EMV	‘86’	Var. up to 125
Issuer Script Identifier	Identification of the Issuer Script	Issuer	O	b	EMV	‘9F18’	4
Issuer Script Template 1	Contains proprietary issuer data for transmission to the ICC before the second GENERATE AC command	Issuer	O	b	EMV	‘71’	var. up to 128
Issuer Script Template 2	Contains proprietary issuer data for transmission to the ICC after the second GENERATE AC command	Issuer	O	b	EMV	‘72’	var. up to 128
Issuer Update Parameter	Parameter from the ICC to indicate the behaviour/ergonomics (e.g. “present-and-hold” or “two presentments” or none) for processing the results of the online authorisation request	ICC	O	b	Kernel	‘9F60’	1

Name	Description	Source	Presence	Format	Specified	Tag	Length
Language Preference	1-4 languages stored in order of preference, each represented by 2 alphabetical characters according to ISO 639. Note: EMVCo strongly recommends that cards be personalised with data element '5F2D' coded in lowercase, but that terminals accept the data element whether it is coded in upper or lower case.	ICC	O	an 2	EMV	'5F2D'	2-8
Magstripe Data Object List (MDOL)	List of data objects (tag and length) to be passed to the card in the GET MAGSTRIPE DATA command	ICC	O	b	Kernel 5	'9F5C'	var. up to 252
Maximum Target Percentage to be Used for Biased Random Selection	Value used in terminal risk management for random transaction selection - present if the Combination supports Random Transaction Selection (EMV Mode only)	Configuration (AID)	C	n 2	EMV	-	1
Merchant Category Code	Classifies the type of business being done by the merchant, represented according to ISO 8583:1993 for Card Acceptor Business Code	Configuration (POS)	O	n 4	EMV	'9F15'	2
Merchant Name and Location	Indicates the name and location of the merchant	Configuration (POS)	M	ans	EMV	'9F4E'	var.
Offline Balance	In the case of a prepaid card, represents the value stored in card. May be returned in the GENERATE AC response.	ICC	O	n 12	Kernel 5	‘9F5F’	6

Name	Description	Source	Presence	Format	Specified	Tag	Length
Online Transaction Context	A set of persistent data elements representing the context of an ongoing online transaction. The *Online Transaction Context* is saved by the Kernel before returning the *Online Request* outcome, and is restored if Kernel is restarted for an Issuer Update. It consists of: • CDOL2 value provided by card • The CVM parameter returned with the *Online Request* outcome • The Transaction Record (EMV Mode – see Annex C) returned with the *Online Request* outcome	Kernel	C	-	Kernel	-	var.
Processing Options Data Object List (PDOL)	Contains a list of terminal resident data objects (tags and lengths) needed by the card in processing the GET PROCESSING OPTIONS command	ICC	M	b	EMV	'9F38'	var.
READ RECORD Response Message Template	Contains the contents of the record read. (Mandatory for SFIs 1-10. Response messages for SFIs 11-30 are outside the scope of EMV, but may use template '70')	ICC	C	var.	EMV	'70'	var. up to 252
‘Recovering from Torn EMV Transaction’ Flag	Internal Kernel variable (Boolean) set to TRUE when the Kernel attempts to recover from a torn transaction (EMV Mode only)	Kernel 5	C	-	Kernel 5	-	-

Name	Description	Source	Presence	Format	Specified	Tag	Length
Recovery Context	A set of persistent Kernel 5 parameters involved in the management of torn EMV transactions. It consists of: - 'Recovering from Torn EMV Transaction' Flag - 'Torn Track 2 Data' - 'Torn CDA Hash Data Buffer'	Kernel 5	C	-	Kernel 5	-	-
Removal Timeout	Present if the Combination supports Issuer Update as Acquirer Option (EMV Mode only). In case of Online Request with "Present and Hold" outcome, this parameter corresponds to the time after which cardholder is asked to remove the card. Value is given in units of 100ms.	Configuration (AID)	C	n 4	Kernel	-	2
Response Message Template Format 1	Contains the data objects (without tags and lengths) returned by the ICC in response to a command	ICC	C	var.	EMV	'80'	var.
Response Message Template Format 2	Contains the data objects (with tags and lengths) returned by the ICC in response to a command	ICC	C	var.	EMV	'77'	var.
Signed Dynamic Application Data	Digital signature on critical application parameters for DDA or CDA	ICC	C	b	EMV	'9F4B'	NIC
Static Data Authentication Tag List	List of tags of primitive data objects defined in this specification whose value fields are to be included in the Signed Static or Dynamic Application Data	ICC	C	—	EMV	'9F4A'	var.

Name	Description	Source	Presence	Format	Specified	Tag	Length
Target Percentage to be Used for Biased Random Selection	Value used in terminal risk management for random transaction selection. Present if the Combination supports Random Transaction Selection (EMV Mode only)	Configuration (AID)	C	n 2	EMV	-	1
Terminal Action Code - Default	Used in Kernel 5 Terminal Action Analysis (EMV Mode only)	Configuration (AID)	O	b	EMV	-	5
Terminal Action Code - Denial	Used in Kernel 5 Terminal Action Analysis	Configuration (AID)	O	b	EMV	-	5
Terminal Action Code - Online	Used in Kernel 5 Terminal Action Analysis (EMV Mode only)	Configuration (AID)	O	b	EMV	-	5
Terminal Compatibility Indicator	Indicates to the card the transaction modes (EMV, Magstripe) supported by the Kernel	Kernel 5	M	b	Kernel 5 See A.4	'9F52'	1
Terminal Country Code	Indicates the country of the terminal, represented according to ISO 3166. Requested in CDOL1.	Configuration (POS)	M	n 3	EMV	'9F1A'	2
Terminal Interchange Profile (dynamic)	Defines the reader CVM requirement and capabilities, as well as other reader capabilities (online capability, contact EMV capability) for the Transaction	Kernel 5	M	b	Kernel 5 See A.5	'9F53'	3
Terminal Interchange Profile (static)	Defines the Cardholder Verification Methods and other reader capabilities (online capability, contact EMV capability) for the Combination	Configuration (AID)	M	b	Kernel 5 See A.5	-	3
Terminal Type	Indicates the environment of the terminal, its communications capability, and its operational control	Configuration (POS)	M	n 2	EMV	'9F35'	1

Name	Description	Source	Presence	Format	Specified	Tag	Length
Terminal Verification Results (TVR)	Status of the different functions as seen from the terminal	Kernel 5	M	b	EMV / Kernel 5	'95'	5
Threshold Value for Biased Random Selection	Value used in terminal risk management for random transaction selection. Present if the Combination supports Random Transaction Selection (EMV Mode only)	Configuration (AID)	C	n 12	EMV	-	6
Torn CDA Hash Data Buffer	A copy of the PDOL related data and CDOL1 related data sent to the card during a torn transaction in EMV Mode. This copy is used to verify the CDA signature during the subsequent transaction recovery process.	Kernel 5	C		Kernel 5	-	Var. up to 507
Torn Track 2 Data	A copy of the card Track 2 Equivalent Data, kept by the Kernel after a torn transaction in EMV Mode to ensure that the card presented for recovery is the same as for the torn transaction	Kernel 5	C	b	Kernel 5	-	Var. up to 19
Track 1 Discretionary Data	Discretionary part of track 1 according to ISO/IEC 7813	ICC	O	ans	EMV	'9F1F'	var.
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)	ICC	M	b	EMV	'57'	Var. up to 19
Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217. Requested in CDOL1.	Configuration (POS)	M	n 3	EMV	'5F2A'	2

Name	Description	Source	Presence	Format	Specified	Tag	Length
Transaction Currency Exponent	Indicates the implied position of the decimal point from the right of the transaction amount represented according to ISO 4217. Required to determine if Status Check is requested.	Configuration (POS)	M	n 1	EMV	‘5F36’	1
Transaction Date	Local date that the transaction was authorised. Requested in CDOL1.	POS	M	n 6	EMV	'9A'	3
Transaction Mode	An internal Kernel indicator storing the transaction mode selected for conducting the transaction. It admits the following values: - Undefined Mode - EMV Mode - Magstripe Mode - Legacy Mode	Kernel 5	M	-	Kernel 5	-	-
Transaction Time	Local time that the transaction was authorised	POS	M	n 6 HHMMSS	EMV	‘9F21’	3
Transaction Type	Indicates the type of financial transaction, represented by the first two digits of the ISO 8583:1987 Processing Code. Requested in CDOL1. Possible values are: - '00' for a purchase transaction - ‘01’ for a cash advance transaction - ‘09’ for a purchase with cashback - ‘20’ for a refund transaction	POS	M	n 2	EMV	'9C'	1
Unpredictable Number	Value to provide variability and uniqueness to the generation of a cryptogram. Requested in CDOL1.	POS	M	b	EMV	'9F37'	4

Annex C Kernel 5 Transaction Record

Table C-1 lists the minimum data elements in the data record returned to the Entry Point, depending on the Transaction Mode (EMV, Legacy, Magstripe) and the Transaction Outcome (Approved, Online Request, Declined).

Data elements that are mentioned as ‘Conditional’ (‘C’) shall be present in the Transaction Record whenever they are provided by the card.

Table C-1: Minimum Data Elements returned as Transaction Record

Data Element Name	Tag	Source	Approved & Online Request (EMV & Legacy Mode)	Online Request (Magstripe Mode)	Declined (all modes)
Amount, Authorised (Numeric)	'9F02'	POS	M	M	-
Amount, Other (Numeric)	'9F03'	POS	M	M	-
Application Cryptogram (AC)	'9F26'	Card	M	-	-
Application Interchange Profile (AIP)	'82'	Card	M	-	-
Application PAN Sequence Number	'5F34'	Card	C	-	-
Application Transaction Counter (ATC)	'9F36'	Card	M	-	-
Cardholder Name	'5F20'	Card	C	C	-
CVM Results	‘9F34'	Kernel 5	M	M	-

Data Element Name	Tag	Source	Approved & Online Request (EMV & Legacy Mode)	Online Request (Magstripe Mode)	Declined (all modes)
Cryptogram Information Data (CID)	'9F27'	Card	M	-	-
Issuer Application Data (IAD)	'9F10'	Card	M	-	-
Transaction Mode[17]	-	Kernel 5	M	M	-
Terminal Country Code	‘9F1A’	POS	M	M	-
Terminal Verification Results (TVR)	'95'	Kernel 5	M	-	-
Track 1 Discretionary Data	'9F1F'	Card	C	C	-
Track 2 Equivalent Data	'57'	Card	M	M	M
Transaction Currency Code	'5F2A'	POS	M	M	-
Transaction Date	‘9A’	POS	M	M	-
Transaction Time	‘9F21’	POS	M	M	-
Transaction Type	'9C'	POS	M	M	-
Unpredictable Number (UN)	'9F37'	POS	M	-	-

[17] Transaction Mode is used by the reader to map the POS Entry Mode data element in the authorisation/clearing message, according to Payment System rules.

Annex D Default Terminal Action Code values

This section details the coding of the default Terminal Action Code values that the Kernel shall use in case the Acquirer has not explicitly parameterised other values for the Combination.

Table D-1: Default Terminal Action Code values

Terminal Action Code - Byte 1 (Leftmost)

Meaning	Denial	Online	Default
Offline data authentication was not performed	0	1	1
SDA failed	0	0	0
ICC data missing	0	0	0
Card appears on terminal exception file	0	1	1
DDA failed	0	0	0
CDA failed	1	0	0
RFU	0	0	0
RFU	0	0	0

Terminal Action Code - Byte 2

Meaning	Denial	Online	Default
ICC and terminal have different application versions	0	0	0
Expired application	0	1	1
Application not yet effective	0	1	0
Requested service not allowed for card product	1	0	0
New card	0	0	0
RFU	0	0	0
RFU	0	0	0
RFU	0	0	0

Terminal Action Code - Byte 3

Meaning	Denial	Online	Default
Cardholder verification was not successful	0	0	0
Unrecognised CVM	0	0	0
PIN Try Limit exceeded	0	0	0
PIN entry required and PIN pad not present or not working	0	0	0
PIN entry required, PIN pad present, but PIN was not entered	0	0	0
Online PIN entered	0	0	0
RFU	0	0	0
RFU	0	0	0

Terminal Action Code - Byte 4

Meaning	Denial	Online	Default
Transaction exceeds floor limit	0	1	1
Lower consecutive offline limit exceeded	0	0	0
Upper consecutive offline limit exceeded	0	0	0
Transaction selected randomly for online processing	0	1	0
Merchant forced transaction online	0	0	0
RFU	0	0	0
RFU	0	0	0
RFU	0	0	0

Terminal Action Code - Byte 5 (Rightmost)

Meaning	Denial	Online	Default
Default TDOL used	0	0	0
Issuer authentication failed	0	0	0
Script processing failed before final GENERATE AC	0	0	0
Script processing failed after final GENERATE AC	0	0	0
RFU	0	0	0
RFU	0	0	0
RFU	0	0	0
RFU	0	0	0

Annex E 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
b	Binary
C	Conditional
Card	As used in these specifications, a consumer device supporting contactless transactions. It may be a plastic card, a mobile phone, a key fob, a watch or any other suitable form factor

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

Chip Grade
An operating mode of the POS System that indicates that this particular acceptance environment and acceptance rules supports chip infrastructure.

CID
Cryptogram Information Data

CL
Contactless

cn
Compressed Numeric

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

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 One of the three Kernel 5 transaction modes. EMV Mode is selected for the transaction in a chip grade acceptance, when also supported by the card.

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

F Format

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 logic to 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

Legacy Mode One of the three Kernel 5 transaction modes. EMV Mode is selected for the transaction in a chip grade acceptance, when the card is a legacy card.

M	Mandatory
Magstripe Mode	One of the three Kernel 5 transaction modes. EMV Mode is selected for the transaction in a magstripe grade acceptance, or when EMV Mode is not supported by the card.
MDOL	Magstripe Data Object List
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
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