EMV®
Contactless Specifications for Payment Systems

Book C-5

Kernel 5 Specification

Version 2.11
June 2023

Legal Notice

The EMV® 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 the EMV® 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 the EMV® 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 the EMV® Specifications.

Revision History

The following changes have been made to Book C-5 since the publication of version 2.10. Change bars are used in this specification to denote the sections that have been updated. Some of the numbering and cross references in this specification have been updated to reflect the modifications made in the new version. In addition to the below, minor editorial clarifications and corrections may be added for readability.

No.	Revision Date	Chapter	Contents of Revision
1	June, 2023	3.4.1.2	Application Primary Account Number (PAN) (Tag '5A') is added as a mandatory Data Element (SB263)
2	June, 2023	2.4.1 2.4.2	Random Transaction Selection is added as an option which the Reader provider may choose in the implementation (SB266)
3	June, 2023	Annex B	Correct Tag values for data elements Transit Agent ID and Transit Related data. (SB269)
4	June, 2023	3.3.1.3 3.3.1.4 4.3	Change the requirements when the Status Word '6F00' is returned to Get Processing Options command (SB286)
5	June, 2023	2.3 3.8.2.1	Change the requirements to provide a Try Another Interface Outcome if the terminal supports the contact interface (SB290)
6	June, 2023	3.7.1.1 3.10.3.4	Add the supplement for the transaction result of the following process. - Terminal Action Analysis - Issuer Update Processing (SB291)
7	June, 2023	3.2 3.11 and others	Remove the feature of Torn Transaction Recovery (SB292)

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 reader providers 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 E: Security and Key Management

EMV L1 Contactless : EMV Contactless Interface Specification

1.4 Reference Materials

The following specifications and standards contain provisions that are referenced in this specification. The latest version shall apply unless a publication date is explicitly stated.

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

[EMV]	*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, “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 requirements
or	Logical OR which connects two conditional requirements
=	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.

2.1 Two Transaction Modes

Kernel 5 shall always support EMV Mode and Legacy Mode.

2.1.1 EMV Mode

EMV Mode is designed for Chip Grade payment infrastructures.

The support of EMV Mode is mandatory on the Kernel side (Acquirer). The card will select to conduct the transaction in EMV Mode when the card supports 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 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 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 determines the most relevant Combination {ADF Name, AID, Kernel ID, Application Priority Indicator} to process the transaction, based on Reader Combinations and the card's ADF parameters in the PPSE Response (Application Priority Indicator, Kernel Identifier).
2. 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.
3. 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 that the card has selected the EMV Mode.
4. The Kernel reads the card data as indicated by the AFL.
5. 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).
6. The Kernel performs Processing Restrictions, which consists of several verifications:
    a. Application Usage Control (EMV Mode only)
    b. Application Expiration Date
    c. Application Effective Date

    These verifications update the Terminal Verification Results (TVR).

7. 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, unless the payment application declines the transaction, then the outcome is Online Authorisation.
8. 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 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.
9. 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 shall 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.

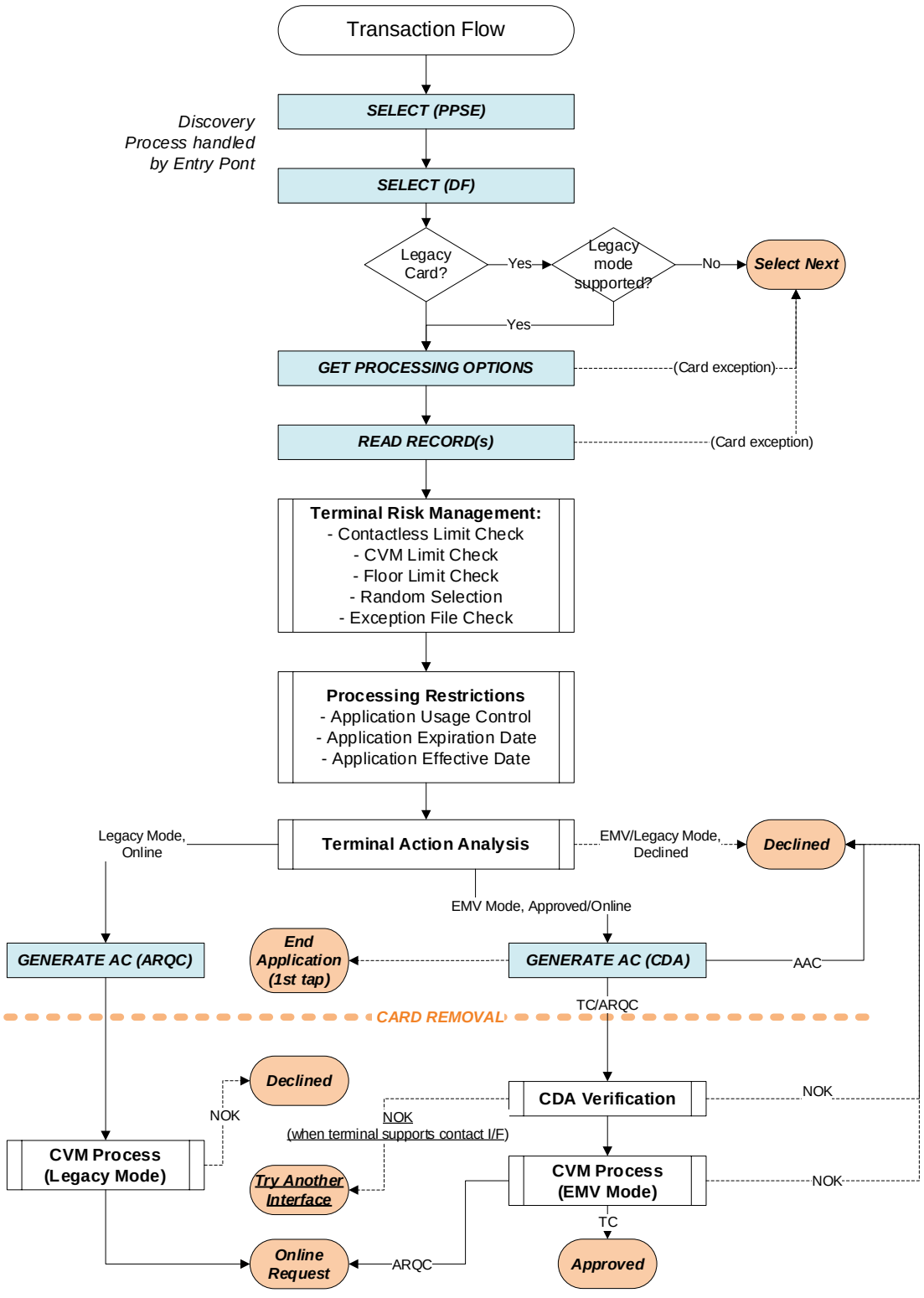
2.3 High Level Transaction Flow

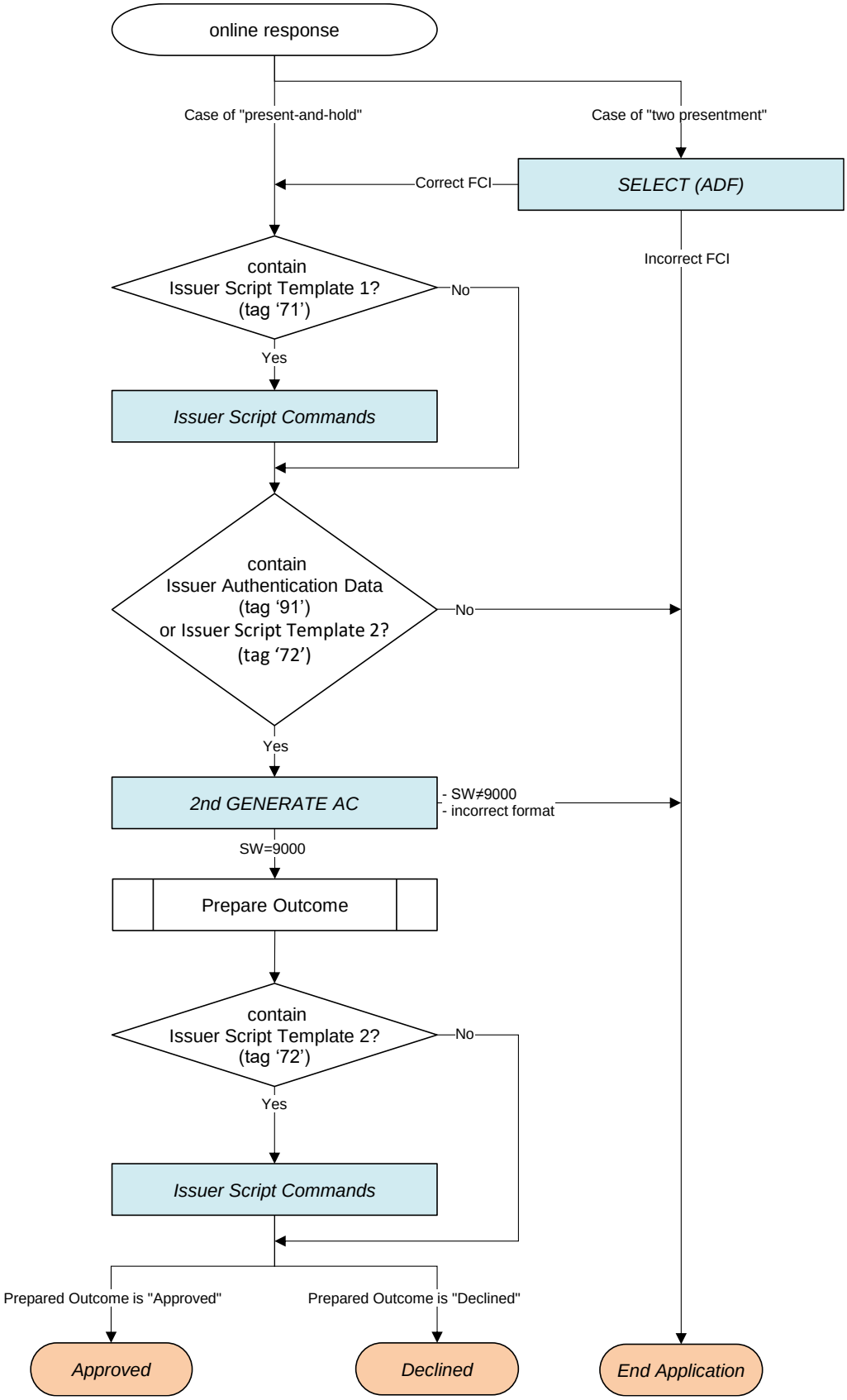
Figure 2-1 below illustrates the high level transaction flow of Kernel 5.

The purpose is to provide a summarised overview of the normal Kernel 5 processing and is not prescriptive. Note that specific processes like Issuer Update is 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:

- **Offline Data Authentication**
  - This implementation option enables support of CDA to authenticate the card. CDA is only used for EMV Mode.
  - Kernel 5 implementations for offline-capable readers, transit readers, or readers accepting On-Device CVM shall 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 is only used for EMV Mode.
  - Implementations for transit readers shall support this option.
  - The Data Exchange mechanism enable readers to update Acquirer Exception File. Readers supporting Exception File Check should support Data Exchange.
  - 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.
- **Random Transaction Selection**
  - This implementation option enables readers to select transactions randomly for online authorisation.
  - Random Transaction Selection is only used for EMV Mode.
  - Implementations for offline with online capable readers shall support this option.
- **Issuer Update**
  - This implementation option enables to convey EMV data (Issuer Authentication Data and/or Issuer Scripts, which are/is 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 shall support both ergonomics, as the choice is indicated by the card.
- Issuer Update is only used for EMV Mode.

- **Cardholder Verification Method**

  The Kernel 5 shall support all Cardholder Verification Methods described in this specification except following case applies:

  - If the Reader supports only Transit Reader, the Reader provider may choose whether to support or not the Cardholder Verification Method.
  - If the Reader supports offline environment only, the Reader provider may choose whether to support or not the following Cardholder Verification Method in the Reader implementation:

    - Online PIN
  - If the Reader supports ATM only, the Reader provider may choose whether to support or not the following Cardholder Verification Method in the Reader implementation:

    - Signature

    - On-Device CVM
  - If the Reader supports Unattended Merchant Terminal only, the Reader provider may choose whether to support or not the following Cardholder Verification Method in the Reader implementation:

    - Signature

    - Online PIN

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.9) for each supported Reader Combination.

- **Legacy Mode**

- This option activates Legacy Mode flow for the associated Reader Combination.

- **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.9).
    - the reader accepts “On-Device CVM” as a Cardholder Verification Method in the Terminal Interchange Profile (see Section A.9).
  - The option is available only if Offline Data Authentication (implementation option) is supported in EMV Mode.
- **Exception File Check**
  - This option activates Acquirer Exception File Check during the transaction.
  - The option is available only if Exception File Check (implementation option) is supported in EMV Mode.
- **Random Transaction Selection**
  - This option activates Random Transaction Selection during Terminal Risk Management.
  - The option is available only if Random Transaction Selection (implementation option) is supported in EMV Mode.
- **Issuer Update**
  - This option activates Issuer Update to convey EMV data (Issuer Authentication Data and/or Issuer Scripts, which are/is 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) is supported in EMV Mode.

3 Kernel 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 : Static Kernel Configuration Parameters) 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 : Dynamic Transaction Parameters); and • FCI received from the card as per section 3.4 in *[EMV CL Book B]* (when applicable).

Table 3-1: Static Kernel Configuration Parameters

Name	Description	Varies by	Presence[1]	Format	Specified	Tag	Length (bytes)
On-Device CVM Contactless Transaction Limit	Indicates the limit for which contactless transactions can be conducted when CVM is On-Device CVM (EMV Mode only).	AID	O	n12	Kernel 5	-	6
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. Indicates the limit for which contactless transactions can be conducted when CVM is other than On-Device CVM (EMV Mode), or when Transaction Mode is Legacy Mode.	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

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

Name	Description	Varies by	Presence[1]	Format	Specified	Tag	Length (bytes)
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
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.9	-	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	C	n 4	EMV	‘9F15’	2

Name	Description	Varies by	Presence[1]	Format	Specified	Tag	Length (bytes)
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
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 shall be present if the Kernel is restarted after an Online Request Outcome. ARC shall not be present if it is a new transaction.	C	an2	EMV	'8A'	2
Issuer Authentication Data	Data sent to the card for online issuer authentication. Issuer Authentication Data may be present if the Kernel is restarted after an Online Request Outcome. Issuer Authentication Data shall not be present if it is a new transaction.	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.** Issuer Script Template 1 may be present if the Kernel is restarted after an Online Request Outcome. Issuer Script Template 1 shall not be present if it is a new transaction.	O	b	EMV	'71'	var. max. 128

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

Name	Description	Presence[2]	Format	Specified	Tag	Length (bytes)
Issuer Script Template 2	Contains proprietary issuer data for transmission to the card after the second GENERATE AC command. **Several occurrences of this data element may be present.** Issuer Script Template 2 may be present if the Kernel is restarted after an Online Request Outcome. Issuer Script Template 2 shall not be present if it is a new transaction.	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
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 – Transaction continuation	
3.2.1.1	**If** Authorisation Response Code (Tag '8A') is present in the Dynamic Transaction Parameters (see Table 3-2), **Then** the Kernel shall proceed with Requirement 3.2.1.2. **Otherwise** the Kernel shall proceed with Requirement 3.2.1.3.
3.2.1.2	**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 the Online Transaction Context and proceed with Issuer Update Processing, as described in section 3.10. **Otherwise** the Kernel shall provide an **End Application** outcome as described in section 3.12.7.

Requirement – SELECT response analysis	
3.2.1.3	**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 3.12.10.

Requirement – Variable Initialisation	
3.2.1.4	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 '00',
3.2.1.5	The Kernel shall reset the following internal variables: • *Online Transaction Context* • Transaction Mode to 'Undefined Mode'

Requirement – Terminal Compatibility Indicator	
3.2.1.6	The Kernel shall set Terminal Compatibility Indicator (Tag '9F52') to '02'

Requirement – Terminal Interchange Profile	
3.2.1.7	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 this stage, the Kernel will detect whether the presented card is a legacy card, and if so, ensure that it has the capability to process such cards.

Requirement – Legacy Mode Detection	
3.2.1.8	**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 3.2.1.9.
3.2.1.9	**If** 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 3.12.10.

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 to 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]*.

The Kernel detects that EMV Mode is selected by the card by checking the value of AIP returned by the card. 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 Status Word returned by the card is '6F00',** **Then** the Kernel shall terminate the transaction and provide an **End Application** Outcome with the following Outcome parameter values: **End Application**: • **Start**: N/A • **Online Response Data**: N/A • **CVM**: N/A • **UI Request on Outcome Present**: Yes Message Identifier: '06' ("CARD ERROR") Status: Ready to Read • **UI Request on Restart Present**: No • **Data Record Present**: No • **Discretionary Data Present**: No • **Alternate Interface Preference**: N/A • **Receipt**: N/A • **Field Off Request**: N/A • **Removal Timeout**: Zero
3.3.1.4	**If** the Status Word returned by the card is different from '9000' and '6F00', **Then** the Kernel shall terminate the transaction and provide a **Select Next** Outcome as described in Section 3.12.10.
3.3.1.5	**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 3.12.10.

Requirement – GPO Response Analysis	
3.3.1.6	**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'), **And** the Terminal Compatibility Indicator Byte 1 Bit 2 is set to '1' ('EMV Mode Supported'), **Then** the Kernel shall set Transaction Mode to 'EMV Mode'. **Else** the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section3.12.10.
3.3.1.7	**If** the AFL (Tag '94') is absent from the data returned to the GET PROCESSING OPTIONS response **Then** the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.12.10.
3.3.1.8	**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 3.12.10.
3.3.1.9	**If any** of the conditions below is true: • 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 1 bit 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 this point, the Kernel needs to determine if all mandatory data elements are present. Even if the Kernel reads data objects that are not recognised by the Kernel (that is, their tags are unknown by the Kernel), the Kernel shall not terminate the transaction.

Requirement – Presence of Mandatory Data Elements

3.4.1.2 **If** 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')
- Application Primary Account Number (PAN) (Tag '5A')

Then the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.12.10.

If Offline Data Authentication is supported, CDA is the one and only mandatory Data Authentication Method[3] supported by the Kernel in 'EMV Mode', hence the Kernel shall ensure that all the appropriate data elements are present.

[3] SDA/DDA is not supported for EMV Mode.

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 1 bit 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')
- Issuer Public Key Remainder (Tag '92'), when required (based on the sizes of tags '9F46' and '90', when both are present)
- ICC Public Key Certificate (Tag '9F46')
- ICC Public Key Exponent (Tag '9F47')
- ICC Public Key Remainder (Tag '9F48'), when required (based on the ICC Public Key Length and the size of tag '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'. (except for when Issuer Public Key Remainder (Tag '92') and ICC Public Key Remainder (Tag '9F48') are not required.)[4]

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.)

[4] If the kernel performs the validation of certificates during CDA Signature verification, it is not mandatory to check the absence of data elements and to set the TVR value described in the requirement 3.4.1.3

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 Transaction Mode is 'Legacy Mode' **And** 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 3.12.10.

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 '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[5] **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]*.

[5] 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	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 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

Requirement – 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 3.7.1.7 (“Terminal Action Analysis Completion”). Note: In this case, "decline" indicates the completion of the refund process by the Kernel. It does not mean the rejection (failure) of the refund process.
3.7.1.2	**If** Transaction Mode is ‘Legacy Mode’ **And** TIP indicates that Reader is a Transit Reader (Byte 1 bit 3 is ‘1’), **Then** the Kernel shall decline the transaction as defined in section 3.12.5.
3.7.1.3	**If** TIP indicates that Reader is a Transit Reader (Byte 1 bit 3 is ‘1’) **And** Exception File Check is supported (implementation and acquirer option) **And** “Card appears on terminal exception file” in TVR is set (Byte 1 bit 5 is ‘1’), **Then** the Kernel shall decline the transaction as defined in section 3.12.5.
3.7.1.4	**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’ or no IAC values are provided by card, the Kernel shall use the following default IAC values: • IAC-Denial: 00 00 00 00 00 • IAC-Online: FF FF FF FF FF • IAC-Default: FF FF FF FF FF

Requirement – Terminal Action Analysis

3.7.1.5 **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.

3.7.1.6 **Terminal Action Analysis**

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

- Terminal Verification Results (TVR)
- TAC/IAC-Denial
- 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

3.7.1.7 **If** the result of the Terminal Action Analysis is to decline the transaction,
Then the Kernel shall decline the transaction as described in Section 3.12.5.

Otherwise the Kernel shall proceed to completion as described in:

- Section 3.8 if Transaction Mode is 'EMV Mode'
- Section 3.9 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 4.1 and *[EMV Book 3]*. [6] 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.

[6] The Kernel shall not change TVR after requesting GENERATE APPLICATION CRYPTOGRAM command and before providing the first Outcome, except the case of the failure of CDA Signature Verification (see 3.8.2.1).

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 3.12.9. 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 3.12.6. 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 3.12.10.

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 that the card has provided all mandatory data elements. The mandatory data elements depend on the transaction context. They are listed in Table 4-4, Table 4-5 and Table 4-6. **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 3.12.5.
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 3.12.5.
3.8.1.10	**If t**he Cryptogram Information Data (Tag '9F27') indicates a TC **And** the Signed Dynamic Application Data (Tag '9F4B') is absent from the card response, **Then** the Kernel shall decline the transaction as defined in section3.12.5.
3.8.1.11	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 3.12.5.
3.8.1.12	**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 3.12.5.

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

Requirement – Card Removal

3.8.1.13 **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
- the Issuer Update Parameter (Tag '9F60') has a value = '02' ("Second Presentment")
- the Issuer Update Parameter (Tag '9F60') has a value = '00' (Issuer Update is not expected, card can be removed)
- Issuer Update is not supported by the Kernel (implementation and acquirer option)

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]* and *[EMV Book 3],* including the retrieval of ICC Public Key.

If any step of signature verification fails,
Then

If the Terminal Interchange Profile (dynamic) indicates 'EMV contact chip supported' (byte 1 bit 2 = '1'),

Then the Kernel shall terminate the transaction with a Try Another Interface Outcome as defined in section 3.12.6.

Else the Kernel shall decline the transaction as defined in section 3.12.5.

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': On-Device CVM Selected
- Other: Not Applicable (no CVM preference)

Requirement – CVM Consistency Check	
3.8.3.2	**If** the Cardholder Verification Status indicates other than '00', '10', '20' or '3x', **Then** the Kernel shall decline the transaction as defined in section 3.12.5.
3.8.3.3	**If** the *Terminal Interchange Profile (dynamic)* indicates 'CVM Required by Reader' (byte 1 bit 8 = '1') **And** the Terminal Interchange Profile (dynamic) does not indicate 'Reader is a Transit Reader' (byte 1 bit 3 = '0') **And** the Cardholder Verification Status indicates '00', **Then** the Kernel shall decline the transaction as defined in section 3.12.5.
3.8.3.4	**If** the *Cardholder Verification Status* has any value among '10', '20' or '3x' (Signature, Online PIN, or On-Device CVM) **And** the *Terminal Interchange Profile (dynamic)* does not indicate 'Reader is a Transit Reader' (byte 1 bit 3 = '0') **And** the corresponding CVM is not supported in the *Terminal Interchange Profile (dynamic),* **Then** the Kernel shall decline the transaction as defined in section 3.12.5.

Requirement – On-Device CVM Contactless Transaction Limit and Contactless Limit Check	
3.8.3.5	**If** the Cardholder Verification Status indicates '3x' **And** the On-Device CVM 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 3.12.10.
3.8.3.6	**If** the Cardholder Verification Status indicates other than '3x' **Then** **If** the Contactless Transaction Limit is present **Then** **If** 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 3.12.10. **Else** **If** the On-Device CVM Contactless Transaction Limit is present **And** the value of Amount, Authorised (Numeric) (Tag '9F02') is greater than or equal to the On-Device CVM Contactless Transaction Limit, **Then** the Kernel shall terminate the transaction and provide a ***Select Next*** Outcome as described in Section 3.12.10

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 – Decision of Transaction Outcome	
3.8.4.1	**If** the Cryptogram Information Data (Tag '9F27') indicates a TC, **Then** the Kernel shall decide the Outcome to ***Approved*** Outcome as defined in section 3.12.1.
3.8.4.2	**If** the Cryptogram Information Data (Tag '9F27') indicates an ARQC, **And** any of the conditions below is true: • the Issuer Update Parameter (Tag '9F60') is absent from the card response **Or** has value = '00' • Issuer Update is not supported by the Kernel (implementation and acquirer option) **Then** the Kernel shall decide the Outcome to ***Online Request*** Outcome as defined in section 3.12.2.
3.8.4.3	**If** the Cryptogram Information Data (Tag '9F27') indicates an ARQC **And** Issuer Update is supported (implementation and acquirer option) **And** the Issuer Update Parameter (Tag '9F60') is present with value '01', **Then** the Kernel shall decide the Outcome to ***Online Request*** Outcome ("**Present and Hold**") as defined in section 3.12.4.
3.8.4.4	**If** the Cryptogram Information Data (Tag '9F27') indicates an ARQC **And** Issuer Update is supported (implementation and acquirer option) **And** the Issuer Update Parameter (Tag '9F60') is present with value '02', **Then** the Kernel shall decide the Outcome to ***Online Request*** Outcome ("**Two Presentments**") as defined in section 3.12.3.

Requirement – Setting of Outcome Parameters

3.8.4.5 **If** the Terminal Interchange Profile (dynamic) indicates 'Reader is a Transit Reader' (byte 1 bit 3 = '1'),

Then the CVM parameter in the ***Approved*** or ***Online Request*** Outcome and CVM Results (Tag '9F34') shall be set to "No CVM".

Else the CVM parameter in the ***Approved*** or ***Online Request*** Outcome and CVM Results (Tag '9F34') 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 the Outcome is an ***Approved*** *Outcome*,

Then

If CVM = Obtain Signature,
Then Message Identifier = '1A' ("Approved, please sign")
Else Message Identifier = '03' ("Approved")

Else (the Outcome is an ***Online Request*** *Outcome)*
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 Outcome is an ***Online Request*** *Outcome ("**Present and Hold**") or **Online Request** Outcome ("**Two Presentments**") as per Requirement* 3.8.4.3 or 3.8.4.4,

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

- Transaction 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)

Requirement – Providing of Transaction Outcome

3.8.4.8 The Kernel shall provide the Outcome and Outcome Parameters.

3.9 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.

3.9.1 GENERATE AC Command

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

Requirement – CDOL1 Processing	
3.9.1.1	The Kernel shall process the CDOL1 and construct the command data for the GENERATE AC command, as described in *[EMV Book 3]*.
3.9.1.2	**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	
3.9.1.3	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]*.
3.9.1.4	The kernel shall not change TVR after requesting GENERATE APPLICATION CRYPTOGRAM command and before providing the first Outcome.
3.9.1.5	**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 3.12.10.

Requirement – GENERATE AC	
3.9.1.6	The Kernel shall ensure that the card response is correctly formatted (see section 4.1). **If** the response to the GENERATE AC command is not parsed correctly **Or** a mandatory data element is missing **Or** the format of a returned data element is incorrect, **Then** the Kernel shall decline the transaction as defined in section 3.12.5.
3.9.1.7	**If** the Cryptogram Information Data (Tag '9F27') does not indicate an ARQC, **Then** the terminal shall decline the transaction as defined in section 3.12.5.

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.

3.9.2 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	
3.9.2.1	**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 3.9.3), with CVM parameter set to "No CVM".

Requirement – CVM Evaluation	
3.9.2.2	**If** the CVM List is absent from the card, **Then** the Kernel shall assume the CVM to be Not Applicable (no CVM preference) and the Kernel shall decline the transaction as defined in section 3.12.5.
3.9.2.3	**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[7] in the list shall determine the CVM requirement for the transaction.
3.9.2.4	**If** no match is found after processing requirement 3.9.2.3, **Then** the Kernel shall decline the transaction as defined in section 3.12.5.

3.9.3 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 – Decision of Online Request Outcome	
3.9.3.1	The Kernel shall decide the Outcome to ***Online Request*** Outcome as defined in section 3.12.2.

[7] It refers to the first matching CVM supported by both terminal and card.CV Rule Byte1bit7 is not evaluated.

Requirement – CVM Consistency Check

3.9.3.2 The CVM parameter in the ***Online Request*** Outcome and CVM Results (Tag '9F34') 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")

Requirement – Providing of Transaction Outcome

3.9.3.4 The Kernel shall provide the Outcome and Outcome Parameters.

3.10 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 shall 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.

3.10.1 Issuer Update Initialisation

Requirement – SELECT response analysis	
3.10.1.1	**If** the *Terminal Interchange Profile (dynamic)* indicates ‘Issuer Update Supported’ (byte 2 bit 8 = ‘1’), **Then** the kernel shall continue with the requirement 3.10.1.2. **Otherwise** the kernel shall provide an ***End Application*** Outcome as defined in Section 3.12.7
3.10.1.2	**If** the FCI has been provided by the reader with 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 3.12.7.

3.10.2 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

3.10.2.1 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[8] 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.

[8] 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

3.10.2.2 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 3.12.7.

Else the Kernel proceeds with Section 3.10.3.

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).

3.10.3 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

3.10.3.1 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 3.12.7.

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

3.10.3.3 **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

3.10.3.4 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 reader:

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.

Note: The final transaction disposition will be determined by the Acquirer in accordance with other respective requirements.

3.10.3.5 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	
3.10.3.6	**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 3.12.7.
3.10.3.7	**If** the response to the GENERATE AC command is not parsed correctly **Or** a mandatory data element is missing (see Table 4-2) **Or** the format of a returned data element is incorrect, **Then** the Kernel shall return an ***End Application*** Outcome as defined in section 3.12.7.
3.10.3.8	**If** the Cryptogram Information Data (Tag '9F27') indicates other than AAC or TC, **Then** the Kernel shall decline the transaction as defined in section 3.12.5.
3.10.3.9	**If t**he Kernel requested AAC, but the CID indicates a TC, **Then** the Kernel shall decline the transaction as defined in section 3.12.5**.**

3.10.4 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	
3.10.4.1	**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 3.12.5.

Requirement – Transaction Outcome	
3.10.4.2	**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 3.12.1.
3.10.4.3	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*.
3.10.4.4	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")
3.10.4.5	The Transaction Record (see Annex C) provided with the Approved Outcome is populated as follows: • Cryptogram Information Data (Tag '9F27'), ATC (Tag '9F36'), Application Cryptogram, Issuer Application Data (Tag '9F10') are the values returned by the card to the second GENERATE AC command. • TVR (Tag '95') is the value updated during Issuer Update Processing. • Other data elements are recovered from the *Online Transaction Context.*
3.10.4.6	**If** the Dynamic Transaction Parameters provide at least one occurrence of Issuer Script Template 2 (Tag '72'), **Then** the Kernel shall proceed with Section 3.10.5 **Else** the Kernel shall return the prepared Transaction Outcome.

3.10.5 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

3.10.5.1 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	
3.10.5.2	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 3.10.4.

3.11 Error Handling

3.11.1 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 3.10).

Requirement – Processing Errors - Default	
3.11.1.1	**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 3.12.10.
3.11.1.2	**If** the response to a command is not parsed correctly as defined for the command in section 4 **Or** a mandatory data element is missing **Or** 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 3.12.10. This rule includes (but is not limited to) the data format errors listed in *[EMV Book 3]* Section 7.5.

3.11.2 Communication Errors

Requirement – Communication Errors – Issuer Updates	
3.11.2.1	**If** a Transmission, Protocol, or Timeout error as defined in *[EMV Level1 Contactless]* is reported to the kernel while executing: • critical Issuer Script commands (see Section 3.10.2) • the second GENERATE AC command (see Section 3.10.3) **Then** the Kernel shall return an ***End Application*** Outcome as defined in Section 3.12.7.

Requirement – Communication Errors – Issuer Updates	
3.11.2.2	**If** a Transmission, Protocol, or Timeout error as defined in *[EMV Level1 Contactless]* is reported to the Kernel while executing non-critical Issuer Script commands (see Section 3.10.5), **Then** the Kernel shall return the Transaction Outcome as previously determined in Section 3.10.4 after the second GENERATE AC command.

Requirement – Communication Errors – General	
3.11.2.3	**If** a Transmission, Protocol, or Timeout error as defined in *[EMV Level1 Contactless]* 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 3.12.8.

3.11.3 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	
3.11.3.1	The Kernel shall be capable of receiving a cancellation order from the reader at any time during transaction processing.
3.11.3.2	**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 3.12.7.

3.12 Transaction Outcomes

3.12.1 Approved

Requirement – Approved Outcome	
3.12.1.1	The Kernel shall make available to the POS system the data elements necessary for an offline clearing record (cf. Annex C).

Requirement – Approved Outcome

3.12.1.2 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, 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"****]***[9]

  [*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

[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).

3.12.2 Online Request

Requirement – Online Request Outcome	
3.12.2.1	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

3.12.2.2 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"****]***[10]

  [*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

[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).

3.12.3 Online Request ("Two Presentments")

Requirement – Online Request Outcome ("Two Presentments")
3.12.3.1 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")

3.12.3.2 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"****]***[11]

  [*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

[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).

3.12.4 Online Request ("Present and Hold")

Requirement – Online Request Outcome ("Present and Hold")
3.12.4.1 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")

3.12.4.2 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/ Online PIN, as applicable
- **UI Request on Outcome Present:** Yes

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

  Status: Processing

  [*Value Qualifier: "Balance"****]***[12]

  [*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)

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

3.12.5 Declined

Requirement – Declined Outcome

3.12.5.1 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"****]***[13]

  [*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

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

3.12.6 Try Another Interface

Requirement – Try Another Interface Outcome

3.12.6.1 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

3.12.7 End Application

Requirement – End Application

3.12.7.1 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.

3.12.8 End Application (with restart – communication error)

Requirement – Communication Errors

3.12.8.1 **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

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

Requirement – On-Device CVM to be Performed

3.12.9.1 **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

3.12.10 Select Next

Requirement – Select Next

3.12.10.1 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

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'	'AE'	GENERATE APPLICATION CRYPTOGRAM	Mandatory
'80'	'A8'	GET PROCESSING OPTIONS	Mandatory
'00'	'B2'	READ RECORD	Mandatory
'00'	'A4'	SELECT	Mandatory

4.1 First GENERATE APPLICATION CRYPTOGRAM

Definition and Scope

The GENERATE APPLICATION CRYPTOGRAM command is used to complete a transaction.

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: Legacy Mode - Data Objects Included in Response to First GENERATE AC

Tag	Length	Description	Presence
(9F27)	(1)	Cryptogram Information Data	M
(9F36)	(2)	Application Transaction Counter	M
(9F26)	(8)	Application Cryptogram	M

Tag	Length	Description	Presence
(9F10)	(8)	Issuer Application Data	M

Note: Tag and length are not included in the response of Legacy Mode.

Table 4-4: 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
'9F50'	1	Cardholder Verification Status	M
'9F10'	var. up to 32	Issuer Application Data	M
'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 [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	M
'9F5F'	6	Offline Balance	O
'9F60'	1	Issuer Update Parameter	O

Table 4-6: 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 incorrectly formatted.

4.2 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 4-2: 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 incorrectly formatted.

4.3 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').

The data elements present in the response may depend on the Transaction Mode selected by the card, as can be seen from the Table 4-3 below.

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

Table 4-3: Data Objects Included in Response to GET PROCESSING OPTIONS

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

Processing State Returned in the Response Message

- '9000' indicates a successful execution of the command during a normal transaction.
- '6985' indicates that the conditions of use are not satisfied.
- '6A80' indicates that the command is incorrectly formatted.
- '6F00' indicates that an unexpected error has occurred.

4.4 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.

4.5 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) (Tag '82')

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
	x	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 (Tag '9F50')

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 selected: 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[14]
				1				Random Transaction Selection supported
					0			fixed to 0b
						1		EMV Mode Supported (fixed to 1b)
							1	Legacy Mode Supported

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*

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

A.4 CVM Results (Tag '9F34')

Table A-4-1: 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: 00111111b – No CVM performed 00011111b – No CVM required 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

Setting of CVM Results

Table A-5-2 shows the setting of CVM Results that correspond to each value of Outcome Parameter CVM.

Table A-5-2: Setting of CVM Results

Outcome Parameter CVM	CVM Results		
	Byte 1	Byte 2	Byte 3
No CVM	'1F' – No CVM required	'00'	'02' – successful
Obtain 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 Device Information (Tag '9F6E')

Table A-6: Device Information

Byte 1 Device type

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x						Device Factor Version In this version, this value is '001'
			x	x	x	x	x	Device Factor Type: 00000b – Card 00001b – Smart Phone 00010b – Key fob 00011b – Watch 00100b – Mobile Tag 00101b – Wristband 00110b – Mobile Phone case or Sleeve 00111b – Glasses 01000b – Tablet Others are RFU

Byte 2 Application Location

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x						RFU
			x	x	x	x	x	SE Type: 00001b – IC CHIP 00010b – SIM 00011b – Embbeded SIM 00100b – MicroSD 00101b – IC tag 00110b – Cloud SE(HCE) Others are RFU

Byte 3-4 RFU

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	RFU

A.6 Issuer Update Parameter (Tag '9F60')

Table A-7: 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.7 Partner Discretionary Data (Tag '9F7C')

Table A-8: Partner Discretionary Data

Data	Length (nibbles)	Digit #	Value
PDD Type Indicator	1	1	0: Set to "0", if this parameter is not used 1: Japanese Issuer 2: Non Japanese Issuer 3-F: RFU
Category Code	1	2	If PDD Type indicator is "1", this field shall be set to Issuer's Category Code. If PDD Type indicator is "0" or "2", this field shall be set to "0".

Data	Length (nibbles)	Digit #	Value
Company Code / Country Code	4	3-6	If PDD Type indicator is “0”, this field shall be set to “0000”. If PDD Type indicator is “1”, this field shall be set to Issuer's Company Code. If PDD Type indicator is “2”, this field shall be set to Issuer Country Code according to ISO 3166.
Issuer Discretionary Field	58	7-64	If PDD Type indicator is “0”, this field shall be set to All “0”. If PDD Type indicator is “1” or “2”, this field shall be set to issuer proprietary data elements.

A.8 Terminal Compatibility Indicator (Tag '9F52')

Table A-9: 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 (fixed to 1b)
							0	fixed to 0b

A.9 Terminal Interchange Profile (static/dynamic) (Tag '9F53')

Table A-10: Terminal Interchange Profile

TIP Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								CVM required by reader / N/A[152]
	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[1623]
	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

[22] 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.

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

Annex B Data Elements Dictionary

Table B-1 defines those data elements which may be used for financial transaction interchange and their mapping onto data.

The reader shall apply padding according to the format of the data elements and the rules as defined in *[EMV Book 1]* and Annex B. The reader shall accept TLV data elements in any order. The format of the TLV data elements is defined in *[EMV Book 3]*, Annex B. A data element with length '00' shall be treated as not present.

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	M	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 Dedicated File (ADF) Name	Identifies the application as described in ISO/IEC 7816-4.	ICC	M	b	EMV	‘4F’	5-16

Name	Description	Source	Presence	Format	Specified	Tag	Length
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.	ICC	M	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	M	var.	EMV	‘94’	var. up to 252
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	M	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	O	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 Selection Registered Proprietary Data (ASRPD)	Proprietary data allowing for proprietary processing during application selection. For further detail, please refer to Specification Bulletin No. 175.	ICC	O	b	EMV	‘9F0A’	var.

Name	Description	Source	Presence	Format	Specified	Tag	Length
Application Transaction Counter (ATC)	Counter maintained by the application in the card (incrementing the ATC is managed by the card)	ICC	M	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
Application Version Number	Version number assigned by the payment system for the application	ICC	O	b	EMV	‘9F08’	2
Authorisation Response Code	Code that defines the disposition of a message. ARC shall be present if the Kernel is restarted after an Online Request Outcome. ARC shall not be present if it is a new transaction.	Issuer	C	an2	EMV	‘8A’	2
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

Name	Description	Source	Presence	Format	Specified	Tag	Length
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.
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

Name	Description	Source	Presence	Format	Specified	Tag	Length
Contactless Transaction Limit	Used in Kernel 5 Terminal Risk Management. Indicates the limit for which contactless transactions can be conducted when CVM is other than On-Device CVM (EMV Mode), or when Transaction Mode is Legacy Mode.	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	M	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
Device Information	Attributes of the device that may be used to identify the specific device where a PAN or a payment token is stored.	ICC	O	an	EMV	'9F6E'	4
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.
File Control Information (FCI) Template	Identifies the FCI template according to ISO/IEC 7816-4.	ICC	M	var.	EMV	'6F'	var. up to 252

Name	Description	Source	Presence	Format	Specified	Tag	Length
Issuer Identification Number (IIN)	The number that identifies the major industry and the card issuer and that forms the first part of the Primary Account Number (PAN)	ICC	O	n 6	EMV	‘42’	3
Issuer Identification Number Extended (IINE)	The number that identifies the major industry and the card issuer and that forms the first part (6 or 8-digits) of the Primary Account Number (PAN). While the first 6-digits of the IINE (tag ’9F0C’) and IIN (tag ‘42’) are the same and there is no need to have both data objects on the card, cards may have both the IIN and IINE data objects present.	ICC	O	n 6 or 8	EMV	‘9F0C’	var. 3 or 4
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

Name	Description	Source	Presence	Format	Specified	Tag	Length
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	M	b	EMV	‘9F10’	var. up to 32
Issuer Authentication Data	Data sent to the card for online issuer authentication. Issuer Authentication Data may be present if the Kernel is restarted after an Online Request Outcome. Issuer Authentication Data shall not be present if it is a new transaction.	Issuer	O	b	EMV	‘91’	8-16
Issuer Code Table Index	Indicates the code table according to ISO/IEC 8859 for displaying the Application Preferred Name.	ICC	O	n 2	EMV	‘9F11’	1
Issuer Country Code	Indicates the country of the issuer according to ISO 3166	ICC	O	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

Name	Description	Source	Presence	Format	Specified	Tag	Length
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. Issuer Script Template 1 may be present if the Kernel is restarted after an Online Request Outcome. Issuer Script Template 1 shall not be present if it is a new transaction.	Issuer	O	b	EMV	'71'	var. up to 128
Issuer Script Template 2	Contains proprietary issuer data for transmission to the card after the second GENERATE AC command. Several occurrences of this data element may be present. Issuer Script Template 2 may be present if the Kernel is restarted after an Online Request Outcome. Issuer Script Template 2 shall not be present if it is a new transaction.	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	Card	'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
Last 4 digits of PAN	Represents the last four digits of the underlying PAN affiliated with the payment token. Its purpose is to support customer service, for example digital wallet display or receipt creation.	Issuer	O	n 4	EMV	'9F25'	2
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)	C	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	Card	'9F5F'	6

Name	Description	Source	Presence	Format	Specified	Tag	Length
On-Device CVM Contactless Transaction Limit	Indicates the limit for which contactless transactions can be conducted when CVM is On-Device CVM (EMV Mode only).	Configuration (AID)	O	n 12	Kernel 5	-	6
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.
Partner Discretionary Data	Partner Discretionary Data, if present, consists of one or more Issuer proprietary elements.	ICC	O	b	Card	'9F7C'	var up to 32
Payment Account Reference	A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated payment tokens.	ICC / Issuer	O	an	EMV	'9F24'	29
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.

Name	Description	Source	Presence	Format	Specified	Tag	Length
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	M	var.	EMV	'70'	var. up to 252
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	M	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	O	—	EMV	'9F4A'	var.
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

Name	Description	Source	Presence	Format	Specified	Tag	Length
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) supported by the Kernel.	Kernel 5	M	b	Kernel 5 See A.8	‘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
Terminal Verification Results (TVR)	Status of the different functions as seen from the terminal	Kernel 5	M	b	EMV / Kernel 5	‘95’	5

Name	Description	Source	Presence	Format	Specified	Tag	Length
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
Token Requestor ID	An 11-digit numeric value that identifies each unique combination of token requestor and token domain(s) for a given token service provider.	ICC / Issuer	O	n 11	EMV	‘9F19’	6
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
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

Name	Description	Source	Presence	Format	Specified	Tag	Length
Transaction Mode	An internal Kernel indicator storing the transaction mode selected for conducting the transaction. It admits the following values: - Undefined Mode - EMV 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
Transit Agent ID	Uniquely identifies the transit agent within each region and location. Requested in CDOL1.	Configuration (AID)	O	b	Kernel	‘DF72’	16
Transit Related Data	Contains transit agent proprietary data for a transit transaction. Requested in CDOL1.	Configuration (AID)	O	b	Kernel	‘DF73’	50
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) and the Transaction Outcome (Approved, Online Request, Declined).[17]

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

Card data which was not provided by the card shall not be returned.[24]

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

[17] Please note that Table C-1 does not list the data elements to be sent in the online authorization request.

[24] For example, the terminal shall not send Tag '9F08' with length 00 in the online authorization request when Tag ‘9F08’ was not provided by the card.

Data Element Name	Tag	Source	Approved & Online Request	Declined
Amount, Authorised (Numeric)	'9F02'	POS	M	M
Amount, Other (Numeric)	'9F03'	POS	M	M
Application Cryptogram (AC)	'9F26'	Card	M	C
Application Interchange Profile (AIP)	'82'	Card	M	M
Application Expiration Date	'5F24'	Card	M	M
Application Label	'50'	Card	M	M
Application PAN	'5A	Card	M	M
Application PAN Sequence Number	'5F34'	Card	C	C
Application Transaction Counter (ATC)	'9F36'	Card	M	C
Application Version Number	'9F08'	Card	C	C
Cardholder Name	'5F20'	Card	C	C
CVM Results[18]	'9F34'	Kernel 5	M	M
Dedicated File Name	'84'	Card	M	M
Cryptogram Information Data (CID)	'9F27'	Card	M	C

[18] About the value of CVM Results, please refer to Table A-5-2: Setting of CVM ResultsTable A-5-2

Data Element Name	Tag	Source	Approved & Online Request	Declined
Device Information	'9F6E'	Card	C	C
Issuer Application Data (IAD)	'9F10'	Card	M	C
Partner Discretionary Data	'9F7C'	Card	C	C
Payment Account Reference	'9F24'	Card	C	C
Transaction Mode[25]	-	Kernel 5	M	M
Terminal Country Code	'9F1A'	POS	M	M
Terminal Verification Results (TVR)	'95'	Kernel 5	M	M
Token Requestor ID	'9F19'	Card	C	C
Track 1 Discretionary Data	'9F1F'	Card	C	C
Track 2 Equivalent Data	'57'	Card	M	M
Transaction Currency Code	'5F2A'	POS	M	M
Transaction Date	'9A'	POS	M	M
Transaction Time	'9F21'	POS	M	M

[25] 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.

Data Element Name	Tag	Source	Approved & Online Request	Declined
Transaction Type	‘9C’	POS	M	M
Unpredictable Number (UN)	‘9F37’	POS	M	M

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

Meaning	Denial	Online	Default
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.
ADF	Application Definition File
AFL	Application File Locator
AID	Application Identifier
AIP	Application Interchange Profile
APDU	Application Protocol Data Unit
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 to approve the transaction
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)

Confirmation Code — A code or password entered into a mobile device in order to confirm that a user wishes to perform a contactless mobile payment transaction.

Contactless card — See “Card”.

Contactless Symbol	The symbol identifying the contactless “landing pane” near the antenna of a contactless acceptance device, where the cardholder shall present the card.
CVM	Cardholder Verification Method
CVS	Cardholder Verification Status
Declined	A Final Outcome to decline the transaction
DOL	Data Object List
EMV®	A trademark owned by EMVCo, referring to the technical specifications published by EMVCo.
EMV Mode	One of the two Kernel 5 transaction modes. EMV Mode is selected for the transaction in a Chip Grade acceptance, when also supported by the card.
EMVCo	The organization that manages the EMV Specifications and their related testing processes.
End Application	A Final Outcome
F	Format
FCI	File Control Information
Final Outcome	Result provided to the reader as a result of Entry Point processing the Outcome from the kernel, or provided directly by Entry Point under exceptional conditions.
GPO	GET PROCESSING OPTIONS command
IAD	Issuer Application Data
ICC	Integrated Circuit Card
Issuer	A financial institution that issues contactless cards or contactless payment applications that reside in consumer devices.

Kernel	The Kernel contains interface routines, security and control functions, and 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 two Kernel 5 transaction modes. Legacy Mode is selected for the transaction in a Chip Grade acceptance, when the card is a legacy card.
M	Mandatory
n	Numeric
N/A	Not Applicable; a possible value for several Outcome and Final Outcome parameters
O	Optional
Online PIN	A method of PIN verification where the PIN entered by the cardholder into the terminal PIN pad is encrypted and included in the online authorisation request message sent to the issuer.
Online Request	A Final Outcome to request online authorization
Outcome	Result from the Kernel processing, provided to Reader, or under exceptional 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.*
RFU	Reserved for Future Use (by EMVCo / JCB) A bit specified as Reserved for Future Use (RFU) is set as specified. A data field having a value coded on multiple bits or bytes cannot be set to a value specified as RFU. If the reader receives a data field having a value specified as RFU, the reader behaves as defined by the requirement that specifically addresses the situation.
SE	Secure Element
Select Next	An Outcome which leads to re-starting the processing at the appropriate start
SFI	Short File Identifier
Status Check Support	Option within the Combination related to the checking of a single unit of currency. A single unit of currency has the value of 1 of the (major) unit of currency as defined in ISO 4217. As an example a single unit of currency for Euro is 1.00.
SW1 SW2	Status Byte 1, Status Byte 2
T	Tag
TC	Transaction Certificate
Terminal	A component of the POS System; described in detail in *[EMV CL Book A].*
TIP	Terminal Interchange Profile
TLV	Tag Length Value
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 Another Interface	A Final Outcome

TVR	Terminal Verification Results
UI	User Interface
var.	Variable Length

***** END OF DOCUMENT *****