EMV®
ContactlessSpecifications for Payment Systems

Book C-4

Kernel 4 Specification

Version 2.6
February 2016

Legal Notice

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

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

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

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

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

Revision Log – Version 2.6

The following changes have been made to this document since the publication of Version 2.5. Some of the numbering and cross references in this version have been updated to reflect changes introduced by the published bulletins. The numbering of existing requirements did not change, unless explicitly stated otherwise.

Incorporated changes described in the following Specification Updates:

Specification Bulletin 176: EMV Book C-4, Version 2.5

Other editorial changes:

1. Updated Section 2.1.1 to clarify the transaction outcome in the case that a transaction mode cannot be determined by the reader.
2. Updated the condition check for Contactless Transaction Limit to “greater than or equal to” in Section 7.2.1.
3. Included checks to ensure that both the reader and the card support a contact interface when determining support for an alternative interface in Section 7.2.1 and Section 11.2.1.
4. Updated Table 12-4 with correct values for parameter settings “Start” and “Online Response Data”.
5. Included a note for Table 4-4: Enhanced Contactless Reader Capabilities – EMV Tag '9F6E' to clarify the purpose of Tag 9F6E Byte 1 bit 6 (Contactless EMV Full Online not supported).
6. Updated “UI Request on Outcome Present” parameter setting for ***Try Another Interface*** to display message with identifier: '1D' (“Please insert card”).

Contents

Figures

Tables

Requirements

1 Introduction

Kernel 4 is a contactless Reader kernel designed for interoperability with a suitable contactless payment application including American Express Contactless Payment Products.

1.1 Scope

This document, the *EMV ContactlessSpecifications for Payment Systems, Kernel 4 Specification*, defines the mandatory and optional functionality required when implementing Kernel 4.

1.2 Audience

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

1.3 Volumes of Contactless Specifications

This specification is part of a ten-volume set:

Book A: Architecture and General Requirements

Book B: Entry Point Specification

Book C-1: Kernel 1 Specification

Book C-2: Kernel 2 Specification

Book C-3: Kernel 3 Specification

Book C-4: Kernel 4 Specification

Book C-5: Kernel 5 Specification

Book C-6: Kernel 6 Specification

Book C-7: Kernel 7 Specification

Book D: Contactless Communication ProtocolSpecification

1.4 Reference Material

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

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

[EMV 4.3]	*EMV Integrated Circuit Card Specifications for Payment Systems*, Version 4.3, November 2011, including:
[EMV 4.3 Book 1]	*EMV Integrated Circuit Card Specifications for Payment Systems*, Book 1, Application Independent ICC to Terminal Interface Requirements
[EMV 4.3 Book 2]	*EMV Integrated Circuit Card Specifications for Payment Systems*, Book 2, Security and Key Management
[EMV 4.3 Book 3]	*EMV Integrated Circuit Card Specifications for Payment Systems*, Book 3, Application Specification
[EMV 4.3 Book 4]	*EMV Integrated Circuit Card Specifications for Payment Systems*, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements
[ISO 3166]	Codes for the representation of names of countries and their subdivisions
[ISO 4217]	Codes for the representation of currencies and funds
[ISO 7813]	Identification cards – Financial transaction cards
[ISO 7816-5]	Identification cards – Integrated circuit cards – Part 5: Registration of application providers
[ISO 8583]	Bank card originated messages – Interchange message specifications – Content for financial transactions

1.5 Notational Conventions

1.5.1 Use of Terms

Terms and definitions are described in *Book A: Architecture and General Requirements*, with the addition of the following.

Delayed Authorisation — In cases where a reader has been deployed in an environment where a real time online transaction authorisation is never possible, a delayed authorisation may be performed. A “Delayed Authorisation” as referred to in this specification is processed by the reader as a Partial Online contactless transaction, with mandatory Offline Data Authentication. Separately from the initial reader and card interaction, a later authorisation request may be made to an Issuer’s system for the purposes of account verification or reservation of funds against an account.

Partial Online — A Partial Online contactless transaction is one where the card may be removed from the operating field of the reader after the first GENERATE AC response has been received. The result of the transaction is based on the response from the Issuer’s authorisation system.

1.5.2 Reserved for Future Use (RFU)

A bit specified as Reserved for Future Use (RFU) shall be set as specified, or to 0b if no indication is given. An entity receiving a bit specified as RFU shall ignore such a bit and shall not change its behaviour, unless explicitly stated otherwise.

A data field having a value coded on multiple bits or bytes shall not be set to a value specified as RFU. An entity receiving a data field having a value specified as RFU, shall behave as defined by a requirement that specifically addresses the situation, or shall consider it a protocol error if no specific behaviour is defined.

1.6 Overview

This volume includes the following sections and annexes:

Section1 contains general information that helps the reader understand and use this specification.

Section2describes the modes in which a contactless card and reader can operate, and details the different flows that a contactless transaction can take.

Section3 provides a high-level overview of processing according to this specification.

Sections4 – 13 detail the different steps that occur in a contactless transaction and specify the command and processing requirements for each step of the transaction.

Annex A details the data elements used in contactless transaction processing using Kernel 4.

Annex B details the Configuration Data that is provided to the kernel by the Terminal and by Entry Point.

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

2 Contactless Modes and Transaction Flows

This section describes the modes in which a contactless card and reader can operate. It also details the different flows that a contactless transaction can take.

2.1 Contactless Modes of Operation

This specification details the two modes in which the card and reader can operate:

EMV mode – This mode of operation is designed for Issuers and Acquirers that are able to support EMV data in the authorisation and clearing messages.

Mag-stripe mode – This mode of operation is designed for Issuers that cannot accept EMV data for contactless transactions and for Acquirers that have not implemented EMV acceptance.

2.1.1 Support for Contactless Modes of Operation

All readers must support EMV mode but shall be configurable to be able to operate in mag-stripe mode only.

All cards and readers that support contactless processing must support contactless mag-stripe mode; therefore cards and readers supporting contactless EMV mode will also support contactless mag-stripe mode.

Requirements – Mandatory Support for Contactless Mag-Stripe Mode	
2.1.1.1a	**If** a card indicates (by setting *AIP* Byte 2 Bit 8 to 0b) that mag-stripe mode is to be performed, **then** the reader shall be able to successfully complete a mag-stripe mode transaction.
2.1.1.2a	**If** a reader supports EMV mode and has been configured to operate in mag-stripe mode only, **and** a card is presented indicating it supports EMV mode (*AIP* Byte 2 Bit 8 is set to 1b), **then** the reader shall be able to successfully complete a mag-stripe mode transaction.

The mode that is used for a transaction is determined by the ability of the card and the reader to support these two modes, as shown in Table 2-1.

Table 2-1: Contactless Mode Selection

	Reader Configured to Support Mag-Stripe Mode Only	Reader Supports Both Mag-Stripe and EMV Modes
Card Supports Mag-Stripe Mode	Mag-stripe mode transaction	Mag-stripe mode transaction
Card Supports Both Mag-Stripe and EMV Modes	Mag-stripe mode transaction	EMV mode transaction

The reader indicates which modes it supports by setting b7 and b8 in *Terminal Type* (Tag '9F35'), resulting in *Terminal Type – Modified* (shown inTable 4-3).

If the card requests *Terminal Type* via the *Processing Options Data Object List (PDOL)* in the GET PROCESSING OPTIONS command, the reader instead returns *Terminal Type – Modified* (as described in section 4.3).If the card requests the *Enhanced Contactless Reader Capabilities* via the *Processing Options Data Object List (PDOL)* in the GET PROCESSING OPTIONS command the reader shall return the *Enhanced Contactless Reader Capabilities*.

The card indicates which mode it supports for the transaction by setting b8 in the second byte of the *Application Interchange Profile (AIP)* that is returned in the GET PROCESSING OPTIONS response: 1b indicates that the card and Issuer support both EMV mode and mag-stripe mode, and 0b indicates that the card supports only mag-stripe mode.

Note that a card that supports both contactless mag-stripe mode and contactless EMV mode will return different *AIP* data depending on the modes of operation that the reader can support. If the reader is configured to support only mag-stripe mode, the card will return an *AIP* value of Byte 2 Bit 8 = 0b; the same card will return an *AIP* value Byte 2 Bit 8 = 1b if the reader supports contactless EMV mode.

If an applicable processing mode cannot be determined, for the transaction, as a result of an incorrect configuration of the reader, or the card, then the reader must terminate the transaction.

Requirements –Support for Contactless EMV Mode	
2.1.1.3a	**If** a reader indicates that it supports EMV mode (by setting *Terminal Type*Bit 8 and Bit 7 to 1b), **and** the card indicates that it is capable of EMV mode (by setting *AIP* Byte 2 Bit 8 to 1b), **then** the reader shall be able to successfully complete an EMV mode transaction.

2.1.2 Card Risk Management Data Object List (CDOL) Switch

A contactless card that supports both EMV mode and mag-stripe mode must implement a feature called CDOL-Switch. CDOL-Switch allows the card to present one of two predefined *Card Risk Management Data Object List (CDOL)* data elements:

If the reader indicates its capability to perform a contactless EMV mode transaction, then a CDOL-Switch enabled card presents a CDOL for EMV mode, Cryptogram Version '01'.

If the reader does not make this indication, then the card presents a CDOL for mag-stripe mode, Cryptogram Version '02'.

2.1.3 Contactless Mag-Stripe Mode Transaction

When a contactless transaction is performed in mag-stripe mode, the EMV data created as part of the transaction must be passed in the existing message data fields. To achieve this, the data that is used to generate the *Application Cryptogram (AC)* (*CDOL* – Cryptogram Version '02') is limited to the following:

Unpredictable Number

Application Transaction Counter (ATC)

Card Verification Results (CVR)

This data along with the *AC* created is passed in the Track 1 / Track 2 data fields. See section 12, Online Processing, for more information.

No EMV data will be returned in the Authorisation Response message.

2.1.4 Contactless EMV Mode Transactions

When a contactless transaction is performed in EMV mode, the reader is capable of sending the standard EMV data elements and there are no restrictions. In this mode the CDOL used corresponds to Cryptogram Version '01'.

2.1.5 Contactless Mobile Transaction

When a transaction is performed as Contactless Mobile the reader may prompt for an action to be performed on the Mobile device by exiting the transaction with a ***Try Again*** Outcome.

A Contactless Mobile:

supports both Mag-stripe and EMV Modes, as described in section 2.1.3 and section 2.1.4,

may support Mobile CVM (typically, a four-digit code stored in the Card, entered by the user via the phone device keypad and verified by the Card).

2.1.5.1 Mobile CVM

Contactless Mobile supports the Mobile CVM. This permits cardholder authentication on the Card using a numeric code, typically four digits. This is similar to Plaintext Offline PIN, in that, it is stored securely in the Card and verified by the Card during the VERIFY command. The reader manages the requirements for Cardholder Verification and processes the CVM List as for EMV. However, the reader performs no part in the Mobile CVM verification process – the Mobile CVM is captured and processed using the VERIFY command by an application on the Card, prior to the transaction. The results are passed to the reader as *Mobile CVM Results*in the response to the GET PROCESSING OPTIONS command or as an exception code in the response to the GENERATE AC command.

2.2 Contactless Transaction Processing

A contactless transaction can be performed in the following ways:

Offline

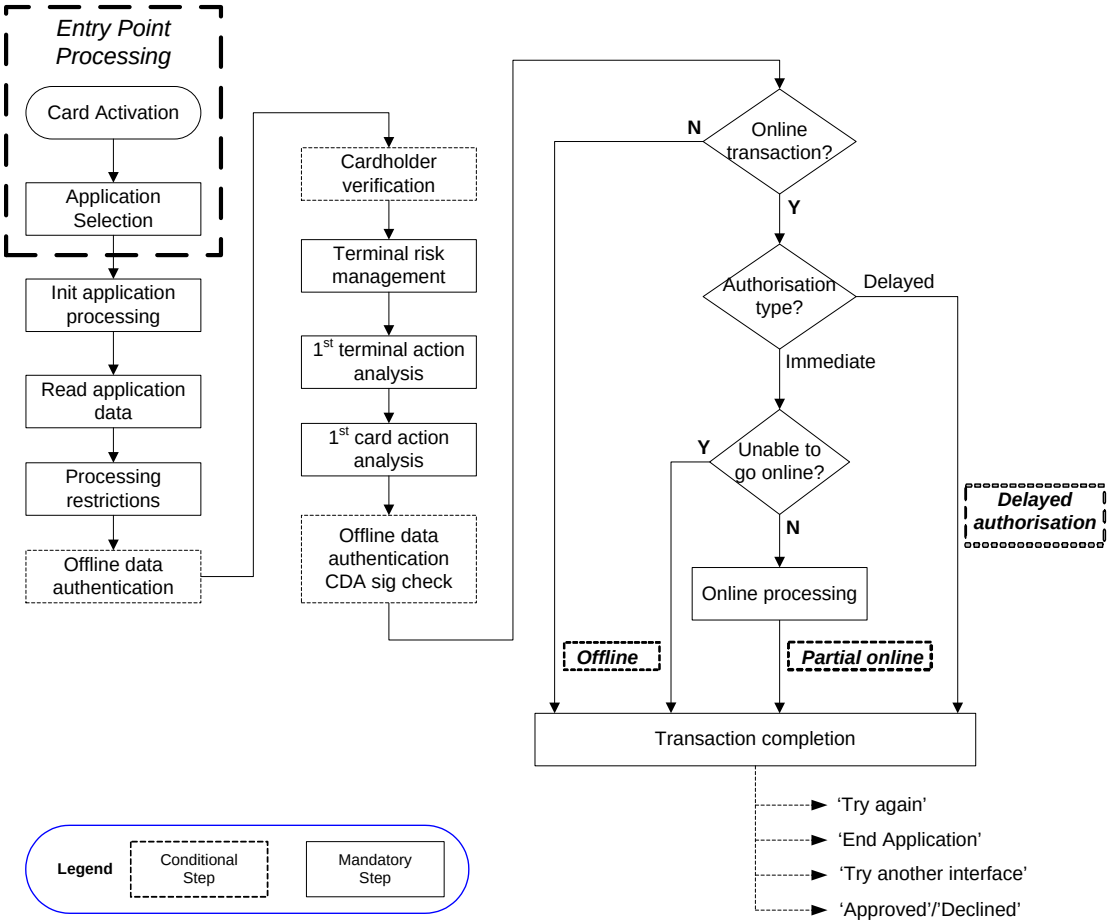
Partial Online with either:

Immediate authorisation or

Delayed authorisation (a “Delayed Authorisation” transaction)

Figure 2-1 shows the transaction flow for a contactless transaction and highlights the different processes performed for each of these options.

Figure 2-1: Transaction Flow Overview



2.2.1 Premature card removal

If the cardholder removes the card from the operating field without being prompted to do so, then the kernel returns control to Entry Point, passing an Outcome of ***Present Card Again*** with the following parameter settings:

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:** 0 • **Language Preference**
UI Request on Restart Present	Yes • **Message Identifier:** '21' (“Present Card Again”) • **Status:** Ready to Read. • **Hold Time:** 0 • **Language Preference**
Data Record Present	No
Discretionary Data Present	No
Alternate Interface Preference	N/A
Receipt	N/A
Field Off Request	N/A
Removal Timeout	Zero

Requirements – Card Early Removal

2.2.1.1a **If** the card leaves the operating field before the cardholder is prompted to remove it from the field,
then the reader shall invoke the User Interface Request Message to display Message Identifier: '21' (“Present Card Again”)
and return control to Entry Point.

2.2.2 Offline Transaction

During an offline transaction, the card and reader either approve or decline a transaction without further online processing.The enablement of Offline Data Authentication is mandatory for the deployment of terminals in offline environments. Only 1st Terminal Action Analysis and 1st Card Action Analysis are performed.

Requirements – Offline Transaction	
2.2.2.1a	**If** a reader indicates that it is offline capable (by setting bits 3-1 of *Terminal Type* (Tag '9F35') appropriately), **then** the reader shall be able to perform an offline transaction.

2.2.3 Partial Online Transaction

In a Partial Online transaction the interaction between the card and the reader ends after 1st Card Action Analysis has completed. The enablement of Offline Data Authentication is mandatory for the deployment of terminals in online capable environments where offline transactions are also possible. The result of the transaction is based on the response from the Issuer's authorisation system.

Requirements – Partial Online Transaction	
2.2.3.1a	**If** a reader indicates that it is online capable (by setting bits 3-1 of *Terminal Type* (Tag '9F35') appropriately), **then** the reader shall be able to perform a Partial Online transaction (i.e. without a second GENERATE AC being sent to the card).

A readerperforming a Partial Online transaction shall prompt the cardholder to remove the card from the field immediately after the completion of 1st Card Action Analysis.

The card should be removed from the operating field only when the reader indicates that it is time to do so.Once the reader has indicated that the card can be removed, whether the card is actually removed or not, the reader will continue to process the transaction as planned.

Requirements – Partial Online Transaction Completion	
2.2.3.2a	**If** a reader is online capable, **and** the reader is conducting a Partial Online transaction, **then** the reader shall complete the transaction as a Partial Online transaction whether the user leaves the card in the field or removes the card when instructed to do so.

2.2.4 Delayed Authorisation

In cases where a reader has been deployed in an environment where a real time online transaction authorisation is not possible, a delayed authorisation may be performed.

A “Delayed Authorisation” as referred to in this specification is processed by the reader as a partial online transaction, with the interaction between the Card and reader being completed after the 1st Card Action Analysis. Offline Data Authentication support is mandatory for all readers supporting Delayed Authorisations. The enablement of Offline Data Authentication is mandatory for the deployment of terminals in delayed authorization environments. If it is determined that the transaction is to be sent online, the transaction shall be approved at the Terminal and a subsequent delayed authorisation request is made to an Issuer’s authorisation system for the purposes of account verification or reservation of funds against an account.

Requirements – Delayed Authorisation	
2.2.4.1a	**If** a reader indicates that it supports Delayed Authorisations, **and** Offline Data Authentication has been performed successfully, **then** the reader shall be able to approve the transaction **and**performa Partial Online with delayed authorisation transaction.
2.2.4.2a	**If** a reader indicates that it supports Delayed Authorisations, **and** the Card returns an AAC in response to the first GENERATE AC, **then** the reader shall not perform Offline Data Authentication and the transaction shall be declined.

2.3 Contactless Transaction Configurations

The options for all possible combinations of processing a contactless transaction are shown in Table 2-2.

Table 2-2: Contactless Transaction Combinations

Contactless Transaction Mode	Card Supports Only Mag-Stripe Mode	Card Supports Both Mag-Stripe and EMV Modes
Mag-Stripe Mode Partial Online with immediate authorisation	The transaction flow is performed until 1st Card Action Analysis is completed. The card may be removed from the operating field and the transaction result will be based on the Issuer authorisation response. An online authorisation is performed with the cryptogram sent in Track 1 / Track 2 data records. However, if the reader is unable to go online, then the transaction will be declined.	The EMV transaction flow is performed until 1st Card Action Analysis is completed. The card may be removed from the operating field and the transaction result will be based on the Issuer authorisation response. A card with CDOL-Switch will present a CDOL for Cryptogram Version '02'. An online authorisation is performed with the cryptogram sent in Track 1 / Track 2 data records. However, if the reader is unable to go online, then the transaction is declined.

Contactless Transaction Mode	Card Supports Only Mag-Stripe Mode	Card Supports Both Mag-Stripe and EMV Modes
Mag-Stripe Mode Partial Online with delayed authorisation	The transaction flow is performed until 1st Card Action Analysis is completed. The card may be removed from the operating field and the transaction result will be based on the card's response. An online authorisation, with the cryptogram sent in Track 1 / Track 2 data records, is performed at a later time.	The EMV transaction flow is performed until 1st Card Action Analysis is completed. Offline Data Authentication is mandatory.The card may be removed from the operating field and the transaction result will be based on the card's response. A card with CDOL-Switch will present a CDOL for Cryptogram Version '02'. An online authorisation, with the cryptogram sent in Track 1 / Track 2 data records, is performed at a later time.
Mag-Stripe Mode Offline	Not applicable.	Not applicable.
EMV Mode Partial Online with immediate authorisation	Not applicable.	The EMV transaction flow is performed until 1st Card Action Analysis is completed. The card may be removed from the operating field and the transaction result will be based on the Issuer authorisation response. A card with CDOL-Switch will present a CDOL for Cryptogram Version '01'.

Contactless Transaction Mode	Card Supports Only Mag-Stripe Mode	Card Supports Both Mag-Stripe and EMV Modes
EMV Mode Partial Online with delayed authorisation	Not applicable.	The EMV transaction flow is performed until 1st Card Action Analysis is completed. Offline Data Authentication is mandatory.The card may be removed from the operating field and the transaction result will be based on the card's response. A card with CDOL-Switch will present a CDOL for Cryptogram Version '01'. An online authorisationis performed at a later time.
EMV Mode Offline	Not applicable.	An offline transaction is performed, if offline is allowed by Issuer configuration settings and Card Risk Management.Offline Data Authentication is mandatory. A card with CDOL-Switch will present a CDOL for Cryptogram Version '01'.

This specification supports the terminal configurations listed inTable 2-3.

Table 2-3: Reader Configurations

Reader Configuration	Definition
Offline only	Offline only readers do not have the ability to obtain a real time online authorisation nor do they have the ability to connect online for an authorisation at a later date. Offline Only readers must perform Offline Data Authentication on all transactions.

Reader Configuration	Definition
Online only	Online only readers require all transactions to be sent online for authorisation and do not have the ability to approve transactions offline. Readers configured in this way do not need to enable Offline Data Authentication. The reader must decline the transaction if it is unable to go online to obtain an authorisation.
Offline with Online Capability	Readers configured in this way are able to process transactions offline or send the transaction online for authorisation if required. Readers configured in this way must enable Offline Data Authentication. If the transaction is required to go online but is unable to (for example due to a communications error), then the Reader must decline the transaction. Readers of this type shall be capable of being configured to operate as Online Only readers.
Delayed Authorisations	In cases where a reader has been deployed in an environment where real time online transaction authorisation is never possible, a delayed authorisation may be performed. Readers configured in this way must enable Offline Data Authentication. A “Delayed Authorisation” as referred to in this specification is processed by the reader as a Partial Online contactless transaction, with mandatory Offline Data Authentication (unless the card has returned an AAC in response to the first GENERATE AC command, in which case ODA does not need to be performed). Separately from the initial reader and card interaction, a later authorisation request may be made to an Issuer’s system for the purposes of account verification or reservation of funds against an account.

Requirements – Transaction Combinations	
2.3.1.1a	**If** all of the following are true: • The terminal is operating in mag-stripe mode. • The terminal is performing a transaction with a mag-stripe or EMV card. • The transaction cannot go online. **Then** the card may be removed after the 1st Card Action Analysis and the terminal shall decline the transaction.
2.3.1.2a	**If** the terminal is performing a Partial Online transaction in EMV mode with an EMV card, **then** the card may be removed after the 1st Card Action Analysis **and** the terminal shall complete the Partial Online transaction in EMV mode.
2.3.1.3a	**If**an offline terminal is EMV capable, **and** the terminal is performing a transaction with a mag-stripe card, **then** the card may be removed after the 1st Card Action Analysis and the terminal shall decline the transaction.
2.3.1.4a	**If** an offline terminal is EMV capable, **and** the terminal is performing a transaction satisfying risk management requirements with an EMV card, **then** the card may be removed after the 1st Card Action Analysis and Offline Data Authentication is performed, and the terminal shall complete the transaction in EMV mode.

3 Processing Overview

The following sections provide detailed information about the interaction between the contactless card and reader during a transaction. All functions mentioned in the following sections are performed as described in this specification where detailed or otherwise as described within *[EMV 4.3 Book 1] – [EMV 4.3 Book 3]*. Some functionality supported by EMV is not permitted or is restricted for contactless transactions.

Card Activation and Application Selection shall be performed as in *Book B: Entry Point Specification*, with new transactions being initiated at Start A or Start B as described in *Book B*.

Figure 2-1 on page 9 shows an overview of the contactless transaction flow from the point at which a contactless card is introduced into the operating field of a reader to the point when the reader completes the transaction.

After processing a contactless transaction, the kernel returns control to Entry Point by passing an Outcome that specifies required actions from Entry Point or the terminal (POS System). Control may subsequently return to the kernel via *Book B* Start B. This 'restart' mechanism enables the kernel to process a retry for failed Mobile CVM processing.

The FCI data made available to the kernel by Entry Point may contain Tag '5F2D' (Language Preference Code), which may be supplied as one of the Outcome parameters in order to indicate a preferred language for the display of User Interface Messages.

4 Initiate Application Processing

4.1 Overview

During Application Initiation, the reader signals to the card that processing of the transaction is beginning. Initiate Application Processing is performed as described in *[EMV 4.3 Book 3]* and *[EMV 4.3 Book 4]*. Upon receipt of the *Application File Locator (AFL)* and *AIP*, the reader proceeds to read the application data records from the card.

The *AFL* is a list of parameters identifying the files and records to be read from the card used in processing the transaction. The *AIP* indicates the capabilities of the card to support specific functions of the application to be taken into consideration by the reader when determining how to process the transaction.

During this phase, the reader will determine whether the transaction is performed in mag-stripe mode or EMV mode.

4.2 Commands

GET PROCESSING OPTIONS

To support Initiate Application Processing as described in *[EMV 4.3 Book 3]*, section 10.1, the card must support the GET PROCESSING OPTIONS command as described in the following section.

If the transaction is taking place as Contactless Mobile, then *Mobile CVM Results*shall be returned in the GET PROCESSING OPTIONS response.(See on Table 8-1:Mobile CVM Results – Tag '9F71')

Requirements – GET PROCESSING OPTIONS	
4.2.1.1a	A reader shall send the GET PROCESSING OPTIONS command to the card following Application Selection.

4.3 Processing Requirements

4.3.1 Pre-PDOL Processing

The reader must reset *Contactless Reader Capabilities*Byte 1 Bit 4 to 0b, 'CVM Not Required' and *Enhanced Contactless Reader Capabilities* byte 3 to 00, since these are specific only to the context of the current transaction. All other *Enhanced Contactless Reader Capabilities* settings (bytes 1, 2 and 4) are defined at Terminal configuration.

Ifthe reader CVM Required Limit Exceeded indicator is set,then the reader shall set:

- *Contactless Reader Capabilities* Byte 1 Bit 4 to 1b, 'CVM Required'
- *Enhanced Contactless Reader Capabilities* Byte 3 Bit 7 to 1b, 'CVM Required'

If the reader is an offline-only reader(i.e. if the Terminal Type is 'x3' or 'x6') or the reader can determine that it is currently unable to go online for authorisation, then it will set *Enhanced Contactless Reader Capabilities* Byte 3 Bit 8 to 1b, 'Terminal is offline only'.

Requirements – Pre-PDOL Processing	
4.3.1.1a	The reader shall reset*Contactless Reader Capabilities*Byte 1 Bit 4 to 0b, 'CVM Not Required' and *Enhanced Contactless Reader Capabilities* byte 3 to 00.
4.3.1.2a	**If** the *Reader CVM Required Limit* is set to 1 **then** the reader shall set *Contactless Reader Capabilities* Byte 1 Bit 4 to 1b, 'CVM Required',andshall set *Enhanced Contactless Reader Capabilities* Byte 3 Bit 7 to 1b, 'CVM Required'.
4.3.1.3a	**If** the reader is an offline-only reader (Reader type 'x3' or 'x6') **or** the reader has determined that it is unable to go online, **then** the reader shall set *Enhanced Contactless Reader Capabilities* Byte 3 Bit 8 to 1b, 'Reader is Offline Only'.

4.3.2 PDOL Processing

The reader determines whether the optional *PDOL*was supplied by the card application in response to Application Selection.

If the *PDOL* is not present, then the reader formats the GET PROCESSING OPTIONS command with the command data field of '8300'.

Requirements – GPO Without PDOL Data	
4.3.2.1a	**If** the card did not specify a PDOL in the response to Application Selection, **then** the reader shall send the GET PROCESSING OPTIONS command with the command data field set to '8300'.

If the *PDOL* was received, the reader formats the GET PROCESSING OPTIONS command to include the data elements requested in the *PDOL* to be sent to the card with this command. The data elements for the *PDOL* must be formatted as defined by *[EMV 4.3 Book 3]*, section 5.4.

Requirements – PDOL Data in GPO	
4.3.2.2a	**If** the card specified a PDOL in response to Application Selection, **then** the reader shall send the GET PROCESSING OPTIONS command with the requested PDOL data, except as described in requirement 4.3.3.1a.

4.3.3 Terminal Type – Modified

If the *PDOL*requested *Terminal Type* (Tag '9F35') and does not contain the *Enhanced Contactless Reader Capabilities* (Tag '9F6E'), the reader returns *Terminal Type – Modified* (as shown in Table 4-3) instead of *Terminal Type*. These values are set by the reader based on the *Terminal Type* combined (OR'd) with a proprietary data element, *Contactless Reader Capabilities* (Tag '9F6D'), that is stored in the reader. See Table 4-1 and Table 4-2for the values of these data elements.

Note that the *Terminal Type – Modified* value is transient and valid only for the purpose of determining the contactless mode to be used for the current transaction being processed (i.e. EMV Mode or Mag-Stripe Mode).

The value of the (unmodified) *Terminal Type* (Tag '9F35') as defined in the configuration data for the Terminal must remain unchanged and only this unmodified Terminal Type should be present in any authorisation and financial submission messages that are sent to the acquirer.

For example:

If Terminal Type (Tag '9F35') in Terminal Configuration data = '22',
andContactless Reader Capabilities (Tag '9F6D') = 'C8',
then Terminal Type – Modified = 'EA'.

In the above example, the value of the *Terminal Type – Modified* that is provided to the Card in the GET PROCESSING OPTIONS command would be 'EA', however the value of the *Terminal Type* (Tag '9F35') that would be sent in any authorisation or submission messages to an acquirer would remain as '22'.

Table 4-1: Terminal Type – EMV Tag '9F35'

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
		0	1					Financial Institution
		1	0					Merchant
		1	1					Cardholder
					0	0	1	Attended – Online Only
					0	1	0	Attended – Offline with Online Capability
					0	1	1	Attended – Offline Only
					1	0	0	Unattended – Online Only
					1	0	1	Unattended – Offline with Online Capability
					1	1	0	Unattended – Offline Only

Table 4-2: Contactless Reader Capabilities – Tag '9F6D'

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0			0				Contactless: Mag-Stripe (Version 1.0)
0	0			1				RFU
0	1			0				Contactless: Mag-Stripe (Version 2.0) or Mag-Stripe – CVM Not Required (Version ≥ 3.0)
0	1			1				Contactless: Mag-Stripe – CVM Required (Version ≥ 3.0)
1	0			0				Contactless: EMV and Mag-Stripe (Version 2.0)
1	0			1				RFU
1	1			0				Contactless: EMV and Mag-Stripe - CVM Not Required (Version ≥ 3.0)
1	1			1				Contactless: EMV and Mag-Stripe - CVM Required (Version ≥ 3.0)

Note: Bits 6 and 5 and Bits 3 to 1 are reserved and must be set to zero. In *Terminal Type – Modified*, these bits will correspond to the values defined in EMV *Terminal Type*, Tag '9F35'.

Table 4-3 defines *Terminal Type – Modified*, which is returned from a contactless capable reader and consists of EMV *Terminal Type*, Tag '9F35' (Table 4-1) OR'd with contactless *Contactless Reader Capabilities*, Tag '9F6D' (Table 4-2).

Table 4-3: Terminal Type – Modified

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
		0	1					Financial Institution
		1	0					Merchant
		1	1					Cardholder
					0	0	1	Attended – Online Only
					0	1	0	Attended – Offline with Online Capability
					0	1	1	Attended – Offline Only
					1	0	0	Unattended – Online Only
					1	0	1	Unattended – Offline with Online Capability
					1	1	0	Unattended – Offline Only
0	0			0				Contactless:Mag-Stripe (Version 1.0)
0	1			0				Contactless:Mag-Stripe (Version 2.0) or Mag-Stripe – CVM Not Required (Version ≥ 3.0)
0	1			1				Contactless: Mag-Stripe – CVM Required (Version ≥ 3.0)
1	0			0				Contactless: EMV and Mag-Stripe (Version 2.0)
1	1			0				Contactless: EMV and Mag-Stripe - CVM Not Required (Version ≥ 3.0)
1	1			1				Contactless: EMV and Mag-Stripe - CVM Required (Version ≥ 3.0)

Requirements – GPO Includes Modified Terminal Type

4.3.3.1a **If**the card requests*Terminal Type*, Tag '9F35'
anddoes not request *Enhanced Contactless Reader Capabilities*, Tag '9F6E' in the PDOL,
then the reader shall send the GET PROCESSING OPTIONS command with the modified *Terminal Type* value which is the *Terminal Type* (Tag '9F35') OR'd with the *Contactless Reader Capabilities* (Tag '9F6D').

4.3.4 Enhanced Contactless Reader Capabilities

If the PDOL contains the *Enhanced Contactless Reader Capabilities*, as defined inTable 4-4, then this should be returned.

Table 4-4: Enhanced Contactless Reader Capabilities – EMV Tag '9F6E'

Terminal Capabilities Byte 1								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
x								1 = Contact mode supported
	1							1 = Contactless Mag-Stripe Mode supported
		0						0 = Contactless EMV full online mode not supported (full online mode is a legacy feature and is no longer supported)
			x					1 = Contactless EMV partial online mode supported
				1				1 = Contactless Mobile Supported
					0			RFU
						0		RFU
							0	RFU
Terminal CVM Capabilities Byte 2								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1								1 = Mobile CVM supported
	x							1 = Online PIN supported
		x						1 = Signature
			x					1 = Plaintext Offline PIN
				0				RFU
					0			RFU
						0		RFU
							0	RFU
Transaction Capabilities Byte 3								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
x								1 = Reader is offline only
	x							1 = CVM Required
		0						RFU
			0					RFU
				0				RFU
					0			RFU
						0		RFU
							0	RFU

Transaction Capabilities Byte 4								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
0								RFU
	0							RFU
		0						RFU
			0					RFU
				0				RFU
					0			RFU
						0		RFU
							0	RFU

Note: Tag 9F6E Byte 1 bit 6 (Contactless EMV full online mode not supported) is present for backward compatibility with previous versions of C4, but does not have any associated logic in determining the operating mode of the transaction. As such, any incorrect value of this bit setting must be ignored by the reader and not impact the transaction processing.

Requirements – GPO Includes Enhanced Contactless Reader Capabilities

4.3.4.1a **If**the card requested *Enhanced Contactless Reader Capabilities,* Tag '9F6E', in the PDOL,
then the reader shall send the GET PROCESSING OPTIONS command with the *Enhanced Contactless Reader Capabilities* value.

4.3.5 Terminal Type

If the *PDOL*requests*Terminal Type* (Tag '9F35') and also requests *Enhanced Contactless Reader Capabilities* (Tag ‘9F6E’), then the reader returns the (unmodified) *Terminal Type as well as the Enhanced Contactless Reader Capabilities* (Tag ‘9F6E’).

Requirements – GPO Includes (unmodified) Terminal Type	
4.3.5.1a	**If**the card requested, in the PDOL,*Terminal Type*, Tag '9F35' **and***Enhanced Contactless Reader Capabilities*, Tag '9F6E', **then** the reader shall send the GET PROCESSING OPTIONS command with the unmodified *Terminal Type* value as well as the *Enhanced Contactless Reader Capabilities*.

4.3.6 GPO Response Check

The reader must check that the format of the response data from the card is compliant to Format 1 or Format 2 as defined by *[EMV 4.3 Book 3]*, section 6.5.8.4.

Requirements – GPO Response Check	
4.3.6.1a	A reader shall check the GPO response data is formed as per *[EMV 4.3 Book 3]*, section 6.5.8.4.

If the response from the card returns the *AFL* and *AIP*, the reader must determine the operating mode for the transaction (see section 4.3.7), then proceed to Read Application Data.

4.3.7 Determination of Operating Mode

As discussed in section 2.1.1, the modes supported by the reader and by the card determine the operating mode that will be used for the transaction. The card sets Byte 2 Bit 8 in the *AIP* (see Table 5-2 on page 34) based on the capabilities of the reader and its own capabilities; the value of that bit determines the operating mode that the reader will use for the following processing steps.

If *AIP* Byte 2 Bit 8 is 1b, the transaction will use EMV mode.

If *AIP* Byte 2 Bit 8 is 0b, the transaction will use mag-stripe mode.

4.3.8 Determination of Transaction Support for Contactless Mobile

The reader must determine whether the transaction is to be processed as Contactless Mobile. If *AIP* Byte 2 Bit 7 is 1b, 'Contactless Mobile supported', then the transaction is to be processed as Contactless Mobile.

Ifthe *Mobile CVM Results*data item is present in the Card response and Byte 3,CVM Result,is '03', 'Mobile CVM Blocked',then the reader shall set *TVR* Byte 3 Bit 6 to 1b, 'Passcode Try Limit Exceeded'.

The *Mobile CVM Results*is to be retained by the reader for processing during Cardholder Verification, see section 8.

Requirements – Determination of Transaction Support for Contactless Mobile	
4.3.8.1a	**If** the Card indicates that it supports Contactless Mobile (*AIP* Byte 2 Bit 7 is 1b) **and***Mobile CVM Results*was present in the Card response to the GET PROCESSING OPTIONS command, **then:** **If**Byte 3,CVM Result,is '03', 'Mobile CVM Blocked', **then** the reader shall set *TVR* Byte 3 Bit 6 to 1b, 'Passcode Try Limit Exceeded'.

5 Read Application Data

5.1 Overview

The reader reads any card data necessary for completing the transaction using the READ RECORD command. The *AFL* is a list identifying the files and records that must be used in the processing of a transaction. The files that are read may be used for application purposes or as authentication data used during Offline Data Authentication for contactless mag-stripe mode transactions only, the reader shall issue a GET DATA command to retrieve the card's *ATC*. This is used during the *ATC* check as described in section 12, Online Processing.

5.2 Commands

READ RECORD

GET DATA

The application must support the READ RECORD and GET DATA command as described in *[EMV 4.3 Book 3]*, section 6.5.11 and section 6.5.7.

5.3 Processing Requirements

The reader must read all data records specified in the *AFL*. If a processing error occurs during this READ RECORD phase, the transaction must be aborted. All data read successfully from the card must be stored by the reader and used when required during the transaction.

The *AFL* must be processed according to *[EMV 4.3 Book 3]*, section 10.2. The encoding of the *AIP* is specified in Table 5-2.

During Read Application Data the card may also return the Card Interface and Payment Capabilities data element as defined in Table 5-1. The reader uses specifically the Card Interface and Payment Capabilities Byte 1 Bit 6, 'Contact EMV Interface Supported', in order to determine whether a request to use an alternative interface can be made.

If the reader supports Dynamic Transaction Limits or Delayed Authorisations, then it uses the *Card Interface and Payment Capabilities* data element to determine the Dynamic Transaction Limits to be applied and the usage settings for Delayed Authorisations respectively. Section 7, *Processing Restrictions,* gives further information on the application of Dynamic Transaction Limits and Delayed Authorisation Usage Control to determine the validity of the transaction.

If the card does not return *Card Interface and Payment Capabilities* data element, then the reader shall assume that:

- Alternative interface is supported by the card,
- A specific set of *Dynamic Reader Limits* are **not** specified by the card,
- Delayed Authorisations are supported by the card.

Table 5-1: Card Interface and Payment Capabilities – Tag '9F70'

Card Interface and Payment Capabilities Byte 1								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
X								1 = Keyed Data Entry Supported (Embossed or Printed PAN)
	X							1 = Physical Magnetic Stripe Supported
		X						1 = Contact EMV Interface Supported
			X					1 = Contactless EMV Interface Supported
				X				1 = Mobile Interface Supported
					0			RFU
						0		RFU
							0	RFU
Card Interface and Payment Capabilities Byte 2								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
X								1 = Delayed authorisation usage information present
	X							1 = Valid at domestic terminals performing contactless delayed authorisation
		X						1 = Valid at international terminals performing contactless delayed authorisation
			0					RFU
				0	0	0	0	No Dynamic Limit Set information available

				X	X	X	X	Values in the range 0001b to 1111b are assigned by the payment system operator to refer to a Dynamic Limit Set

It is not the reader's responsibility to ensure the integrity of the data read from the card, unless it is a specific requirement of the EMV specifications. As long as the data retrieved within a READ RECORD command correctly breaks down into valid Tag/Length/Value (TLV) data elements, the reader can assume it is valid, and the integrity of the data element placed in a card is the responsibility of the Issuer.

Unless processing a DOL, if a data object is read from the card that is not recognised thenthe unrecognised data object shall be ignored and the transaction shall continue as if the data object had not been present (exceptifthe data is required and shall be retained for kernel processing[1]).

It is important to ensure that an invalid data element value does not cause the reader to become unusable or lock up.

If any data element in Table 14-3 is missing, then the transaction ***must*** be terminated independent of the transaction mode.

For mag-stripe transactions there are further checks to be completed which are detailed in Section 7.2.4.

Processing rules governing data validation (missing or erroneous data on the card) are detailed in *[EMV 4.3 Book 3]*, section 7.5.

Requirements – READ RECORDs	
5.3.1.1a	The reader shall successfully read all records indicated by the *AFL*.
5.3.1.2a	The reader shall successfully read all data elements within all records and capture the correct values.
5.3.1.3a	**If** any mandatory data element is missing, **then** the reader shall terminate processing with a suitable error.
5.3.1.4a	**Unless** processing a DOL, **if** a data object is read from the card that is not recognised, **then** the unrecognised data object shall be ignored and the transaction shall continue as if the data object had not been present.

[1] For example, for Offline Data Authentication as stated in *[EMV 4.3 Book 3],* section 10.2.

Requirements – READ RECORDs

5.3.1.5a **If** a processing error occurs during the READ RECORD stage, **then** the reader shall abort the transaction with suitable indication and logging.

Table 5-2: Application Interchange Profile (*AIP*)

***AIP* Byte 1 (Leftmost)**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
0								RFU (Reserved for future use)
	x							1b = SDA supported 0b = SDA not supported
		0						DDA supported
			x					1b = Cardholder verification supported 0b = Cardholder verification not supported
				1				Terminal Risk Management is to be performed
					x			1b= Issuer Authentication is supported 0b = Issuer Authentication is not supported
						0		Reserved for use by EMV Contactless Specifications
							x	1b = CDA supported 0b = CDA not supported

***AIP* Byte 2 (Rightmost)**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
x								0b = Mag-Stripe Mode Only Supported 1b = EMV and Mag-Stripe Modes Supported
	x							0b = Contactless Mobile is not supported 1b = Contactless Mobile supported
		x						0b = Host Card Emulation (HCE) is not supported 1b = HCE is supported
			0					RFU
				0				RFU
					0			RFU
						0		RFU
							0	RFU

5.4 GET DATA

For contactless mag-stripe mode transactions only the reader shall issue a GET DATA command to retrieve the card's *ATC*. The GET DATA command must be performed as defined in *[EMV 4.3 Book 3]*, section 6.5.7. The value of the *ATC* shall be stored for use in the later *ATC* (risk management) check.

Requirements – GET DATA *ATC*

5.4.1.1a **If** the card or terminal setting indicates mag-stripe mode, **then** the terminal shall issue a GET DATA command on the *ATC*.

6 Offline Data Authentication

6.1 Overview

All Contactless readers must support the following two forms of Offline Data Authentication, as described in the *[EMV 4.3]* specifications:

SDA

CDA

The enablement of Offline Data Authentication must be configurable for deployment.

Requirements – Offline Data Authentication	
6.1.1.1a	All Readers shall support Static Data Authentication.
6.1.1.2a	All Readers shall support Combined DDA/Application Cryptogram Generation (CDA).
6.1.1.3a	The enablement of Offline Data Authentication in all Readers must be configurable for deployment.

6.2 Processing Requirements

If the reader has Offline Data Authentication enabled, then Offline Data Authentication must be performed as described in *[EMV 4.3 Book 2]*, sections 5 and 6, and *[EMV 4.3 Book 3]*, section 10.3.

The reader determines whether the card should be authenticated using either SDA or CDA based on the card's ability to support these methods, as indicated in the *AIP*. The Offline Data Authentication methods enabled by the reader are identified in *Terminal Capabilities* (Tag '9F33').

6.2.1 Offline Data Authentication not performed

If the reader is enabled for Offline Data Authentication and the transaction is to be declined offline, or if the reader is not enabled for Offline Data Authentication, then Offline Data Authentication ***must not*** be performed.

If Offline Data Authentication is not performed, then the reader must set TVR byte 1 bit 8 to 1b, 'Offline data authentication was not performed'.

Requirements - Offline Data Authentication not performed	
6.2.1.1a	**If** the card and the reader has ODA enabled, **and** the transaction is to be declined offline, **then** ODA is not performed.
6.2.1.2a	**If** the reader does not have ODA enabled, **then** ODA is not performed.
6.2.1.3a	**If** ODA is not performed, **then** the reader shall set TVR byte 1 bit 8 to 1b, 'Offline data authentication was not performed'.

6.2.2 Single ODA Method Supported

If CDA is the only Offline Data Authentication method supported by the cardand enabled by the reader, then the reader shall authenticate the card using CDA.

If SDA is the only Offline Data Authentication method supported by the cardand enabled by the reader, then the reader shall authenticate the card using SDA.

Requirements – Offline Data Authentication When Card Supports a Single Method	
6.2.2.1a	**If**a card indicates support of only CDA method, **and** the following conditions are true: • ODA is required • Reader has CDA enabled **then** the reader performs CDA.
6.2.2.2a	**If**a card indicates support of only SDA method, **and** the following conditions are true: • ODA is required • Reader has SDA enabled **then** the reader performs SDA.

6.2.3 Multiple ODA Methods Supported

If more than one Offline Data Authentication method is supported by the card and enabled by the reader, then CDA takes priority over SDA.

Requirements – Offline Data Authentication Priority

6.2.3.1a **If**a card indicates support of both SDA and CDA methods, **and** the following conditions are true:

- ODA is required
- Reader has both SDA and CDA **enabled**

then the reader performs CDA.

6.2.4 Scheme Certification Authority Public Keys

In order that Offline Data Authentication can be performed by a reader, the reader must be configured with the necessary *Certification Authority Public Keys (CAPK)*.

Requirements – Offline Data Authentication Keys

6.2.4.1a The terminal shall be able to hold a minimum of six Certification Authority Public Keys per AID.

6.2.5 Static Data Authentication

If SDA is determined to be performed, it must be performed as described in *[EMV 4.3 Book 2]*, sections 5 and 6, and *[EMV 4.3 Book 3]*, section 10.3.The reader ***must*** set the *TVR* byte 1 bit 2 to 1b, 'SDA Selected'.

During SDA the reader will validate the signed Static Application Data read from the card. If SDA fails, the reader must set *TVR* Byte 1 Bit 7 to 1b, 'Offline Static Data Authentication Failed'.

Requirements – Static Offline Data Authentication

6.2.5.1a	**If** the Offline Data Authentication method being employed is SDA, **then** • It shall be performed as per *[EMV 4.3 Book 2]*, section 5 and 6, and *[EMV 4.3 Book 3]*, section 10.3. • The reader shall set the *TVR* byte 1 bit 2 to 1b, 'SDA Selected'.
6.2.5.2a	**If** Static Data Authentication fails, **then** the reader shall set *TVR* Byte 1 Bit 7 to 1b, 'Offline Static Data Authentication Failed'.

6.2.6 Combined Dynamic Data Authentication / AC Generation

If CDA is to be performed, the processing for this takes place during 1st Terminal Action Analysis and 1st Card Action Analysis. CDA must be performed as specified in *[EMV 4.3 Book 2]*, section 6.6. If 1st Terminal Action Analysisdetermines that the transaction is requested to be transmitted online for authorisation, the first GENERATE AC command must request a CDA signature with the request for an ARQC.

If CDA fails, the reader must set *TVR* Byte 1 Bit 3 to 1b, 'CDA Failed'.

Requirements – Combined Dynamic Offline Data Authentication	
6.2.6.1a	**If** the Offline Data Authentication method being employed is CDA, **then** it shall be performed as per *[EMV 4.3 Book 2]*, section 6.6.
6.2.6.2a	**If** the Offline Data Authentication method being employed is CDA **and**the readerdetermines that an *ARQC*is to be requested at first GENERATE AC stage **then**the readershall request a CDA signature at first GENERATE AC stage.
6.2.6.3a	**If**CDAfails, **then** the reader shall set *TVR* Byte 1 Bit 3 to 1b, 'CDA Failed'.

7 Processing Restrictions

7.1 Overview

At this point in the transaction the reader uses the data gathered from the card during Read Application Data to ascertain the particular restrictions under which this transaction can be carried out.

7.2 Processing Requirements

The reader applies a set of dynamic transaction limits and performs several types of checks and adjustments:

- EMV Processing Restrictions
- Supplementary Processing Restrictions
- Data elements for mag-stripe mode

Depending on the reader configuration, the outcomes of the checks and adjustments are evaluated against a set of Issuer Action Codes (IACs) and Terminal Action Codes (TACs) during 1st Terminal Action Analysis.

7.2.1 Apply Dynamic Transaction Limits

The reader may contain three transaction amount limits, which are configured per Application Identifier (AID), which control the parameters of a contactless transaction. Specifically, a set of transaction amount limits may be comprised of one or more of the following:

- *ReaderContactless Transaction Limit* - the amount limit allowed for contactless transactions,
- *Reader Contactless Floor Limit* - the amount limit at which online authorisation is requested,and
- *Reader CVM Required Limit* - the amount limit at which cardholder verification is requested

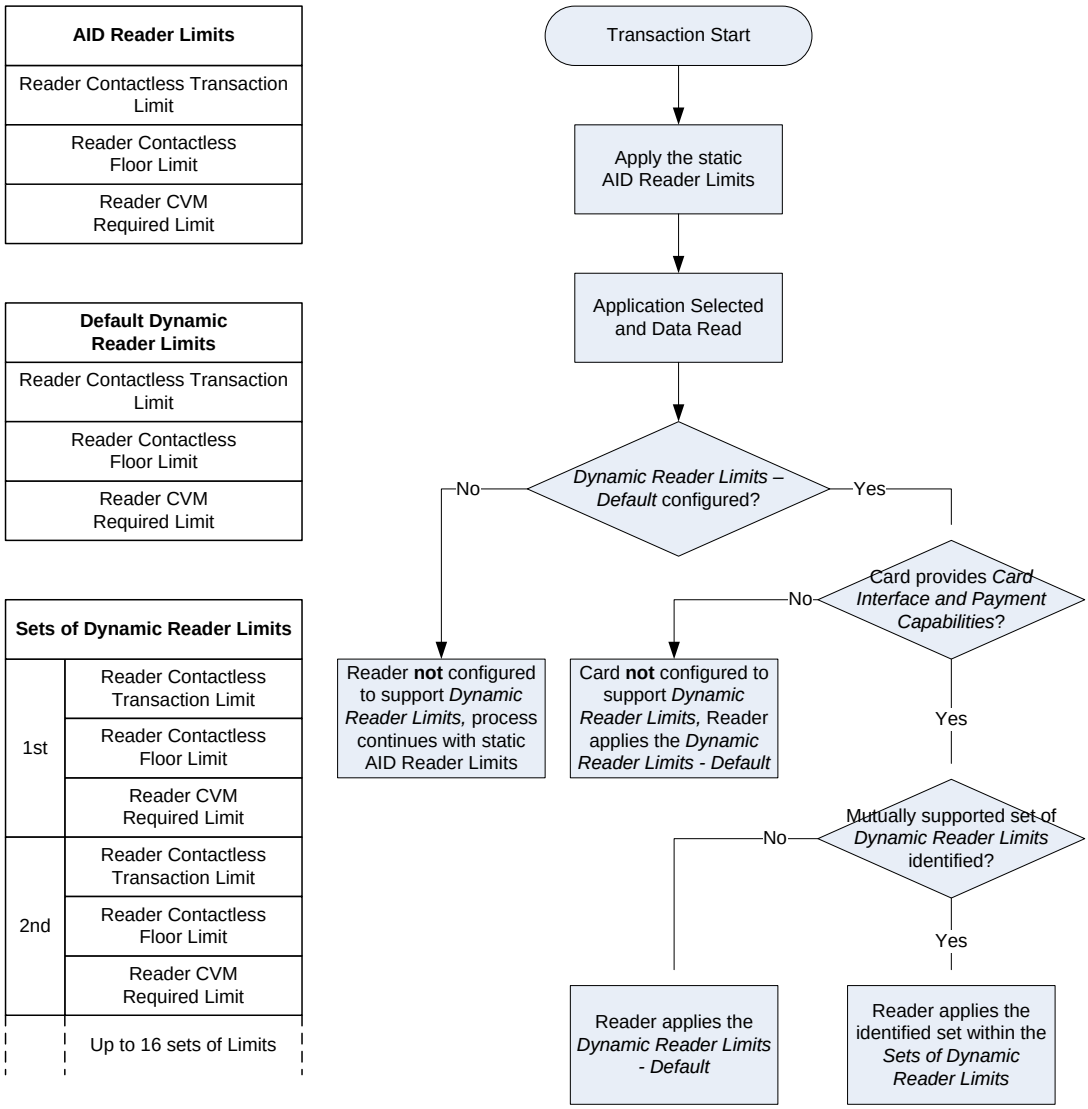
In addition to these AID Reader Limits, the reader may also contain one or more set of dynamic transaction amount limits, known as a set of *Dynamic Reader Limits.*

Multiple sets of *Dynamic Reader Limits* may bepresent on the reader, and are collectively referred to as the *Sets of Dynamic Reader Limits*. In order for the reader to support Dynamic Transaction Limits, then it **must** be configured with a default set of dynamic transaction amount limits, known as *Dynamic Reader Limits – Default*.

The reader must support this Dynamic Transaction Limits as a configurable function.

Figure 7-1illustrates the part of the process flow relevant to applying Dynamic Transaction Limits that control the parameters of a transaction:

Figure 7-1:Dynamic Reader Limits



1. Processing for Dynamic Transaction Limits shall be performed as follows: **If** the reader has *Dynamic Reader Limits – Default* configured,
   And the card provides the *Card Interface and Payment Capabilities* data element (Tag ‘9F70’),
   Then the reader shall attempt to select specific set of *Dynamic Reader Limits* from the *Sets of Dynamic Reader Limits*for a transaction,based on the ‘Dynamic Limits Set’ identifier value specified in*Card Interface and Payment Capabilities*Byte 2 Bits 4-1, with the following outcome:

a. **If**a corresponding set of *Dynamic Reader Limits* is successfully selected within the *Sets of Dynamic Reader Limits* present on the reader,
Then the referenced set of*Dynamic Reader Limits* from this selection is used by the reader to dynamically override the AID Reader Limits applied by Entry Point.
Else the reader shall apply *Dynamic Reader Limits – Default* as theset of *Dynamic Reader Limits* to override the AID Reader Limits applied by Entry Point.

2. **Elseif** the card does not provide the *Card Interface and Payment Capabilities* data element,
Then the Card is deemed to not support *Dynamic Reader* Limits and thereader shall apply *Dynamic Reader Limits – Default* as the set of*Dynamic Reader Limits* to override the AID Reader Limits applied by Entry Point.

3. **If** the reader does not have*Dynamic Reader Limits – Default* configured,
Then the reader does not support Dynamic Transaction Limits and thereader shall continue to apply the AID Reader Limits for the transaction.

Requirements – Processing Restrictions: Select Non-Default Dynamic Reader Limits	
7.2.1.1a	**If** Reader is configured with Dynamic Reader Limits – Default, **and**Card Interface and Payment Capabilities is present, **Then** the reader shall attempt to select a set of Dynamic Reader Limits from Sets of Dynamic Reader Limitsidentified using Card Interface and Payment Capabilities Byte 2 Bits 4-1, 'Dynamic Limits Set'.

Requirements – Processing Restrictions: Select Default Dynamic Reader Limits

7.2.1.2a **If** Reader is configured with *Dynamic Reader Limits – Default*,and any of the following is true:

- Card Interface and Payment Capabilities is absent,or
- *Card Interface and Payment Capabilities* Byte 2 Bits 4-1, 'Dynamic Limits Set', does not correspond to a set of *Dynamic Reader Limits* present on the Reader

Then the reader shall apply *Dynamic Reader Limits – Default* as the set of *Dynamic Reader Limits* to be used for the transaction.

Requirements – Processing Restrictions: Reader does not support Dynamic Transaction Limits

7.2.1.3a **If**the Reader is **not** configured with *Dynamic Reader Limits – Default*,
Then the reader does not support Dynamic Transaction Limits and the reader shall continue to apply the AID Reader Limits for the transaction.

If a set of *Dynamic Reader Limits* is selected and this set contains the relevant limit, the Kernel shall update the 'Contactless Application Not Allowed', 'Reader Contactless Floor Limit Exceeded' and 'Reader CVM Required Limit Exceeded' indicators as follows:

If*Amount, Authorised* is greater than or equal tothe Reader Contactless Transaction Limit in the selected *Dynamic Reader Limits*,
then set 'Contactless Application Not Allowed' to 1.

If*Amount, Authorised* is greater than the Reader Contactless Floor Limitin the selected *Dynamic Reader Limits*,
then set 'Reader Contactless Floor Limit Exceeded' to 1,
else set 'Reader Contactless Floor Limit Exceeded' to 0.

IfAmount, Authorised is greater than or equal to the Reader CVM Required Limitin the selected *Dynamic Reader Limits*,
then set 'Reader CVM Required Limit Exceeded' to 1,
else set 'Reader CVM Required Limit Exceeded' to 0.

Requirements – Processing Restrictions: Update Indicators Using Dynamic Reader Limits	
7.2.1.4a	**If** a set of *Dynamic Reader Limits* has been selected, **and**this set contains a Reader Contactless Transaction Limit**,** **and**the value of *Amount, Authorised* is greater than or equal to thislimit, **then**the Kernel shall set the 'Contactless Application Not Allowed' indicator to 1.
7.2.1.5a	**If** a set of *Dynamic Reader Limits* has been selected **and**this set contains a Reader Contactless Floor Limit, then: **If**the value of *Amount, Authorised* is greater than the Reader Contactless Floor Limit in the selected*Dynamic Reader Limits*, **then** the Kernel shall set the 'Reader Contactless Floor Limit Exceeded' indicator to 1, **else** the Kernel shall set the 'Reader Contactless Floor Limit Exceeded' indicator to 0.
7.2.1.6a	**If** a set of *Dynamic Reader Limits* has been selected **and**this set contains a Reader CVM Required Limit, then: **If**the value of Amount, Authorised is greater than or equal to the Reader CVM Required Limit in the selected*Dynamic Reader Limits***,** **then** the Kernel shall set the 'Reader CVM Required Limit Exceeded' indicator to 1, **else**the Kernel shall set the 'Reader CVM Required Limit Exceeded' indicator to 0.

If the 'Contactless Application Not Allowed' indicator is set to 1,and the transaction is taking place in EMV mode, and both the card and the reader support an alternative (contact) interface, the Kernel shall return control to Entry Point with a Final Outcome ***Try Another Interface***with the following parameter settings:

Start	**N/A**
Online Response Data	N/A
CVM	N/A
UI Request on Outcome Present	Yes • **Message Identifier:** '1D' (“Please insert card”) • **Status:** Processing Error: Conditions for use of contactless not satisfied • **Hold Time:** 0 • **Language Preference**
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

Requirements – Processing Restrictions: ‘Contactless Application NotAllowed’ indicator

7.2.1.7a **If** the ‘Contactless Application Not Allowed’ indicator is set to 1,
and the transaction is taking place in EMV mode,
and the reader supports an alternative (contact) interface,
and any of the following conditions are true:

- Card Interface and Payment Capabilities is not present,
- *Card Interface and Payment Capabilities* Byte 1 Bit 6 is set to 1b, ‘Contact EMV interface supported’,

then the kernel returns control to Entry Point, passing a Final Outcome of ***Try Another Interface***.

If the 'Contactless Application Not Allowed' indicator is set to 1, and either the reader or the card does not support an alternative interface, or the transaction is not taking place in EMV mode, then the Kernel shall return control to Entry Point with a Final Outcome of ***End Application*** and the following parameters set:

Start	N/A
Online Response Data	N/A
CVM	N/A
UI Request on Outcome Present	Yes • **Message Identifier:** '1C' ("Insert, Swipe or Try Another Card") • **Status:** Ready to Read • **Hold Time:** 0 • **Language Preference**
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

Requirements – Processing Restrictions: 'Contactless Application NotAllowed' indicator

7.2.1.8a **If** the 'Contactless Application Not Allowed' indicator is set to 1,
and*Card Interface and Payment Capabilities* Byte 1 Bit 6 is set to 0b, 'Contact EMV interface supported',
or the reader does not supports an alternative (contact) interface,
or the transaction is not taking place in EMV mode,
Then the kernel returns control to Entry Point, passing a FinalOutcome of ***End Application***.

7.2.2 EMV Processing Restrictions

The reader performs Processing Restrictions, as defined in *[EMV 4.3 Book 3]*, section 10.4, and *[EMV 4.3 Book 4]*, sections 6.3.3 and 6.7.2, to determine whether the transaction should be allowed. Processing Restrictions cover the following mandatory checks performed by the reader:

7.2.2.1 Application Version Number

Application Version Number, if present in the card, is compared to a reader resident *Application Version Number*. The reader must store an *Application Version Number* for each *Application Identifier (AID)* supported by the reader.

Requirements – Processing Restrictions: Application Version Number	
7.2.2.1a	The reader shall compare the application version number returned by the card in the READ RECORD phase to the one held by the reader. **If** the application version number returned by the card is different to that held by the reader, **then** the reader shall set *TVR* Byte 2 Bit 8 to 1b, 'ICC and terminal have different application versions'.

7.2.2.2 Application Usage Control

Application Usage Control (AUC) is used to determine whether any geographical or transaction type restrictions have been imposed on the card product, e.g. it may be used to restrict a card's use for domestic or international cash, or goods and services:

Domestic Usage Check – If the *Issuer Country Code* read from the card is equal to the *Terminal Country Code*, then the transaction is defined as 'Domestic'. The reader checks that the transaction type (e.g. Cash, Goods, or Services) for the transaction being processed is permitted in a 'Domestic' environment according to the card's *AUC*.

Requirements – Processing Restrictions: AUC Domestic

7.2.2.2a The reader shall compare the *Issuer Country Code* read from the card to the *Terminal Country Code*.

If the country codes are the same,
then:

The transaction is considered Domestic.

Ifthe *Application Usage Control*indicates that the card is **not** valid for the transaction type being performed (domestic cash, goods, or services),
then the reader shall set *TVR* Byte 2 Bit 5 to 1b, 'Requested service not allowed for card product'.

International Usage Check - If the *Issuer Country Code* read from the card is not equal to the *Terminal Country Code*, then the transaction is defined as 'International'. The reader checks that the transaction type for the transaction being processed is permitted in an 'International' environment according to the card's *AUC*.

Requirements – Processing Restrictions: AUC International

7.2.2.3a The reader shall compare the *Issuer Country Code* read from the card to the *Terminal Country Code*.

If the country codes are different,
then:

The transaction is considered International.

Ifthe *Application Usage Control*indicates that the card is **not** valid for the transaction type being performed (international cash, goods, or services),
then the reader shall set *TVR* Byte 2 Bit 5 to 1b, 'Requested service not allowed for card product'.

Transaction Environment Check – If the reader is an ATM, then the reader checks that the card's *AUC* has Byte 1 Bit 2 set to 1b, 'Valid for use at an ATM'. If the reader is other than an ATM (e.g. POS), then the reader must verify that the card's *AUC* has Byte 1 Bit 1 set to 1b, 'Valid at Readers other than an ATM'.

Requirements – Processing Restrictions: AUC Environment for an ATM

7.2.2.4a **If**thereader is an ATM,
then:

The reader shall check the *Application Usage Control* to determine whether the card can be used at an ATM.

If the transaction cannot be performed at an ATM,
then the reader shall set *TVR* Byte 2 Bit 5 to 1b, 'Requested service not allowed for card product'.

Requirements – Processing Restrictions: AUC Environment for other than an ATM

7.2.2.5a **If** the reader is not an ATM,
then:

The readershall check the *Application Usage Control* to determine whether the card can be used at other than an ATM.

If the transaction cannot be performed at other than an ATM,
then the readershall set *TVR* Byte 2 Bit 5 to 1b, 'Requested service not allowed for card product'.

Table 7-1illustrates the bit settings for the AUC data element retrieved from the card.

Table 7-1:Bit Settings for Application Usage Control (AUC)

Byte 1 (leftmost)								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
X								1 = Valid for Domestic Cash Transactions
	X							1 = Valid for International Cash Transactions
		X						1 = Valid for Domestic Goods
			X					1 = Valid for International Goods
				X				1 = Valid for Domestic Services
					X			1 = Valid for International Services
						X		1 = Valid at ATMs
							X	1 = Valid at Terminals other than ATMs

Byte 2 (rightmost)								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
0								0 = Domestic Cashback not allowed
	0							0 = International Cashback not allowed
		0						RFU by EMV Specifications
			0					RFU by EMV Specifications
				0				RFU by EMV Specifications
					0			RFU by EMV Specifications
						0		RFU by EMV Specifications
							0	RFU by EMV Specifications

Note: The ISO Country Code of the Chip Card Issuer determines whether a transaction is domestic or international. If the ISO Country Code for the Chip Card and the reader are the same, then the transaction is domestic. If the ISO Country Code in the reader is different from the Chip Card, then the transaction is international.

7.2.2.3 Effective and Expiration Date Checking

Effective and expiration dates are checked to ensure that the application is not pre-valid and not expired.

If the transaction date is prior to the *Application Effective Date*, the readermust set *TVR* Byte 2 Bit 6 to 1b, 'Application not effective yet'.

If the transaction date is past the *Application Expiration Date*, the readermust set *TVR* Byte 2 Bit 7 to 1b, 'Application Expired'.

Requirements – Processing Restrictions: Dates

7.2.2.6a **If** the transaction date is prior to the card *Application Effective Date*,
then the reader shall set *TVR* Byte 2 Bit 6 to 1b, 'Application not effective yet'.

7.2.2.7a **If** the transaction date is past the card *Application Expiration Date*,
then the readershall set *TVR* Byte 2 Bit 7 to 1b, 'Application Expired'.

7.2.3 Supplementary Processing Restrictions

This only applies to Delayed Authorisation terminals.

7.2.3.1 Delayed Authorisation Usage Check

The Delayed Authorisation Usage Checkbits in the Card Interface and Payment Capabilities data element are used to determine whether any restrictionhas been imposed on the use of the card product when a delayed authorisation is to be performed.

If the *Card Interface and Payment Capabilities data element is not* present, then delayed authorisations are permitted if supported by the reader.

Domestic Delayed Authorisation Usage Check – If the *Issuer Country Code* read from the card is equal to the *Terminal Country Code*, then the transaction is defined as 'Domestic'. If the readersupports delayed authorisation, it checks whether a delayed authorisation transaction is permitted in a 'Domestic' environment according to the card's *Delayed Authorisation Usage Check bits*.

Requirements – Supplementary Processing Restrictions: Domestic Delayed Authorisation

7.2.3.1a **If***Card Interface and Payment Capabilities* is present
and*Card Interface and Payment Capabilities Byte 2 Bit 8 is set to 1b*
and thereaderindicates that it supports Delayed Authorisations,
then:

The readershall compare the *Issuer Country Code* read from the card to the *Terminal Country Code*.

If the country codes are the same,
then:

- The transaction is considered Domestic.
- **If***Card Interface and Payment Capabilities Byte 2 Bit 7 is set to 0b*,
  then the readershall set *TVR* Byte 2 Bit 5 to 1b, 'Requested service not allowed for card product'.

International Delayed Authorisation Usage Check – If the *Issuer Country Code* read from the card is not equal to the *Terminal Country Code*, then the transaction is defined as 'International'. If the readersupports delayed authorisation, it checks whether a delayed authorisation transaction is permitted in an 'International' environment according to the card's *Delayed Authorisation Usage Check bits*.

Requirements – Supplementary Processing Restrictions: International Delayed Authorisation

7.2.3.2a **If***Card Interface and Payment Capabilities* is present
and*Card Interface and Payment Capabilities Byte 2 Bit 8 is set to 1b*
and thereaderindicates that it supports Delayed Authorisations,
then:

The readershall compare the *Issuer Country Code* read from the card to the *Terminal Country Code*.

If the country codes are different,
then:

- The transaction is considered International.
- **If***Card Interface and Payment Capabilities Byte 2 Bit 6 is set to 0b*,
  then the readershall set *TVR* Byte 2 Bit 5 to 1b,
  'Requested service not allowed for card product'.

7.2.4 Data Elements for Mag-Stripe Mode

If the transaction is performed in mag-stripe mode, the readermust ensure that all data elements needed for the Acquirer message generation are present. All data elements in Table 14-4 and Table 14-5 must be retrieved from the Card.

If any of the listed data elements is missing, then the transaction is terminated and the kernel returns control to Entry Point with a Final Outcome of ***End Application*** and the following parameters set:

Start	N/A
Online Response Data	N/A
CVM	N/A
UI Request on Outcome Present	Yes • **Message Identifier:** '1C' (“Insert, Swipe or Try Another Card”) • **Status:** Ready to Read • **Hold Time:** 0 • **Language Preference**
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

Requirements – Data Elements for Mag-Stripe Mode

7.2.4.1a **If** the transaction is performed in Mag-stripe mode
and any of the *elements in* Table 14-4 *and* Table 14-5are not retrieved successfully from the card,
then the kernel terminates the transaction and returns control to Entry Point with a Final Outcome of ***End Application***.

8 Cardholder Verification

8.1 Overview

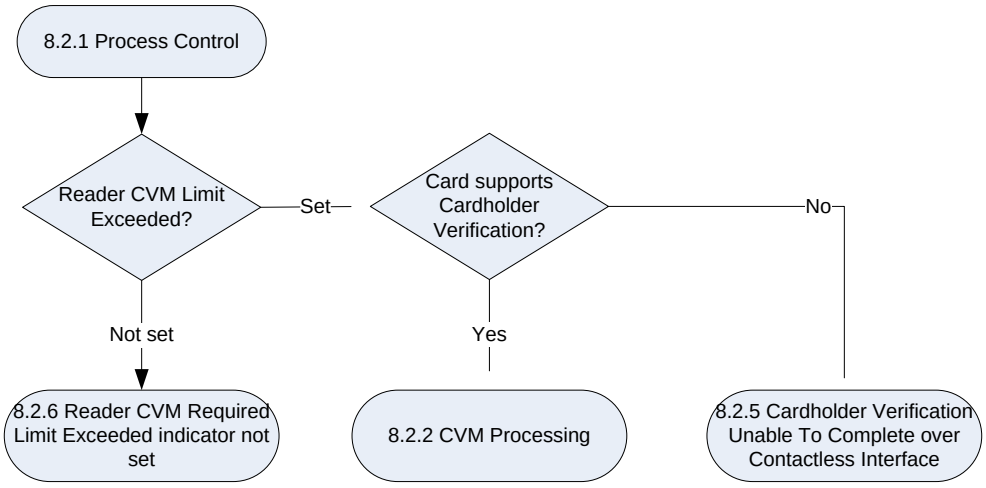
Cardholder Verification must be performed as defined in this section with additional reference to *Cardholder Verification Methods (CVM) List* processing as detailed in *[EMV 4.3 Book 3]*, section 10.5, and *[EMV 4.3 Book 4]*, section 6.3.4.

The card Issuer is allowed to determine the CVM(s) to be used with its cards via the use of the *CVM List*. This list is used to identify the priority order of the various CVM(s) supported, starting with the preferred CVM of the Issuer.

8.2 Processing Requirements

8.2.1 Process Control

Figure 8-1: Process Control



Cardholder Verification processing must be performed as follows:

If the *Reader CVM Required Limit Exceeded* indicator is set,
then:

- **If** the Card Supports Cardholder Verification (*AIP* Byte 1 Bit 5 is set to 1b), **then** perform Cardholder Verification processing as described in section 8.2.2, *CVM Processing*.

- **Else** if the Card does not support Cardholder Verification (*AIP* Byte 1 Bit 5 is set to 0b),
  thencontinue processing as described in section 8.2.5, *Cardholder Verification Unable To Complete over Contactless Interface*.

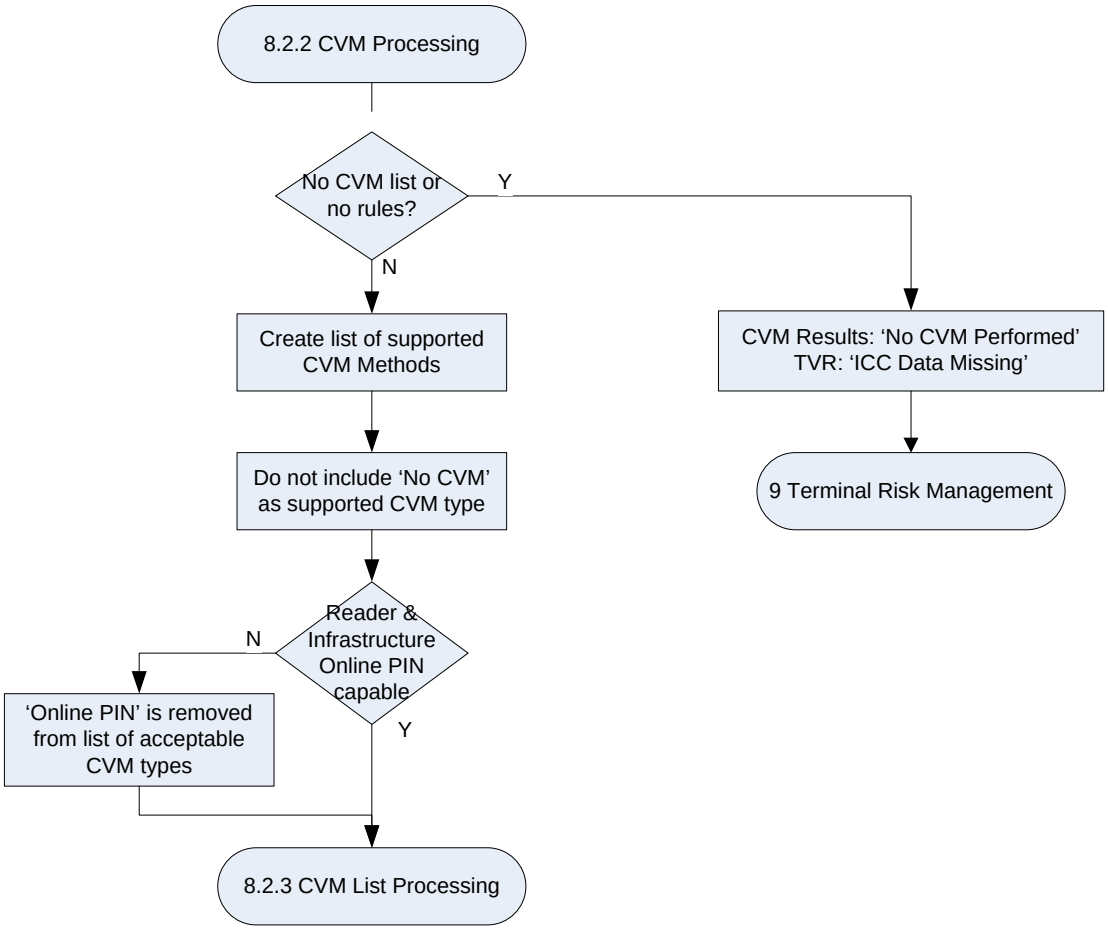
Otherwise perform Cardholder Verification processing as described in section 8.2.6,*Reader CVM Required Limit Exceeded Indicator Not Set*.

Requirements –Cardholder Verification Processing	
8.2.1.1a	**If***Reader CVM Required Limit Exceeded indicator is set,* **and**the Card supports Cardholder Verification (*AIP* Byte 1 Bit 5 is set to 1b), **then** the reader shall perform Cardholder Verification processing as described in section 8.2.2, *CVM Processing*.
8.2.1.2a	**If***Reader CVM Required Limit Exceeded indicator is set,* **and**the Card does not supports Cardholder Verification (*AIP* Byte 1 Bit 5 is set to 0b), **then** the reader shall complete transaction processing as described in section 8.2.5, *Cardholder Verification Unable To Complete over Contactless Interface*.
8.2.1.3a	**If***Reader CVM Required Limit Exceeded indicator is not set,* ***then** the reader* shall perform Cardholder Verification processing as described in section 8.2.6, *Reader CVM Required Limit Exceeded Indicator Not Set.*

8.2.2 *CVM Processing*

If the *Reader CVM Required Limit Exceeded* indicator is set, then CVM Processing shall continue as follows.

Figure 8-2: CVM Processing



8.2.2.1 CVM List Empty or Not Present

If the CVM List is not present or is empty (i.e. present but does not contain any rules),
then:

- The reader shallset CVM Results to '3F 00 00'–'No CVM performed'.
- The reader shall set *TVR* Byte 1 Bit 6 to 1b, 'ICC Data Missing'.
- CVM processing is complete, and Terminal Risk Management is performed.

else CVM Processing continues as in section 8.2.2.2.

Requirements – Card Supports Cardholder Verification but CVM List Not Present

8.2.2.1a **If** the Card indicates it supports Cardholder Verification (*AIP* Byte 1 Bit 5 is set to 1b),
andthe CVM list is not present or is empty,
then the reader shall set *TVR* Byte 1 Bit 6 to 1b, 'ICC Data Missing', and shall set CVM Results to '3F 00 00',
and processing continues with Terminal Risk Management.

8.2.2.2 Supported CVM Methods

The reader shall create a list of supported CVM methods, as described in *[EMV 4.3 Book 3], section 10.5*, with the additional conditions:

> The reader shall not include 'No CVM required' as one of its supported methods.
>
> If the reader or the associated acquiring infrastructure does not support Online PIN, then 'Online PIN' shall not be included as one of the supported methods.

Once the list of supported CVM methods is created, the process continues as described in Section8.2.3, *CVM List Processing*.

Requirements – Reader CVM Supported Methods

8.2.2.2a The reader creates a list of Supported CVM Methodswith the below conditions, following which processing proceeds as described in Section8.2.3, *CVM List Processing*:

- The reader must not include 'No CVM required' as one of its supported methods.
- **If** either the reader or the associated acquiring infrastructure for the payment system card being processed does not support the Cardholder Verification Method of Online PIN,
  then the reader must not include 'Online PIN' as one of its supported methods.

8.2.3 CVM List Processing

CVM List Processing proceeds as described in *[EMV 4.3 Book 3]*, section 10.5, with the following modifications:

- **If** the card contains a *CVM List* with a CVM method which is mutually supported by both card and reader, and satisfies the CVM condition codes, **then** the reader shall store the CVM determined and use it to set the CVM Outcome parameter when subsequently requested (i.e. as part of Final Outcome parameter settings during a request for online processing or transaction completion).
- 'Online PIN' CVM is carried out as per Section 8.2.3.1, *Online PIN CVM*.
- 'Mobile CVM' is processed as per Section 8.2.3.2, *Mobile CVM*.
- **If** there is no common CVM method shared by both the card and reader, **then** the processing continues as described in Section 8.2.5, *Cardholder Verification Unable To Complete over Contactless Interface*.

Requirements – CVM List Processing

8.2.3.1a **If** all of the following are true:

- The Reader *CVM Required Limit Exceeded* indicator is set.
- The card supports Cardholder Verification (Card *AIP* Byte 1 Bit 5 is set to 1b).
- The *CVM List* is present and contains at least one entry.

Then, the following steps are carried out**:**

1. The reader shall examine the first CVM in the CVM List.
2. **If** the reader supports the CVM, and the Condition Code of the CVM method is equal to '00', '02' or '03', **then** the reader shall save the matching CVM and return the CVM recorded in the Final Outcome.
3. **Else if** another CVM is present in the *CVM List*, **then** the reader shall repeat the process in this requirement from step 2, using the next CVM in the *CVM List*.

8.2.3.1 Online PIN CVM

If the applicable CVM for the transaction is *Online PIN*, then the reader shall set the TVR Byte 3 Bit 3, 'Online PIN entered' in anticipation of online PIN being entered. The process then proceeds with Section 9, *Terminal Risk Management*.

The online PIN shall be entered after *1st Card Action Analysis*, once the card processing is complete and the card can be removed from the reader. Following PIN entry, the reader proceeds to online authorisation as described in Section 12, *Online Processing* (online PIN transactions require online authorisation).

Requirements – Online PIN	
8.2.3.2a	**If** Online PIN CVM is to be performed, **then**the reader shall set *TVR* Byte 3 Bit 3 to 1b, 'Online PIN entered' and request a PIN after the card is removed.

8.2.3.2 Mobile CVM

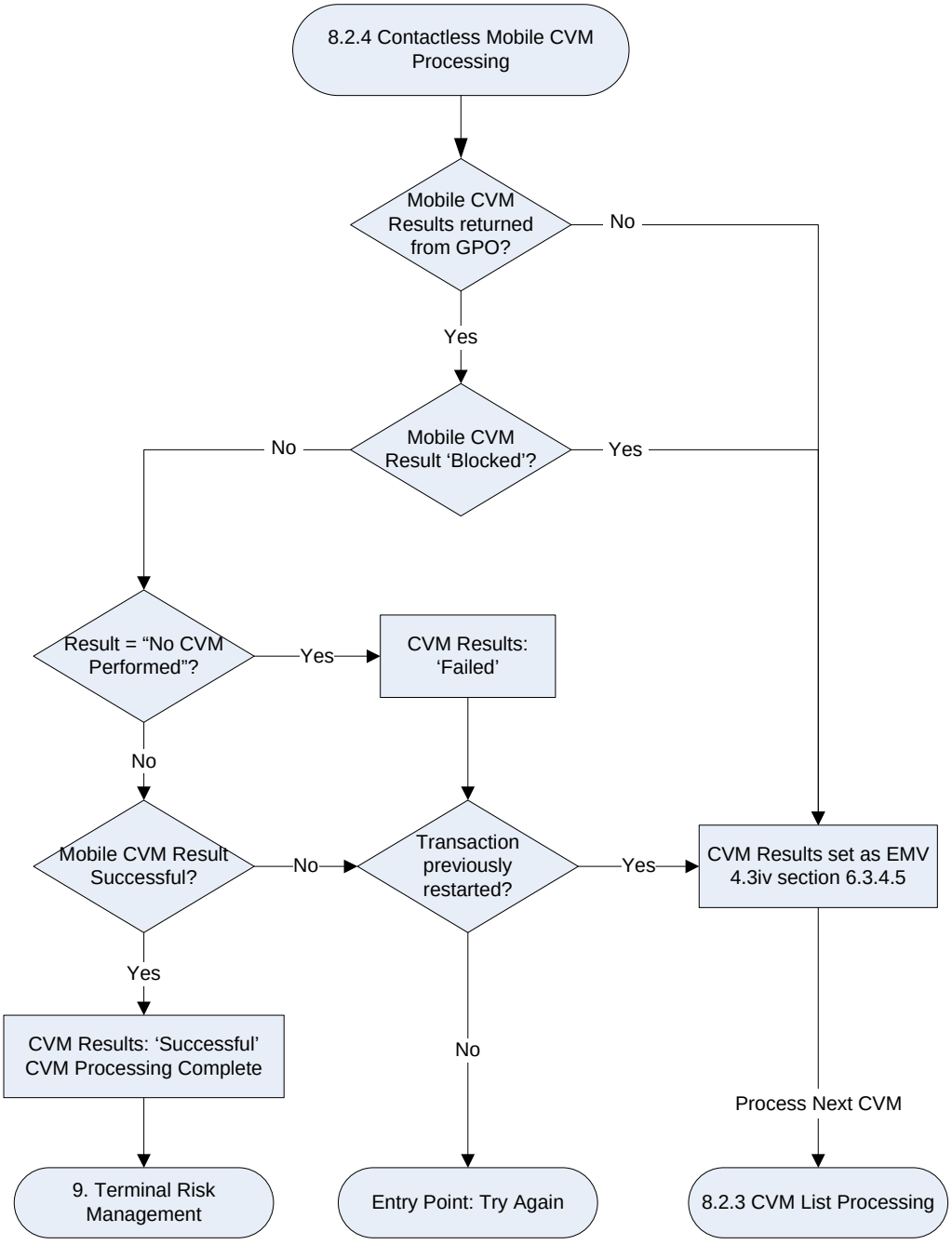
In the context of Contactless Mobile transaction processing, *Plaintext Offline PIN* is redefined as '*Mobile CVM*'. (The *Mobile CVM* is typically an offline "Passcode" stored in the Card application.)

Reader support for *Mobile CVM* is indicated by the *Enhanced Contactless Reader Capabilities* Byte 2 Bit 8 as 1b, 'Mobile CVM is Supported'. Card support for *Mobile CVM* is indicated in the CV Rule, as Byte 1 Bit 6-1 = 000001b, 'Plaintext PIN verification performed by ICC'.

When the applicable CVM is *Mobile CVM*, then CVM processing is carried out as described in section 8.2.4, *Contactless Mobile CVM Processing*.

8.2.4 Contactless Mobile CVM Processing

Figure 8-3: Contactless Mobile CVM Processing



When Mobile CVM is supported, the Card Application includes the *Mobile CVM Results* as defined in Table 8-1 in the Format 2 response to the GET PROCESSING OPTIONS command.

Table 8-1:Mobile CVM Results – Tag '9F71'

***Mobile CVM Results* Byte 1 – CVM Performed**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
0	0	0	0	0	0	0	1	Mobile CVM Performed
0	0	1	1	1	1	1	1	No CVM Performed
***Mobile CVM Results* Byte 2 – CVM Condition**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
0	0	0	0	0	0	0	0	Mobile CVM not Required
0	0	0	0	0	0	1	1	Terminal Required CVM
***Mobile CVM Results* Byte 3 – CVM Result**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
0	0	0	0	0	0	0	0	Unknown (if Mobile CVM not performed)
0	0	0	0	0	0	0	1	Mobile CVM Failed
0	0	0	0	0	0	1	0	Mobile CVM Successful
0	0	0	0	0	0	1	1	Mobile CVM Blocked

When the reader is to perform *Mobile CVM* as a result of CVM List processing, it must not be carried out as ‘Plaintext Offline PIN’ described in *[EMV 4.3 Book 3]*, section 10.5.1, but must be processed as follows:

If *Mobile CVM Results* was not returned in the GET PROCESSING OPTIONS response, the readershall consider that the Mobile CVM is unsuccessfuland set the *CVM results* as per *[EMV 4.3 Book 4]*, section 6.3.4.5. The processing then continues as defined in section 8.2.3, *CVM List Processing*.

If *Mobile CVM Results* was returned in the GET PROCESSING OPTIONS response, then:

- **If** CVM Result (Byte 3 of *Mobile CVM Results*) is '03', ‘Mobile CVM Blocked’,
  thenthe readershall consider that the Mobile CVM is unsuccessful and set the *CVM results* as per *[EMV 4.3 Book 4]*, section 6.3.4.5. The processing then continues as defined in section 8.2.3, *CVM List Processing*.
- *Mobile CVM Results* Byte 1, CVM Performed, is processed as follows:
  - **If***Mobile CVM Results*Byte 1 is a value other than ‘3F’ or ‘01’, **then***Mobile CVM* is considered unsuccessful andtheprocess continues as per Section 8.2.4.1, *Mobile CVM Outcome*.

- **If***Mobile CVM Results* Byte 1 is equal to '3F' (‘No CVM Performed’),
  then the reader shall set *CVM Results*, Byte 3, CVM Result to ‘01’, ‘Failed’ and shall consider that Mobile CVM is unsuccessful.The process continues as per Section 8.2.4.1, *Mobile CVM Outcome*.
- **If***Mobile CVM Results* Byte 1 is equal to '01' (‘Mobile CVM Performed’**),**
  then CVM method processing continues byexamining*Mobile CVM Results* Byte 3, CVM Result, as perbelow.

- *Mobile CVM Results* Byte 3, CVM Result, is processed as follows:
  - **If** Byte 3 is equal to '02',‘Mobile CVM Successful’,
    then the reader*s*ets *CVM Results*, Byte 3, CVM Result to '02',‘Successful’. It shall consider that Mobile CVM is successful and the process continues as per Section 8.2.4.1, *Mobile CVM Outcome*.
    else the reader sets CVM Results, Byte 3, CVM Result to '01',‘Failed’. It shall consider that Mobile CVMis unsuccessfuland the process continues as per Section 8.2.4.1, *Mobile CVMOutcome*.

8.2.4.1 Mobile CVM Outcome

If*Mobile CVM* is considered successful **then** the CVM List processing is complete. The process continues with Section9, *Terminal Risk Management*.

If*Mobile CVM* is considered unsuccessful **and** the current transaction has not previously been restarted, **then** the reader sets a Restart indicator to indicate that the transaction is exiting with a ***Try Again*** Outcome with the below parameters set:

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:** 10 • **Language Preference**
UI Request on Restart Present	Yes • **Message Identifier:** '21' (“Present Card Again”) • **Status: Processing Error** • **Hold Time:** 0 • **Language Preference**
Data Record Present	No
Discretionary Data Present	No
Alternate Interface Preference	N/A
Receipt	N/A
Field Off Request	N/A
Removal Timeout	Zero

If*Mobile CVM* is considered unsuccessful **and** the current transaction has previously been restarted, **then***Mobile CVM* method has failed and the CVM list processing continues as defined in section 8.2.3, *CVM List Processing*.

Requirements – Contactless Mobile CVM Processing	
8.2.4.1a	**If***Mobile CVM Results* was not returned in the GET PROCESSING OPTIONS response, **then**Mobile CVM is unsuccessful the *CVM results* are set as per *[EMV 4.3 Book 4]*, section 6.3.4.5.The processing then continues with CVM List processing as defined in section 8.2.3, *CVM List Processing*.
8.2.4.2a	**If***Mobile CVM Results* Byte 3, CVM Result, is equal to '03', 'Mobile CVM Blocked', **then** Mobile CVM is unsuccessful the *CVM results* are set as per *[EMV 4.3 Book 4]*, section 6.3.4.5.The processing then continues with CVM List processing as defined in section 8.2.3, *CVM List Processing*.
8.2.4.3a	**If***Mobile CVM Results* Byte 1, CVM Performed, is equal to '3F', 'No CVM performed', **and** the transaction has previously been restarted, **then** Mobile CVM is unsuccessful and the reader shall set *CVM Results* Byte 3, CVM Result to '01', 'Failed' **and**CVM List processing continues as defined in section 8.2.3, *CVM List Processing*.
8.2.4.4a	**If***Mobile CVM Results* Byte 1, CVM Performed, is equal to '3F', 'No CVM performed', **and** the transaction has not previously been restarted, **then**the kernel returns control to Entry Point, passing a Final Outcome of ***Try Again***.
8.2.4.5a	**If***Mobile CVM Results* Byte 1, CVM Performed, is equal to '01', **and***Mobile CVM Results* Byte 3, CVM Result is equal to '02', 'Successful', **then** the reader considers Mobile CVM successful and**:** • Sets CVM Results, Byte 3, CVM Result to '02', 'Successful' • Continues the transaction process with Section 9, *Terminal Risk Management*.

Requirements – Contactless Mobile CVM Processing	
8.2.4.6a	**If***Mobile CVM Results* Byte 1, CVM Performed, is equal to '01', **and***Mobile CVM Results* Byte 3, CVM Result, is equal to '01', 'Failed', **then** Mobile CVM is unsuccessful and the reader shall set CVM Results, Byte 3, CVM Result, to '01', 'Failed'.
8.2.4.7a	**If** all of the following are true: • *Mobile CVM Results* Byte 1, CVM Performed, is equal to '01', • *Mobile CVM Results* Byte 3, CVM Result, is **not** equal to '02', 'Successful', • Transaction has not previously been restarted **Then** the kernel returns control to Entry Point, passing a Final Outcome of ***Try Again***.
8.2.4.8a	**If** all of the following are true: • *Mobile CVM Results* Byte 1, CVM Performed, is equal to '01', • *Mobile CVM Results* Byte 3, CVM Result, is **not** equal to '02', 'Successful', • Transaction has previously been restarted **Then** Mobile CVM has failed and the reader shall set *CVM Results*, Byte 3, CVM Result, to '01', 'Failed' and CVM List processing continues as defined in section 8.2.3, *CVM List Processing*.
8.2.4.9a	**If** all of the following are true: • *Mobile CVM Results* Byte 1, CVM Performed, is **not** equal to '3F', 'No CVM performed' or '01', 'CVM Performed', • The transaction has previously been restarted, **Then** Mobile CVM has failed and the reader shall set *CVM Results* Byte 3, CVM Result to '01', 'Failed' and CVM List processing continues as defined in section 8.2.3, *CVM List Processing*.

Requirements – Contactless Mobile CVM Processing

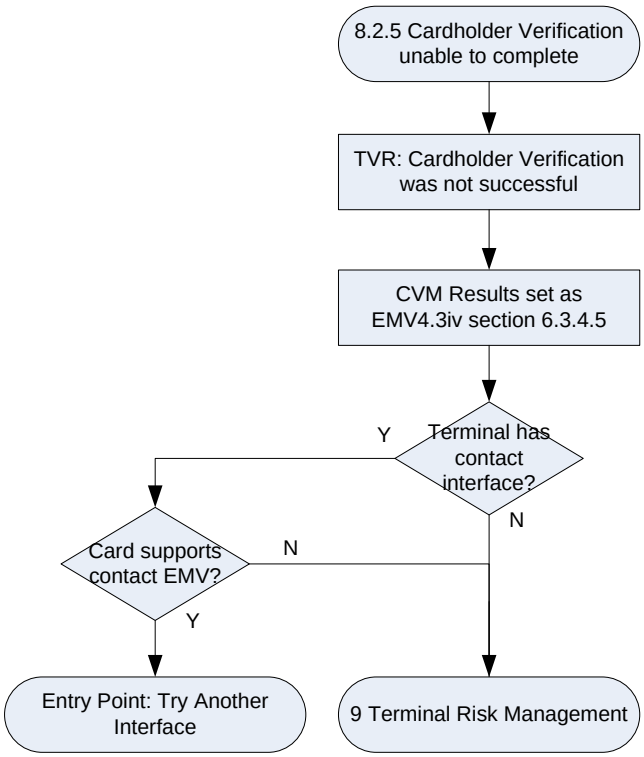
8.2.4.10a **If** all of the following are true:

- *Mobile CVM Results* Byte 1, CVM Performed, is **not** equal to '3F', 'No CVM performed' or '01', 'CVM performed',
- The transaction has not previously been restarted,

Then the kernel returns control to Entry Point, passing a Final Outcome of ***Try Again***.

8.2.5 Cardholder Verification Unable To Complete over Contactless Interface

Figure 8-4: Cardholder Verification Unable To Complete



If Cardholder Verification cannot be performed over the Contactless interface, **then**:

The readershall set *TVR* Byte 3 Bit 8 to 1b, 'Cardholder Verification was not successful'.

CVM Results to '3F 00 01'.

If the transaction is taking place in EMV mode and the reader has a Contact interface **then**:

If the *Card Interface and Payment Capabilities* Byte 1 Bit 6 is 1b, 'Contact EMV Interface supported',
or if *Card Interface and Payment Capabilities*is not present,
then the kernel returns control to Entry Point, passing a Final Outcome of ***Try Another Interface*** with the following parameter settings:

Start	**N/A**
Online Response Data	N/A
CVM	N/A
UI Request on Outcome Present	Yes • **Message Identifier:**'1D' (“Please insert card”) • **Status:** Processing Error: Conditions for use of contactless not satisfied • **Hold Time:** 0 • **Language Preference**
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

Else if the *Card Interface and Payment Capabilities* Byte 1 Bit 6 is 0b, ‘Contact EMV Interface supported’, then CVM processing is completed and the transaction continues with Terminal Risk Management.

Else if the transaction is not taking place in EMV mode or the reader does not have a Contact interface then CVM processing is completed and the transaction continues with Terminal Risk Management.

Requirements – Cardholder Verification Unable To Continue over Contactless Interface

8.2.5.1a **If** all of the following are true:

The *Reader CVM Required Limit Exceeded* indicator is set.

The card supports Cardholder Verification (Card *AIP* Byte 1 Bit 5 is set to 1b).

There is not a mutually supported CVM across the contactless interface.

The transaction is taking place in EMV mode and the reader has an alternative interface.

The *Card Interface and Payment Capabilities*Byte 1 Bit 6 is set to 1b, 'Contact EMV Interface supported'.

Then the reader shall:

Set *TVR* Byte 3 Bit 8 to 1b, 'Cardholder Verification was not successful'.

Set CVM Results to '3F 00 01'.

Return a Final Outcome of ***Try Another Interface***.

8.2.5.2a **If** all of the following are true:

The *Reader CVM Required Limit Exceeded* indicator is set.

The card supports Cardholder Verification (Card *AIP* Byte 1 Bit 5 is set to 1b).

There is not a mutually supported CVM across the contactless interface.

The transaction is taking place in EMV mode and the reader has an alternative interface.

The *Card Interface and Payment Capabilities*element is not present.

Then thereader shall:

Set *TVR* Byte 3 Bit 8 to 1b, 'Cardholder Verification was not successful'.

Set CVM Results to '3F 00 01'.

Return a Final Outcome of ***Try Another Interface***.

Requirements – Cardholder Verification Unable To Continue over Contactless Interface	
8.2.5.3a	**If** all of the following are true: The *Reader CVM Required Limit Exceeded* indicator is set. The card supports Cardholder Verification (Card *AIP* Byte 1 Bit 5 is set to 1b). There is not a mutually supported CVM across the contactless interface. The transaction is taking place in EMV mode **and** the reader has an alternative interface. The *Card Interface and Payment Capabilities*element Byte 1 Bit 6 is set to 0b, 'Contact EMV Interface supported'. **Then** thereader shall: Set *TVR* Byte 3 Bit 8 to 1b, 'Cardholder Verification was not successful'. Set CVM Results to '3F 00 01'. The transaction continues with Terminal Risk Management.
8.2.5.4a	**If** all of the following are true: The *Reader CVM Required Limit Exceeded* indicator is set. The card supports Cardholder Verification (Card *AIP* Byte 1 Bit 5 is set to 1b). There is not a mutually supported CVM across the contactless interface The transaction is taking place in EMV mode **and** thereader does not have an alternative interface **Then** thereader shall: Set *TVR* Byte 3 Bit 8 to 1b, 'Cardholder Verification was not successful'. Set CVM Results to '3F 00 01'. The transaction continues with Terminal Risk Management.

Requirements – Cardholder Verification Unable To Continue over Contactless Interface

8.2.5.5a **If** all of the following are true:

The *Reader CVM Required Limit Exceeded* indicator is set.

The card supports Cardholder Verification (Card *AIP* Byte 1 Bit 5 is set to 1b).

There is not a mutually supported CVM across the contactless interface

The transaction is taking place in mag-stripe mode

Then thereader shall:

Set *TVR* Byte 3 Bit 8 to 1b, 'Cardholder Verification was not successful'.

Set CVM Results to '3F 00 01'.

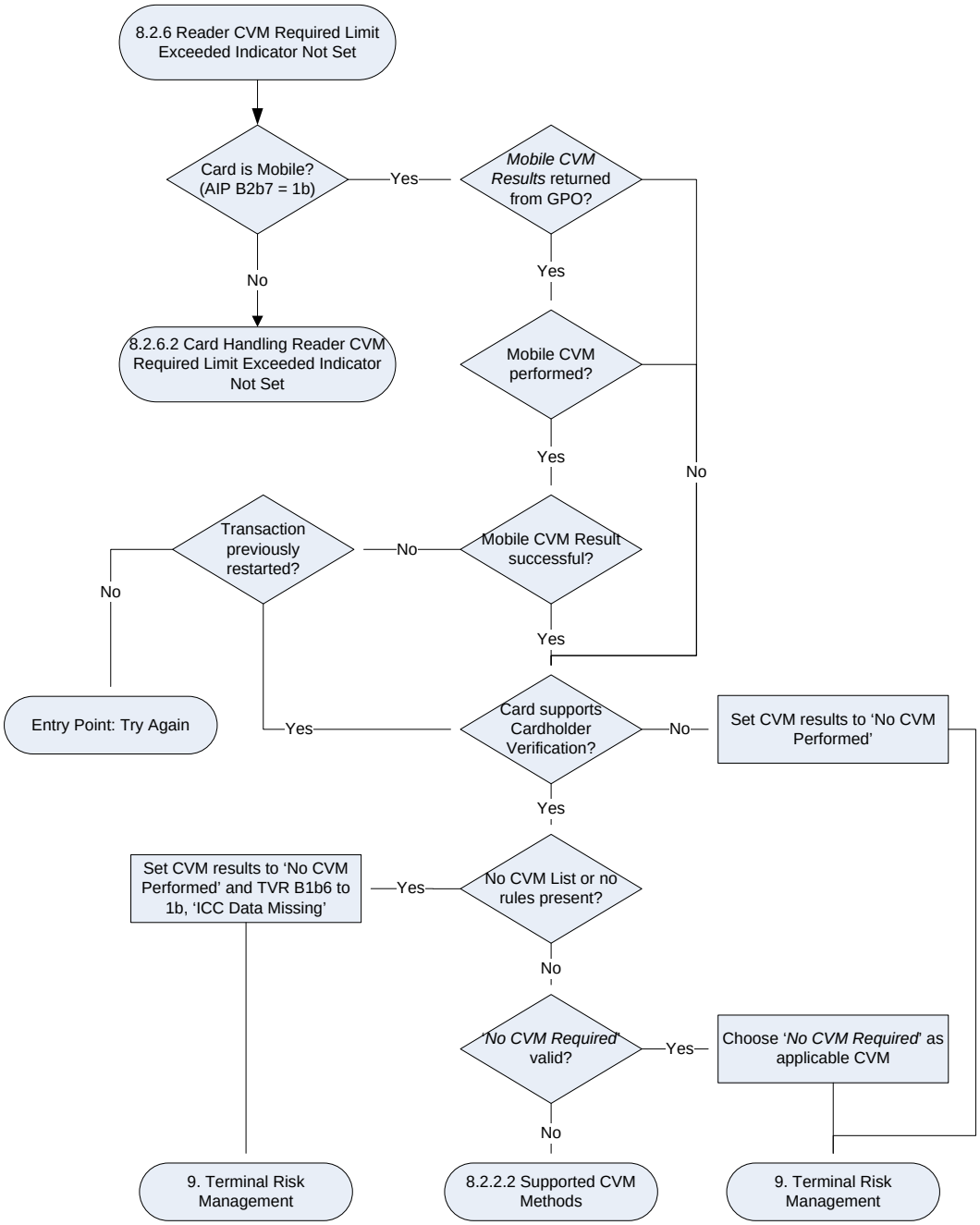
The transaction continues with Terminal Risk Management.

8.2.6 *Reader CVM Required Limit Exceeded* Indicator Not Set

If the Reader CVM Required Limit Exceeded indicator is not set then the reader shall determine if the transaction was carried out by a mobile card or not. The reader shall check if the card supports the method no cardholder verification or not.

8.2.6.1 Contactless Mobile CVM Result Validation

Figure 8-5: Contactless Mobile CVM Result Validation



When the value of the *Amount Authorised* does not exceed the *Reader CVM Required Limit*, the reader determines if the card application is Mobile-based by checking the setting for AIP Byte 2 Bit 7, 'Contactless Mobile Supported' as follows.

- **If** *AIP* Byte 2 Bit 7 is equal to 0b, 'Contactless Mobile Supported',
  then the transaction is **not** Contactless Mobile and processing continues as per section8.2.6.2, *Card Handling Reader CVM Required Limit Exceeded Indicator Not Set*.
  else the transaction **is** Contactless Mobile and processing continues as below.

The following process happens when the transaction is Contactless Mobile:

1. **If** the *Mobile CVM Results* was returned in the GET PROCESSING OPTIONS response
   then:
   a. **If** *Mobile CVM Results* Byte 1 is equal to '01', 'Mobile CVM Performed',
      and *Mobile CVM Results* Byte 3 is equal to '01', 'Failed',
      and the transaction has not previously been restarted,
      then the kernel returns control to Entry Point, passing a Final Outcome of ***Try Again*** with the parameter settings defined in Table 8-2.
   b. **Else** process continues with step 2 below**.**
2. **Else If** the Card supports Cardholder Verification (*AIP* Byte 1 Bit 5 is set to 1b),
   Then:
   a. **If** the CVM List is not present or is empty,
      then the reader shall set TVR byte 1, bit 6 'ICC Data missing' to 1b, and set the CVM Results as per *[EMV 4.3 Book 4]*, section 6.3.4.5, and transaction processing continues with Section9, *Terminal Risk Management*.
   b. **else If** the Card contains a CVM list that includes the '*No CVM Required*' method and CVM Condition Code that is valid for the transaction,
      then 'No CVM Required' is performed as per *[EMV 4.3 Book 3]*, section 10.5, thus considering the CVM successful and the transaction flow continues with Section 9, *Terminal Risk Management*.
   c. **else If** the CVM list does not include '*No CVM Required*' and an applicable CVM Condition Code that is valid for the transaction,
      then continue CVM processing as defined in Section 8.2.2.2, *Supported CVM Methods*.
3. **else** the Card does not support Cardholder Verification (*AIP* Byte 1 bit 5 is set to 0b) and CVM List processing is not performed. The CVM Results are set as per *[EMV 4.3 Book 4]*, section 6.3.4.5, and transaction processing continues with Section 9, *Terminal Risk Management*.

Table 8-2:Final Outcome Parameter Settings

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:** 10 • **Language Preference**
UI Request on Restart Present	Yes • **Message Identifier:** '21' (“Present Card Again”) • **Status: Processing Error** • **Hold Time:** 0 • **Language Preference**
Data Record Present	No
Discretionary Data Present	No
Alternate Interface Preference	N/A
Receipt	N/A
Field Off Request	N/A
Removal Timeout	Zero

Requirements – Contactless Mobile CVM Result Validation

8.2.6.1a **If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response,
and*Mobile CVM Results* Byte 1 is '01', ‘Mobile CVM performed’,
and*Mobile CVM Results* Byte 3 is '01', ‘Failed’,
and the transaction has not previously been restarted,
Then the kernel returns control to Entry Point, passing a Final Outcome of ***Try Again***.

Requirements – Contactless Mobile CVM Result Validation	
8.2.6.2a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is '01', 'Mobile CVM performed', **and***Mobile CVM Results* Byte 3 is '01', 'Failed', **and** the transaction has been restarted, **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b)**,** **and** the Card does not have a CVM List or has no CVM rules, **then** thereader shall set *TVR* Byte 1 Bit 8 to 1b, 'ICC Data Missing', **and**set CVM Results to '3F 00 00'–'No CVM performed' and the transaction proceeds with Terminal Risk Management, 9.
8.2.6.3a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is '01', 'Mobile CVM performed', **and***Mobile CVM Results* Byte 3 is '01', 'Failed', **and** the transaction has been restarted, **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b), **and** the Card contains a CVM list that includes 'No CVM Required', **and**CVM Condition Code supported for the transaction, **Then**'No CVM' is performed **and** this shall be stored and used to set the CVM Parameter as part of the Final Outcome parameter settings when sending the transaction online or completing an approved transaction.
8.2.6.4a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is '01', 'Mobile CVM performed', **and***Mobile CVM Results* Byte 3 is '01', 'Failed', **and** the transaction has been restarted, **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b), **and** the Card contains a CVM list that does not include 'No CVM Required', **and** CVM Condition Code supported for the transaction, **Then**CVM List processing shall be performed as defined in 8.2.3.

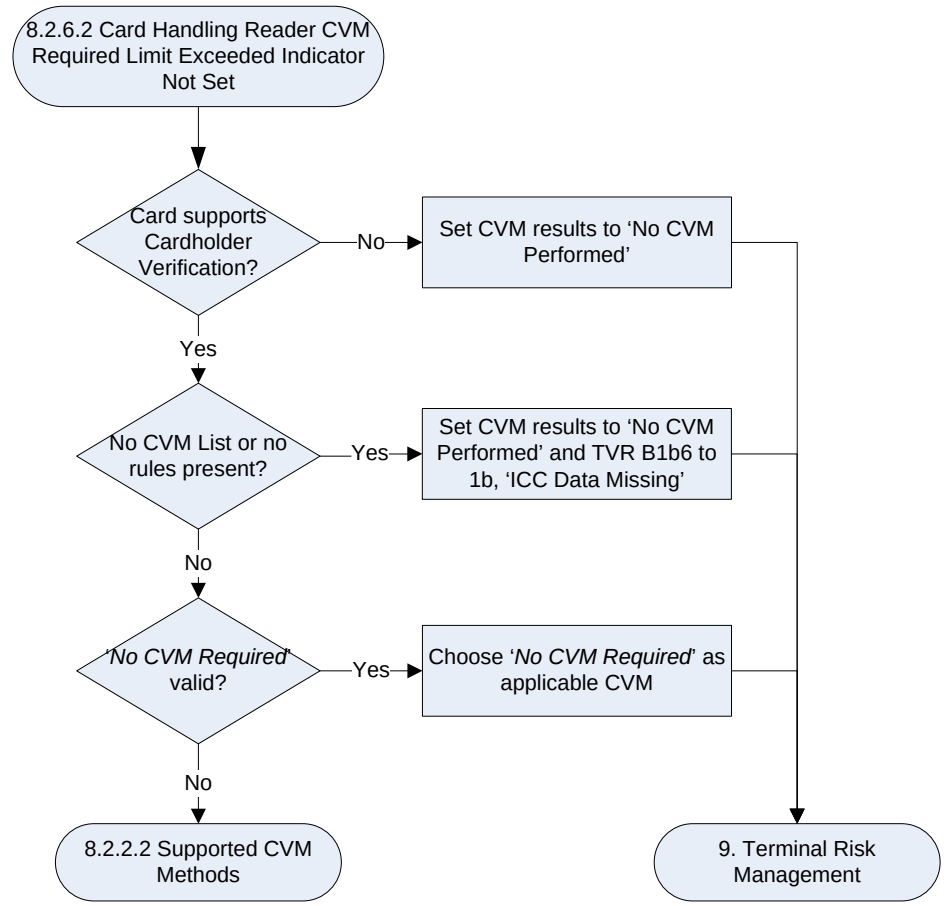
Requirements – Contactless Mobile CVM Result Validation	
8.2.6.5a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is '01', 'Mobile CVM performed', **and***Mobile CVM Results* Byte 3 is not set to '01', 'Failed', **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b), **and** the Card does not have a CVM List or has no CVM rules, **then** thereader shall set *TVR* Byte 1 Bit 8 to 1b, 'ICC Data Missing', **and**set CVM Results to '3F 00 00'–'No CVM performed', and the transaction proceeds with Terminal Risk Management, 9.
8.2.6.6a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is '01', 'Mobile CVM performed', **and***Mobile CVM Results* Byte 3 is not set to'01', 'Failed', **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b), **and** the Card contains a CVM list that includes 'No CVM Required', **and** CVM Condition Code supported for the transaction, **Then** 'No CVM' is performed **and** this shall be stored and used to set the CVM Parameter as part of the Final Outcome parameter settings when sending the transaction online or completing an approved transaction.
8.2.6.7a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is '01', 'Mobile CVM performed', **and***Mobile CVM Results* Byte 3 is not set to'01', 'Failed', **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b), **and** the Card contains a CVM list that does not include 'No CVM Required', **and** CVM Condition Code supported for the transaction, **Then**CVM List processing shall be performed as defined in 8.2.3.

Requirements – Contactless Mobile CVM Result Validation	
8.2.6.8a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is not set to '01', 'Mobile CVM performed', **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b), **and** the Card does not have a CVM List or has no CVM rules, **then** thereader shall set *TVR* Byte 1 Bit 8 to 1b, 'ICC Data Missing', **and**set CVM Results to '3F 00 00'–'No CVM performed'.
8.2.6.9a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is not set to '01', 'Mobile CVM performed', **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b), **and** the Card contains a CVM list that includes 'No CVM Required', **and** CVM Condition Code supported for the transaction, **Then** 'No CVM' is performed **and** this shall be stored and used to set the CVM Parameter as part of the Final Outcome parameter settings when sending the transaction online or completing an approved transaction.
8.2.6.10a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is not set to '01', 'Mobile CVM performed', **and** the Card supports Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 1b), **and** the Card contains a CVM list that does not include 'No CVM Required', **and** CVM Condition Code supported for the transaction, **Then**CVM List processing shall be performed as defined in 8.2.3.

Requirements – Contactless Mobile CVM Result Validation	
8.2.6.11a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is '01', 'Mobile CVM performed', **and***Mobile CVM Results* Byte 3 is '01', 'Failed', **and** the transaction has been restarted, **and** the Card does not support Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 0b), **then** thereader shall set CVM Results to '3F 00 00'–'No CVM performed'.
8.2.6.12a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is '01', 'Mobile CVM performed', **and***Mobile CVM Results* Byte 3 is not set to '01', 'Failed', **and** the Card does not support Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 0b), **then** thereader shall set CVM Results to '3F 00 00'–'No CVM performed'.
8.2.6.13a	**If***Mobile CVM Results* were returned in the GET PROCESSING OPTIONS response, **and***Mobile CVM Results* Byte 1 is not set to '01', 'Mobile CVM performed', **and** the Card does not support Cardholder Verification (*AIP*, Byte 1 bit 5 is set to 0b), **then** thereader shall set CVM Results to '3F 00 00'–'No CVM performed'.

8.2.6.2 Card Handling Reader CVM Required Limit Exceeded Indicator Not Set

Figure 8-6: Card Handling Reader CVM Required Limit Exceeded Indicator Not Set



The following process, also depicted in Figure 8-7, is carried out when the transaction is **not** Contactless Mobile, i.e.*AIP* Byte 2 Bit 7 is equal to 0b, 'Contactless Mobile Supported':

1. **If** the Card supports Cardholder Verification (*AIP* Byte 1 Bit 5 is set to 1b), **then:**

    a. **If** the CVM List is not present or is empty,
    then the reader shall set TVR byte 1, bit 6 'ICC Data missing' to 1b, and set the CVM Results as per *[EMV 4.3 Book 4]*, section 6.3.4.5, and transaction processing continues with Section9, *Terminal Risk Management*.

    b. **else If** the Card contains a CVM list which includes the '*No CVM Required*' method and CVM Condition Code that is valid for the

transaction,
then 'No CVM Required' is performed as per *[EMV 4.3 Book 3]*, section 10.5, thus considering the CVM successful and the transaction flow continues with Section 9, *Terminal Risk Management*.

c. **else If** the Card contains a CVM list which does not include 'No CVM Required' and an applicable CVM Condition Code that is valid for the transaction,
then continue CVM processing as defined in section8.2.2.2, *Supported CVM Methods*.

2. **else** the Card does not support Cardholder Verification (*AIP* Byte 1 bit 5 is set to 0b) and CVM List processing is not performed. The CVM Results are set as per *[EMV 4.3 Book 4]*, section 6.3.4.5, and transaction processing continues with Section 9, *Terminal Risk Management*.

Requirements – CVM Processing – Card Supports Cardholder Verification but CVM List Not Present or Empty

8.2.6.14a **If** the *Reader CVM Required Limit Exceeded* indicator is not set,
and the card *AIP* Byte 2 Bit 7 is 0b ('Contactless Mobile Supported'),
and the following are true:

- The card *AIP* Byte 1 Bit 5 is 1b, ('Cardholder verification supported'), **and**
- *CVM List* is not present, **or**
- *CVM List* is empty,

Then the reader sets the *CVM Results* to 'No CVM Performed' and this shall be stored and used to set the CVM Parameter as part of the Final Outcome parameter settings. The transaction processing continues with Section 9, *Terminal Risk Management*.

Requirements – CVM Processing – Card Supports Cardholder Verification and CVM List contains 'No CVM Required'

8.2.6.15a **If** the *Reader CVM Required Limit Exceeded* indicator is not set,
and the card *AIP* Byte 2 Bit 7 is 0b ('Contactless Mobile Supported'),
and the following are true:

- The card *AIP* Byte 1 Bit 5 is 1b, ('Cardholder verification supported'), **and**
- *CVM List* contains 'No CVM required', **and**
- *Valid CVM condition code for the transaction*

Then the reader shall perform 'No CVM Required' as per *[EMV 4.3 Book 3]*, section 10.5, thus considering the CVM successful and the transaction flow continues with Section 9, *Terminal Risk Management*.

Requirements – CVM Processing – Card Supports Cardholder Verification and CVM list is present but does not contain 'No CVM Required'

8.2.6.16a **If** the *Reader CVM Required Limit Exceeded* indicator is not set,
and the card *AIP* Byte 2 Bit 7 is 0b ('Contactless Mobile Supported'),
and the following are true:

- The card *AIP* Byte 1 Bit 5 is 1b, ('Cardholder verification supported'), **and**
- *CVM List* is present, **and**
- *CVM List does not* contain 'No CVM required'

Then the reader shall continue CVM processing as defined in section8.2.2.2, *Supported CVM Methods*.

Requirements – CVM Processing – Card Does Not Support Cardholder Verification	
8.2.6.17a	**If** the *Reader CVM Required Limit Exceeded* indicator is not set, **and**the card *AIP* Byte 2 Bit 7 is 0b ('Contactless Mobile Supported'), **and** the card *AIP* Byte 1 Bit 5 is 0b, ('Cardholder verification supported'), **then** the reader shall not perform CVM List processing. The CVM Results are set as per *[EMV 4.3 Book 4]*, section 6.3.4.5, and transaction processing continues with Section 9, *Terminal Risk Management*.

9 Terminal Risk Management

9.1 Overview

During a transaction, certain risk management checks are performed by the reader, for example, floor limits as defined in *[EMV 4.3 Book 3]*, section 10.6, and *[EMV 4.3 Book 4]*, section 6.3.5.

Terminal Risk Management shall always be performed, regardless of the setting of the Terminal Risk Management is to be performed bit in the *AIP* read from the card.

Requirements – Terminal Risk Management Not Requested By Card	
9.1.1.1a	**If**a Card with *AIP* Byte 1 Bit 4 = 0b (Terminal Risk Management) is presented*,* **then** Terminal Risk Management shall be performed.

Requirements – Terminal Risk Management Requested By Card	
9.1.1.2a	**If**the Card indicates that Terminal Risk Management is to be performed (*AIP* Byte 1 Bit 4 is set to 1b)*,* **then** Terminal Risk Management shall be performed.

Terminals may optionally support an exception/hot list file and a card account number may be checked against this list if present. Results of the risk management check are stored in a reader resident data element called*TVR*.

Reader processing decisions based on the outcome of the above checks are configurable, determined by the card and reader resident data elements which are the *IACs* and the *TACs*. (See section10, 1st Terminal Action Analysis.)

9.2 Processing Requirements

Terminal Risk Management must be performed as defined in *[EMV 4.3 Book 3]*, section 10.6, and *[EMV 4.3 Book 4]*, section 6.3.5 with the exception that random transaction selection and velocity checking shall not be performed.

9.2.1 Floor Limit Checking

Readers shall support a *Reader Contactless Floor Limit* in place of any other *Terminal Floor Limit*. The *Reader Contactless Floor Limit* is checked during Entry Point processing (refer to *Book B*) and the *Reader Contactless Floor Limit Exceeded* indicator may be set as a result.

Requirements – Terminal Risk Management – Floor Limit Checking	
9.2.1.1a	**If** the *Reader Contactless Floor Limit Exceeded* indicator is set to 1, **then** the reader shall set *TVR* Byte 4 Bit 8 to 1b, 'Transaction exceeds floor limit'.

9.2.2 Random Transaction Selection

Readers ***must not*** support random transaction selection processing for contactless transactions.

9.2.3 Velocity Checking

Readers ***must not*** support velocity checking processing for contactless transactions.

9.2.4 Exception File Checking

When the terminal indicates to the reader that a Terminal Exception File/ Hotlist is supported, then the reader may format a Data Exchange Request message containing the card PAN, PAN Sequence Number, and Expiry Date and send to the terminal[2]. If the response data returned indicates a match is found on the Terminal Exception File/ Hotlist, then the reader shall set *TVR* Byte 1 Bit 5 to 1b, 'Card appears on Terminal Exception File'.

Requirements – Terminal Risk Management – Exception File Checking	
9.2.4.1a	**If** the card response data matches that found on the Exception File / Hotlist, **then** the reader shall set *TVR* Byte 1 Bit 5 to 1b, 'Card appears on terminal exception file'.

[2] Alternatively in some Terminal or POS System architectures the Exception File / Hotlist checking may take place after the Reader and Card interaction has completed and the final transaction outcome will be determined subsequently.

10 1st Terminal Action Analysis

10.1 Overview

Terminal Action Analysis applies rules on the card, set by the Issuer, and on the reader, set by the Scheme, to the transaction to determine if it should request of the card whether the transaction be approved offline, declined offline, or sent online for authorisation as defined in *[EMV 4.3 Book 3]*, section 10.7, and *[EMV 4.3 Book 4]*, section 6.3.6.

The Terminal Action Analysis function may be executed at several places during a transaction to eliminate the need for unnecessary processing. As described in *[EMV 4.3 Book 3]*, section 6.7.

10.2 Processing Requirements

1st Terminal Action Analysis comprises two stages:

Checking of the Offline Processing Results

Requesting a cryptogram from the card

10.2.1 Offline Processing Results

The reader examines the results of Offline processing recorded in the *TVR* during the transaction so far, for example, during Terminal Risk Management, to determine the action to be taken. The TVR settings are shown in Table 10-1.

Table 10-1: Terminal Verification Results (TVR) Settings

***TVR* Byte 1 (Leftmost)**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	x	x	x	x	x	x	x	Offline Data Authentication was not performed
x	1	x	x	x	x	x	x	Offline Static Data Authentication Failed
x	x	1	x	x	x	x	x	Card Data Missing
x	x	x	1	x	x	x	x	Card appears on Terminal Exception File
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	1	x	x	Combined DDA/AC (CDA) Failed
x	x	x	x	x	x	1	x	SDA Selected
x	x	x	x	x	x	x	0	RFU
***TVR* Byte 2**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	x	x	x	x	x	x	x	Card and Terminal have different application versions
x	1	x	x	x	x	x	x	Expired Application
x	x	1	x	x	x	x	x	Application not effective yet
x	x	x	1	x	x	x	x	Requested service not allowed for Card product
x	x	x	x	1	x	x	x	New Card
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU
***TVR* Byte 3**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	x	x	x	x	x	x	x	Cardholder Verification failed
x	1	x	x	x	x	x	x	Unrecognised CVM
x	x	1	x	x	x	x	x	Passcode Try Limit exceeded
x	x	x	1	x	x	x	x	PIN entry required and PIN pad not present or

								not working
x	x	x	x	1	x	x	x	PIN entry required, PIN pad present, but PIN was not entered
x	x	x	x	x	1	x	x	Online PIN entered
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU
***TVR* Byte 4**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	x	x	x	x	x	x	x	Transaction Exceeds Floor Limit
x	1	x	x	x	x	x	x	Lower consecutive offline limit exceeded
x	x	1	x	x	x	x	x	Upper consecutive offline limit exceeded
x	x	x	1	x	x	x	x	Transaction selected randomly for online processing
x	x	x	x	1	x	x	x	Merchant forced transaction online
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU
***TVR* Byte 5 (Rightmost)**								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
1	x	x	x	x	x	x	x	Default TDOL used
x	1	x	x	x	x	x	x	Issuer Authentication was unsuccessful
x	x	1	x	x	x	x	x	Script processing failed before final GENERATE AC
x	x	x	1	x	x	x	x	Script processing failed after final GENERATE AC
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

The review of the offline processing results, in the *TVR*, is performed against the *IACs*(obtained from the Card, as set by the Issuer) and the *TACs*(in the terminal, as set by the Scheme). A setting of the corresponding bit in either the *IACs* or *TACs* will determine the outcome of the Terminal Action Analysis as described below.

The *TAC* settings depend on the terminal's capabilities and its configuration. Each reader configuration type (see Table 2-3) has its own *TAC* settings.

There are three sets of *IACs* and corresponding *TACs*:

• *IAC – Denial* • *TAC – Denial*	Defines conditions that determine whether a transaction should be declined offline.

• *IAC – Online* • *TAC – Online*	Defines conditions that determine whether a transaction should be transmitted online for authorisation.
• *IAC – Default* • *TAC – Default*	Defines conditions that determine whether to decline a transaction that was required to be sent online but that the reader is unable to send online.

The checks performed by the reader depend on its configuration. The reader checks each of the above sets of *IACs* and *TACs* against the results of the current transaction recorded in the *TVR* in the order given in Table 10-2.

Table 10-2: Reader Configurations IAC/TAC Checks

Offline Only	Online Only	Offline with Online Capability	Delayed Authorisation
IAC/TAC – Denial	IAC/TAC – Denial	IAC/TAC – Denial IAC/TAC – Online IAC/TAC – Default	IAC/TAC – Denial IAC/TAC – Online

10.2.1.1 Offline Only Terminal

The reader must compare the *IAC – Denial* and *TAC – Denial* with the results of the current transaction as recorded in the *TVR*. If any of the corresponding bits are set, then the transaction is requested to be declined and the reader must:

Set the cryptogram type to be requested in the GENERATE AC command to *AAC*.

Refer to section 10.2.4, Request *AC* in First GENERATE AC.

Otherwise the reader shall request a TC.

Requirements – Terminal Action Analysis – Offline Only Compare Denial Codes	
10.2.1.1a	During Terminal Action Analysis the an Offline Only terminal shall compare the *Terminal Action Code – Denial* and the *Issuer Action Code – Denial* read from the card with the results as recorded by the *TVR*. **If**the reader is Offline only, **and**any corresponding bits are set, **then** the reader shall request an *AAC* at first GENERATE AC stage, **else** the reader shall request a TC at the first GENERATE AC stage.

10.2.1.2 Online Only Terminal

The reader must compare the *IAC – Denial* and *TAC – Denial* with the results of the current transaction as recorded in the *TVR*. If any of the corresponding bits are set, then the transaction is requested to be declined and the reader must:

Set the cryptogram type to be requested in the GENERATE AC command to *AAC*.

Refer to section 10.2.4, Request *AC* in First GENERATE AC.

Requirements – Terminal Action Analysis – Online Only Compare Denial Codes	
10.2.1.2a	During Terminal Action Analysis the an Online Only terminal shall compare the *Terminal Action Code – Denial* and the *Issuer Action Code – Denial* read from the card with the results as recorded by the *TVR*. **If**the reader is Online only, **and** any corresponding bits are set, **then** the reader shall request an *AAC* at first GENERATE AC stage.

If the reader is unable to go online, and unless Merchant specific configurations in support of Kernel 4 as required by payment system rules allow otherwise, then the transaction is requested to be declined and the reader must:

Set the cryptogram type to be requested in the GENERATE AC command to *AAC*.

Refer to section 10.2.4, Request *AC* in First GENERATE AC.

Otherwise the reader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.

Requirements – Terminal Action Analysis – Online Only Terminal Unable To Go Online

10.2.1.3a **If**theterminal is online only but is unable to complete an online connection,
then during the reader shall request an *AAC* at first GENERATE AC stage.
Else The reader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.

10.2.1.3 Offline with Online Capability Terminal

The reader carries out the following steps to determine the transaction disposition to be requested in first Generate AC stage:

1. The reader must compare the *IAC – Denial* and *TAC – Denial* with the results of the current transaction as recorded in the *TVR,*with the following outcome:
    a. **If** any of the corresponding bits are set,
    then the transaction is requested to be declined offline and the reader must set the cryptogram type to be requested in the GENERATE AC command to *AAC*.

Requirements – Terminal Action Analysis – Offline with Online Capability Compare Denial Codes

10.2.1.4a During Terminal Action Analysis the an Offline with Online Capability terminal shall compare the *Terminal Action Code – Denial* and the *Issuer Action Code – Denial* read from the card with the results as recorded by the *TVR*.

Ifthe reader is Offline with Online capability,
and any corresponding bits are set,
thenthe transaction is requested to be declined offline andthe reader shall request an *AAC* at first GENERATE AC stage.

2. **If** the transaction was **not** declined offline in step 1,
    then the reader must compare the *IAC – Online* and *TAC – Online* with the results of the current transaction as recorded in the *TVR*, with the following outcome:

a. **If** any of the corresponding bits are set,
then the transaction is requested to be processed online and thereader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.
Else the transaction is requested to be approved offline and the reader must set the cryptogram type to be requested in the GENERATE AC command to *TC*.

Requirements – Terminal Action Analysis – Offline with Online Capability Terminal Compare Online Codes

10.2.1.5a During Terminal Action Analysis an Offline with Online Capability terminal shall compare the *Terminal Action Code – Online* and the *Issuer Action Code – Online* read from the card with the results as recorded by the *TVR*.

Ifthe terminal is Offline with Online capability*,*
and any of the corresponding bits are set*,*
thenthe transaction is requested to be processed online andthe reader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.
else the transaction is requested to be approved offline and the reader must set the cryptogram type to be requested in the GENERATE AC command to *TC*.

If the cryptogram to be requested is an *ARQC*, and the reader is unable to go online, and unless Merchant specific configurations in support of Kernel 4 as required by payment system rules allow otherwise,
thenthe reader must compare the *IAC-Default* and *TAC -Default* with the results of the current transaction as recorded in the *TVR*, with the following outcome:

1. **If** any of the corresponding bits are set,
then the transaction is requested to be declined offline and the reader must set the cryptogram type to be requested in the GENERATE AC command to *AAC*.
else the transaction is requested to be approved offline and the reader must set the cryptogram type to be requested in the GENERATE AC command to *TC*.

Requirements – Terminal Action Analysis – Offline with Online Capability Terminal Unable To Go Online

10.2.1.6a During Terminal Action Analysis the an Offline with Online Capability terminal shall compare the *Terminal Action Code – Default* and the *Issuer Action Code – Default* read from the card with the results as recorded by the *TVR*.

Ifthe terminal is Offline with Online capability but is unable to complete an online connection,
and any of the corresponding bits are set
thenthe transaction is requested to be declined offline and the reader shall request an *AAC* at first GENERATE AC stage.
Else the transaction is requested to be approved offline andthe reader must set the cryptogram type to be requested in the GENERATE AC command to *TC*.

Otherwise the reader shall request a TC.

10.2.1.4 Delayed Authorisation Terminal

A reader that supports delayed authorisation carries out the following steps todetermine the transaction disposition to be requested in first Generate AC stage:

1. The reader must compare the *IAC – Denial* and *TAC – Denial* with the results of the current transaction as recorded in the *TVR,* with the following outcome:
    a. **If** any of the corresponding bits are set,
    then the transaction is requested to be declined offline and the reader must set the cryptogram type to be requested in the GENERATE AC command to *AAC*.

Requirements – Terminal Action Analysis – Delayed Authorisation Terminal Compare Denial Codes

10.2.1.7a During Terminal Action Analysis the a Delayed Authorisation terminal shall compare the *Terminal Action Code – Denial* and the *Issuer Action Code – Denial* read from the card with the results as recorded by the *TVR*.

Ifthe reader is a Delayed Authorisation terminal,
and any corresponding bits are set,
thenthe transaction is requested to be declined offline and the reader shall request an *AAC* at first GENERATE AC stage.

2. **If** the transaction was **not** declined offline in step 1,
   then the reader must compare the *IAC – Online* and *TAC – Online* with the results of the current transaction as recorded in the *TVR*, with the following outcome:

   a. **If** any of the corresponding bits are set,
      thenthe transaction is requested to be processed online and thereader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.
      else the transaction is requested to be approved offline and the reader must set the cryptogram type to be requested in the GENERATE AC command to *TC*.

Requirements – Terminal Action Analysis – Delayed Authorisation Terminal Compare Online Codes

10.2.1.8a During Terminal Action Analysis a Delayed Authorisation terminal shall compare the *Terminal Action Code – Online* and the *Issuer Action Code – Online* read from the card with the results as recorded by the *TVR*.

Ifthe terminal is Delayed Authorisation,
and any of the corresponding bits are set,
thenthe transaction is requested to be processed online and the reader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC,*
elsethe transaction is requested to be approved offline andthe reader shall request a TC at the GENERATE AC.

10.2.2 Zero Amount Allowed and Status Check Requested Validation

The *Zero Amount Allowed* and *Status Check Support* flags are checked during Entry Point processing (refer to *Book B*). The corresponding 'Zero Amount' and 'Status Check Requested' indicators are set as a result and processing should continue as follows:

If the 'Zero Amount' indicator is set to 1 and the current cryptogram type to be requested is **not** an *AAC*, then the reader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.

If the 'Status Check Requested' indicator is set to 1and the current cryptogram type to be requested is **not** an *AAC*, then the reader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.

Requirements – Zero Amount Allowed

10.2.2.1a **If** the reader supports Zero Amount Allowed,
and the Zero Amount indicator is set to 1 during Entry Point processing,
and the current cryptogram type to be requested is **not** an *AAC*,
then the reader shall request an *ARQC* at first GENERATE AC stage.

10.2.2.2a **If** the reader supports Zero Amount Allowed,
and the Zero Amount indicator is set to 0 during Entry Point processing,
or the current cryptogram type to be requested is an *AAC*,
then the reader shall determine which cryptogram to request based on the normal Terminal Action Analysis process.

Requirements – Status Check Requested

10.2.2.3a **If** the reader supports Status Check,
and the Status Check Requested indicator is set to 1 during Entry Point processing,
and the current cryptogram type to be requested is **not** an *AAC*,
then the reader shall request an *ARQC* at first GENERATE AC stage.

Requirements – Status Check Requested	
10.2.2.4a	**If** the reader supports Status Check, **and** the Status Check Requested indicator is set to 0 during Entry Point processing, **or** the current cryptogram type to be requested is an *AAC*, **then** the reader shall determine which cryptogram to request based on the normal Terminal Action Analysis process.

10.2.3 Additional Processing for Contactless Mag-Stripe Mode

10.2.3.1 Generation of Unpredictable Number

The reader shall generate an *Unpredictable Number* as follows:

Retrieve the *Unpredictable Number Range* from the Configuration data provided for Kernel 4. The default range is 0 to 60, which is also the minimum range. Note that the number range is inclusive, so a range of 0 to 60 should be capable of generating 61 integer numbers in the range 0 to 60.

Readers must carry out one of the following two checks:

Generate a random number of months in the range 0 to *Unpredictable Number Range*. The random number generation algorithm must generate a statistically flat distribution of values within the configured range and the random number must not be predictable.

Transform a previously computed *Unpredictable Number* (e.g. from Entry Point processing) into a random number of month (RNM) within the required range. The transformation shall apply a modulo operation to the *Unpredictable Number* with *Unpredictable Number Range* plus one.

$$RNM: = UN_{EMV} \bmod (\text{Unpredictable Number Range} + 1)$$

Subtract the random number of months generated from the *Application Effective Date* retrieved from the card. Discard the DD to leave a four digit random number in YYMM format.

Left Pad the result with two bytes of zeros to obtain a four-byte *Unpredictable Number* formatted as ‘0000YYMM’

Store the four-byte *Unpredictable Number* with a tag of '9F37' so that it may be retrieved when processing the *CDOL1*.

The *Unpredictable Number Range* must be stored in a secure manner and protected from modification in the same way in which public keys and other sensitive data elements are protected.

Requirements – Unpredictable Number	
10.2.3.1a	For mag-stripe mode transactions, the terminal shall generate an unpredictable number using the *Unpredictable Number Range* and the *Application Effective Date*. The result shall be '0000YYMM' where YYMM is the unpredictable number generated and stored in Tag '9F37'. This number shall not be predictable and shall provide a flat distribution of values within the required range.

10.2.3.2 Construction of Transaction Related Data

Transaction related data must be processed as specified in *[EMV 4.3 Book 3]*, section 5.4.

Requirements – GENERATE AC Data Construction	
10.2.3.2a	In the GENERATE AC command, the terminal shall send to the card the data elements that the card requested in *CDOL1*.

10.2.4 Request *AC* in First GENERATE AC

The 1st Terminal Action Analysis processing concludes with the issuance of the first GENERATE AC command to the card.

When CDA is to be performed the reader indicates that to the card in the reference control parameter as defined in *[EMV 4.3 Book 2]*, section 6.6.

The reader formats the GENERATE AC command to request a *TC*, an *AAC*, or an *ARQC* from the card dependent on the results of the review of the offline processing results described in section 10.2.1, Offline Processing Results.

A request for a *TC* indicates that the reader is requesting that the transaction be approved offline.

A request for an *AAC* indicates that the reader is requesting that the transaction be declined offline. Note that there is no need to perform CDA if the reader requests *AAC*.

A request for an *ARQC* indicates that the reader is requesting that the transaction be sent online for authorisation.

In response to the GENERATE AC command issued by the reader, the card will (on completion of any Card Risk Management) return an *AC* to the reader. The card may in some circumstances override the reader's decision for the transaction disposition (Approve, Decline, Go Online) in accordance with the rules defined in *[EMV 4.3 Book 3]*, section 10.8.

11 1st Card Action Analysis

11.1 Overview

The purpose of Card Action Analysis is to allow the card to perform a number of predefined risk management tests and use the results of these tests to decide upon an appropriate action. These tests are carried out on the details of this transaction and the outcome of previous transactions. They determine if positive online authorisation is required for this transaction to be completed, whether the transaction can be completed with local offline authorisation or whether the transaction should be declined offline.

These card tests are performed regardless of the outcome of the Terminal Risk Management checks carried out by the reader on this transaction. The *AC* produced by the card in response to a GENERATE AC command, is used by the Issuer of the card to validate the transaction and the card. When CDA generation is being performed the card generates a dynamic signature that is returned to the reader with the *AC*. This is then validated by the reader before the transaction progresses to any further stages. *ACs* perform two roles:

The *ARQC* when sent in an online authorisation request message allows the Issuer to authenticate that they actually issued the card. Each card contains a unique DES key that is used to generate the cryptogram. This key, which is known only by the card Issuer, is then used in their host systems to validate the *AC* received in the Authorisation Request Message.

When sent in a clearing or advice message (*TC, ARQC* or *AAC*), the cryptogram can be used to authenticate the integrity of the transaction parameters or data (i.e. Amount, Date, Time, etc.), as they pass through the various processing systems between reader and Issuer. This can also be used in dispute resolution to confirm the parameters of a transaction post event.

When operating in mag-stripe mode, the card will either return an *ARQC* or an *AAC*.

11.2 Processing Requirements

The reader is not involved in 1st Card Action Analysis, however it is triggered by the reader issuing the GENERATE AC command to the card, and the reader is informed of the result of this process in the response data returned by the card.

The card generates the *AC* using application data and a secret DES key (the *AC DEA Keys*) stored on the card. (When CDA is being performed, the card will also create a dynamic signature that includes the *TC* or *ARQC*.)

Subsequent processing depends on the type of cryptogram returned and the results of Offline Data Authentication if CDA is performed. When a CDA signature is returned by the card the reader uses the *CAPK* to validate this dynamic signature as described in *[EMV 4.3 Book 2]*, section 6.6.

11.2.1 Format of the Response to GENERATE AC Command

The reader must check that the format of the response data is compliant to Format 1 or Format 2 as defined by *[EMV 4.3 Book 3]*, section 6.5.5.4 when CDA is not used, or Format 2 when CDA is used (see *[EMV 4.3 Book 2]*, section 6.6).

If the response is in the incorrect format then the reader determines whether an alternative interface is supported as follows:

- **If** the transaction is taking place in EMV mode**,**
  and the reader supports an alternative (contact) interface**,**
  and any of the following conditions are true:
    - *Card Interface and Payment Capabilities* is not present.
    - *Card Interface and Payment Capabilities* Byte 1 Bit 6 is set to 1b, ‘Contact EMV interface supported’.

  thenthe card and the reader support an alternative interface and the kernel returns control to Entry Point with a Final Outcome of ***Try Another Interface***and parameters set as per Table 11-1.
  Else the card and the reader **do not** support an alternative interface, and the transaction shall be terminated. The kernel returns control to Entry Point with a Final Outcome of ***End Application***and parameters set as perTable 11-2.

Table 11-1:Card Action analysis - Final Outcome Parameter Settings for 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:**Processing Error: Conditions for use of contactless not satisfied • **Hold Time:** 0 • **Language Preference**
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

Table 11-2: Card Action analysis - Final Outcome Parameter Settings for End Application

Start	N/A
Online Response Data	N/A
CVM	N/A
UI Request on Outcome Present	Yes • **Message Identifier:** '1C' (“Insert, Swipe or Try Another Card”) • **Status:** Ready to Read • **Hold Time:** 0 • **Language Preference**
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

Requirements – Card Action Analysis Return Formats

11.2.1.1a **If** CDA is not used,
then:

The terminal shall check that the GENERATE AC response is either in Format 1**or** Format 2.

If the response is not in Format 1 **or** Format 2
and an alternative interface is supported by the reader and the card,
then the kernel returns control to Entry Point with a Final Outcome of ***Try Another Interface***.

Requirements – Card Action Analysis Return Formats
11.2.1.2a **If** CDA is used, **then**: The terminal shall check that the format of the GENERATE AC response is in Format 2 or Format 1 as appropriate: **If**either: • The card returns an AAC and the response is not in Format 1, • **or**the card returns an AC other than an AAC and the response is not in Format 2, **and**an alternative interface is supported by the reader and the card, **then** the kernel returns control to Entry Point with a Final Outcome of ***Try Another Interface***.
11.2.1.3a **If** CDA is not used, **then**: The terminal shall check that the GENERATE AC response is either in Format 1**or** Format. **If** the response is not in Format 1**or** Format 2, **and** an alternative interface is **not** supported by the reader and the card, **then** the transaction shall be terminated. The kernel returns control to Entry Point with a Final Outcome of ***End Application***.

Requirements – Card Action Analysis Return Formats	
11.2.1.4a	**If** CDA is used, **then**: The terminal shall check that the format of the GENERATE AC response is in Format 2 or Format 1 as appropriate: **If**either: • The card returns an AAC and the response is not in Format 1, • **or**the card returns an AC other than an AAC and the response is not in Format 2, **and**an alternative interface is **not** supported by the reader and the card, **then** the transaction shall be terminated. The kernel returns control to Entry Point with a Final Outcome of ***End Application***.

11.2.2 General Card Action Analysis

Requirements – Card Action Analysis Processing	
11.2.2.1a	**If** the terminal requests CDA at first GENERATE AC, **and** the card responds with an *AAC*, **then** the terminal shall not set *TVR* Byte 1 Bit 3 to 1b, 'CDA failed'.
11.2.2.2a	**If** the terminal requests CDA with *TC* at first GENERATE AC, **then** **If** thecard responds with a TC, then the terminal shall validate the signature, **elseIf** the card responds with an *ARQC*, then the terminal shall validate the signature and extract the *ARQC*.
11.2.2.3a	**If** the terminal requests CDA with *ARQC* at first GENERATE AC, **then** the terminal shall validate the signature and extract the *ARQC*.

11.2.3 Card Returns SW = '6984'

If Card Risk Management has determined that a Mobile CVM is required, but has not been successfully entered then Status Word '6984' is returned by the Card.

If the card returns SW=6984 **and** the transaction has **not** been restarted,
then the kernel returns control to Entry Point, passing a Final Outcome of ***Try Again*** with the parameter settings defined in Table 11-4.
Else if the card returns SW=6984 **and** the transaction has been restarted,
then an error condition has occurred and the kernel returns control to Entry Point with a Final Outcome of ***End Application*** and the parameters defined in Table 11-4.

Note that ***Try Again*** processing invokes the collection of the Mobile CVM by the Cardholder's mobile device. The processing by the reader on retry is handled by CVM processing as per Section8.2.4, *Contactless Mobile CVM Processing*. The process flow is not expected to result in a second Status Word '6984' (and consequently a re-entry to the flow would be an error).

Table 11-3: Card returns SW=6984 – Try Again Parameter Settings

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:**10 • **Language Preference**
UI Request on Restart Present	Yes • **Message Identifier:** '21' ("Present Card Again") • **Status:** Ready to Read. • **Hold Time:** 0 • **Language Preference**
Data Record Present	No
Discretionary Data Present	No
Alternate Interface Preference	N/A
Receipt	N/A
Field Off Request	N/A
Removal Timeout	Zero

Table 11-4:Card returns SW=6984 – *End Application* Parameter Settings

Start	N/A
Online Response Data	N/A
CVM	N/A
UI Request on Outcome Present	Yes • **Message Identifier:**'1C' (“Insert, Swipe or Try Another Card”) • **Status:**Ready to Read • **Hold Time:** 0 • **Language Preference**
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

Requirements – Card returns SW=6984 and transaction has not been restarted

11.2.3.1a **If**the Card returns SW=6984 **and**the transaction has **not** been restarted,
Then the kernel returns control to Entry Point, passing a Final Outcome of ***Try Again*** with the parameter settings defined in Table 11-3.

Requirements – Card returns SW=6984 and transaction has been restarted

11.2.3.2a **If**the Card returns SW=6984 **and**the transaction has been restarted,
Then an error condition has occurred and the kernel returns control to Entry Point, passing a Final Outcome of ***EndApplication*** with the parameter settings defined inTable 11-4.

11.2.4 Card Returns a *TC*

For offline-approved transactions:

The reader shall send a User Interface Request Message with the following parameters set:

Message Identifier: '17' ("Card read OK. Please remove card")

Status: Card Read Successfully

Hold Time: 300ms

Language Preference: If returned by the card during Application Selection

A *TC* is generated and Offline Data Authentication will be performed if applicable.

If *TVR* Byte 1 Bit 3 is set to 1b, 'CDA Failed', then the reader continues with section 13.3, Transaction Completion – Transaction Declined; else the reader continues with section 13.2, Transaction Completion – Transaction Approved.

Requirements – Card Action Analysis Return *TC*	
11.2.4.1a	**If**thecard returns a TC, **then:** **If** Offline Data Authentication is not required to be performed, **then**the terminal shall approve the transaction, returning control to Entry Point as defined in 13.2.
11.2.4.2a	**If**thecard returns a TC, **then:** **If** Offline Data Authentication is required to be performed, **and**Offline Data Authentication is successful, **then**the terminal shall approve the transaction, returning control to Entry Point as defined in 13.2**.**
11.2.4.3a	**If** the card returns a TC, **then:** **If** Offline Data Authentication is required to be performed, **and** Offline Data Authentication is unsuccessful, **then** the terminal shall decline the transaction, returning control to Entry Point as defined in13.3.

11.2.5 Card Returns an *AAC*

For offline-declined transactions:

The reader shall send a User Interface Request Message with the following parameters set:

Message Identifier: '17' ("Card read OK. Please remove card")

Status: Card Read Successfully

Hold Time: 300ms

Language Preference: If returned by the card during Application Selection

The cryptogram generated by the card is an *AAC* and the reader continues with section13.3, Transaction Completion – Transaction Declined.

Requirements – Card Action Analysis Return *AAC*	
11.2.5.1a	**If** the card returns an AAC, **then**the terminal shall decline the transaction, returning control to Entry Point as defined in13.3.

11.2.6 Card Returns an *ARQC*

If the card returns an *ARQC* in the response to the first GENERATE AC command,Offline Data Authentication will be performed if applicable.

If *TVR* Byte 1 Bit 3 is set to 1b, 'CDA Failed, then the transaction will be declined and processing continues with section 13.3, Transaction Completion – Transaction Declined.

Requirements – Card Action Analysis Return *ARQC* – CDA failure	
11.2.6.1a	**If** a terminal sends the first GENERATE AC, **and** the terminal receives an *ARQC* with CDA which fails, **then** the terminal shall decline the transaction, returning control to Entry Point as defined in13.3.

Subsequent processing depends upon both the reader configuration and the transaction mode.

11.2.6.1 Reader is Offline Only

For both contactless EMV mode and contactless mag-stripe mode transactions, if the reader is offline only, then the transaction shall be declined.

Requirements – Card Action Analysis Return *ARQC* – Offline Only Terminal

11.2.6.2a **If** all of the following are true:

The terminal is an offline only terminal.

The terminal sends the first GENERATE AC to a card.

The terminal receives an *ARQC*.

then the terminal shall decline the transaction, returning control to Entry Point as defined in13.3.

11.2.6.2 Reader is either Online Only or Offline with Online Capability

For both contactless EMV mode and contactless mag-stripe mode transactions, the reader shall send a User Interface Request Message with the following parameters set:

Message Identifier: '17' (“Card read OK. Please remove card”)

Status: Card Read Successfully

Hold Time: 300ms

Language Preference: If returned by the card during Application Selection

Requirements – Card Action Analysis Return *ARQC* – EMV Mode (partial online) or Mag-Stripe Mode at Online Capable Terminal

11.2.6.3a **If** all of the following are true:

The terminal is configured to be either online only or offline with online capability.

The transaction mode is either contactless EMV (partial online) or contactless mag-stripe.

The terminal sends the first GENERATE AC to a card.

The terminal receives an *ARQC*.

If Offline Data Authentication is required to be performed, it is performed successfully.

then the terminal shall perform an online transaction(See section 12).

11.2.6.4a **If** all of the following are true:

The terminal is configured to be either online only or offline with online capability.

The transaction mode is either contactless EMV (partial online with immediate authorisation) or contactless mag-stripe.

The terminal sends the first GENERATE AC to a card.

The terminal receives an *ARQC*.

If Offline Data Authentication is required to be performed, it is performed successfully.

The online connection cannot be completed.

then the terminal shall decline the transaction, returning control to Entry Point as defined in13.3, unless Merchant specific configurations in support of Kernel 4 as required by payment system rules allow otherwise.

The mechanism used to send the transaction online depends upon the transaction mode.

11.2.6.3 Terminal supports Delayed Authorisations

For both contactless EMV mode and contactless mag-stripe mode transactions, the reader shall send a User Interface Request Message with the following parameters set:

Message Identifier: '17' ("Card read OK. Please remove card")

Status: Card Read Successfully

Hold Time: 300ms

Language Preference: If returned by the card during Application Selection

Requirements – Card Action Analysis Return *ARQC* – EMV Mode (partial online) or Mag-Stripe Mode at Delayed Authorisations Terminal

11.2.6.5a **If** all of the following are true:

The terminal is configured to support Delayed Authorisations.

The transaction mode is either contactless EMV (partial online) or contactless mag-stripe.

The terminal sends the first GENERATE AC to a card.

The terminal receives an *ARQC*.

Offline Data Authentication is performed successfully.

then the terminal shall approve the transaction, returning control to Entry Point as defined in 13.2.

12 Online Processing

12.1 Overview

If the card or reader determines that the transaction requires an online authorisation, and if the reader has online capability, the reader transmits an online authorisation message to the Acquirer. This may be immediately or at a later time if the reader is configured to perform Delayed Authorisations.

Online Processing, as defined in *[EMV 4.3 Book 3]*, section 10.9, and *[EMV 4.3 Book 4]*, section 6.3.8, allows the Issuer's host system to authenticate and decision the transactions using the Issuer's host-based risk management parameters. An online authorisation request is initiated by the response from the first GENERATE AC command being an *ARQC*.

Requirements – Online Processing	
12.1.1.1a	**If** the terminal requests online authorisation, **and** the terminal is not configured for Delayed Authorisations, **then**the terminal shall attempt to send the transaction online for authorisation
12.1.1.2a	**If** the card requests online authorisation, **and** the terminal is not configured for Delayed Authorisations, **then**the terminal shall attempt to send the transaction online for authorisation
12.1.1.3a	**If** the terminal requests online authorisation, **and** the terminal is configured for Delayed Authorisations, **then**the terminal shall accept the transaction locally, **and**send the transaction online for authorisation at a later time.
12.1.1.4a	**If** the card requests online authorisation, **and** the terminal is configured for Delayed Authorisations, **then**the terminal shall accept the transaction locally, **and**send the transaction online for authorisation at a later time.

12.2 Processing Requirements

12.2.1 Contactless Mag-Stripe Mode Processing

The response data field in Format 1 or Format 2 must be parsed as specified in *[EMV 4.3 Book 3]*, section 6.5.5.4.

The following data elements must be extracted and stored locally for further usage:

Cryptogram Information Data (CID)

The *ATC* value post the GENERATE AC command

Application Cryptogram (AC)

12.2.1.1 *ATC* Check

The reader shall validate that the post GENERATE AC *ATC* has the same value as the *ATC* retrieved in the Read Application Data transaction phase. If the two values do not match, a suspected fraudulent transaction has been attempted and the transaction must be declined.

Requirements – Online Processing Mag-Stripe *ATC* Check	
12.2.1.1a	**If** the transaction is a mag-stripe mode transaction, **then**: The terminal shall compare the *ATC* returned by the GET DATA command to the *ATC* returned in the GENERATE AC command. **If** the *ATC* values do not match, **then** the terminal shall decline the transaction.

12.2.1.2 *AC* Check

The reader shall check the *CID* to check that it indicates that the card returned an *ARQC*. If not, the card declined the transaction and the transaction must be declined.

Requirements – Online Processing – Mag-Stripe *AC* Check

12.2.1.2a **If** the transaction is a mag-stripe transaction,
then:

The terminal shall validate the *AC* returned.

If the *AC* is not an*ARQC*,
then the terminal shall decline the transaction.

12.2.1.3 Pseudo-Magnetic Stripe Generation

The payment data needs to be formatted into pseudo magnetic stripe Track 1 and Track 2 data. The pseudo Track 1 and Track 2 are returned to the POS terminal which sends them to the authorisation host as part of the authorisation request. The online authorisation host uses the pseudo track data to identify and authenticate the card.

Requirements – Online Processing – Pseudo-Magnetic Stripe Generation

12.2.1.3a **If** the transaction is a mag-stripe mode transaction,
then the payment data shall be formatted into pseudo magnetic stripe Track 1 and Track 2 which the POS will send to the host.

Several data items retrieved or generated in the course of the transaction are formatted and included within this pseudo track data:

Account Number

The PAN retrieved from the card in the Read Application Data phase is in an EMV compressed numeric format. This needs to be converted into the appropriate character format for inclusion in Track 1 or Track 2.

Cardholder Name

The *Cardholder Name* retrieved from the card in the Read Application Data phase is a variable length alphanumeric data item with a length up to 26 bytes.

The Cardmember name for inclusion in Track 1 is formed from the *Cardholder Name* as follows:

If *Cardholder Name* is longer than 21 bytes, it should be truncated to the leftmost 21 bytes.

If *Cardholder Name* is less than 21 bytes long, it should be right padded with space characters to fill the field.

Note: The *Cardholder Name* retrieved from the card may contain a generic name common for all cards.

Application Transaction Counter (ATC)

The *ATC* retrieved from the card is a two-byte hex value. It shall be converted to a decimal value and padded with leading zeros, if necessary, prior to populating the applicable Track 1 or Track 2 field. The resulting full five digits are then placed in the applicable field of the track data.

Application Expiration Date

The *Application Expiration Date* retrieved from the card is in YYMMDD format. The DD will need to be dropped prior to populating the relevant field of the track data.

Application Cryptogram

The 5CSC data field in the track data is used to convey a portion of the cryptogram returned from the card in response to the GENERATE AC command.

The cryptogram is an eight-byte hex value. In order to populate this field, the most significant five bytes are first discarded. The remaining three least significant bytes are converted to a decimal value prior to populating this field.

For example, Cryptogram = '123569ABCD112987'. Discard the five most significant bytes leaving '112987'. Convert this to decimal giving a value of 1124743. If the resultant value is less than five digits long, pad with leading zeros to get a five digit value. The last five digits – 24743 – are then placed in this field of the track data.

Service Code

The *Service Code* will need to be extracted from the *Track 2 Equivalent Data* retrieved from the card. The *Track 2 Equivalent Data* item is formatted as follows:

Table 12-1: Track 2 Equivalent Data

Field Name	Length
Account Number (PAN)	15
Field Separator ('D')	1
Card Expiration Date (YYMM)	4
Service Code	3
Padding (arbitrary values)	12
Language Code	2
Padding ('F')	1

The reader shall generate pseudo magnetic stripe Track 1 and Track 2 data as specified in Table 12-2 and Table 12-3. The constructed track data is made available to the reader for online authorisation and standard payment processing.

Table 12-2: Layout of Track 1 for Mag-Stripe Mode Transaction

Field 45 – Track 1 Data	Start Sentinel	1 byte
	Format Code	1 byte
	PAN	15 bytes
	Field Separator	1 byte
	Cardmember name	21 bytes
	ATC	5 bytes
	Field Separator	1 byte
	Card Expiration Date	4 bytes
	Service Code	3 bytes
	Unpredictable Number(Format: YYMM – see section 10.2.3.1)	4 bytes
	Cryptogram	5 bytes
	End Sentinel	1 byte

Table 12-3: Layout of Track 2 for Mag-Stripe Mode Transaction

Track 2 Data	Start Sentinel	1 byte
	PAN	15 bytes
	Field Separator	1 byte
	Card Expiration Date	4 bytes
	Service Code	3 bytes
	Unpredictable Number(Format: YYMM – see section 10.2.3.1)	4 bytes
	Cryptogram	5 bytes
	ATC	5 bytes
	End Sentinel	1 byte

12.2.2 Partial Online Processing

At this stage in the transaction the card and reader interaction is complete, and the card may be removed. If a reader is not performing a delayed authorisation transaction, then it carries out the following process after it formats a User Interface Request Message to send the “Remove card” prompt (as described in Section11.2.6, *Card Returns an ARQC*):

- **If** a reader is not performing a delayed authorisation transaction,
  and is able to go online,
  then the kernel returns control to Entry Point to send the transaction online, passing a Final Outcome of ***Online Request*** with the parameter settings defined in Table 12-4. The reader processes the final outcome and formats the authorisation request to be transmitted to the Acquirer for online authorisation. The reader determines the transaction disposition based on the online response indication, as defined in *Book A*.
  Elseif the reader is unable to go online,
  Then the reader has not succeeded in going online and the transaction ***must*** be declined as per Section 13.3, *Transaction Declined*.

Table 12-4:Partial Online - Parameter Settings

Start	N/A
Online Response Data	N/A
CVM	As determined in section 8.2, Cardholder Verification – Processing Requirements
UI Request on Outcome Present	Yes • **Message Identifier:**'1B' (“Authorising, Please Wait”) • **Status:**Processing • **Hold Time:** 0 • **Language Preference**
UI Request on Restart Present	**No**
Data Record Present	Yes
Discretionary Data Present	No
Alternate Interface Preference	N/A
Receipt	N/A
Field Off Request	N/A
Removal Timeout	Zero

12.2.3 Delayed Authorisation Processing

At this stage in the transaction the card and reader interaction is complete, and the card may be removed. A reader that is performing a delayed authorisation transaction carries out the following process after it formats a User Interface Request Message to send the “Remove card” prompt (as described in Section 11.2.6.3, *Terminal Supports Delayed Authorisation*):

- **If** the reader is performing a delayed authorisation transaction,
  then the kernel returns control to Entry Point to complete the transaction as per Section 13.2, *Transaction Approved*. The authorisation request is transmitted to the Acquirer for online authorisation at a later time.

13 Transaction Completion

13.1 Overview

Once the transaction has either been approved or declined, the card's role in the transaction is complete. The reader will then complete the transaction with one of the Final Outcomes indicated below.

13.2 Transaction Approved

If the transaction is approved then the kernel returns control to Entry Point, passing a Final Outcome of ***Approved*** with the following parameter settings:

Start	N/A
Online Response Data	N/A
CVM	As determined in section 8.2, Cardholder Verification – Processing Requirements
UI Request on Outcome Present	Yes • **Message Identifier:** '03' ("Approved") • **State:** Card Read Successfully • **Hold Time:** 0 • **Language Preference**
UI Request on Restart Present	No
Data Record Present	Yes
Discretionary Data Present	No
Alternate Interface Preference	N/A
Receipt	N/A
Field Off Request	N/A
Removal Timeout	Zero

13.3 Transaction Declined

If the transaction is declined, then the kernel returns control to Entry Point, passing a Final Outcome of ***Declined*** with the following parameter settings:

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 • **Hold Time:** 0 • **Language Preference**
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

14 Membership-Related Data Processing

14.1 Overview

The Card Issuer may require unique Membership Reference Number or Membership Product or Scheme information be stored on the Card for processing at a reader that supports such a Membership scheme. To support this functionality the Card may hold ***optional*** data elements that provide values to support such Membership Related Data Processing.

During the Read Application Data phase of a transaction the reader may recover optional tags from the Card associated with a Membership Scheme by use of the READ RECORD command, and reading the data elements from the data files that have been personalised on the Card during initial Card Issuance.

14.2 Data

The following data elements held on the Chip, are used by the reader:

- **Membership Product Identifier (Tag '9F5A')** - The presence of the *Membership Product Identifier* on the Card is optional. The value of the field indicates which product (or 'scheme') is supported.
- **Product Membership Number (Tag '9F5B')** - The presence of the *Product Membership Number* on the Card is optional. The field is dependent on a valid *Membership Product Identifier* being available. The value of the field, if present, indicates the membership number associated with the product.

The *Membership Product Identifier* indicates that the Card is part of a membership scheme. The *Product Membership Number* optionally indicates the Cardholder's membership number for the membership scheme. Only one *Membership Product Identifier* and *Product Membership Number* pair may exist per Card.

14.3 Processing Requirements

The reader will read the membership details from the Card during Read Application Data processing using the READ RECORD commands. If the reader supports a membership scheme, then it may use the data in the *Membership Product Identifier* to identify whether the Card is in a scheme that the reader supports. If the reader requires a membership number associated with that scheme then the reader will use the *Product Membership Number* retrieved from the Card. The reader can then utilise these values to perform any Membership processing it requires. Any Membership Related Data processing ***must*** take place after the Read Application Data phase of the transaction and ***must not*** negatively impact the remainder of the payment transaction flow, processing or performance.

The functionality to be performed as part of Membership Related Data is outside the scope of this specification.

Requirements – Membership-Related Data	
14.3.1.1a	**If** the reader supports the use of Membership Data, **then** the reader shall make use of the Membership Data read during Read Application Data processing if the data is available.
14.3.1.2a	**If** the reader supports the use of Membership Data, **then** the reader shall not impact the transaction processing or performance.

Annex A Kernel 4 Data Elements

This annex defines the data elements used for Kernel 4 processing.

Section A.1 lists all data elements.

Section A.2 lists transaction data.

Section A.3lists the minimum data elements required for an EMV mode data record and for a mag-stripe mode data record.

Section A.4lists the minimum data elements required for authorisation and Clearing and Settlement.

A.1 Data Elements

Table 14-1: Data Elements

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Additional Terminal Capabilities	Indicates the data input and output capabilities of the terminal	Terminal	b	'9F40'	5		
Alternate Interface Support	Indicates whether the terminal supports an alternate payment interface to the contactless reader.	Terminal		—		Contact Mag-stripe Other	
Amount, Authorised	Authorised amount of the transaction (excluding adjustments).	Terminal	n 12	'9F02'	6		
Amount, Other	Secondary amount associated with the transaction representing a cashback amount	Terminal	n 12	'9F03'	6		
Application Cryptogram (AC)	AC computed by the card during a transaction.	Card	b 64	'9F26'	8	Can be: • ARQC • AAC • TC	This is a transient data element, returned to the reader in the response to the first GENERATE AC or second GENERATE AC command.
Application Currency Code	Indicates the currency in which the account is managed.	Card	n 3	'9F42'	2	Coded according to *[ISO 4217]*	An optional data object made available to the reader via the READ RECORD command.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Application Effective Date	Date from which the card application may be used.	Card	n 6 YYMMDD	'5F25'	3		A mandatory data object made available to the reader via the READ RECORD command for mag-stripe mode.
Application Expiration Date	Date after which the card application expires.	Card	n 6 YYMMDD	'5F24'	3		A mandatory data object made available to the reader via the READ RECORD command.
Application File Locator (AFL)	Indicates the location (SFI, range of records) of the AEFs related to a given application.	Card	var.	'94'	var. up to 64		This data element is returned to the reader following GET PROCESSING OPTIONS.
Application Interchange Profile (*AIP*)	Indicates the capabilities of the card to support specific functions in the application.	Card	b 16	'82'	2		A mandatory data object made available to the reader via the GET PROCESSING OPTIONS command.
Application Primary Account Number (PAN)	Card number.	Card	var. up to cn 19	'5A'	var. up to 10	The Primary Account Number must be maintained as the same value for both the Kernel 4 mag-stripe mode and the EMV mode.	A mandatory data object made available to the reader via the READ RECORD command. For Kernel 4 mag-stripe mode processing, the PAN must be limited to fifteen digits in order to leave room for the cryptogram and ATC in Track 2.
Application Primary Account Number (PAN) Sequence Number	Identifies and differentiates cards (applications) with the same PAN.	Card	n 2	'5F34'	1	Due to limitations set by Kernel 4 mag-stripe mode, this must be set to 00 or be otherwise predictable by the Issuer	An optional data object made available to the reader via the READ RECORD.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Application Priority Indicator	Indicates the priority of a given application or group of applications in a directory.	Card	b 8	'87'	1		Optional data element returned in response to a SELECT command.
Application Public Key Certificate	Application Public Key Certificate used during CDA.	Card	b	'9F46'	var. up to 128		Used for CDA.
Application Public Key Exponent	Exponent of Application Public Key	Card	b	'9F47'	1 or 3		Used for CDA.
Application Public Key Remainder	Remaining digits of Application Public Key.	Card	b	'9F48'	var.	See *[EMV 4.3 Book 2]*, section 6.1.	Used for CDA.
Application Selection Indicator	This parameter is used by the terminal during Application Selection. The Terminal determines which card applications are supported. If the indicator is set ON, then the terminal must recognise all applications on the card whose AID begins with the entire AID kept within the terminal.	Terminal	At the discretion of the terminal; not sent across the interface	—	See format		
Application Template	Template containing one or more data objects relevant to an application directory entry according to *[ISO 7816-5]*.	Card	b	'61'	var. up to 252		Templates are used to define TLV structures that contain other data elements.
Application Transaction Counter (ATC)	Counter maintained by the application in the card.	Card	b 16	'9F36'	2	Initial value is zero. It is incremented by 1 each time a transaction is performed.	A mandatory data object made available to the reader via the GET DATA command for mag-stripe mode.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Application Usage Control (AUC)	Indicates Issuer-specified restrictions on the geographic usage and services allowed for the card application.	Card	b 16	'9F07'	2		A data object made available to the reader via the READ RECORD command.
Application Version Number	Version number assigned by the Issuer for the application.	Card	b 16	'9F08'	2	For this specification the Application Version Number must always be '0001'.	An optional data object made available to the reader via the READ RECORD command.
Authorisation Code	Non-zero value generated by the Authorisation Systems for an approved transaction.	Issuer	an 6	'89'	6	Issuer Specific	Proprietary Code returned from Issuer Authorisation systems.
Authorisation Response Code (ARC)	Data element generated by the Issuer Host System or the reader indicating the disposition of the transaction.	Issuer or Terminal	an 2	'8A'	2	Codes generated as indicated in *[ISO 8583]*.	The value present forms part of the Issuer Authentication Data if received from the Issuer. The data is also sent to the card as part of the second GENERATE AC command forming part of the CDOL2.
Authorisation Response Cryptogram (ARPC)	A cryptogram generated by the Issuer Host System during an online transaction	Issuer	b 64	—	8		A cryptogram generated by the Issuer Host System and included in the Issuer Authentication Data to be returned to the reader and sent to the chip card in the response to an online transaction. Refer to Issuer Authentication Data in this table.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Card Interface and Payment Capabilities	Data element indicating: • Other interfaces supported by the device. • Issuer-specified restrictions on usage at delayed authorisation terminals. • Dynamic Limit Set associated with the card.	Card	b 16	9F70	2	See Table 5-1.	An optional data object made available to the reader via the READ RECORD command.
Card Risk Management Data Object List 1 (CDOL1)	List of data objects (tag and length) to be passed to the card application with the first GENERATE AC command.	Card	b	'8C'	var. up to 252		A mandatory data object made available to the reader via the READ RECORD command.
Card Risk Management Data Object List 2 (CDOL2)	List of data elements (tag and length) to be passed to the card application with the second GENERATE AC command.	Card	b	'8D'	var. up to 252		An optional data object made available to the reader via the READ RECORD command.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Cardholder Name	Indicates Cardholder Name according to *[ISO 7813]*.	Card	ans 2-26	'5F20'	2-26	This data element may contain a static value different from the actual Cardmember Name (e.g. 'Valued Customer'). Maximum length of this data element if transmitted in an online authorisation request is 21 bytes.	A mandatory data object made available to the reader via the READ RECORD command for mag-stripe mode.
Cardholder Verification Method (CVM) List	Identifies a prioritised list of methods of verification of the cardholder supported by the card application.	Card	b	'8E'	var. up to 32		An optional data object made available to the reader via the READ RECORD command.
Cardholder Verification Results (CVR)	Proprietary data element indicating the exception conditions that occurred during Card Risk Management.	Card	b 32	—	4		Transmitted to the reader in Issuer Application Data during GENERATE AC processing.
Certification Authority Public Key	Payment system public key used for offline data authentication.	Terminal	Per payment system specifi-cations	—	Per pay-ment system specifi-cations	Value generated by the payment system CA and loaded to terminal by acquirer.	Terminals must be capable of holding a minimum of six CAPKs per AID

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Certification Authority Public Key Index	Identifies the certification authority's public key in conjunction with the Registered Identification Provider (RID) for use in static data authentication.	Card	b 8	'8F'	1	Values assigned by the authorised Certification Authority	
Contactless Reader Capabilities	A proprietary data element with bits 8, 7, and 4 only used to indicate a terminal's capability to support Kernel 4 mag-stripe or EMV contactless. This data element is OR'd with *Terminal Type*, Tag'9F35', resulting in a modified Tag '9F35', which is passed to the card when requested.	Terminal	n 2	'9F6D'	1	00 = Kernel 4 Contactless (Version 1.0 mag-stripe only) 40 = Kernel 4 (Contactless Version ≥ 2.0 mag-stripe only) 80 = Kernel 4 (Contactless Version ≥2.0 EMV mode and mag-stripe mode)	Configured in a reader compliant with Kernel 4 and passed to the card via a modified *Terminal Type*, Tag '9F35' when Tag '9F35' is present in the PDOL of the card
Cryptogram Information Data (CID)	Indicates the type of cryptogram (TC, ARQC or AAC) returned by the card and the actions to be performed by the terminal.	Card	b 8	'9F27'	1	Bits 8-7: 00 = AAC 01 = TC 10 = ARQC 11 = AAR (not supported)	This is information the application returns to the reader indicating the type of AC being sent. It is generated dynamically and not subsequently stored within the application.
Cryptogram Version Number	Proprietary data element indicating the version of the TC, AAC/ARQC algorithm used by the application.	Card	b 8	Issuer Specific	1	Value = '01' or '02' for this specification	Data element held within CDOL. Transmitted in the Issuer Application Data.
Delayed Authorisations Supported	Defines whether the terminal is configured to perform delayed authorisations.	Terminal	Implementation specific	—	Implementation specific		

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Dynamic Reader Limits	A set of dynamic reader limits comprising a: • Reader Contactless Transaction Limit, if present • Reader Contactless Floor Limit, if present • Reader CVM Required Limit, if present If the Kernel selects a particular Dynamic Reader Limits, the limits in this selection are used by the Kernel to override the limits Reader Contactless Transaction Limit,Reader Contactless Floor Limit and Reader CVM Required Limit used by Entry Point.	Terminal	Implementation specific	—	Implementation specific	Assigned by the payment system	
Dynamic Reader Limits – Default	A set of *Dynamic Reader Limits*, to be applied to a transaction when *Sets of Dynamic Reader Limits* does not contain an applicable set of *Dynamic Reader Limits*.	Terminal	Implementation specific	—	Implementation specific	Assigned by the payment system	
Enhanced Contactless Reader Capabilities	Proprietary Data Element for managing Contactless transactions and includes Contactless terminal capabilities (static) and contactless Mobile transaction (dynamic data) around CVM	Terminal	b 32	'9F6E'	4		Returned to the Card in the GET PROCESSING OPTIONS in response to PDOL.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Issuer Action Code – Default	Specifies conditions that cause a transaction to be declined if it might have been approved online, but the reader is unable to process the transaction online.	Card	b 40	'9F0D'	5		A data object made available to the reader via the READ RECORD command.
Issuer Action Code – Denial	Specifies conditions that cause the decline of a transaction without attempting to go online.	Card	b 40	'9F0E'	5		A data object made available to the reader via the READ RECORD command.
Issuer Action Code – Online	Specifies conditions that cause a transaction to be transmitted online.	Card	b 40	'9F0F'	5		A data object made available to the reader via the READ RECORD command.
Issuer Application Data	Contains proprietary application data for transmission to the Issuer in all transaction messages.	Card	b	'9F10'	var. 32		This is a transient data element that is constructed by concatenating other data elements as indicated.
Issuer Authentication Data	Issuer data transmitted to card for online Issuer authentication.	Issuer	b 64-128	'91'	var. up to 16	The Issuer Authentication Data consists of the following data: • First 8 bytes = ARPC • Last 2 bytes = Authorisation Response Code	This data is transmitted to the card by the reader in the EXTERNAL AUTHENTICATE command.
Issuer Country Code	Indicates the country of the Issuer, represented according to *[ISO 3166]*.	Card	n 3	'5F28'	2	According to *[ISO 3166]*	An optional data object made available to the reader via the READ RECORD command.
Issuer Public Key Certificate	Issuer's public key certified by a certification authority for use in static data authentication.	Card	b 512-1984	'90'	var. 64-248		

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Issuer Public Key Exponent	Issuer-specified data to be used with the Issuer's public key algorithm for static data authentication.	Card	b	'9F32'	1 or 3		
Issuer Public Key Remainder	Remaining digits of the Issuer's public key to be hashed.	Card	b	'92'	var.	See *[EMV 4.3 Book 2]*, section 6.1.	
Membership Product Identifier	A product identifier for the membership scheme.	Card	an	'9F5A'	Var up to 8		An optional data element used by the Terminal to determine whether card is in a supported membership scheme.
Mobile CVM Results	Proprietary data element returned from the Card in the GET PROCESSING OPTIONS response, indicating the status of Mobile CVM entry.	Card	b 32	'9F71'	3	Byte 1: CVM Performed '01' = Performed '3F' = Not performed Byte 2: '03' Byte 3: CVM Result '00' = Unknown '01' = Failed '02' = Successful '03' = Blocked	Retained locally for use during Cardholder Verification
Offline Capability	Offline capable terminals are capable of performing offline contactless transactions.	Terminal	Implementation specific	—	Implementation specific		
Online Capability (Partial)	Terminals that are Online Capable must be capable of performing Partial Online contactless transactions.	Terminal	Implementation specific	—	Implementation specific		

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Point of Service Data Code	A series of codes that identify the terminal capability, security data, and specific conditions present at the time a transaction took place at the point of service.	Terminal	an	—	12		For further information regarding this element, please refer to the Payment Scheme Network Specifications.
Processing Options Data Object List (PDOL)	Contains a list of reader resident data objects (tags and lengths) needed by the ICC in processing the GET PROCESSING OPTIONS command.	Card	b	'9F38'	var.		
Product Membership Number	A unique number to identify the cardholder as part of the scheme.	Card	an	‘9F5B’	Var up to 32		An optional data element used by the Terminal to uniquely identify the cardholder as being part of the membership scheme. If present then tag ‘9F5A’ must also be present.
Reader Contactless Floor Limit	Indicates the contactless floor limit.	Entry Point	n 12	—	6		
Reader Contactless Transaction Limit	Indicates the limit for which contactless transactions can be conducted.	Entry Point	n 12	—	6		
Reader CVM Required Limit	Indicates the limit for which CVM is required.	Terminal	b	—	—	—	
Removal Timeout	Indicates whether a timeout function should be started with the time specified.	Terminal	Implementation specific	—	Implementation specific		
Service Code	Contains the Service Code elements.	Card	n 3	'5F30'	2	Should be coded according to *[ISO 7813]*.	An optional data element retrievable via the READ RECORD command.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Sets of Dynamic Reader Limits	A collection of *Dynamic Reader Limits*. The collection shall be capable of holding fifteen sets of *Dynamic Reader Limits*. Each set shall apply to a particular card “Dynamic Limit Set”. Each set of *Dynamic Reader Limits* shall be addressable by the card “Dynamic Limit Set” to which it pertains.	Terminal	Implementation specific	—	Implementation specific	Assigned by the payment system	
Short File Identifier (SFI)	Identifies the SFI to be used in the commands related to a given AEF.	Card	b 8	'88'	1	Values are 1-10: Governed by joint payment systems	These are pointers to the records readable during READ APPLICATION DATA.
Signed Application Data	Digital signature on critical application parameters that is used in static data authentication.	Card	b 512-1984	'93'	64-248		
Static Data Authentication Tag List	List of tags of primitive data objects defined in *[EMV 4.3 Book 3]* whose value fields are to be included in the signed static or dynamic application data.	Card	—	'9F4A'	var.	Tag '82' (Application Interchange Profile)	
Status Check Support	This flag indicates whether the reader is able to use a single unit of currency check to determine whether the card is genuine and active.	Entry Point	Implementation specific	Implementation specific	Implementation specific		

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Terminal Action Code – Default	Specifies the Acquirer's conditions that cause a transaction to be rejected if it might have been approved online, but the reader is unable to process the transaction online.	Terminal	b 40	—	5		Used with Issuer Action Codes, to decide on action to be taken during Terminal Action Analysis.
Terminal Action Code – Denial	Specifies the Acquirer's conditions that cause a transaction to be denied without an attempt to go online.	Terminal	b 40	—	5		Used with Issuer Action Code, to decide on action to be taken during Terminal Action Analysis.
Terminal Action Code – Online	Specifies the Acquirer's conditions that cause a transaction to be transmitted online.	Terminal	b 40	—	5		Used with Issuer Action Code, to decide on action to be taken during Terminal Action Analysis.
Terminal Capabilities	Indicates the card data input, CVM, and security capabilities of the terminal.	Terminal	b 24	'9F33'	3	Defined in *[EMV 4.3 Book 4]*, Annex A2.	
Terminal Country Code	Indicates the country of the terminal.	Terminal	n 3	'9F1A'	2	According to *[ISO 3166]*.	
Terminal Exception File	A file of account numbers to be used by the terminal, for which it has been predetermined that there shall be an authorisation decision of denial.	Terminal		—			
Terminal Floor Limit	Indicates the floor limit in the Terminal.	Entry Point	b 32	'9F1B'	4		
Terminal Type	Indicates the environment of the terminal, its communication capability, and its operational control.	Terminal	n 2	'9F35'	1	As per *[EMV 4.3]*.	

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Terminal Verification Results	Status of the different functions as seen from the terminal.	Terminal	b 40	'95'	5		Data object included in CDOL1 and CDOL2
Track 1 Data	Data carried in Network messages containing information to identify the card account and other details sourced from chip data.						For further information regarding this element, please refer to the Payment Scheme Network Specifications and section 12 in this specification
Track 2 Data	Data carried in Network messages containing information to identify the card account and other details sourced from chip data.						For further information regarding this element, please refer to the Payment Scheme Network Specifications and section 12 in this specification
Track 2 Equivalent Data	Image of magnetic stripe Track 2. (For Kernel 4, Track 2 Equivalent Data may not be an exact image of magnetic stripe Track 2.)	Card	Cn	'57'	var. up to 19	According to *[ISO 7813]*	Mandatory data element available via READ RECORD command for mag-stripe mode must be present in SFI 1 Record 1.
Transaction Currency Code	Indicates the currency code of the transaction.	Terminal	n 3	'5F2A'	2	According to *[ISO 4217]*	
Transaction Date	Local date that the transaction was authorised.	Terminal	n 6	'9A'	3	As YYMMDD	
Transaction Type	Indicates the type of financial transaction, represented by the first two digits of *[ISO 8583:1987]* Processing Code. The actual values to be used for the Transaction Type data element are defined by the relevant payment system.	Terminal or reader	n 2	'9C'	1		

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Unpredictable Number	Value to provide variability and uniqueness to the generation of the AC.	Terminal	b 32	'9F37'	4		This is an Unpredictable Number fed into the card application by the reader and used within the two GENERATE AC processes. The data element is not then subsequently stored within an application on the card.
Unpredictable Number Range	Specifies the range in which the unpredictable number must be generated in for contactless mag-stripe mode.	Terminal		—			The default minimum range is 0 to 60. Note that the number range is inclusive, so a range of 0 to 60 should be capable of generating 61 integer numbers in the range 0 to 60.
Zero Amount Allowed	This flag indicates whether a transaction with a zero amount is permitted.	Entry Point	Implementation specific	Implementation specific	Implementation specific		

A.2 Transaction Data

Table 14-2: Transaction Data

Data Object	Presence	Tag	Source
Amount, Authorised	M	'9F02'	Terminal
Amount, Other	M	'9F03'	Terminal
Application Effective Date	M	'5F25'	Card
Application PAN Sequence Number	M	'5F34'	Card
Application Primary Account Number (PAN)	M	'5A'	Card
Application Version Number	M	'9F08'	Card
Card Risk Management Data Object List 1 (CDOL1)	M	'8C'	Card
Cardholder Name	M	'5F20'	Card
Issuer Action Code – Default	M	'9F0D'	Card
Issuer Action Code – Denial	M	'9F0E'	Card
Issuer Action Code – Online	M	'9F0F'	Card
Issuer Country Code	M	'5F28'	Card
Terminal Country Code	M	'9F1A'	Terminal
Terminal Verification Results	M	'95'	
Track 2 Equivalent Data	M	'57'	Card
Transaction Currency Code	M	'5F2A'	Reader (configured) or Terminal (dynamic)
Transaction Date	M	'9A'	
Transaction Type	M	'9C'	Terminal or Reader depending on implementation
Unpredictable Number	M	'9F37'	Entry Point

A.3 Read Record Data

All data supplied to the reader for use in the processing of a financial transaction that is not dynamically maintained by the card will be held in file records and presented to the reader during the appropriate READ RECORD commands.

Table 14-3: Mandatory Read Record Data Objects – EMV & Mag-stripe Mode

Data Object	Presence	Comments
Application Primary Account Number	M	The account number associated with this application.
Application Expiration Date	M	Date after which the card application expires.
Card Risk Management Data ObjectList 1 (CDOL1)	M	Used during GENERATE AC

Table 14-4: Additional Mandatory Read Record Data Objects – Mag-stripe Mode

Data Object	Presence	Comments
Application Effective Date	M	The date from which the card application may be used. Required for Unpredictable Number generation.
Cardholder Name	M	This field is required for Mag-stripe mode where pseudo Track 1 is generated.
Track 2 Equivalent Data	M	Track 2 Equivalent Data should be present in SFI 1 Record 1.

The data objects listed in Table 14-5are not retrievable by the READ RECORD command but may be retrieved by the reader using the GET DATA command.

Table 14-5:Additional Mandatory Get Data Data Objects – Mag-stripe Mode

Data Object	Presence	Comments
ATC	M	This field is required for Mag-stripe mode.

A.4 Data Records

The following tables list the minimum data elements required for authorisation and Clearing and Settlement: Table 14-6 lists data elements for EMV mode and Table 14-7 lists those for mag-stripe mode. For further information regarding these elements, please refer to the Payment Scheme Network Specifications.

Table 14-6: Data Record for EMV Mode (Minimum Data Elements)

Data Object	Auth Message	Clearing Message
Amount, Authorised	M	M
Amount, Other	M	M
Application Cryptogram	M	M
Application Interchange Profile (*AIP*)	M	M
Application PAN Sequence Number	M	M
Application Transaction Counter (ATC)	M	M
Cryptogram Information Data	M	M
Issuer Application Data	M	M
Point of Service Data Code[3]	M	M
Terminal Country Code	M	M
Terminal Verification Results (TVR)	M	M
Track 2 Data	M	—
Transaction Currency Code	M	M
Transaction Date	M	M
Transaction Type	M	M
Unpredictable Number	M	M

[3] May be constructed using Tag '9F33' *Terminal Capabilities* and other terminal parameters and transaction characteristics as necessary.

Table 14-7: Data Record for Mag-Stripe Mode (Minimum Data Elements)

Data Object	Auth Message	Clearing Message
Point of Service Data Code[4]	M	M
Track 1 Data [5]	C	—
Track 2 Data[6]	C[7]	—

[4]May be constructed using Tag '9F33' *Terminal Capabilities* and other terminal parameters and transaction characteristics as necessary.

[5]Sourced from Tag '57'*Track 2 Equivalent Data* and other chip data elements as described in section 12.2.

[6]Sourced from Tag '57'*Track 2 Equivalent Data*.

[7] At least one of Track 1 and Track 2 shall be present and sent in the authorisation message. Track 1/Track 2 to be constructed as described in section 12.2.

Annex B Configuration Data

This annex lists the data that the terminal and Entry Point shall make available to the kernel.

B.1 Configuration Data Provided by the Terminal

Table 14-8 and Table 14-9 list the static configuration data per AID that the terminal shall make available to the kernel (for EMV mode and mag-stripe mode respectively).

Table 14-8: Kernel Configuration Data (EMV acceptance environment)

Name	Tag	Description
Application Version Number	'9F08'	The version number assigned by the payment scheme for the kernel application.
Cardholder Verification Method (CVM) Capability	—	Defines the CVM capabilities of the terminal (e.g. Signature, Enciphered Online PIN, No CVM Support).
Certification Authority Public Keys	—	A terminal shall be capable of holding six CAPKs.
Contactless Reader Capabilities	'9F6D'	A proprietary data element with bits 8, 7, and 4 only used to indicate a terminal's capability to support Kernel 4 contactless mag-stripe mode or contactless EMV mode.
Delayed Authorisations Supported	—	Defines whether the terminal is configured to perform delayed authorisations.
Dynamic Reader Limits – Default	—	A set of *Dynamic Reader Limits*, to be applied to a transaction when *Sets of Dynamic Reader Limits* does not contain an applicable set of *Dynamic Reader Limits*.

Name	Tag	Description
Enhanced Contactless Reader Capabilities	'9F6E'	Proprietary Data Element for managing Contactless transactions and includes Contactless terminal capabilities (static) and contactless Mobile transaction (dynamic data) around CVM
Offline Capability	—	Offline capable terminals are capable of performing offline contactless transactions.
Online Capability (Partial)	—	Online capable terminals are capable of performing Partial Online contactless transactions.
Sets of Dynamic Reader Limits	—	A collection of *Dynamic Reader Limits*. The collection shall be capable of holding fifteen sets of *Dynamic Reader Limits*. Each set shall apply to a particular card “Dynamic Limit Set”. Each set of *Dynamic Reader Limits* shall be addressable by the card “Dynamic Limit Set” to which it pertains.
Terminal Action Codes	—	A set of *Terminal Action Codes* (Online, Decline, and Default) shall be available.
Terminal Exception File	—	A file of account numbers to be used by the terminal, for which it has been predetermined that there shall be an authorisation decision of denial.
Terminal Type	'9F35'	Indicates the environment of the terminal, its communication capability, and its operational control.
Unpredictable Number Range	—	Specifies the range in which the unpredictable number must be generated in for contactless mag-stripe mode.

Table 14-9: Kernel Configuration Data (Mag-Stripe Terminal)

Name	Tag	Description
Application Version Number	'9F08'	The version number assigned by the payment scheme for the kernel application.
Cardholder Verification Method (CVM) Capability	—	Defines the CVM capabilities of the terminal (e.g. Signature, Enciphered Online PIN, No CVM Support).
Certification Authority Public Keys	—	A terminal shall be capable of holding six CAPKs.
Contactless Reader Capabilities	'9F6D'	A proprietary data element with bits 8, 7, and 4 only used to indicate a terminal's capability to support Kernel 4 mag-stripe or EMV contactless.
Delayed Authorisations Supported	—	Defines whether the terminal is configured to perform delayed authorisations.
Enhanced Contactless Reader Capabilities	'9F6E'	Proprietary Data Element for managing Contactless transactions and includes Contactless terminal capabilities (static) and contactless Mobile transaction (dynamic data) around CVM
Dynamic Reader Limits – Default	—	A set of *Dynamic Reader Limits*, to be applied to a transaction when *Sets of Dynamic Reader Limits* does not contain an applicable set of *Dynamic Reader Limits*.
Online Capability (Partial)	—	Mag-stripe only terminals must be capable of supporting Partial Online functionality

Name	Tag	Description
Sets of Dynamic Reader Limits	—	A collection of *Dynamic Reader Limits*. The collection shall be capable of holding fifteen sets of *Dynamic Reader Limits*. Each set shall apply to a particular card “Dynamic Limit Set” combination. Each set of *Dynamic Reader Limits* shall be addressable by the card “Dynamic Limit Set” to which it pertains.
Terminal Action Codes	—	A set of *Terminal Action Codes* (Online, Decline, and Default) shall be available.
Terminal Exception File	—	A file of account numbers to be used by the terminal, for which it has been predetermined that there shall be an authorisation decision of denial.
Terminal Type	'9F35'	Indicates the environment of the terminal, its communication capability, and its operational control.
Unpredictable Number Range	—	Specifies the range in which the unpredictable number must be generated in for contactless mag-stripe mode.

B.2 Configuration Data Provided by Entry Point

Table 14-10: Entry Point Configuration Data

Status Check Support flag
Zero Amount Allowed flag
Reader Contactless Transaction Limit
Reader Contactless Floor Limit
Reader Contactless Floor Limit Exceeded
Reader CVM Required Limit
Reader CVM Required Limit Exceeded
Terminal Floor Limit (Tag '9F1B'), if present

Annex C Glossary

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

AAC	Application Authentication Cryptogram
AAR	Application Authentication Referrals
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.
AEF	Application Elementary File
AFL	Application File Locator
AIP	Application Interchange Profile
an	Alphanumeric characters
ans	Alphanumeric Special characters, as defined in *[EMV 4.3 Book 4]*, Annex B
APDU	Application Protocol Data Unit
Application Cryptogram	Cryptogram returned by the card; one of the following cryptogram types: TC Transaction Certificate ARQC Authorisation Request Cryptogram AAC Application Authentication Cryptogram
Approved	A Final Outcome
ARC	Authorisation Response Code
ARPC	Authorisation Response Cryptogram
ARQC	Authorisation Request Cryptogram

ASCII	American Standard Code for Information Interchange
ATC	Application Transaction Counter
ATM	Automated Teller Machine
AUC	Application Usage Control
b	Binary or Bit string
CAPK	Certification Authority Public Key
Card	As used in these specifications, a consumer device supporting contactless transactions.
CDA	Combined Dynamic Data Authentication/Application Cryptogram
CDOL	Card Risk Management Data Object List
CID	Cryptogram Information Data
5CSC [field]	5-digit Card Security Code
CVR	Card Verification Results
DDA	Dynamic Data Authentication
DEA	Data Encryption Algorithm
Declined	A Final Outcome
Delayed Authorisation	Designates a Partial Online contactless transaction plus mandatory Offline Data Authentication. For more information, see section 1.5.
DES	Digital Encryption Standard
EMV®	A global standard for credit and debit payment cards based on chip card technology. The *EMV Integrated Circuit Card Specifications for Payment Systems* are developed and maintained by EMVCo.

EMVCo	EMVCo LLC is the organisation of payment systems that manages, maintains, and enhances the EMV specifications. EMVCo is currently operated by American Express, JCB, MasterCard, and Visa.
End Application	A Final Outcome
Final Outcome	Result provided to the reader as a result of Entry Point processing the Outcome from the kernel, or provided directly by Entry Point under exception conditions.
Full Online	Designates a transaction in which the card remains in the operating field while an online authorisation request is processed, and EMV response data may be returned.Kernel 4 does not support such transactions.
GENAC1	First GENERATE AC
GPO	Get Processing Options
IAC	Issuer Action Code
ICC	Integrated Circuit Card. Synonymous with ‘Smart Card’ and ‘Card’
ISO	International Organization for Standardization
N/A	Not Applicable; a possible value for several Outcome and Final Outcome parameters
ODA	Offline Data Authentication
Online Request	A Final Outcome
OR	Bitwise OR
Outcome	Result from the kernel processing, provided to Entry Point, or under exception conditions, result of Entry Point processing. In either case, a primary value with a parameter set.
PAN	Primary Account Number

Partial Online	Designates a transaction in which the card may be removed from the operating field early in the transaction and the result of the transaction is based on the response from the Issuer's authorisation system. For more information, see section 1.5.
PSN	PAN Sequence Number
RID	Registered Application Provider Identifier
RNM	Random Number of Month
SDA	Static Data Authentication
Select Next	An Outcome (not used by Kernel 4)
SFI	Short File Identifier [ISO7816-4]
TAC	Terminal Action Code
TC	Transaction Certificate
TDOL	Transaction Certificate Data Object List
Try Again	An Outcome
Try Another Interface	A Final Outcome
TVR	Terminal Verification Results
UI	User Interface
UN	Unpredictable Number

*** END OF DOCUMENT ***