

EMV^{®*}

Contactless Specifications for Payment Systems

Book C-4

Kernel 4 Specification

Version 2.1
March 2011

* EMV is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo.

© 2011 EMVCo, LLC ("EMVCo"). All rights reserved. Any and all uses of the EMV Specifications ("Materials") shall be permitted only pursuant to the terms and conditions of the license agreement between the user and EMVCo found at <http://www.emvco.com/specifications.aspx>.

EMV

Contactless Specifications for Payment Systems

Book C-4

Kernel 4 Specification

Version 2.1
March 2011

© 2011 EMVCo, LLC ("EMVCo"). All rights reserved. Any and all uses of these Specifications is subject to the terms and conditions of the EMVCo Terms of Use agreement available at www.emvco.com and the following supplemental terms and conditions.

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

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

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

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

Contents

1	Introduction.....	1
1.1	Scope.....	1
1.2	Audience.....	1
1.3	Volumes of Contactless Specifications.....	1
1.4	Reference Material	2
1.5	Use of Terms	3
1.6	Overview.....	4
2	Contactless Modes and Transaction Flows	5
2.1	Contactless Modes of Operation	5
2.1.1	Support for Contactless Modes of Operation.....	5
2.1.2	Card Risk Management Data Object List (CDOL) Switch.....	7
2.1.3	Contactless Mag-Stripe Mode Transaction.....	7
2.1.4	Contactless EMV Mode Transactions.....	7
2.2	Contactless Transaction Processing	8
2.2.1	Offline Transaction.....	10
2.2.2	Partial Online Transaction.....	10
2.2.3	Full Online Transaction	11
2.2.4	Partial Online vs. Full Online Transactions	12
2.3	Contactless Transaction Configurations	16
2.4	Optimised Transaction Processing	20
3	Processing Overview	27
4	Initiate Application Processing	29
4.1	Overview.....	29
4.2	Commands	29
4.3	Processing Requirements.....	30
4.3.1	PDOL Processing	30
4.3.2	Determination of Operating Mode.....	33
4.3.3	Fixed Records for Offline Data Authentication (Optimised Transaction Processing)	33
5	Read Application Data.....	39
5.1	Overview.....	39
5.2	Commands	39
5.3	Processing Requirements.....	39
5.4	GET DATA.....	42

6	Offline Data Authentication (Unoptimised Processing)	43
6.1	Overview	43
6.2	Processing Requirements	44
6.2.1	Multiple ODA Methods Supported	44
6.2.2	Scheme Certification Authority Public Keys	44
6.2.3	Static Data Authentication	45
6.2.4	Combined Dynamic Data Authentication / AC Generation	45
7	Processing Restrictions	47
7.1	Overview	47
7.2	Processing Requirements	47
7.2.1	EMV Processing Restrictions	48
7.2.2	Data Elements for Mag-Stripe Mode	51
7.2.3	TVR Adjustment for Optimised Transaction Processing	52
8	Cardholder Verification	53
8.1	Overview	53
8.2	Processing Requirements	53
8.2.1	<i>Reader CVM Required Limit Exceeded</i> Indicator Is Set	54
8.2.2	<i>Reader CVM Required Limit Exceeded</i> Indicator Not Set	58
9	Terminal Risk Management	61
9.1	Overview	61
9.2	Processing Requirements	62
9.2.1	Floor Limit Checking	62
9.2.2	Exception File Checking	62
10	1st Terminal Action Analysis	63
10.1	Overview	63
10.2	Processing Requirements	64
10.2.1	Offline Processing Results	64
10.2.2	Zero Amount Allowed and Status Check Requested Validation	68
10.2.3	Additional Processing for Contactless Mag-Stripe Mode	69
10.2.4	Request AC in First GENERATE AC	71
11	1st Card Action Analysis	73
11.1	Overview	73
11.2	Processing Requirements	74
11.2.1	General Card Action Analysis	74
11.2.2	Card Returns a TC	75

11.2.3 Card Returns an AAC	76
11.2.4 Card Returns an ARQC	77
11.2.5 Format of the Response to GENERATE AC Command	85
12 Offline Data Authentication (Optimised Processing)	87
12.1 Overview	87
12.2 Processing Requirements	88
13 Online Processing	95
13.1 Overview	95
13.2 Processing Requirements	96
13.2.1 Contactless Mag-Stripe Mode (Partial Online Only)	96
13.2.2 Contactless Mag-Stripe Mode	101
13.2.3 Contactless EMV Mode – Partial Online	101
13.2.4 Contactless EMV Mode – Full Online	102
14 Issuer Authentication	107
14.1 Overview	107
14.2 Processing Requirements	107
15 2nd Terminal Action Analysis	109
15.1 Overview	109
15.2 Processing Requirements	112
15.2.1 CDA	112
15.2.2 Advice Messages	113
16 2nd Card Action Analysis	115
16.1 Overview	115
16.2 Processing Requirements	115
17 Issuer Script Processing	117
17.1 Overview	117
17.2 Processing Requirements	117
18 Transaction Completion	119
18.1 Overview	119
18.2 Transaction Approved	119
18.3 Transaction Declined	120
Annex A Kernel 4 Data Elements	121
A.1 Data Elements	122

A.2 Transaction Data	135
A.3 Data Records.....	136
Annex B Configuration Data	139
B.1 Configuration Data Provided by the Terminal.....	139
B.2 Configuration Data Provided by Entry Point	142
Annex C Terminal Action Codes.....	143
C.1 TAC Values for Terminals with Offline Only Capability.....	144
C.2 TAC Values for Other Terminals.....	144
Annex D Glossary	145

Figures

Figure 2-1: Transaction Flow Overview	9
---	---

Tables

Table 2-1: Contactless Mode Selection	6
Table 2-2: Contactless Transaction Combinations	16
Table 2-3: Reader Configurations Supporting ODA Data Read	21
Table 4-1: Terminal Type – EMV Tag '9F35'	31
Table 4-2: Kernel 4 Reader Capabilities – Tag '9F6D'	31
Table 4-3: Terminal Type – Modified	32
Table 4-4: Fixed File Locations for Offline Authentication Data	33
Table 4-5: Mandatory Card Data Element Grouping for Optimised Transaction Processing	34
Table 4-6: Optimised Transaction Processing Conditions	35
Table 5-1: Application Interchange Profile (AIP)	41
Table 10-1: Terminal Verification Results Settings	72
Table 12-1: Offline Data Authentication	89
Table 13-1: Track 2 Equivalent Data	99
Table 13-2: Layout of Track 1 for Mag-Stripe Mode Transaction	99
Table 13-3: Layout of Track 2 for Mag-Stripe Mode Transaction	100
Table A-1: Data Elements	122
Table A-2: Transaction Data	135
Table A-3: Data Record for EMV Mode (Minimum Data Elements)	136
Table A-4: Data Record for Mag-Stripe Mode (Minimum Data Elements)	137
Table B-1: Kernel Configuration Data (EMV acceptance environment)	139
Table B-2: Kernel Configuration Data (Mag-Stripe Terminal)	141
Table B-3: Entry Point Configuration Data	142
Table C-1: Terminal Action Codes	143
Table C-2: Offline Only Terminals: TAC – Denial and TAC – Default	144
Table C-3: TAC Values for Terminals Other Than Offline Only	144

Requirements

Requirements – Mandatory Support for Contactless Mag-Stripe Mode	5
Requirements – Optional Support for Contactless EMV Mode	6
Requirements – Offline Transaction	10
Requirements – Partial Online Transaction	10
Requirements – Full Online Transaction	11
Requirements – Partial Online Override	12
Requirements – Partial Online User Message	12
Requirements – Card Removal Timer Expired Indicator	13
Requirements – Partial Online Transaction Completion	14
Requirements – Card Early Removal	15
Requirements – Transaction Combinations	19
Requirements – READ RECORD – Online Only Terminal, Optimised Transaction Processing	23
Requirements – READ RECORD – Online Capable Terminal, Optimised Transaction Processing	24
Requirements – READ RECORD – Online Only and Online Capable Terminals, Optimised Transaction Processing	26
Requirements – READ RECORD – Offline Capable Terminals, Optimised Transaction Processing	26
Requirements – GET PROCESSING OPTIONS	29
Requirements – GPO Without PDOL Data	30
Requirements – PDOL Data in GPO	30
Requirements – GPO Includes Modified Terminal Type	32
Requirements – GPO Response Check	32
Requirements – READ RECORDs for ODA	36
Requirements – READ RECORDs	40
Requirements – GET DATA ATC	42
Requirements – Offline Data Authentication	43
Requirements – Offline Data Authentication Priority	44
Requirements – Offline Data Authentication Keys	44

Requirements – Static Offline Data Authentication	45
Requirements – Combined Dynamic Offline Data Authentication	45
Requirements – Processing Restrictions: Application Version Number	48
Requirements – Processing Restrictions: AUC Domestic	49
Requirements – Processing Restrictions: AUC International	49
Requirements – Processing Restrictions: AUC Environment.....	50
Requirements – Processing Restrictions: Dates	50
Requirements – Data Elements for Mag-Stripe Mode	51
Requirements – TVR Adjustment for Optimised Transaction Processing	52
Requirements – Reader CVM Supported Methods	54
Requirements – CVM Processing	56
Requirements – Online PIN	57
Requirements – CVM Processing	58
Requirements – CVM Processing – Card Supports Cardholder Verification.....	59
Requirements – Terminal Risk Management	61
Requirements – Terminal Risk Management	62
Requirements – Terminal Risk Management	62
Requirements – Terminal Action Analysis	65
Requirements – Terminal Action Analysis	65
Requirements – Terminal Action Analysis	66
Requirements – Terminal Action Analysis	67
Requirements – Terminal Action Analysis	67
Requirements – Zero Amount Allowed	68
Requirements – Status Check Requested	68
Requirements – Unpredictable Number	70
Requirements – GENERATE AC Data Construction.....	70
Requirements – Card Action Analysis Processing	74
Requirements – Card Action Analysis Return TC.....	75
Requirements – Card Action Analysis Return AAC	76
Requirements – Card Action Analysis Return ARQC – Partial Online	80

Requirements – Card Action Analysis Return <i>ARQC</i> – Full Online.....	82
Requirements – Card Action Analysis Return <i>ARQC</i> – Mag-Stripe Mode	84
Requirements – Card Action Analysis Return Formats	86
Requirements – Optimised Offline Data Authentication	87
Requirements – Optimised Offline Data Authentication Processing	88
Requirements – Online Processing	95
Requirements – Online Processing Mag-Stripe <i>ATC</i> Check	96
Requirements – Online Processing Mag-Stripe <i>AC</i> Check	97
Requirements – Online Processing Mag-Stripe <i>AC</i> Check	97
Requirements – Online Processing Partial EMV Online Fail.....	101
Requirements – Online Processing Full EMV Online	102
Requirements – Online Processing Full EMV Online	103
Requirements – Online Processing Full EMV Online	104
Requirements – Issuer Authentication.....	107
Requirements – Terminal Action Analysis	109
Requirements – Terminal Action Analysis	110
Requirements – Terminal Action Analysis	110
Requirements – Terminal Action Analysis Processing	112
Requirements – Terminal Action Analysis Advices	113
Requirements – Card Action Analysis <i>AAC</i>	115
Requirements – Issuer Scripts	117

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 Contactless Specifications 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 seven-volume set:

Book A: Architecture and General Requirements

Book B: Entry Point Specification (supersedes Entry Point v1.0)

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 D: Contactless Communication Protocol (replaces CCP v2.0.1)

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 4.2]	<i>EMV Integrated Circuit Card Specifications for Payment Systems</i> , Version 4.2, June 2008, including:
[EMV 4.2 Book 1]	<i>EMV Integrated Circuit Card Specifications for Payment Systems</i> , Book 1, Application Independent ICC to Terminal Interface Requirements
[EMV 4.2 Book 2]	<i>EMV Integrated Circuit Card Specifications for Payment Systems</i> , Book 2, Security and Key Management
[EMV 4.2 Book 3]	<i>EMV Integrated Circuit Card Specifications for Payment Systems</i> , Book 3, Application Specification
[EMV 4.2 Book 4]	<i>EMV Integrated Circuit Card Specifications for Payment Systems</i> , 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 Use of Terms

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

Delayed Authorisation	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 and (if Offline Data Authentication is being performed) after any subsequent records read that may be required. The result of the transaction is based on the response from the Issuer's authorisation system.
Full Online	During a Full Online contactless transaction, the card remains in the operating field of the Reader while an online authorisation request is processed, and EMV response data may be returned to the card during this transaction. This scenario applies only to contactless transactions being performed in EMV mode.

1.6 Overview

This volume includes the following chapters and annexes:

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

Chapter 2 describes the modes in which a contactless card and Reader can operate, and details the different flows that a contactless transaction can take.

Chapter 3 provides a high-level overview of processing according to this specification.

Chapters 4 – 18 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 details the Terminal Action Codes (TACs).

Annex D 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 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 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

- 2.1.1.1 If a card indicates (by setting *A/P* 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.
-

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 Supports Mag-Stripe Mode	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 in Table 4-3 on page 32).

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 requirement 4.3.1.3).

- 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 supports 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.

Requirements – Optional Support for Contactless EMV Mode

- 2.1.1.2 **If** a Reader indicates that it supports EMV mode (by setting b7 and b8 of *Terminal Type* 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 Chapter 13, Online Processing, for more information.

No EMV data will be returned in the Authorisation Response message; therefore Issuer Authentication is not supported as part of contactless mag-stripe mode.

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'.

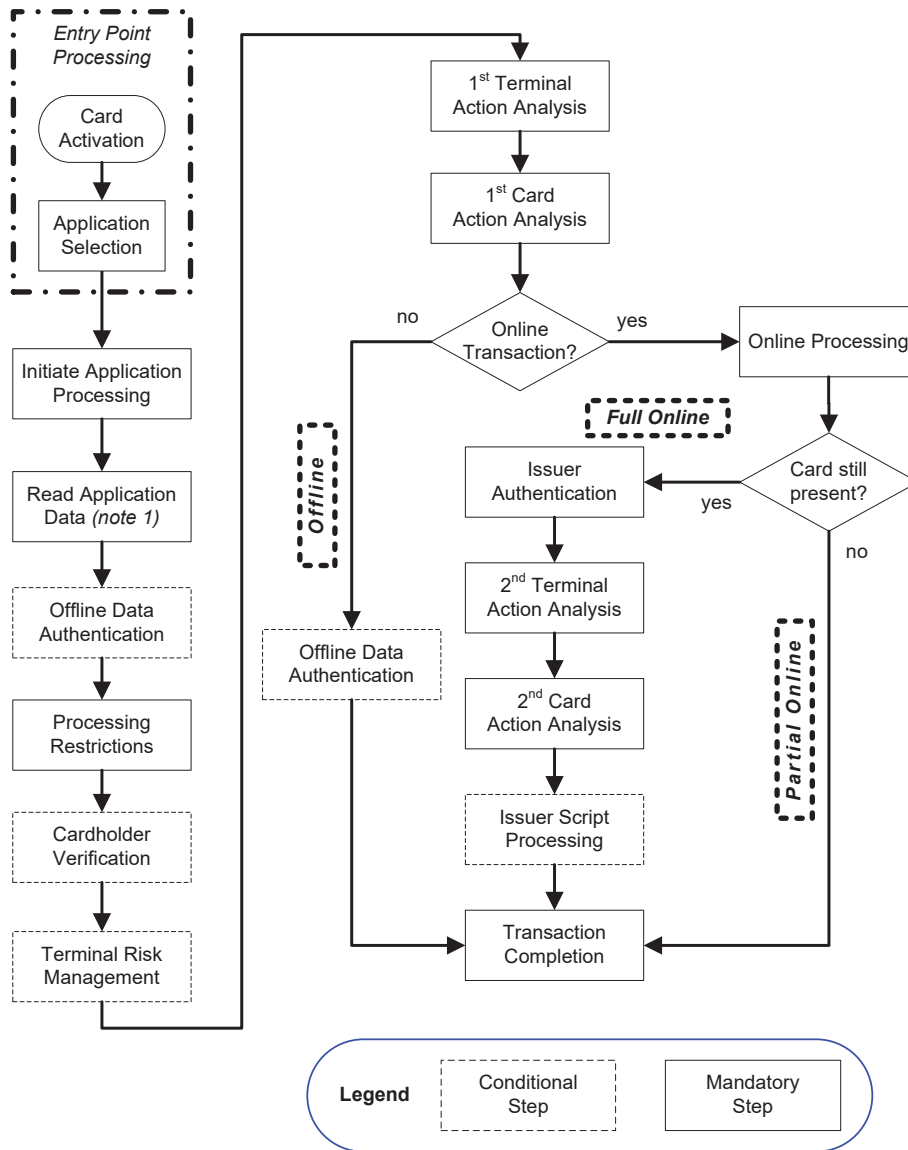
2.2 Contactless Transaction Processing

A contactless transaction can be performed in one of three different ways:

- Offline
- Partial Online
- Full Online (EMV mode only)

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

Figure 2-1: Transaction Flow Overview



Note 1: In the case of Readers where Offline Data Authentication is optimised, certain data is read later in the transaction flow, after the card has responded to the first GENERATE AC command. (See Table 4-6 on page 35.)

2.2.1 Offline Transaction

During an offline transaction, the card and Reader either approve or decline a transaction without further online processing. Only 1st Terminal Action Analysis and 1st Card Action Analysis are performed.

Requirements – Offline Transaction

- 2.2.1.1 **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 without any online processing or further card interaction following the 1st Card Action Analysis.
-

2.2.2 Partial Online Transaction

A Partial Online transaction is a variation of a Full Online transaction, in which the interaction between the card and the Reader ends after 1st Card Action Analysis has completed. 2nd Terminal Action Analysis and 2nd Card Action Analysis are not performed and the result of the transaction is based on the response from the Issuer's authorisation system.

Requirements – Partial Online Transaction

- 2.2.2.1 **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).
-

2.2.3 Full Online Transaction

During a Full Online transaction (EMV mode only), the card, Reader, and Issuer authorisation system approve or decline a transaction. Interactions between the card and Reader occur before and after online processing. The card must remain in the operating field until the authorisation response from the Issuer is received.

1st Terminal Action Analysis, 1st Card Action Analysis, 2nd Terminal Action Analysis, and 2nd Card Action Analysis are all performed. EXTERNAL AUTHENTICATE and Issuer Script Processing also take place if applicable as indicated by the data returned in the online response.

Requirements – Full Online Transaction

- 2.2.3.1 **If** a Reader is configured to perform Full Online transactions, **then** the Reader shall be able to perform a Full Online transaction including a second GENERATE AC, EXTERNAL AUTHENTICATE, and Issuer Script Processing when applicable.
-

2.2.4 Partial Online vs. Full Online Transactions

Whether a transaction is performed as a Full Online or Partial Online transaction depends on three conditions:

- whether the transaction is being processed in EMV mode or mag-stripe mode
- whether the Reader is capable of processing Full Online transactions (and configured to enable this option)
- whether the Issuer authorisation response is received in time

For acceptance environments which have a high speed online authorisation capability and where a contactless card may readily remain held in the field, a Reader may provide support for Full Online functionality. Readers supporting Full Online functionality must be able via configuration option to be set to perform Partial Online functionality when required by the implementation environment.

Requirements – Partial Online Override

2.2.4.1 **If** a Reader supports Full Online transactions,
then the Reader shall support a configuration option that allows this capability to be turned off and the Reader set to perform Partial Online transactions instead.

A Reader deployed for quick transactions may only provide for Partial Online transactions in order to release the card from the operating field as fast as possible. As such, the cardholder will be prompted to remove the card from the field immediately after the completion of 1st Card Action Analysis (and, in the case of optimised cards, any subsequent READ RECORDs required for Offline Data Authentication).

Requirements – Partial Online User Message

2.2.4.2 **If** a Reader supports Partial Online transactions,
and the Reader does not support Full Online transactions,
then, immediately following 1st Card Action Analysis (and, in the case of optimised cards, any subsequent READ RECORDs required for Offline Data Authentication), the Reader shall invoke the User Interface Request Message to send a 'Remove card' prompt to the user.

Readers capable of Full Online processing will rely on Timeout Services of the POS System requested via a Final Outcome in order to decide between Partial Online and Full Online processing. The Reader examines the Timeout Indicator returned in the response to an Online Request:

- If the Timeout Indicator is set to true (1), then the transaction is completed as a Partial Online transaction.
- Else (the Timeout Indicator is set to false (0)) the transaction is completed as a Full Online transaction.

Requirements – Card Removal Timer Expired Indicator

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

- A Reader is online capable.
- The Reader is capable of Full Online processing.
- The Reader is currently configured to support Full Online transactions.

Then:

- The Reader shall examine the Timeout Indicator returned with the Online Response.
- **If** the Timeout Indicator is set to true (1),
then the Reader shall complete the transaction as a Partial Online transaction.

Else (the Timeout Indicator is set to false (0)) the Reader shall complete the transaction as a Full Online transaction.

Regardless of how the transaction is being performed, 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. For example, if the Reader plans to perform a Partial Online transaction and indicates that the card can be removed after 1st Card Action Analysis is complete, it will not try to perform Issuer Authentication even if the card is still in the field of the Reader.

Requirements – Partial Online Transaction Completion

- 2.2.4.4 **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.
-

If the cardholder removes the card from the operating field without being prompted to do so, then for transactions being performed as Partial Online, the kernel returns control to Entry Point, passing an Outcome of **Try 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

- 2.2.4.5 **If** a transaction is being performed as a Partial Online transaction, **and** the card leaves the operating field before the cardholder is prompted to remove it from the field, **then** the Reader shall prompt the user to 'Present Card Again'.

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 ¹	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.	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.
Mag-Stripe Mode Full Online	Not applicable. ²	Not applicable. ²

¹ This may include "Delayed Authorisations" – where the transaction response is based on that from an intermediate system or Issuer's agent, pending a subsequent (i.e. delayed) authorisation request to the Issuer.

² Transactions in mag-stripe mode will never perform Issuer Authentication. (If an EXTERNAL AUTHENTICATE command is received by a card when performing a transaction in mag-stripe mode, the card will reject the command.)

Contactless Transaction Mode	Card Supports Only Mag-Stripe Mode	Card Supports Both Mag-Stripe and EMV Modes
Mag-Stripe Mode Offline	A mag-stripe mode card will always return an <i>ARQC</i> to the first <i>GENERATE AC</i> command.³ However, if the Reader is unable to go online, then the transaction will be declined.	When operating in mag-stripe mode, the card will always return an <i>ARQC</i> to the first <i>GENERATE AC</i> command.³ However, if the Reader is unable to go online, then the transaction is declined.
EMV Mode Partial Online ⁴	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'.
EMV Mode Full Online	Not applicable.	A full EMV online transaction is performed including 2nd Card Action Analysis. The card remains in the operating field throughout the transaction. The transaction result will be based on the outcome of 2nd Terminal Action Analysis and 2nd Card Action Analysis. A card with CDOL-Switch will present a CDOL for Cryptogram Version '01'.

³ Assuming that the Terminal has not requested an AAC.

⁴ This may include "Delayed Authorisations".

Contactless Transaction Mode	Card Supports Only Mag-Stripe Mode	Card Supports Both Mag-Stripe and EMV Modes
EMV Mode Offline	Not applicable.	A full EMV offline transaction is performed, if offline is allowed by Issuer configuration settings and Card Risk Management. A card with CDOL-Switch will present a CDOL for Cryptogram Version '01'.

Requirements – Transaction Combinations

2.3.1.1 **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.

2.3.1.2 **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.

2.3.1.3 **If** the terminal is performing a Full Online transaction in EMV mode with an EMV card,
then the card may be removed after the 2nd Card Action Analysis and the terminal shall complete the online transaction in EMV mode.

2.3.1.4 **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.

2.3.1.5 **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 are performed, and the terminal shall complete the transaction in EMV mode.

2.4 Optimised Transaction Processing

To reduce the processing time of a contactless transaction, an optional but recommended model for optimising the transaction is specified. If a Reader supports this optimised processing model and if the contactless card is similarly optimised (see section 4.3.3), then the Reader shall delay reading the records for Offline Data Authentication until after the first GENERATE AC command. (Contactless cards that run on Kernel 4 must accept a READ RECORD command before or after the first GENERATE AC command has been issued.)

In this model, at the time that the cryptogram is requested in the first GENERATE AC, the Reader has not performed Offline Data Authentication. Therefore, the *Terminal Verification Results (TVR)* bits relating to Offline Data Authentication must be set to 0b in both the GENERATE AC request and the clearing message.

Readers that always go online do not need to support Offline Data Authentication and do not need to read the records specific to SDA or CDA, unless such terminals are enabled to request CDA with Signature as part of the first GENERATE AC, or in the case of terminals processing a transaction in EMV mode at terminals capable of Full Online EMV mode transaction when unable to go online.

For Partial Online transactions performed by Readers supporting Delayed Authorisations, Offline Data Authentication must be performed.

Alternatively in an unoptimised Reader, Offline Data Authentication can be performed after Read Application Data and before 1st Terminal Action Analysis (according to a standard EMV transaction flow), as long as in doing so the Reader still meets the performance requirements detailed within *Book A*.

Table 2-3 details the requirements to perform Offline Data Authentication and read the associated application data.

Table 2-3: Reader Configurations Supporting ODA Data Read

Reader Configuration	Offline Data Authentication	Read Application Data
Online only	Conditional (As described in this table in the right hand column)	If card and Reader support CDA and a Signature is returned with the ARQC in the response to the first GENERATE AC command Or/ If SDA is the chosen ODA method, then SDA must be performed if the terminal is capable of performing Full Online contactless transactions and the terminal has determined it is unable to go online In the case that CDA or SDA is required to be performed, then Offline Data Authentication data should be read from the assigned records on the card as defined in section 4.3.3. Otherwise Offline Data Authentication data need not be read from the assigned records on the card

Reader Configuration	Offline Data Authentication	Read Application Data
Offline with Online capability	Conditional (Mandatory if transaction is performed offline or as described in this table in the right hand column)	If the transaction is to be approved offline Or/ If card and Reader support CDA and a Signature is returned with the ARQC in the response to the first GENERATE AC command Or/ If SDA is the chosen ODA method, then SDA must be performed if the terminal is capable of performing Full Online contactless transactions and the terminal has determined it is unable to go online In the case that CDA or SDA is required to be performed, then Offline Data Authentication data should be read from the assigned records on the card as defined in section 4.3.3. Otherwise Offline Data Authentication data need not be read from the assigned records on the card
Delayed Authorisations (Refer to section 1.5)	Mandatory	Offline Data Authentication data should be read from the assigned records on the card as defined in section 4.3.3.
Offline only	Mandatory	Offline Data Authentication data should be read from the assigned records on the card as defined in section 4.3.3.

Requirements – READ RECORD – Online Only Terminal, Optimised Transaction Processing

2.4.1.1 If all of the following are true:

- The Reader is online only.
- The Reader supports optimised processing.
- The Reader requested and received an *ARQC* without CDA Signature from the GENERATE AC.

Then the Reader shall not perform READ RECORDs for SFI 2, 3, or 4.

2.4.1.2 If all of the following are true:

- The Reader is online only.
- The Reader supports optimised processing.
- The Reader requested and received an *ARQC* with CDA Signature from the GENERATE AC.

Then the Reader shall perform READ RECORDs for SFI 2 and 4.

2.4.1.3 If all of the following are true:

- The Reader is online only.
- The Reader supports optimised processing.
- The Reader supports Delayed Authorisation.
- The Reader is performing a transaction with a card using SDA.
- The Reader requested and received an *ARQC* without CDA Signature from the GENERATE AC.

Then the Reader shall perform READ RECORDs for SFI 2 and 3.

Requirements – READ RECORD – Online Capable Terminal, Optimised Transaction Processing

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

- The Reader is online capable.
- The Reader supports optimised processing.
- The Reader received an *ARQC* without CDA Signature from the GENERATE AC.

Then the Reader shall not perform READ RECORDs for SFI 2, 3, or 4.

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

- The Reader is online capable.
- The Reader supports optimised processing.
- The Reader received an *ARQC* with CDA Signature from the GENERATE AC.

Then the Reader shall perform READ RECORDs for SFI 2 and 4.

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

- The Reader is online capable.
- The Reader supports optimised processing.
- The Reader supports Delayed Authorisation.
- The Reader is performing a transaction using CDA.

Then:

- The Reader shall request an *ARQC* with CDA Signature at the first GENERATE AC.
 - **If** the Reader receives an *ARQC* with Signature, **then** the Reader shall perform READ RECORDs for SFI 2 and 4.
-

Requirements – READ RECORD – Online Capable Terminal, Optimised Transaction Processing

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

- The Reader is online capable.
- The Reader supports optimised processing.
- The Reader supports Delayed Authorisation.
- The Reader is performing a transaction with an optimised card using SDA.

Then:

- The Reader shall request an *ARQC* at the first *GENERATE AC*.
- **If** the Reader receives an *ARQC* with Signature,
then the Reader shall perform *READ RECORDs* for SFI 2 and 3.

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

- The Reader is online capable.
- The Reader supports optimised processing.
- The Reader supports Delayed Authorisation.
- The Reader is performing a transaction with a card using SDA.
- The Reader requested and received an *ARQC* without CDA Signature from the *GENERATE AC*

Then the Reader shall perform *READ RECORDs* for SFI 2 and 3.

Requirements – READ RECORD – Online Only and Online Capable Terminals, Optimised Transaction Processing

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

- The Reader is online only or online capable.
- The Reader is capable of Full Online EMV processing.
- The Reader supports optimised processing.
- The Reader attempts to perform an online transaction with an SDA capable card.
- The Reader is unable to go online.

Then the Reader shall perform READ RECORDs for SFI 2 and 3 after the first GENERATE AC.

Requirements – READ RECORD – Offline Capable Terminals, Optimised Transaction Processing

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

- The Reader is offline capable.
- The Reader supports optimised processing.
- The Reader is performing an offline transaction with a card using SDA only.

Then the Reader shall perform READ RECORDs for SFI 2 and 3 following the GENERATE AC command.

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

- The Reader is offline capable.
- The Reader supports optimised processing.
- The Reader is performing an offline transaction with a card using SDA and CDA.

Then the Reader shall perform READ RECORDs for SFI 2 and 4 following the GENERATE AC command.

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 4.2 Book 1] – [EMV 4.2 Book 3]. Some functionality supported by EMV is not permitted or is restricted for contactless transactions.

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.

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*.

When processing a contactless transaction according to this specification, 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 D. This 'restart' mechanism enables the kernel to process an online authorisation response message, EMV response data, or an 'Unable to go Online' condition.

The FCI data made available to Kernel 4 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 4.2 Book 3] and [EMV 4.2 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 4.2 Book 3], section 10.1, the card must support the GET PROCESSING OPTIONS command as described in the following section.

Requirements – GET PROCESSING OPTIONS

- 4.2.1.1 A Reader shall send the GET PROCESSING OPTIONS command to the card following Application Selection.
-

4.3 Processing Requirements

4.3.1 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

- 4.3.1.1 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 4.2 Book 3], section 5.4.

Requirements – PDOL Data in GPO

- 4.3.1.2 If the card specified a PDOL in the response to Application Selection,
then the Reader shall send the GET PROCESSING OPTIONS command with the requested PDOL data, except as described in requirement 4.3.1.3.

If the *PDOL* requested *Terminal Type* (Tag '9F35'), the Reader instead returns *Terminal Type – Modified*, as shown in Table 4-3. These values are set by the Reader based on the *Terminal Type* combined (OR'd) with a proprietary data element, *Kernel 4 Reader Capabilities* (Tag '9F6D'), that is stored in the Reader. See Table 4-1 and Table 4-2 for the values of these data elements.

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: Kernel 4 Reader Capabilities – Tag '9F6D'

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0			0				Contactless – Mag-Stripe Version 1.0
0	1			0				Contactless – Mag-Stripe Version 2.0.1
1	0			0				Contactless – EMV and Mag-Stripe Version 2.0.1

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 *Kernel 4 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
1	0			0				Contactless – EMV and Mag-Stripe 2.0

Requirements – GPO Includes Modified Terminal Type

4.3.1.3 If the card requested *Terminal Type*, Tag '9F35', 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 *Kernel 4 Reader Capabilities* (Tag '9F6D').

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 4.2 Book 3], section 6.5.8.4.

Requirements – GPO Response Check

4.3.1.4 A Reader shall check the GPO response data is formed as per [EMV 4.2 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 4.3.2), then proceed to Read Application Data.

4.3.2 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 *A/P* (see Table 5-1 on page 41) 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 *A/P* Byte 2 Bit 8 is 1b, the transaction will use EMV mode.
- If *A/P* Byte 2 Bit 8 is 0b, the transaction will use mag-stripe mode.

4.3.3 Fixed Records for Offline Data Authentication (Optimised Transaction Processing)

Optimised cards will use records in *Short File Identifier (SFI)* 2, 3, and 4 to hold data specific to Offline Data Authentication. The *AFL* will indicate these records to the Reader. The data will be organised into specific *SFI* according to the Offline Data Authentication method supported by the card, as detailed in Table 4-4.

Only data required for Offline Data Authentication will be included in these records, therefore a Reader that does not support Offline Data Authentication, does not need to read these records, or any record in *SFI* 2, 3, or 4.⁵

Mag-Stripe Version 1.0 contactless cards may hold all data (including data required for SDA) in *SFI* 1. An optimised Reader should process such a card according to the processing conditions described in Table 4-6.

Table 4-4: Fixed File Locations for Offline Authentication Data

SDA Data	SFI 2 and SFI 3
CDA Data	SFI 2 and SFI 4

⁵ Terminals supporting optimised transaction processing shall read the records for Offline Data Authentication according to whether the card being processed is optimised or unoptimised. (See Table 4-6.)

Table 4-5: Mandatory Card Data Element Grouping for Optimised Transaction Processing

Short File Identifier	Description	Value
SFI 1	Track 2 Equivalent data (must be in record 1)	'57'
	Cardholder Name	'5F20'
	CDOL 1	'8C'
	CDOL2	'8D'
	Application Version Number	'9F08'
	Application Usage Control (may be signed)	'9F07'
	Issuer Country Code (may be signed)	'5F28'
	Application Currency Code	'9F42'
	CVM List (may be signed)	'8E'
	Application Effective Date (may be signed)	'5F25'
	Application Expiration Date (may be signed)	'5F24'
	Application Primary Account Number (PAN) (may be signed)	'5A'
	Application PAN Sequence Number (may be signed)	'5F34'
	Issuer Action Code – Default (may be signed)	'9F0D'
	Issuer Action Code – Denial (may be signed)	'9F0E'
	Issuer Action Code – Online (may be signed)	'9F0F'
SFI 2	Certification Authority Public Key Index	'8F'
	Static Data Authentication Tag List (may be signed)	'9F4A'
	Issuer Public Key Certificate	'90'
	Issuer Public Key Reminder	'92'
	Issuer Public Key Exponent	'9F32'
SFI 3	Signed Static Application Data	'93'
SFI 4	Application Public Key Certificate	'9F46'
	Application Public Key Exponent	'9F47'
	Application Public Key Remainder	'9F48'

Table 4-6: Optimised Transaction Processing Conditions

Reader Capability	Card Record Structure	SDA	CDA
Unoptimised	Unoptimised (SFI 1 only)	All records read as per <i>AFL</i> during Read Application Data (i.e. prior to GENAC1 (first GENERATE AC)) Offline Authentication performed prior to GENAC1 as normal.	All records read as per <i>AFL</i> during Read Application Data (i.e. prior to GENAC1) Offline Authentication performed post GENAC1 as normal.
Unoptimised	Optimised (SFI 1, 2, 3 / 4)	All records read as per <i>AFL</i> during Read Application Data (i.e. prior to GENAC1) Offline Authentication performed prior to GENAC1 as normal.	All records read as per <i>AFL</i> during Read Application Data (i.e. prior to GENAC1) Offline Authentication performed post GENAC1 as normal.
Optimised	Unoptimised (SFI 1 only)	All records read as per <i>AFL</i> during Read Application Data (i.e. prior to GENAC1) Offline Authentication performed post GENAC1 if required.	All records read as per <i>AFL</i> during Read Application Data (i.e. prior to GENAC1) Offline Authentication performed post GENAC1 if required.
Optimised	Optimised (SFI 1, 2, 3 / 4)	SFI 1 read during Read Application Data (i.e. prior to GENAC1) SFI 2 and 3 read if necessary post GENAC1. Offline Authentication performed post GENAC1 if required.	SFI 1 read during Read Application Data (i.e. prior to GENAC1) SFI 2 and 4 read if necessary post GENAC1. Offline Authentication performed post GENAC1 if required.

For readers capable of optimised processing, only the records necessary for the form of Offline Data Authentication being performed should be read.

Requirements – READ RECORDs for ODA

4.3.3.1 **If the Reader is unoptimised,
then:**

- For SDA or CDA optimised and unoptimised cards, the Reader shall send READ RECORDs as per the *AFL* during Read Application Data before GENAC1 (first GENERATE AC).
- **If SDA is required,
then** it is performed prior to GENAC1.
- **If CDA is required,
then** it is performed post-GENAC1.

4.3.3.2 **If the Reader is optimised,
and the card is unoptimised,
then:**

- The Reader shall send READ RECORDs as per the *AFL* during Read Application Data.
- **If the transaction requires ODA,
then** SDA or CDA is performed post-GENAC1.

4.3.3.3 **If the Reader is optimised,
and the SDA card is optimised,
then:**

- The Reader shall send READ RECORD for SFI 1 during Read Application Data.
 - **If the transaction requires ODA,
then:**
 - The Reader shall send READ RECORD for SFI 2 and 3 during Read Application Data.
 - SDA is performed post-GENAC1.
-

Requirements – READ RECORDs for ODA

4.3.3.4 **If** the Reader is optimised,
and the CDA card is optimised,
then:

- The Reader shall send READ RECORD for SFI 1 during Read Application Data.
 - **If** the transaction requires ODA
then:
 - The Reader shall send READ RECORD for SFI 2 and 4 during Read Application Data.
 - CDA is performed post-GENAC1.
-

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.⁶

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 Chapter 13, Online Processing.

5.2 Commands

- READ RECORD
- GET DATA

The application must support the READ RECORD and GET DATA command as described in [EMV 4.2 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 4.2 Book 3], section 10.2. The encoding of the *AIP* is specified in Table 5-1.

The data supporting Offline Data Authentication is stored in fixed locations as defined in section 4.3.3.

⁶ Terminals supporting optimised transaction processing shall read the records for Offline Data Authentication according to whether the card being processed is optimised or unoptimised. (See Table 4-6.)

The Reader will decide whether to read the data related to Offline Data Authentication or not, depending on its capability to conduct Full Online transactions as described below.

Readers may support Optimised Transaction Processing and delay reading records required for Offline Data Authentication until after the first GENERATE AC command has been performed. Refer to Table 4-6 for further information on optimised and unoptimised Readers and cards.

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 then the unrecognised data object shall be ignored and the transaction shall continue as if the data object had not been present (except if the data is required and shall be retained for kernel processing⁷).

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

Processing rules governing data validation (missing or erroneous data on the card) are detailed in [EMV 4.2 Book 3], section 7.5.

Requirements – READ RECORDs

5.3.1.1 The Reader shall successfully read all records indicated by the *AFL*.

5.3.1.2 The Reader shall successfully read all data elements within all records and capture the correct values.

5.3.1.3 **If** any mandatory data element is missing,
then the Reader shall terminate processing with a suitable error.

5.3.1.4 **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.

⁷ For example, for Offline Data Authentication as stated in [EMV 4.2 Book 3], section 10.2.

Requirements – READ RECORDs

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

Table 5-1: Application Interchange Profile (AIP)

AIP Byte 1 (Leftmost)								Meaning
b8	b7	b6	b5	b4	b3	b2	b1	
0								RFU (Reserved for future use)
	X							1b = SDA supported 0b = SDA not supported
		X						DDA supported
			X					1b = Cardholder verification supported 0b = Cardholder verification not supported
				1				Terminal Risk Management is to be performed
					1			Issuer Authentication is supported
						0		RFU
							X	1b = CDA supported 0b = CDA not supported
AIP Byte 2 (Rightmost)								Meaning
b8	b7	b6	b5	b4	b3	b2	b1	
X								0b = Mag-Stripe Mode Only Supported 1b = EMV and Mag-Stripe Modes Supported
	0							RFU
		0						RFU
			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 4.2 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*

- 5.4.1.1 **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 (Unoptimised Processing)

6.1 Overview

Contactless Readers must support the following two forms of Offline Data Authentication, as described in the [EMV 4.2] specifications:

- SDA
- CDA

Online only Readers are not mandated to support Offline Data Authentication (unless they also support 'Delayed Authorisations' or are capable of performing Full Online transaction).

Requirements – Offline Data Authentication

- 6.1.1.1 With the exception of online only terminals with no support for Delayed Authorisation or not capable of Full Online processing, terminals shall support Static Data Authentication.
 - 6.1.1.2 With the exception of online only terminals with no support for Delayed Authorisation or not capable of Full Online processing, terminals shall support Combined DDA/Application Cryptogram Generation (CDA).
-

6.2 Processing Requirements

Offline Data Authentication must be performed as described in [EMV 4.2 Book 2], chapters 5 and 6, and [EMV 4.2 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 methods supported by the Terminal are identified in *Terminal Capabilities* (Tag '9F33').

6.2.1 Multiple ODA Methods Supported

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

Requirements – Offline Data Authentication Priority

- 6.2.1.1 If a card indicates support of both SDA and CDA methods,
and ODA is required,
then the terminal performs CDA.
-

6.2.2 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

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

6.2.3 Static Data Authentication

If SDA is determined to be performed, it must be performed as described in [EMV 4.2 Book 2], chapters 5 and 6, and [EMV 4.2 Book 3], section 10.3.

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

6.2.3.1 **If** the Offline Data Authentication method being employed is SDA, **then** it shall be performed as per [EMV 4.2 Book 2], chapters 5 and 6, and [EMV 4.2 Book 3], section 10.3.

6.2.3.2 **If** Static Data Authentication fails, **then** the terminal shall set TVR Byte 1 Bit 7 to 1b, 'Offline Static Data Authentication Failed'.

6.2.4 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 4.2 Book 2], section 6.6.

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

Requirements – Combined Dynamic Offline Data Authentication

6.2.4.1 **If** the Offline Data Authentication method being employed is CDA, **then** it shall be performed as per [EMV 4.2 Book 2], section 6.6.

6.2.4.2 **If** CDA fails, **then** the terminal 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. Additionally, in the case that the Reader is processing the transaction using Optimised Transaction Processing for Offline Data Authentication, the *TVR* settings relating to Offline Data Authentication are adjusted at this point.

7.2 Processing Requirements

The Reader performs several types of checks and adjustments:

- EMV Processing Restrictions
- Data elements for mag-stripe mode
- TVR adjustment for Optimised Transaction Processing

The outcomes of these 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 EMV Processing Restrictions

The Reader performs Processing Restrictions, as defined in [EMV 4.2 Book 3], section 10.4, and [EMV 4.2 Book 4], sections 6.3.3 and 6.7.2, to see whether the transaction should be allowed. Processing Restrictions cover the following mandatory checks performed by the Reader:

- Comparison of the card's *Application Version Number*, if present in the card, 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

7.2.1.1 The terminal shall compare the application version number returned by the card in the READ RECORD phase to the one held by the terminal and indicate the result in *TVR* Byte 2 Bit 8.

- *Application Usage Control (AUC)* – This 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

7.2.1.2 The terminal 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.
- The terminal shall check *Application Usage Control* to determine whether the card is valid for the transaction type being performed (domestic cash, goods, or services).

If not,
then the terminal 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

7.2.1.3 The terminal 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.
- The terminal shall check *Application Usage Control* to determine whether the card is valid for the transaction type being performed (international cash, goods, or services).

If not,
then the terminal 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 the bit 'Valid for use at an ATM' set to 1b. If the Reader is other than an ATM (e.g. POS), then the Reader must verify that the card's *AUC* has the bit 'Valid at Readers other than an ATM' set to 1b.

Requirements – Processing Restrictions: AUC Environment

7.2.1.4 If the terminal is a POS,
then:

- The terminal shall check the *Application Usage Control* to determine whether the card can be used at a POS.
- If the transaction cannot be performed on the POS,
then the terminal shall set *TVR* Byte 2 Bit 5 to 1b, 'Requested service not allowed for card product'.

-
- Effective and Expiration Date Checking – These checks ensure that the application is not pre-valid and not expired.
 - If the transaction date is prior to the *Application Effective Date*, the terminal must set *TVR* Byte 2 Bit 6 to 1b, 'Application not effective yet'.
 - If the transaction date is past the *Application Expiration Date*, the terminal must set *TVR* Byte 2 Bit 7 to 1b, 'Application Expired'.

Requirements – Processing Restrictions: Dates

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

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

7.2.2 Data Elements for Mag-Stripe Mode

If the transaction is performed in mag-stripe mode, the terminal must ensure that all data elements needed for the Acquirer message generation are present by verifying that the following data items have been retrieved from the card:

- *Application Transaction Counter (ATC)*
- *Application Primary Account Number (PAN)*
- *Application Primary Account Number (PAN) Sequence Number*
- *Cardholder Name*
- *Card Risk Management Data Object List 1 (CDOL1)*
- *Track 2 Equivalent Data*

If any of the listed data elements is missing, the Reader must set *TVR* Byte 2 Bit 5 to 1b, 'Requested service not allowed for card product'.

Requirements – Data Elements for Mag-Stripe Mode

- 7.2.2.1 **If** the transaction is performed in mag-stripe mode
and any of the *ATC*, *PAN*, *PSN*, *Cardholder Name*, *CDOL1*, or
Track 2 Equivalent Data is not retrieved successfully from the card,
then the terminal shall set *TVR* Byte 2 Bit 5 to 1b, 'Requested
service not allowed for card product'.
-

7.2.3 TVR Adjustment for Optimised Transaction Processing

The Reader must apply the following *TVR* adjustment only if Optimised Transaction Processing for Offline Data Authentication is being performed:

- If the Reader is processing the transaction using the Optimised Transaction Processing model for Offline Data Authentication, the Reader sets the following *TVR* Bytes to 0b:
 - Byte 1 Bit 8 (Offline Data Authentication was not performed)⁸
 - Byte 1 Bit 7 (Offline Static Data Authentication failed)
 - Byte 1 Bit 4 (CDA failed)

Requirements – TVR Adjustment for Optimised Transaction Processing

- 7.2.3.1 An optimised terminal performing an online transaction shall provide a *TVR* with the relevant ODA bits set to 0b (Byte 1 Bits 8, 7, and 4).
-

⁸ Although Offline Data Authentication has not been performed, *TVR* Byte 1 Bit 8 must be set to 0b rather than 1b to avoid an incorrect decision when using the *Terminal Action Codes* and *Issuer Action Codes* during 1st Terminal Action Analysis. (Offline Data Authentication has not been performed because Optimised Offline Data Authentication is being performed for this transaction after 1st Card Action Analysis.)

8 Cardholder Verification

8.1 Overview

If supported, Cardholder Verification must be performed as defined in this section with additional reference to *CVM List* processing as detailed in [EMV 4.2 Book 3], section 10.5, and [EMV 4.2 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 *Cardholder Verification Methods (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

Cardholder Verification processing must be performed as follows:

- If the *Reader CVM Required Limit Exceeded* indicator is set, then perform Cardholder Verification processing as described in section 8.2.1.
- Otherwise perform Cardholder Verification processing as described in section 8.2.2.

8.2.1 ***Reader CVM Required Limit Exceeded Indicator Is Set***

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

8.2.1.1 CVM Processing

Requirements – Reader CVM Supported Methods

8.2.1.1 The Reader creates a list of Supported CVM Methods:

- 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.

Mutually Supported CVM Identified

- If the card contains a *CVM List* with a method which both card and Reader support, 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).

No Mutually Supported CVM Identified – Card Supports Cardholder Verification

- If the card supports Cardholder Verification, but there is no common method shared by both card and Reader, then:
 - If the terminal supports an alternate interface, then a request for the cardholder to use another interface is initiated as follows: 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: '18' ("Please insert/swipe 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

- If the terminal does not support an alternate interface, then the terminal shall set *TVR* Byte 3 Bit 8 to 1b, 'Cardholder Verification was not successful'. Transactions should be approved/declined based on the *IACs/TACs*.

Card does not support Cardholder Verification or CVM List not present

- If the card does not support Cardholder Verification or the *CVM List* is not present or is empty, then the Reader should set the CVM Outcome parameter to 'N/A' at this point and use it to populate the CVM Outcome parameter when returning a Final Outcome during an online authorisation request or completion of an approved transaction.

Note: A CVM Outcome Parameter of 'N/A' indicates that the kernel passes responsibility for determining further processing to the POS System. The POS System may have acceptance rules relating to CVM, specific to location, environment, and possibly payment system. In this case, the 'N/A' indicates that the kernel has no preference and that these rules should be applied as applicable.

Requirements – CVM Processing

8.2.1.2 **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 terminal shall examine the first CVM in the *CVM List*.
- **A. If** the terminal supports the CVM,
then the Reader shall save the matching CVM and return the CVM recorded in the Final Outcome.

Else:

- **If** the Condition Code of the CVM is 'If terminal supports the CVM',
and another CVM is present in the *CVM List*,
then the terminal shall repeat this requirement from point "A", using the next CVM in the *CVM List*.
 - **If** no mutually supported CVM is shared by the card and the Reader,
then:
 - **If** another interface is supported,
then the transaction terminates with a request that the transaction be attempted using another interface (contact chip, mag-stripe swiped transaction, etc.).
Else the transaction is approved/declined based on the *IACs/TACs*.
-

Requirements – CVM Processing

8.2.1.3 **If** the *Reader CVM Required Limit Exceeded* indicator is set,
and either of the following is true:

- The card does not support Cardholder Verification (Card *AIP* Byte 1 Bit 5 is set to 0b),
- **or** the *CVM List* is not present or is empty.

Then:

- The Reader shall set the CVM to 'N/A' 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.

(In this case the POS System will determine the appropriate CVM and other transaction processing according to any acceptance rules relating to CVM, specific to location, environment, and payment system.)

Requirements – Online PIN

8.2.1.4 **If** Online PIN is to be performed,
then the terminal shall request a PIN and set *TVR* Byte 3 Bit 3, 'Online PIN entered'.

8.2.2 ***Reader CVM Required Limit Exceeded Indicator Not Set***

Card does not support Cardholder Verification or CVM List not present

If the *Reader CVM Required Limit Exceeded* indicator is not set and if the card does not support Cardholder Verification or has no *CVM List*, then the Reader shall set the CVM to 'No CVM required' and use this when returning a Final Outcome.

Requirements – CVM Processing

8.2.2.1 **If** the *Reader CVM Required Limit Exceeded* indicator is not set, **and** any of the following is true:

- The card *AIP* Byte 1 Bit 5 is 0b ('Cardholder verification not supported'),
- **or** no *CVM List* is present,
- **or** the *CVM List* is empty.

Then the Reader sets the CVM to 'No CVM required' 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.

Card supports Cardholder Verification

- If the card supports Cardholder Verification and the card contains a *CVM List* with the CVM of 'No CVM required' supported for the transaction, then the Reader shall set the CVM to 'No CVM required' and use this to set the CVM parameter when returning a Final Outcome.
- Otherwise if the card does not support 'No CVM required' for this transaction, then the Reader will determine if any mutually supported Cardholder Verification Method is supported and use the identified CVM to set the CVM parameter when returning a Final Outcome. If no mutually supported CVM is identified, then the Reader will return a request to the terminal to use another interface if present.

Requirements – CVM Processing – Card Supports Cardholder Verification

8.2.2.2 If the *Reader CVM Required Limit Exceeded* indicator is not set, **and** the card *AIP* Byte 1 Bit 5 is 1b ('Cardholder verification supported'),
then:

- If the card's *CVM List* indicates that 'No CVM required' is supported,
then the Reader sets the CVM to 'No CVM required' 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.

Else:

- The Reader creates a list of Supported CVM 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.
- The terminal shall examine the first CVM in the *CVM List*.
- **A. If** the terminal supports the CVM,
then the Reader shall save the matching CVM and return the CVM recorded in the Final Outcome.

Else:

- If the Condition Code of the CVM is 'If terminal supports the CVM',
and another CVM is present in the *CVM List*,
then the terminal shall repeat this requirement from point "A", using the next CVM in the *CVM List*.
- If no mutually supported CVM is shared by the card and the Reader,
then:

Requirements – CVM Processing – Card Supports Cardholder Verification

- **If** another interface is supported,
then the transaction terminates with a request that the transaction be attempted using another interface (contact chip, mag-stripe swiped transaction, etc.).
Else the transaction is approved/declined based on the *IACs/TACs*.
-

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 4.2 Book 3], section 10.6, and [EMV 4.2 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

- 9.1.1.1 If a test card with *AIP* Byte 1 Bit 4 = 0b (Terminal Risk Management) is presented,
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 Chapter 10, 1st Terminal Action Analysis.)

9.2 Processing Requirements

Terminal Risk Management must be performed as defined in [EMV 4.2 Book 3], section 10.6, and [EMV 4.2 Book 4], section 6.3.5.

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

- 9.2.1.1 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'.
-

Readers are not required to support random transaction selection processing for contactless.

9.2.2 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 terminal⁹. 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

- 9.2.2.1 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'.
-

⁹ 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 4.2 Book 3], section 10.7, and [EMV 4.2 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 4.2 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. The review of the offline processing results, in the *TVR*, is performed against the *IACs* and the *TACs*. 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. Offline only terminals have a separate set of *TAC* values than online terminals

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

• <i>IAC – Denial</i> • <i>TAC – Denial</i>	Defines conditions that determine whether a transaction should be declined offline
• <i>IAC – Online</i> • <i>TAC – Online</i>	Defines conditions that determine whether a transaction should be transmitted online for authorisation
• <i>IAC – Default</i> • <i>TAC – Default</i>	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 Reader must compare the *IAC – Denial* and *TAC – Denial* with the results of the current transaction as recorded in the *TVR*¹⁰, and 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.
- Set the *Authorisation Response Code (ARC)* to value 'Z1' indicating 'Offline declined'. Refer to section 10.2.4, Request AC in First GENERATE AC.

¹⁰ If the terminal is performing optimised transaction processing, then Offline Data Authentication has not yet been performed, and all *TVR* settings related to offline data authentication will be set to 0b.

Requirements – Terminal Action Analysis

10.2.1.1 During Terminal Action Analysis the 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 any corresponding bits are set,
then the terminal shall request an AAC at first GENERATE AC stage and shall set the response code to ‘Z1’ – ‘Offline declined’.

Else (no corresponding bits are set):

- The terminal shall approve the transaction.
- **If** the terminal is offline capable,
then the terminal shall set the response code to ‘Y1’ – ‘Offline approved’.

The subsequent processing is determined by the capability of the Reader to go online:

- If the Reader has the capability to connect online for authorisation, then the Reader must compare the *IAC – Online* and *TAC – Online* 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 transmitted online for authorisation and the Reader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.

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

Requirements – Terminal Action Analysis

10.2.1.2 **If** the terminal is online capable
then during Terminal Action Analysis:

- The 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*.
 - **If** any corresponding bits are set,
then the terminal shall request an *ARQC* at first GENERATE AC stage.
-

- If the Reader has the capability to connect online for authorisation, but none of the corresponding bits in the Online and Decline Action Codes are set, then 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*.
 - Set the *ARC* to value 'Y1' indicating 'Offline approved'.

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

Requirements – Terminal Action Analysis

10.2.1.3 **If** the terminal is online capable,
then during Terminal Action Analysis:

- The 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* and also the *Terminal Action Code – Denial* and the *Issuer Action Code – Denial* read from the card with the results as recorded by the *TVR*.
- **If** none of the corresponding bits are set,
then the terminal shall request a *TC* at first GENERATE AC stage.

-
- If the Reader is not online capable, then the Reader must compare the *IAC – Default* and *TAC – Default* 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*.
- Set the *ARC* to value 'Z3' indicating 'Unable to go online, offline declined'.

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

Requirements – Terminal Action Analysis

10.2.1.4 **If** the terminal is not online capable,
then during Terminal Action Analysis:

- The 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.
- **If** any of the corresponding bits are set,
then the terminal shall request an AAC with ARC 'Z3' at first GENERATE AC stage.

-
- If none of the above checks result in the transaction being declined or sent online for authorisation, then 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.
 - Set the ARC to value 'Y3' indicating 'Unable to go online, offline approved'.

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

Requirements – Terminal Action Analysis

10.2.1.5 **If** the terminal is online capable but unable to complete an online connection,
then during Terminal Action Analysis:

- The 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.
- **If** none of the corresponding bits are set,
then the terminal shall request a TC with ARC 'Y3' at first GENERATE AC stage.

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, 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 1, then the Reader must set the cryptogram type to be requested in the GENERATE AC command to *ARQC*.

Requirements – Zero Amount Allowed

10.2.2.1 **If** the Reader supports Zero Amount Allowed,
and the Zero Amount indicator is set to 1 during Entry Point processing,
then the Reader shall request an *ARQC* at first GENERATE AC stage.

10.2.2.2 **If** the Reader supports Zero Amount Allowed,
and the Zero Amount indicator is set to 0 during Entry Point processing,
then the Reader shall determine which cryptogram to request based on the normal Terminal Action Analysis process.

Requirements – Status Check Requested

10.2.2.3 **If** the Reader supports Status Check,
and the Status Check Requested indicator is set to 1 during Entry Point processing,
then the Reader shall request an *ARQC* at first GENERATE AC stage.

10.2.2.4 **If** the Reader supports Status Check,
and the Status Check Requested indicator is set to 0 during Entry Point processing,
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.
$$\text{RNM} := \text{UN}_{\text{EMV}} \bmod (\text{Unpredictable Number Range} + 1)$$
- 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

- 10.2.3.1 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 4.2 Book 3], section 5.4.

Requirements – GENERATE AC Data Construction

- 10.2.3.2 In the GENERATE AC command, the terminal shall send to the card the data elements that the card requested in the CDOL.
-

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 4.2 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.
- 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 4.2 Book 3], section 10.8.

Table 10-1: Terminal Verification Results Settings

Meaning	Byte	Bits
Offline Data Authentication was not performed	1	8
Offline Static Data Authentication Failed		7
Card Data Missing		6
Card appears on Terminal Exception File		5
RFU		4
Combined DDA/AC Generation (CDA) Failed		3
RFU		2 to 1
Card and terminal have different application versions	2	8
Expired application		7
Application not effective yet		6
Requested service not allowed for Card product		5
New Card		4
RFU		3 to 1
Cardholder Verification failed	3	8
Unrecognised CVM		7
RFU		6
RFU		5
RFU		4
Online PIN entered		3
RFU		2 to 1
Transaction exceeds floor limit	4	8
Lower consecutive offline limit exceeded		7
Upper consecutive offline limit exceeded		6
Transaction selected randomly for online processing		5
Merchant forced transaction online		4
RFU		3 to 1
Default TDOL used	5	8
Issuer Authentication was unsuccessful		7
RFU		6 to 1

11 1st Card Action Analysis

11.1 Overview

The purpose of Card Action Analysis is to allow the card to perform a number of pre-defined 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 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 4.2 Book 2], section 6.6.

11.2.1 General Card Action Analysis

Requirements – Card Action Analysis Processing

11.2.1.1 **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, 'CDA failed'.

11.2.1.2 **If** the terminal requests CDA with TC at first GENERATE AC,
then the terminal shall validate the signature.

11.2.1.3 **If** the terminal requests CDA with ARQC at first GENERATE AC,
then the terminal shall validate the signature and extract the ARQC.

11.2.1.4 **If** the terminal supports optimisation,
and the terminal requests an ARQC from an optimised card supporting CDA,
then CDA is performed on the first GENERATE AC.

11.2.1.5 **If** the terminal requests a TC with ARC 'Y3' (Unable to go online, offline approved) on second GENERATE AC,
then the terminal shall perform ODA.

11.2.1.6 **If** the terminal requests an ARQC for a Delayed Authorisation,
then the terminal shall perform ODA.

11.2.2 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 (i.e. if optimised processing is supported or CDA required) refer to Chapter 12, Offline Data Authentication (Optimised Processing).

Requirements – Card Action Analysis Return *TC*

11.2.2.1 If the transaction is approved offline,
then the terminal shall request a *TC* at first GENERATE AC and
successful ODA is required.

- If *TVR* Byte 1 Bit 3 is set to 1b, 'CDA Failed', then the Reader continues with section 18.3, Transaction Completion – Transaction Declined; else the Reader continues with section 18.2, Transaction Completion – Transaction Approved.

11.2.3 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 section 18.3, Transaction Completion – Transaction Declined.

Requirements – Card Action Analysis Return AAC

11.2.3.1 **If** the transaction is declined offline,
then the terminal shall request an AAC at first GENERATE AC.

11.2.4 Card Returns an ARQC

If the card returns an ARQC in the response to the first GENERATE AC command, then processing continues as follows:

- If the transaction is being processed in EMV mode:
 - If the Reader is not capable of processing a Full Online EMV contactless transaction (see section 2.2), then continue with section 11.2.4.1.
 - If the Reader is capable of processing a Full Online EMV contactless transaction (see section 2.2), then continue with section 11.2.4.2.
- For contactless mag-stripe mode transactions, continue with section 11.2.4.3.

11.2.4.1 Partial Online Transaction EMV Mode

The processing described in this section is performed if the transaction is being processed in EMV mode and the Reader is not capable of processing a Full Online EMV contactless transaction:

- If the Reader is online capable and is also capable of performing contact EMV transactions, then a request for the cardholder to use the contact EMV interface is initiated as follows:¹¹ The kernel returns control to Entry Point, passing a Final Outcome of **Try Another Interface** with the following parameter settings:

¹¹ The expected usage scenario is that a card performing a transaction in EMV mode is a dual interface card. Alternative acceptance procedures at the POS for any alternative form factors operating in EMV mode would be handled locally.

Start	N/A
Online Response Data	N/A
CVM	N/A
UI Request on Outcome Present	Yes • Message Identifier: '18' ("Please insert/swipe 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

- If the card returns an *ARQC* with signature, then Offline Data Authentication shall be performed if necessary (see Chapter 12).

If Offline Data Authentication fails, then the transaction shall be declined (see section 18.3, Transaction Completion – Transaction Declined), else processing continues as follows:

- 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

- If the Reader is online capable and is only capable of performing contactless transactions, then the Reader attempts to send the EMV contactless transaction online as follows: The kernel returns control to Entry Point, passing a Final Outcome of **Online Request** with the following parameter settings:

Start	D
Online Response Data	Any
CVM	As determined in section 8.2, Cardholder Verification – Processing Requirements
UI Request on Outcome Present	Yes • Message Identifier: '1B' ("Authorising, Please Wait") • State: Processing • Hold Time: 0 • Language Preference
UI Request on Restart Present	Yes • Message Identifier: '16' ("Processing") • State: Processing • Hold Time: 0 • Language Preference
Data Record Present	Yes
Discretionary Data Present	No
Alternate Interface Preference	N/A
Receipt	N/A
Field Off Request	N/A
Removal Timeout	Zero

After Entry Point restarts the kernel at Start D, processing continues as described in section 13.2.3, Contactless EMV Mode – Partial Online.

- If the terminal is offline only, then the transaction shall be declined.

Requirements – Card Action Analysis Return ARQC – Partial Online

11.2.4.1 **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.

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

- The terminal is a dual-interface terminal only capable of Partial Online.
- The terminal sends the first GENERATE AC to a dual-interface card.
- The terminal receives an ARQC with CDA which passes.

Then the terminal shall direct the user to insert the card into the contact reader.

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

- The terminal is a contactless interface terminal only capable of Partial Online.
- The terminal sends the first GENERATE AC to a card.
- The terminal receives an ARQC with CDA which passes.

Then the terminal shall perform an online transaction.

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

- The terminal is a contactless interface offline terminal.
- The terminal sends the first GENERATE AC to a card.
- The terminal receives an ARQC with CDA which passes.

Then the terminal shall decline the transaction.

11.2.4.2 Full Online Transaction EMV Mode

The processing described in this section is performed if the transaction is being processed in EMV mode and the Reader is capable of processing a Full Online EMV contactless transaction.

- If an ARQC was returned by the card, then Offline Data Authentication shall be performed if necessary (see Chapter 12).
 - If Offline Data Authentication fails, then the transaction shall be processed as described in section 15, 2nd Terminal Action Analysis.
 - If Offline Data Authentication succeeds, then the Reader attempts to send the transaction online as follows: The kernel returns control to Entry Point, passing a Final Outcome of **Online Request** with the following parameter settings:

Start	D
Online Response Data	Any
CVM	As determined in section 8.2, Cardholder Verification – Processing Requirements
UI Request on Outcome Present	Yes • Message Identifier: '1B' ("Authorising, Please Wait") • State: Processing • Hold Time: 0 • Language Preference
UI Request on Restart Present	Yes • Message Identifier: '16' ("Processing") • Status: Processing • Hold Time: 0 • Language Preference
Data Record Present	Yes
Discretionary Data Present	No
Alternate Interface Preference	N/A
Receipt	N/A
Field Off Request	N/A
Removal Timeout	Set according to the Removal Timeout Kernel Configuration Parameter.

Requirements – Card Action Analysis Return *ARQC* – Full Online

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

- The terminal is capable of performing a Full Online EMV contactless transaction.
- The terminal sends the first GENERATE AC to a card.
- The terminal receives an *ARQC*.
- ODA (if performed) passes.

Then the terminal shall perform the Full Online transaction. (See Chapter 13.)

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

- The terminal is capable of performing a Full Online EMV contactless transaction.
- The terminal receives an *ARQC*.
- The online connection does not complete.

Then the terminal shall send the second GENERATE AC to the card.

11.2.4.3 Mag-Stripe Mode Transactions

The processing in this section is performed for 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
- Offline data authentication shall be performed if necessary (see Chapter 12).
- If TVR Byte 1 Bit 3 is set to 1b, 'CDA Failed', or TVR Byte 1 Bit 7 is set to 1b, 'SDA Failed', then the transaction will be declined and processing continues with section 18.3, Transaction Completion – Transaction Declined.
- Else if the Reader is online capable, then the Reader attempts to send the mag-stripe contactless transaction online as follows: The kernel returns control to Entry Point, passing a Final Outcome of **Online Request** 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: '1B' ("Authorising, Please Wait") • State: 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

- Else if the Reader is only capable of performing Offline transactions, then the transaction shall be declined.

Requirements – Card Action Analysis Return ARQC – Mag-Stripe Mode

11.2.4.7 If all of the following are true:

- The terminal is online capable.
- The terminal receives an *ARQC* from a card.
- The mode is set to mag-stripe (by the card or terminal).
- ODA passes.

Then the terminal shall send the transaction online. (See Chapter 13.)

11.2.4.8 If all of the following are true:

- The terminal is online capable.
- The terminal receives an *ARQC* from a card.
- The mode is set to mag-stripe (by the card or terminal).
- The online connection cannot be completed.

Then the terminal shall decline the transaction.

11.2.4.9 If all of the following are true:

- An offline terminal receives an *ARQC* from a card.
- The mode is set to mag-stripe (by the card or terminal).

Then the terminal shall decline the transaction.

11.2.5 Format of the Response to GENERATE AC Command

The Reader must check that the format of the response data is compliant to Format 1 as defined by [EMV 4.2 Book 3], section 6.5.5.4, or Format 2 or Format 1 as appropriate if CDA is used (see [EMV 4.2 Book 2], section 6.6).

If the response is in the incorrect format, then 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 – Card Action Analysis Return Formats

11.2.5.1 **If** CDA is not used,
then:

- The terminal shall check that the GENERATE AC response is in Format 1.
- **If** the response is not in Format 1,
then the kernel returns control to Entry Point with a Final Outcome of ***End Application***.

11.2.5.2 **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** the response is not in Format 1 or 2 or is in the incorrect format,
then the kernel returns control to Entry Point with a Final Outcome of ***End Application***.
-

12 Offline Data Authentication (Optimised Processing)

12.1 Overview

If the Reader is using the optimised transaction process and the result of 1st Card Action Analysis is that the transaction is to be approved offline (*TC* returned to the GENERATE AC command) and additionally in the case of CDA when an *ARQC* has been requested by the Reader, then Offline Data Authentication is performed.

(If the Reader is not using the optimised transaction process, see section 6, Offline Data Authentication (Unoptimised Processing) for more details on how Offline Data Authentication is performed.)

If the transaction is declined offline (*AAC* returned) Offline Data Authentication is not performed.

Requirements – Optimised Offline Data Authentication

12.1.1.1 If the transaction is declined offline (*AAC* returned),
then Offline Data Authentication is not performed.

The two types of Offline Data Authentication are Combined Dynamic Data Authentication/*Application Cryptogram* (CDA) and Static Data Authentication (SDA). Offline Data Authentication must be performed as described in [EMV 4.2 Book 2], sections 5 and 6.

The CDA signature is generated over a *TC* when a *TC* is requested and returned and over an *ARQC* when an *ARQC* is requested and returned, as illustrated in the following summary.

Reader Requests	Card Generates One of the Following
CDA + <i>TC</i>	<i>TC</i> with signature
	<i>ARQC</i> with signature
	<i>AAC</i> (no signature)
CDA + <i>ARQC</i>	<i>ARQC</i> with signature
	<i>AAC</i> (no signature)

12.2 Processing Requirements

Offline Data Authentication must be performed as described in [EMV 4.2 Book 2], sections 5 and 6, and [EMV 4.2 Book 3], section 10.3.

For optimised cards, the records associated with Offline Data Authentication are located only in *SFI* 2, 3, or 4 (see section 4.3.3 for more information). This allows an optimised Reader to read only the appropriate records when it has determined that it is performing Offline Data Authentication.

Readers supporting optimised transaction processing shall process optimised and unoptimised cards according to the processing rules described in Table 4-6.

If the card does not contain an *SFI* 2, then the card has not been optimised and the Reader will read the Offline Data Authentication records as detailed in Chapter 3, Processing Overview, Chapter 5, Read Application Data, and Chapter 6, Offline Data Authentication (Unoptimised Processing).

Requirements – Optimised Offline Data Authentication Processing

- 12.2.1.1 **If** the terminal supports Optimised Processing,
but the card does not contain *SFI* 2,
then the card has not been optimised and processing is as per an unoptimised terminal.
-

Table 12-1 outlines scenarios in support of optimised Offline Data Authentication.

Table 12-1: Offline Data Authentication

Reader Supports Only Offline Transactions (Reader must perform Offline Data Authentication on all transactions)	
SDA Optimised Processing	SDA shall be performed after 1st Card Action Analysis and the Reader must indicate that the card can be removed from the Reader operating field as soon as the records have been read. If SDA fails, the Reader must decline the transaction (see <i>TACs</i>, Annex C) and continue with section 18.3, Transaction Completion – Transaction Declined. SDA is not required if the card returned an Offline decline response.
CDA Optimised Processing	The Reader must include the request for the CDA signature in the first GENERATE AC command. Upon receipt of the signature, the Reader reads the records associated with CDA and indicates the card can be removed from the Reader operating field. The Reader then completes CDA processing. If CDA fails, the Reader must decline the transaction (see <i>TACs</i>, Annex C) and continue with section 18.3, Transaction Completion – Transaction Declined. CDA is not required if the card returned an Offline decline response, since the CDA signature cannot be generated over an AAC.

Reader Supports Only Online Transactions (Offline Data Authentication is conditional as described in this table)	
SDA Optimised Processing	If SDA is the chosen ODA method, if the terminal is capable of performing Full Online contactless transactions, and if the terminal has determined that it is unable to go online, then SDA must be performed. In the case that CDA or SDA is required to be performed, then Offline Data Authentication data should be read from the assigned records on the card as defined in section 4.3.3. Otherwise Offline Data Authentication data need not be read from the assigned records on the card
CDA Optimised Processing	If card and Reader support CDA and a Signature is returned with the ARQC in the response to the first GENERATE AC command, then CDA is performed. In the case that CDA or SDA is required to be performed, then Offline Data Authentication data should be read from the assigned records on the card as defined in section 4.3.3. Otherwise Offline Data Authentication data need not be read from the assigned records on the card
Reader Supports Delayed Authorisation Transactions (Reader must perform Offline Data Authentication on all transactions)	
SDA Optimised Processing	SDA shall be performed after 1st Card Action Analysis and the Reader must indicate that the card can be removed from the Reader operating field as soon as the records have been read. The Reader must not indicate the transaction is approved until after SDA has completed. If SDA fails, the Reader must decline the transaction (see TACs, Annex C) and continue with section 18.3, Transaction Completion – Transaction Declined. SDA is not required if the card returned an Offline decline response.
CDA Optimised Processing	CDA shall be performed in all transactions and the Reader must request the CDA signature with the first GENERATE AC command. Upon receipt of the signature, the Reader will read the CDA records and indicate the card can be removed from the Reader operating field. The Reader must not indicate the transaction is approved until after CDA has completed. If CDA fails, the Reader must decline the transaction (see TACs, Annex C) and continue with section 18.3, Transaction Completion – Transaction Declined. CDA is not required if the transaction is declined.

Reader Supports Online and Offline Transactions (Reader must support Offline Data Authentication)	
SDA Optimised Processing	The terminal will determine whether or not to perform SDA based on the card's response to 1st Card Action Analysis. • If a card responds with an Offline decline, then SDA is not performed and the terminal is not required to read the associated records. • If the card responds with an Offline approval, the terminal must perform SDA. The terminal must indicate the card can be removed from the terminal operating field as soon as the records have been read. If SDA fails, the terminal must decline the transaction. (See <i>TACs</i>, Annex C.) • If a card responds with a need to go Online, then the following processing should be followed: • If the transaction is being processed in EMV mode and the terminal is capable of processing a Full Online EMV transaction and each of the following conditions are true: • the reader is unable to go online • the card is still present in the field • the removal timer has not expired Then the Reader is required to read the associated records and perform SDA before the second GENERATE AC command. <i>TVR</i> Byte 1 Bit 7 should be updated accordingly with the results of SDA (Successful or Failed). The default <i>TAC/IAC</i> should be checked and the transaction approved/declined accordingly. If the transaction is being processed in mag-stripe mode or in a terminal that can only process Partial Online transactions, then SDA is not performed and the terminal is not required to read the associated records.

Reader Supports Online and Offline Transactions (Reader must support Offline Data Authentication)	
CDA Optimised Processing	The terminal will determine whether or not to perform CDA based on the card's response to 1st Card Action Analysis. However, in the following cases, the terminal must include a request for the CDA signature as part of the first GENERATE AC command: • when the terminal requests an Offline approval • when the transaction is in EMV mode and being performed in a terminal which supports Full Online EMV contactless transactions • If the card responds with an Offline approval, it will include the CDA signature and the terminal must perform CDA. The terminal must indicate that the card can be removed from the terminal operating field as soon as the records have been read. If CDA fails, the terminal must decline the transaction. (See <i>TACs</i>, Annex C.) • If the card responds with a need to go Online and includes a CDA Signature (for example when the terminal has requested a <i>TC</i> with CDA but the card requests that the transaction be sent Online), then the terminal must perform CDA. The terminal must indicate the card can be removed from the terminal operating field as soon as the records have been read.¹² If CDA fails, the terminal must decline the transaction. • If the card responds with a need to go Online and includes a CDA Signature for a transaction being performed in EMV mode at a terminal capable of Full Online EMV processing and if the terminal is unable to go online, then the terminal must update <i>TVR</i> Byte 1 Bit 3 with the results of CDA before the second GENERATE AC command. If CDA fails, the terminal must decline the transaction. • If the card responds with a need to go Online but without a signature being requested or returned, then CDA is not performed. Therefore, the terminal is not required to read the associated records.

¹² With the exception of Full Online EMV transactions, in which case the card removal prompt is controlled by the removal timer and associated processing as described in Chapter 13.

Reader Supports Online and Offline Transactions (Reader must support Offline Data Authentication)	
	• If the card responds with an Offline Decline, then it will not return a signature and CDA is not performed. Therefore, the terminal is not required to read the associated records.

13 Online Processing

13.1 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. Online Processing, as defined in [EMV 4.2 Book 3], section 10.9, and [EMV 4.2 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

13.1.1.1 **If** the terminal requests online authorisation,
then the terminal shall attempt to send the transaction online for authorization.

13.1.1.2 **If** the card requests online authorisation,
then the terminal shall attempt to send the transaction online for authorization.

13.2 Processing Requirements

13.2.1 Contactless Mag-Stripe Mode (Partial Online Only)

The response data field in Format 1 or Format 2 must be parsed as specified in [EMV 4.2 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)*

13.2.1.1 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

13.2.1.1 If the transaction involves a mag-stripe card,
then:

- The terminal shall compare the *ATC* returned by the GET DATA command to the *ATC* returned in the GENERATE AC command.
 - If the *ATCs* do not match,
then the terminal shall decline the transaction.
-

13.2.1.2 AC Check

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

Requirements – Online Processing Mag-Stripe AC Check

- 13.2.1.2 **If** the transaction involves a mag-stripe card,
then:
- The terminal shall validate the *AC* returned.
 - **If** the *AC* is not a *TC* or *ARQC*,
then the terminal shall decline the transaction.

13.2.1.3 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 Mag-Stripe AC Check

- 13.2.1.3 **If** the transaction involves a contactless mag-stripe mode card,
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 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.

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 prior to populating the applicable Track 1 or Track 2 field. The resulting full five digits¹³ 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.

¹³ In earlier versions of the Kernel 4 specification, only the three lower order digits of the ATC were placed into Track 1 and Track 2 data for transmission in the online message. In this version of the specification, this has been increased to enable the full five digits of the ATC to be sent.

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 13-1: Track 2 Equivalent Data

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

The Reader shall generate pseudo magnetic stripe Track 1 and Track 2 data as specified in Table 13-2 and Table 13-3. The constructed track data is made available to the Reader for online authorisation and standard payment processing.

Table 13-2: 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	4 bytes
	Cryptogram	5 bytes
	End Sentinel	1 byte

Table 13-3: 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	4 bytes
	Cryptogram	5 bytes
	ATC	5 bytes
	End Sentinel	1 byte

13.2.2 Contactless Mag-Stripe Mode

At this stage in the transaction the Outcome parameters as set in section 11.2.4.3 are returned to Entry Point and the authorisation request is subsequently transmitted to the Acquirer for online authorisation. The terminal determines the transaction disposition based on the online response indication, as defined in Book A.

13.2.3 Contactless EMV Mode – Partial Online

At this stage in the transaction the cardholder is prompted to remove the card from the Reader and the Reader shall format a User Interface Request Message to send the 'Remove card' prompt. The Outcome parameters as set in section 11.2.4.1 are returned to Entry Point and the authorisation request is subsequently transmitted to the Acquirer for online authorisation.

On return from the Online Authorisation Request, Kernel 4 is Restarted as a result of Entry Point Start D, and processing continues as follows:

- If the Reader receives the *Transaction Disposition* indicating an authorisation APPROVAL response from the Issuer, then the response must be stored and the Reader must continue with section 18.2, Transaction Completion – Transaction Approved.
- If the Reader receives the *Transaction Disposition* indicating an authorisation DECLINE response from the Issuer, then the response must be stored and the Reader must continue with section 18.3, Transaction Completion – Transaction Declined.
- If the Reader was unable to connect to the Acquirer for online authorisation (offline device or communications failure), resulting in the 'Unable to Go Online' flag being set to 1b, then the Reader must accept or reject the transaction by checking the *TAC – Default* and *IAC – Default* and, depending on the results, must continue with either section 18.2, Transaction Completion – Transaction Approved or section 18.3, Transaction Completion – Transaction Declined.

Requirements – Online Processing Partial EMV Online Fail

13.2.3.1 **If** an EMV transaction requires Partial Online authorisation,
and the transaction fails to complete Partial Online authorisation,
then the terminal shall process the transaction according to the
TAC – Default and *IAC – Default*.

13.2.4 Contactless EMV Mode – Full Online

At this stage in the transaction the Outcome parameters as set in section 11.2.4.2 are returned to Entry Point and the authorisation request is subsequently transmitted to the Acquirer for online authorisation.

On return from the Online Authorisation Request, Kernel 4 is Restarted as a result of Entry Point Start D, and processing continues as follows:

- If the Card Removal Timer has not expired:

If the Timeout Indicator is false (0) and the card is still in the operating field of the Reader, then, when the Reader Kernel 4 restarts from Entry Point Start D, the Reader must continue processing according to the following rules:

- **The Reader received an authorisation response from the Issuer and (EMV) card response data is returned.** On receipt of the card data the Reader must pass the *Issuer Authentication Data* received from the Acquirer to the card in the EXTERNAL AUTHENTICATE command as part of Issuer Authentication. (See section 14, Issuer Authentication.)

Requirements – Online Processing Full EMV Online

13.2.4.1 **If** the terminal receives an authorisation response from the Issuer,
and EMV card data has been returned,
then the Reader shall send the Issuer Authentication Data to the card in the EXTERNAL AUTHENTICATE command.

- **The Reader received an authorisation response but no card response data is returned from the Acquirer.** On receipt of the card data, a magnetic stripe or 'downgraded' response (indicating they had not connected to the Issuer), the Reader must derive the *ARC* based on the *Transaction Disposition* data received from the Acquirer as described in Chapter 16, 2nd Card Action Analysis. The *ARC* is passed to the card in the second GENERATE AC command and the Reader continues with Transaction Completion without performing Issuer Authentication.

Requirements – Online Processing Full EMV Online

13.2.4.2 **If the terminal receives an authorisation response, and card issuer response data has not been returned, then the terminal shall derive the *ARC* from the acquirer data which is passed in the second GENERATE AC command with no prior EXTERNAL AUTHENTICATE.**

- **The Reader is unable to connect to the Acquirer for online authorisation (offline device or communications failure).** If the 'Unable to Go Online' flag is set, then the Reader must continue with 2nd Terminal Action Analysis as detailed in section 15.2 without performing Issuer Authentication. The decision process for acceptance or rejection of the transaction is determined by checking the *IAC & TAC – Default*.

If the card has been removed from the operating field of the Reader by the cardholder and there is no response to either the EXTERNAL AUTHENTICATE or second GENERATE AC command, then the Reader shall alert the User of the error via a User Interface Request Message:

- The Reader shall send a User Interface Request Message with the following parameters set:
 - **Message Identifier:** '0F' ("Processing error")
 - **Status:** Processing Error
 - **Hold Time:** 20
- The kernel returns control to Entry Point, passing a Final Outcome of **End Application** with the following parameter settings:

Start	N/A
Online Response Data	N/A
CVM	N/A
UI Request on Outcome Present	Yes • Message Identifier: '21' ("Present Card Again") • 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 – Online Processing Full EMV Online

13.2.4.3 If there is no response from the card to the EXTERNAL AUTHENTICATE or the second GENERATE AC command, **then** the Reader shall advise the user of the error via a User Interface Request Message and shall ask the user to present their card again.

- If the Card Removal Timer has Expired:

If the Timeout Indicator is true (1), then when Kernel 4 is restarted from Entry Point Start D, the Reader must process the data returned as a result of the restart according to the following rules:

- If the Reader receives the *Transaction Disposition* indicating an authorisation APPROVAL response, then the response must be stored and the Reader must continue with section 18.2, Transaction Completion – Transaction Approved.
- If the Reader receives the *Transaction Disposition* indicating an authorisation DECLINE response, then the response must be stored and the Reader must continue with section 18.3, Transaction Completion – Transaction Declined.

If the Reader was unable to connect to the Acquirer for online authorisation (offline device or communications failure), and the 'Unable to Go Online' flag is set to 1b, then the Reader must accept or reject the transaction by checking the *TAC – Default* and *IAC – Default* and, depending on the results, continue with either section 18.2, Transaction Completion – Transaction Approved or section 18.3, Transaction Completion – Transaction Declined.

14 Issuer Authentication

Issuer Authentication is performed only in a Full Online EMV mode transaction.

14.1 Overview

In markets that support EMV enabled network messages the authorisation response message for an EMV mode contactless transaction may contain *Issuer Authentication Data*.

For Readers supporting Full Online EMV mode and if Online Processing concludes with Entry Point Start D for Kernel 4 restart and *Issuer Authentication Data* is present and the card is still present in the operating field, the *Issuer Authentication Data* must be forwarded to the card. The card will validate whether the response came from the valid Issuer. This validation is called 'Issuer Authentication'. If Online Processing does not conclude with the Reader receiving *Issuer Authentication Data*, the Reader continues to 2nd Terminal Action Analysis.

Requirements – Issuer Authentication

- 14.1.1.1 **If** the authorisation response contains Issuer Authentication Data (i.e. including an *ARPC*),
and the card remains in the field,
then the terminal shall send an EXTERNAL AUTHENTICATE to the card.
-

14.2 Processing Requirements

Issuer Authentication allows the card to verify that the response message received from an online authorisation request is from the genuine Issuer of the card. Issuer Authentication is performed by the Reader passing *Issuer Authentication Data*, received in the Card Authorisation Response Message from the Issuer, to the card in an EXTERNAL AUTHENTICATE command.

EXTERNAL AUTHENTICATE is performed as described in [EMV 4.2 Book 3], section 6.5.4.

15 2nd Terminal Action Analysis

2nd Terminal Action Analysis is performed only in a Full Online EMV mode transaction.

15.1 Overview

This function is described in [EMV 4.2 Book 1] through [EMV 4.2 Book 4]. There are three distinct cases:

- **Online (*Issuer Authentication Data* received from Issuer):** If the Issuer returns *Issuer Authentication Data* (comprising an *Authorisation Response Cryptogram (ARPC)* and *Authorisation Response Code (ARC)*, Tag '8A') as part of the authorisation response, then the Reader requests a second GENERATE AC using the *ARC* to determine whether to request that the card approve or decline the transaction. *ARC* values of '00', '08', '10', or '11' indicate that the Issuer approved the transaction; any other values returned in the *ARC* should be processed by the Reader as a request to decline the transaction. (Note that *ARC* values are formatted as ASCII – e.g. '00' is represented as '3030'.)

Requirements – Terminal Action Analysis

15.1.1.1 If the authorisation response contains *Issuer Authentication Data* (comprised of the *ARPC* and *ARC*),
then:

- The terminal shall send an EXTERNAL AUTHENTICATE followed by the second GENERATE AC command using the *ARC* provided in the authorisation response.
 - **If** the *ARC* value is '00', '08', '10', or '11',
then the terminal requests *TC*;
else the terminal requests *AAC*.
-

- **Online (*Issuer Authentication Data* not received from Issuer):** If the Reader does not receive any *Issuer Authentication Data* in the response, then the Reader must use the disposition of the transaction indicated in the response message from the Acquirer to determine whether to request the card to approve or decline the transaction. For the purposes of setting the *ARC* for the second *GENERATE AC* when requested in *CDOL2*, values of '00' should be used to indicate an Approval and '05' when the disposition from the Acquirer indicates a request to decline the transaction. (Note that *ARC* values are formatted as ASCII – e.g. '00' is represented as '3030'.)

Requirements – Terminal Action Analysis

15.1.1.2 **If** the authorisation response does not contain an *Authorisation Response Cryptogram (ARPC)*,
then:

- The terminal shall not send an *EXTERNAL AUTHENTICATE*.
- The terminal shall send a second *GENERATE AC* command using the *ARC* provided in the authorisation response.
 - **If** the acquirer approved the transaction,
then the terminal requests *TC*,
else it requests *AAC*.

-
- **Unable to go Online:** If the Reader was unable to go online, resulting in the 'Unable to Go Online' flag being set to 1b, then the Reader examines the *Terminal Action Codes* resident in the Reader and the *IACs* read from the card to determine whether to request offline approval or offline decline from the card.

Requirements – Terminal Action Analysis

15.1.1.3 **If** the terminal attempted to send the transaction online,
and the transaction cannot complete online,
then:

- The terminal shall check the *Terminal Action Code – Default* and *Issuer Action Code – Default* to determine whether to accept or reject the transaction.
 - **If** the transaction is accepted,
then the terminal requests *TC* with *ARC* 'Y3'.
 - **If** the transaction is declined,
then the terminal requests *AAC* with *ARC* 'Z3'.
-

2nd Terminal Action Analysis occurs only if:

- The card is still present after online processing, and
 - The transaction was processed online, or
 - The transaction was unable to go online after receiving an *ARQC*, or
 - CDA failed after receiving an *ARQC*.

15.2 Processing Requirements

The Reader looks at the results from Online Processing to determine which cryptogram type (*AAC* or *TC*) to request the card to generate. If the Reader was unable to go online, then it will send an *ARC* set to 'Z3' or 'Y3' to the card as part of the command data in the second *GENERATE AC* command.

If the Reader went online but received a 'downgraded' response from the Issuer or Acquirer (i.e. did not receive the *Issuer Authentication Data*), then the Reader derives the *ARC* based on the transaction disposition in the 'downgraded' response, and issues it to the card in the command data for the second *GENERATE AC* command.

If the Reader went online and *Issuer Authentication Data* was returned by the Issuer, then the *ARC* received in the *Issuer Authentication Data* is sent to the card in the command data (as defined in CDOL2) for the second *GENERATE AC* command.

An *AC* is requested using the *GENERATE AC* command, as defined in [EMV 4.2 Book 3], section 6.5.5.

15.2.1 CDA

If the *TVR* indicates that CDA failed, and an *ARQC* was received in the first *GENERATE AC* command, then the transaction is declined offline and the Reader requests an *AAC* in the second *GENERATE AC*. The *ARC* must be set to 'Z3'.

Requirements – Terminal Action Analysis Processing

- 15.2.1.1 If CDA is performed and failed,
 then the terminal shall decline the transaction regardless of the
 settings in the *IAC* and *TAC* data elements.
-

The request for the second *GENERATE AC* must not request that CDA be performed.

15.2.2 Advice Messages

When the Reader receives a response to a GENERATE AC command, the response includes the *CID*, a data element that indicates whether the card has requested an advice message be created. Cards compliant with this specification may set bits requesting advice depending on the value assigned to the *Application Default Action* data element.

If the card has indicated in the *CID* that an advice is required, then the Reader decides what action to take, if any. For instance, if the Reader is required to transmit a data capture record or a reversal message for that transaction, then it is not necessary for the Reader to also transmit an advice. If the Reader is required to transmit an advice, then the Reader shall determine whether to transmit an offline or online advice based upon its capabilities and any local market requirements. Advices are not required to be supported unless stipulated by local market conditions.

Requirements – Terminal Action Analysis Advices

- 15.2.2.1 **If** the card sets the 'Advice required' bit in the CID in the response data,
then the terminal shall not reject the transaction.
-

16 2nd Card Action Analysis

2nd Card Action Analysis is performed only in a Full Online EMV mode transaction.

16.1 Overview

As a result of 2nd Terminal Action Analysis, the card shall receive a second GENERATE AC command, requesting either that the transaction be declined (AAC) or approved (TC).

16.2 Processing Requirements

The Reader is not involved in the 2nd Card Action Analysis; however 2nd Card Action Analysis is triggered by the Reader issuing the card a GENERATE AC command requesting either a TC or AAC, depending on the results of 2nd Terminal Action Analysis, and the Reader is informed of the result of this process in the response data returned by the card:

- 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
- If the response from the card returned a TC, then the transaction is approved and processing should continue from section 18.2, Transaction Completion – Transaction Approved.
- If the response from the card returned an AAC, then the transaction is declined and processing should continue from section 18.3, Transaction Completion – Transaction Declined.

Requirements – Card Action Analysis AAC

16.2.1.1 If the card returns an AAC in response to the second GENERATE AC command,
then the terminal shall decline the transaction.

17 Issuer Script Processing

17.1 Overview

Only Readers that are capable of processing a Full Online EMV transaction are required to support Issuer Script Processing.

It is mandatory that any Issuer Scripts received be processed as described in [EMV 4.2 Book 3], sections 6 and 10.10, and [EMV 4.2 Book 4], section 6.3.9.

17.2 Processing Requirements

Issuer Script Processing allows the card Issuer to transmit a command to the contactless card in an authorisation response message only when a transaction is being performed in EMV mode and in a Reader capable of Full Online EMV transaction processing. This command, or set of commands, must be forwarded to the contactless card at the correct time.

A Reader compliant with this specification must support Issuer Scripts labelled with either Tag '72' or Tag '71'.

The Reader shall submit Issuer Scripts with Tag '71' to the card for processing prior to issuing the final GENERATE AC command. Issuer Scripts with Tag '72' shall be submitted after issuing the final GENERATE AC command.

Issuer Scripts will contain only commands to be executed by the card. The only processing requirement of the Reader is to extract the command or commands from the script or scripts in the order they are received in the authorisation response message and to pass them to the card to be processed, then to check and report the results returned from the card.

Requirements – Issuer Scripts

- 17.2.1.1 **If** the Reader is capable of Full Online EMV transaction processing, **and** an Issuer Script with Tag '71' or Tag '72' is present in the Online Response Data forwarded from the terminal, **then** the Reader shall extract the Issuer Script Commands and forward them to the card as described in EMV.
-

18 Transaction Completion

18.1 Overview

When either the transaction was approved or declined offline or once the card has responded to the final GENERATE AC command (and returned any Records Read for optimised processing after first GENERATE AC), the card's role in the transaction is complete. The Reader will then complete with one of the Final Outcomes indicated below.

18.2 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

18.3 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

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 on page 135 lists transaction data.
- Section A.3 on page 136 lists the minimum data elements required for an EMV mode data record and for a mag-stripe mode data record.

A.1 Data Elements

Table A-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	Authorized 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.
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.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
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	A mandatory data object made available to the Reader via the READ RECORD command.
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.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
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 4.2 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.	

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 mandatory 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 <i>[ISO 8583]</i> .	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 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 64		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 64		A mandatory data object made available to the Reader via the READ RECORD command.
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.	An optional data object made available to the Reader via the READ RECORD command.
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		A mandatory data object made available to the Reader via the READ RECORD command.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
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 specifications	—	Per payment system specific actions	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
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	
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
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 mandatory 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 mandatory 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 mandatory 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.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
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		
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 4.2 Book 2], section 6.1, Keys and Certificates.	
Kernel 4 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 <i>Terminal Type</i> , 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 <i>Terminal Type</i> , Tag '9F35' when Tag '9F35' is present in the PDOL of the card
Offline Capability	Offline capable terminals are capable of performing offline contactless transactions.	Terminal	Implementation specific	—	Implementation specific		

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
Online Capability (Partial or Full)	Terminals that are Online Capable must be capable of performing Partial Online contactless transactions. Online capable terminals may optionally provide support for a Full Online contactless transaction.	Terminal	Implementation specific	—	Implementation specific		
Optimised ODA Support	Indicates support for Optimised processing during SDA or CDA as described in this specification.	Terminal	Implementation specific	—	Implementation specific		
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.		
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	—	—	—	

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
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.
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 4.2 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		
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.

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
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 4.2 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 4.2].	
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

Name	Description	Source	Format	Tag	Length	Values	Location/Usage
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 Chapter 13 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 Chapter 13 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 <i>/ISO 7813</i>	Mandatory data element available via READ RECORD command 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 <i>/ISO 4217</i>	
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 <i>/ISO 8583:1987</i> 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 A-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
Card Risk Management Data Object List 2 (CDOL2)	M	'8D'	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 Data Records

The following tables list the minimum data elements required for authorisation and Clearing and Settlement: Table A-3 lists data elements for EMV mode and Table A-4 lists those for mag-stripe mode. For further information regarding these elements, please refer to the Payment Scheme Network Specifications.

Table A-3: Data Record for EMV Mode (Minimum Data Elements)

Data Object	Presence	Auth Message	Clearing Message
Amount, Authorised	M	M	M
Amount, Other	M	M	M
Application Cryptogram	M	M	M
Application Interchange Profile (AIP)	M	M	M
Application PAN Sequence Number	M	M	M
Application Transaction Counter (ATC)	M	M	M
Cryptogram Information Data	M	M	M
Issuer Application Data	M	M	M
Point of Service Data Code ¹⁴	M	M	M
Terminal Country Code	M	M	M
Terminal Verification Results (TVR)	M	M	M
Track 2 Data	M	M	—
Transaction Currency Code	M	M	M
Transaction Date	M	M	M
Transaction Type	M	M	M
Unpredictable Number	M	M	M

¹⁴ May be constructed using Tag '9F33' *Terminal Capabilities* and other terminal parameters and transaction characteristics as necessary.

Table A-4: Data Record for Mag-Stripe Mode (Minimum Data Elements)

Data Object	Presence	Auth Message	Clearing Message
Point of Service Data Code ¹⁵	M	M	M
Track 1 Data ¹⁶	C	C	—
Track 2 Data ¹⁷	C ¹⁸	C	—

¹⁵ May be constructed using Tag '9F33' *Terminal Capabilities* and other terminal parameters and transaction characteristics as necessary.

¹⁶ Sourced from Tag '57' *Track 2 Equivalent Data* and other chip data elements as described in section 13.2.

¹⁷ Sourced from Tag '57' *Track 2 Equivalent Data*.

¹⁸ 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 13.2.

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 B-1 and Table B-2 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 B-1: Kernel Configuration Data (EMV acceptance environment)

Name	Tag	Description
Alternate Interface Support	—	Indicates whether the terminal supports an alternate interface to the contactless interface (e.g. Contact Chip).
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.
Delayed Authorisations Supported	—	Defines whether the terminal is configured to perform delayed authorisations.
Kernel 4 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.
Offline Capability	—	Offline capable terminals are capable of performing offline contactless transactions.

Name	Tag	Description
Online Capability (Partial or Full)	—	Terminals that are Full Online Capable: - Must be capable of performing both Partial Online contactless transactions and Full Online EMV transactions. - Must be able to be configured to perform only Partial Online transactions.
Optimised ODA Support	—	Indicates whether the terminal supports optimisation for Offline Data Authentication.
Removal Timeout (in 100ms increments)	—	Terminals that support Full Online must support a Timer in order to determine whether the contactless transaction should take place as a Full Online or Partial Online transaction.
Terminal Action Codes	—	A set of <i>Terminal Action Codes</i> (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 B-2: Kernel Configuration Data (Mag-Stripe Terminal)

Name	Tag	Description
Alternate Interface Support	—	Indicates whether the terminal supports an alternate interface to the contactless interface (e.g. Contact Chip).
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.
Delayed Authorisations Supported	—	Defines whether the terminal is configured to perform delayed authorisations.
Kernel 4 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.
Online Capability (Partial)	—	Mag-stripe only terminals must be capable of supporting Partial Online functionality
Terminal Action Codes	—	A set of <i>Terminal Action Codes</i> (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 B-3: Entry Point Configuration Data

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

Annex C Terminal Action Codes

Table C-1 shows the mandated values for *Terminal Action Codes* for Kernel 4. Section C.1 explains the meaning of the bits that are set.

Table C-1: Terminal Action Codes

	TAC	Byte 1	Bytes 2–5
Terminals with Offline Only capability	<i>TAC – Denial</i>	'DC 50 84 00 00'	All set to zero
	<i>TAC – Online</i>	Not applicable	
	<i>TAC – Default</i>	'DC 50 84 00 00'	
All other terminals	<i>TAC – Denial</i>	'C4 00 00 00 00'	
	<i>TAC – Online</i>	'C4 00 00 00 00'	
	<i>TAC – Default</i>	'C4 00 00 00 00'	

C.1 TAC Values for Terminals with Offline Only Capability

For terminals with Offline Only capability:

- *TAC – Online* does not apply.
- *TAC – Denial* is set to 'DC 50 84 00 00', as explained in Table C-2.
- *TAC – Default* is set to 'DC 50 84 00 00', as explained in Table C-2.

Table C-2: Offline Only Terminals: TAC – Denial and TAC – Default

Meaning	Byte	Bits
Offline Data Authentication was not performed	1	8
Offline Static Data Authentication failed		7
Card appears on Terminal Exception File		5
Offline Dynamic Data Authentication failed		4
Combined DDA/AC Generation failed		3
Expired application	2	7
Requested service not allowed for card product		5
Cardholder Verification was not successful	3	8
Online PIN entered		3

C.2 TAC Values for Other Terminals

For terminals other than those with Offline Only capability, all three *TAC* values are set to 'C4 00 00 00 00', as explained in Table C-3.

Table C-3: TAC Values for Terminals Other Than Offline Only

Meaning	Byte	Bits
Offline Data Authentication was not performed	1	8
Offline Static Data Authentication failed		7
Combined DDA/AC Generation failed		3

Annex D 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 <i>[EMV 4.2 Book 4]</i> Annex B						
APDU	Application Protocol Data Unit						
Application Cryptogram	Cryptogram returned by the card; one of the following cryptogram types: <table data-bbox="646 1444 1247 1575"> <tr> <td>TC</td><td>Transaction Certificate</td></tr> <tr> <td>ARQC</td><td>Authorisation Request Cryptogram</td></tr> <tr> <td>AAC</td><td>Application Authentication Cryptogram</td></tr> </table>	TC	Transaction Certificate	ARQC	Authorisation Request Cryptogram	AAC	Application Authentication Cryptogram
TC	Transaction Certificate						
ARQC	Authorisation Request Cryptogram						
AAC	Application Authentication Cryptogram						
Approved	A Final Outcome						
AUC	Authorization Response Code						
ARPC	Authorization Response Cryptogram						

ARQC	Authorization 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
<i>Declined</i>	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 <i>EMV Integrated Circuit Card Specifications for Payment Systems</i> are developed and maintained by EMVCo.

EMVCo	EMVCo LLC is the organization of payment systems that manages, maintains, and enhances the EMV specifications. EMVCo is currently operated by American Express, JCB, MasterCard, and Visa.
<i>End Application</i>	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 For more information, see section 1.5.
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
<i>Online Request</i>	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
<i>Select Next</i>	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
<i>Try Again</i>	An Outcome
<i>Try Another Interface</i>	A Final Outcome
TVR	Terminal Verification Results
UI	User Interface
UN	Unpredictable Number