EMV '96
Integrated Circuit Card Terminal Specification for Payment Systems

Version 3.0
June 30, 1996

Table of Contents

Tables

Figures

THIS PAGE LEFT INTENTIONALLY BLANK

1. Scope

The *Integrated Circuit Card Terminal Specification for Payment Systems* defines the mandatory, recommended, and optional terminal requirements necessary to support the acceptance of integrated circuit cards (ICCs) in accordance with the *Integrated Circuit Card Specification for Payment Systems* and the *Integrated Circuit Card Application Specification for Payment Systems*. Application-specific terminal requirements unique to individual payment systems and those functions not required to support interchange are not covered in this specification.

This specification applies to all terminals operating in attended or unattended environments, having offline or online capabilities, and supporting transaction types such as purchase of goods, services, and cash. Terminals include but are not limited to automated teller machines (ATMs), branch terminals, cardholder-activated terminals, electronic cash registers, personal computers, and point of service (POS) terminals.

In particular, this specification addresses:

- Functional requirements, such as those emerging from the *Integrated Circuit Card Specification for Payment Systems* and the *Integrated Circuit Card Application Specification for Payment Systems*
- General physical characteristics
- Software architecture including software and data management
- Security requirements
- Cardholder interface
- Acquirer interface

This specification provides the requirements necessary to support the implementation of ICCs. These requirements are in addition to those already defined by individual payment systems and acquirers for terminals that accept magnetic stripe cards. ICC and magnetic stripe acceptance capability may co-exist in the same terminal.

This specification assumes familiarity with the *Integrated Circuit Card Specification for Payment Systems* and the *Integrated Circuit Card Application Specification for Payment Systems*. It is intended for use by payment system members, terminal manufacturers, and designers of applications using ICCs.

Adherence to the mandatory requirements, which are denoted by 'shall', ensures that terminals are compliant with the *Integrated Circuit Card Specification for Payment Systems* and the *Integrated Circuit Card Application Specification for Payment Systems* as well as with this specification. The recommended requirements are denoted by 'should' and the optional requirements by 'may'.

It is recognised that different terminal implementations exist depending on business environment and intended usage. This specification defines requirements for those features and functions that are applicable according to the particular operating environment of the terminal.

This specification does not address cardholder or merchant operating procedures, which are established by individual payment systems.

This specification does not provide sufficient detail to be used as a specification for terminal procurement.

Individual payment systems and acquirers will define complementary requirements applicable to different situations which will provide more detailed specifications applicable to terminal implementations.

2. Normative References

The following standards contain provisions that are referenced in this specification:

Europay, MasterCard, and Visa (EMV):June 30, 1996	Integrated Circuit Card Application Specification for Payment Systems
Europay, MasterCard, and Visa (EMV):June 30, 1996	Integrated Circuit Card Specification for Payment Systems
FIPS Pub 180-1:1995	Secure Hash Standard
ISO 3166:1993	Codes for the representation of names of countries
ISO 4217:1990	Codes for the representation of currencies and funds
ISO 4909:1987	Bank cards - Magnetic stripe data contents for track 3
ISO/IEC 7816-5:1994	Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers
ISO 8583:1987	Bank card originated messages - Interchange message specifications - Content for financial transactions
ISO 8583:1993	Financial transaction card originated messages - Interchange message specifications
ISO 8859:1987	Information processing - 8-bit single-byte coded graphic character sets
ISO 9564-1:1991	Banking - PIN management and security - PIN protection principles and techniques
ISO 9564-2:1991	Banking - PIN management and security - Approved algorithms for PIN encipherment
ISO 13491:1995	Banking - Secure cryptographic devices (retail) (Committee Draft)

3. Definitions

The following terms are used in this specification:

Application - The application protocol between the card and the terminal and its related set of data.

Byte - 8 bits.

Card - Payment card as defined by a payment system.

Certification Authority - Trusted third party that establishes a proof that links a public key and other relevant information to its owner.

Command - Message sent by the terminal to the ICC that initiates an action and solicits a response from the ICC.

Cryptogram - Result of a cryptographic operation.

Development System - Hardware and software used to develop terminal programs and applications.

Exclusive-OR - Binary addition with no carry, giving the following values:

0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0

Function - Process accomplished by one or more commands and resultant actions that are used to perform all or part of a transaction.

Integrated Circuit(s) - Electronic component(s) designed to perform processing and/or memory functions.

Integrated Circuit(s) Cards - Card into which one or more integrated circuits are inserted to perform processing and memory functions.

Interface Device - That part of a terminal into which the ICC is inserted, including such mechanical and electrical devices that may be considered part of it.

Kernel - The set of functions required to be present on every terminal implementing a specific interpreter. The kernel contains device drivers, interface routines, security and control functions, and the software for translating from the virtual machine language to the language used by the real machine. In other words, the kernel is the implementation of the virtual machine on a specific real machine.

Key Pad - Arrangement of numeric, command, and, where required, function and/or alphanumeric keys laid out in a specific manner.

Library - A set of high-level software functions with a published interface, providing general support for terminal programs and/or applications.

Magnetic Stripe - Stripe containing magnetically encoded information.

Nibble - The four most significant or least significant bits of a byte.

Payment System - For the purposes of these specifications, Europay International S.A., MasterCard International Incorporated, or Visa International Service Association.

PIN Pad - Arrangement of numeric and command keys to be used for personal identification number (PIN) entry.

Response - Message returned by the ICC to the terminal after the processing of a command message received by the ICC.

Script - A command or string of commands transmitted by the issuer to the terminal for the purpose of being sent serially to the ICC.

Socket - An execution vector defined at a particular point in an application and assigned a unique number for reference.

Terminal - Device used in conjunction with the ICC at the point of transaction to perform a financial transaction. The terminal incorporates the interface device and may also include other components and interfaces such as host communications.

Transaction - An action taken by a terminal at the user's request. For a POS terminal, a transaction might be payment for goods, etc. A transaction selects among one or more applications as part of its processing flow.

Virtual Machine - A theoretical microprocessor architecture that forms the basis for writing application programs in a specific interpreter software implementation.

4. Abbreviations and Notations

The following abbreviations and notations are used in this specification.

AAC	Application Authentication Cryptogram
AAR	Application Authorisation Referral
AC	Application Cryptogram
AID	Application Identifier
an	Alphanumeric
ans	Alphanumeric Special
API	Application Program Interface
ARPC	Authorisation Response Cryptogram
ARQC	Authorisation Request Cryptogram
ATM	Automated Teller Machine
b	Binary
CAD	Card Accepting Device
cn	Compressed Numeric
CPU	Central Processing Unit
CVM	Cardholder Verification Method
HHMMSS	Hours, Minutes, Seconds
IC	Integrated Circuit
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
IFD	Interface Device
I/O	Input/Output
ISO	International Organisation for Standardisation
MMDD	Month, Day

n	Numeric
N_{CA}	Length of Certification Authority Public Key Modulus
PAN	Primary Account Number
PC	Personal Computer
PDOL	Processing Options Data Object List
PIN	Personal Identification Number
POS	Point of Service
pos.	Position
RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
SW1	Status Word 1
SW2	Status Word 2
TC	Transaction Certificate
TDOL	Transaction Certificate Data Object List
var.	Variable
YYMM	Year, Month
YYMMDD	Year, Month, Day

THIS PAGE LEFT INTENTIONALLY BLANK

Part I

General Requirements

1. Terminal Types and Capabilities

1.1 Terminal Types

As described in the scope, this specification addresses a broad spectrum of terminals. For the purpose of this specification, terminals are categorised by the following:

- Environment: Attended or unattended
- Communication: Online or offline
- Operational control: Financial institution, merchant, or cardholder

Within this specification, online reflects online communication to acquirer (or its agent). The acquirer is assumed to be capable of communicating to the issuer (or its agent).

The type of terminal shall be indicated in Terminal Type. The coding of Terminal Type using the three categories is shown in Annex A.

An explanation of attended, unattended, online, offline, and operational control follows:

Attended - An attendant (agent of the merchant or of the acquirer) is present at the point of transaction and participates in the transaction by entering transaction-related data. The transaction occurs 'face to face'.

Unattended - The cardholder conducts the transaction at the point of transaction without the participation of an attendant (agent of the merchant or of the acquirer). The transaction does not occur 'face to face'.

Online only - The transaction can only be completed online in real time, such as transmitting an authorisation message.

Offline with online capability - Depending upon transaction characteristics, the transaction can be completed offline by the terminal or online in real time. It is equivalent to 'online with offline capability'.

Offline only - The transaction can only be completed offline by the terminal.

Operational control - The entity responsible for the operation of the terminal. This does not necessarily equate to the actual owner of the terminal.

1.2 Terminal Capabilities

For the purpose of this specification, terminal capabilities are described in Terminal Capabilities and Additional Terminal Capabilities. The following categories shall be indicated in Terminal Capabilities:

- **Card data input capability** - Indicates all the methods supported by the terminal for entering the information from the card into the terminal.
- **Cardholder Verification Method (CVM) capability** - Indicates all the methods supported by the terminal for verifying the identity of the cardholder at the terminal.
- **Security capability** - Indicates all the methods supported by the terminal for authenticating the card at the terminal and whether or not the terminal has the ability to capture a card.

The following categories shall be indicated in Additional Terminal Capabilities:

- **Transaction type capability** - Indicates all the types of transactions supported by the terminal.
- **Terminal data input capability** - Indicates all the methods supported by the terminal for entering transaction-related data into the terminal.
- **Terminal data output capability** - Indicates the ability of the terminal to print or display messages and the character set code table(s) referencing the part(s) of ISO 8859 supported by the terminal.

The coding of Terminal Capabilities and Additional Terminal Capabilities using these categories is shown in Annex A.

1.3 Terminal Configurations

Terminal capabilities and device components vary depending on the intended usage and physical environment. A limited set of configuration examples follow.

Figure I-1 illustrates an example of an attended terminal where the integrated circuit (IC) interface device (IFD) and PIN pad are integrated but separate from the POS device (such as for an electronic fund transfer terminal or an electronic cash register).

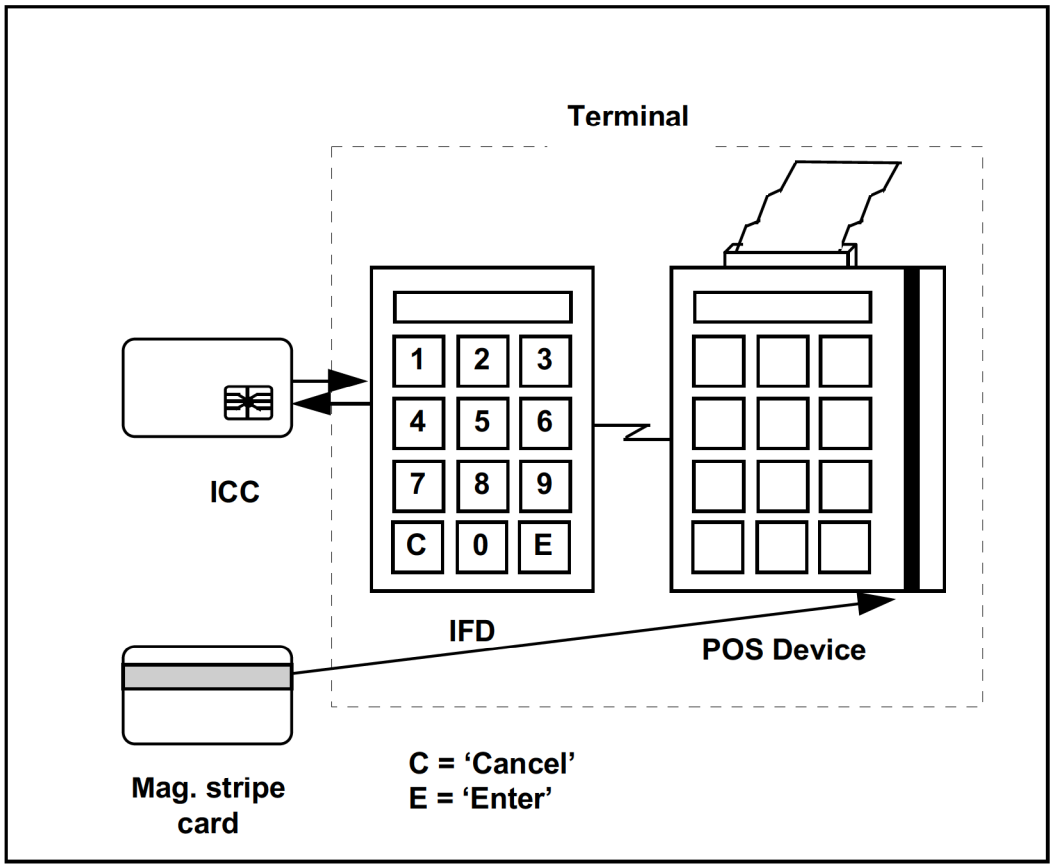

Figure I-1 - Example of an Attended Terminal

Figure I-2 illustrates an example of merchant host concentrating devices, which may be of various types and capabilities.

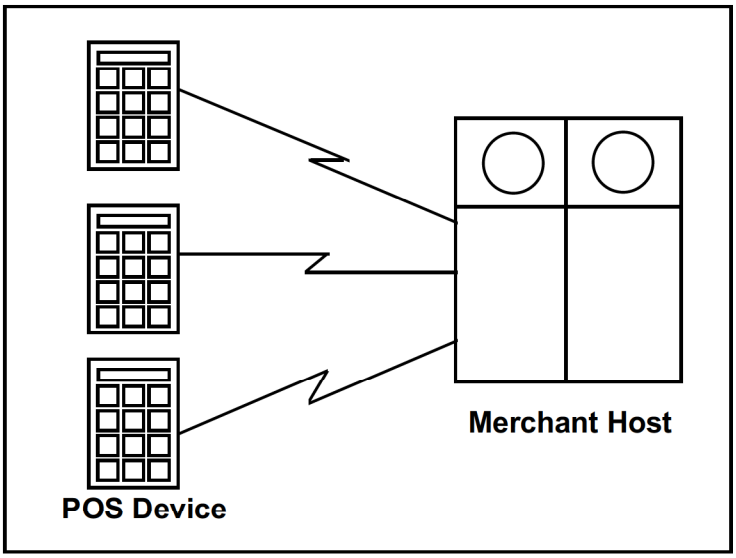

Figure I-2 - Example of a Merchant Host

Within this specification a merchant host to which is connected a cluster of POS devices shall be considered, in its totality, as a 'terminal' regardless of the distribution of functions between the host and POS devices. (See section III-3, of this specification for terminal data management requirements.)

Figure I-3 illustrates an example of a cardholder-controlled terminal that is connected via a public network to a merchant or acquirer host.

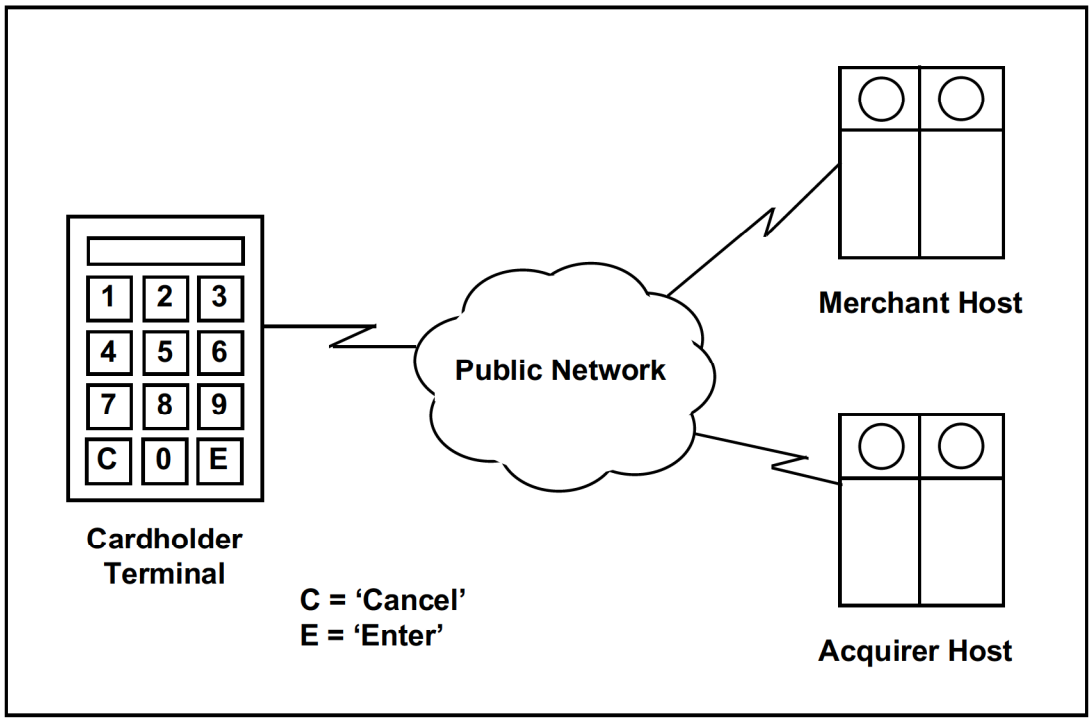

Figure I-3 - Example of a Cardholder-Controlled Terminal

2. Functional Requirements

This specification does not replicate the *Integrated Circuit Card Specification for Payment Systems* and the *Integrated Circuit Card Application Specification for Payment Systems* but describes the implementation issues and the impact of these parts on the terminal.

This section uses standard messages described in section III-1.2, of this specification to illustrate the appropriate message displays for the transaction events described below.

The usage of Authorisation Response Code, CVM Results, and Issuer Script Results is specified in this section. See Annex A for additional information on coding.

2.1 Integrated Circuit Card Specification for Payment Systems

The terminal shall comply with all Parts of the *Integrated Circuit Card Specification for Payment Systems.* It shall support all data elements and commands subject to the conditions described in section I-2.3.

2.2 Integrated Circuit Card Application Specification for Payment Systems

The terminal shall comply with the *Integrated Circuit Card Application Specification for Payment Systems.* It shall support all functions subject to the conditions described in section I-2.3.

Sections 2.2.1 to 2.2.9 expand upon the terminal functions described in the *Integrated Circuit Card Application Specification for Payment Systems.*

2.2.1 Initiate Application Processing

When the Processing Options Data Object List (PDOL) includes an amount field (either Amount, Authorised or Amount, Other), a merchant-controlled terminal (Terminal Type = '2x') shall provide the amount at this point in transaction processing. If the amount is not yet available, the terminal shall obtain the amount and should display the 'Enter Amount' message.

As described in the *Integrated Circuit Card Application Specification for Payment Systems*, if the card returns SW1 SW2 = '6985' in response to the GET PROCESSING OPTIONS command indicating that the transaction cannot be performed with this application, the terminal should display the 'Not Accepted' message and shall return to application selection. The terminal shall not allow that application to be selected again.

2.2.2 Data Authentication

An online-only terminal supporting no form of data authentication as indicated in Terminal Capabilities shall set to '1' the 'Data authentication was not performed' bit in the Terminal Verification Results.

All other terminals shall be capable of performing static data authentication as described in the *Integrated Circuit Card Application Specification for Payment Systems*. They may also be capable of performing dynamic data authentication as described in the *Integrated Circuit Card Application Specification for Payment Systems*.

2.2.3 Processing Restrictions

If the card and terminal Application Version Numbers are different, the terminal shall attempt to continue processing the transaction. If it is unable to continue, the terminal shall abort the transaction and should display the 'Not Accepted' message.

When processing the Application Usage Control, the terminal must know whether or not it is an ATM. See Annex A, Terminal Type, for information on identifying an ATM.

A terminal supporting cashback should not offer cashback facility to the cardholder if the Application Usage Control does not allow this option.

2.2.4 Cardholder Verification Processing

The CVMs supported by the terminal are indicated in Terminal Capabilities. In addition, the terminal shall recognise the CVM codes for 'No CVM required' and 'Fail CVM processing', which may be present in the card's CVM List.

2.2.4.1 Offline CVM

When the applicable CVM is an offline PIN, the terminal should issue a GET DATA command to the card to retrieve the PIN Try Counter prior to issuing the VERIFY command.

If the PIN Try Counter is not retrievable or the GET DATA command is not supported by the ICC, the terminal shall prompt for PIN entry.

If the value of the PIN Try Counter is zero, indicating no remaining PIN tries, the terminal should not allow offline PIN entry. The terminal shall set the 'PIN Try Limit exceeded' bit in the Terminal Verification Results to '1'. The terminal shall not display any specific message regarding PINs, shall not set the CVM Results, and shall continue cardholder verification processing in accordance with the card's CVM List.

If the value of the PIN Try Counter is not zero, indicating remaining PIN tries, the terminal shall prompt for PIN entry such as by displaying the message 'Enter PIN'.

If offline PIN verification by the ICC is successful, the terminal shall set byte 3 of the CVM Results to 'successful'. Otherwise, the terminal shall not set the CVM Results and shall continue cardholder verification processing in accordance with the card's CVM List.

2.2.4.2 Online CVM

When the applicable CVM is an online PIN, the IFD shall not issue a VERIFY command. Instead, the PIN pad shall encipher the PIN upon entry for transmission in the authorisation or financial transaction request.

The terminal shall allow a PIN to be entered for online verification even if the card's PIN Try Limit is exceeded.

The terminal shall set byte 3 of the CVM Results to 'unknown'.

2.2.4.3 PIN Entry Bypass

If a PIN is required for entry as indicated in the card's CVM List, an attended terminal with an operational PIN pad may have the capability to bypass PIN entry before or after several unsuccessful PIN tries.[1] If this occurs, the terminal shall set the 'PIN entry required, PIN pad present, but PIN was not entered' bit in the Terminal Verification Results to '1' and shall not set the 'PIN Try Limit exceeded' bit to '1'. The terminal shall consider this CVM unsuccessful, shall not set the CVM Results, and shall continue cardholder verification processing in accordance with the card's CVM List.

2.2.4.4 Signature (Paper)

When the applicable CVM is signature, the terminal shall set byte 3 of the CVM Results to 'unknown'. At the end of the transaction, the terminal shall print a receipt with a line for cardholder signature. (See Annex A, Terminal Capabilities, for requirements for the terminal to support signature as a CVM.)

2.2.4.5 CVM Results

When the applicable CVM is 'No CVM required', the terminal shall set byte 3 of the CVM Results to 'successful'. When the applicable CVM is 'Fail CVM processing', the terminal shall set byte 3 of the CVM Results to 'failed'.

The terminal shall set bytes 1 and 2 of the CVM Results with the Method Code and Condition Code of the last CVM performed.

If the last CVM performed was not considered successful (byte 3 of the CVM Results is not set to 'successful' or 'unknown'), the terminal shall set byte 3 of the CVM Results to 'failed'.

---

[1] This prevents a genuine cardholder who does not remember the PIN from having to keep entering incorrect PINs until the PIN is blocked in order to continue with the transaction.

If no CVM was performed (no CVM List present or no CVM conditions satisfied), the terminal shall set byte 1 of the CVM Results to 'No CVM performed'.

2.2.5 Terminal Risk Management

In addition to the terminal risk management functions described in the *Integrated Circuit Card Application Specification for Payment Systems* and regardless of the coding of the card's Application Interchange Profile concerning support of terminal risk management, a terminal may support an exception file per application.

When the terminal has an exception file listing cards and associated applications, the terminal shall check the presence of the application selected (identified by data such as the Application Primary Account Number (PAN) and the Application PAN Sequence Number) in the exception file.

If a match is found in the exception file, the terminal shall set the 'Card appears in exception file' bit in the Terminal Verification Results to '1'.

2.2.6 Terminal Action Analysis

As described in the *Integrated Circuit Card Application Specification for Payment Systems*, during terminal action analysis the terminal determines whether the transaction should be approved offline, declined offline, or transmitted online by comparing the Terminal Verification Results with both Terminal Action Code - Denial and Issuer Action Code - Denial, both Terminal Action Code - Online and Issuer Action Code - Online, and both Terminal Action Code - Default and Issuer Action Code - Default.

- If the terminal decides to accept the transaction offline, it shall set the Authorisation Response Code to 'Offline approved'.[2]
- If the terminal decides to decline the transaction offline, it shall set the Authorisation Response Code to 'Offline declined'.
- If the terminal decides to transmit the transaction online, it shall not set a value for the Authorisation Response Code nor change the value for the Authorisation Response Code returned in the response message.

2.2.7 Card Action Analysis

The terminal shall process the transaction as follows as a result of the data returned in Cryptogram Information Data by the card in the response to the GENERATE APPLICATION CRYPTOGRAM (AC) command.

---

[2] This does not mean that the transaction will be approved. The card makes the final decision and returns it to the terminal in its response to the first GENERATE AC command.

- If the card indicates an approval, the terminal should display the 'Approved' message and shall complete the transaction.

- If the card indicates a decline, the terminal should display the 'Declined' message and shall decline the transaction.

- If the card indicates to process online, the terminal shall transmit an authorisation or financial transaction request message, if capable. (See section III-2.2.1, of this specification for exception handling when the terminal is unable to go online.)

- If the card indicates a referral, the terminal shall perform referrals as described in section I-2.4.2.

- When an advice is requested by the card and advices are supported by the terminal:

  – If the transaction is captured, the terminal shall not create an advice message.

  – If the transaction is not captured (such as a decline), the terminal shall either transmit an online advice if online data capture is performed by the acquirer or create an offline advice for batch data capture.

- If the card indicates 'Service not allowed', the terminal should display the 'Not Accepted' message and shall terminate the transaction.

2.2.8 Online Processing

Depending on the Authorisation Response Code returned in the response message, the terminal shall determine whether to accept or decline the transaction. It shall issue the second GENERATE AC command to the ICC indicating its decision.

The result of card risk management performed by the ICC is made known to the terminal through the return of the Cryptogram Information Data indicating either a transaction certificate (TC) for an approval or an application authentication cryptogram (AAC) for a decline.

When online data capture is performed by the acquirer, the terminal shall send a reversal message if the final decision of the card is to decline a transaction for which the Authorisation Response Code is 'Online approved'.

2.2.9 Issuer-to-Card Script Processing

The terminal shall be able to support at least one or more Issuer Scripts in each authorisation or financial transaction response it receives, where the total length of all Issuer Scripts in the response is no greater than 24 bytes except where payment system rules and procedures define the processing of Issuer Script(s) longer than 24 bytes.

The terminal shall be able to recognise the tag for the Issuer Script transmitted in the response message. If the tag is '71', the terminal shall process the script before issuing the second GENERATE AC command. If the tag is '72', the terminal shall process the script after issuing the second GENERATE AC command.

For each Issuer Script processed, the terminal shall report the Script Identifier (when present) with its result in the Issuer Script Results. If an error code was returned by the card for one of the single Script Commands, the terminal shall set the first nibble of byte 1 of the Issuer Script Results to 'Script processing failed' and the second nibble with the sequence number of the Script Command in the order it appears in the Issuer Script. If no error code was returned by the card, the terminal shall set the first nibble of byte 1 of the Issuer Script Results to 'Script processing successful' and the second nibble to '0'.

The terminal shall transmit the Issuer Script Results in the batch data capture message (financial record or offline advice), the financial transaction confirmation message, or the reversal message. If no message is created for the transaction (such as a decline), the terminal shall create an advice to transmit the Issuer Script Results, if terminal supports advices.

2.3 Conditions for Support of Functions

A terminal supporting offline CVM capability shall support the VERIFY command. A terminal not supporting offline CVM capability need not support the VERIFY command.

A terminal supporting dynamic data authentication shall support static data authentication.

An offline-only terminal and an offline terminal with online capability shall support static data authentication.

An online-only terminal need not support dynamic nor static data authentication. Individual payment systems will define rules for this case.

An offline-only terminal and an offline terminal with online capability shall support terminal risk management. An offline-only terminal and an online-only terminal need not support random transaction selection.

An online-only terminal need not support all of the terminal risk management functions. In this case, the acquirer (or its agent) should process the transaction instead of the terminal according to the *Integrated Circuit Card Application Specification for Payment Systems*. In other words, the acquirer should perform the remaining terminal risk management functions. Individual payment systems will define rules for this case.

A financial institution- or merchant-controlled terminal (Terminal Type = '1x' or '2x') shall support the terminal risk management functions described in the *Integrated Circuit Card Application Specification for Payment Systems*. A

cardholder-controlled terminal (Terminal Type = '3x') need not support terminal risk management.

2.4 Other Functional Requirements

2.4.1 Amount Entry and Management

The amount of a transaction shall be indicated to the cardholder preferably by means of a terminal display or labels, such as posted prices on a vending machine, or alternatively by printing on a receipt.

When the amounts are entered through the use of a key pad, the terminal should allow the amount to be displayed during entry. The attendant or cardholder should be able to either correct the amounts entered prior to authorisation and proceed with the transaction or cancel the transaction if the amount was entered incorrectly.

The cardholder should be able to validate the original or corrected amount when the transaction amount is known before authorisation. If PIN entry occurs immediately after the amounts are entered, PIN entry can act as the validation of the amount (see section 4.2 for security requirements). If PIN entry does not occur immediately after the amounts are entered, the terminal should display the '(Amount) OK?' message for the cardholder to validate the amount fields.

If the authorisation takes place before the final transaction amount is known (for example, petrol at fuel dispenser, amount before tip at restaurant), the Amount, Authorised data object represents the estimated transaction amount and the Transaction Amount data object represents the final transaction amount as known at the end of the transaction.

The cardholder may have the ability to separately enter or identify a cashback amount prior to authorisation if the terminal supports cashback and the card's Application Usage Control indicates that cashback is allowed for the transaction. When cashback is allowed, the cashback amount shall be transmitted in the Amount, Other data object. The amounts transmitted in Amount, Authorised and Transaction Amount shall include both the purchase amount and cashback amount (if present).

When passed to the ICC as part of the command data, the Amount, Authorised and Amount, Other shall be expressed with implicit decimal point (for example, '123' represents £1.23 when the currency code is '826').

2.4.2 Voice Referrals

A manual voice referral process may be initiated by the card or by the issuer. Only attended terminals should support voice referral processing.

If a voice referral is indicated and it is not possible to perform such a referral, such as at an unattended terminal, default procedures for handling the transaction will be developed by an individual payment system.[3]

2.4.2.1 Referrals Initiated by Card

If the card responds to the first GENERATE AC by requesting a voice referral (as indicated in the Cryptogram Information Data), an attended terminal shall display the 'Call Your Bank' message to the attendant. Appropriate application data, such as the Application PAN, shall be displayed or printed to the attendant in order to perform the referral. Appropriate messages shall be displayed requesting the attendant to enter data indicating that the transaction has been approved or declined as a result of the referral process. The attendant may manually override the referral process and may accept or decline the transaction without performing a referral, or the attendant may force the transaction online.

As a result of the referral process or override, the terminal shall set the Authorisation Response Code to 'Approved (after card-initiated referral)' if approved or 'Declined (after card-initiated referral)' if not. The terminal shall bypass the issuance of the EXTERNAL AUTHENTICATE command and issue the second GENERATE AC command requesting either a TC for an approval or an AAC for a decline.

If the transaction is forced online (by the terminal or the attendant), the terminal shall not set the Authorisation Response Code and shall transmit an authorisation or financial transaction request message using the Application Authorisation Referral (AAR) as an Authorisation Request Cryptogram (ARQC). The terminal shall continue normal online processing of the transaction (see section 2.2.8).

2.4.2.2 Referrals Initiated by Issuer

When the Authorisation Response Code in the authorisation response message indicates that a voice referral should be performed by the attendant, prior to issuing the second GENERATE AC command, an attended terminal shall display the 'Call Your Bank' message to the attendant. Appropriate application data, such as the Application PAN, shall be displayed or printed to the attendant in order to perform the referral. Appropriate messages shall be displayed requesting the attendant to enter data indicating that the transaction has been approved or declined as a result of the referral process. The attendant may manually override the referral process and may accept or decline the transaction without performing a referral.

The terminal shall not modify the Authorisation Response Code. The terminal shall issue the second GENERATE AC command requesting either a TC for an approval

---

[3] For example, the terminal may decline the transaction or override the referral response by approving the transaction offline or, as in the case where the card initiates the referral, transmit the transaction online.

or an AAC for a decline. If an Authorisation Response Cryptogram (ARPC) is present in the authorisation response message, the terminal may issue the EXTERNAL AUTHENTICATE command either before or after the referral data is manually entered.

2.4.3 Transaction Forced Online

An attended terminal may allow an attendant to force a transaction online, such as in a situation where the attendant is suspicious of the cardholder. If this function is performed, it should occur at the beginning of the transaction. If this occurs, the terminal shall set the 'Merchant forced transaction online' bit in the Terminal Verification Results to '1'. Payment systems rules will determine whether the attendant is allowed to perform such a function.

2.4.4 Transaction Forced Acceptance

An attended terminal may allow an attendant to force acceptance of the transaction, even if the card has returned an AAC indicating that the transaction is to be declined. If this occurs, the transaction shall be captured for clearing as a financial transaction either by sending an online financial advice or within the batch data capture. The terminal shall not modify the Authorisation Response Code and shall set an indicator that the attendant forced acceptance of the transaction in the online advice or batch data capture. Payment systems rules will determine whether the attendant is allowed to perform such a function.

2.4.5 Transaction Sequence Counter

The terminal shall maintain a Transaction Sequence Counter that is incremented by one for each transaction performed by the terminal. The Transaction Sequence Counter may be common to both ICC and non-ICC transactions.

The initial value of this counter is one. When the Transaction Sequence Counter reaches its maximum value, it shall be reset to one. A value of zero is not allowed. (See Annex B for details on this data element.)

The Transaction Sequence Counter may be used for transaction logging or auditing as well as for input to the application cryptogram calculation.

2.4.6 Unpredictable Number

The terminal shall be able to generate an Unpredictable Number, which may be used for input to the application cryptogram algorithm to ensure the unpredictability of data input to this calculation or for random transaction selection for terminal risk management. An unpredictable number shall be generated in accordance with an individual payment system's specifications.