EMV2000
Integrated Circuit Card
Specifications for Payment Systems

Book 4

Cardholder, Attendant, and Acquirer Interface Requirements

Version 4.0
December, 2000

These Materials and all of the content contained herein are provided "AS IS" "WHERE IS" and "WITH ALL FAULTS" and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these materials. EMVCO MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE MATERIALS AND INFORMATION CONTAINED HEREIN. EMVCO SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE.

EMVCo makes no representation or warranty with respect to intellectual property rights of any third parties in or in relation to the Materials. EMVCo undertakes no responsibility of any kind to determine whether any particular physical implementation of any part of these Materials may violate, infringe, or otherwise use the patents, copyrights, trademarks, trade secrets, know-how, and/or other intellectual property rights of third parties, and thus any person who implements any part of these Materials should consult an intellectual property attorney before any such implementation. WITHOUT LIMITATION, EMVCO SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO INTELLECTUAL PROPERTY SUBSISTING IN OR RELATING TO THESE MATERIALS OR ANY PART THEREOF, INCLUDING BUT NOT LIMITED TO ANY AND ALL IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT OR SUITABILITY FOR ANY PURPOSE (WHETHER OR NOT EMVCO HAS BEEN ADVISED, HAS REASON TO KNOW, OR IS OTHERWISE IN FACT AWARE OF ANY INFORMATION).

Without limitiation to the foregoing, the Materials provide for the use of public key encryption technology, which is the subject matter of patents in several countries. Any party seeking to implement these Materials is solely responsible for determining whether their activities require a license to any technology including, but not limited to, patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights.

Table of Contents

Part I - General requirements

Part II - Software Architecture

Part III - Cardholder, Attendant and Acquirer Interface

Annexes

Table of Figures

Table of Tables

THIS PAGE LEFT INTENTIONALLY BLANK

1. Scope

The *Cardholder, Attendant, and Acquirer Interface Requirements 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 *Application Independent ICC to Terminal Interface Requirements* (Book 1), the *Security and Key Management* (Book 2) and the *Application Specification* (Book 3). 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 *Application Independent ICC to Terminal Interface Requirements, Security and Key Management* and the *Application Specification*

- General physical characteristics

- Software architecture including software and data management

- 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 *Application Independent ICC to Terminal Interface Requirements, Security and Key Management* and the *Application Specification*. 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 *Application Independent ICC to Terminal Interface Requirements, Security and Key Management* and the *Application Specification* 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:

EMV2000 Version 4.0: December 2000	Integrated Circuit Card Specifications for Payment Systems: Book 1 - Application Independent ICC to Terminal Interface Requirements
EMV2000 Version 4.0: December 2000	Integrated Circuit Card Specifications for Payment Systems: Book 2 - Security and Key Management
EMV2000 Version 4.0: December 2000	Integrated Circuit Card Specifications for Payment Systems: Book 3 - Application Specification
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 technology - 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 algorithm(s) for PIN encipherment

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.

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, Notations and Terminology

The following abbreviations and notations are used in this specification.

AAC	Application Authentication Cryptogram
AAR	Application Authorisation Referral
AC	Application Cryptogram
AID	Application Identifier
API	Application Program Interface
ARQC	Authorisation Request Cryptogram
ATM	Automated Teller Machine
CAD	Card Accepting Device
CPU	Central Processing Unit
CVM	Cardholder Verification Method
DDOL	Dynamic Data Authentication Data Object List
EN	European Norm
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
NF	Norme Française
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
UL	Underwriters Laboratories Incorporated
YYMM	Year, Month
YYMMDD	Year, Month, Day

The following terminology is used:

proprietary	Not defined in and/or outside the scope of this specification
shall	Denotes a mandatory requirement
should	Denotes a recommendation

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 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).

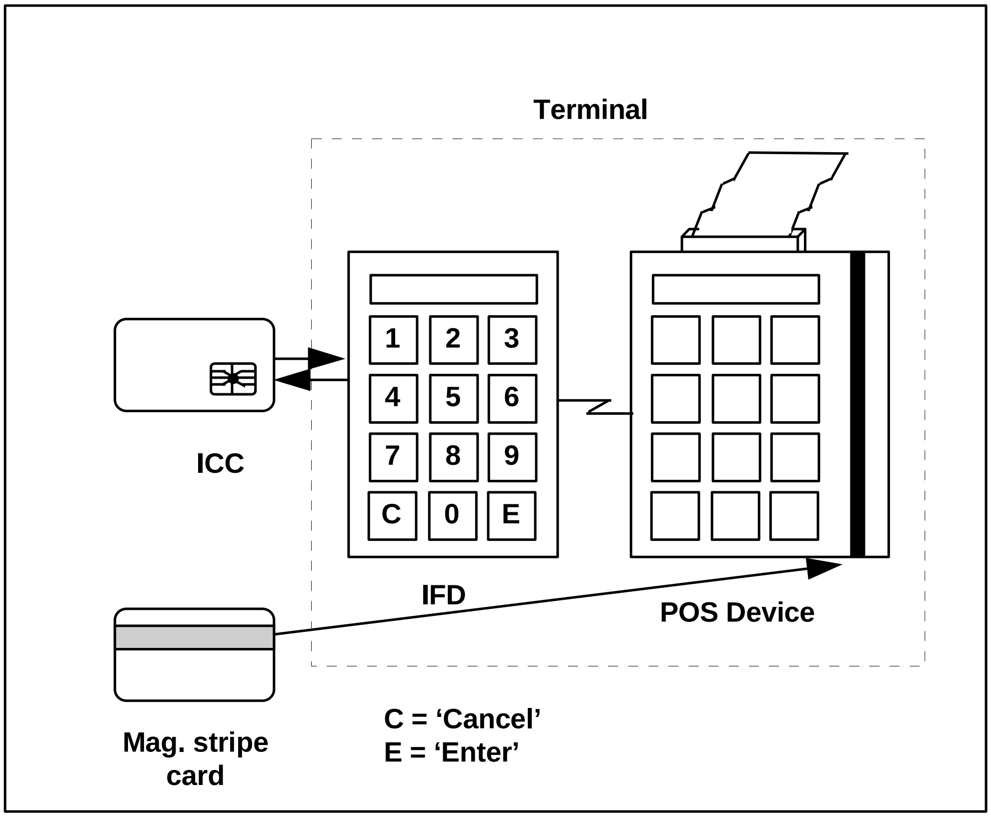

Figure 1 - Example of an Attended Terminal

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

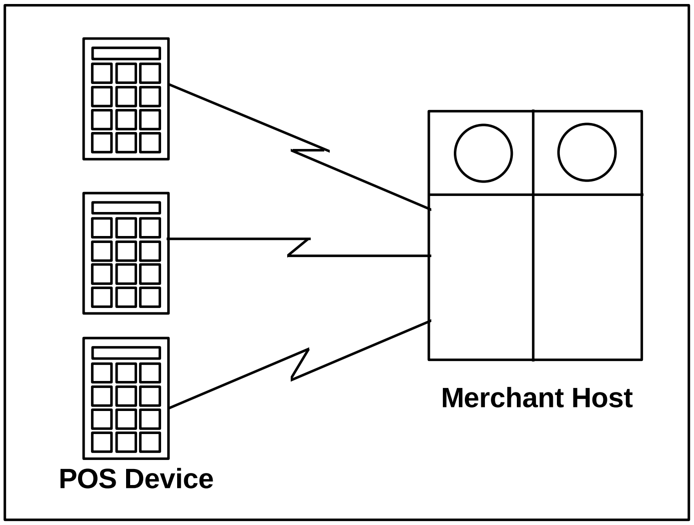

Figure 2 - Example of a Merchant Host

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 6, of this specification for terminal data management requirements.)

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

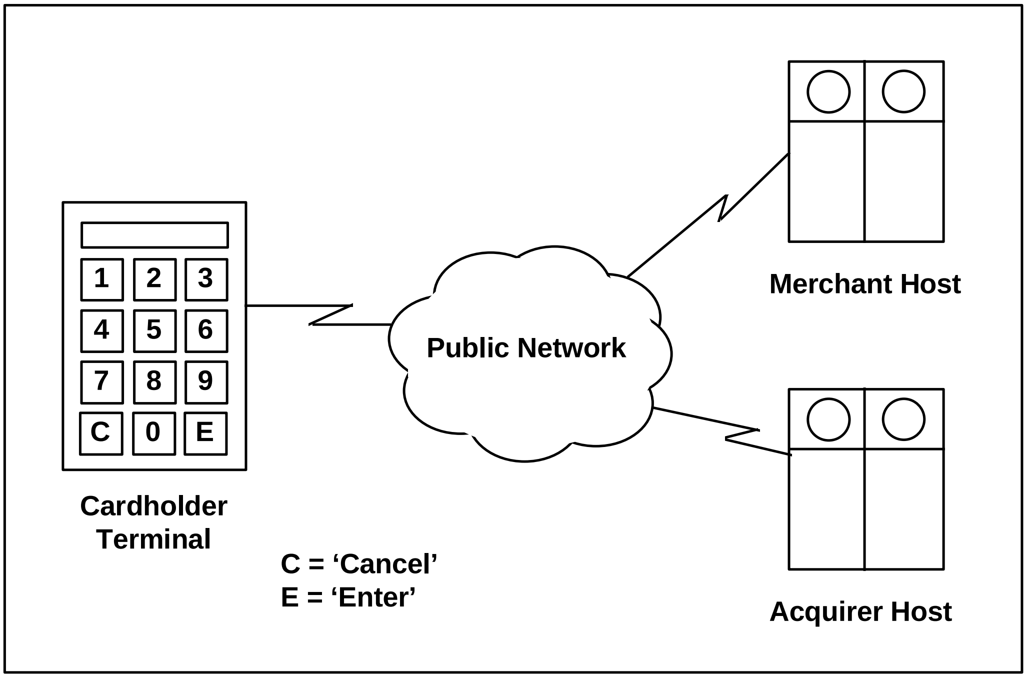

Figure 3 - Example of a Cardholder-Controlled Terminal

2. Functional Requirements

This specification does not replicate Book 1 *Application Independent ICC to Terminal Interface Requirements*, Book 2 *Security and Key Management* and Book 3 *Application Specification* but describes the implementation issues and the impact of these parts on the terminal.

This section uses standard messages described in section 7.2, 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 Application Independent ICC to Terminal Interface Requirements

The terminal shall comply with all Parts of the *Application Independent ICC to Terminal Interface Requirements.* It shall support all data elements and commands subject to the conditions described in section 2.3.

2.2 Security and Key Management

The terminal shall comply with all Parts of the *Security and Key Management* (Book 2). It shall support all data elements and commands subject to the conditions described in section 2.3.

2.3 Application Specification

The terminal shall comply with Book 3,the *Application Specification*. It shall support all functions subject to the conditions described in section 2.3.

Sections 2.3.1 to 2.3.9 expand upon the terminal functions described in the *Application Specification.*

2.3.1 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.

2.3.2 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 Book 3 *Application Specification*. They may also be capable of performing dynamic data authentication as described in Book 3 *Application Specification*.

2.3.3 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.

2.3.4 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.

2.3.4.1 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 either the VERIFY command or GET CHALLENGE 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.

2.3.4.2 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'.

2.3.4.3 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.

2.3.4.4 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.)

2.3.4.5 CVM Results

When the applicable CVM is 'No CVM required', if the terminal supports 'No CVM required' it 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'.

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'.

[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.

2.3.5 Terminal Risk Management

In addition to the terminal risk management functions described in Book 3 *Application Specification* 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'.

2.3.6 Terminal Action Analysis

As described in Book 3 *Application Specification* 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.

2.3.7 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.

- 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.

[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 to process online, the terminal shall transmit an authorisation or financial transaction request message, if capable. (See section 8.2.1, 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 2.5.2.

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

– 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.

- If Combined DDA/AC generation failed as shown in section 6.6.2 of Book 2 *Security and Key Management*, the terminal shall set the Combined DDA/AC Generation Failed bit in the TVR to '1'. Subsequently:

  – If the card has return a TC as indicated in the CID bit, the terminal shall decline the transaction.

  – If the card has return an ARQC as indicated in the CID bit, the terminal shall complete the transaction processing by performing immediately a second Generate_AC requesting for an AAC.

2.3.8 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'.

2.3.9 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 shall be less than or equal to 128 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.

2.4 Conditions for Support of Functions

A terminal supporting offline PIN verification shall support the VERIFY command. A terminal supporting offline PIN encipherment shall also support the GET CHALLENGE command. A terminal not supporting offline PIN verification 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 Book 3 *Application Specification*. 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 Book 3 *Application Specification*. A cardholder-controlled terminal (Terminal Type = ‘3x’) need not support terminal risk management.

2.5 Other Functional Requirements

2.5.1 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 Book 2 *Security and Key Management*). 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’).

2.5.2 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.

An attended terminal shall be capable of supporting voice referrals, (i.e., they shall be capable of displaying the appropriate message when the card or issuer indicates a referral). An unattended terminal is not required to support voice referrals. If a referral cannot be performed, default procedures are in place for the individual payment systems to decide how the transaction shall be handled (e.g., go online, approve offline, or decline offline).

2.5.2.1 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 2.3.8).

2.5.2.2 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 or an AAC for a decline. If the Issuer Authentication Data 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.

2.5.3 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.

2.5.4 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.

2.5.5 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 Book 3 *Application Specification* 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.

2.5.6 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.

One example of a method for generating the Unpredictable Number is performing an exclusive-OR operation on all the previous ARQCs, TCs, AACs, and AARs.[3] (See Book 3 *Application Specification* for details on this data element.)

2.6 Card Reading

If the terminal does not have a combined IC and magnetic stripe reader, when the magnetic stripe of the card is read and the service code begins with a '2' or a '6' indicating that an IC is present, the terminal shall prompt for the card to be inserted into the IC reader such as by displaying the 'Use Chip Reader' message.

If the terminal has a combined IC and magnetic stripe reader, when the magnetic stripe of the card is read and the service code begins with a '2' or a '6' indicating that an IC is present, the terminal shall process the transaction using the IC.

2.6.1 IC Reader

The IFD should have a pictogram near the card slot indicating how to insert the card into the IC reader.

As soon as the card is inserted into the reader, the message 'Please Wait' should be displayed to reassure the cardholder or attendant that the transaction is being processed so that the card is not removed prematurely.

When the card is inserted into the IFD, the card should be accessible to the cardholder at all times during the transaction. When the card is not accessible at all times or when the terminal has a 'tight grip' to hold the card, there should be a mechanism, for example, a button, to recall or release the card in case of terminal malfunction, even if there is a power failure. For an unattended terminal with card capture capability, where captured cards remain in the secure housing of the terminal (such as for an ATM), the card release function is not required.

When the card is inserted into the IFD, the cardholder or attendant should not be able to accidentally dislodge the card from the reader.

If the card is removed from the terminal prior to completion of the transaction, the terminal should abort the transaction and should ensure that neither the card nor the terminal is damaged. The message 'Processing Error' should be displayed. (For additional requirements on abnormal termination of transaction processing, see Book 3 *Application Specification*.)

2.6.2 Exception Handling

When an attended terminal attempts and fails to read the ICC but the magnetic stripe of the card is successfully read, the terminal shall set the POS Entry Mode Code in the transaction message(s) to 'Magnetic stripe read, last transaction was

[3] This exclusive-OR operation is performed at each GENERATE AC response on the current application cryptogram and the previous exclusive-OR result, which is stored in the terminal.

an unsuccessful IC read' if the service code on the magnetic stripe indicates that an IC is present.[4]

2.7 Date Management

2.7.1 Data Authentication

The terminal shall be capable of properly calculating dates associated with data authentication (certificate expiration dates) for dates before, including, and after the year 2000.

2.7.2 Processing Restrictions

The terminal shall be capable of properly calculating dates associated with processing restrictions (Application Expiration Date, Application Effective Date) for dates before, including, and after the year 2000.

2.7.3 Data Management

To ensure the accuracy of the data elements Transaction Date (local date) and Transaction Time (local time), the terminal shall ensure that it is able to accurately calculate, store, and display date-dependent fields representing the year 2000 and subsequent years without compromising the integrity of dates or their use, including calculations for leap years. This requirement applies to terminals supporting clocks as well as those that update the date and the time based upon on-line messages.

The terminal should process a 2-digit year (YY) as follows:

- YY in the range 00-49 inclusive is treated as having the value 20YY
- YY in the range 50-99 inclusive is treated as having the value 19YY

The same rules shall be used if the terminal converts 2-digit years in format YY to 4-digit years in format YYYY.

[4] This does not imply that the terminal shall support this ISO 8583:1987 data element. An issuer or an acquirer may define an equivalent data element. The specific code will be set by individual payment systems.

3. Physical Characteristics

Physical characteristics vary depending on the intended usage of the terminal, the environment at the point of transaction (including its security), and the terminal configuration.

3.1 Key Pad

A terminal should have a key pad for the entry of transaction-related data and its functional operation. The key pad shall support one or more types of keys:

- Numeric: ‘0’ - ‘9’
- Alphabetic and special: For example, ‘A’ - ‘Z’, ‘*’, ‘#’,
- Command: ‘Cancel’, ‘Enter’, ‘Clear’
- Function: Application-dependent keys, such as a selection key, ‘F1’, ‘F2’, ‘Backspace’, ‘Escape’

A key pad may consist of a single key, such as a function key that could be a button on a vending machine to indicate selection of an application or to indicate that a receipt is to be printed.

A touch screen is considered to be a key pad (see Book 2 *Security and Key Management* for security requirements).

3.1.1 Command Keys

Command keys are used to control the flow of data entry by the cardholder or attendant. The description of the command keys is as follows:

Enter	Confirms an action
Cancel	Either cancels the whole transaction or, if no ‘Clear’ key is present, cancels the operation in progress
Clear	Erases all the numeric or alphabetic characters previously entered

The following colours, if used, shall be reserved for the command keys, either for the lettering or for the keys themselves:

Enter	Green
Cancel	Red
Clear	Yellow

When the command keys are horizontally arranged, the ‘Cancel’ and ‘Enter’ keys should be located on the bottom row of the key pad, and ‘Cancel’ should be the furthest key left and ‘Enter’ should be the furthest key right. When the command keys are vertically arranged, ‘Cancel’ should be the uppermost key and ‘Enter’ the lowest key.

3.1.2 PIN Pad

The terminal should be designed and constructed to facilitate the addition of a PIN pad, if not already present, such as having a serial port.

If the terminal supports PIN entry, a separate key pad may be present for PIN entry or the same key pad may be used for both PIN entry and entry of other transaction-related data. The PIN pad shall comprise the numeric and ‘Enter’ and ‘Cancel’ command keys. If necessary, the command key for ‘Clear’ may also be present.

The numeric layout of the PIN pad shall comply with ISO 9564 as shown in Figure 4, except for cardholder-controlled terminals such as personal computers (PCs), where the keyboard may contain a numeric key pad in a different format for PIN entry. An example of the placement of the ‘Cancel’ and ‘Enter’ keys on the bottom row is shown in Figure 4.

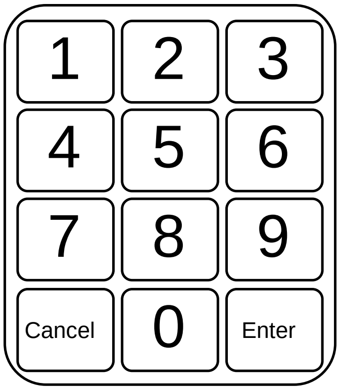

Figure 4 - PIN Pad Layout

The key for ‘5’ should have a tactile identifier (for example, a notch or raised dot) to indicate to those whose sight is impaired that this is the central key from which all others may be deduced.

3.2 Display

A display is used to help the cardholder or attendant monitor transaction flow and data entry, validate transaction-related data, and select options.

An attended terminal shall have a display for the attendant and may have an additional display for the cardholder, such as when a PIN pad is present. In order that different information may be displayed and different languages used for the attendant and cardholder, it is recommended that an attended terminal has two separate displays.

An unattended terminal should have a cardholder display.

At a minimum, the message display shall be capable of displaying at least 32 alphanumeric characters (two lines of 16 positions each). The two lines of 16 characters should be simultaneously displayed. To facilitate the display of different languages used in different geographical areas, the terminal should support a graphic display.

A terminal capable of supporting several applications should have a display that can provide cardholder application selection by allowing the 16-character Application Preferred Name(s) or Application Label(s) stored in the ICC to be displayed.

3.3 Memory Protection

Software as well as data initialised in the terminal or any part of the terminal, including cryptographic keys, shall not be erased or altered for the period of time the software and data are valid.

When the terminal supports batch data capture, the captured transactions and advices stored in the terminal shall not be erased or altered until the next reconciliation with the acquiring system.

3.4 Clock

Offline-only terminals and offline terminals with online capability shall have a clock with the local date and time.

The date is used for checking certificate expiration dates for data authentication and/or offline PIN encipherment as well as application expiration/effective dates for processing restrictions. The time may be used for assuring transaction identification uniqueness as well as for input to the application cryptogram algorithm.

3.5 Printer

A terminal should have a printer for receipt printing. If present, the printer shall be able to print at least 20 alphanumeric characters per line (see section 7.4 of this specification).

Cardholder-controlled terminal (Terminal Type = ‘3x’) need not include a printer.

3.6 Magnetic Stripe Reader

In addition to an IC reader, a terminal shall be equipped with a magnetic stripe reader, except when payment system rules indicate otherwise. These rules will cover situations when a magnetic stripe reader is not required or not allowed for a financial institution- or merchant-controlled terminal (Terminal Type = ‘1x’ or

‘2x’). A cardholder-controlled terminal (Terminal Type = ‘3x’) need not include a magnetic stripe reader.

The magnetic stripe reader shall be able to read the full track 1 and/or track 2 and process according to the payment system rules.

Part II

Software Architecture

4. Terminal Software Architecture

This section is intended to provide insight for terminal manufacturers into the future direction of the payment system applications and the consequent requirements for terminal functionality. While terminals without this functionality may operate satisfactorily in today's environment, changes in that environment will enhance the longevity of and provide functional advantages to terminals incorporating the software design principles in this section.

4.1 Environmental Changes

In today's environment, support of payment system functions is provided in the typical POS terminal by one or possibly two applications based on the limited data available from the magnetic stripe of a payment system card. Differences in cards presented are largely contained in host systems and are usually transparent to the terminal software.

The ICC replaces this environment with cards that may have multiple diverse applications, with significantly larger amounts of data representing a large number of options that must be interpreted by the terminal. The typical terminal will support multiple applications, with varying degrees of similarity. Applications may be modified annually, presenting additional challenges to software migration in the terminal. New applications will almost certainly be added during the life of a terminal. There will be a need to add applications efficiently and without risk to existing applications. Modification or addition of applications should be done in such a way that unaffected applications need not be re-certified. Code should be reusable and sharable with adequate security controls to accomplish such migration with efficiency and integrity.

Greater differentiation between the payment systems should be anticipated at the terminal, expressed by data contained within the ICC. This may (and probably will) be carried down to regional and even issuer levels, requiring the terminal to keep a library of routines available for selection by the card. The terminal may support only a subset of alternative routines, but terminals that support more will be at an advantage in the marketplace.

At the level of this specification, the payment systems view two alternative software architectures as providing the capabilities required. These two alternatives are called the ‘Application Program Interface (API)’ and the ‘Interpreter’ approaches.

4.2 Application Libraries

With either the API or the interpreter approach, the terminal should have the ability to maintain an application library of modules or routines that may be dynamically incorporated into the processing of a given transaction. Modules in the application library may be complete application programs, or they may be subroutines to be called upon at the direction of data within the terminal or the ICC. In the case of an interpreter capability, these modules will be code, written in a virtual machine instruction set implemented within the terminal, to be interpreted by the terminal control program. In the case of the API approach, modules will be object code written to the specific terminal architecture.

In either case, modules within the application library may be dynamically invoked either by logic with the terminal application software or under the direction of referencing data kept within the ICC. The format and specification of external references are under control of the individual payment systems.

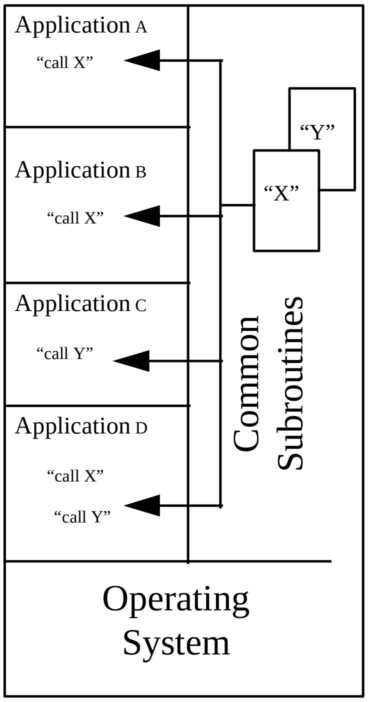

Figure 5 - Terminal Software

A terminal may contain several libraries, some accessible to all applications and some restricted to particular applications or payment systems.

4.3 Application Program Interface

This section describes a terminal software architecture through which application programs can make use of a set of essential and frequently used functions provided in terminals through a standard interface - the API.

The API takes the form of a library of functions that can be used by all applications stored in the terminal. The functions in the library may be dynamically linked into the application programs that use them.

The provision of these functions as a library in the terminal has a number of advantages:

- Each application program in the terminal does not need to include the same code to implement standardised functionality. The implementation of only one copy of code in each terminal to perform this functionality is very efficient in terminal memory.
- Application programs do not need to take account of particular terminal hardware configurations, as these will be transparent to the application program at the API. The implications of a particular terminal's hardware implementation are embedded within the code of the library function that has been certified for that terminal.

- Certification of new terminal application programs will take place against the standardised and approved API function library for a particular terminal and does not require the re-certification of existing terminal applications programs (as would be the case with a single terminal program). The verification of firewalls between application programs is considerably eased by this architecture.

While a single library of functions is used to construct the API, the library contains functions in two broad classes:

- Functions that implement the application selection functionality described in Book 1 *Application Independent ICC to Terminal Interface Requirements* (for example, Application Selection)

- Functions that implement essential and frequently used terminal hardware functionality (for example, display, get key entry, etc.)

Functions in the library may use other functions within the library. For example, static data authentication may use a terminal hardware function to read data from an application on the card.

Functions in the library may be written using either terminal dependent object code or a more general virtual machine instruction set.

4.4 Interpreter

4.4.1 Concept

The purpose of this section is to describe the general architecture underlying an interpreter implementation and give a brief overview of how it relates to the future environment for payment system applications.

Use of ICC technology necessitates altering the firmware in all terminals that accept ICCs. To facilitate this transition, an interpreter may be implemented as a software system that is compact, efficient, and easy to maintain and enhance for future payment system needs. The name arises from the capability of a terminal to contain central processing unit (CPU)-independent application programs and plugs that can be interpreted during a transaction to determine the terminal's behaviour.

An interpreter implementation defines a single software kernel, common across multiple terminal types. This kernel creates a virtual machine that may be implemented on each CPU type and that provides drivers for the terminal's input/output (I/O) and all low-level CPU-specific logical and arithmetic functions. High-level libraries, terminal programs and payment applications using standard kernel functions may be developed and certified once; thereafter, they will run on any conforming terminal implementing the same virtual machine without change. Therefore, a significant consequence of an interpreter is a simplified and uniform set of test and certification procedures for all terminal functions.

To summarise, interpreters provide the following major benefits:

- A kernel with generalised ICC support functions, to be installed in each terminal only once. The kernel lifetime is expected to match that of the terminal (7-10 years).

- One version of the terminal software kernel across multiple processor and terminal types. Therefore, only one certification and validation is needed for software libraries, terminal programs, and payment applications on the set of terminal types supported using a common interpreter/virtual machine.

- Terminal kernel certification independent of applications, so certification only needs to be performed once for each terminal type using a common interpreter/virtual machine. A terminal type is defined as a specific configuration of terminal CPU and I/O functions.

- Support for CPU-independent plugs that can be interpreted during a transaction to enhance a terminal's behaviour. CPU independence means that only one certification and validation is needed for this code.

4.4.2 Virtual Machine

The application software in every terminal using the interpreter approach is written in terms of a common virtual machine. The virtual machine is a theoretical microprocessor with standard characteristics that define such things as addressing mode, registers, address space, etc.

The virtual machine accesses memory in two areas: code space and data space. All code accesses are internal to the virtual machine only and are not available to programs; the memory fetch and store operators access data space only. Translated program code only exists in code space. No terminal software (libraries or other functions external to the kernel) can make any assumptions regarding the nature or content of code space or attempt to modify code space in any way. This restriction, plus the complete absence of a symbol table, adds significantly to program security.

4.4.3 Kernel

A kernel contains all functions whose implementation depends upon a particular platform (CPU and operating system). It includes a selected set of commands, plus a number of specialised functions, such as terminal I/O support and program loader/interpreter support.

4.4.4 Application Code Portability

Virtual machine emulation may be accomplished by one of three methods: interpreting virtual machine instructions, translating the virtual machine language into a directly executable 'threaded code' form, or translating it into actual code for the target CPU. The latter two methods offer improved performance at a modest cost in complexity.

The kernel for each particular CPU type is written to make that processor emulate the virtual machine. The virtual machine concept makes a high degree of standardisation possible across widely varying CPU types and simplifies program portability, testing, and certification issues.

Programs may be converted to an intermediate language, between the high level source language used by the programmer and the low-level machine code required by the microprocessor, and subsequently transported to the target terminal to be processed by the terminal into an executable form.

4.5 Plugs and Sockets

One function of ICCs is to improve transaction security by incorporating and managing enciphered data and participating actively in the transaction validation process. Under this concept, the payment systems define a number of procedures (referred to as 'sockets') that may be inserted by the application programmer (and hence under acquirer control and under payment system supervision) to act as placeholders for the addition of enhancing code during transaction processing.

Sockets are intended to be placed at various points in existing terminal applications or even in the terminal program itself. They are used to refer to library functions and may even occur inside a library function if a payment system foresees the need to change the way a library function operates.

Sockets are initialised to default behaviours. If no further action is taken by the terminal program, the default behaviour of these procedures will be to do nothing when they are executed.

Plugs are executable code, written in the machine language or virtual machine instruction set supported by the terminal, that may be inserted at points defined by sockets to enhance the default terminal logic. Plugs may already exist in the terminal to be invoked under control of data in the ICC and logic in the terminal. Plugs may also come from an input device (such as the ICC or a host system connected to the terminal), but only if agreed by the payment system, issuer, acquirer, and merchant. Special care may be required for ICC plugs if they can modify a socket's behaviour or be placed in the program flow prior to successful card authentication.

At the conclusion of a transaction, the sockets are restored to their original application default behaviours.

The proposed terminal architecture does not propose that ICCs contain entire applications but only plugs that enhance existing terminal applications.

Figure 6 illustrates the relationship between plugs and sockets.

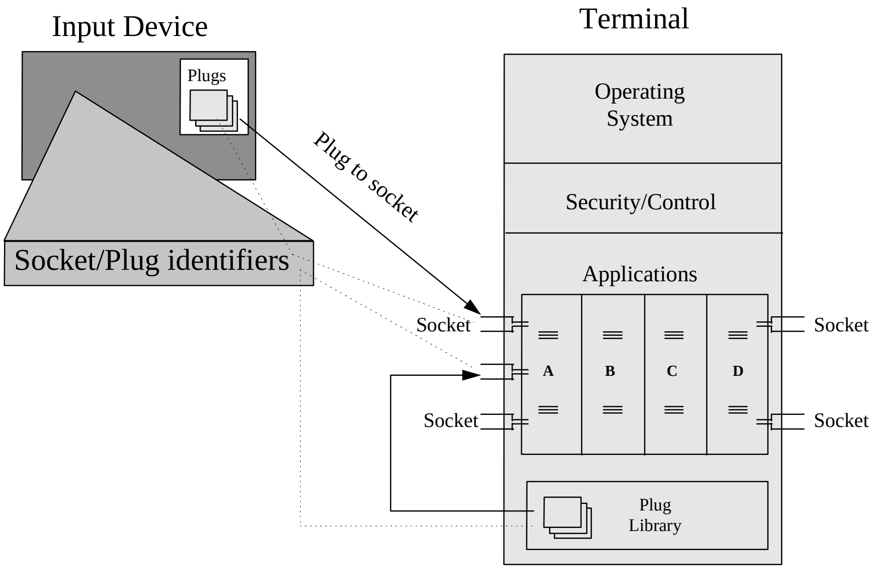

Figure 6 - Socket/Plug Relationship

5. Software Management

A means of software upgrade shall be supported wherever this is not in conflict with national legal restrictions. The software upgrade may be facilitated from a remote site over a network or locally.

Software upgrade may be performed under terminal application control or under terminal owner or acquirer human control.

When software upgrade is performed under terminal application control, prior to accepting new software, the terminal shall:

- Verify the identity of the party loading the software, since only software issued by the terminal manufacturer, owner, or a third party approved by the owner or acquirer can be loaded in the terminal.
- Verify the integrity of the loaded software.

When both tests are successful, the terminal shall notify the party loading the software whether the load was successfully performed or not.

To facilitate ICC application upgrade from one version to another, the terminal should be able to support at least two versions of the ICC application, as identified by the terminal's Application Version Numbers.

6. Data Management

The data elements listed in this section shall be initialised in the terminal or obtainable at the time of a transaction (definitions for these data are in Book 3 *Application Specification*). There may be additional data elements required for initialisation, such as those currently used for magnetic stripe processing.

Whenever a data element is initialised or updated, data integrity shall be assured.

Data elements resident in the terminal shall be under the control of one of the following parties:

- Terminal manufacturer: For example, IFD Serial Number
- Acquirer (or its agent): For example, Merchant Category Code
- Merchant: For example, Local Date and Local Time (these may be controlled by either the merchant or acquirer)

The terminal shall be constructed in such a way that:

- Terminal Capabilities and Additional Terminal Capabilities are initialised in the terminal before the terminal is placed in its operational state.
- Terminal Type is initialised in the terminal at the moment of installation.
- Terminal Capabilities, Additional Terminal Capabilities, and Terminal Type cannot be modified unintentionally or by unauthorised access.
- Whenever the terminal’s capabilities are updated or modified, Terminal Capabilities, Additional Terminal Capabilities, and Terminal Type are accurately updated.

The terminal should be constructed in such a way that the data which is under control of the acquirer is only initialised and updated by the acquirer (or its agent).

6.1 Application Independent Data

The following data elements are application independent and shall be unique to the terminal (see section 1.3 of this specification for different terminal configurations):

- Local Date
- Local Time
- Terminal Country Code
- Transaction Sequence Counter

The following data elements are application independent and may be specific to each device constituting the terminal, such as a host concentrating a cluster of devices (see Figure 2 in Part I of this specification for an example):

- Additional Terminal Capabilities
- IFD Serial Number
- Terminal Capabilities
- Terminal Type

The terminal shall have parameters initialised so that it can identify what language(s) are supported to process the card's Language Preference (see section 7.1 of this specification).

6.2 Application Dependent Data

The following data elements are application dependent and, if required, are specified by individual payment system specifications:

- Acquirer Identifier
- Application Identifier (AID)
- Application Version Number
- Certification Authority Public Key[5] (required if terminal supports offline data authentication and/or offline PIN encipherment)

– Certification Authority Public Key Exponent

– Certification Authority Public Key Modulus

- Certification Authority Public Key Index[6] (required if terminal supports offline data authentication and/or offline PIN encipherment): the key index in conjunction with the Registered Application Provider Identifier (RID) of the payment system Application Identifier (AID) identifies the key and the algorithm for offline data authentication and/or PIN encipherment.
- Default Dynamic Data Authentication Data Object List (DDOL) (required if terminal supports dynamic data authentication)
- Default Transaction Certificate Data Object List (TDOL) (If not present, a default TDOL with no data objects in the list shall be assumed)

[5] See Book 2 *Security and Key Management*

[6] See Book 2 *Security and Key Management*

- Maximum Target Percentage to be used for Biased Random Selection (required if offline terminal with online capability)
- Merchant Category Code
- Merchant Identifier
- Merchant Name and Location
- PIN Pad Secret Keys (required if the PIN pad and IC reader are not an integrated tamper-evident device or if the terminal supports enciphering PINs for online verification)[7]
- Target Percentage to be used for Random Selection (required if offline terminal with online capability)
- Terminal Action Code - Default, Terminal Action Code - Denial, Terminal Action Code - Online (required if non-zero values to be used[8])
- Terminal Floor Limit (required if offline terminal or offline terminal with online capability)
- Terminal Identification
- Terminal Risk Management Data (if required by individual payment system rules)
- Threshold Value for Biased Random Selection (required if offline terminal with online capability)
- Transaction Currency Code
- Transaction Currency Exponent
- Transaction Reference Currency Code
- Transaction Reference Currency Conversion
- Transaction Reference Currency Exponent

The terminal shall provide the necessary logical key slots to handle the active and future replacement Certification Authority Public Keys necessary for data authentication and/or offline PIN encipherment. Each logical key slot shall contain the following data: RID, Certification Authority Public Key Index, Certification Authority Public Key.

[7] More than one secret key may be needed.

[8] According to Book 3 the *Application Specification*, the default value consists of all bits set to ‘0’, although ‘Data authentication was not performed’, ‘Static data authentication failed’, and ‘Dynamic data authentication failed’ bits are strongly recommended to be set to ‘1’ in the Terminal Action Code - Default and Terminal Action Code - Online.

When the Certification Authority Public Key is loaded to the terminal, the terminal shall verify the Certification Authority Public Key Check Sum to detect a key entry or transmission error. The method for calculating this check sum is by the terminal-supported Secure Hash Algorithm. If the verification process fails, the terminal shall not accept the Certification Authority Public Key and, if operator action is needed, the terminal shall display an error message. After the Certification Authority Public Key is successfully loaded, the terminal should store the Certification Authority Public Key Check Sum.

A means for updating data elements specific to payment system applications shall be supported wherever this is not in conflict with national legal restrictions. Data update may be facilitated from a remote site over a network or locally.

THIS PAGE LEFT INTENTIONALLY BLANK

Part III

Cardholder, Attendant, and Acquirer Interface

7. Cardholder and Attendant Interface

7.1 Language Selection

The terminal shall support at least the local language which is the language of common usage in the terminal's locality or region. The messages displayed to the attendant shall always be in the local language. To display the standard messages defined in section 7.2, the terminal shall support the relevant character set defined in the corresponding part of ISO 8859.

Depending on the local environment and business conditions, the terminal should support multiple languages for displaying the set of messages described in section 7.2 to the cardholder. A terminal supporting multiple languages may need additional parts of ISO 8859 to display characters relevant to these languages.

ISO 8859 consists of several parts, each part specifying a set of up to 191 characters coded by means of a single 8-bit byte. Each part is intended for use for a group of languages. All parts of ISO 8859 contain a common set of 95 characters, coded between '20' (hexadecimal) and '7E' (hexadecimal) as shown in Annex B. This common character set allows the terminal to display Application Label(s) and messages in multiple languages using Latin characters without using diacritic marks (see example in Annex B).

A terminal supporting multiple languages shall compare the card's Language Preference with the languages supported in the terminal at the beginning of the transaction.

If a match is found, the language with the highest preference shall be used in the messages displayed to the cardholder. Language Preference is coded so that the language with the highest preference appears first and the lowest preference appears last.

If no match is found and the terminal supports more than one language, the terminal shall allow the cardholder to select the preferred language at the beginning of the transaction. The messages shall be displayed to the cardholder in the selected language.

If no match is found or the terminal supports only one language, the terminal shall display messages in that language.

When a message is displayed to the cardholder as well as the attendant, it should be displayed to the attendant in the local language and to the cardholder in the preferred language, if supported.

7.2 Standard Messages[9]

To ensure consistency in the messages displayed by the terminal and the PIN pad, the following set of messages (or their equivalent meaning) shall be used in the languages of preference for the cardholder and attendant.

The messages shall be uniquely identified by a two-character message identifier as shown below. The message identifier is for identification purposes only and is not to be displayed to the cardholder or attendant. Values '01' - '12' (hexadecimal) are described below. Values '13' - '3F' (hexadecimal) are reserved for assignment according to this specification. Values '40' - '7F' (hexadecimal) are reserved for use by the individual payment systems. Values '80' - 'BF' (hexadecimal) are reserved for use by acquirers. Values 'C0' - 'FF' (hexadecimal) are reserved for use by issuers.

There may be additional messages displayed for the attendant or cardholder.

Note: messages may be displayed simultaneously, such as 'Incorrect PIN' and 'Enter PIN'.

'01' - (AMOUNT)

Indicates the transaction amount to both the cardholder and attendant.

'02' - (AMOUNT) OK?

Invites a response from the cardholder indicating agreement or disagreement with the displayed transaction amount. Agreement or disagreement should be denoted by pressing the 'Enter' or 'Cancel' keys, respectively.

'03' - APPROVED

Indicates to the cardholder and attendant that the transaction has been approved.

'04' - CALL YOUR BANK

Indicates to the cardholder or attendant to contact the issuer or acquirer, as appropriate, such as for voice referrals.

'05' - CANCEL OR ENTER

When used with the 'Enter PIN' message, instructs the cardholder to validate PIN entry by pressing the 'Enter' key or to cancel PIN entry by pressing the 'Cancel' key.

[9] This specification does not imply that the terminal shall support a set of standard messages in English.

‘06’ - CARD ERROR

Indicates to the cardholder or attendant a malfunction of the card or a non-conformance to answer-to-reset.

‘07’ - DECLINED

Indicates to the cardholder and attendant that the online or offline authorisation has not been approved.

‘08’ - ENTER AMOUNT

Instructs the cardholder at an unattended terminal or the attendant at an attended terminal to enter the amount of the transaction. Confirmation or cancellation of amount entry should be denoted by pressing the ‘Enter’ or ‘Cancel’ keys, respectively.

‘09’ - ENTER PIN

Invites the cardholder to enter the PIN for the first and subsequent PIN tries. An asterisk is displayed for each digit of the PIN entered.

‘0A’ - INCORRECT PIN

Indicates that the PIN entered by the cardholder does not match the reference PIN.

‘0B’ - INSERT CARD

Instructs to insert the ICC into the IFD. Correct insertion should be noted by displaying the message ‘Please Wait’ to reassure the cardholder or attendant that the transaction is being processed.

‘0C’ - NOT ACCEPTED

Indicates to the cardholder and attendant that the application is not supported or there is a restriction on the use of the application, for example, the card has expired.

‘0D’ - PIN OK

Indicates that offline PIN verification was successful.

‘0E’ - PLEASE WAIT

Indicates to the cardholder and attendant that the transaction is being processed.

‘0F’ - PROCESSING ERROR

Displayed to the cardholder or attendant when the card is removed before the processing of a transaction is complete or when the transaction is aborted because of a power failure, or the system or terminal has malfunctioned, such as communication errors or time-outs.

‘10’ - REMOVE CARD

Instructs to remove the ICC from the IFD.

‘11’ - USE CHIP READER

Instructs to insert ICC into the IC reader of the IFD.

‘12’ - USE MAG STRIPE

Instructs to insert ICC into the magnetic stripe reader of the terminal after IC reading fails, when the IC and magnetic stripe readers are not combined.

‘13’ - TRY AGAIN

Invites the cardholder to re-execute the last action performed.

7.3 Application Selection

A terminal shall support explicit application selection as described in Book 1 *Application Independent ICC to Terminal Interface Requirements*. A terminal may support application selection using the payment systems directory as described in Book 1 *Application Independent ICC to Terminal Interface Requirements*.

A terminal supporting more than one application should offer the cardholder the ability to select an application or confirm the selection proposed by the terminal. Applications supported by both the ICC and the terminal shall be presented to the cardholder in priority sequence according to the card’s Application Priority Indicator, if present, with the highest priority listed first.

A terminal allowing cardholder selection or confirmation shall create a list of ICC applications that are supported by the terminal as described in Book 1 *Application Independent ICC to Terminal Interface Requirements* and display:

- The Application Preferred Name(s), if present and if the Issuer Code Table Index indicating the part of ISO 8859 to use is present and supported by the terminal (as indicated in Additional Terminal Capabilities).

- Otherwise, the Application Label(s), if present, by using the common character set of ISO 8859 (see Annex B).

A terminal not offering the cardholder the ability to select or confirm a selection shall determine those applications supported by both the card and the terminal that may be selected without confirmation of the cardholder according to Application Priority Indicator, if present. The terminal shall select the application with the highest priority from those.

If the card returns SW1 SW2 other than ‘9000’ in response to the SELECT command indicating that the transaction cannot be performed with the selected application:

- A terminal allowing cardholder selection or confirmation should display the ‘Try Again’ message and shall present to the cardholder the list of applications supported by both the ICC and the terminal without this application

- A terminal not offering cardholder selection or confirmation shall select the application with the next highest priority among those supported by both the ICC and the terminal that may be selected without cardholder confirmation.

If no application can be selected, the terminal should display the ‘Not Accepted’ message and shall terminate the transaction.

The application used for the transaction shall be identified on the transaction receipt by the partial Application PAN (or the full PAN, if allowed by payment system rules) and the AID.

7.4 Receipt

Whenever a receipt is provided, it shall contain the AID in addition to the data required by payment system rules.[10] The AID shall be printed as hexadecimal characters.

[10] The receipt may contain the partial Application PAN (or full if allowed).

8. Acquirer Interface

8.1 Message Content

Messages typically flow from the terminal to the acquirer and from the acquirer to the issuer. Message content may vary from one link to another, with data being added to enrich the message at the acquirer. To enrich the message, the acquirer stores static point of transaction data elements[11] based on the Merchant Identifier and/or the Terminal Identifier. These data elements are implicitly referred to by the Merchant/Terminal Identifier(s) and therefore may be absent in terminal to acquirer messages.[12] In the following sections, this implicit relationship is indicated by a specific condition: 'Present if the Merchant/Terminal Identifier(s) do not implicitly refer to the (data element)'.

Message content may also vary due to data requested by the acquirer but not the issuer, such as for transaction capture or audit. The ICC stored data elements are implicitly known by the issuer[13] based on the AID and/or PAN and therefore may be absent in acquirer to issuer messages. In the following sections, this implicit relationship is indicated by a specific condition: 'Present if requested by the acquirer'.

Data requirements may differ depending on terminal operational control, which is recognised through a specific condition: 'Present for Terminal Type = xx'. For example, Merchant Identifier is provided only for a merchant-controlled terminal (Terminal Type = '2x').

An authorisation message shall be used when transactions are batch data captured. A financial transaction message shall be used when online data capture is performed by the acquirer. An offline advice shall be conveyed within batch data capture when supported. An online advice or a reversal message shall be transmitted real-time, similarly to an authorisation or financial transaction message.

This section describes requirements associated with ICC transactions and distinguishes between new data elements and existing data elements used for magnetic stripe transactions. Data elements referred to as existing are those defined in ISO 8583:1987, though actual terminal message contents are usually specific to (each of) the acquiring system(s) to which the terminal is connected.

[11] These data elements indicate point of transaction acceptance characteristics that rarely change, such as Merchant Category Code, Acquirer Identifier, or Terminal Country Code.

[12] At a minimum, all data listed in the Card Risk Management Data Object Lists and the TDOL shall be available at the point of transaction.

[13] These data elements reflect card acceptance conditions and restrictions that rarely change, such as Application Interchange Profile, Application Usage Control, or Issuer Action Codes.

Data elements marked with an asterisk are the minimum set of data elements to be supported in authorisation request and response messages, as well as clearing messages, for ICC transactions.

For informational purposes, Annex C describes an example for conversion into message data elements.

8.1.1 Authorisation Request

An authorisation request should convey the data elements contained in Table 1 and Table 2 subject to the specified conditions.

Table 1 contains the new data elements specifically created for an ICC transaction.

Data Element	Condition
Application Interchange Profile *	
Application Transaction Counter *	
ARQC *	
Cryptogram Information Data *	
CVM Results	
IFD Serial Number	Present if Terminal Identifier does not implicitly refer to IFD Serial Number
Issuer Application Data *	Present if provided by ICC in GENERATE AC command response
Terminal Capabilities	
Terminal Type	
Terminal Verification Results *	
Unpredictable Number*	Present if input to application cryptogram calculation

Table 1 - New Authorisation Request Data Elements

Table 2 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Acquirer Identifier	Present for Terminal Type = ‘1x’ or ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single acquirer
Amount, Authorised *	
Amount, Other *	Present if cashback used for current transaction
Application Effective Date	Present if in ICC
Application Expiration Date	Present if not in Track 2 Equivalent Data
Application PAN *	Present if not in Track 2 Equivalent Data
Application PAN Sequence Number *	Present if in ICC
Enciphered PIN Data	Present if CVM performed is ‘enciphered PIN for online verification’
Merchant Category Code	Present for Terminal Type = ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single merchant category
Merchant Identifier	Present for Terminal Type = ‘2x’ if Terminal Identifier does not implicitly refer to a single merchant
POS Entry Mode	
Terminal Country Code *	
Terminal Identifier	
Track 2 Equivalent Data	Present if in ICC
Transaction Currency Code *	
Transaction Date *	
Transaction Time	Present if Terminal Type = ‘x2’, ‘x3’, ‘x5’, or ‘x6’
Transaction Type *	

Table 2 - Existing Authorisation Request Data Elements

8.1.2 Financial Transaction Request

A financial transaction request should convey the data elements contained in Table 3 and Table 4 subject to the specified conditions.

Table 3 contains the new data elements created specifically for an ICC transaction.

Data Element	Condition
Application Interchange Profile *	
Application Transaction Counter *	
Application Usage Control	Present if requested by acquirer
ARQC *	
Cryptogram Information Data *	
CVM List	Present if requested by acquirer
CVM Results	
IFD Serial Number	Present if Terminal Identifier does not implicitly refer to IFD Serial Number
Issuer Action Code - Default	Present if requested by acquirer
Issuer Action Code - Denial	Present if requested by acquirer
Issuer Action Code - Online	Present if requested by acquirer
Issuer Application Data *	Present if provided by ICC in GENERATE AC command response
Terminal Capabilities	
Terminal Type	
Terminal Verification Results *	
Unpredictable Number *	Present if input to application cryptogram calculation

Table 3 - New Financial Transaction Request Data Elements

Table 4 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Acquirer Identifier	Present for Terminal Type = ‘1x’ or ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single acquirer
Amount, Authorised *	Present if final transaction amount is different from authorised amount
Amount, Other *	Present if cashback used for current transaction
Application Effective Date	Present if in ICC
Application Expiration Date	Present if not in Track 2 Equivalent Data
Application PAN *	Present if not in Track 2 Equivalent Data
Application PAN Sequence Number *	Present if in ICC
Enciphered PIN Data	Present if CVM performed is ‘Enciphered PIN for online verification’.
Issuer Country Code	Present if requested by acquirer
Merchant Category Code	Present for Terminal Type = ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single merchant category
Merchant Identifier	Present for Terminal Type = ‘2x’ if Terminal Identifier does not implicitly refer to a single merchant
POS Entry Mode	
Terminal Country Code *	
Terminal Identifier	
Track 2 Equivalent Data	Present if in ICC
Transaction Amount *	
Transaction Currency Code *	
Transaction Date *	
Transaction Time	Present if Terminal Type = ‘x2’, ‘x3’, ‘x5’, or ‘x6’
Transaction Type *	

Table 4 - Existing Financial Transaction Request Data Elements

8.1.3 Authorisation or Financial Transaction Response

Authorisation and financial transaction responses should convey the data elements contained in Table 5 and Table 6 subject to the specified conditions:

Table 5 contains the new data elements specifically created for an ICC transaction.

Data Element	Condition
Issuer Authentication Data *	Present if online issuer authentication performed
Issuer Script * • Issuer Script Template 1 • Issuer Script Template 2	Present if commands to ICC are sent by issuer

Table 5 - New Authorisation or Financial Transaction Response Data Elements

Table 6 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Acquirer Identifier	Present for Terminal Type = ‘1x’ or ‘2x’ if in request message
Amount, Authorised	
Authorisation Code	Present if transaction is approved
Authorisation Response Code	
Terminal Identifier	
Transaction Date	
Transaction Time	

Table 6 - Existing Authorisation or Financial Transaction Response Data Elements

8.1.4 Financial Transaction Confirmation

A financial transaction confirmation should convey the data elements contained in Table 7 and Table 8 subject to the specified conditions.

Table 7 contains the new data elements specifically created for an ICC transaction.

Data Element	Condition
Issuer Script Results	Present if script commands to ICC are delivered by terminal
TC or AAC	

Table 7 - New Financial Transaction Confirmation Data Elements

Table 8 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Terminal Identifier	

Table 8 - Existing Financial Transaction Confirmation Data Elements

8.1.5 Batch Data Capture

Batch data capture should convey the data elements contained in Table 9 and Table 10 subject to the specified conditions. Message Type is used to distinguish between an offline advice and a financial record.

Table 9 contains the new data elements specifically created for an ICC transaction.

Data Element	Condition
Application Interchange Profile *	
Application Transaction Counter *	
Application Usage Control	Present if requested by acquirer
Cryptogram Information Data *	
CVM List	Present if requested by acquirer
CVM Results	
IFD Serial Number	Present if Terminal Identifier does not implicitly refer to IFD Serial Number
Issuer Action Code - Default	Present if requested by acquirer
Issuer Action Code - Denial	Present if requested by acquirer
Issuer Action Code - Online	Present if requested by acquirer
Issuer Application Data *	Present if provided by ICC in GENERATE AC command response
Issuer Script Results	Present if script commands to ICC are delivered by terminal
Terminal Capabilities	
Terminal Type	
Terminal Verification Results *	
TC/ARQC or AAC *	ARQC may be used as TC substitute
Unpredictable Number *	Present if input to application cryptogram calculation

Table 9 - New Batch Data Capture Data Elements

Table 10 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Acquirer Identifier	Present if for Terminal Type = '1x' or '2x' Merchant Identifier or Terminal Identifier does not implicitly refer to a single acquirer
Amount, Authorised *	Present if final transaction amount is different from authorised amount
Amount, Other *	Present if cashback used for current transaction
Application Effective Date	Present if in ICC
Application Expiration Date	
Application PAN *	
Application PAN Sequence Number *	Present if in ICC
Authorisation Code	Present if transaction is approved
Authorisation Response Code	
Issuer Country Code	Present if requested by acquirer
Merchant Category Code	Present for Terminal Type = '2x' if Merchant Identifier or Terminal Identifier does not implicitly refer to a single merchant category
Merchant Identifier	Present for Terminal Type = '2x' if Terminal Identifier does not implicitly refer to a single merchant
Message Type	
POS Entry Mode	
Terminal Country Code *	
Terminal Identifier	
Transaction Amount *	
Transaction Currency Code *	Present if Merchant Identifier or Terminal Identifier does not implicitly refer to a single transaction currency accepted at point of transaction

Transaction Date *	
Transaction Time	
Transaction Type *	

Table 10 - Existing Batch Data Capture Data Elements

8.1.6 Reconciliation

A reconciliation should convey the existing data elements necessary for ICC transactions and subject to the specified conditions.

Data Element	Condition
Acquirer Identifier	Present for Terminal Type = ‘1x’ or ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single acquirer
Amount, Net Reconciliation	
Merchant Identifier	Present for Terminal Type = ‘2x’ if Terminal Identifier implicitly does not refer to a single merchant
Reconciliation Currency Code	Present if Merchant Identifier or Terminal Identifier does not implicitly refer to a single transaction currency accepted at point of transaction
Terminal Identifier	
Transactions Number (per transaction type)	
Transactions Amount (per transaction type)	

Table 11 - Existing Reconciliation Data Elements

8.1.7 Online Advice

An online advice should convey the data elements contained in Tables 12 and 13 subject to the specified conditions.

Table 12 contains the new data elements specifically created for an ICC transaction.

Data Element	Condition
Application Interchange Profile	
Application Transaction Counter	
Cryptogram Information Data	
CVM Results	
IFD Serial Number	Present if Terminal Identifier does not implicitly refer to IFD Serial Number
Issuer Application Data	Present if provided by ICC in GENERATE AC command response
Issuer Script Results	Present if script commands to ICC are delivered by terminal
Terminal Capabilities	
Terminal Type	
Terminal Verification Results	
TC or AAC	
Unpredictable Number	Present if input to application cryptogram calculation

Table 12 - New Online Advice Data Elements

Table 13 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Acquirer Identifier	Present for Terminal Type = ‘1x’ or ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single acquirer
Amount, Authorised	Present if final transaction amount is different from authorised amount
Application Effective Date	Present if in ICC
Application Expiration Date	Present if not in Track 2 Equivalent Data
Application PAN	Present if not in Track 2 Equivalent Data
Application PAN Sequence Number	Present if in ICC
Authorisation Response Code	
Merchant Category Code	Present for Terminal Type = ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single merchant category
Merchant Identifier	Present for Terminal Type = ‘2x’ if Terminal Identifier does not implicitly refer to a single merchant
POS Entry Mode	
Terminal Country Code	Present if Terminal Identifier or IFD Serial Number does not implicitly refer to a single terminal country
Terminal Identifier	
Track 2 Equivalent Data	Present if in ICC
Transaction Amount	
Transaction Currency Code	Present if Merchant Identifier or Terminal Identifier does not implicitly refer to a single transaction currency accepted at point of transaction
Transaction Date	
Transaction Time	Present if Terminal Type = ‘x2’, ‘x3’, ‘x5, or ‘x6’
Transaction Type	

Table 13 - Existing Online Advice Data Elements

8.1.8 Reversal

A reversal should convey the data elements contained in Table 14 and Table 15 subject to the specified conditions.

Table 14 contains the new data elements specifically created for an ICC transaction.

Data Element	Condition
Application Interchange Profile	
Application Transaction Counter	
IFD Serial Number	Present if Terminal Identifier does not implicitly refer to IFD Serial Number
Issuer Application Data	Present if provided by ICC in GENERATE AC command response
Issuer Script Results	Present if script commands to ICC are delivered by terminal
Terminal Capabilities	
Terminal Type	
Terminal Verification Results	

Table 14 - New Reversal Data Elements

Table 15 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Acquirer Identifier	Present for Terminal Type = ‘1x’ or ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single acquirer
Application Expiration Date	Present if not in Track 2 Equivalent Data
Application PAN	Present if not in Track 2 Equivalent Data
Application PAN Sequence Number	Present if in ICC
Authorisation Response Code	
Merchant Category Code	Present for Terminal Type = ‘2x’ if Merchant Identifier or Terminal Identifier does not implicitly refer to a single merchant category
Merchant Identifier	Present for Terminal Type = ‘2x’ if Terminal Identifier does not implicitly refer to a single merchant
Original Data Elements	Present if available at terminal
POS Entry Mode	
Terminal Country Code	Present if Terminal Identifier or IFD Serial Number does not implicitly refer to a single terminal country
Terminal Identifier	
Track 2 Equivalent Data	Present if in ICC
Transaction Amount	
Transaction Currency Code	Present if Merchant Identifier or Terminal Identifier does not implicitly refer to a single transaction currency accepted at point of transaction
Transaction Date	
Transaction Time	Present if Terminal Type = ‘x2’, ‘x3’, ‘x5, or ‘x6’
Transaction Type	

Table 15 - Existing Reversal Data Elements

8.2 Exception Handling

This section describes exception conditions that may occur during real-time authorisation, financial transaction, or online advice and the associated actions the terminal shall perform.

In this section, the term 'authorisation' applies to authorisation messages as well as financial transaction messages.

8.2.1 Unable to Go Online

During transaction processing, the terminal may send an authorisation request to the acquirer due to at least one of the following conditions:

- Online-only terminal type
- Attendant action (for example, merchant suspicious of cardholder)
- Terminal risk management parameters set by the acquirer
- Terminal action analysis in comparing Terminal Verification Results with Issuer Action Code - Online (see the Book 3 *Application Specification*)
- Card action analysis via its response to the first GENERATE AC command: Cryptogram Information Data indicates ARQC returned (see Book 3 *Application Specification*.)

If the terminal is unable to process the transaction online, as described in Book 3 *Application Specification*, the terminal shall compare the Terminal Verification Results with both Terminal Action Code - Default and Issuer Action Code - Default to determine whether to accept or decline the transaction offline and shall issue the second GENERATE AC command to the ICC indicating its decision:

- If the terminal accepts the transaction, it shall set the Authorisation Response Code to 'Unable to go online, offline accepted'.
- If the terminal declines the transaction, it shall set the Authorisation Response Code to 'Unable to go online, offline declined'.

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 TC for an approval or an AAC for a decline.

8.2.2 Downgraded Authorisation

When the authorisation response received by the terminal does not contain the Issuer Authentication Data, the terminal shall not execute the EXTERNAL AUTHENTICATE command and shall set the 'Issuer authentication was performed' bit in the Transaction Status Information to '0', as described in Book

3 *Application Specification*. The terminal shall continue processing based on the Authorisation Response Code returned in the response message as described in section 2.3.6 of this specification.

Note: If the acquirer or the intermediate network is unable to support ICC messages, the terminal should send messages compliant with current payment system specifications. Payment systems will determine compliance requirements for message content.

8.2.3 Authorisation Response Incidents

The authorisation response may not be correctly received by the terminal. The following incidents may occur:

- Response not received or received too late (for example, network failure, time-out)
- Response with invalid format or syntax
- Request not received by the authorisation host (for example, network failure)

After repeat(s) of the authorisation request, the terminal shall process the transaction as being unable to go online. As described in Book 3 *Application Specification,* the terminal shall compare the Terminal Verification Results with both Terminal Action Code - Default and Issuer Action Code - Default to determine whether to accept or decline the transaction offline and shall issue the second GENERATE AC command to the ICC indicating its decision:

- If the terminal accepts the transaction, it shall set the Authorisation Response Code to 'Unable to go online, offline accepted'.
- If the terminal declines the transaction, it shall set the Authorisation Response Code to 'Unable to go online, offline declined'.

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 TC for an approval or an AAC for a decline.

When online data capture is performed by the acquirer, the terminal shall send a reversal message regardless of the final decision on the transaction (to ensure that if the authorisation host received a request and sent a response, the transaction is cancelled). If the transaction is finally approved offline (TC returned by the ICC), the terminal shall create a financial record to be forwarded to the acquirer.

8.2.4 Script Incidents

The Issuer Script may not be correctly processed. The following incidents may occur:

- Script length error: The response message contains one (or more) Issuer Script(s) whose cumulative total length is larger than the script length supported by the network or terminal.

- Script with incorrect format or syntax: The terminal is unable to correctly parse the Issuer Script(s) into single Script Commands, as specified in Book 3 *Application Specification*.

If either of these incidents occur, the terminal shall terminate the processing of the Issuer Script in which the incident occurred, shall read if possible the Script Identifier (when present) and shall report it as not performed in the Issuer Script Results of the financial transaction confirmation or batch data capture message. The terminal shall continue processing any subsequent Issuer Script.

8.2.5 Advice Incidents

If the terminal is unable to create an advice when requested by the card in the Cryptogram Information Data returned in the response to the GENERATE AC command as described in section 2.3.7, of this specification, the terminal shall terminate the transaction.

Annexes

Annex A - Coding of Terminal Data Elements

This annex provides the coding for the Terminal Type, Terminal Capabilities, Additional Terminal Capabilities, CVM Results, Issuer Script Results, and Authorisation Response Code.

Coding of data (bytes or bits) indicated as RFU shall be '0'.

Neither the terminal nor the card shall check the data indicated as RFU.

A1. Terminal Type

Environment	Operational Control Provided By:		
	Financial Institution	Merchant	Cardholder[14]
Attended			
Online only	11	21	--
Offline with online capability	12	22	--
Offline only	13	23	--
Unattended			
Online only	14	24	34
Offline with online capability	15	25	35
Offline only	16	26	36

Table 16 - Terminal Type

Terminal Types '14', '15', and '16' with cash disbursement capability (Additional Terminal Capabilities, byte 1, 'cash' bit = '1') are considered to be ATMs. All other Terminal Types are not considered to be ATMs.

[14] For the purpose of this specification, an attended cardholder-controlled terminal is considered to be a nonexistent category.

Examples of terminal types are:

- Attended and controlled by financial institution: Branch terminal
- Attended and controlled by merchant: Electronic cash register, portable POS terminal, stand-alone POS terminal, host concentrating POS terminal
- Unattended and controlled by financial institution: ATM, banking automat
- Unattended and controlled by merchant: Automated fuel dispenser, pay telephone, ticket dispenser, vending machine
- Unattended and controlled by cardholder: Home terminal, personal computer, screen telephone, Payphones, Digital interactive Television / Set Top Boxes.

See Annex E for more detailed examples.

A2. Terminal Capabilities

In the tables, a ‘1’ means that if that bit has the value ‘1’, the corresponding ‘meaning’ applies. An ‘x’ means that the bit does not apply

Byte 1: Card Data Input Capability

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Manual key entry
x	1	x	x	x	x	x	x	Magnetic stripe
x	x	1	x	x	x	x	x	IC with contacts
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 17 - Terminal Capabilities

Byte 2: CVM Capability

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Plaintext PIN for ICC verification
x	1	x	x	x	x	x	x	Enciphered PIN for online verification
x	x	1	x	x	x	x	x	Signature (paper)
x	x	x	1	x	x	x	x	Enciphered PIN for offline verification
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 17 - Terminal Capabilities

If the terminal supports a CVM of signature, the terminal shall be an attended terminal (Terminal Type = ‘x1’, ‘x2’, or ‘x3’) and shall support a printer (Additional Terminal Capabilities, byte 4, ‘Print, attendant’ bit = ‘1’).

Byte 3: Security Capability

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Static data authentication
x	1	x	x	x	x	x	x	Dynamic data authentication
x	x	1	x	x	x	x	x	Card capture
x	x	x	1	x	x	x	x	Combined Dynamic Data Authentication/Application Cryptogram Generation
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 17 - Terminal Capabilities

A3. Additional Terminal Capabilities

In the tables, a ‘1’ means that if that bit has the value ‘1’, the corresponding ‘meaning’ applies. An ‘x’ means that the bit does not apply

Byte 1: Transaction Type Capability

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cash
x	1	x	x	x	x	x	x	Goods
x	x	1	x	x	x	x	x	Services
x	x	x	1	x	x	x	x	Cashback
x	x	x	x	1	x	x	x	Inquiry[15]
x	x	x	x	x	1	x	x	Transfer[16]
x	x	x	x	x	x	1	x	Payment[17]
x	x	x	x	x	x	x	1	Administrative

Table 18 - Additional Terminal Capabilities

[15] For the purpose of this specification, an inquiry is a request for information about one of the cardholder’s accounts.

[16] For the purpose of this specification, a transfer is a movement of funds by a cardholder from one of its accounts to another of the cardholder’s accounts, both of which are held by the same financial institution.

[17] For the purpose of this specification, a payment is a movement of funds from a cardholder account to another party, for example, a utility bill payment.

Byte 2: Transaction Type Capability, continued

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

Table 18 - Additional Terminal Capabilities

Byte 3: Terminal Data Input Capability

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Numeric keys
x	1	x	x	x	x	x	x	Alphabetic and special characters keys
x	x	1	x	x	x	x	x	Command keys
x	x	x	1	x	x	x	x	Function keys
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 18 - Additional Terminal Capabilities

Byte 4: Terminal Data Output Capability[18]

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Print, attendant
x	1	x	x	x	x	x	x	Print, cardholder
x	x	1	x	x	x	x	x	Display, attendant
x	x	x	1	x	x	x	x	Display, cardholder
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	1	x	Code table 10
x	x	x	x	x	x	x	1	Code table 9

Table 18 - Additional Terminal Capabilities

The code table number refers to the corresponding part of ISO 8859.

[18] If the terminal is attended (Terminal Type = ‘x1’, ‘x2’, or ‘x3’) and there is only one printer, the ‘Print, attendant’ bit shall be set to ‘1’ and the ‘Print, cardholder’ bit shall be set to ‘0’.

If the terminal is attended and there is only one display, the ‘Display, attendant’ bit shall be set to ‘1’ and the ‘Display, cardholder’ bit shall be set to ‘0’.

If the terminal is unattended (Terminal Type = ‘x4’, ‘x5’, or ‘x6’), the ‘Print, attendant’ and ‘Display, attendant’ bits shall be set to ‘0’.

Byte 5: Terminal Data Output Capability, continued

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Code table 8
x	1	x	x	x	x	x	x	Code table 7
x	x	1	x	x	x	x	x	Code table 6
x	x	x	1	x	x	x	x	Code table 5
x	x	x	x	1	x	x	x	Code table 4
x	x	x	x	x	1	x	x	Code table 3
x	x	x	x	x	x	1	x	Code table 2
x	x	x	x	x	x	x	1	Code table 1

Table 18 - Additional Terminal Capabilities

A4. CVM Results

Byte 1: CVM Performed

Last CVM of the CVM List actually performed by the terminal: One-byte CVM Code of the CVM List as defined in Book 3 *Application Specification* (‘3F’ if no CVM is performed)

Byte 2: CVM Condition

One-byte CVM Condition Code of the CVM List as defined in Book 3 *Application Specification*

Byte 3: CVM Result

Result of the (last) CVM performed as known by the terminal:

‘0’ = Unknown (for example, for signature)
‘1’ = Failed (for example, for offline PIN)
‘2’ = Successful (for example, for offline PIN)

A5. Issuer Script Results

Byte 1: Script Result

<u>First nibble:</u> Result of the Issuer Script processing performed by the terminal:

‘0’ = Script not performed
‘1’ = Script processing failed
‘2’ = Script processing successful

<u>Second nibble:</u> Sequence number of the Script Command

‘0’	= Not specified
‘1’ to ‘E’	= Sequence number from 1 to 14
‘F’	= Sequence number of 15 or above

Bytes 2-5: Script Identifier

Script Identifier of the Issuer Script received by the terminal, if available, zero filled if not. Mandatory if more than one Issuer Script was received by the terminal.

Bytes 1-5 are repeated for each Issuer Script processed by the terminal.

A6. Authorisation Response Code

When transmitted to the card, the Authorisation Response Code obtained from the authorisation response message shall include at least the following:

- Online approved
- Online declined
- Referral (initiated by issuer)
- Capture card

In addition, the terminal shall be able to generate and transmit to the card the following new response codes when transactions are not authorised online:

Response Code	**Value**
Offline approved	Y1
Offline declined	Z1
Approval (after card-initiated referral)	Y2
Decline (after card-initiated referral)	Z2
Unable to go online, offline approved	Y3
Unable to go online, offline declined	Z3

Table 19 - Response Codes

The terminal shall never modify the Authorisation Response Code returned in the response message[19].

[19] The card's final decision is reflected in the Cryptogram Information Data and not in the Authorisation Response Code.

Annex B - Common Character Set

The character set common to all parts of ISO 8859 is as shown in Table 20:

				b8	0	0	0	0	0	0	0	0
				b7	0	0	0	0	1	1	1	1
				b6	0	0	1	1	0	0	1	1
				b5	0	1	0	1	0	1	0	1
b4	b3	b2	b1		00	01	02	03	04	05	06	07
0	0	0	0	00			SP	0	@	P	‘	p
0	0	0	1	01			!	1	A	Q	a	q
0	0	1	0	02			“	2	B	R	b	r
0	0	1	1	03			#	3	C	S	c	s
0	1	0	0	04			$	4	D	T	d	t
0	1	0	1	05			%	5	E	U	e	u
0	1	1	0	06			&	6	F	V	f	v
0	1	1	1	07			‘	7	G	W	g	w
1	0	0	0	08			(	8	H	X	h	x
1	0	0	1	09			)	9	I	Y	i	y
1	0	1	0	10			*	:	J	Z	j	z
1	0	1	1	11			+	;	K	[	k	{
1	1	0	0	12			,	<	L	\	l	|
1	1	0	1	13			-	=	M	]	m	}
1	1	1	0	14			.	>	N	^	n	~
1	1	1	1	15			/	?	O	_	o	

Table 20 - Common Character Set

The following is an example of the use of the common character set to display the ‘Approved’ message in French without supporting the part of ISO 8859 that allows the relevant diacritic marks to be displayed.

If the terminal supports Part 1 of ISO 8859 (the Latin 1 alphabet) and supports the display of the standard messages in French, when a card indicates in its Language Preference that French is the preferred language, the terminal can display the 'Approved' message as 'Accepté', using the appropriate diacritic marks.

If the terminal does not support Part 1 of ISO 8859 (the Latin alphabet) but supports Part 8 (the Hebrew alphabet), the terminal is still able to support the display of the standard messages in French by using the common character set. When a card indicates in its Language Preference that French is the preferred language, the terminal can display the 'Approved' message as 'Accepte', without the use of diacritic marks. The cardholder should be able to comprehend the message.

Annex C - Example of Data Element Conversion

For the data elements listed in section 8.2 of this specification, the following table illustrates an example of the relationship between:

- The ICC-related data described in Book 3 *Application Specification* and the terminal-related data described in this specification.

- The data transmitted in messages as defined in ISO 8583:1987 and bit 55 from ISO 8583:1993

This does not imply that ISO 8583 is required as the message standard.

Tag	ICC Data	Bit	Message Data Name
'9F01'	Acquirer Identifier	32	Acquiring Institution Identification Code
'9F02' or '81'	Amount, Authorised	4 30	Amount, Transaction (authorisation) Amount, Original Transaction (batch data capture, financial transaction)
'9F04' or '9F03'	Amount, Other	54	Additional Amounts
'9F26'	AAC	55	ICC System-Related Data
'5F25'	Application Effective Date	see note 1	Date, Effective (YYMM only)
'5F24'	Application Expiration Date	14	Date, Expiration (YYMM only)
'82'	Application Interchange Profile	55	ICC System-Related Data
'5A'	Application PAN	2	PAN
'5F34'	Application PAN Sequence Number	23	Card Sequence Number
'9F36'	Application Transaction Counter	55	ICC System-Related Data
'9F07'	Application Usage Control	55	ICC System-Related Data
'9F28'	ARQC	55	ICC System-Related Data

Tag	ICC Data	Bit	Message Data Name
‘89’	Authorisation Code	38	Authorisation Identification Response
‘8A’	Authorisation Response Code	39	Response Code
‘9F27’	Cryptogram Information Data	55	ICC System-Related Data
‘8E’	CVM List	55	ICC System-Related Data
‘9F34’	CVM Results	55	ICC System-Related Data
--	Enciphered PIN Data	52	PIN Data
‘9F1E’	IFD Serial Number	see note 2	Card Accepting Device (CAD) Management
‘9F0D’	Issuer Action Code - Default	55	ICC System-Related Data
‘9F0E’	Issuer Action Code - Denial	55	ICC System-Related Data
‘9F0F’	Issuer Action Code - Online	55	ICC System-Related Data
‘BF10'	Issuer Application Data	55	ICC System-Related Data
‘91’	Issuer Authentication Data	55	ICC System-Related Data
‘5F28’	Issuer Country Code	20	Country Code, PAN Extended
‘71’ or ‘72’	Issuer Script Template 1 or 2	55	ICC System-Related Data
--	Issuer Script Results	55	ICC System-Related Data
‘9F15’	Merchant Category Code	18	Merchant Type
‘9F16’	Merchant Identifier	42	Card Acceptor Identification
‘9F39’	POS Entry Mode	22	POS Entry Mode (pos. 1-2)
‘5F30’	Service Code	40	Service Code
‘9F33’	Terminal Capabilities	see note 2	CAD Management

Tag	ICC Data	Bit	Message Data Name
‘9F1A’	Terminal Country Code	19 43	Acquiring Institution Country Code CAD Acceptor Name/Location (if terminal/acquirer countries are different)
‘9F1C’	Terminal Identification	41	Card Acceptor Terminal Identification
‘9F35’	Terminal Type	see note 2	CAD Management
‘95’	Terminal Verification Results	55	ICC System-Related Data
‘57’	Track 2 Equivalent Data	35	Track 2 Data
--	Transaction Amount	4	Amount, Transaction
‘9F29’	Transaction Certificate	55	ICC System-Related Data
‘5F2A’	Transaction Currency Code	49	Currency Code, Transaction
‘9A’	Transaction Date	13	Date, Local Transaction (MMDD only)
‘9F21’	Transaction Time	12	Time, Local Transaction
‘9C’	Transaction Type	3	Processing Code (pos. 1-2)
‘9F37’	Unpredictable Number	55	ICC System-Related Data

Table 21 - Data Element Conversion

Note 1: Only defined in ISO 8583:1993

Note 2: Only defined in additional/private data element of ISO 8583:1987 or ISO 8583:1993

THIS PAGE LEFT INTENTIONALLY BLANK

Annex D - Informative Terminal Guidelines

D1. Terminal Usage

In view of the installation of terminals within a various number of environments and locations, it is recognised that throughout the world different attempts have been made to group the relevant guidelines into different categories:

- Climatological conditions where the terminal is used (climatisation, outdoor, indoor)
- Mechanical conditions (such as vibration, shocks, drop-tests)
- Electronic restrictions (such as isolation, security, penetration)

The guidelines have been documented in industry standards established in Europe and the United States (see Annex D5 for informative references).

D2. Power Supply

D2.1 External Power Supply

The power supply provides the required voltage and current to all components of the terminal. The power supply should complies with the relevant national safety regulations.

D2.2 Battery Requirements

An internal battery is used to prevent loss of sensitive data residing in the terminal in case of power supply breakdown.

For portable terminals, the battery caters for the support of the necessary terminal functions (see the *Application Independent ICC to Terminal Interface Requirements* – Book 1 for power/current requirements).

Further power consumption reduction can be foreseen by energising the terminal automatically at card insertion.

D3. Key Pad

To prevent that characters printed on the keys of the key pad from becoming illegible after a while, precautions should be taken so that they:

- Have wear-resistant lettering
- Are able to function in normal operating environment including resistance to soft drink spills, alcohol, detergents, gasoline, etc.
- When operated as outdoor terminals, can resist the temperature ranges commonly encountered.

D4. Display

To cater for the visually disabled people, characters on the display are visible in all lighting conditions (bright overhead or dim diffuse light) and the size of the characters is large enough to be read from a distance of 1 meter.

D5. Informative References

IEC 950:1991	Safety of information technology equipment, including electrical business equipment, second edition. (Amendment 1-1992) (Amendment 2-1993)
IEC 801-2:1991	Electromagnetic compatibility for industrial-process measurement and control equipment - Part 2: Electrostatic discharge requirements, second edition
IEC 802-3:1984	Electromagnetic compatibility for industrial-process measurement and control equipment - Part 3: Radiated electromagnetic field requirements, first edition
IEC 801-4:1988	Electromagnetic compatibility for industrial-process measurement and control equipment - Part 4: Electrical fast transient/burst requirements, first edition
IEC 68-2-5:1975	Basic environmental testing procedures - Part 2: Tests - test Sa: Simulated solar radiation at ground level, first edition
IEC 68-2-6:1982	Basic environmental testing procedures - Part 2: Tests - test Fc and guidance: Vibration (sinusoidal), fifth edition. (Amendment 1: 1983) (Amendment 2: 1985)
IEC 68-2-11:1981	Basic environmental testing procedures - Part 2: Tests - test Ka: Salt mist, third edition
IEC 68-2-27:1987	Basic environmental testing procedures - Part 2: Tests - Guidance for damp heat tests, third edition
IEC 68-2-32:1975	Basic environmental testing procedures - Part 2: Tests - test Ed: Free fall, second edition. (Amendment 2-1990 incorporating Amendment 1)
EN 60-950:1988	Safety of information technology equipment including electrical business equipment
EN 41003:1993	Particular safety requirements for equipment to be connected to telecommunication networks

UL 1950:1993	Safety of information technology equipment including electrical business equipment
NF C 20-010:1992	Degrees of protection provided by enclosure (IP code)
NF C 98-310:1989	Financial transaction terminals[20]
NF C 98-020:1986	Telephone and telematic equipment. Electromagnetic compatibility

[20] This standard applies only to stand-alone terminals.

THIS PAGE LEFT INTENTIONALLY BLANK

Annex E - Examples of Terminals

For informational purposes only, this annex provides some examples of the physical and functional characteristics of terminals. Each example describes the setting of Terminal Type, Terminal Capabilities, and Additional Terminal Capabilities according to the specific terminal characteristics. This annex does not establish any requirements as such.

E1. Example 1 - POS Terminal or Electronic Cash Register

Characteristics	Example 1
Physical:	
Key pad	Attendant key pad (numeric and function keys) + PIN pad
Display	One for attendant One for cardholder
Printer	Yes for attendant
Magnetic stripe reader	Yes
IC reader	Yes
Functional:	
Language selection	Supports part 1 of ISO 8859
Transaction type	Goods, cashback
Static data authentication	Yes
Cardholder verification	Offline PIN, signature
Card capture	No
Online capable	Yes
Offline capable	Yes

Table 22 - Example of POS Terminal or Electronic Cash Register

The coding of the Terminal-Related Data for this example is the following:

- Terminal Type = ‘22’
- Terminal Capabilities, byte 1 = ‘E0’ (hexadecimal)
  byte 2 = ‘A0’ (hexadecimal)
  byte 3 = ‘80’ (hexadecimal)
- Additional Terminal Capabilities, byte 1 = ‘50’ (hexadecimal)
  byte 2 = ‘00’ (hexadecimal)
  byte 3 = ‘B0’ (hexadecimal)
  byte 4 = ‘B0’ (hexadecimal)
  byte 5 = ‘01’ (hexadecimal)

E2. Example 2 - ATM

Characteristics	Example 2
Physical:	
Key pad	PIN pad + function keys
Display	Yes for cardholder
Printer	Yes for cardholder
Magnetic stripe reader	Yes
IC reader	Yes
Functional:	
Language selection	Supports part 5 of ISO 8859
Transaction type	Cash, inquiry, transfer, payment
Static data authentication	Yes
Cardholder verification	Offline PIN, online PIN
Card capture	Yes
Online capable	Yes
Offline capable	No

Table 23 - Example of ATM

The coding of the Terminal-Related Data for this example is the following:

- Terminal Type = ‘14’

- Terminal Capabilities, byte 1 = ‘60’ (hexadecimal)
  byte 2 = ‘C0’ (hexadecimal)
  byte 3 = ‘A0’ (hexadecimal)

- Additional Terminal Capabilities, byte 1 = ‘8E’ (hexadecimal)
  byte 2 = ‘00’ (hexadecimal)
  byte 3 = ‘B0’ (hexadecimal)
  byte 4 = ‘50’ (hexadecimal)
  byte 5 = ‘05’ (hexadecimal)

E3. Example 3 - Vending Machine

Characteristics	**Example 3**
Physical:	
Key pad	Function keys
Display	No
Printer	No
Magnetic stripe reader	Yes
IC reader	Yes
Functional:	
Language selection	No
Transaction type	Goods
Static data authentication	Yes
Cardholder verification	No
Card capture	No
Online capable	No
Offline capable	Yes

Table 24 - Example of Vending Machine

The coding of the Terminal-Related Data for this example is the following:

- Terminal Type = ‘26’

- Terminal Capabilities, byte 1 = ‘60’ (hexadecimal)

byte 2 = ‘00’ (hexadecimal)
byte 3 = ‘80’ (hexadecimal)

- Additional Terminal Capabilities, byte 1 = ‘40’ (hexadecimal)
  byte 2 = ‘00’ (hexadecimal)
  byte 3 = ‘10’ (hexadecimal)
  byte 4 = ‘00’ (hexadecimal)
  byte 5 = ‘00’ (hexadecimal)