

EMV[®]

Integrated Circuit Card Specifications for Payment Systems

Book 4

Cardholder, Attendant, and Acquirer Interface Requirements

Version 4.4
October 2022

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

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

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

Revision Log – Version 4.4

The following changes have been made to Book 4 since the publication of Version 4.3. Numbering and cross references in this version have been updated to reflect changes introduced by the published bulletins.

Incorporated changes described in the following Specification Bulletins:

- Specification Bulletin no. 103 : Unpredictable Number generation
- Specification Bulletin no. 144: Terminal Unpredictable Number generation
- Specification Bulletin no. 148: Clarification on Terminal Support of Multiple Application Version Numbers per AID
- Specification Bulletin no. 151: Clarification on Cardholder Selection and Cardholder Confirmation
- Specification Bulletin no. 163: Changes to PIN Pad requirements
- Specification Bulletin no. 164: Electronic Signature Capture and Electronic Receipt Delivery
- Specification Bulletin no. 178, Third Edition: Tokenisation Data Objects – Payment Account Reference (PAR)
- Specification Bulletin no. 185, Second Edition: Biometric Terminal Specification
- Specification Bulletin 197: Tokenisation Data Objects – Token Requestor ID and Last 4 Digits of PAN
- Specification Bulletin no. 220, Second Edition: EMV® Contact Kernel Output
- Specification Bulletin no. 231: Issuer Identification Number Extended (IINE)
- Specification Bulletin no. 243: Introduction of XDA/ODE for EMV Specifications

Minor editorial clarifications and corrections, including those described in the following:

- Specification Bulletin no. 243: Introduction of XDA/ODE for EMV Specifications

Contents

Part I – General

1	Scope	12
1.1	Changes in Version 4.4	12
1.2	Structure	12
1.3	Underlying Standards	13
1.4	Audience	14
2	Normative References	15
3	Definitions	18
4	Abbreviations, Notations, Conventions, and Terminology	26
4.1	Abbreviations	26
4.2	Notations	33
4.3	Data Element Format Conventions	35
4.4	Terminology	36

Part II – General Requirements

5	Terminal Types and Capabilities	38
5.1	Terminal Types	38
5.2	Terminal Capabilities	39
5.3	Terminal Configurations	40
6	Functional Requirements	43
6.1	Application Independent ICC to Terminal Interface Requirements	43
6.2	Security and Key Management	43
6.3	Application Specification	43
6.3.1	Initiate Application Processing	44
6.3.2	Offline Data Authentication	44
6.3.3	Processing Restrictions	47
6.3.4	Cardholder Verification Processing	47
6.3.5	Terminal Risk Management	53
6.3.6	Terminal Action Analysis	53
6.3.7	Card Action Analysis	54
6.3.8	Online Processing	55
6.3.9	Issuer-to-Card Script Processing	55
6.4	Conditions for Support of Functions	56
6.5	Other Functional Requirements	57

6.5.1	Amount Entry and Management	57
6.5.2	Voice Referrals	57
6.5.3	Transaction Forced Online	58
6.5.4	Transaction Forced Acceptance	58
6.5.5	Transaction Sequence Counter	59
6.5.6	Unpredictable Number	59
6.6	Card Reading	59
6.6.1	IC Reader	60
6.6.2	Exception Handling	60
6.7	Date Management	61
6.7.1	Data Authentication	61
6.7.2	Processing Restrictions	61
6.7.3	Date Management	61
7	Physical Characteristics	62
7.1	Keypad	62
7.1.1	Command Keys	63
7.1.2	PIN Pad	64
7.2	Display	65
7.3	Memory Protection	65
7.4	Clock	65
7.5	Receipt Printer	65
7.6	Magnetic Stripe Reader	66

Part III – Software Architecture

8	Terminal Software Architecture	68
8.1	Environmental Changes	68
8.2	Application Libraries	69
8.3	Application Program Interface	70
8.4	Interpreter	71
8.4.1	Concept	71
8.4.2	Virtual Machine	72
8.4.3	Kernel	72
8.4.4	Application Code Portability	72
8.4.5	Kernel Output	73
8.5	Plugs and Sockets	75
8.6	Biometric Terminal	77
9	Software Management	78
10	Data Management	79
10.1	Application Independent Data	79

10.1.1	Terminal Related Data	79
10.1.2	Transaction Related Data	80
10.2	Application Dependent Data	81

Part IV – Cardholder, Attendant, and Acquirer Interface

11	Cardholder and Attendant Interface	85
11.1	Language Selection	85
11.2	Standard Messages	86
11.3	Application Selection	89
11.4	Receipt	89
12	Acquirer Interface	90
12.1	Message Content	90
12.1.1	Authorisation Request	92
12.1.2	Financial Transaction Request	94
12.1.3	Authorisation or Financial Transaction Response	96
12.1.4	Financial Transaction Confirmation	97
12.1.5	Batch Data Capture	97
12.1.6	Reconciliation	100
12.1.7	Online Advice	101
12.1.8	Reversal	103
12.2	Exception Handling	105
12.2.1	Unable to Go Online	105
12.2.2	Downgraded Authorisation	106
12.2.3	Authorisation Response Incidents	106
12.2.4	Script Incidents	107
12.2.5	Advice Incidents	107

Part V – Annexes

Annex A	Coding of Terminal Data Elements	109
A1	Terminal Type	109
A2	Terminal Capabilities	110
A3	Additional Terminal Capabilities	112
A4	CVM Results	115
A5	Issuer Script Results	116
A6	Authorisation Response Code	116
A7	Biometric Terminal Capabilities	117

Annex B	Common Character Set	119
Annex C	Example Data Element Conversion	121
Annex D	Informative Terminal Guidelines	124
D1	Terminal Usage	124
D2	Power Supply	124
D2.1	External Power Supply	124
D2.2	Battery Requirements	124
D3	Keypad	125
D4	Display	125
D5	Informative References	125
Annex E	Examples of Terminals	127
E1	Example 1 – POS Terminal or Electronic Cash Register	128
E2	Example 2 – ATM	129
E3	Example 3 – Vending Machine	130
Index		131

Tables

Table 1: Terms Describing Terminal Types	38
Table 2: Setting of CVM Results, TVR bits, and TSI bits following CVM Processing	51
Table 3: Card Action Analysis	54
Table 4: Key Types	62
Table 5: Command Keys	63
Table 6: Command Key Colours	63
Table 7: Application Dependent Data Elements	81
Table 8: Standard Messages	87
Table 9: ICC-specific Authorisation Request Data Elements	92
Table 10: Existing Authorisation Request Data Elements	93
Table 11: ICC-specific Financial Transaction Request Data Elements	94
Table 12: Existing Financial Transaction Request Data Elements	95
Table 13: ICC-specific Authorisation or Financial Transaction Response Data Elements	96
Table 14: Existing Authorisation or Financial Transaction Response Data Elements	96
Table 15: ICC-specific Financial Transaction Confirmation Data Elements	97
Table 16: Existing Financial Transaction Confirmation Data Elements	97
Table 17: ICC-specific Batch Data Capture Data Elements	98
Table 18: Existing Batch Data Capture Data Elements	99
Table 19: Existing Reconciliation Data Elements	100
Table 20: ICC-specific Online Advice Data Elements	101
Table 21: Existing Online Advice Data Elements	102
Table 22: ICC-specific Reversal Data Elements	103
Table 23: Existing Reversal Data Elements	104

Annexes

Table 24: Terminal Type	109
Table 25: Terminal Capabilities Byte 1 – Card Data Input Capability	110
Table 26: Terminal Capabilities Byte 2 – CVM Capability	111
Table 27: Terminal Capabilities Byte 3 – Security Capability	111
Table 28: Add'l Term. Capabilities Byte 1 – Transaction Type Capability	112
Table 29: Add'l Term. Capabilities Byte 2 – Transaction Type Capability	113
Table 30: Add'l Term. Capabilities Byte 3 – Terminal Data Input Capability	113
Table 31: Add'l Term. Capabilities Byte 4 – Term. Data Output Capability	114
Table 32: Add'l Term. Capabilities Byte 5 – Term. Data Output Capability	115
Table 33: CVM Results	115
Table 34: Issuer Script Results	116
Table 35: Authorisation Response Codes	116
Table 36: Biometric Term. Cap. Byte 1 – Offline Biometric Capabilities	117
Table 37: Biometric Term. Cap. Byte 2 – Online Biometric Capabilities	118
Table 38: Biometric Terminal Capabilities Byte 3 – RFU	118
Table 39: Common Character Set	119
Table 40: Data Element Conversion	121
Table 41: Example of POS Terminal or Electronic Cash Register	128

Table 42: Example of ATM	129
Table 43: Example of Vending Machine	130

Figures

Figure 1: Example of an Attended Terminal	40
Figure 2: Example of a Merchant Host	41
Figure 3: Example of a Cardholder-Controlled Terminal	42
Figure 4: PIN Pad Layout	64
Figure 5: Terminal Software	69
Figure 6: Socket/Plug Relationship	76
Figure 7: Architecture of Biometric Terminal and Card	77

Part I

General

1 Scope

This document, the *Integrated Circuit Card Specifications for Payment Systems - Book 4, 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 other documents of the *Integrated Circuit Card Specifications for Payment Systems*, all available on <http://www.emvco.com>:

- Book 1 – Application Independent ICC to Terminal Interface Requirements
- Book 2 – Security and Key Management
- Book 3 – Application Specification

1.1 Changes in Version 4.4

This release incorporates all relevant Specification Bulletins, Application Notes, amendments, etc. published up to the date of this release.

The Revision Log at the beginning of the Book provides additional detail about changes to this specification.

1.2 Structure

Book 4 consists of the following parts:

- Part I - **General**
- Part II - **General Requirements**
- Part III - **Software Architecture**
- Part IV - **Cardholder, Attendant, and Acquirer Interface**
- Part V - **Annexes**

Part I includes this introduction, as well as data applicable to all Books: normative references, definitions, abbreviations, notations, data element format convention, and terminology.

Part II addresses:

- Functional requirements, such as those emerging from the other Books of the *Integrated Circuit Card Specifications for Payment Systems*
- General physical characteristics

Part III addresses software architecture including software and data management.

Part IV discusses:

- Cardholder and attendant interface
- Acquirer interface

Part V discusses the coding of terminal data elements, lists the common character set, provides an example data element conversion, includes informative terminal guidelines, and provides examples of the physical and functional characteristics of terminals.

The Book also includes a revision log and an index.

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.

This specification defines 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.

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 cover application-specific terminal requirements unique to individual payment systems and those functions not required to support interchange.
- Does not address cardholder or merchant operating procedures, which are established by individual payment systems.
- 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 that will provide more detailed specifications applicable to terminal implementations.

1.3 Underlying Standards

This specification is based on the ISO/IEC 7816 series of standards and should be read in conjunction with those standards. However, if any of the provisions or definitions in this specification differ from those standards, the provisions herein shall take precedence.

1.4 Audience

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

2 Normative References

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

EMV Contact Interface Specification	EMV Level 1 Specifications for Payment Systems, EMV Contact Interface Specification
EMV Tokenisation Framework	EMV Payment Tokenisation Specification – Technical Framework Framework specification for an interoperable Payment Tokenisation solution.
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
IEEE P1363	Standard Specifications For Public-Key Cryptography
ISO 639-1	Codes for the representation of names of languages – Part 1: Alpha-2 Code Note: This standard is updated continuously by ISO. Additions/changes to ISO 639-1:1988: Codes for the Representation of Names of Languages are available on: http://www.loc.gov/standards/iso639-2/php/code_changes.php
ISO 3166	Codes for the representation of names of countries and their subdivisions
ISO 4217	Codes for the representation of currencies and funds
ISO/IEC 7812-1	Identification cards – Identification of issuers — Part 1: Numbering System
ISO/IEC 7813	Identification cards – Financial transaction cards
ISO/IEC 7816-4	Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange
ISO/IEC 7816-5	Identification cards — Integrated circuit cards — Part 5: Registration of application providers
ISO/IEC 7816-6	Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange

ISO/IEC 7816-11	Identification cards – Integrated circuit cards – Personal verification through biometric methods
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/IEC 8825-1	Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
ISO/IEC 8859	Information processing – 8-bit single-byte coded graphic character sets
ISO 9362	Banking – Banking telecommunication messages – Bank identifier codes
ISO 9564-1	Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems
ISO/IEC 9796-2	Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms
ISO/IEC 9797-1	Information technology – Security techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2	Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 10116	Information technology – Security techniques – Modes of operation for an <i>n</i> -bit block cipher
ISO/IEC 10118-3	Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions
ISO/IEC 11770-6	Information technology – Security techniques – Key management – Part 6: Key derivation
ISO 13616	Banking and related financial services – International bank account number (IBAN)

ISO/IEC 14888-3	Information technology – Security techniques – Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms
ISO/IEC 15946-1	Information technology – Security techniques – Cryptographic techniques based on elliptic curves — Part 1: General
ISO/IEC 15946-5	Information technology – Security techniques – Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation
ISO 16609	Banking – Requirements for message authentication using symmetric techniques
ISO/IEC 18031	Information technology – Security techniques – Random bit generation
ISO/IEC 18033-2	Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers
ISO/IEC 18033-3	Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers
ISO/IEC 19772	Information technology – Security techniques – Authenticated encryption
ISO/IEC 19785-3	Information technology – Common Biometric Exchange Formats Framework – Patron format specifications
ISO/IEC 19794	Information technology – Biometric data interchange formats
ISO/IEC 19794-2	Information technology – Biometric data interchange formats – Part 2: Finger minutiae data
SEC 1	Elliptic Curve Cryptography (available at http://www.secg.org)

3 Definitions

The following terms are used in one or more books of these specifications.

Application	The application protocol between the card and the terminal and its related set of data.
Application Authentication Cryptogram	An Application Cryptogram generated by the card when declining a transaction.
Application Cryptogram	A cryptogram generated by the card in response to a GENERATE AC command. See also: <ul style="list-style-type: none">• Application Authentication Cryptogram• Authorisation Request Cryptogram• Transaction Certificate
Authentication	The provision of assurance of the claimed identity of an entity or of data origin.
Authorisation Request Cryptogram	An Application Cryptogram generated by the card when requesting online authorisation.
Authorisation Response Cryptogram	A cryptogram generated by the issuer in response to an Authorisation Request Cryptogram.
Biometric Data Block	<p>A block of data with a specific format that contains information captured from a biometric capture device and that could be used as follows:</p> <ul style="list-style-type: none">• stored in the card as part of the biometric reference template• sent to the ICC in the data field of the PIN CHANGE/UNBLOCK command• sent to the ICC in the data field of the VERIFY command for offline biometric verification• sent online for verification <p>The format of the BDB is outside the scope of this specification.</p>

Biometric Reference Template	Biometric data stored in the card as reference. Data provided by a biometric capture device would be compared against the biometric reference template to determine a match.
Biometric Verification	The process of determining that the biometrics presented, such as finger, palm, iris, voice, or facial, are valid.
Byte	8 bits.
Card	A payment card as defined by a payment system.
Certificate	The public key and identity of an entity together with some other information, rendered unforgeable by signing with the private key of the certification authority which issued that certificate.
Certification Authority	Trusted third party that establishes a proof that links a public key and other relevant information to its owner.
Ciphertext	Enciphered information.
Combined DDA/Application Cryptogram Generation	A form of offline dynamic data authentication.
Command	A message sent by the terminal to the ICC that initiates an action and solicits a response from the ICC.
Command Chaining	A mechanism where consecutive command-response pairs can be chained.
Compromise	The breaching of secrecy or security.
Concatenation	Two elements are concatenated by appending the bytes from the second element to the end of the first. Bytes from each element are represented in the resulting string in the same sequence in which they were presented to the terminal by the ICC, that is, most significant byte first. Within each byte bits are ordered from most significant bit to least significant. A list of elements or objects may be concatenated by concatenating the first pair to form a new element, using that as the first element to concatenate with the next in the list, and so on.

Contact	A conducting element ensuring galvanic continuity between integrated circuit(s) and external interfacing equipment.
Cryptogram	Result of a cryptographic operation.
Cryptographic Algorithm	An algorithm that transforms data in order to hide or reveal its information content.
Data Integrity	The property that data has not been altered or destroyed in an unauthorised manner.
Decipherment	The reversal of a corresponding encipherment.
DEM1	A family of data encapsulation mechanisms defined in ISO/IEC 18033-2.
Digital Signature	An asymmetric cryptographic transformation of data that allows the recipient of the data to prove the origin and integrity of the data, and protect the sender and the recipient of the data against forgery by third parties, and the sender against forgery by the recipient.
Dynamic Data Authentication	A form of offline dynamic data authentication
Elliptic Curve Cryptography	Public key cryptography based on the algebraic structure of elliptic curves over finite fields.
Encipherment	The reversible transformation of data by a cryptographic algorithm to produce ciphertext.
Exclusive-OR	Binary addition with no carry, giving the following values: $0 + 0 = 0$ $0 + 1 = 1$ $1 + 0 = 1$ $1 + 1 = 0$
Extended Data Authentication	A form of offline dynamic data authentication.
Facial Verification	The process of determining that the face presented is valid.
Financial Transaction	The act between a cardholder and a merchant or acquirer that results in the exchange of goods or services against payment.

Finger Verification	The process of determining that the finger presented is valid.
Function	A process accomplished by one or more commands and resultant actions that are used to perform all or part of a transaction.
Hash Function	<p>A function that maps strings of bits to fixed-length strings of bits, satisfying the following two properties:</p> <ul style="list-style-type: none">• It is computationally infeasible to find for a given output an input which maps to this output.• It is computationally infeasible to find for a given input a second input that maps to the same output. <p>Additionally, if the hash function is required to be collision-resistant, it must also satisfy the following property:</p> <ul style="list-style-type: none">• It is computationally infeasible to find any two distinct inputs that map to the same output.
Hash Result	The string of bits that is the output of a hash function.
I2OSP	An integer to octet string conversion primitive function defined in ISO/IEC 18033-2.
Integrated Circuit(s)	Electronic component(s) designed to perform processing and/or memory functions.
Integrated Circuit(s) Card	A 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 as may be considered part of it.
Iris Verification	The process of determining that the iris presented is valid.
Issuer Action Code	<p>Any of the following, which reflect the issuer-selected action to be taken upon analysis of the TVR:</p> <ul style="list-style-type: none">• Issuer Action Code – Default• Issuer Action Code – Denial• Issuer Action Code – Online

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	A sequence of symbols that controls the operation of a cryptographic transformation.
Key Introduction	The process of generating, distributing, and beginning use of a key pair.
Key Withdrawal	The process of removing a key from service as part of its revocation.
Keypad	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.
Logical Compromise	The compromise of a key through application of improved cryptanalytic techniques, increases in computing power, or combination of the two.
Magnetic Stripe	The stripe containing magnetically encoded information.
Message	A string of bytes sent by the terminal to the card or vice versa, excluding transmission-control characters.
Message Authentication Code	A symmetric cryptographic transformation of data that protects the sender and the recipient of the data against forgery by third parties.
Nibble	The four most significant or least significant bits of a byte.
Offline Data Encipherment	Offline encipherment of data, in particular for cardholder PIN and biometric data. See Book 2.
Padding	Appending extra bits to either side of a data string.
Palm Verification	The process of determining that the palm presented is valid.

Path	Concatenation of file identifiers without delimitation.
Payment System Environment	A logical construct within the ICC, the entry point to which is a Directory Definition File (DDF) named '1PAY.SYS.DDF01'. This DDF contains a Payment System Directory which in turn contains entries for one or more Application Definition Files (ADFs) which are formatted according to this specification.
Physical Compromise	The compromise of a key resulting from the fact that it has not been securely guarded, or a hardware security module has been stolen or accessed by unauthorised persons.
PIN Pad	Arrangement of numeric and command keys to be used for personal identification number (PIN) entry. Also known as a “PIN Entry Device” (PED).
Plaintext	Unenciphered information.
Potential Compromise	A condition where cryptanalytic techniques and/or computing power has advanced to the point that compromise of a key of a certain length is feasible or even likely.
Private Key	That key of an entity’s asymmetric key pair that should only be used by that entity. In the case of a digital signature scheme, the private key defines the signature function.
Public Key	That key of an entity’s asymmetric key pair that can be made public. In the case of a digital signature scheme, the public key defines the verification function.
Public Key Certificate	The public key information of an entity signed by the certification authority and thereby rendered unforgeable.
Response	A message returned by the ICC to the terminal after the processing of a command message received by the ICC.
RSA-KEM	A family of key encapsulation mechanisms defined in ISO/IEC 18033-2.
RSATransform	The RSA exponentiation that is used for encryption and decryption, and generating and verifying a signature.

Script	A command or a string of commands transmitted by the issuer to the terminal for the purpose of being sent serially to the ICC as commands.
Secret Key	A key used with symmetric cryptographic techniques and usable only by a set of specified entities.
Socket	An execution vector defined at a particular point in an application and assigned a unique number for reference.
Static Data Authentication	Offline static data authentication
Symmetric Cryptographic Technique	A cryptographic technique that uses the same secret key for both the originator's and recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.
Template	Value field of a constructed data object, defined to give a logical grouping of data objects.
Terminal	The 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.
Terminal Action Code	Any of the following, which reflect the acquirer-selected action to be taken upon analysis of the TVR: <ul style="list-style-type: none">• Terminal Action Code – Default• Terminal Action Code – Denial• Terminal Action Code – Online
Terminate Card Session	End the card session by deactivating the IFD contacts according to EMV Contact Interface Specification and displaying a message indicating that the ICC cannot be used to complete the transaction.
Terminate Transaction	Stop the current application and deactivate the card.
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.

Transaction Certificate	An Application Cryptogram generated by the card when accepting a transaction.
Virtual Machine	A theoretical microprocessor architecture that forms the basis for writing application programs in a specific interpreter software implementation.
Voice Verification	The process of determining that the voice presented is valid.

4 Abbreviations, Notations, Conventions, and Terminology

4.1 Abbreviations

a	Alphabetic (see section 4.3, Data Element Format Conventions)
AAC	Application Authentication Cryptogram
AAD	Additional Authenticated Data
AC	Application Cryptogram
ADF	Application Definition File
AEF	Application Elementary File
AES	Advanced Encryption Standard
AFL	Application File Locator
AID	Application Identifier
AIP	Application Interchange Profile
an	Alphanumeric (see section 4.3)
ans	Alphanumeric Special (see section 4.3)
APDU	Application Protocol Data Unit
API	Application Program Interface
ARC	Authorisation Response Code
ARPC	Authorisation Response Cryptogram
ARQC	Authorisation Request Cryptogram
ASI	Application Selection Indicator
ASN	Abstract Syntax Notation
ATC	Application Transaction Counter
ATM	Automated Teller Machine
ATR	Answer to Reset

AUC	Application Usage Control
b	Binary (see section 4.3)
BCD	Binary Coded Decimal
BDB	Biometric Data Block
BEK	Biometric Encryption Key
BER	Basic Encoding Rules (defined in ISO/IEC 8825-1)
BHT	Biometric Header Template
BIC	Bank Identifier Code
BIT	Biometric Information Template
BMK	Biometric MAC Key
CA	Certification Authority
CAD	Card Accepting Device
C-APDU	Command APDU
CBC	Cipher Block Chaining
CBEFF	Common Biometric Exchange Formats Framework
CCD	Common Core Definitions
CCI	Common Core Identifier
CCYYMMDD	Year (4 digits), Month, Day
CDA	Combined DDA/Application Cryptogram Generation
CDOL	Card Risk Management Data Object List
CID	Cryptogram Information Data
CLA	Class Byte of the Command Message
cn	Compressed Numeric (see section 4.3)
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSU	Card Status Update
CV	Cryptogram Version
CV Rule	Cardholder Verification Rule

CVM	Cardholder Verification Method
CVR	Card Verification Results
DDA	Dynamic Data Authentication
DDF	Directory Definition File
DDOL	Dynamic Data Authentication Data Object List
DES	Data Encryption Standard
DF	Dedicated File
DIR	Directory
DOL	Data Object List
ECB	Electronic Code Book
EC-SDSA	Elliptic Curve Schnorr Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EF	Elementary File
EN	European Norm
FC	Format Code
FCI	File Control Information
Hex	Hexadecimal
HHMMSS	Hours, Minutes, Seconds
HMAC	Keyed-hash Message Authentication Code
I/O	Input/Output
IAC	Issuer Action Code (Denial, Default, Online)
IAD	Issuer Application Data
IBAN	International Bank Account Number
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ICCD	Issuer Certified Card Data
IEC	International Electrotechnical Commission
IFD	Interface Device

IIN	Issuer Identification Number
IINE	Issuer Identification Number Extended
INS	Instruction Byte of Command Message
ISO	International Organization for Standardization
KD	Key Derivation
KDF	Key Derivation Function
K_M	Master Key
K_S	Session Key
L	Length
l.s.	Least Significant
Lc	Exact Length of Data Sent by the TAL in a Case 3 or 4 Command
LCOL	Lower Consecutive Offline Limit
L_{DD}	Length of the ICC Dynamic Data
Le	Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command
Lr	Length of Response Data Field
LRC	Longitudinal Redundancy Check
M	Mandatory
m.s.	Most Significant
MAC	Message Authentication Code
max.	Maximum
MF	Master File
MK	ICC Master Key for session key generation
MMDD	Month, Day
MMYY	Month, Year
n	Numeric (see section 4.3)
N_{CA}	Length of the Certification Authority Public Key Modulus

NF	Norme Française
N_{FIELD}	Length of a finite field element
N_{HASH}	Output length of a hash function
N_I	Length of the Issuer Public Key Modulus
N_{IC}	Length of the ICC Public Key Modulus
NIST	National Institute for Standards and Technology
N_{PE}	Length of the ICC PIN Encipherment Public Key Modulus
N_{SIG}	Length of an ECC Digital Signature
O	Optional
O/S	Operating System
ODA	Offline Data Authentication
ODE	Offline Data Encipherment
P1	Parameter 1
P2	Parameter 2
PAN	Primary Account Number
PAR	Payment Account Reference
PC	Personal Computer
P_{CA}	Certification Authority Public Key
PDOL	Processing Options Data Object List
P_I	Issuer Public Key
P_{IC}	ICC Public Key
PIN	Personal Identification Number
PIX	Proprietary Application Identifier Extension
POS	Point of Service
pos.	Position
PSE	Payment System Environment
R-APDU	Response APDU

RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
RSA	Rivest, Shamir, Adleman Algorithm
S _{CA}	Certification Authority Private Key
SDA	Static Data Authentication
SDAD	Signed Dynamic Application Data
SFI	Short File Identifier
SHA-1	Secure Hash Algorithm 1
SHA-2	Secure Hash Algorithm 2 (includes SHA-256 and SHA-512)
SHA-256	Secure Hash Algorithm 256
SHA-3	Secure Hash Algorithm 3
S _I	Issuer Private Key
S _{IC}	ICC Private Key
SK	Session Key
SW1	Status Byte One
SW2	Status Byte Two
TAA	Terminal Action Analysis
TAC	Terminal Action Code(s) (Default, Denial, Online)
TAL	Terminal Application Layer
TC	Transaction Certificate
TDOL	Transaction Certificate Data Object List
TLV	Tag Length Value
TPDU	Transport Protocol Data Unit
TSI	Transaction Status Information
TVR	Terminal Verification Results
UCOL	Upper Consecutive Offline Limit
UL	Underwriters Laboratories Incorporated
UN	Unpredictable Number

var.	Variable (see section 4.3)
XDA	Extended Data Authentication
YYMM	Year, Month
YYMMDD	Year, Month, Day

4.2 Notations

'0' to '9' and 'A' to 'F'	16 hexadecimal characters
xx	Any value
$A := B$	A is assigned the value of B
$A = B$	Value of A is equal to the value of B
$A \equiv B \pmod n$	Integers A and B are congruent modulo the integer n, that is, there exists an integer d such that $(A - B) = dn$
$A \pmod n$	The reduction of the integer A modulo the integer n, that is, the unique integer r, $0 \leq r < n$, for which there exists an integer d such that $A = dn + r$
A / n	The integer division of A by n, that is, the unique integer d for which there exists an integer r, $0 \leq r < n$, such that $A = dn + r$
$Y := \text{ALG}(K)[X]$	Encipherment of a data block X with a block cipher as specified in Book 2 section A1, using a secret key K
$X = \text{ALG}^{-1}(K)[Y]$	Decipherment of a data block Y with a block cipher as specified in Book 2 section A1, using a secret key K
$Y := \text{Sign}(S_K)[X]$	The signing of a data block X with an asymmetric reversible algorithm as specified in Book 2 section A2, using the private key S_K
$X = \text{Recover}(P_K)[Y]$	The recovery of the data block X with an asymmetric reversible algorithm as specified in Book 2 section A2, using the public key P_K
$C := (A B)$	The concatenation of an n -bit number A and an m -bit number B, which is defined as $C = 2^m A + B$.
Leftmost	Applies to a sequence of bits, bytes, or digits and used interchangeably with the term “most significant”. If $C = (A B)$ as above, then A is the leftmost n bits of C.

Rightmost	Applies to a sequence of bits, bytes, or digits and used interchangeably with the term “least significant”. If $C = (A \parallel B)$ as above, then B is the rightmost m bits of C.
$H := \text{Hash}[\text{MSG}]$	Hashing of a message MSG of arbitrary length using a 160-bit hash function
$X \oplus Y$	The symbol ' \oplus ' denotes bit-wise exclusive-OR and is defined as follows: $X \oplus Y$ The bit-wise exclusive-OR of the data blocks X and Y. If one data block is shorter than the other, then it is first padded to the left with sufficient binary zeros to make it the same length as the other.
$\text{MIN}(x, y)$	The smaller of values x and y.

4.3 Data Element Format Conventions

The EMV specifications use the following data element formats:

- a Alphabetic data elements contain a single character per byte. The permitted characters are alphabetic only (a to z and A to Z, upper and lower case).
- an Alphanumeric data elements contain a single character per byte. The permitted characters are alphabetic (a to z and A to Z, upper and lower case) and numeric (0 to 9).

There is one exception: The permitted characters for Payment Account Reference are alphabetic *upper case* (A to Z) and numeric (0 to 9).
- ans Alphanumeric Special data elements contain a single character per byte. The permitted characters and their coding are shown in the Common Character Set table in Book 4 Annex B.

There is one exception: The permitted characters for Application Preferred Name are the non-control characters defined in the ISO/IEC 8859 part designated in the Issuer Code Table Index associated with the Application Preferred Name.
- b These data elements consist of either unsigned binary numbers or bit combinations that are defined elsewhere in the specification.

Binary example: The Application Transaction Counter (ATC) is defined as “b” with a length of two bytes. An ATC value of 19 is stored as Hex '00 13'.

Bit combination example: Processing Options Data Object List (PDOL) is defined as “b” with the format shown in Book 3 section 5.4.
- cn Compressed numeric data elements consist of two numeric digits (having values in the range Hex '0'–'9') per byte. These data elements are left justified and padded with trailing hexadecimal 'F's.

Example: The Application Primary Account Number (PAN) is defined as “cn” with a length of up to ten bytes. A value of 1234567890123 may be stored in the Application PAN as Hex '12 34 56 78 90 12 3F FF' with a length of 8.
- n Numeric data elements consist of two numeric digits (having values in the range Hex '0' – '9') per byte. These digits are right justified and padded with leading hexadecimal zeroes. Other specifications sometimes refer to this data format as Binary Coded Decimal (“BCD”) or unsigned packed.

Example: Amount, Authorised (Numeric) is defined as “n 12” with a length of six bytes. A value of 12345 is stored in Amount, Authorised (Numeric) as Hex '00 00 00 01 23 45'.
- var. Variable data elements are variable length and may contain any bit combination. Additional information on the formats of specific variable data elements is available elsewhere.

4.4 Terminology

business agreement	An agreement reached between a payment system and its business partner(s).
proprietary	Not defined in this specification and/or outside the scope of this specification
shall	Denotes a mandatory requirement
should	Denotes a recommendation

Part II

General Requirements

5 Terminal Types and Capabilities

5.1 Terminal Types

As described in section 1, 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

Table 1 defines the terms used to describe terminal types.

Term	Definition
Attended	An attendant (an 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 normally only be approved in real time by transmission of an authorisation request 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	Identifies the entity responsible for the operation of the terminal. This does not necessarily equate to the actual owner of the terminal.

Table 1: Terms Describing Terminal Types

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.

5.2 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/IEC 8859 supported by the terminal.

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

5.3 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).

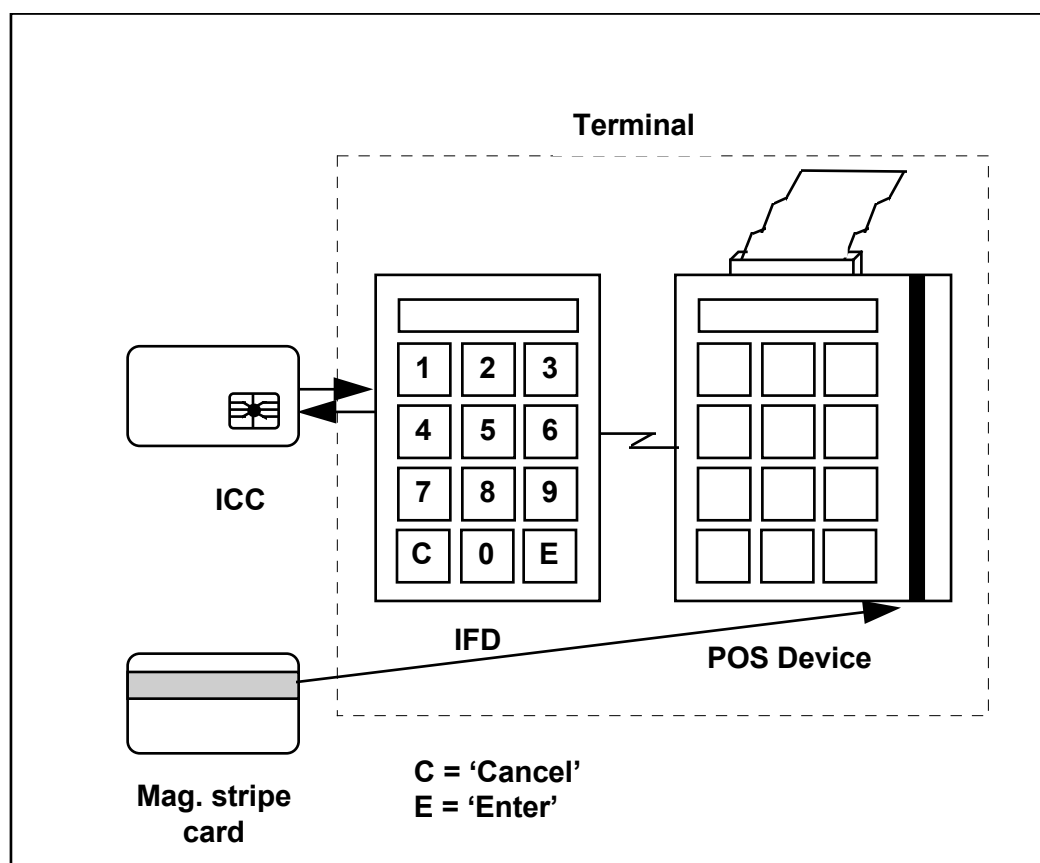


Figure 1: Example of an Attended Terminal

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

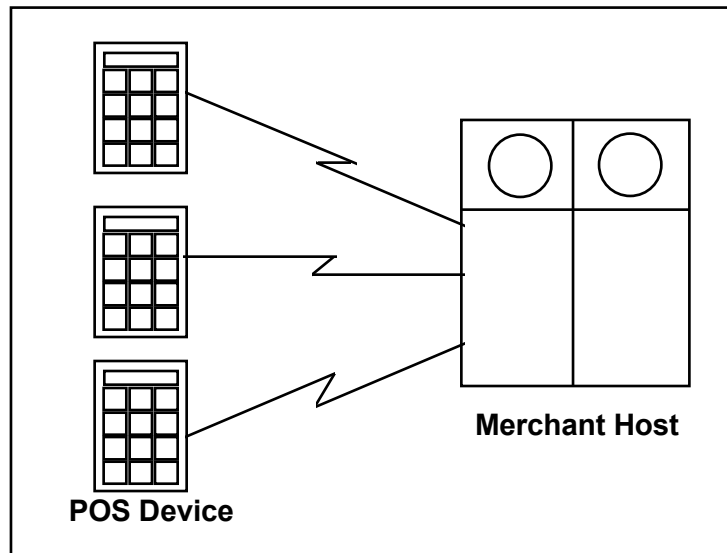


Figure 2: Example of a Merchant Host

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 10 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.

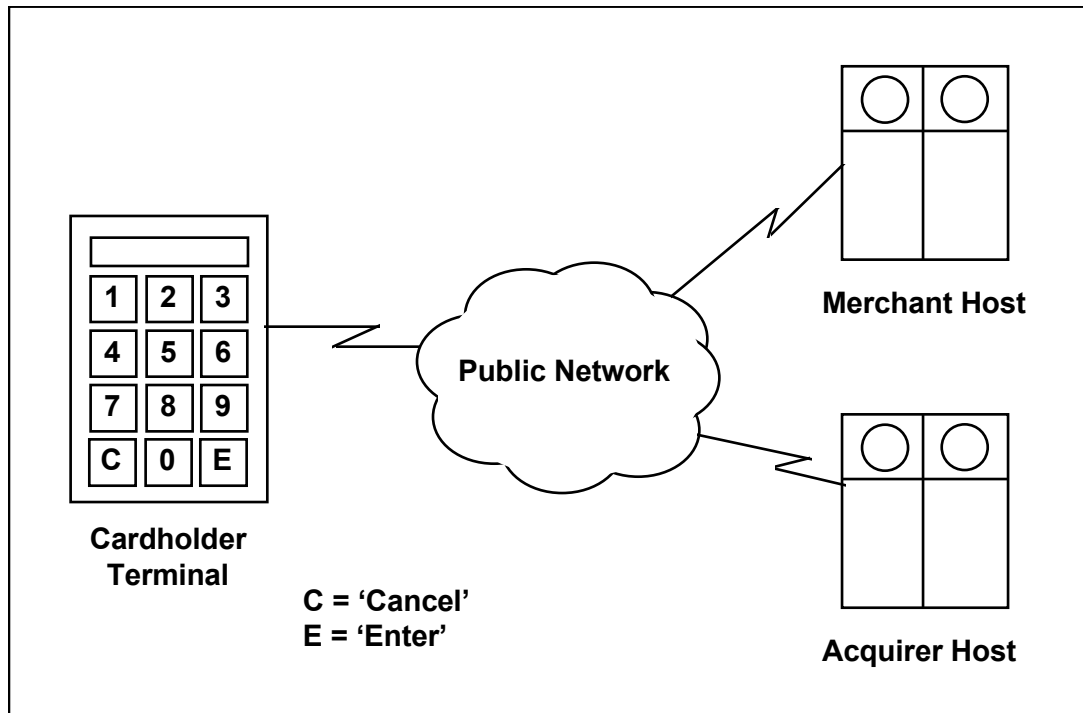


Figure 3: Example of a Cardholder-Controlled Terminal

6 Functional Requirements

This Book does not replicate the other Books of the *Integrated Circuit Card Specifications for Payment Systems* but describes the implementation issues and the impact of those Books on the terminal.

This section uses standard messages described in section 11.2 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.

6.1 Application Independent ICC to Terminal Interface Requirements

The terminal shall comply with all Parts of Book 1. It shall support all data elements and commands subject to the conditions described in section 6.3.

6.2 Security and Key Management

The terminal shall comply with all Parts of Book 2. It shall support all data elements and commands subject to the conditions described in section 6.3.

6.3 Application Specification

The terminal shall comply with all Parts of Book 3. It shall support all functions subject to the conditions described in this section.

Sections 6.3.1 to 6.3.9 expand upon the terminal functions described in Book 3.

6.3.1 Initiate Application Processing

When the Processing Options Data Object List (PDOL) includes an amount field (either Amount, Authorised or Amount, Other), an attended terminal (Terminal Type = 'x1', 'x2', or 'x3') 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. For any other terminal type, if the terminal is unable to provide the amount at this point in transaction processing, the amount field in the data element list shall be filled with hexadecimal zeroes.

As described in Book 3, 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, then 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 for this card session as defined in EMV Contact Interface Specification.

6.3.2 Offline Data Authentication

An online-only terminal supporting no form of offline data authentication as indicated in Terminal Capabilities shall set to 1 the 'Offline data authentication was not performed' bit in the Terminal Verification Results (TVR). (For details, see Book 3 Annex C.)

All other terminals shall be capable of performing SDA, DDA, optionally CDA, and optionally XDA, as described in Books 2 and 3.

6.3.2.1 CDA

The following section applies when the selected form of offline data authentication is CDA.

When CDA fails prior to the final Terminal Action Analysis (for example, Issuer Public Key recovery fails) preceding the issuance of a first GENERATE AC command or a second GENERATE AC command in the case 'unable to go online', the terminal shall set the TVR bit for 'CDA failed' to 1 and request the cryptogram type determined by Terminal Action Analysis. In this case, the GENERATE AC command shall not request a CDA signature and no further CDA processing is performed.

When a CDA failure is detected after the final Terminal Action Analysis preceding the issuance of a first or second GENERATE AC command, the terminal shall set the 'CDA failed' bit in the TVR to 1 and the following rules apply:

If CDA fails in conjunction with the first GENERATE AC:

- If the Cryptogram Information Data (CID) indicates that the card has returned a TC, the terminal shall decline the transaction and not perform a second GENERATE AC command.
- If the CID indicates that the card has returned an ARQC, the terminal shall complete the transaction processing by performing an immediate second GENERATE AC command requesting an AAC.

If CDA fails in conjunction with the second GENERATE AC, the terminal shall decline the transaction

If as part of dynamic signature verification the CID was retrieved from the ICC Dynamic Data (as recovered from the Signed Dynamic Application Data), then it is this value that shall be used to determine the cryptogram type. Otherwise the cleartext CID in the GENERATE AC response shall be used.

6.3.2.2 XDA

When the selected form of offline data authentication is XDA, the terminal shall perform the processing defined in the following sections when XDA fails. The first three sections address the three different ways in which XDA can fail and the fourth section describes terminal processing after first GENERATE AC XDA failure.

Note: In the following sections, ‘final TAA’ means the Terminal Action Analysis that occurs immediately before issuance of a GENERATE AC command.

6.3.2.2.1 CA ECC Public Key Retrieval Failure

If the terminal experiences a CA ECC Public Key retrieval error, the terminal shall set the ‘CA ECC key missing’ bit in the TVR to 1 *before* the final TAA preceding the first GENERATE AC command. In this case the terminal omits ECC key recovery and XDA signature verification and continues with the processing defined in section 6.3.2.2.4.

6.3.2.2.2 ECC Key Recovery Failure

If the terminal experiences an ECC Issuer Public Key or ICC Public Key recovery error, the terminal shall:

- Set the ‘ECC key recovery failed’ bit in the TVR *after* issuance of the first GENERATE AC command but *before* the TAA that occurs following the first GENERATE AC command. However, the ‘ECC key recovery failed’ bit is not set if the ‘CA ECC key missing’ bit is set.
- Perform the processing defined in section 6.3.2.2.4.

Note: The terminal may perform ECC key recovery before issuance of the first GENERATE AC command, but setting of the ‘ECC key recovery failed’ bit in the TVR must occur after issuance of the first GENERATE AC command to ensure that the result of final TAA preceding the first GENERATE AC command does not vary based upon when ECC key recovery is performed by the terminal. If the TVR is included as input to generation of the Application Cryptogram, the issuer should set the ‘ECC key recovery failed’ bit in the TVR to 0 when performing Application Cryptogram verification, as the value of that bit may have changed after the Application Cryptogram was generated.

6.3.2.2.3 XDA Signature Verification Failure

After a GENERATE AC command, if either of the following is true:

- the Signed Dynamic Application Data (SDAD) was not received in the GENERATE AC response
- verification of the Signed Dynamic Application Data (SDAD) failed

then when ECC key recovery has ended, the terminal shall:

- Set the 'XDA signature verification failed' bit in the TVR to 1 if CA ECC key retrieval and ECC key recovery were successful.
- For the first GENERATE AC, perform the processing defined in section 6.3.2.2.4.
- For the second GENERATE AC, decline the transaction. **Note:** This will only apply if XDA was successful on the first GENERATE AC as otherwise section 6.3.2.2.4 applies which specifies that the XDA signature on the second GENERATE AC is not verified.

6.3.2.2.4 Terminal Processing After First GENERATE AC XDA Failure

The terminal performs the processing described in this section when it experiences an XDA failure, specifically a CA ECC public key retrieval failure (as defined in section 6.3.2.2.1), an ECC key recovery failure (as defined in section 6.3.2.2.2) or an XDA signature verification failure for first GENERATE AC (as defined in section 6.3.2.2.3).

If the CID indicated that the card returned a TC or ARQC, the terminal shall:

- Perform TAA using the TAC-Denial and IAC-Denial. If the IAC-Denial does not exist, a default value with all bits set to 0 is used.
- If the result of this TAA is to decline the transaction (that is, a TVR bit is 1 and the corresponding TAC-Denial or IAC-Denial bit is also 1), the terminal shall:
 - If the CID indicated that the card returned a TC, no second GENERATE AC command shall be issued to complete the transaction.
 - If the CID indicated that the card returned an ARQC, a second GENERATE AC command requesting an AAC shall be issued to complete the transaction.

Otherwise (the result of this TAA is not to decline the transaction), the terminal shall attempt to send the transaction online for authorisation¹ and:

- The TVR value included in the online authorisation shall include the updated values of the 'ECC key recovery failed' and the 'XDA signature verification failed' bits.

Note: If the TVR is included as input to generation of the Application Cryptogram, the issuer should set the 'ECC key recovery failed' and the 'XDA signature verification failed' bits in the TVR to 0 when performing Application Cryptogram verification, as the value of those bits may have changed after the Application Cryptogram was generated.

- If the terminal is able to process the transaction online, then:
 - If the CID indicated that the card returned a TC, the terminal shall not issue a second GENERATE AC command to complete the transaction. Depending on the Authorisation Response Code returned in the response message, the terminal shall determine whether to accept or decline the transaction.

¹ In this scenario, a cryptogram type of TC may be sent in the online authorisation.

- If the CID indicated that the card returned an ARQC, the terminal shall issue a second GENERATE AC command to complete the transaction as described in section 6.3.8. Although an XDA signature will be requested it shall not be verified by the terminal.²
- If the terminal is for any reason unable to process the transaction online, then:
 - The terminal shall decline the transaction
 - If the CID indicated that the card returned a TC, the terminal shall not issue a second GENERATE AC command to complete the transaction.
 - If the CID indicated that the card returned an ARQC, the terminal shall issue a second GENERATE AC command requesting an AAC to complete the transaction. Although an XDA signature will be requested it shall not be verified by the terminal.

If the CID indicated that the card returned an AAC, the terminal shall decline the transaction without issuing a second GENERATE AC command.

6.3.3 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 section A1 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.

6.3.4 Cardholder Verification Processing

Recognition of a CVM means the CVM Code is understood by the terminal but not necessarily supported by the terminal. The terminal shall recognise the EMV-defined CVM codes in Book 3 section C3 including the CVM codes for 'No CVM required' and 'Fail CVM processing'. The terminal may also recognise proprietary CVM Codes not defined in section C3.

Support for a CVM means the terminal has the hardware and software necessary to perform the CVM. Support for EMV-defined CVM codes is indicated in the following manner:

- For EMV-defined CVM codes, support is indicated in Terminal Capabilities and Biometric Terminal Capabilities.

² An XDA signature is requested only for the sake of consistency – the terminal ignores the XDA signature provided in the response to the second GENERATE AC because it is known that if the issuer has authorised the transaction then it was despite XDA failure on the first GENERATE AC.

- For CVM codes not defined in EMV, support may be known implicitly.
- For Combination CVMs, both CVM codes must be supported.
- Fail CVM shall always be considered supported.

A CVM can be performed only if it is both recognised and supported.

6.3.4.1 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, or 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 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 TVR to 1 (for details on TVR, see Book 3 Annex C),
- shall not display any specific message regarding PINs, and
- shall continue cardholder verification processing in accordance with the card's CVM List.

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 continue cardholder verification processing in accordance with the card's CVM List. (CVM Results is described in section 6.3.4.5 and coded according to section A4.)

6.3.4.2 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'.

6.3.4.3 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.³ If this occurs, the terminal:

- shall set the 'PIN entry required, PIN pad present, but PIN was not entered' bit in the TVR to 1,
- shall not set the 'PIN Try Limit exceeded' bit in the TVR to 1,
- shall consider this CVM unsuccessful, and
- shall continue cardholder verification processing in accordance with the card's CVM List.

When PIN entry has been bypassed for one PIN-related CVM, it may be considered bypassed for any subsequent PIN-related CVM during the current transaction.

6.3.4.4 Signature

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 provide a way to capture cardholder signature (e.g., by printing a line for the cardholder signature on the merchant's copy of the receipt, or by using an electronic panel). (See section A2 for requirements for the terminal to support signature as a CVM.)

6.3.4.5 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. After a successful CVM, CVM Results reflect the successful CVM. After an unsuccessful CVM with byte 1 bit 7 of the CV Rule set to 0 (fail cardholder verification), CVM Results reflect the unsuccessful CVM. After an unsuccessful CVM with byte 1 bit 7 set to 1 (apply succeeding CVM), CVM Results reflect this unsuccessful CVM only when no subsequent CVMs are performed; that is, when for each subsequent CV Rule either the CVM condition is not satisfied or the CVM condition is satisfied but the CVM method is not supported or is not recognised. If a subsequent CVM is performed, CVM Results reflect the outcome of the subsequent CVM.

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'.

³ 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.

Table 2 on the following page shows the setting of CVM Results, Byte 3 of Terminal Verification Results (TVR) related to CVM processing, and the Transaction Status Information (TSI) bit for CVM processing for some conditions that may occur during CVM List processing. Please note that for the first five entries in the table, the second byte of the CVM Results has no actual meaning so it is recommended it be set to '00'.

Conditions	Corresponding CVM Results			TVR Byte 3	TSI Byte 1 bit 7
	Byte 1 (CVM Performed)	Byte 2 (CVM Condition)	Byte 3 (CVM Result)		
When the card does not support cardholder verification (AIP bit 5=0)	'3F' (Book 4 section 6.3.4.5 and section A4)	'00' (no meaning)	'00'	--	0
When CVM List is not present or the CVM List has no CVM rules	'3F' (Book 4 section 6.3.4.5 and section A4)	'00' (no meaning)	'00'	--	0 (Book 3 section 10.5)
When no CVM Conditions in CVM List are satisfied	'3F' (Book 4 section 6.3.4.5 and section A4)	'00' (no meaning)	'01'	bit 8 = 1	1
When the terminal does not support any of the CVM Codes in CVM List where the CVM Condition was satisfied	'3F' (Book 4 section 6.3.4.5 and section A4)	'00' (no meaning)	'01'	bit 8 = 1	1
When the terminal does not recognise any of the CVM Codes in CVM List (or the code is RFU) where the CVM Condition was satisfied	'3F' (Book 4 section 6.3.4.5 and section A4)	'00' (no meaning)	'01'	bit 8 = 1 bit 7 = 1	1
When the (last) performed CVM is 'Fail CVM processing'	'00' or '40' (Not recommended for cards.)	The CVM Condition Code for the CVM Code in Byte 1	'01' (Book 4 section 6.3.4.5 and section A4)	bit 8 = 1	1
When the last performed CVM fails	The CVM Code for the last performed CVM	The CVM Condition Code for the CVM Code in Byte 1	'01'	bit 8 = 1 ⁴	1
When the CVM performed is 'Signature'	'1E' or '5E' (CVM Code for 'Signature')	The CVM Condition Code for the CVM Code in Byte 1	'00' (Book 4 section 6.3.4.4 and section A4)	--	1

Table 2: Setting of CVM Results, TVR bits, and TSI bits following CVM Processing

⁴ Errors with PIN related CVMs may also result in the setting of other PIN-related TVR bits.

Conditions	Corresponding CVM Results			TVR Byte 3	TSI Byte 1 bit 7
	Byte 1 (CVM Performed)	Byte 2 (CVM Condition)	Byte 3 (CVM Result)		
When the CVM performed is 'Online PIN'	'02' or '42' (CVM Code for 'Online PIN')	The CVM Condition Code for the CVM Code in Byte 1	'00' (Book 4 section 6.3.4.2 and section A4)	bit 3 = 1	1
When the CVM performed is 'No CVM required'	'1F' or '5F' (CVM code for 'No CVM Required')	The CVM Condition Code for the CVM Code in Byte 1	'02' (Book 4 section 6.3.4.5 and section A4)	--	1
When a CVM is performed and fails with the failure action being 'Go to Next' and then the end of the CVM List is reached without another CVM Condition being satisfied	The last CVM Code in the CVM List for which the CVM Condition was satisfied (but that failed).	The CVM Condition Code for the CVM Code in Byte 1	'01'	bit 8 = 1	1
When the CVM performed is a combination CVM Code, and at least one fails and the failure action is Fail CVM	CVM Code for the combination CVM	The CVM Condition Code for the CVM Code in Byte 1	'01'	bit 8 = 1 ⁴	1
When the CVM performed is a combination CVM Code, and one passes and the result of the other is 'unknown'	CVM Code for the combination CVM	The CVM Condition Code for the CVM Code in Byte 1	'00'	--	1

Table 2: Setting of CVM Results, TVR bits, and TSI bits following CVM Processing, continued

6.3.5 Terminal Risk Management

In addition to the terminal risk management functions described in Book 3 and regardless of the coding of the card's Application Interchange Profile bit setting for 'Terminal Risk Management is to be performed', 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 card (identified by data such as the Application Primary Account Number (PAN) and the Application PAN Sequence Number taken from the currently selected application) 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 TVR to 1.

6.3.6 Terminal Action Analysis

As described in Book 3, during terminal action analysis the terminal determines whether the transaction should be approved offline, declined offline, or transmitted online by comparing the TVR 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'.⁵
- 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.

⁵ 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.

6.3.7 Card Action Analysis

In response to the GENERATE APPLICATION CRYPTOGRAM (AC) command, the card returns CID. Based on the CID, the terminal shall process the transaction as follows:

If the card indicates:	then the terminal:
approval	<ul style="list-style-type: none"> • shall complete the transaction • should display the 'APPROVED' message
decline	<ul style="list-style-type: none"> • shall decline the transaction • should display the 'DECLINED' message
process online	shall transmit an authorisation or financial transaction request message, if capable (See section 12.2.1 for exception handling when the terminal is unable to go online.)
advice, and if advices are supported by the terminal and terminal acquirer interface protocol	<ul style="list-style-type: none"> • shall not, if the transaction is captured, create an advice message. • shall, if the transaction is not captured (such as a decline), either transmit an online advice if online data capture is performed by the acquirer, or create an offline advice for batch data capture. (See section 12.2.5 for exception handling when the terminal is unable to create an advice)
advice, and if advices are not supported by the terminal and terminal acquirer interface protocol	does not create an advice.
'Service not allowed'	<ul style="list-style-type: none"> • shall terminate the transaction • should display the 'NOT ACCEPTED' message

Table 3: Card Action Analysis

6.3.8 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 if the card returned an ARQC in the first GENERATE AC response.

The result of card risk management performed by the ICC is made known to the terminal through the return of the CID 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'.

6.3.9 Issuer-to-Card Script Processing

The terminal shall be able to support 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.

Note: In this case and when only one Issuer Script (tag '71' or '72') is sent, and no Issuer Script Identifier is used, the maximum length of the Issuer Script Command (tag '86') is limited to 124 bytes. This implies that the maximum available useful command data (Lc) is limited to 119 bytes for a Case 3 command.

Note: A terminal or special device used for biometric enrolment or update, i.e. to store a biometric template in the card as the biometric reference template or later update the biometric reference template, shall be able to support one or more Issuer Scripts, where the total length of all Issuer Scripts is more than 128 bytes. The maximum size is dependent on the program(s) supported by the terminal.

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 most significant nibble of byte 1 of the Issuer Script Results to 'Script processing failed' and the least significant 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 most significant nibble of byte 1 of the Issuer Script Results to 'Script processing successful' and the least significant nibble to '0'. See section A5 for details.

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 the terminal supports advices.

6.4 Conditions for Support of Functions

A terminal supporting offline PIN verification or offline biometric verification shall support the VERIFY command. A terminal supporting offline PIN encipherment or offline biometric encipherment shall also support the GET CHALLENGE command. A terminal not supporting offline PIN verification nor offline biometric verification need not support the VERIFY command.

An offline-only terminal and an offline terminal with online capability shall support both SDA and DDA, may optionally support CDA, and may optionally support XDA.

An online-only terminal need not support SDA or DDA or CDA or XDA. 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. 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. A cardholder-controlled terminal (Terminal Type = '3x') need not support terminal risk management.

6.5 Other Functional Requirements

6.5.1 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 keypad 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. 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. 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').

6.5.2 Voice Referrals

A manual voice referral process may be initiated by the issuer.

An attended terminal shall be capable of supporting voice referrals, (that is, it shall be capable of alerting the attendant when the 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 (for example, approve offline, or decline offline).

6.5.2.1 Referrals Initiated by Card

This functionality was removed by bulletin SU42.

6.5.2.2 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 either display the 'CALL YOUR BANK' message to the attendant, or shall alert the attendant in some other way that the Issuer has requested a voice referral. Appropriate application data, such as the Application PAN, should be displayed or printed to the attendant in order to perform the referral. Appropriate messages should 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. If the card returned an ARQC in the first GENERATE AC response, 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.

6.5.3 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 TVR to 1. Payment systems rules will determine whether the attendant is allowed to perform such a function.

6.5.4 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.

6.5.5 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 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.

6.5.6 Unpredictable Number

The terminal shall be able to generate an Unpredictable Number (tag '9F37') to be used for input to the card cryptograms (Application Cryptograms and DDA/CDA signatures) so as to ensure the unpredictability of data input to this calculation and thereby the freshness of the cryptogram.

A terminal may use the same Unpredictable Number throughout a transaction. The Unpredictable Number could be generated by a dedicated hardware random number generator or could, for example, be a function of previous Application Cryptograms, the terminal Transaction Sequence Counter and other variable data (e.g. date/time). In the second example the function could be a hash function or a keyed encipherment function.

Book 2 section 11.3 provides an example of an approved method for generating the Unpredictable Number using a hash function

6.6 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.

6.6.1 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.)

6.6.2 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 an unsuccessful IC read' if the service code on the magnetic stripe indicates that an IC is present.⁶

Payment system rules determine whether fallback to magnetic stripe is allowed after the failure of an IC-read transaction. This behaviour is outside the scope of EMV specifications.

⁶ 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.

6.7 Date Management

6.7.1 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.

6.7.2 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.

6.7.3 Date 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.

7 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.

7.1 Keypad

A terminal should have a keypad for the entry of transaction-related data and its functional operation. The keypad shall support one or more types of keys, as listed in Table 4.

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'

Table 4: Key Types

A keypad 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 cardholder receipt is to be provided.

A touch screen is considered to be a keypad. (See Book 2 for security requirements.)

7.1.1 Command Keys

Command keys are used to control the flow of data entry by the cardholder or attendant. Table 5 describes the command keys:

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

Table 5: Command Keys

If the colours green, red, or yellow are used, either for key lettering or the keys themselves, it is recommended that they be reserved for the command keys according to Table 6:

Enter	Green
Cancel	Red
Clear	Yellow

Table 6: Command Key Colours

When the command keys are horizontally arranged, the 'Cancel' and 'Enter' keys should be located on the bottom row of the keypad, 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.

7.1.2 PIN Pad

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

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

It is recommended that the numeric layout of the PIN pad 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 keypad 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.

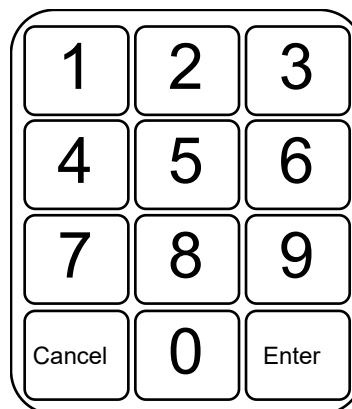


Figure 4: PIN Pad Layout

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.

7.2 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.

7.3 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.

7.4 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 ODE 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.

7.5 Receipt Printer

A terminal may have a printer for receipt printing. Alternatively, receipts may be provided by electronic means such as email (see complementary payment systems documentation for additional information).

Cardholder-controlled terminal (Terminal Type = '3x') need not provide receipts.

7.6 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 III

Software Architecture

8 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.

8.1 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.

8.2 Application Libraries

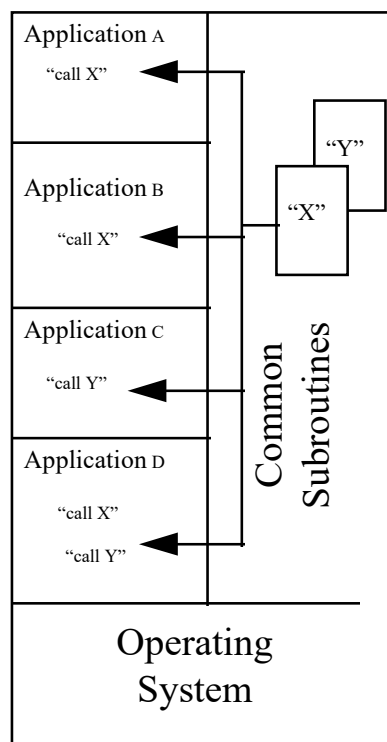


Figure 5: Terminal Software

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.

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

8.3 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
- 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, SDA 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.

8.4 Interpreter

8.4.1 Concept

This section describes the general architecture underlying an interpreter implementation and gives 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.

8.4.2 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.

8.4.3 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.

8.4.4 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.

8.4.5 Kernel Output

Recommendation

In order to meet country or regional requirements the kernel should be capable of outputting the latest value for the following data:

1. Any card originated data used in a transaction,
2. Any kernel originated data used in a transaction, including kernel configuration data and data provided by the acceptance device (such as the amount),
3. Data that can be used to identify the terminal (such as Terminal Identifier, or proprietary data that may be used to that effect)

Mandate

For kernels that are unable to output all of the data outlined above, the kernel shall at a minimum be capable of outputting the latest value for the following data:

- Amount, Authorised (Numeric) ('9F02')
- Amount, Other (Numeric) ('9F03')
- Application Cryptogram ('9F26')
- Application Effective Date ('5F25')
- Application Expiration Date ('5F24')
- Application Interchange Profile ('82')
- Application Label ('50')
- Application PAN ('5A')
- Application PAN Sequence Number ('5F34')
- Application Preferred Name ('9F12')
- Application Transaction Counter ('9F36')
- Application Usage Control ('9F07')
- Application Version Number ('9F09')
- Cardholder Name ('5F20')
- Cardholder Name Extended ('9F0B')
- Cryptogram Information Data ('9F27')
- CVM List ('8E')
- CVM Results ('9F34')
- DF Name ('84')
- Interface Device Serial Number ('9F1E')
- Issuer Action Codes ('9F0D', '9F0E', '9F0F')

- Issuer Application Data ('9F10')
- Issuer Code Table Index ('9F11')
- Issuer Country Code ('5F28')
- Issuer Script Results (-)
- Language Preference ('5F2D')
- Merchant Category Code ('9F15')
- Merchant Identifier ('9F16')
- Payment Account Reference ('9F24')
- Terminal Capabilities ('9F33')
- Terminal Country Code ('9F1A')
- Terminal Identification ('9F1C')
- Terminal Type ('9F35')
- Terminal Verification Results ('95')
- Track 2 Equivalent Data ('57')
- Transaction Currency Code ('5F2A')
- Transaction Date ('9A')
- Transaction Status Information ('9B')
- Transaction Time ('9F21')
- Transaction Type ('9C')
- Unpredictable Number ('9F37')

**Card originated data objects that are not mandatory are only required to be made available by the kernel when they are provided by the card.*

8.5 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.

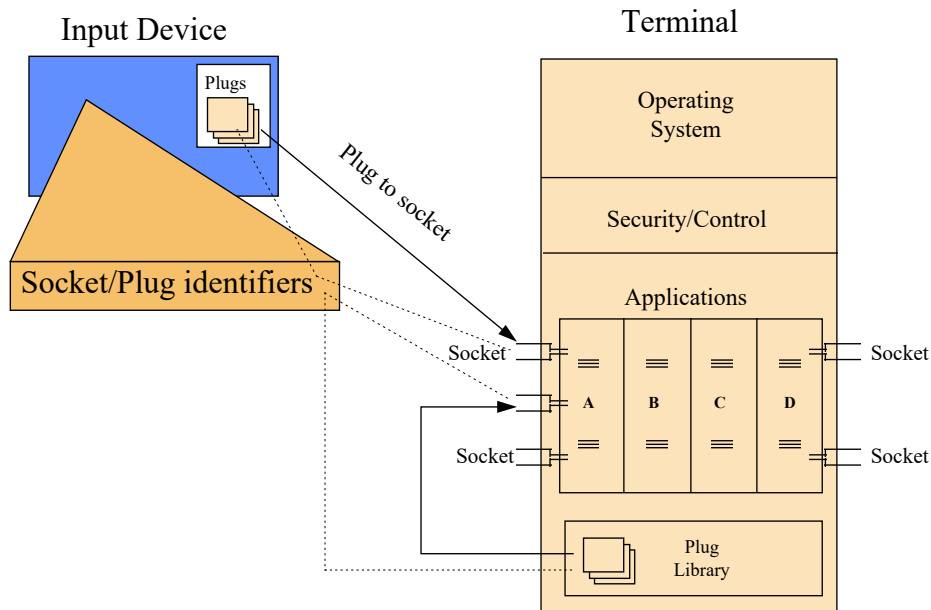


Figure 6: Socket/Plug Relationship

8.6 Biometric Terminal

Figure 7 shows the high level architecture of the Biometric Terminal and Card.

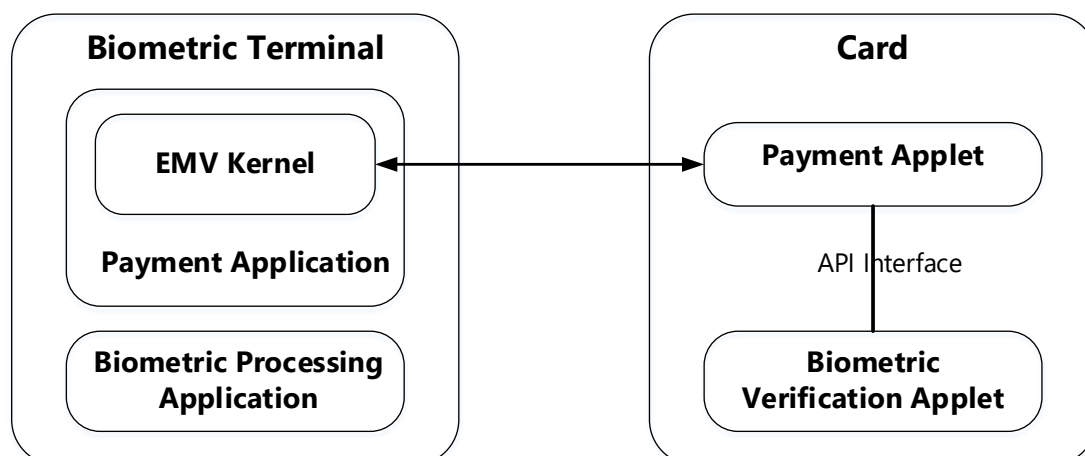


Figure 7: Architecture of Biometric Terminal and Card

Note: The Biometric Processing Application could be implemented as an integrated part of or as a separate component from the Biometric Terminal. Figure 7 shows one example of the Biometric Terminal and Card implementation.

As shown in Figure 7, the Biometric Terminal has a Biometric Processing Application, which supports at least one biometric verification method among facial, finger, iris, palm, and voice verifications.

If the Biometric Processing Application supports finger verification, it shall be able to support the capture of any of the ten fingers. Similarly, if it supports palm verification it shall be able to support the capture of both left and right palms; and if it supports iris verification, it shall be able to support the capture of both left and right irises.

For each supported biometric verification method, the Biometric Processing Application shall support at least one ISO format specified in ISO/IEC 19794 for interoperability and may support others to satisfy the business requirements, such as performance, liveness detection, etc.

Note: When the Biometric Processing Application supports one ISO format specified in ISO/IEC 19794, it shall support all possible values of the mandatory biometric comparison algorithm parameters defined in the standard. For example, if the Biometric Processing Application supports ISO/IEC 19794-2, it shall support all possible values of the minutiae order indication defined in ISO/IEC 19794-2.

The Biometric Processing Application shall be able to construct the Biometric Data Block (BDB) using the biometric template captured by the biometric capture device and communicate the BDB to the EMV Kernel.

The mechanism on how the biometric capture device captures the biometric template and transmits it to the Biometric Processing Application, and how the Biometric Processing Application transmits the BDB to the EMV Kernel is not in the scope of this specification.

9 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.

10 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.) Additional data elements may be 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 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).

10.1 Application Independent Data

The terminal resident application independent data elements identified in this section shall be initialised in and obtainable from the terminal prior to the issuance of the GET PROCESSING OPTIONS command in the Initiate Application Processing function described in Book 3 section 10.1. The data shall not change during the transaction. Any data sent in the authorisation request message shall have the same value as that provided to the card as listed in the PDOL (if present) and CDOL1, including Local Date and Local Time if appropriate.

10.1.1 Terminal Related Data

The following data elements are application independent and shall be unique to the terminal (see section 5.3 for different terminal configurations):

- IFD Serial Number
- Local Date
- Local Time
- Terminal Country Code
- Transaction Sequence Counter

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 11.1).

10.1.2 Transaction Related Data

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 for an example):

- Additional Terminal Capabilities
- Terminal Capabilities
- Terminal Type

The terminal shall be constructed in such a way that these data objects cannot be modified unintentionally or by unauthorised access.

These data objects may be varied on a transaction by transaction basis which means that for each transaction, the terminal may invoke a different value for these data objects based on certain characteristics and parameters of the transaction (selection criteria). Support of this functionality is optional for the terminal. The implementation of this functionality is left to the discretion of the terminal manufacturer and is outside the scope of EMV.

10.2 Application Dependent Data

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

Data Elements	Notes
Acquirer Identifier	
Application Identifier (AID)	
Application Version Number	
Certification Authority Public Key (RSA) <ul style="list-style-type: none"> • Certification Authority Public Key Exponent • Certification Authority Public Key Modulus 	Required if terminal supports offline data authentication and/or ODE using RSA. See Book 2.
Certification Authority Public Key (ECC)	Required if terminal supports offline data authentication and/or ODE using ECC. See Book 2.
Certification Authority Public Key Index	Required if terminal supports offline data authentication and/or ODE: The key index in conjunction with the Registered Application Provider Identifier (RID) of the payment system AID identifies the key and the algorithm for offline data authentication and/or ODE. See Book 2.
Default Dynamic Data Authentication Data Object List (DDOL)	Required if terminal supports DDA or CDA.
Default Transaction Certificate Data Object List (TDOL)	If not present, a default TDOL with no data objects in the list shall be assumed.
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	
Target Percentage to be used for Random Selection	Required if offline terminal with online capability.

Table 7: Application Dependent Data Elements

Data Elements	Notes
Terminal Action Code - Default Terminal Action Code - Denial Terminal Action Code - Online	Required if non-zero values to be used ⁷
Terminal Capabilities	If the terminal supports XDA or ECC ODE for any application, the terminal shall support an independently configurable Terminal Capabilities value for each application.
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	

Table 7: Application Dependent Data Elements, continued

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 ODE. Each logical key slot shall contain the following data: RID, Certification Authority Public Key Index, and Certification Authority Public Key.

When the public key is installed into the terminal, the terminal shall verify the integrity of the public key to detect a key entry or transmission error. This may be done by verifying a Certification Authority Public Key Check Sum (for RSA) or self-signed Certification Authority Public Key Certificate (for ECC). See Book 2 section 11.2. If the verification process fails, the terminal shall not accept the public key and, if operator action is needed, the terminal shall display an error message.

⁷ According to Book 3, the default value consists of all bits set to 0, although the ‘Offline data authentication was not performed’, ‘SDA failed’, ‘DDA failed’, ‘CDA failed’, ‘CA ECC key missing’, ‘ECC key recovery failed’, and ‘XDA signature verification failed’ bits are strongly recommended to be set to 1 in the Terminal Action Code - Default and Terminal Action Code - Online.

Note: Alternative integrity verification techniques may be used. The integrity of the stored Certification Authority Public Keys should be verified periodically.

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.

Part IV

Cardholder, Attendant, and Acquirer Interface

11 Cardholder and Attendant Interface

11.1 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. To display the standard messages defined in section 11.2, the terminal shall support the common character set as defined in Annex B, and should support the relevant character set defined in the corresponding part of ISO/IEC 8859 when necessary.

Depending on the local environment and business conditions, the terminal should support multiple languages for displaying the set of messages described in section 11.2 to the cardholder. A terminal supporting multiple languages may need additional parts of ISO/IEC 8859 to display characters relevant to these languages.

ISO/IEC 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/IEC 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).

If the terminal supports multiple languages, selection of the language to be used for displaying cardholder messages is performed prior to the issuance of the GET PROCESSING OPTIONS command; otherwise the local language is used to display cardholder messages. Language selection may be performed either by using the EMV language selection process (based on language preference indicated by the card), or by using a proprietary process.

If the EMV language selection process is used, the following rules apply:

- If the card does provide a Language Preference data object, the terminal shall compare the card's language preferences with the languages it supports:
 - If a match is found, the language with the highest preference shall be used for the messages displayed to the cardholder. (The Language Preference data object is coded so that the language with the highest preference appears first and the lowest preference appears last.)
 - If no match is found, the terminal shall allow the cardholder to select their preferred language if it has a means for allowing such selection. Messages shall be displayed to the cardholder in the selected language or, if the terminal has no means of offering language selection to the cardholder, in the local language.

- If the card does not provide a Language Preference data object, the terminal shall allow the cardholder to select their preferred language if it has a means for allowing such selection. Messages shall be displayed to the cardholder in the selected language or, if the terminal has no means of offering language selection to the cardholder, in the local language.

Alternatively terminals may support a proprietary language selection process which is outside the scope of EMV. If such a proprietary language selection process is used, the EMV language selection process shall not be performed. The language selected using the proprietary process shall be used throughout the transaction.

Messages should be displayed to the attendant in the language of the attendant's choice or, if the terminal has no means of offering language selection to the attendant, in the local language. Messages displayed to the attendant and cardholder may be displayed in different languages if supported by the terminal.

11.2 Standard Messages⁸

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' – '13' (hexadecimal) are described in Table 8.
- Values '14' – '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'.

⁸ This specification does not imply that the terminal shall support a set of standard messages in English.

Message Identifier	Message	Definition
'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.
'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.

Table 8: Standard Messages

Message Identifier	Message	Definition
'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 when 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, when the IC and magnetic stripe readers are not combined.
'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.

Table 8: Standard Messages, continued

11.3 Application Selection

A terminal shall support application selection using the ‘List of AIDs’ method as described in Book 1 section 12.3.3. A terminal may support application selection using the payment systems directory as described in Book 1.

A terminal supporting more than one application should offer the cardholder the ability to select an application and 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 and confirmation shall create a list of ICC applications that are supported by the terminal as described in Book 1 and shall display:

- the Application Preferred Name(s), if present and if the Issuer Code Table Index indicating the part of ISO/IEC 8859 to use is present and supported by the terminal (as indicated in Additional Terminal Capabilities)
- otherwise, the Application Label(s), by using the common character set of ISO/IEC 8859 (see Annex B)

A terminal offering the cardholder neither the ability to select nor 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 and 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 offering neither cardholder selection nor 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.

11.4 Receipt

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

12 Acquirer Interface

12.1 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 ⁹ 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.¹⁰ 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 ¹¹ 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.

⁹ These data elements indicate point of transaction acceptance characteristics that rarely change, such as Merchant Category Code, Acquirer Identifier, or Terminal Country Code.

¹⁰ 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.

¹¹ These data elements reflect card acceptance conditions and restrictions that rarely change, such as Application Interchange Profile, Application Usage Control, or Issuer Action Codes.

This section describes requirements associated with ICC transactions and distinguishes between existing data elements used for magnetic stripe transactions and those created specifically for ICC 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. For ICC transactions, the values of all card-originated data contained in acquirer interface messages shall be as read from the chip. It is not acceptable to populate the messages partially with data read from the chip and partially with data read from the magnetic stripe (if also read).

For informational purposes, Annex C describes an example of converting ICC-related and terminal-related data into message data elements.

12.1.1 Authorisation Request

An authorisation request should convey the data elements contained in Table 9 and Table 10 subject to the specified conditions.

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

Data Element	Condition
Application Cryptogram * ¹²	
Application Interchange Profile *	
Application Transaction Counter *	
CID	The CID does not need to be forwarded to the issuer; the presence of this data element is defined in the respective payment system network interface specifications.
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
Payment Account Reference (PAR)	Present if provided by ICC, at the discretion of the acquirer, subject to payment system requirements.
Terminal Capabilities	
Terminal Type	
Token Requestor ID	If in ICC, the presence of this data element is at the discretion of the acquirer, subject to payment system requirements.
TVR *	
Unpredictable Number*	Present if input to application cryptogram calculation

Table 9: ICC-specific Authorisation Request Data Elements

¹² 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.

Table 10 contains the 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 * ¹³	
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 10: Existing Authorisation Request Data Elements

¹³ 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.

12.1.2 Financial Transaction Request

A financial transaction request should convey the data elements contained in Table 11 and Table 12 subject to the specified conditions.

Table 11 contains the data elements created specifically for an ICC transaction.

Data Element	Condition
Application Cryptogram * ¹⁴	
Application Interchange Profile *	
Application Transaction Counter *	
Application Usage Control	Present if requested by acquirer
CID	The CID does not need to be forwarded to the issuer; the presence of this data element is defined in the respective payment system network interface specifications.
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
Payment Account Reference (PAR)	Present if provided by ICC, at the discretion of the acquirer, subject to payment system requirements.
Terminal Capabilities	
Terminal Type	
Token Requestor ID	If in ICC, the presence of this data element is at the discretion of the acquirer, subject to payment system requirements.
TVR *	
Unpredictable Number *	Present if input to application cryptogram calculation

Table 11: ICC-specific Financial Transaction Request Data Elements

Table 12 contains the data elements necessary for an ICC transaction.

¹⁴ 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.

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 * ¹⁵	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 12: Existing Financial Transaction Request Data Elements

¹⁵ 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.

12.1.3 Authorisation or Financial Transaction Response

Authorisation and financial transaction responses should convey the data elements contained in Table 13 and Table 14 subject to the specified conditions.

Table 13 contains the data elements specifically created for an ICC transaction.

Data Element	Condition
Issuer Authentication Data * ¹⁶	Present if online issuer authentication performed
Issuer Script * <ul style="list-style-type: none"> • Issuer Script Template 1 • Issuer Script Template 2 	Present if commands to ICC are sent by issuer
Last 4 Digits of PAN	If the ICC has an affiliated payment token, the presence of this data element is dependent on payment system requirements.
Payment Account Reference (PAR)	Present if ICC has PAR assigned, subject to payment system requirements.

Table 13: ICC-specific Authorisation or Financial Transaction Response Data Elements

Table 14 contains the 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 14: Existing Authorisation or Financial Transaction Response Data Elements

¹⁶ 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.

12.1.4 Financial Transaction Confirmation

A financial transaction confirmation should convey the data elements contained in Table 15 and Table 16 subject to the specified conditions.

Table 15 contains the 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 15: ICC-specific Financial Transaction Confirmation Data Elements

Table 16 contains the data elements necessary for an ICC transaction.

Data Element	Condition
Terminal Identifier	

Table 16: Existing Financial Transaction Confirmation Data Elements

12.1.5 Batch Data Capture

Batch data capture should convey the data elements contained in Table 17 and Table 18 subject to the specified conditions. Message Type is used to distinguish between an offline advice and a financial record.

Table 17 contains the data elements specifically created for an ICC transaction.

Data Element	Condition
Application Cryptogram * ¹⁷ (i.e., TC, ARQC, or AAC)	ARQC may be used as TC substitute
Application Interchange Profile *	
Application Transaction Counter *	
Application Usage Control	Present if requested by acquirer
CID	The CID does not need to be forwarded to the issuer; the presence of this data element is defined in the respective payment system network interface specifications.
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
Payment Account Reference (PAR)	Present if provided by ICC, at the discretion of the acquirer, subject to payment system requirements.
Terminal Capabilities	
Terminal Type	
Token Requestor ID	If in ICC, the presence of this data element is at the discretion of the acquirer, subject to payment system requirements.
TVR *	
Unpredictable Number *	Present if input to application cryptogram calculation

Table 17: ICC-specific Batch Data Capture Data Elements

¹⁷ 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.

Table 18 contains the 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 * ¹⁸	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

Table 18: Existing Batch Data Capture Data Elements

¹⁸ 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.

Data Element	Condition
Transaction Date *	
Transaction Time	
Transaction Type *	

Table 18: Existing Batch Data Capture Data Elements, continued

12.1.6 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 19: Existing Reconciliation Data Elements

12.1.7 Online Advice

An online advice should convey the data elements contained in Table 20 and Table 21 subject to the specified conditions.

Table 20 contains the data elements specifically created for an ICC transaction.

Data Element	Condition
Application Cryptogram (TC or AAC)	
Application Interchange Profile	
Application Transaction Counter	
CID	
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
Payment Account Reference (PAR)	Present if provided by ICC, at the discretion of the acquirer, subject to payment system requirements.
Terminal Capabilities	
Terminal Type	
Token Requestor ID	If in ICC, the presence of this data element is at the discretion of the acquirer, subject to payment system requirements.
TVR	
Unpredictable Number	Present if input to application cryptogram calculation

Table 20: ICC-specific Online Advice Data Elements

Table 21 contains the 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 21: Existing Online Advice Data Elements

12.1.8 Reversal

A reversal should convey the data elements contained in Table 22 and Table 23 subject to the specified conditions.

Table 22 contains the 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
Payment Account Reference (PAR)	Present if provided by ICC, at the discretion of the acquirer, subject to payment system requirements.
Terminal Capabilities	
Terminal Type	
Token Requestor ID	If in ICC, the presence of this data element is at the discretion of the acquirer, subject to payment system requirements.
TVR	

Table 22: ICC-specific Reversal Data Elements

Table 23 contains the 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 23: Existing Reversal Data Elements

12.2 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.

12.2.1 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 TVR with Issuer Action Code - Online and Terminal Action Code - Online (see Book 3 section 10.7)
- Card action analysis via its response to the first GENERATE AC command: CID indicates ARQC returned (see Book 3)
- Terminal action analysis after first GENERATE AC with an XDA failure (see section 6.3.2.2.4)

If the terminal is unable to process the transaction online, as described in Book 3, the terminal shall compare the TVR with both Terminal Action Code - Default and Issuer Action Code - Default to determine whether to accept or decline the transaction offline and, if the card returned an ARQC in the first GENERATE AC response, the terminal 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 CID indicating either a TC for an approval or an AAC for a decline.

12.2.2 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 (TSI) to 0, as described in Book 3. The terminal shall continue processing based on the Authorisation Response Code returned in the response message as described in section 6.3.6.

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.

12.2.3 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)¹⁹, if any, of the authorisation request, the terminal shall process the transaction as being unable to go online. As described in Book 3, the terminal shall compare the TVR with both Terminal Action Code - Default and Issuer Action Code - Default to determine whether to accept or decline the transaction offline and, if the card returned an ARQC in the first GENERATE AC response, the terminal 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 CID 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.

¹⁹ Acquirers or networks may require that an authorisation request be repeated in the event that a valid response is not obtained. Requirements for such repeat(s) are outside the scope of EMV.

12.2.4 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.

If either of these incidents occurs, 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.

Book 3 Annex E gives some examples of TVR and TSI bit setting following script processing.

12.2.5 Advice Incidents

If the terminal supports advices but is unable to create an advice when requested by the card in the CID returned in the response to the GENERATE AC command as described in section 6.3.7, the terminal shall terminate the transaction.

Part V

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 ²⁰
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 24: 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.

²⁰ For the purpose of this specification, an attended cardholder-controlled terminal is considered to be a non-existent 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

This section provides the coding for Terminal Capabilities:

- Byte 1: Card Data Input Capability
- Byte 2: CVM Capability
- Byte 3: Security Capability

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.

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 25: Terminal Capabilities Byte 1 – Card Data Input 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
x	x	x	1	x	x	x	x	Enciphered PIN for offline verification (RSA ODE)
x	x	x	x	1	x	x	x	No CVM Required
x	x	x	x	x	1	x	x	Online Biometric
x	x	x	x	x	x	1	x	Offline Biometric
x	x	x	x	x	x	x	1	Enciphered PIN for offline verification (ECC ODE)

Table 26: Terminal Capabilities Byte 2 – CVM Capability

If the terminal supports a CVM of signature, the terminal shall be an attended terminal (Terminal Type = 'x1', 'x2', or 'x3') and shall support signature capture by paper or electronic means (Additional Terminal Capabilities, byte 4, 'Print or electronic, attendant' bit = 1).

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	SDA
x	1	x	x	x	x	x	x	DDA
x	x	1	x	x	x	x	x	Card capture
x	x	x	0	x	x	x	x	RFU
x	x	x	x	1	x	x	x	CDA
x	x	x	x	x	1	x	x	XDA
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 27: Terminal Capabilities Byte 3 – Security Capability

A3 Additional Terminal Capabilities

This section provides the coding for Additional Terminal Capabilities:

- Byte 1: Transaction Type Capability
- Byte 2: Transaction Type Capability
- Byte 3: Terminal Data Input Capability
- Byte 4: Terminal Data Output Capability
- Byte 5: Terminal Data Output Capability

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.

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 ²¹
x	x	x	x	x	1	x	x	Transfer ²²
x	x	x	x	x	x	1	x	Payment ²³
x	x	x	x	x	x	x	1	Administrative

Table 28: Add'l Term. Capabilities Byte 1 – Transaction Type Capability

²¹ For the purpose of this specification, an inquiry is a request for information about one of the cardholder's accounts.

²² 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.

²³ 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.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cash Deposit ²⁴
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 29: Add'l Term. Capabilities Byte 2 – Transaction Type 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 30: Add'l Term. Capabilities Byte 3 – Terminal Data Input Capability

²⁴ A cash deposit is considered to be a transaction at an attended or unattended terminal where a cardholder deposits cash into a bank account related to an application on the card used.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning ²⁵
1	x	x	x	x	x	x	x	Print or electronic, attendant 1: Paper receipt, attendant, or Paper Signature, or Electronic Signature
x	1	x	x	x	x	x	x	Print or electronic, cardholder 1: Paper receipt, cardholder, or Electronic Receipt, 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 31: Add'l Term. Capabilities Byte 4 – Term. Data Output Capability

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

²⁵ If the terminal is attended (Terminal Type = 'x1', 'x2', or 'x3') and there is only one printer and electronic receipts are not supported, the 'Print or electronic, attendant' bit shall be set to 1 and the 'Print or electronic, 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 or electronic, attendant' and 'Display, attendant' bits shall be set to 0.

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 32: Add'l Term. Capabilities Byte 5 – Term. Data Output Capability

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

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 ('3F' if no CVM is performed)
Byte 2	CVM Condition	One-byte CVM Condition Code of the CVM List as defined in Book 3 or '00' if no actual CVM was performed
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) or set to '1' if no CVM Condition Code was satisfied or if the CVM Code was not recognised or not supported

Table 33: CVM Results

A5 Issuer Script Results

Byte 1	Script Result	<p><u>Most significant nibble:</u> Result of the Issuer Script processing performed by the terminal:</p> <p>'0' = Script not performed</p> <p>'1' = Script processing failed</p> <p>'2' = Script processing successful</p> <p><u>Least significant nibble:</u> Sequence number of the Script Command</p> <p>'0' = Not specified</p> <p>'1' to 'E' = Sequence number from 1 to 14</p> <p>'F' = Sequence number of 15 or above</p>
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.

Table 34: Issuer Script Results

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 new response codes listed in Table 35 when transactions are not authorised online:

Authorisation Response Code	Value
Offline approved	Y1
Offline declined	Z1
Unable to go online, offline approved	Y3
Unable to go online, offline declined	Z3

Table 35: Authorisation Response Codes

The terminal shall never modify the Authorisation Response Code returned in the response message.²⁶

A7 Biometric Terminal Capabilities

This section provides the coding for Biometric Terminal Capabilities:

- Byte 1: Offline Biometric Capabilities
- Byte 2: Online Biometric Capabilities
- Byte 3: RFU

If any of the Offline Biometric Capabilities is supported in Biometric Terminal Capabilities, then the ‘Offline Biometric’ bit of the Terminal Capabilities shall be set to 1. If any of the Online Biometric Capabilities is supported in Biometric Terminal Capabilities, then the ‘Online Biometric’ bit of the Terminal Capabilities shall be set to 1.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Facial biometric for offline verification
x	1	x	x	x	x	x	x	Finger biometric for offline verification
x	x	1	x	x	x	x	x	Iris biometric for offline verification
x	x	x	1	x	x	x	x	Palm biometric for offline verification
x	x	x	x	1	x	x	x	Voice biometric for offline verification
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 36: Biometric Term. Cap. Byte 1 – Offline Biometric Capabilities

²⁶ The card’s final decision is reflected in the Cryptogram Information Data and not in the Authorisation Response Code.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Facial biometric for online verification
x	1	x	x	x	x	x	x	Finger biometric for online verification
x	x	1	x	x	x	x	x	Iris biometric for online verification
x	x	x	1	x	x	x	x	Palm biometric for online verification
x	x	x	x	1	x	x	x	Voice biometric for online verification
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 37: Biometric Term. Cap. Byte 2 – Online Biometric Capabilities

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 38: Biometric Terminal Capabilities Byte 3 – RFU

Annex B Common Character Set

Table 39 shows the character set common to all parts of ISO/IEC 8859:

		b8	0	0	0	0	0	0	0	0	0	0	0
		b7	0	0	0	0	1	1	1	1	1	1	1
		b6	0	0	1	1	0	0	1	1	1	1	1
		b5	0	1	0	1	0	1	0	1	0	1	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 39: 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/IEC 8859 that allows the relevant diacritic marks to be displayed.

If the terminal supports Part 1 of ISO/IEC 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/IEC 8859 (the Latin 1 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 ‘ACCEPTTE’, without the use of diacritic marks. The cardholder should be able to comprehend the message.

Annex C Example Data Element Conversion

For the data elements listed in section 12.1, Table 40 illustrates an example of the relationship between:

- the ICC-related data described in Book 3 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'	Application Cryptogram	55	ICC System-Related Data
'5F25'	Application Effective Date	see note	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

Table 40: Data Element Conversion

Note: Only defined in ISO 8583:1993.

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	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
'9F10'	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
'9F25'	Last 4 Digits of PAN		See EMV Tokenisation Framework
'9F15'	Merchant Category Code	18	Merchant Type
'9F16'	Merchant Identifier	42	Card Acceptor Identification
'9F24'	Payment Account Reference (PAR)		See EMV Tokenisation Framework
'9F39'	POS Entry Mode	22	POS Entry Mode (pos. 1–2)
'5F30'	Service Code	40	Service Code
'9F33'	Terminal Capabilities	see note	CAD Management

Table 40: Data Element Conversion, continued

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

Tag	ICC Data	Bit	Message Data Name
'9F1A'	Terminal Country Code	19	Acquiring Institution Country Code
		43	Card Acceptor Name/Location (if terminal/acquirer countries are different)
'9F1C'	Terminal Identification	41	Card Acceptor Terminal Identification
'9F35'	Terminal Type	see note	CAD Management
'9F19'	Token Requestor ID		See EMV Tokenisation Framework
'95'	TVR	55	ICC System-Related Data
'57'	Track 2 Equivalent Data	35	Track 2 Data
—	Transaction Amount	4	Amount, Transaction
'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 40: Data Element Conversion, continued

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

Annex D Informative Terminal Guidelines

D1 Terminal Usage

Because terminals are installed in a variety of environments and locations, it is recognised that throughout the world different attempts have been made to group relevant guidelines into different categories:

- Climatic conditions where the terminal is used (climate controlled, 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 section 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 comply 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 supports necessary terminal functions (see EMV Contact Interface Specification for power/current requirements).

Power consumption can be reduced by energising the terminal automatically at card insertion.

D3 Keypad

To prevent characters printed on the keys of the keypad 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 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 ²⁷
NF C 98-020:1986	Telephone and telematic equipment. Electromagnetic compatibility

²⁷ This standard applies only to stand-alone terminals.

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
<u>Physical:</u>	
Keypad	Attendant keypad (numeric and function keys) + PIN pad
Display	One for attendant One for cardholder
Printer	Yes for attendant
Magnetic stripe reader	Yes
IC reader	Yes
<u>Functional:</u>	
Language selection	Supports Part 1 of ISO/IEC 8859
Transaction type	Goods, cashback
SDA, DDA	Yes
Cardholder verification	Offline PIN, signature
Card capture	No
Online capable	Yes
Offline capable	Yes

Table 41: 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 = 'C0' (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
<u>Physical:</u>	
Keypad	PIN pad + function keys
Display	Yes for cardholder
Printer	Yes for cardholder
Magnetic stripe reader	Yes
IC reader	Yes
<u>Functional:</u>	
Language selection	Supports Part 5 of ISO/IEC 8859
Transaction type	Cash, inquiry, transfer, payment
SDA	No
Cardholder verification	Online PIN
Card capture	Yes
Online capable	Yes
Offline capable	No

Table 42: 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 = '40' (hexadecimal)
 byte 3 = '20' (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
<u>Physical:</u>	
Keypad	Function keys
Display	No
Printer	No
Magnetic stripe reader	Yes
IC reader	Yes
<u>Functional:</u>	
Language selection	No
Transaction type	Goods
SDA, DDA	Yes
Cardholder verification	No
Card capture	No
Online capable	No
Offline capable	Yes

Table 43: 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 = 'C0' (hexadecimal)
- Additional Terminal Capabilities, byte 1 = '40' (hexadecimal)
 byte 2 = '00' (hexadecimal)
 byte 3 = '10' (hexadecimal)
 byte 4 = '00' (hexadecimal)
 byte 5 = '00' (hexadecimal)

Index

A

Abbreviations.....	26
Acquirer Interface	
Exception Handling	105
Advice Incidents	107
Authorisation Response Incidents	106
Downgraded Authorisation	106
Script Incidents	107
Unable to Go Online	105
Message Content.....	90
Authorisation Request.....	92
Authorisation Response	96
Batch Data Capture	97
Financial Transaction Confirmation.....	97
Financial Transaction Request	94
Financial Transaction Response.....	96
Online Advice	101
Reconciliation	100
Reversal	103
Additional Terminal Capabilities	
Terminal Data Input Capability	113
Terminal Data Output Capability.....	114, 115
Transaction Type Capability	112, 113
Advice Incidents.....	107
Amount Entry and Management.....	57
Application Dependent Data.....	81
Application Independent Data	79
Application Independent ICC to Terminal Interface	
Requirements	43
Application Selection.....	89
Application Specification	43
Authorisation Request.....	92
Authorisation Response	96
Authorisation Response Code	
Coding	116
Authorisation Response Incidents.....	106

B

Batch Data Capture.....	97
Battery Requirements	124
Biometric Terminal Capabilities	
Offline Biometric Capabilities	117

C

Card Action Analysis.....	54
Card Reading	59
Exception Handling	60
IC Reader.....	60

Cardholder and Attendant Interface	
Application Selection.....	89
Language Selection	85
Standard Messages.....	86
Cardholder Verification	See CVM
Character Set.....	119
Coding	
Additional Terminal Capabilities	112
Authorisation Response Code	116
Terminal Capabilities.....	110
Terminal Data Elements.....	109
Terminal Type.....	109
Command Keys	63
Common Character Set.....	119
Conditions for Support of Functions.....	56
CVM.....	47
CVM Results	49

D

Data Element Conversion, Example	121
Data Element Format Conventions	35
Data Elements	
Authorisation Request	
Existing	93
ICC-specific	92
Batch Data Capture	
Existing	99
ICC-specific	97
Financial Transaction Confirmation	
Existing	97
ICC-specific	97
Financial Transaction Request	
Existing	94
ICC-specific	94
Online Advice	
Existing	102
ICC-specific	101
Reconciliation	
Existing	100
Response	
Existing	96
ICC-specific	96
Reversal	
Existing	104
ICC-specific	103
Data Elements, Terminal	109
Data Management	79
Application Dependent Data	81
Application Independent Data.....	79
Data, Application Dependent.....	81
Data, Application Independent	79
Date Management	61
Definitions	18
Display.....	65, 125

Downgraded Authorisation..... 106

E

Example of Data Element Conversion..... 121
 Examples of Terminals 127
 Exception Handling 60, 105
 Advice Incidents 107
 Authorisation Response Incidents 106
 Downgraded Authorisation 106
 Script Incidents 107
 Unable to Go Online 105
 External Power Supply 124

F

Financial Transaction Confirmation 97
 Financial Transaction Request..... 94
 Financial Transaction Response..... 96
 Functional Requirements 43
 Amount Entry and Management 57
 Application Independent ICC to Terminal Interface 43
 Application Specification
 Data Authentication 44
 Application Specification..... 43
 Initiate Application Processing 44
 Application Specification
 Processing Restrictions 47
 Application Specification
 Cardholder Verification Processing 47
 Application Specification
 Cardholder Verification Processing
 Offline CVM 48
 Application Specification
 Cardholder Verification Processing
 Online CVM..... 48
 Application Specification
 Cardholder Verification Processing
 PIN Entry Bypass..... 49
 Application Specification
 Cardholder Verification Processing
 Signature (Paper)..... 49
 Application Specification
 Cardholder Verification Processing
 CVM Results 49
 Application Specification
 Terminal Risk Management 53
 Application Specification
 Terminal Action Analysis 53
 Application Specification
 Card Action Analysis 54
 Application Specification
 Online Processing 55
 Application Specification
 Issuer-to-Card Script Processing..... 55
 Card Reading 59
 Exception Handling..... 60
 IC Reader 60

Conditions for Support of Functions 56
 Data Management 61
 Date Authentication 61
 Date Management 61
 Processing Restrictions 61
 Security and Key Management 43
 Transaction Forced Acceptance 58
 Transaction Forced Online 58
 Transaction Sequence Counter..... 59
 Unpredictable Number 59
 Voice Referrals 57
 Functions
 Conditions for Support..... 56

I

IC Reader 60
 Informative References 125
 Informative Terminal Guidelines 124
 Display 125
 Keypad 125
 Power Supply 124
 Terminal Usage..... 124
 Initiate Application Processing 44
 Issuer-to-Card Script Processing 55

K

Key Colours 63
 Key Types..... 62
 Keypad..... 62, 125
 Command Keys..... 63
 PIN Pad 64

L

Language Selection..... 85

M

Magnetic Stripe Reader..... 66
 Memory Protection 65
 Merchant Host 41
 Message Content..... 90
 Authorisation Request..... 92
 Authorisation Response 96
 Batch Data Capture 97
 Financial Transaction Confirmation..... 97
 Financial Transaction Request 94
 Financial Transaction Response..... 96
 Online Advice 101
 Reconciliation 100
 Reversal 103
 Messages
 Standard 86

N

Normative References..... 15
 Notations..... 33

O

Offline CVM..... 48
 Offline Data Authentication..... 44
 Online Advice..... 101
 Online CVM..... 48
 Online Processing..... 55

P

Physical Characteristics..... 62
 Clock..... 65
 Display..... 65
 Keypad..... 62
 Command Keys..... 63
 PIN Pad..... 64
 Magnetic Stripe Reader..... 66
 Memory Protection..... 65
 Printer..... 65
 PIN Entry Bypass..... 49
 PIN Pad..... 64
 Plugs and Sockets..... 75
 Power Supply..... 124
 Printer..... 65
 Processing Restrictions..... 47, 61

R

Reconciliation..... 100
 References
 Informative..... 125
 Normative..... 15
 Referrals..... 57
 Reversal..... 103
 Revision Log..... 3

S

Scope..... 12
 Script Incidents..... 107
 Security and Key Management..... 43
 Signature (Paper)..... 49
 Socket/Plug Relationship..... 76
 Software Management..... 78
 Standard Messages..... 86

T

Terminal
 Capabilities..... 39
 Configurations..... 40
 Attended..... 40
 Cardholder-Controlled..... 42
 Merchant Host..... 41
 Examples..... 127
 ATM..... 129
 POS Terminal or Electronic Cash Register..... 128
 Vending Machine..... 130
 Types..... 38
 Terminal Action Analysis..... 53
 Terminal Capabilities
 Card Data Input Capability..... 110
 CVM Capability..... 111
 Security Capability..... 111
 Terminal Data Elements, Coding..... 109
 Terminal Guidelines, Informative..... 124
 Terminal Risk Management..... 53
 Terminal Software Architecture..... 68
 Application Libraries..... 69
 Application Program Interface..... 70
 Environmental Changes..... 68
 Interpreter
 Application Code Portability..... 72
 Concept..... 71
 Kernel..... 72
 Virtual Machine..... 72
 Plugs and Sockets..... 75
 Terminal Type, Coding..... 109
 Terminal Types, Terminology..... 38
 Terminal Usage..... 124
 Terminal Verification Results..... See TVR
 Terminology..... 36
 Transaction Forced Acceptance..... 58
 Transaction Forced Online..... 58
 Transaction Sequence Counter..... 59
 Transaction Status Information..... See TSI
 TSI..... 106
 TVR..... 44, 48, 49, 53, 58

U

Unable to Go Online..... 105
 Unpredictable Number..... 59

V

Voice Referrals..... 57