Annex A Data Elements Dictionary

Table 33 defines those data elements that may be used for financial transaction interchange and their mapping onto data objects and files. Table 34 lists the data elements in tag sequence.

The characters used in the "Format" column are described in section 4.3, Data Element Format Convention.

A1 Data Elements by Name

Name	Description	Source	Format	Template	Tag	Length
Account Type	Indicates the type of account selected on the terminal, coded as specified in Annex G	Terminal	n 2	—	'5F57'	1
Acquirer Identifier	Uniquely identifies the acquirer within each payment system	Terminal	n 6-11	—	'9F01'	6
Additional Terminal Capabilities	Indicates the data input and output capabilities of the terminal	Terminal	b	—	'9F40'	5
Amount, Authorised (Binary)	Authorised amount of the transaction (excluding adjustments)	Terminal	b	—	'81'	4

Table 33: Data Elements Dictionary

Name	Description	Source	Format	Template	Tag	Length
Amount, Authorised (Numeric)	Authorised amount of the transaction (excluding adjustments)	Terminal	n 12	—	'9F02'	6
Amount, Other (Binary)	Secondary amount associated with the transaction representing a cashback amount	Terminal	b	—	'9F04'	4
Amount, Other (Numeric)	Secondary amount associated with the transaction representing a cashback amount	Terminal	n 12	—	'9F03'	6
Amount, Reference Currency	Authorised amount expressed in the reference currency	Terminal	b	—	'9F3A'	4
Application Cryptogram	Cryptogram returned by the ICC in response of the GENERATE AC command	ICC	b	'77' or '80'	'9F26'	8
Application Currency Code	Indicates the currency in which the account is managed according to ISO 4217	ICC	n 3	'70' or '77'	'9F42'	2
Application Currency Exponent	Indicates the implied position of the decimal point from the right of the amount represented according to ISO 4217	ICC	n 1	'70' or '77'	'9F44'	1
Application Discretionary Data	Issuer or payment system specified data relating to the application	ICC	b	'70' or '77'	'9F05'	1-32
Application Effective Date	Date from which the application may be used	ICC	n 6 YYMMDD	'70' or '77'	'5F25'	3

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Application Expiration Date	Date after which application expires	ICC	n 6 YYMMDD	'70' or '77'	'5F24'	3
Application File Locator (AFL)	Indicates the location (SFI, range of records) of the AEFs related to a given application	ICC	var.	'77' or '80'	'94'	var. up to 252
Application Dedicated File (ADF) Name	Identifies the application as described in ISO/IEC 7816-5	ICC	b	'61'	'4F'	5-16
Application Identifier (AID) – terminal	Identifies the application as described in ISO/IEC 7816-5	Terminal	b	—	'9F06'	5-16
Application Interchange Profile	Indicates the capabilities of the card to support specific functions in the application	ICC	b	'77' or '80'	'82'	2
Application Label	Mnemonic associated with the AID according to ISO/IEC 7816-5	ICC	ans with the special character limited to space	'61' or 'A5'	'50'	1-16
Application Preferred Name	Preferred mnemonic associated with the AID	ICC	ans (see section 4.3)	'61' or 'A5'	'9F12'	1-16
Application Primary Account Number (PAN)	Valid cardholder account number	ICC	cn var. up to 19	'70' or '77'	'5A'	var. up to 10

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Application Primary Account Number (PAN) Sequence Number	Identifies and differentiates cards with the same PAN	ICC	n 2	'70' or '77'	'5F34'	1
Application Priority Indicator	Indicates the priority of a given application or group of applications in a directory	ICC	b	'61' or 'A5'	'87'	1
Application Reference Currency	1-4 currency codes used between the terminal and the ICC when the Transaction Currency Code is different from the Application Currency Code; each code is 3 digits according to ISO 4217	ICC	n 3	'70' or '77'	'9F3B'	2-8
Application Reference Currency Exponent	Indicates the implied position of the decimal point from the right of the amount, for each of the 1-4 reference currencies represented according to ISO 4217	ICC	n 1	'70' or '77'	'9F43'	1-4

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Application Selection Indicator	For an application in the ICC to be supported by an application in the terminal, the Application Selection Indicator indicates whether the associated AID in the terminal must match the AID in the card exactly, including the length of the AID, or only up to the length of the AID in the terminal There is only one Application Selection Indicator per AID supported by the terminal	Terminal	At the discretion of the terminal. The data is not sent across the interface	—	—	See format
Application Template	Contains one or more data objects relevant to an application directory entry according to ISO/IEC 7816-5	ICC	b	'70'	'61'	var. up to 252
Application Transaction Counter (ATC)	Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC)	ICC	b	'77' or '80'	'9F36'	2
Application Usage Control	Indicates issuer's specified restrictions on the geographic usage and services allowed for the application	ICC	b	'70' or '77'	'9F07'	2
Application Version Number	Version number assigned by the payment system for the application	ICC	b	'70' or '77'	'9F08'	2
Application Version Number	Version number assigned by the payment system for the application	Terminal	b	—	'9F09'	2

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Authorisation Code	Value generated by the authorisation authority for an approved transaction	Issuer	As defined by the Payment Systems	—	'89'	6
Authorisation Response Code	Code that defines the disposition of a message	Issuer/ Terminal	an 2	—	'8A'	2
Authorisation Response Cryptogram (ARPC)	Cryptogram generated by the issuer and used by the card to verify that the response came from the issuer.	Issuer	b	—	—	4 or 8
Bank Identifier Code (BIC)	Uniquely identifies a bank as defined in ISO 9362.	ICC	var.	'BF0C' or '73'	'5F54'	8 or 11
Card Risk Management Data Object List 1 (CDOL1)	List of data objects (tag and length) to be passed to the ICC in the first GENERATE AC command	ICC	b	'70' or '77'	'8C'	var. up to 252
Card Risk Management Data Object List 2 (CDOL2)	List of data objects (tag and length) to be passed to the ICC in the second GENERATE AC command	ICC	b	'70' or '77'	'8D'	var. up to 252

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Card Status Update (CSU)	Contains data sent to the ICC to indicate whether the issuer approves or declines the transaction, and to initiate actions specified by the issuer. Transmitted to the card in Issuer Authentication Data.	Issuer	b	—	—	4
Cardholder Name	Indicates cardholder name according to ISO 7813	ICC	ans 2-26	'70' or '77'	'5F20'	2-26
Cardholder Name Extended	Indicates the whole cardholder name when greater than 26 characters using the same coding convention as in ISO 7813	ICC	ans 27-45	'70' or '77'	'9F0B'	27-45
Cardholder Verification Method (CVM) List	Identifies a method of verification of the cardholder supported by the application	ICC	b	'70' or '77'	'8E'	10-252
Cardholder Verification Method (CVM) Results	Indicates the results of the last CVM performed	Terminal	b	—	'9F34'	3
Certification Authority Public Key Check Sum	A check value calculated on the concatenation of all parts of the Certification Authority Public Key (RID, Certification Authority Public Key Index, Certification Authority Public Key Modulus, Certification Authority Public Key Exponent) using SHA-1	Terminal	b	—	—	20

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Certification Authority Public Key Exponent	Value of the exponent part of the Certification Authority Public Key	Terminal	b	—	—	1 or 3
Certification Authority Public Key Index	Identifies the certification authority's public key in conjunction with the RID	ICC	b	'70' or '77'	'8F'	1
Certification Authority Public Key Index	Identifies the certification authority's public key in conjunction with the RID	Terminal	b	—	'9F22'	1
Certification Authority Public Key Modulus	Value of the modulus part of the Certification Authority Public Key	Terminal	b	—	—	NCA (up to 248)
Command Template	Identifies the data field of a command message	Terminal	b	—	'83'	var.
Cryptogram Information Data	Indicates the type of cryptogram and the actions to be performed by the terminal	ICC	b	'77' or '80'	'9F27'	1
Data Authentication Code	An issuer assigned value that is retained by the terminal during the verification process of the Signed Static Application Data	ICC	b	—	'9F45'	2
Dedicated File (DF) Name	Identifies the name of the DF as described in ISO/IEC 7816-4	ICC	b	'6F'	'84'	5-16

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Default Dynamic Data Authentication Data Object List (DDOL)	DDOL to be used for constructing the INTERNAL AUTHENTICATE command if the DDOL in the card is not present	Terminal	b	—	—	var.
Default Transaction Certificate Data Object List (TDOL)	TDOL to be used for generating the TC Hash Value if the TDOL in the card is not present	Terminal	b	—	—	var.
Directory Definition File (DDF) Name	Identifies the name of a DF associated with a directory	ICC	b	'61'	'9D'	5-16
Directory Discretionary Template	Issuer discretionary part of the directory according to ISO/IEC 7816-5	ICC	var.	'61'	'73'	var. up to 252
Dynamic Data Authentication Data Object List (DDOL)	List of data objects (tag and length) to be passed to the ICC in the INTERNAL AUTHENTICATE command	ICC	b	'70' or '77'	'9F49'	up to 252
Enciphered Personal Identification Number (PIN) Data	Transaction PIN enciphered at the PIN pad for online verification or for offline verification if the PIN pad and IFD are not a single integrated device	Terminal	b	—	—	8

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
File Control Information (FCI) Issuer Discretionary Data	Issuer discretionary part of the FCI	ICC	var.	'A5'	'BF0C'	var. up to 222
File Control Information (FCI) Proprietary Template	Identifies the data object proprietary to this specification in the FCI template according to ISO/IEC 7816-4	ICC	var.	'6F'	'A5'	var.
File Control Information (FCI) Template	Identifies the FCI template according to ISO/IEC 7816-4	ICC	var.	—	'6F'	var. up to 252
ICC Dynamic Number	Time-variant number generated by the ICC, to be captured by the terminal	ICC	b	—	'9F4C'	2-8
Integrated Circuit Card (ICC) PIN Encipherment Public Key Certificate	ICC PIN Encipherment Public Key certified by the issuer	ICC	b	'70' or '77'	'9F2D'	NI

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Integrated Circuit Card (ICC) PIN Encipherment Public Key Exponent	ICC PIN Encipherment Public Key Exponent used for PIN encipherment	ICC	b	'70' or '77'	'9F2E'	1 or 3
Integrated Circuit Card (ICC) PIN Encipherment Public Key Remainder	Remaining digits of the ICC PIN Encipherment Public Key Modulus	ICC	b	'70' or '77'	'9F2F'	NPE – NI + 42
Integrated Circuit Card (ICC) Public Key Certificate	ICC Public Key certified by the issuer	ICC	b	'70' or '77'	'9F46'	NI
Integrated Circuit Card (ICC) Public Key Exponent	ICC Public Key Exponent used for the verification of the Signed Dynamic Application Data	ICC	b	'70' or '77'	'9F47'	1 to 3
Integrated Circuit Card (ICC) Public Key Remainder	Remaining digits of the ICC Public Key Modulus	ICC	b	'70' or '77'	'9F48'	NIC – NI + 42

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Interface Device (IFD) Serial Number	Unique and permanent serial number assigned to the IFD by the manufacturer	Terminal	an 8	—	'9F1E'	8
International Bank Account Number (IBAN)	Uniquely identifies the account of a customer at a financial institution as defined in ISO 13616.	ICC	var.	'BF0C' or '73'	'5F53'	Var. up to 34
Issuer Action Code - Default	Specifies the issuer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online	ICC	b	'70' or '77'	'9F0D'	5
Issuer Action Code - Denial	Specifies the issuer's conditions that cause the denial of a transaction without attempt to go online	ICC	b	'70' or '77'	'9F0E'	5
Issuer Action Code - Online	Specifies the issuer's conditions that cause a transaction to be transmitted online	ICC	b	'70' or '77'	'9F0F'	5
Issuer Application Data	Contains proprietary application data for transmission to the issuer in an online transaction. **Note:** For CCD-compliant applications, Annex C, section C7 defines the specific coding of the Issuer Application Data (IAD). To avoid potential conflicts with CCD-compliant applications, it is strongly recommended that the IAD data element in an application that is not CCD-compliant should not use the coding for a CCD-compliant application	ICC	b	'77' or '80'	'9F10'	var. up to 32

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Issuer Authentication Data	Data sent to the ICC for online issuer authentication	Issuer	b	—	'91'	8-16
Issuer Code Table Index	Indicates the code table according to ISO/IEC 8859 for displaying the Application Preferred Name	ICC	n 2	'A5'	'9F11'	1
Issuer Country Code	Indicates the country of the issuer according to ISO 3166	ICC	n 3	'70' or '77'	'5F28'	2
Issuer Country Code (alpha2 format)	Indicates the country of the issuer as defined in ISO 3166 (using a 2 character alphabetic code)	ICC	a 2	'BF0C' or '73'	'5F55'	2
Issuer Country Code (alpha3 format)	Indicates the country of the issuer as defined in ISO 3166 (using a 3 character alphabetic code)	ICC	a 3	'BF0C' or '73'	'5F56'	3
Issuer Identification Number (IIN)	The number that identifies the major industry and the card issuer and that forms the first part of the Primary Account Number (PAN)	ICC	n 6	'BF0C' or '73'	'42'	3
Issuer Public Key Certificate	Issuer public key certified by a certification authority	ICC	b	'70' or '77'	'90'	NCA
Issuer Public Key Exponent	Issuer public key exponent used for the verification of the Signed Static Application Data and the ICC Public Key Certificate	ICC	b	'70' or '77'	'9F32'	1 to 3

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Issuer Public Key Remainder	Remaining digits of the Issuer Public Key Modulus	ICC	b	'70' or '77'	'92'	NI – NCA + 36
Issuer Script Command	Contains a command for transmission to the ICC	Issuer	b	'71' or '72'	'86'	var. up to 261
Issuer Script Identifier	Identification of the Issuer Script	Issuer	b	'71' or '72'	'9F18'	4
Issuer Script Results	Indicates the result of the terminal script processing	Terminal	b	—	—	var.
Issuer Script Template 1	Contains proprietary issuer data for transmission to the ICC before the second GENERATE AC command	Issuer	b	—	'71'	var.
Issuer Script Template 2	Contains proprietary issuer data for transmission to the ICC after the second GENERATE AC command	Issuer	b	—	'72'	var.
Issuer URL	The URL provides the location of the Issuer's Library Server on the Internet.	ICC	ans	'BF0C' or '73'	'5F50'	var.
Language Preference	1-4 languages stored in order of preference, each represented by 2 alphabetical characters according to ISO 639 **Note:** EMVCo strongly recommends that cards be personalised with data element '5F2D' coded in lowercase, but that terminals accept the data element whether it is coded in upper or lower case.	ICC	an 2	'A5'	'5F2D'	2-8

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Last Online Application Transaction Counter (ATC) Register	ATC value of the last transaction that went online	ICC	b	—	'9F13'	2
Log Entry	Provides the SFI of the Transaction Log file and its number of records	ICC	b	'BF0C' or '73'	'9F4D'	2
Log Format	List (in tag and length format) of data objects representing the logged data elements that are passed to the terminal when a transaction log record is read	ICC	b	—	'9F4F'	var.
Lower Consecutive Offline Limit	Issuer-specified preference for the maximum number of consecutive offline transactions for this ICC application allowed in a terminal with online capability	ICC	b	'70' or '77'	'9F14'	1
Maximum Target Percentage to be used for Biased Random Selection	Value used in terminal risk management for random transaction selection	Terminal	—	—	—	—
Merchant Category Code	Classifies the type of business being done by the merchant, represented according to ISO 8583:1993 for Card Acceptor Business Code	Terminal	n 4	—	'9F15'	2

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Merchant Identifier	When concatenated with the Acquirer Identifier, uniquely identifies a given merchant	Terminal	ans 15	—	'9F16'	15
Merchant Name and Location	Indicates the name and location of the merchant	Terminal	ans	—	'9F4E'	var.
Message Type	Indicates whether the batch data capture record is a financial record or advice	Terminal	n 2	—	—	1
Personal Identification Number (PIN) Pad Secret Key	Secret key of a symmetric algorithm used by the PIN pad to encipher the PIN and by the card reader to decipher the PIN if the PIN pad and card reader are not integrated	Terminal	—	—	—	—
Personal Identification Number (PIN) Try Counter	Number of PIN tries remaining	ICC	b	—	'9F17'	1
Point-of-Service (POS) Entry Mode	Indicates the method by which the PAN was entered, according to the first two digits of the ISO 8583:1987 POS Entry Mode	Terminal	n 2	—	'9F39'	1
Processing Options Data Object List (PDOL)	Contains a list of terminal resident data objects (tags and lengths) needed by the ICC in processing the GET PROCESSING OPTIONS command	ICC	b	'A5'	'9F38'	var.
Proprietary Authentication Data	Contains issuer data for transmission to the card in the Issuer Authentication Data of an online transaction.	Issuer	b	—	—	var. up to 8

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
READ RECORD Response Message Template	Contains the contents of the record read. (Mandatory for SFIs 1-10. Response messages for SFIs 11-30 are outside the scope of EMV, but may use template '70')	ICC	var.	—	'70'	var. up to 252
Response Message Template Format 1	Contains the data objects (without tags and lengths) returned by the ICC in response to a command	ICC	var.	—	'80'	var.
Response Message Template Format 2	Contains the data objects (with tags and lengths) returned by the ICC in response to a command	ICC	var.	—	'77'	var.
Service Code	Service code as defined in ISO/IEC 7813 for track 1 and track 2	ICC	n 3	'70' or '77'	'5F30'	2
Short File Identifier (SFI)	Identifies the AEF referenced in commands related to a given ADF or DDF. It is a binary data object having a value in the range 1 to 30 and with the three high order bits set to zero.	ICC	b	'A5'	'88'	1
Signed Dynamic Application Data	Digital signature on critical application parameters for DDA or CDA	ICC	b	'77' or '80'	'9F4B'	NIC
Signed Static Application Data	Digital signature on critical application parameters for SDA	ICC	b	'70' or '77'	'93'	NI

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Static Data Authentication Tag List	List of tags of primitive data objects defined in this specification whose value fields are to be included in the Signed Static or Dynamic Application Data	ICC	—	'70' or '77'	'9F4A'	var.
Target Percentage to be Used for Random Selection	Value used in terminal risk management for random transaction selection	Terminal	—	—	—	—
Terminal Action Code - Default	Specifies the acquirer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online	Terminal	b	—	—	5
Terminal Action Code - Denial	Specifies the acquirer's conditions that cause the denial of a transaction without attempt to go online	Terminal	b	—	—	5
Terminal Action Code - Online	Specifies the acquirer's conditions that cause a transaction to be transmitted online	Terminal	b	—	—	5
Terminal Capabilities	Indicates the card data input, CVM, and security capabilities of the terminal	Terminal	b	—	'9F33'	3
Terminal Country Code	Indicates the country of the terminal, represented according to ISO 3166	Terminal	n 3	—	'9F1A'	2
Terminal Floor Limit	Indicates the floor limit in the terminal in conjunction with the AID	Terminal	b	—	'9F1B'	4

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Terminal Identification	Designates the unique location of a terminal at a merchant	Terminal	an 8	—	'9F1C'	8
Terminal Risk Management Data	Application-specific value used by the card for risk management purposes	Terminal	b	—	'9F1D'	1-8
Terminal Type	Indicates the environment of the terminal, its communications capability, and its operational control	Terminal	n 2	—	'9F35'	1
Terminal Verification Results	Status of the different functions as seen from the terminal	Terminal	b	—	'95'	5
Threshold Value for Biased Random Selection	Value used in terminal risk management for random transaction selection	Terminal	—	—	—	—
Track 1 Discretionary Data	Discretionary part of track 1 according to ISO/IEC 7813	ICC	ans	'70' or '77'	'9F1F'	var.
Track 2 Discretionary Data	Discretionary part of track 2 according to ISO/IEC 7813	ICC	cn	'70' or '77'	'9F20'	var.

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Track 2 Equivalent Data	Contains the data elements of track 2 according to ISO/IEC 7813, excluding start sentinel, end sentinel, and Longitudinal Redundancy Check (LRC), as follows: Primary Account Number Field Separator (Hex 'D') Expiration Date (YYMM) Service Code Discretionary Data (defined by individual payment systems) Pad with one Hex 'F' if needed to ensure whole bytes	ICC	b n, var. up to 19 b n 4 n 3 n, var. b	'70' or '77'	'57'	var. up to 19
Transaction Amount	Clearing amount of the transaction, including tips and other adjustments	Terminal	n 12	—	—	6
Transaction Certificate Data Object List (TDOL)	List of data objects (tag and length) to be used by the terminal in generating the TC Hash Value	ICC	b	'70' or '77'	'97'	var. up to 252
Transaction Certificate (TC) Hash Value	Result of a hash function specified in Book 2, Annex B3.1	Terminal	b	—	'98'	20

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217	Terminal	n 3	—	'5F2A'	2
Transaction Currency Exponent	Indicates the implied position of the decimal point from the right of the transaction amount represented according to ISO 4217	Terminal	n 1	—	'5F36'	1
Transaction Date	Local date that the transaction was authorised	Terminal	n 6 YYMMDD	—	'9A'	3
Transaction Personal Identification Number (PIN) Data	Data entered by the cardholder for the purpose of the PIN verification	Terminal	b	—	'99'	var.
Transaction Reference Currency Code	Code defining the common currency used by the terminal in case the Transaction Currency Code is different from the Application Currency Code	Terminal	n 3	—	'9F3C'	2
Transaction Reference Currency Conversion	Factor used in the conversion from the Transaction Currency Code to the Transaction Reference Currency Code	Terminal	n 8	—	—	4
Transaction Reference Currency Exponent	Indicates the implied position of the decimal point from the right of the transaction amount, with the Transaction Reference Currency Code represented according to ISO 4217	Terminal	n 1	—	'9F3D'	1

Table 33: Data Elements Dictionary, continued

Name	Description	Source	Format	Template	Tag	Length
Transaction Sequence Counter	Counter maintained by the terminal that is incremented by one for each transaction	Terminal	n 4-8	—	'9F41'	2-4
Transaction Status Information	Indicates the functions performed in a transaction	Terminal	b	—	'9B'	2
Transaction Time	Local time that the transaction was authorised	Terminal	n 6 HHMMSS	—	'9F21'	3
Transaction Type	Indicates the type of financial transaction, represented by the first two digits of the ISO 8583:1987 Processing Code. The actual values to be used for the Transaction Type data element are defined by the relevant payment system	Terminal	n 2	—	'9C'	1
Unpredictable Number	Value to provide variability and uniqueness to the generation of a cryptogram	Terminal	b	—	'9F37'	4
Upper Consecutive Offline Limit	Issuer-specified preference for the maximum number of consecutive offline transactions for this ICC application allowed in a terminal without online capability	ICC	b	'70' or '77'	'9F23'	1

Table 33: Data Elements Dictionary, continued

When the length defined for the data object is greater than the length of the actual data, the following rules apply:

- A data element in format n is right justified and padded with leading hexadecimal zeroes.
- A data element in format cn is left justified and padded with trailing hexadecimal 'F's.
- A data element in format a, an, or ans is left justified and padded with trailing hexadecimal zeroes.

When data is moved from one entity to another (for example, card to terminal), it shall always be passed in order from high order to low order, regardless of how it is internally stored. The same rule applies when concatenating data.

Note: Data that can occur in template '70' or '77' can never occur in both.

A2 Data Elements by Tag

Name	Template	Tag
Issuer Identification Number (IIN)	'BF0C' or '73'	'42'
Application Dedicated File (ADF) Name	'61'	'4F'
Application Label	'61' or 'A5'	'50'
Track 2 Equivalent Data	'70' or '77'	'57'
Application Primary Account Number (PAN)	'70' or '77'	'5A'
Cardholder Name	'70' or '77'	'5F20'
Application Expiration Date	'70' or '77'	'5F24'
Application Effective Date	'70' or '77'	'5F25'
Issuer Country Code	'70' or '77'	'5F28'
Transaction Currency Code	—	'5F2A'
Language Preference	'A5'	'5F2D'
Service Code	'70' or '77'	'5F30'
Application Primary Account Number (PAN) Sequence Number	'70' or '77'	'5F34'
Transaction Currency Exponent	—	'5F36'
Issuer URL	'BF0C' or '73'	'5F50'
International Bank Account Number (IBAN)	'BF0C' or '73'	'5F53'
Bank Identifier Code (BIC)	'BF0C' or '73'	'5F54'
Issuer Country Code (alpha2 format)	'BF0C' or '73'	'5F55'
Issuer Country Code (alpha3 format)	'BF0C' or '73'	'5F56'
Account Type	—	'5F57'
Application Template	'70' or '77'	'61'
File Control Information (FCI) Template	—	'6F'

Table 34: Data Elements Tags

Name	Template	Tag
READ RECORD Response Message Template	—	'70'
Issuer Script Template 1	—	'71'
Issuer Script Template 2	—	'72'
Directory Discretionary Template	'61'	'73'
Response Message Template Format 2	—	'77'
Response Message Template Format 1	—	'80'
Amount, Authorised (Binary)	—	'81'
Application Interchange Profile	'77' or '80'	'82'
Command Template	—	'83'
Dedicated File (DF) Name	'6F'	'84'
Issuer Script Command	'71' or '72'	'86'
Application Priority Indicator	'61' or 'A5'	'87'
Short File Identifier (SFI)	'A5'	'88'
Authorisation Code	—	'89'
Authorisation Response Code	—	'8A'
Card Risk Management Data Object List 1 (CDOL1)	'70' or '77'	'8C'
Card Risk Management Data Object List 2 (CDOL2)	'70' or '77'	'8D'
Cardholder Verification Method (CVM) List	'70' or '77'	'8E'
Certification Authority Public Key Index	'70' or '77'	'8F'
Issuer Public Key Certificate	'70' or '77'	'90'
Issuer Authentication Data	—	'91'
Issuer Public Key Remainder	'70' or '77'	'92'
Signed Static Application Data	'70' or '77'	'93'
Application File Locator (AFL)	'77' or '80'	'94'
Terminal Verification Results	—	'95'
Transaction Certificate Data Object List (TDOL)	'70' or '77'	'97'
Transaction Certificate (TC) Hash Value	—	'98'
Transaction Personal Identification Number (PIN) Data	—	'99'

Table 34: Data Elements Tags, continued

Name	Template	Tag
Transaction Date	—	'9A'
Transaction Status Information	—	'9B'
Transaction Type	—	'9C'
Directory Definition File (DDF) Name	'61'	'9D'
Acquirer Identifier	—	'9F01'
Amount, Authorised (Numeric)	—	'9F02'
Amount, Other (Numeric)	—	'9F03'
Amount, Other (Binary)	—	'9F04'
Application Discretionary Data	'70' or '77'	'9F05'
Application Identifier (AID) - terminal	—	'9F06'
Application Usage Control	'70' or '77'	'9F07'
Application Version Number	'70' or '77'	'9F08'
Application Version Number	—	'9F09'
Cardholder Name Extended	'70' or '77'	'9F0B'
Issuer Action Code - Default	'70' or '77'	'9F0D'
Issuer Action Code - Denial	'70' or '77'	'9F0E'
Issuer Action Code - Online	'70' or '77'	'9F0F'
Issuer Application Data	'77' or '80'	'9F10'
Issuer Code Table Index	'A5'	'9F11'
Application Preferred Name	'61' or 'A5'	'9F12'
Last Online Application Transaction Counter (ATC) Register	—	'9F13'
Lower Consecutive Offline Limit	'70' or '77'	'9F14'
Merchant Category Code	—	'9F15'
Merchant Identifier	—	'9F16'
Personal Identification Number (PIN) Try Counter	—	'9F17'
Issuer Script Identifier	'71' or '72'	'9F18'

Table 34: Data Elements Tags, continued

Name	Template	Tag
Terminal Country Code	—	'9F1A'
Terminal Floor Limit	—	'9F1B'
Terminal Identification	—	'9F1C'
Terminal Risk Management Data	—	'9F1D'
Interface Device (IFD) Serial Number	—	'9F1E'
Track 1 Discretionary Data	'70' or '77'	'9F1F'
Track 2 Discretionary Data	'70' or '77'	'9F20'
Transaction Time	—	'9F21'
Certification Authority Public Key Index	—	'9F22'
Upper Consecutive Offline Limit	'70' or '77'	'9F23'
Application Cryptogram	'77' or '80'	'9F26'
Cryptogram Information Data	'77' or '80'	'9F27'
ICC PIN Encipherment Public Key Certificate	'70' or '77'	'9F2D'
ICC PIN Encipherment Public Key Exponent	'70' or '77'	'9F2E'
ICC PIN Encipherment Public Key Remainder	'70' or '77'	'9F2F'
Issuer Public Key Exponent	'70' or '77'	'9F32'
Terminal Capabilities	—	'9F33'
Cardholder Verification Method (CVM) Results	—	'9F34'
Terminal Type	—	'9F35'
Application Transaction Counter (ATC)	'77' or '80'	'9F36'
Unpredictable Number	—	'9F37'
Processing Options Data Object List (PDOL)	'A5'	'9F38'
Point-of-Service (POS) Entry Mode	—	'9F39'
Amount, Reference Currency	—	'9F3A'
Application Reference Currency	'70' or '77'	'9F3B'
Transaction Reference Currency Code	—	'9F3C'
Transaction Reference Currency Exponent	—	'9F3D'
Additional Terminal Capabilities	—	'9F40'
Transaction Sequence Counter	—	'9F41'

Table 34: Data Elements Tags, continued

Name	Template	Tag
Application Currency Code	'70' or '77'	'9F42'
Application Reference Currency Exponent	'70' or '77'	'9F43'
Application Currency Exponent	'70' or '77'	'9F44'
Data Authentication Code	—	'9F45'
ICC Public Key Certificate	'70' or '77'	'9F46'
ICC Public Key Exponent	'70' or '77'	'9F47'
ICC Public Key Remainder	'70' or '77'	'9F48'
Dynamic Data Authentication Data Object List (DDOL)	'70' or '77'	'9F49'
Static Data Authentication Tag List	'70' or '77'	'9F4A'
Signed Dynamic Application Data	'77' or '80'	'9F4B'
ICC Dynamic Number	—	'9F4C'
Log Entry	'BF0C' or '73'	'9F4D'
Merchant Name and Location	—	'9F4E'
Log Format	—	'9F4F'
File Control Information (FCI) Proprietary Template	'6F'	'A5'
File Control Information (FCI) Issuer Discretionary Data	'A5'	'BF0C'

Table 34: Data Elements Tags, continued

Annex B Rules for BER-TLV Data Objects

As defined in ISO/IEC 8825, a BER-TLV data object consists of 2-3 consecutive fields:

- The tag field (T) consists of one or more consecutive bytes. It indicates a class, a type, and a number (see Table 35). The tag field of the data objects described in this specification is coded on one or two bytes.
- The length field (L) consists of one or more consecutive bytes. It indicates the length of the following field. The length field of the data objects described in this specification which are transmitted over the card-terminal interface is coded on one or two bytes.

  Note: Three length bytes may be used if needed for templates '71' and '72' and tag '86' (to express length greater than 255 bytes), as they are not transmitted over the card-terminal interface.
- The value field (V) indicates the value of the data object. If L = '00', the value field is not present.

A BER-TLV data object belongs to one of the following two categories:

- A primitive data object where the value field contains a data element for financial transaction interchange.
- A constructed data object where the value field contains one or more primitive or constructed data objects. The value field of a constructed data object is called a template.

The coding of BER-TLV data objects is defined as follows.

B1 Coding of the Tag Field of BER-TLV Data Objects

Table 35 describes the first byte of the tag field of a BER-TLV data object:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							Universal class
0	1							Application class
1	0							Context-specific class
1	1							Private class
		0						Primitive data object
		1						Constructed data object
			1	1	1	1	1	See subsequent bytes
			Any other value <31					Tag number

Table 35: Tag Field Structure (First Byte) BER-TLV

According to ISO/IEC 8825, Table 36 defines the coding rules of the subsequent bytes of a BER-TLV tag when tag numbers ≥ 31 are used (that is, bits b5 - b1 of the first byte equal '11111').

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								Another byte follows
0								Last tag byte
	Any value > 0							(Part of) tag number

Table 36: Tag Field Structure (Subsequent Bytes) BER-TLV

Before, between, or after TLV-coded data objects, '00' bytes without any meaning may occur (for example, due to erased or modified TLV-coded data objects).

Note: It is strongly recommended that issuers do not use tags beginning with 'FF' for proprietary purposes, as existing terminals may not recognise 'FF' as the beginning of a constructed private class tag.

The tag field of a BER-TLV data object is coded according to the following rules:

- The following application class templates defined in ISO/IEC 7816 apply: '61' and '6F'.
- The following range of application class templates is defined in Part II: '70' to '7F'. The meaning is then specific to the context of an application according to this specification. Tags '78', '79', '7D', and '7E' are defined in ISO/IEC 7816-6 and are not used in this specification.
- The application class data objects defined in ISO/IEC 7816 and described in Part II are used according to the ISO/IEC 7816 definition.
- Context-specific class data objects are defined in the context of this specification or in the context of the template in which they appear.
- The coding of primitive context-specific class data objects in the ranges '80' to '9E' and '9F00' to '9F4F' is reserved for this specification.
- The coding of primitive context-specific class data objects in the range '9F50' to '9F7F' is reserved for the payment systems.
- The coding of tag 'BF0C' and constructed context-specific class data objects in the range 'BF20' to 'BF4F' is reserved for this specification.
- The coding of constructed context-specific class data objects in the ranges 'BF10' to 'BF1F' and 'BF50' to 'BF6F' is reserved for the payment systems.
- The coding of constructed context-specific class data objects in the ranges 'BF01' to 'BF0B', 'BF0D' to 'BF0F', and 'BF70' to 'BF7F' is left to the discretion of the issuer.
- The coding of primitive and constructed private class data objects is left to the discretion of the issuer.

B2 Coding of the Length Field of BER-TLV Data Objects

When bit b8 of the most significant byte of the length field is set to 0, the length field consists of only one byte. Bits b7 to b1 code the number of bytes of the value field. The length field is within the range 1 to 127.

When bit b8 of the most significant byte of the length field is set to 1, the subsequent bits b7 to b1 of the most significant byte code the number of subsequent bytes in the length field. The subsequent bytes code an integer representing the number of bytes in the value field. Two bytes are necessary to express up to 255 bytes in the value field.

B3 Coding of the Value Field of Data Objects

A data element is the value field (V) of a primitive BER-TLV data object. A data element is the smallest data field that receives an identifier (a tag).

A primitive data object is structured as illustrated in Figure 16:

Tag (T)	Length (L)	Value (V)

Figure 16: Primitive BER-TLV Data Object (Data Element)

A constructed BER-TLV data object consists of a tag, a length, and a value field composed of one or more BER-TLV data objects. A record in an AEF governed by this specification is a constructed BER-TLV data object. A constructed data object is structured as illustrated in Figure 17:

Tag (T)	Length (L)	Primitive or constructed BER-TLV data object number 1	...	Primitive or constructed BER-TLV data object number n

Figure 17: Constructed BER-TLV Data Object

Annex C Coding of Data Elements Used in Transaction Processing

This annex provides the coding for dynamic card data elements and specific data elements used to control the transaction flow in the terminal or to record the status of processing for the transaction. 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.

Data (bytes or bits) indicated as RFU shall be set to 0.

C1 Application Interchange Profile

AIP Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	1	x	x	x	x	x	x	SDA supported
x	x	1	x	x	x	x	x	DDA supported
x	x	x	1	x	x	x	x	Cardholder verification is supported
x	x	x	x	1	x	x	x	Terminal risk management is to be performed
x	x	x	x	x	1	x	x	Issuer authentication is supported [19]
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	1	CDA supported

AIP Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	Reserved for use by the EMV Contactless Specifications
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 37: Application Interchange Profile

[19] When this bit is set to 1, Issuer Authentication using the EXTERNAL AUTHENTICATE command is supported

C2 Application Usage Control

Application Usage Control Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Valid for domestic cash transactions
x	1	x	x	x	x	x	x	Valid for international cash transactions
x	x	1	x	x	x	x	x	Valid for domestic goods
x	x	x	1	x	x	x	x	Valid for international goods
x	x	x	x	1	x	x	x	Valid for domestic services
x	x	x	x	x	1	x	x	Valid for international services
x	x	x	x	x	x	1	x	Valid at ATMs
x	x	x	x	x	x	x	1	Valid at terminals other than ATMs

Application Usage Control Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Domestic cashback allowed
x	1	x	x	x	x	x	x	International cashback allowed
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: Application Usage Control

C3 Cardholder Verification Rule Format

CV Rule Byte 1 (Leftmost): Cardholder Verification Method (CVM) Codes

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								RFU
	0							Fail cardholder verification if this CVM is unsuccessful
	1							Apply succeeding CV Rule if this CVM is unsuccessful
		0	0	0	0	0	0	Fail CVM processing
		0	0	0	0	0	1	Plaintext PIN verification performed by ICC
		0	0	0	0	1	0	Enciphered PIN verified online
		0	0	0	0	1	1	Plaintext PIN verification performed by ICC and signature (paper)
		0	0	0	1	0	0	Enciphered PIN verification performed by ICC
		0	0	0	1	0	1	Enciphered PIN verification performed by ICC and signature (paper)
		0	x	x	x	x	x	Values in the range 000110-011101 reserved for future use by this specification
		0	1	1	1	1	0	Signature (paper)
		0	1	1	1	1	1	No CVM required
		1	0	x	x	x	x	Values in the range 100000-101111 reserved for use by the individual payment systems
		1	1	x	x	x	x	Values in the range 110000-111110 reserved for use by the issuer
		1	1	1	1	1	1	This value is not available for use

Table 39: CVM Codes

CV Rule Byte 2 (Rightmost): Cardholder Verification Method (CVM) Condition Codes

Value	Meaning
'00'	Always
'01'	If unattended cash
'02'	If not unattended cash and not manual cash and not purchase with cashback
'03'	If terminal supports the CVM [20]
'04'	If manual cash
'05'	If purchase with cashback
'06'	If transaction is in the application currency [21] and is under X value (see section 10.5 for a discussion of "X")
'07'	If transaction is in the application currency and is over X value
'08'	If transaction is in the application currency and is under Y value (see section 10.5 for a discussion of "Y")
'09'	If transaction is in the application currency and is over Y value
'0A' - '7F'	RFU
'80' - 'FF'	Reserved for use by individual payment systems

Table 40: CVM Condition Codes

Note: For Condition Codes '01', '04', and '05', please refer to EMVCo General Bulletin No. 14 - Migration Schedule for New CVM Condition Codes.

[20] Support for a CVM is described in EMV Book 4, Section 6.3.4 first paragraph..

[21] That is, Transaction Currency Code = Application Currency Code.

C4 Issuer Code Table Index

Value	Refers to
'01'	Part 1 of ISO/IEC 8859
'02'	Part 2 of ISO/IEC 8859
'03'	Part 3 of ISO/IEC 8859
'04'	Part 4 of ISO/IEC 8859
'05'	Part 5 of ISO/IEC 8859
'06'	Part 6 of ISO/IEC 8859
'07'	Part 7 of ISO/IEC 8859
'08'	Part 8 of ISO/IEC 8859
'09'	Part 9 of ISO/IEC 8859
'10'	Part 10 of ISO/IEC 8859

Table 41: Issuer Code Table Index

C5 Terminal Verification Results

TVR Byte 1: (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Offline data authentication was not performed
x	1	x	x	x	x	x	x	SDA failed
x	x	1	x	x	x	x	x	ICC data missing
x	x	x	1	x	x	x	x	Card appears on terminal exception file [22]
x	x	x	x	1	x	x	x	DDA failed
x	x	x	x	x	1	x	x	CDA failed
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

TVR Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	ICC and terminal have different application versions
x	1	x	x	x	x	x	x	Expired application
x	x	1	x	x	x	x	x	Application not yet effective
x	x	x	1	x	x	x	x	Requested service not allowed for card product
x	x	x	x	1	x	x	x	New card
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 42: Terminal Verification Results

[22] There is no requirement in this specification for an exception file, but it is recognised that some terminals may have this capability.

TVR Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cardholder verification was not successful
x	1	x	x	x	x	x	x	Unrecognised CVM
x	x	1	x	x	x	x	x	PIN Try Limit exceeded
x	x	x	1	x	x	x	x	PIN entry required and PIN pad not present or not working
x	x	x	x	1	x	x	x	PIN entry required, PIN pad present, but PIN was not entered
x	x	x	x	x	1	x	x	Online PIN entered
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

TVR Byte 4:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Transaction exceeds floor limit
x	1	x	x	x	x	x	x	Lower consecutive offline limit exceeded
x	x	1	x	x	x	x	x	Upper consecutive offline limit exceeded
x	x	x	1	x	x	x	x	Transaction selected randomly for online processing
x	x	x	x	1	x	x	x	Merchant forced transaction online
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 42: Terminal Verification Results, continued

TVR Byte 5 (Rightmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Default TDOL used
x	1	x	x	x	x	x	x	Issuer authentication failed
x	x	1	x	x	x	x	x	Script processing failed before final GENERATE AC
x	x	x	1	x	x	x	x	Script processing failed after final GENERATE AC
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

Table 42: Terminal Verification Results, continued

C6 Transaction Status Information

TSI Byte 1 (Leftmost):

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Offline data authentication was performed
x	1	x	x	x	x	x	x	Cardholder verification was performed
x	x	1	x	x	x	x	x	Card risk management was performed
x	x	x	1	x	x	x	x	Issuer authentication was performed
x	x	x	x	1	x	x	x	Terminal risk management was performed
x	x	x	x	x	1	x	x	Script processing was performed
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

TSI Byte 2 (Rightmost):

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 43: Transaction Status Information

Annex D Transaction Log Information

D1 Purpose

Provide support for accessing a transaction log file by special devices.

D2 Conditions of Execution

This optional function is intended to be executed by special devices.

D3 Sequence of Execution

This function may be executed after Application Selection.

D4 Description

To get the Transaction Log information, the two following data elements are used: Log Entry and Log Format.

Table 44 describes the format of the Log Entry data element (tag '9F4D'):

Byte	Format	Length	Value
1	b	1	SFI containing the cyclic transaction log file
2	b	1	Maximum number of records in the transaction log file

Table 44: Log Entry

Devices that read the transaction log use the Log Entry data element to determine the location (SFI) and the maximum number of transaction log records.

The SFI shall be in the range 11 to 30.

The Transaction Log records shall be accessible using the READ RECORD command as specified in section 6.5.11. The file is a cyclic file as defined in ISO/IEC 7816-4. Record #1 is the most recent transaction. Record #2 is the next prior transaction, etc.

The Transaction Log records shall not be designated in the Application File Locator. Each record is a concatenation of the values identified in the Log Format data element. The records in the file shall not contain the Application Elementary File (AEF) Data Template (tag '70').

The Log Format and the Transaction Log records shall remain accessible when the application is blocked.

To read the transaction log information, the special device uses the following steps:

- Perform Application Selection and retrieve the Log Entry data element located in the FCI Issuer Discretionary Data. If the Log Entry data element is not present, the application does not support the Transaction Log function.
- Issue a GET DATA command to retrieve the Log Format data element.
- Issue READ RECORD commands to read the Transaction Log records.

D5 Example

Note that the following data elements are shown for example purposes only.

A Log Entry data element equal to '0F14' indicates that the transaction log file is located in SFI 15 ('0F') and contains a maximum of 20 records ('14').

A Log Format data element equal to '9A039F21035F2A029F02069F4E149F3602' indicates that the transaction log records have the following content:

Data Content	Tag	Length
Transaction Date	'9A'	3
Transaction Time	'9F21'	3
Transaction Currency Code	'5F2A'	2
Amount, Authorised	'9F02'	6
Merchant Name and Location	'9F4E'	20
Application Transaction Counter	'9F36'	2

Table 45: Example of Log Format

In Table 45, lengths and tags are shown for clarity. They do not appear in the log record which is the concatenation of values (no TLV coding).

Data elements listed in the Log Format may come from the terminal and the card. Terminal data elements such as Merchant Name and Location might have been passed to the card in the PDOL or CDOL data.

Annex E TVR and TSI Bit Settings Following Script Processing

Four possible scenarios can occur when processing a script. These scenarios are described below, together with the expected results in terms of the setting of the appropriate TVR bits, the TSI bit, and the Issuer Script Results.

In the following descriptions:

- "TVR bits" refers to TVR byte 5 bit 6 and bit 5 (depending on whether it is a tag '71' and/or tag '72' script) as defined in Table 42.
- "TSI bit" refers to TSI byte 1 bit 3 as defined in Table 43.

The Issuer Script Results are defined in Book 4, Annex A5.

E1 Scenarios

Scenario 1

A script is received, it parses correctly, the commands are sent to the card, and the card returns '9000', '62xx', or '63xx' to all commands received.

In this scenario the terminal:

- shall set the TSI bit
- shall not set the TVR bits
- shall set the first byte of the Issuer Script Results to '2x', 'Script processing successful'.

Scenario 2

A script is received, it parses correctly, the commands are sent to the card, but the card does not return '9000', '62xx', or '63xx' to one of the commands received.

In this scenario the terminal:

- shall set the TSI bit
- shall set the appropriate TVR bit(s)
- shall set the first byte of the Issuer Script Results to '1x', 'Script processing failed'
- shall send no further commands from that script to the card, even if they exist.

Scenario 3

A script is received, it does not parse correctly, and so no commands are sent to the card.

In this scenario the terminal:

- shall set the TSI bit
- shall set the appropriate TVR bit(s)
- shall set the first byte of the Issuer Script Results to '00', 'Script not performed'.

Scenario 4

No script is received. In this scenario the terminal shall set neither the TSI bit nor the TVR bit(s).

In this event there will be no Issuer Script Results.

E2 Additional Information

It is possible, but not recommended, that commands may be sent to the card 'on the fly' as a script is parsed. In this event:

- If a parsing error occurs before any commands are sent to the card, the terminal shall set the first byte of the Issuer Script Results to '00' and shall set the appropriate TVR bits and the TSI bit.
- If a parsing error occurs after any command has been sent to the card, the terminal shall set the first byte of the Issuer Script Results to '1x', and shall set the appropriate TVR bits and the TSI bit.

If more than one script is received, the terminal:

- shall set the TSI bit
- shall set the TVR bit(s) (as described in Scenarios 2 and 3) if any error occurs
- shall set the Issuer Script Results as described in Scenarios 1 through 3 for each script on a script-by-script basis
- shall process all Issuer scripts

Annex F Status Words Returned in EXTERNAL AUTHENTICATE

The terminal shall issue an EXTERNAL AUTHENTICATE command to the card only if the card indicates in byte 1 bit 3 of the AIP that it supports issuer authentication using the EXTERNAL AUTHENTICATE command.

The terminal shall issue only one EXTERNAL AUTHENTICATE command to the card during a transaction. As stated in section 10.9, there is a complementary card requirement to this which states that the card shall return status '6985', 'Command Not Supported', to the second and any subsequent EXTERNAL AUTHENTICATE commands received during the transaction.

Table 46 explains various status values the terminal may receive in response to the (first) EXTERNAL AUTHENTICATE command issued to the card, and the action the terminal shall take as a result.

Status	Explanation	Terminal Action
'9000'	Issuer authentication was successful.	The terminal shall continue with the transaction.
'6300' or any other status except '6985' and '9000'	Issuer authentication failed.	The terminal shall set the 'Issuer authentication failed' bit in the TVR to 1, and continue with the transaction.
'6985'	Issuer authentication failed and the card is in an error state (it has indicated in the AIP that it supports EXTERNAL AUTHENTICATE, but in the status returned that it does not).	This condition should never occur; in the event that it does, the behaviour of the terminal is indeterminate and it shall either terminate the transaction OR set the 'Issuer authentication failed' bit in the TVR to 1, and continue with the transaction.

Table 46: Terminal Action after (First) EXTERNAL AUTHENTICATE Response

Annex G Account Type

Value	Account Type
00	Default - unspecified
10	Savings
20	Cheque/debit
30	Credit
All other values RFU	

Table 47: Account Type

Part V

Common Core Definitions

Introduction

This Part describes an optional extension to this Book, to be used when implementing the Common Core Definitions (CCD).

These Common Core Definitions specify a minimum common set of card application implementation options, card application behaviours, and data element definitions sufficient to accomplish an EMV transaction. Terminals certified to be compliant with the existing EMV Specifications will, without change, accept cards implemented according to the Common Core Definitions, since the Common Core Definitions are supported within the existing EMV requirements.

To be compliant with the Common Core Definitions, an implementation shall implement all the additional requirements in the Common Core Definitions Parts of all affected Books.

Changed and Added Sections

Each section heading below refers to the section in this Book to which the additional requirements apply, or introduces new sections where required. The text defines requirements for a common core implementation, in addition to the requirements already specified in the referenced section of EMV.

Part II - Data Elements and Commands

6 Commands for Financial Transaction

6.2 Response APDU Format

For the following commands used during transaction processing, the body of the response APDU is a constructed data object with tag equal to '77' of which the value field may contain one or more BER-TLV coded data objects.

- GENERATE AC
- GET PROCESSING OPTIONS
- INTERNAL AUTHENTICATE

Tag	Value
'77'	Response Message Template Format 2

Table CCD 1: Body of Response APDU Structure

6.5 Commands

6.5.4 EXTERNAL AUTHENTICATE Command-Response APDUs

6.5.4.1 Definition and Scope

The CCD-compliant application shall support issuer authentication using the second GENERATE AC command. The CCD-compliant application shall indicate that the EXTERNAL AUTHENTICATE command is not supported in EMV applications by setting bit 3 in byte 1 of the AIP to 0.

6.5.5 GENERATE APPLICATION CRYPTOGRAM Command-Response APDUs

6.5.5.1 Definition and Scope

The CCD-compliant application shall support issuer authentication using the second GENERATE AC command.

6.5.5.3 Data Field Sent in the Command Message

CDOL2 shall include tag '8A' (Authorisation Response Code) and tag '91' (Issuer Authentication Data).

6.5.5.4 Data Field Returned in the Response Message

The response message shall be a BER-TLV coded constructed data object introduced by tag '77' and contains only the data shown in Table CCD 2.

Tag	Value
'9F27'	Cryptogram Information Data
'9F36'	Application Transaction Counter
'9F26'	Application Cryptogram
'9F10'	Issuer Application Data

Table CCD 2: Format 2 GENERATE AC Response Message Data Field

The required data elements for the response returned in an envelope as specified for the CDA feature (described in section 6.6 of Book 2) are shown in Book 2 Table CCD 1 and Table CCD 2.

The Cryptogram Information Data returned in the GENERATE AC response message is coded according to Table CCD 3:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							AAC
0	1							TC
1	0							ARQC
1	1							RFU
		0	0					Payment System-specific cryptogram
				0				No advice required
					0	0	0	No information given

Table CCD 3: Coding of Cryptogram Information Data

6.5.8 GET PROCESSING OPTIONS Command-Response APDUs

6.5.8.2 Command Message

The CCD-compliant application shall not preclude support for PDOL.

6.5.8.4 Data Field Returned in the Response Message

The response message shall be a BER-TLV coded constructed data object introduced by tag '77' and contains only the data shown in Table CCD 4.

Tag	Value
'82'	Application Interchange Profile
'94'	Application File Locator

Table CCD 4: Format 2 GET PROCESSING OPTIONS Response Message Data Field

6.5.9 INTERNAL AUTHENTICATE Command-Response APDUs

6.5.9.4 Data Field Returned in the Response Message

The response message shall be a BER-TLV coded constructed data object introduced by tag '77' and contains only the data shown in Table CCD 5.

Tag	Value
'9F4B'	Signed Dynamic Application Data

Table CCD 5: Format 2 Internal Authenticate Response Message Data Field

6.5.12.2 Command Message

To allow an issuer to use offline plaintext PIN verification as a possible CVM, a CCD-compliant card shall support the VERIFY command with parameter P2 = '80' as defined in Book 3, Table 23.

Part III - Debit and Credit Application Specification

7 Files for Financial Transaction Interchange

7.3 Data Retrievable by GET DATA Command

The ICC shall support the GET DATA command for retrieval of the primitive data object with tag '9F17' (PIN Try Counter).

9 GENERATE AC Command Coding

9.2 Command Data

9.2.2 Transaction Certificate Data

The CCD-compliant application shall not contain a TDOL. The CCD-compliant application shall not request the terminal to generate a TC Hash Value (that is, tag '98' shall not be included in CDOL1 or CDOL2).

The following Section 9.2.3 applies to a CCD-compliant application.

9.2.3 Common Core Definitions Card Verification Results

In response to the GENERATE AC command and as part of the Issuer Application Data, the CCD-compliant application shall return the Card Verification Results (CVR). The CVR includes information for the issuer regarding the results of Card Risk Management processing and application processing. The format of the CVR for a CCD-compliant application is specified in CCD Annex C7.3.

9.2.3.1 Options Related to Setting/Resetting of Counters and Indicators

The issuer shall have the option of specifying whether a new card is required to set the 'Go Online on Next Transaction Was Set' bit.

The issuer shall have the option of specifying whether the CCD-compliant application requires issuer authentication to be performed for the application to approve (TC) an online transaction.

The issuer shall have the option of specifying whether the CCD-compliant application requires issuer authentication to pass when performed for the application to approve (TC) an online transaction.

If the CCD-compliant application does not require issuer authentication to be performed for the application to approve (TC) an online transaction, the issuer shall have the option of specifying whether the CCD-compliant application requires issuer authentication to pass for resetting all the following non-velocity-checking indicators:

- Issuer Authentication Failed
- Last Online Transaction Not Completed
- Issuer Script Processing Failed
- Go Online on Next Transaction Was Set

If the CCD-compliant application does not require issuer authentication to pass when performed for the application to approve (TC) an online transaction, the issuer shall have the option of specifying whether the CCD-compliant application requires issuer authentication to pass for resetting all the following non-velocity checking indicators:

- Last Online Transaction Not Completed
- Issuer Script Processing Failed
- Go Online on Next Transaction Was Set

If the CCD-compliant application does not require issuer authentication to be performed or does not require issuer authentication to pass when performed for the application to approve (TC) an online transaction, the issuer shall have the option of specifying whether the CCD-compliant application requires issuer authentication to pass for resetting the velocity-checking offline transaction count(s) and cumulative amount(s).

The issuer shall have the option of indicating whether the application shall use the 'Update Counters' bits in the CSU to update the velocity-checking count(s) and cumulative amount(s) associated with the offline transaction limits referred to in bits b8 - b5 of byte 3 of the CVR, if the 'CSU Created by Proxy for the Issuer' bit in the CSU is set to 1.

If the 'CSU Created by Proxy for the Issuer' bit is set to 1 in the CSU, and if the issuer specifies that 'Update Counters' shall not be used, then the issuer shall have the option of indicating whether the application:

- shall not update the offline counters
- shall set the offline counters to zero
- shall set the offline counters to the upper offline limits
- shall add the transaction to the offline counter(s)

9.2.3.2 Setting and Resetting of Bits in the CVR

The following describes the conditions under which each bit in the CVR of a Common Core Definitions card is set or reset.

Application Cryptogram Type Returned in Second GENERATE AC

In the first GENERATE AC response, these bits shall be set to Second GENERATE AC Not Requested.

In the second GENERATE AC response, these bits shall be set to the value of bits b8 – b7 of the Cryptogram Information Data returned in the response to the second GENERATE AC command of the current transaction (AAC or TC).

Application Cryptogram Type Returned in First GENERATE AC

In both the first and second GENERATE AC response, these bits shall be set to the value of bits b8 – b7 of the Cryptogram Information Data returned in the response to the first GENERATE AC command of the current transaction (AAC, TC, or ARQC).

CDA Performed

In the first GENERATE AC response, this bit shall be set if and only if Signed Dynamic Data is returned in the response to the first GENERATE AC command of the current transaction.

In the second GENERATE AC response, this bit shall be set if and only if Signed Dynamic Data is returned in the response to the first or second GENERATE AC command (or both) of the current transaction.

Offline DDA Performed

In both the first and second GENERATE AC response, this bit shall be set if and only if Signed Dynamic Application Data is returned in the response to the INTERNAL AUTHENTICATE command of the current transaction.

Issuer Authentication Not Performed

In the second GENERATE AC response, this bit shall be set if and only if the CCD-compliant application did not receive Issuer Authentication Data. This may be the case either if the transaction was unable to go online or if the issuer did not provide Issuer Authentication Data in the response message.

In the first GENERATE AC response, this bit shall be set to the value it had in the most recent second GENERATE AC response sent by the CCD-compliant application.

Issuer Authentication Failed

This bit shall be set in the GENERATE AC response if and only if issuer authentication was performed and failed. In the first GENERATE AC response, it indicates issuer authentication failed in a previous online transaction. In the second GENERATE AC response, it indicates either that issuer authentication failed in the current transaction, or that issuer authentication failed in a previous transaction and the bit was not reset.

Once set, this bit shall remain set until either:

- issuer authentication is successful,
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),
  - issuer authentication was not performed,
  - the CCD-compliant application does not require issuer authentication to be performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of non-velocity-checking indicators.

Low Order Nibble of PIN Try Counter

In both the first and second GENERATE AC response, these bits shall be set to the value of the low-order nibble (bits b4-b1) of the PIN Try Counter.

Offline PIN Verification Performed

In both the first and second GENERATE AC response, this bit shall be set if and only if Offline PIN Verification has been performed (successfully or unsuccessfully) on the current transaction.

Offline PIN Verification Performed and PIN Not Successfully Verified

In both the first and second GENERATE AC response, this bit shall be set if and only if Offline PIN Verification has been performed on the current transaction and the PIN was not successfully verified during processing of the current transaction.

PIN Try Limit Exceeded

In both the first and second GENERATE AC response, this bit shall be set if and only if the PIN Try Counter is zero.

Last Online Transaction Not Completed

This bit shall be set in the first GENERATE AC response if and only if in the previous transaction, the CCD-compliant application requested to go online and the transaction was not completed (that is, the second GENERATE AC command was not received).

Once set, this bit shall remain set until either:

- issuer authentication is successful,
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),
  - issuer authentication was not performed,
  - the CCD-compliant application does not require issuer authentication to be performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of non-velocity-checking indicators.
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),
  - issuer authentication was performed and failed,
  - the CCD-compliant application does not require issuer authentication to pass when performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of non-velocity-checking indicators.

Lower Offline Transaction Count Limit Exceeded

In both the first and second GENERATE AC response, this bit shall be set if the CCD-compliant application has exceeded an issuer-specified lower limit for the number of transactions approved offline. This bit may represent the condition of multiple counters. At the least, all transactions approved offline whose amounts were not cumulated shall be included in at least one transaction count. This bit may also be set under additional conditions specified by the issuer.

Upper Offline Transaction Count Limit Exceeded

In both the first and second GENERATE AC response, this bit shall be set if the CCD-compliant application has exceeded an issuer-specified upper limit for the number of transactions approved offline. This bit may represent the condition of multiple counters. At the least, all transactions approved offline whose amounts were not cumulated shall be included in at least one transaction count. This bit may also be set under additional conditions specified by the issuer.

Lower Cumulative Offline Amount Limit Exceeded

In both the first and second GENERATE AC response, this bit shall be set if the CCD-compliant application has exceeded an issuer-specified lower limit for cumulative amounts approved offline. This bit may represent the condition of multiple counters. At the least, all domestic transactions approved offline shall be included in at least one cumulative amount. This bit may also be set under additional conditions specified by the issuer.

Upper Cumulative Offline Amount Limit Exceeded

In both the first and second GENERATE AC response, this bit shall be set if the CCD-compliant application has exceeded an issuer-specified upper limit for cumulative amounts approved offline. This bit may represent the condition of multiple counters. At the least, all domestic transactions approved offline shall be included in at least one cumulative amount. This bit may also be set under additional conditions specified by the issuer.

Issuer-discretionary bit 1 – Issuer-discretionary bit 4:

These bits are set in the first and second GENERATE AC response at the discretion of the issuer. The meaning of these bits is defined by the issuer and is outside the scope of this specification.

Number of Successfully Processed Issuer Script Commands Containing Secure Messaging

In the first and second GENERATE AC response, these bits shall be set to the number of commands successfully processed with secure messaging.

Issuer Script Processing Failed

In both the first and second GENERATE AC response, this bit shall be set if and only if processing of a command with secure messaging failed.

Once set, this bit shall remain set until a subsequent GENERATE AC command where either:

- issuer authentication is successful,
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),
  - issuer authentication was not performed
  - the CCD-compliant application does not require issuer authentication to be performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of non-velocity-checking indicators.
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),
  - issuer authentication was performed and failed,
  - the CCD-compliant application does not require issuer authentication to pass when performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of non-velocity-checking indicators.

Offline Data Authentication Failed on Previous Transaction

In both the first and second GENERATE AC response, this bit shall be set if and only if, in the TVR returned during the previous transaction, any of the following bits was set:

- SDA Failed
- DDA Failed
- CDA Failed

Once set, this bit shall remain set until a subsequent transaction is performed that meets either of the following conditions:

- the previous transaction successfully went online, or
- the previous transaction was approved offline.

If either condition is met the bit is reset in the first GENERATE AC response.

Go Online on Next Transaction Was Set

In both the first and second GENERATE AC response, this bit shall be set if and only if the 'Set Go Online on Next Transaction' bit of the last successfully recovered CSU was set, or it is a new card and the issuer has specified that a new card is required to set the 'Go Online on Next Transaction Was Set' bit.

Once set, this bit shall remain set until a subsequent GENERATE AC command where either:

- all of the following conditions are true:
  - issuer authentication is successful, and
  - the Set Go Online on Next Transaction bit of the CSU is not set.
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),
  - issuer authentication was not performed,
  - the CCD-compliant application does not require issuer authentication to be performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of non-velocity-checking indicators.
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),
  - issuer authentication was performed and failed,
  - the CCD-compliant application does not require issuer authentication to pass when performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication for resetting of non-velocity-checking indicators.

Unable to go Online

This bit shall be set in the second GENERATE AC response if and only if the Authorization Response Code, tag '8A', returned from the terminal indicates the terminal was unable to go online (set to 'Y3' or 'Z3').

9.2.3.3 Mandatory Actions Due to CVR Bit Settings

This section provides a list of mandatory actions that shall be taken by the CCD-compliant application, and issuer-configurable options that shall be supported by the CCD-compliant application.

Issuer Authentication Not Performed

The issuer shall have the option of specifying that if this bit is set, whether the CCD-compliant application shall:

- force transactions at online-capable terminals to go online,
- or allow the transaction to remain offline.

The issuer shall have the option of specifying that if this bit is set, and either the transaction occurs at an offline-only terminal or the terminal is unable to go online, whether the CCD-compliant application shall:

- be allowed to approve (TC) the transaction, or
- decline the transaction.

Issuer Authentication Failed

The issuer shall have the option of specifying that if this bit is set, whether the CCD-compliant application shall:

- force transactions at online-capable terminals to go online,
- or allow the transaction to remain offline.

The issuer shall have the option of specifying that if this bit is set, and either the transaction occurs at an offline-only terminal or the terminal is unable to go online, whether the CCD-compliant application shall:

- be allowed to approve (TC) the transaction, or
- decline the transaction.

PIN Try Limit Exceeded

The issuer shall have the option of specifying that if this bit is set, the CCD-compliant application shall decline the transaction offline.

The issuer shall have the option of specifying that if this bit is set, whether the CCD-compliant application shall:

- force transactions at online-capable terminals to go online,
- or allow the transaction to remain offline.

The issuer shall have the option of specifying that if this bit is set, and either the transaction occurs at an offline-only terminal or the terminal is unable to go online, whether the CCD-compliant application shall:

- be allowed to approve (TC) the transaction, or
- decline the transaction.

The ICC shall not block the application or the card due to this bit being set.

Last Online Transaction Not Completed

If this bit is set, the CCD-compliant application shall force the transaction at online-capable terminals to go online.

The issuer shall have the option of specifying that if this bit is set, and either the transaction occurs at an offline-only terminal or the terminal is unable to go online, whether the CCD-compliant application shall:

- be allowed to approve (TC) the transaction, or
- decline the transaction.

Lower Offline Transaction Count Limit Exceeded

If this bit is set in the first GENERATE AC response, the CCD-compliant application shall force the transaction at online-capable terminals to go online.

Upper Offline Transaction Count Limit Exceeded

If this bit is set and either the transaction occurs at an offline-only terminal or the terminal is unable to go online, the CCD-compliant application shall decline the transaction. However, the issuer shall have the option of allowing the CCD-compliant application to override this decline for a transaction at Terminal Type 26.

Lower Cumulative Offline Amount Limit Exceeded

If this bit is set in the first GENERATE AC response, the CCD-compliant application shall force the transaction at online-capable terminals to go online.

Upper Cumulative Offline Amount Limit Exceeded

If this bit is set and either the transaction occurs at an offline-only terminal or the terminal is unable to go online, the CCD-compliant application shall decline the transaction. However, the issuer shall have the option of allowing the CCD-compliant application to override this decline for a transaction at Terminal Type 26.

Issuer Script Processing Failed

The issuer shall have the option of specifying that if this bit is set, whether the CCD-compliant application shall:

- force transactions at online-capable terminals to go online,
- or allow the transaction to remain offline.

Go Online on Next Transaction Was Set

The issuer shall have the option of specifying that if this bit is set, and either the transaction occurs at an offline-only terminal or the terminal is unable to go online, whether the CCD-compliant application shall:

- be allowed to approve (TC) the transaction, or
- decline the transaction.

9.3 Command Use

The CCD-compliant application shall respond to the first GENERATE AC with any of the following cryptogram types:

- TC
- ARQC
- AAC

The CCD-compliant application shall respond to the second GENERATE AC (if applicable) with either of the following cryptogram types:

- TC
- AAC

10 Functions Used in Transaction Processing

10.5 Cardholder Verification

The CCD-compliant application shall support Cardholder Verification. It shall indicate this by setting the Application Interchange Profile byte 1, bit 5 to 1.

10.5.1 Offline PIN Processing

The CCD-compliant application shall be capable of supporting offline plaintext PIN verification. It is the issuer's option whether or not to use offline plaintext PIN as a cardholder verification method.

10.8 Card Action Analysis

The CCD-compliant application shall not request that the terminal send an advice message to the issuer.

10.8.1 Terminal Messages for an AAC

The CCD-compliant application shall set bits b3-b1 of the CID to '000' in the GENERATE AC command response.

10.8.2 Advice Messages

The CCD-compliant application shall not request the terminal to send an advice message. Bit b4 of the Cryptogram Information Data shall be set to 0.

10.10 Issuer-to-Card Script Processing

An issuer shall send no more than one issuer script template in an authorization response message. The script template may contain multiple commands. The script template may be tag '71' or tag '72'.

10.11 Completion

The following Section 10.11.1 applies to a CCD-compliant application.

10.11.1 Additional Completion Actions for a CCD-Compliant Application

10.11.1.1 Actions Taken by CCD-compliant Application After Issuer Authentication is Successful

After issuer authentication is successful, if the 'CSU Created by Proxy for the Issuer' bit in the CSU is set to 1, and if the issuer specifies that 'Update Counters' shall not be used, then the following shall govern the behaviour of velocity-checking counters and cumulative amounts associated with the offline transaction limits referred to in bits b8-b5 of byte 3 of the CVR:

- If the issuer specifies that the application shall not update the offline counters, no offline counter or cumulative amount is modified.
- If the issuer specifies that the application shall set the offline counters to zero, the application will reset all the offline counters and cumulative amounts to zero. By doing so, the issuer allows the application to accept offline transactions, up to the offline limits.
- If the issuer specifies that the application shall set the offline counters to the upper offline limits, the offline counters and cumulative amounts will be set to their respective upper limits.
- If the issuer specifies that the application shall add the transaction to the offline counter(s), the transaction will be included in the offline counters or cumulative amounts as if it were an offline transaction.

This section describes the actions to be taken by the CCD-compliant application due to the setting of each bit in the CSU after issuer authentication is successful..

Issuer Approves Online Transaction

If 'Issuer Approves Online Transaction' is set and the terminal requests a TC, the application shall approve the transaction by returning a TC.

If 'Issuer Approves Online Transaction' is not set, the application shall decline the transaction by returning an AAC.

Card Block

If 'Card Block' is set, all applications in the ICC shall be permanently disabled, including applications that may be selected implicitly. For all subsequent SELECT commands the card shall return the status bytes 'Function not supported' (SW1-SW2 = '6A81') and perform no other action.

Application Block

If 'Application Block' is set, the currently selected application shall be invalidated. An invalidated application shall return the status bytes 'Selected file invalidated' (SW1-SW2 = '6283') in response to a SELECT command and return only an AAC in response to the GENERATE AC command.

Update PIN Try Counter

If 'Update PIN Try Counter' is set, the application shall update the PIN Try Counter (PTC) with the value contained in bits b4-b1 of byte 1 of the CSU. If the PIN is blocked, updating the value of the PTC with a non-zero value unblocks the PIN. Updating the value of the PTC with a zero value blocks the PIN.

If 'Update PIN Try Counter' is not set, no update of the PTC shall be performed by the application.

The value contained in bits b4-b1 of byte 1 of the CSU shall never be interpreted by the application.

Set Go Online on Next Transaction

If 'Set Go Online on Next Transaction' is set, the application shall force subsequent transactions at online-capable terminals to go online (that is, the CCD-compliant application shall return an ARQC in response to the first GENERATE AC command if a TC or an ARQC is requested). The application shall continue to try to go online at online-cable terminals until a subsequent GENERATE AC command where either:

- all of the following conditions are true:
  - issuer authentication is successful, and
  - the Set Go Online on Next Transaction bit of the CSU is not set.
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),
  - issuer authentication was not performed,
  - the CCD-compliant application does not require issuer authentication to be performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of non-velocity-checking indicators."
- or all of the following conditions are true:
  - the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online),

- issuer authentication was performed and failed,
- the CCD-compliant application does not require issuer authentication to pass when performed for the application to approve (TC) an online transaction, and
- the CCD-compliant application does not require issuer authentication to pass for resetting of non-velocity-checking indicators.

Update Counters

'Update Counters' (bits b2-b1 of byte 2 of the CSU) govern the behaviour of velocity-checking counters and cumulative amounts associated with the offline transaction limits referred to in bits b8-b5 of byte 3 of the CVR if either of the following is true:

- the 'CSU Created by Proxy for the Issuer' bit in the CSU is set to 0
- the issuer specifies that the application shall use the 'Update Counters' bits in the CSU to update the velocity-checking count(s) and cumulative amount(s) regardless of the bit setting for 'CSU Created by Proxy for the Issuer'

If 'Update Counters' is set to 'Do Not Update Offline Counters', no offline counter or cumulative amount shall be modified.

If 'Update Counters' is set to 'Reset Offline Counters to Zero', the application shall reset all the offline counters and cumulative amounts to zero. By doing so, the issuer allows the application to accept offline transactions, up to the offline limits.

If 'Update Counters' is set to 'Set Offline Counters to Upper Offline Limits', the application shall set the offline counters and cumulative amounts to their respective upper limits.

If 'Update Counters' is set to 'Add Transaction to Offline Counters', the application shall include the transaction in the offline counters or cumulative amounts as if it were an offline transaction.

10.11.1.2 Other Completion Actions

After the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online), the CCD-compliant application shall reset to zero the velocity-checking offline transaction count(s) and cumulative offline amount(s) if either of the following are true:

- all of the following conditions are true:
  - the terminal requested a TC,
  - issuer authentication was not performed,

  - the CCD-compliant application does not require issuer authentication to be performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of velocity-checking counters.
- or all of the following conditions are true:
  - the terminal requested a TC,
  - issuer authentication was performed and failed,
  - the CCD-compliant application does not require issuer authentication to pass when performed for the application to approve (TC) an online transaction, and
  - the CCD-compliant application does not require issuer authentication to pass for resetting of velocity-checking counters.

After the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online), the CCD-compliant application shall approve the transaction if all of the following conditions are true:

- the terminal requested a TC, and
- one of the following is true:
  - issuer authentication is successful and the 'Issuer Approves Online Transaction bit' of the recovered CSU is set to 1, or
  - issuer authentication was not performed and the CCD-compliant application does not require issuer authentication to be performed for the application to approve (TC) an online transaction, or
  - issuer authentication was performed and failed and the CCD-compliant application does not require issuer authentication to pass when performed for the application to approve (TC) an online transaction.

After the transaction successfully went online (that is, the Authorisation Response Code does not indicate that the terminal was unable to go online), the CCD-compliant application shall decline the transaction in the second GENERATE AC response if either of the following conditions are true:

- both of the following are true:
  - issuer authentication was not performed, and
  - the CCD-compliant application requires issuer authentication to be performed for the application to approve (TC) an online transaction,
- or both of the following are true:
  - issuer authentication was performed and failed, and

- the CCD-compliant application requires issuer authentication to pass when performed for the application to approve (TC) an online transaction.

After the transaction did not successfully complete online (that is the Authorisation Response Code indicates that the terminal was unable to go online), the CCD-compliant application shall decide whether to approve or decline the transaction.

Part IV - Annexes

Annex A Data Elements Dictionary

For the data elements shown in Table CCD 6:

- If the source is 'Terminal', the data element shall not be included in any DOL used by a CCD-compliant application.
- If the source is 'ICC', the data element shall not be identified in the AFL of a CCD-compliant application.

Data Element Name	Tag	Source
Amount, Reference Currency	'9F3A'	Terminal
Application Reference Currency	'9F3B'	ICC
Application Reference Currency Exponent	'9F43'	ICC
Default Dynamic Data Authentication Data Object List (DDOL)	—	Terminal
Transaction Certificate (TC) Hash Value	'98'	Terminal

Table CCD 6: Data Elements Not Used by a CCD-Compliant Application

Table CCD 7 lists data elements (in addition to those defined in Annex A) that are defined within the context of the Common Core Definitions.

Name	Description	Source	Format	Template	Tag	Length
Card Verification Results (CVR)	Contains data sent to the issuer indicating exception conditions that occurred during the current and previous transactions. Transmitted to the terminal in Issuer Application Data as specified in Table CCD 9.	ICC	b	—	—	5
Common Core Identifier (CCI)	Data sent to the issuer identifying the format of the Issuer Application Data and the method for calculating the Application Cryptogram. Transmitted to the terminal in Issuer Application Data as specified in Table CCD 9. Contains the following: Format Code (FC) Cryptogram Version (CV)	ICC	b	—	—	1
Derivation Key Index (DKI)	Data sent to the issuer identifying the issuer's derivation key for deriving the card's ICC Master Keys. Transmitted to the terminal in Issuer Application Data as specified in Table CCD 9.	ICC	b	—	—	1
Issuer Discretionary Data	Contains issuer proprietary application data for transmission to the issuer in an online transaction. Transmitted to the terminal in Issuer Application Data as specified in Table CCD 9.	ICC	b	—	—	15

Table CCD 7: Additional Data Elements Defined for CCD

Annex C Coding of Data Elements Used in Transaction Processing

Please add the following sections after Annex C.6.

C7 Issuer Application Data for a Common Core Definitions-Compliant Application

The CCD-compliant application shall have an Issuer Application Data (IAD) field of fixed length, 32 bytes long, with the following attributes:

- Byte 1 shall be set to '0F'.
- Byte 2 shall be the Common Core Identifier (CCI).
- Byte 17 shall be set to '0F'.

The CCD-compliant application shall support the selection of different Issuer Application Data if:

- the card requests the Terminal Type and the Additional Terminal Capabilities in PDOL, and
- the values provided by the terminal in the PDOL related data for the Terminal Type and the first two bytes of the Additional Terminal Capabilities are '34' and '0000' respectively.

C7.1 Common Core Identifier

The CCI shall identify the format of the IAD, and the Cryptogram Version (CV). Values in the range '00' to '9F' are reserved to avoid conflict with legacy Cryptogram Version Numbers.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Common Core IAD Format Code (FC).
1	0	1	0					CCD Version 4.1 IAD Format (='A')
				x	x	x	x	Common Core Cryptogram Version (CV)
				0	1	0	1	CCD Version 4.1 Cryptogram Version (= '5' for Triple DES)
				0	1	1	0	CCD Version 4.1 Cryptogram Version (= '6' for AES)

Table CCD 8: Common Core Identifier

Bits b8 - b5 of the CCI shall indicate the Format Code (FC). Values in the range 'A' - 'F' shall indicate a CCD-specified IAD format (all values RFU by EMVCo for CCD).

Bits b4 - b1 of the CCI shall indicate the Cryptogram Version (CV) for the Application Cryptogram. The CV indicates:

- The cryptogram input data and key derivation method the CCD-compliant application uses to generate the Application Cryptogram.
- The cryptogram input data (including CSU coding), key derivation method, and ARPC method the CCD-compliant application expects the issuer to use when generating the Authorisation Response Cryptogram.

Values in the range '4' - 'F' shall indicate a CCD-specified cryptogram algorithm and data set (all values RFU by EMVCo for CCD). Values in the range '0' - '3' shall indicate a proprietary cryptogram algorithm. When using the CV range '0' - '3', applications are not CCD-compliant.

C7.2 Issuer Application Data for Format Code 'A'

The format and coding of the IAD with a Format Code of 'A' shall be as shown in Table CCD 9:

Byte(s)	Contents	Description
1	Length Indicator	Length of EMVCo-defined data in IAD. Set to '0F'.
2	CCI	Common Core Identifier
3	DKI	Derivation Key Index
4-8	CVR	Card Verification Results (see section C7.3)
9-16	Counters	Contents are at the discretion of the Payment System.
17	Length Indicator	Length of Issuer Discretionary Data field in IAD. Set to '0F'.
18-32	Issuer Discretionary Data	Contents are at the discretion of the issuer.

Table CCD 9: Issuer Application Data for Format Code 'A'

C7.3 Card Verification Results

The coding of the CVR for a Common Core IAD Format Code of value 'A' shall be as shown in Table CCD 10.

CVR Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x							Application Cryptogram Type Returned in Second GENERATE AC
0	0							AAC
0	1							TC
1	0							Second GENERATE AC Not Requested
1	1							RFU
		x	x					Application Cryptogram Type Returned in First GENERATE AC
		0	0					AAC
		0	1					TC
		1	0					ARQC
		1	1					RFU
				1				CDA Performed
					1			Offline DDA Performed
						1		Issuer Authentication Not Performed
							1	Issuer Authentication Failed

CVR Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Low Order Nibble of PIN Try Counter
				1				Offline PIN Verification Performed
					1			Offline PIN Verification Performed and PIN Not Successfully Verified
						1		PIN Try Limit Exceeded
							1	Last Online Transaction Not Completed

Table CCD 10: Card Verification Results for Format Code 'A'

CVR Byte 3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								Lower Offline Transaction Count Limit Exceeded
	1							Upper Offline Transaction Count Limit Exceeded
		1						Lower Cumulative Offline Amount Limit Exceeded
			1					Upper Cumulative Offline Amount Limit Exceeded
				1				Issuer-discretionary bit 1
					1			Issuer-discretionary bit 2
						1		Issuer-discretionary bit 3
							1	Issuer-discretionary bit 4

CVR Byte 4

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Number of Successfully Processed Issuer Script Commands Containing Secure Messaging
				1				Issuer Script Processing Failed
					1			Offline Data Authentication Failed on Previous Transaction
						1		Go Online on Next Transaction Was Set
							1	Unable to go Online

CVR Byte 5

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

Table CCD 10: Card Verification Results for Format Code 'A', continued

C8 Card Status Update for a Common Core Definitions-Compliant Application

The Issuer Authentication Data shall include a Card Status Update (CSU) of fixed length, 4 bytes long. The coding of the CSU is shown in Table CCD 11.

CSU Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								Proprietary Authentication Data Included
	0	0	0					RFU
				x	x	x	x	PIN Try Counter

CSU Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								Issuer Approves Online Transaction
	1							Card Block
		1						Application Block
			1					Update PIN Try Counter
				1				Set Go Online on Next Transaction
					1			CSU Created by Proxy for the Issuer
						x	x	Update Counters
						0	0	Do Not Update Offline Counters
						0	1	Set Offline Counters to Upper Offline Limits
						1	0	Reset Offline Counters to Zero
						1	1	Add Transaction to Offline Counter

Note: The 'CSU Created by Proxy for the Issuer' bit shall be set in the CSU if and only if the CSU is generated by a proxy for the Issuer.

Table CCD 11: Card Status Update for Cryptogram Versions '5' and '6'

CSU Byte 3

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

CSU Byte 4

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	Issuer-Discretionary

Table CCD 11: Card Status Update for Cryptogram Versions '5' and '6', continued

The default value for issuer-discretionary data in the CSU is zero.

Annex D Transaction Log Information

If the CCD-compliant application supports transaction logging, it shall be supported using the method specified in Annex D.

Index

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V