CB2A AUTHORISATION

VERSION 1.6.3

TABLE OF CONTENTS

1. OVERVIEW OF DOCUMENT

CB2A Authorisation documentation includes the following volumes:

Volume 0: Presentation of Document

Volume 1: General Principles

Volume 2: Data Field Dictionary

Volume 3.1: Network Management

Volume 3.2: Face-to-Face Payment/Unattended Payment

Volume 3.3: Remote Payment/Secured Electronic Commerce

2. PRESENTATION OF DOCUMENT

2.1. PREFACE

The present version includes all CB2A Authorisation documentation.

2.2. SCOPE OF PRESENT VERSION

The present version includes the following payment services:

- Face-to-face payment
- Unattended terminal payment
- Remote payment
- Secured electronic commerce
- Payment for Reservation and Rental of Goods or Services
- Recurring payment
- Unattended rental terminal payment
- Payment using Multi-Service Banking ATMs
- Funds transfer

The present version includes the following technologies:

- Card in contact mode
- Card in contactless mode
- Cardholder not present – Remote Payment
- Cardholder not present – Secured electronic commerce

The present version includes the following functionalities:

- Partial Authorisation
- Digital Wallets

3. HISTORY

CB2A version	Publication date	Version	Comment
CB2A 1.6.3	September 30th 2022		First version
CB2A 1.6.3	January 6th 2023		- **2 forgotten change sheets of CB2A 1.6.0 – March 2019:** - 1085: length of field 56 type 0010 (IP address) is 4…45 and not 15 - 1107: Values for UPI and Discover in selected brand (field 56 type 0003) - **Editorial changes in volume 2:** - Length of field 2 is LLVAR …19 and not 199 - Field 22 – ‘Pin entry capability’: correction of value 2 description - Field 119 type 0042: correction of the length in list by field number
CB2A 1.6.3	February 14th 2023		- New change sheet 1559: MPAT - New reason code to allow to send the PAR to the acceptor

4. LIST OF CHANGES IN VERSION 1.6.3 – SEPTEMBER 2022

CB2A Authorisation V1.6.3 September 2022
-
UPDATE DETAILS

Table of contents

1449 – TIP management

Background:

The payment service with tip management allows the cardholder to pay a tip in addition to the payment for goods and services. The management of the transaction including the tip is done in a single electronic payment operation.
It means there is a single cardholder authentication, if applicable, a single authorisation, if applicable and a single clearing.
The beneficiary of the transaction identified in the payment transaction is the merchant, for the total amount (for payment of good and services plus the tip amount).
The TIP amount is identified as an additional amount in the authorisation request, in a dedicated subfield of the protocol.

Note: some merchants allow cardholders to also pay an amount of donation made for the benefit of a charitable association during the payment. Donation amount is not sent in authorisation request but may be sent in data capture messages.

Implementation:

Change in volume 2 – Data Dictionary

2.3.3 Definition of data fields used

…

Field 54

Additional amounts

…

□ **Amount type ____ n2**

Values	Description
…	
44	Tip amount
…	

…

Change in volume 3.2 – Face-to-face payment – Unattended payment

7. Message descriptions

A: Payment autho. req. (EMV chip and contactless EMV chip) : **0100**
B: Payment autho. request (magn. stripe and contactless magn. stripe): **0100**
C: Resp. to payment autho. req. (contact and contactless) : **0110**

N°	**Definition**	**A**	**B**	**C**
…				
54	Additional amounts,	C(118)	C(118).	C(118)
…				
44	Tip amount	C(119)	C(119)	CQI
…				

…

N°	**Comments**
…	
118	Mandatory if at least one of the following amount types is present
…	
119	Mandatory for transaction with tip
…	

1452 – Ecommerce

Background:

Mastercard AN2941 Digital Remote Commerce Enhancements

Mastercard is introducing a new cryptogram type to support enhanced amount and merchant verification. To support the requirements above, Mastercard introduces a new subelement 003 'Remote Commerce Acceptor Identifier' in DE104.
This identifier may consist of merchant business website URL or reverse domain name.
A new data element 'Remote Commerce Acceptor Identifier' is needed in CB2A.

Electronic Commerce Authentication Type

Editorial changes: the wording is reviewed.

Electronic Commerce Authentication Type upgrade

In CB2A, downgrade is already managed but some schemes may also upgrade it. New values are needed for modified Electronic Commerce Authentication Type.
For Visa, the ECI to taken in account is the one that Visa sends in the authorisation response.

Electronic Commerce Security Level Indicator

For Mastercard, the SLI is provided in authorisation response message and must be sent in clearing.
The SLI is added.

3RI

Some data elements related to cardholder's authentication need to be populated in MITs with 3RI.

Visa Network Merchant-Initiated Transaction Service

It is a network solution that can help acquirers and their merchants to manage the transaction identifier lifecycle of merchant-initiated transactions. This service requests a purchase identifier. It's added to CB2A.

Visa: exemption status indicator

Authorisation request responses contain the exemption status (validated/honoured or failed validation/not honoured) for some authentication exemptions.

Visa Token Service

Visa identifies transactions eligible for token services in authorisation request response. Acquirers are required to send the information in clearing transactions.

Implementation:

Change in volume 2 – Data field dictionary

2.3.1 Alphabetical list

Data element	Field no.	Sub-field no.
…		
Authentication exemption status indicator	119	0017
…		
Extended Electronic Commerce Indicator	119	0016
…		
Purchase identifier	119	0042
Purchase identifier type	119	0041
…		
Remote commerce acceptor identifier	119	0028
…		
Transaction eligible for token services	119	0359

…

2.3.2 List by field number

N°		Format		
...		…		
119		Reserved for national use	LL2VAR	b…999
	…	…		
	0016	Extended Electronic Commerce Indicator		n3
	0017	Authentication exemption status indicator		an1
	…	…		
	0028	Remote commerce acceptor identifier		b…115
…				
	0041	Purchase identifier type		an1
	0042	Purchase identifier		an32
…				
	0359	Transaction eligible for token services		an1
…				

…

2.3.3 Definition of the data fields used

Field 59 **Format: LLLVAR b …255**

National data

…

➢ *TYPE = 0407: ELECTRONIC COMMERCE AUTHENTICATION TYPE*

…

Values	Description
…	
20	Authentication cryptogram issued from a server
21	Authentication cryptogram issued from a XPay or token cryptogram with authentication delegated to device

…

➢ *TYPE = 0413: MODIFIED ELECTRONIC COMMERCE AUTHENTICATION TYPE*

Data format: b1 Number of bytes transported: 1

Informs the acceptor and/or the CB acquirer that the security mode initially planned for the transaction has been changed.

Values	Description
09	~~Secured by any means other than those corresponding to the other values~~ No authentication cryptogram
20	Authentication cryptogram issued from a server
21	Authentication cryptogram issued from a XPay or token cryptogram with authentication delegated to device

…

Field 119 Format: LL2VAR b …999

Reserved for national use (Données nationales)

❑ **Data type**____ **b2**

Type	Description	Repeatability
…		
0016	Extended Electronic Commerce Indicator	
0017	Authentication exemption status indicator	
…		
0028	Remote commerce acceptor identifier	
…		
0041	Purchase identifier type	
0042	Purchase identifier	
…		
0359	Transaction eligible for token services	
…		

➢ TYPE = 0016: EXTENDED ELECTRONIC COMMERCE INDICATOR

Data format: n3 Number of bytes transported: 2

SLI (Security Level Indicator) in electronic commerce.

…

➢ TYPE = 0017: AUTHENTICATION EXEMPTION STATUS INDICATOR

Data format: an1 Number of bytes transported: 1

Indicates the status of the exemption.

…

➢ TYPE = 0028: REMOTE COMMERCE ACCEPTOR IDENTIFIER

Data format: b…115 Number of bytes transported: …115

This identifier may consist of part of merchant business website URL or reverse domain name which allows to perform the dynamic linking validation.

…

➢ TYPE = 0041: PURCHASE IDENTIFIER TYPE

Data format: an1 Number of bytes transported: 1

The following list is provided for example. Refer to schemes' rules:

Type	Meaning
0	Free text
1	Order number
3	Rental agreement number
4	Hotel folio number
5	Invoice number

➢ TYPE = 0042: PURCHASE IDENTIFIER

Data format: an32 Number of bytes transported: 32

Allows to uniquely identify a payment agreement using the same PAN or token under the same merchant and the same payment use case

…

➢ TYPE = 0359: TRANSACTION ELIGIBLE FOR TOKEN SERVICES

Data format: an1 Number of bytes transported: 1

Allows the scheme to indicate whether the transaction is eligible for its token services

…

Volume 3.3 – Remote payment secured electronic commerce

4 Requirements related to multiple payment

Subsequent transactions

…

Data	CB2A Authorisation field	CB2A Authorisation settings
…		
DS transaction ID	56 type 0023 data element UUID applies to nomenclature 1 of the initial transaction	Transaction specific value for 3RI MIT
	Field 56 type 0046/ DS transaction ID	Copy of field 56 type 0023 data element UUID applies to nomenclature 1 of the initial transaction (*)
ACS transaction ID	56 type 0023 data element UUID applies to nomenclature 2 of the initial transaction	Transaction specific value for 3RI MIT
	Field 56 type 0046/ ACS transaction ID	Copy of field 56 type 0023 data element UUID applies to nomenclature 2 of the initial transaction (*)
Authentication merchant name	Field 56 type 0036	Transaction specific value for 3RI MIT
	Field 56 type 0046/ Merchant name	Copy of field 56 type 0036 of the initial transaction (*)
Authentication date	Field 56 type 0037	Transaction specific value for 3RI MIT
	Field 56 type 0046/ Authentication date	Copy of field 56 type 0037 of the initial transaction (*)
Authentication amount	Field 56 type 0038	Transaction specific value for 3RI MIT
	Field 56 type 0046/ Authentication amount	Copy of field 56 type 0038 of the initial transaction (*)
Cardholder authentication value of the current transaction	Field 59 type 0401	~~Absent~~Transaction specific value for 3RI MIT, otherwise absent
Electronic commerce transaction authentication type of the current transaction	Field 59 type 0407	~~Absent~~Transaction specific value for 3RI MIT, otherwise absent
…		

Electronic commerce cryptogram calculation method of the current transaction	Field 59 type 0411	Absent
Three-domain secure results of the current transaction	Field 59 type 0412	~~Absent~~Transaction specific value for 3RI MIT, otherwise absent
Three-domain secure results, others of the current transaction	Field 59 type 0419	~~Absent~~Transaction specific value for 3RI MIT, otherwise absent
…		

8 Message descriptions

A: Authorisation request : **0100**	**B:** Response to authorisation request : **0110**

N°	**Definition**	**A**	**B**
…			
59	Reserved for national use	C(2)	C(2)
…			
0416	Electronic Commerce Indicator	C(29)	C(163)
…			
119	Reserved for national use	C(2)	C(2)
…			
0016	Extended Electronic Commerce Indicator	.	C(163)
0017	Authentication exemption status indicator	.	C(164)
…			
0028	Remote commerce acceptor identifier	C(163)	.
…			
0041	Purchase identifier type	C(29)	.
0042	Purchase identifier	C(29)	.
…			
0359	Transaction eligible for token services		C(164)
…			

N°	**Comments**
…	
29	Mandatory if available, otherwise absent
…	
163	Mandatory for some international schemes
164	May be sent by some international schemes

1458 – MOTO identification

Background:

Mastercard identifies separately mail order and telephone order whereas this difference is not present in CB2A.
It's needed to identify separately mail order and telephone order.

(Note : Corresponding Mastercard data is CIS DE 61 SF4 – 'POS Cardholder Presence')

Implementation:

Change in volume 2 – Data Dictionary

2.3.3 Definition of data fields used

…

Field 25

Point of service condition code

…

Value	Description
…	
52	Mail order
53	Telephone order
…	

…

1459 – Response codes

Background:

Some new response codes are created. New response codes are identified in each payment context.

Implementation:

Change in volume 2 – Data field dictionary

2.3 Data field descriptions

…

Field 39 Format: an2

Response code

…

Value	Description
…	
46	Business specific error
…	
62	Restricted card
…	
93	Transaction cannot be completed-Violation of Law
…	
R0	Stop payment order
…	

…

Change in volume 3.2 – Face-to-face payment – Unattended payment

2. Response codes

…

2.1 Response codes for a face-to-face payment authorisation request

No.	Description
…	
46	Business specific error
62	Restricted card
6P	Verification data failed
77	Closed account
78	Blocked, first used or special condition—new cardholder not activated or card is temporarily blocked
82	Negative online CAM, dCVV, iCVV, or CVV results Or Offline PIN authentication interrupted
93	Transaction cannot be completed-Violation of Law
…	

…

2.2 Response codes for an unattended payment authorisation request

No.	Description
…	
46	Business specific error
62	Restricted card
6P	Verification data failed
77	Closed account
78	Blocked, first used or special condition—new cardholder not activated or card is temporarily blocked
82	Negative online CAM, dCVV, iCVV, or CVV results Or Offline PIN authentication interrupted
93	Transaction cannot be completed-Violation of Law
…	

…

Change in volume 3.3 – Remote payment – Secured electronic commerce

2. Response codes

2.1 Response codes for a remote payment authorisation request

No.	Description
…	
46	Business specific error
62	Restricted card
6P	Verification data failed
77	Closed account
78	Blocked, first used or special condition—new cardholder not activated or card is temporarily blocked
93	Transaction cannot be completed-Violation of Law
R0	Stop payment order
…	

…

1462 – SoftPOS

Background:

This evolution helps identifying with more precision different types of mobile acceptance of smartphone or tablet:

- mPOS (Mobile Point Of Sale) defines a terminal based on a smartphone or a tablet with all cardholder payment steps done on a PCI PTS dongle,
- SPoC (Software-based PIN entry on COTS (Commercial off-the-shelf)) defines a terminal based on a smartphone or a tablet using a PCI PTS dongle to read the card. PIN code is done on the device screen,
- CPoC (Contactless Payment on COTS (Commercial off-the-shelf)) defines a terminal based on a smartphone or a tablet without PCI PTS dongle. the card is read in contactless mode using the NFC device and there is no PIN entry
- MPoC (Mobile Payments on COTS (Commercial off-the-shelf)) defines a terminal based on a smartphone or a tablet without PCI PTS dongle, the card is read in contactless mode with PIN entry on the device screen

Three new values are created in existing CB2A field 47 type 31 'Point of interaction information' to identify the SPoC, CPoC and MPoC solutions.
The definition of the existing label is modified to identify mPOS solutions.

Implementation:

Change in volume 2 – Data Dictionary

2.3.3 Definition of data fields used

…

Field 47

Additional data - National

…

TYPE = 31: POINT OF INTERACTION INFORMATION

Data format: n 1 Number of bytes transported: 1

Value	Description
1	~~Mobile acceptance solution~~ mPOS (smartphone/tablet with a PCI PTS dongle to read the card with PIN entry on the dongle)
2	SPoC (smartphone/tablet with a PCI PTS dongle to read the card with PIN entry on the device screen)
3	CPoC (smartphone/tablet without dongle, when the card is read in contactless mode using the NFC device and there is no PIN entry)
4	MPoC (smartphone/tablet without dongle, when the card is read in contactless mode with PIN entry on the device screen)

1481 – Track 2 – Conditions of presence

Background:

Track 2 is absent in resubmissions. Conditions of presence are modified.

Implementation:

Change in volume 3.2 – Face-to-face payment / ADM/SST/LAT payment

7 Message descriptions

A: Payment autho. req. (EMV chip and contactless EMV chip) : **0100**
B: Payment autho. request (magn. stripe and contactless magn. stripe): **0100**
C ; Resp. to payment autho. req. (contact and contactless) : **0110**

N°	Definition	A	B	C
…				
55	Integrated circuit card system related data	C(2)	C(2)	C(2)
…				
0057	Track 2 equivalent data	C(~~8~~4165)	C(48)	
…				

N°	Comments
…	
48	Mandatory if available for a contactless transaction
…	
165	Mandatory if present in the card application and if function code not equal to 104 and 105 (resubmission), otherwise absent
…	

1559 – MPAT: PAR to send to the acceptor

Background:

The Issuer may send the PAR in authorisation request response. A new message reason code allows to indicate that it can be transmitted to the Acceptor.

Implementation:

Change in volume 2

…

Field 59 **Format: LLLVAR b …255**

National data

…

TYPE = 0101: MESSAGE REASON CODE

…

Value	Description
Values 1500 to 1999 specify the reason why a request message (0100) was sent instead of an advice (0120).	
… **1684** …	PAR to send to the Acceptor

…

GENERAL PRINCIPLES

TABLE OF CONTENTS

1 INTRODUCTION

The present volume contains the following information:

- Purpose of the authorisation protocol
- General principles and role of CB2A Authorisation
- Examples of standard exchanges

2 PURPOSE OF AUTHORISATION PROTOCOL

The CB2A Authorisation protocol is used in dialogs between an acceptance system and an acquirer system.

This authorisation service must have at least one authorisation request transaction.

Network management messages enable Big Retailers to manage the dialogs.

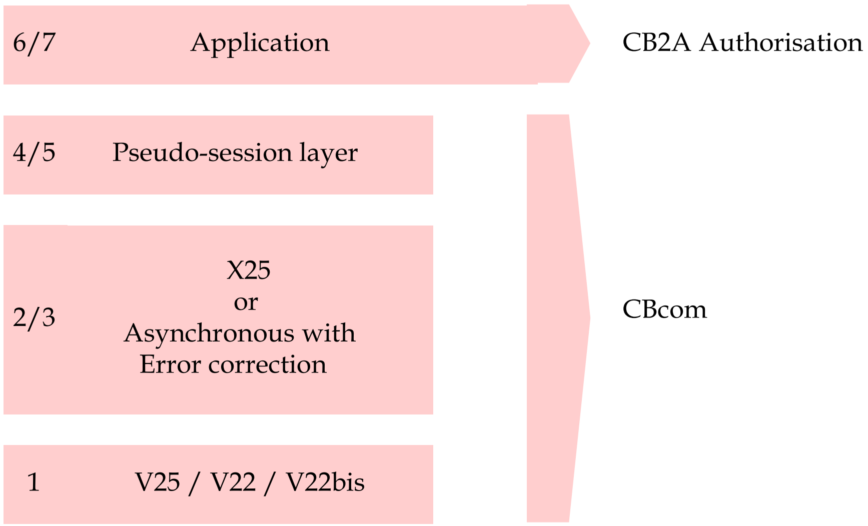
3 GENERAL PRINCIPLES

3.1 ROLE OF CB2A AUTHORISATION PROTOCOL

The CB2A Authorisation protocol and CBcom specifications are complementary documents. Their common features are the following:

- Optimisation of response times
- Compliance with international standards
- Simple to implement
- Easy to include new functionalities
- Secure access to the authorisation system.

The architecture is based on the OSI reference model and can be represented as follows:



3.2 DEFINITIONS

The term **message** refers to a set of data elements used to send information from an Acceptor to an Acquirer, and vice versa.

A **transaction** contains a request message and a request response message.

The term **equipment** refers to a hardware device in which the CB electronic payment software has been installed.

This definition includes stand-alone terminals, Online systems (Terminal + Server), systems with electronic payment software, CB electronic payment modules integrated in distribution systems for goods or services.

The term **Terminal** refers to any acceptance point device for cards.
This definition includes all devices able to acquire cardholder data.

3.3 SERVICES

3.3.1 AUTHORISATION SERVICE

This service is based on authorisation requests and the following messages:

- 0100: authorisation request
- 0110: authorisation request response.

3.3.2 NETWORK MANAGEMENT SERVICE

There are several types of network management messages:

- **sign-on**, used by a system to open a dialog in the Authorisation service
- **sign-off**, used by a system to close a dialog in the Authorisation service
- **echo test**, used by an Acceptor system to keep a session open, maintain an activity online, and check the status of the connection to its Acquirer partner.

Network management uses the following messages:

- 0800: request
- 0810: request response

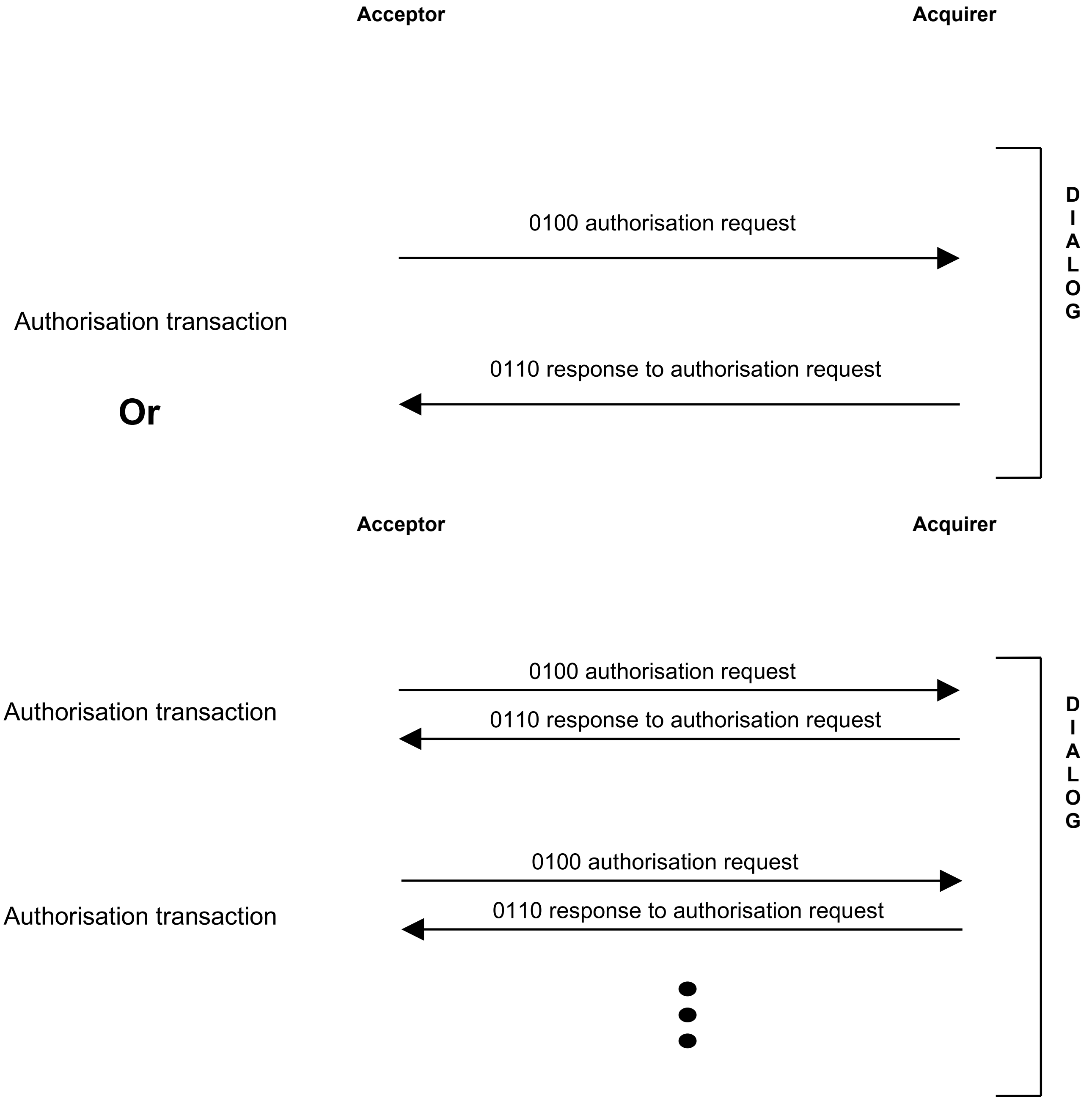
Only systems likely to maintain a session open for executing the authorisation service would find this service of benefit. These messages have therefore been introduced exclusively for use by "Big Retailer" Acceptors and Acquirer systems.

4 OVERVIEW OF MESSAGES

4.1 AUTHORISATION REQUESTS

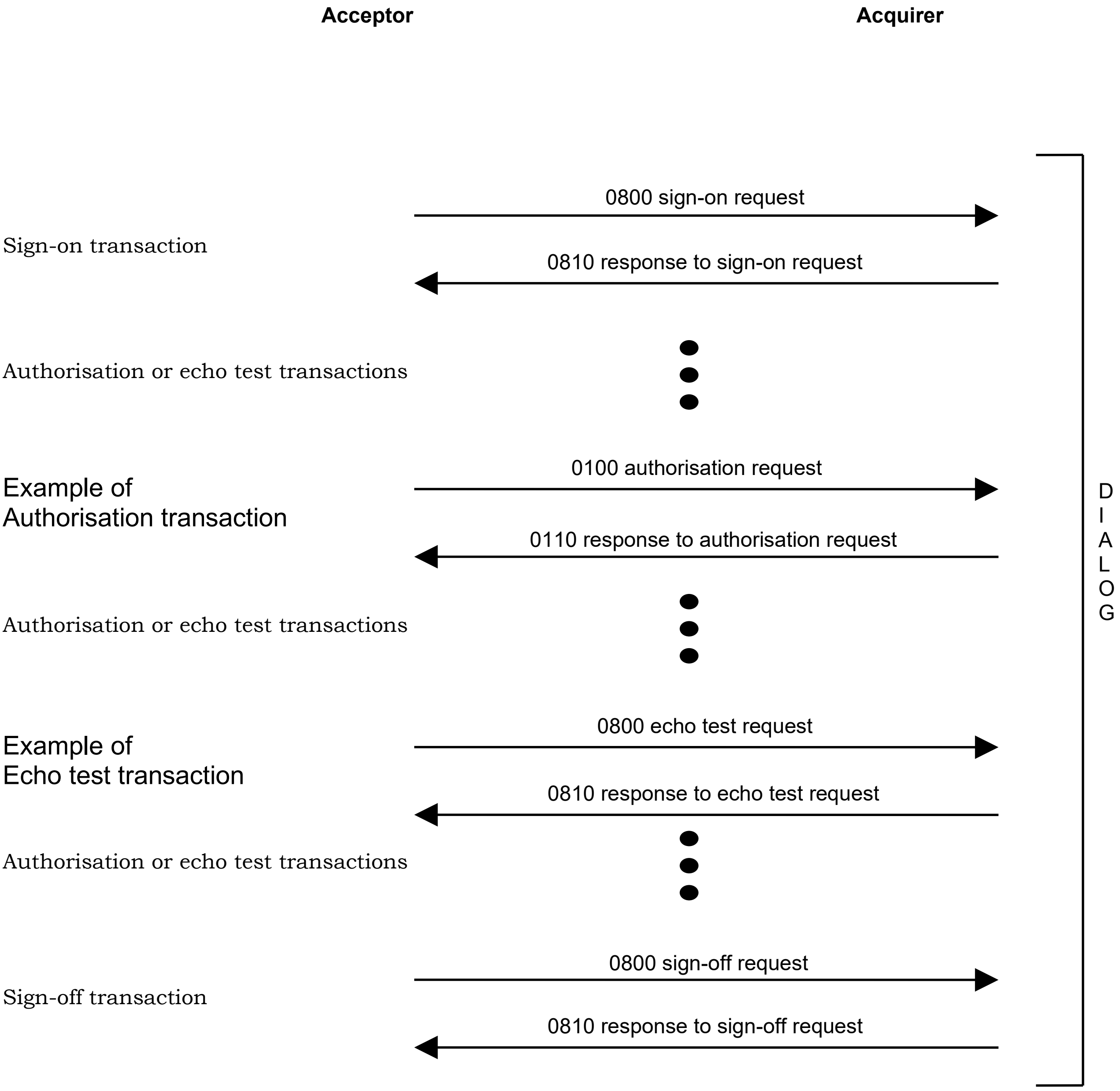
4.1.1 DIALOG WITHOUT NETWORK MANAGEMENT

For acceptance systems that do not use the network management service, it is possible to have a single authorisation request or to have a succession of several authorisation requests. In this case, the dialog will be managed by both systems (acceptor and acquirer) by means of timers.


Acceptor
Acquirer
0100 authorisation request
DIALOG
Authorisation transaction
0110 response to authorisation request
Or
Acceptor
Acquirer
0100 authorisation request
Authorisation transaction
0110 response to authorisation request
DIALOG
0100 authorisation request
Authorisation transaction
0110 response to authorisation request

4.1.2 DIALOG WITH NETWORK MANAGEMENT

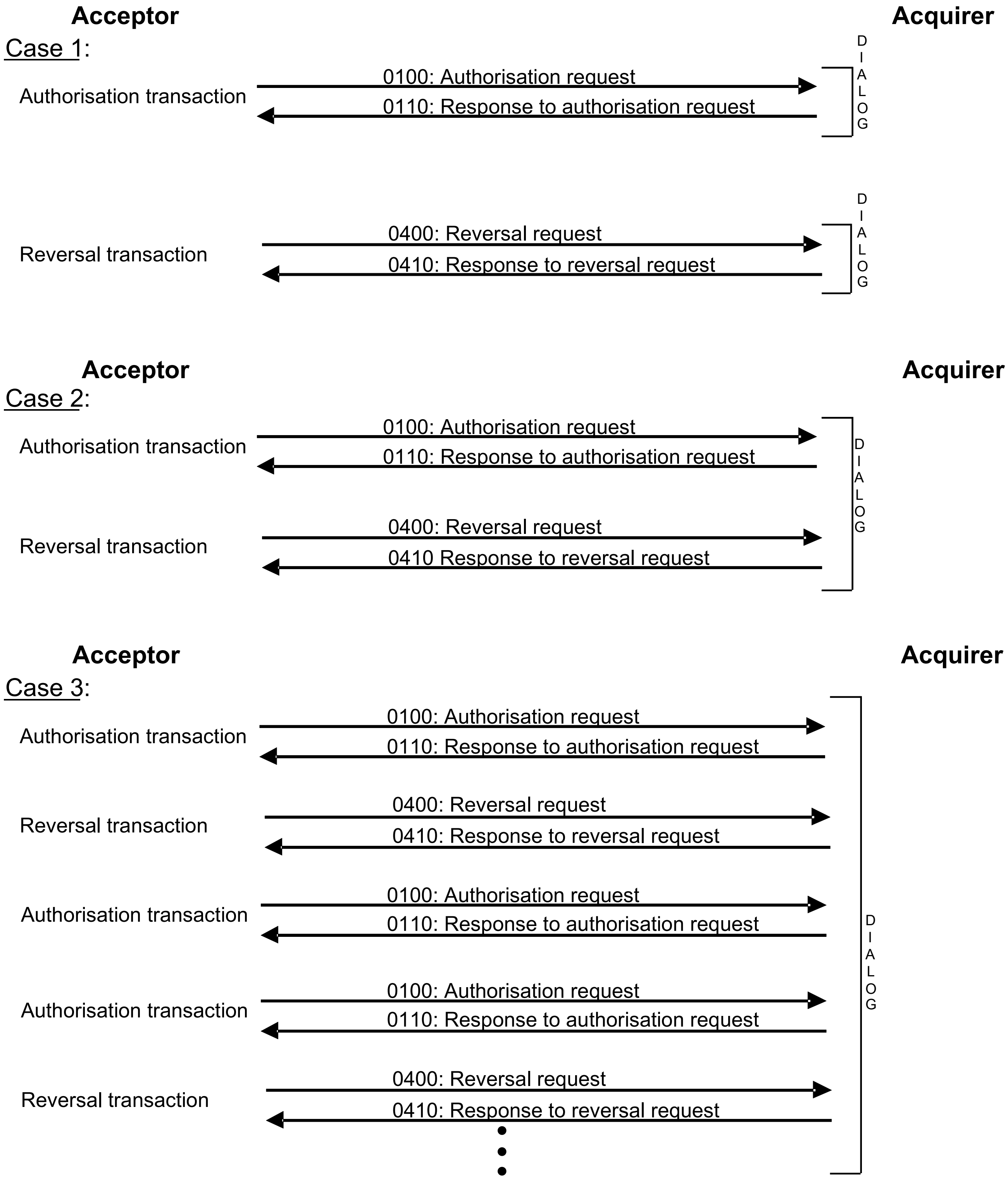
The dialog is always opened with a "sign-on" transaction.
The dialog is closed by a "sign-off" transaction unless there is a technical problem.
Only the acceptance system is authorised to initiate requests.
Between the sign-on and sign-off transactions, there may be a succession of authorisation and echo test transactions, which do not take place in any specified order.


Acceptor
Acquirer
Sign-on transaction
0800 sign-on request
0810 response to sign-on request
Authorisation or echo test transactions
Example of Authorisation transaction
0100 authorisation request
0110 response to authorisation request
Authorisation or echo test transactions
Example of Echo test transaction
0800 echo test request
0810 response to echo test request
Authorisation or echo test transactions
Sign-off transaction
0800 sign-off request
0810 response to sign-off request
DIALOG

4.2 REVERSAL REQUESTS

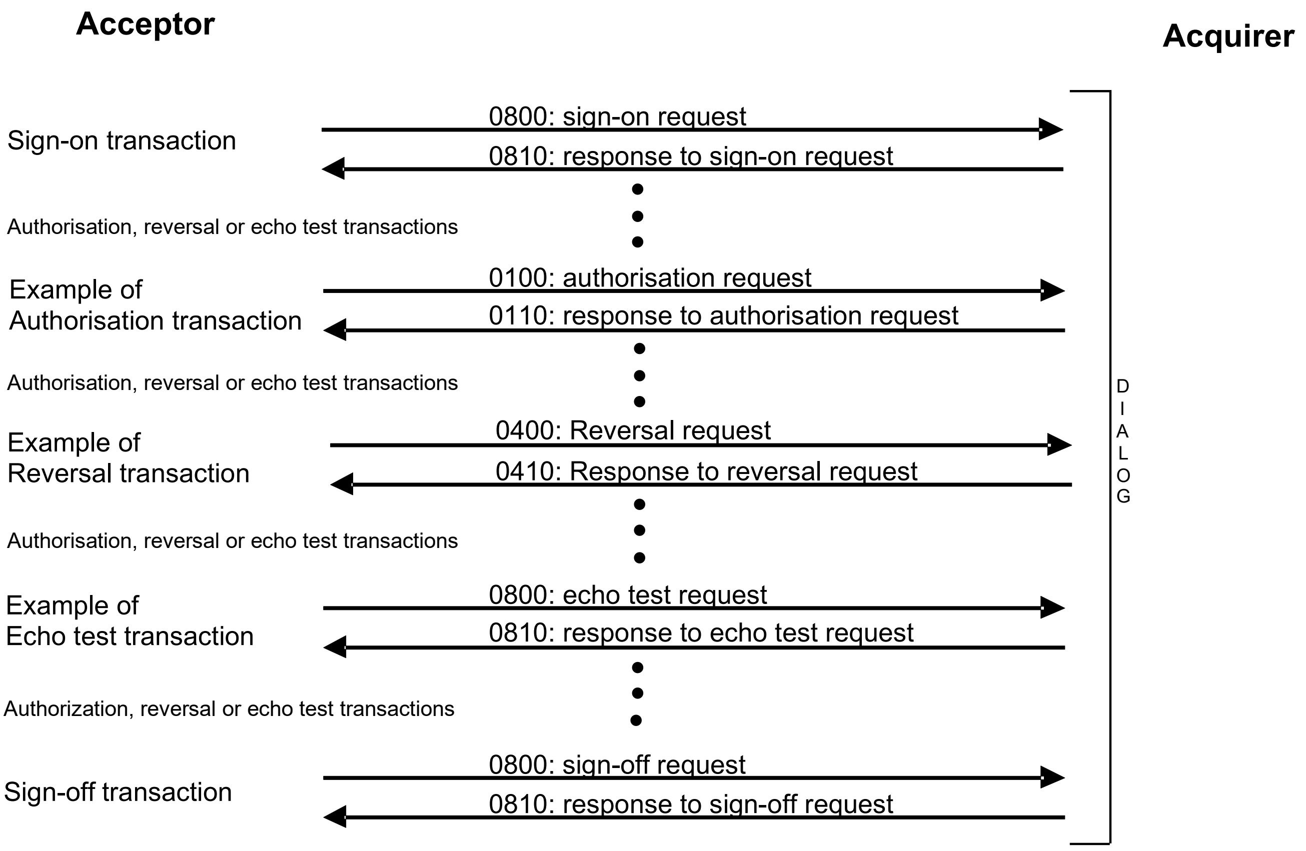
4.2.1 DIALOG WITHOUT NETWORK MANAGEMENT

For acceptance systems that do not use the network management service, it is possible to have a single authorisation/reversal request or to have a succession of several authorisation/reversal requests. In this case, the dialog will be managed by both systems (acceptor and acquirer) by means of timers.


Acceptor
Acquirer
Case 1:
Authorisation transaction
0100: Authorisation request
0110: Response to authorisation request
DIALOG
Reversal transaction
0400: Reversal request
0410: Response to reversal request
DIALOG
Acceptor
Acquirer
Case 2:
Authorisation transaction
0100: Authorisation request
0110: Response to authorisation request
Reversal transaction
0400: Reversal request
0410 Response to reversal request
DIALOG
Acceptor
Acquirer
Case 3:
Authorisation transaction
0100: Authorisation request
0110: Response to authorisation request
Reversal transaction
0400: Reversal request
0410: Response to reversal request
Authorisation transaction
0100: Authorisation request
0110: Response to authorisation request
Authorisation transaction
0100: Authorisation request
0110: Response to authorisation request
Reversal transaction
0400: Reversal request
0410: Response to reversal request
DIALOG

4.2.2 DIALOG WITH NETWORK MANAGEMENT

The dialog is always opened with a "sign-on" transaction.
The dialog is closed by a "sign-off" transaction unless there is a technical problem.
Only the acceptance system is authorised to initiate requests.
Between the sign-on and sign-off transactions, there may be a succession of authorisation, reversal and echo test transactions, which do not take place in any specified order.


Acceptor
Acquirer
Sign-on transaction
0800: sign-on request
0810: response to sign-on request
Authorisation, reversal or echo test transactions
Example of
Authorisation transaction
0100: authorisation request
0110: response to authorisation request
Authorisation, reversal or echo test transactions
Example of
Reversal transaction
0400: Reversal request
0410: Response to reversal request
Authorisation, reversal or echo test transactions
Example of
Echo test transaction
0800: echo test request
0810: response to echo test request
Authorization, reversal or echo test transactions
Sign-off transaction
0800: sign-off request
0810: response to sign-off request
DIALOG

5 DEFINITION AND MANAGEMENT OF TIMERS

This section describes the values related to the different timers for the Authorisation function.

The timers can only be negotiated in the long connection request (IPDU CN) or in the data transfers (IPDU DE) of network management messages (Sign-On/Sign-Off, Echo test).

In addition, during the timer negotiation the negotiated value takes effect as from the response until a new negotiation.

5.1 NON-RESPONSE TIMER (TNR)

The issuing system monitors the response from the receiving system via the non-response timer (TNR). This timer is managed and initiated by the system which sent the message.

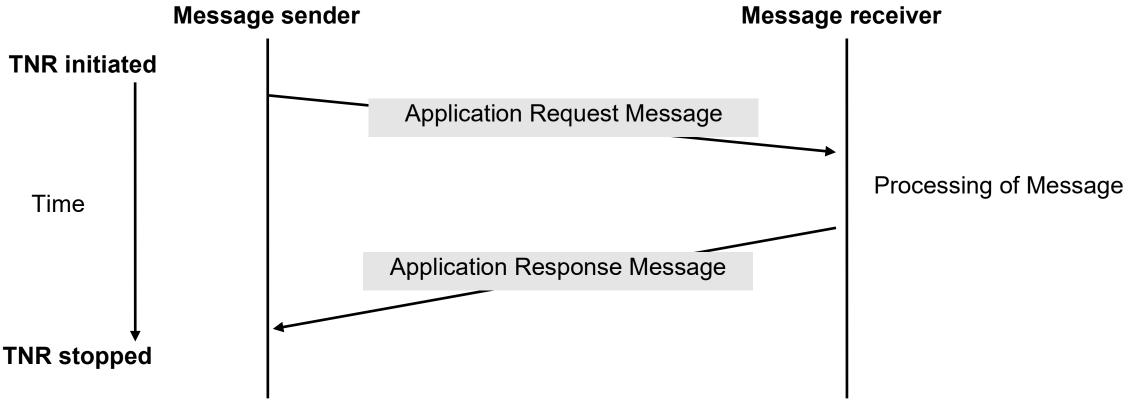
Description of timer:

- Can be negotiated during the connection or during the transfer.
- The issuing system initiates the non-response timer (TNR) when it sends a Request message.
- The issuing system stops the non-response timer (TNR) when it receives the Response message.

Expected behaviour in case of a timeout:

- IPDU_AB with a response code PI01 set to 27 is sent (TNR timer timeout).

Non-Response Timer (TNR)



5.2 GUARANTEED RESPONSE TIMER (TGR)

The guaranteed response timer (TGR) enables the receiving system to monitor the sending of the response.

Description of timer:

- Can be negotiated during the connection or during the transfer.
- The receiving system initiates the guaranteed response timer (TNR) when it sends a Request message.
- The receiving system stops the guaranteed response timer (TNR) when it sends the Response message.

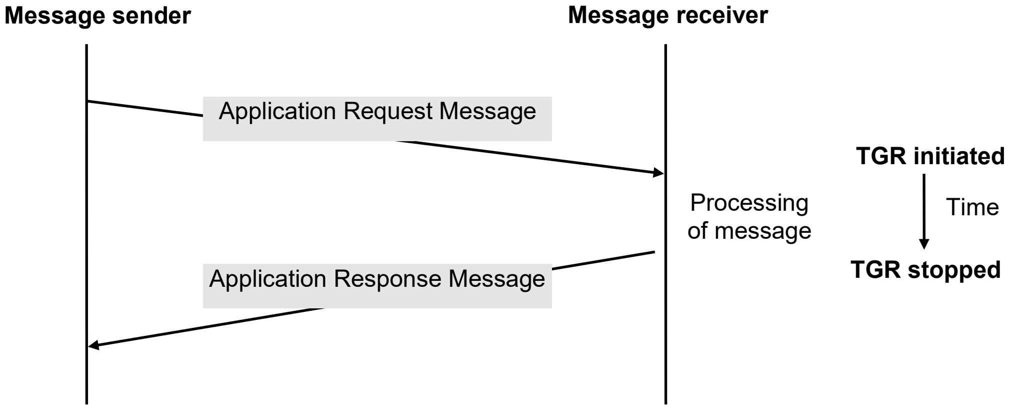
Expected behaviour in case of a timeout:

- * IPDU_AB with a response code PI01 set to 26 is sent (TGR timeout).
- * IPDU_AB with a response code PI01 set to 27 is sent (TNR timer timeout).

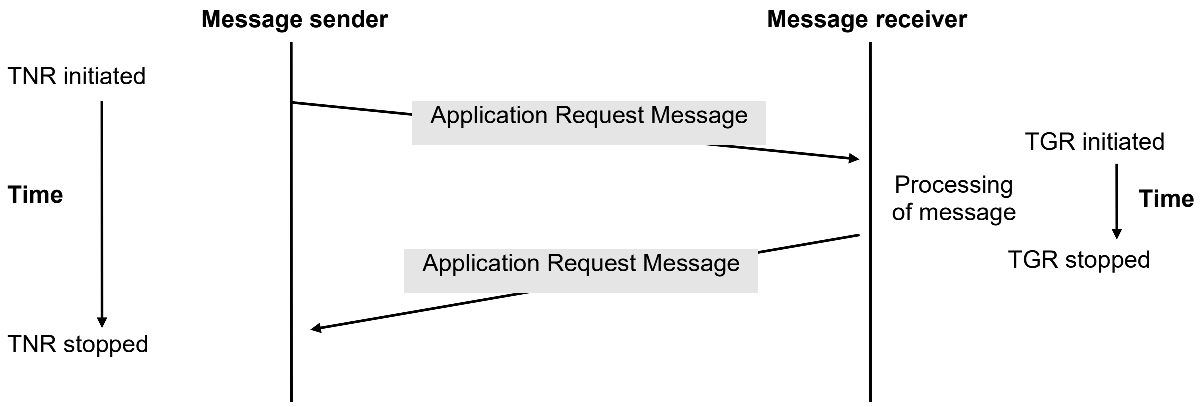
In all cases, the following is essential for the management of the dialog:

TNR > TGR + 2 * (maximum transit time)

Guaranteed Response Timer (TGR)



Combination of Non-Response Timer (TNR) and Guaranteed Response Timer (TGR)



The TNR and TGR timers are initiated when a Request message that requires a Response is sent or received.

5.3 INACTIVITY MONITORING TIMER (TSI)

The inactivity monitoring timer (TSI) enables the receiving system to manage the absence of dialog (Pseudo-Session layer). The value can be negotiated.

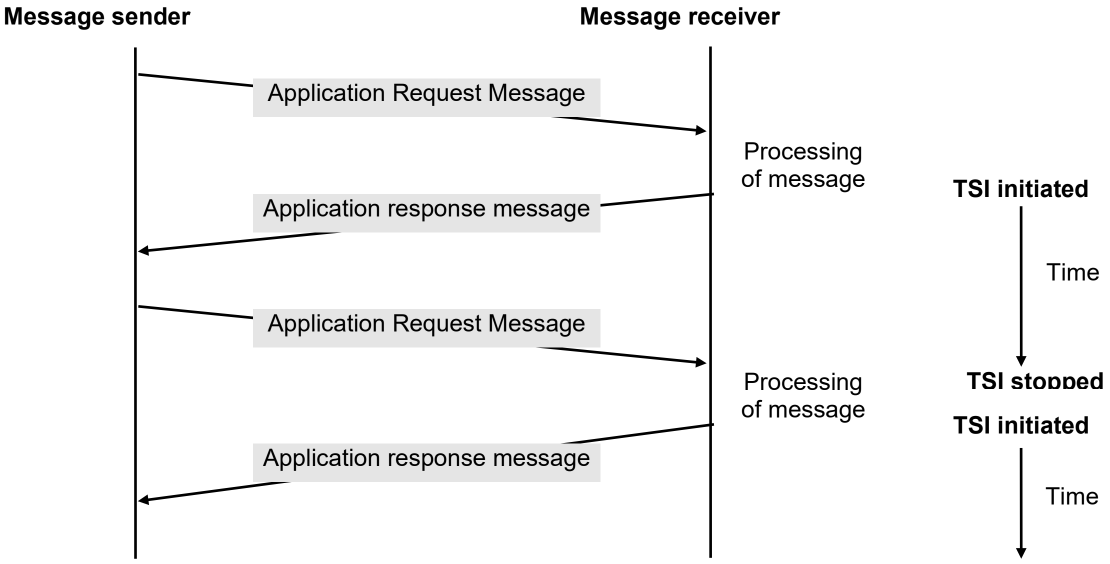
Description of timer:

- Can be negotiated.
- The receiving system initiates the inactivity monitoring timer (TSI) when it sends a Response message.

Expected behaviour in case of a timeout:

- IPDU_AB with a response code PI01 set to 25 (TSI timeout).

Inactivity Monitoring Timer (TSI)



5.4 MAINTAINED ACTIVITY TIMER (TMA)

A specific message (echo test), which is sent when the maintained activity timer (TMA) times out, enables the sending system to confirm the availability of and connection to the receiving system.

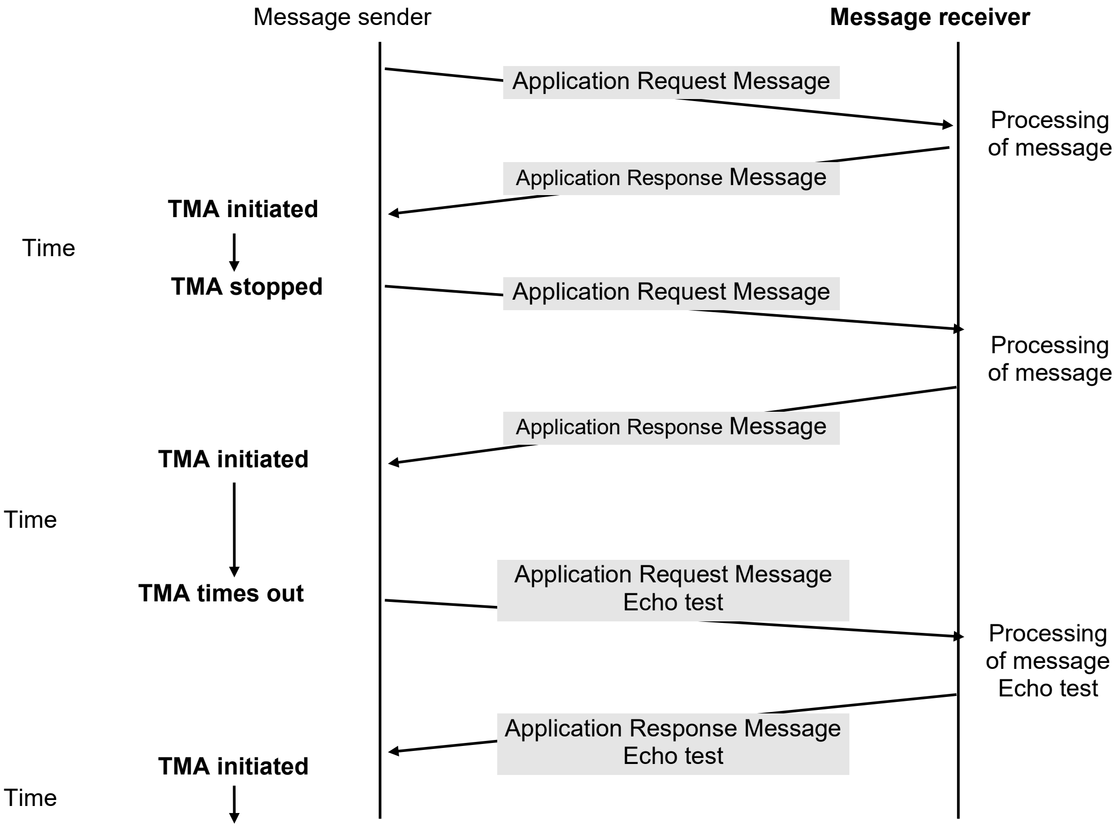
Description of timer:

- The different parties must agree to use this timer.
- Can be negotiated.
- The sending system initiates the Maintained Activity Timer (TMA) when it receives a response and does not intend to send a new request.
- The sending system stops the TMA when it wants to send transactions related to a service.

Expected behaviour in case of a timeout:

- The sending system sends an echo test message when the maintained activity timer (TMA) times out. It reactivates the timer it receives the response to the maintained activity message (echo test).

Maintained Activity Timer (TMA)


Message sender
Message receiver
Application Request Message
Processing of message
Application Response Message
TMA initiated
Time
TMA stopped
Application Request Message
Processing of message
Application Response Message
TMA initiated
Time
TMA times out
Application Request Message Echo test
Processing of message Echo test
Application Response Message Echo test
TMA initiated
Time

5.5 MAINTAINED ACTIVITY MONITORING TIMER (TSM)

The two systems that agreed to monitor maintained activity (echo test) must execute mutual monitoring.
This monitoring is executed as follows:

* The sending system activates the maintained activity timer (TMA).

* The receiving system activates the maintained activity monitoring timer (TSM).

Description of timer:

* The different parties must agree to use this timer.

* Cannot be negotiated.

* The receiving system activates the TSM as soon as it is possible to receive an echo test, in accordance with the defined rules.

* The receiving system activates its maintained activity monitoring timer (TSM) when it has sent the response to the maintained activity message (echo test).

* It stops the timer it when it receives a request message.

Expected behaviour in case of a timeout:

* IPDU_AB with a response code PI01 set to 28 is sent (TSM timeout).

The receiving system deducts a possible TSM value from the negotiated value of the TMA, in compliance with the TSM > TMA rule.

Note about the maintained activity monitoring timer (TSM) and the inactivity monitoring timer (TSI)

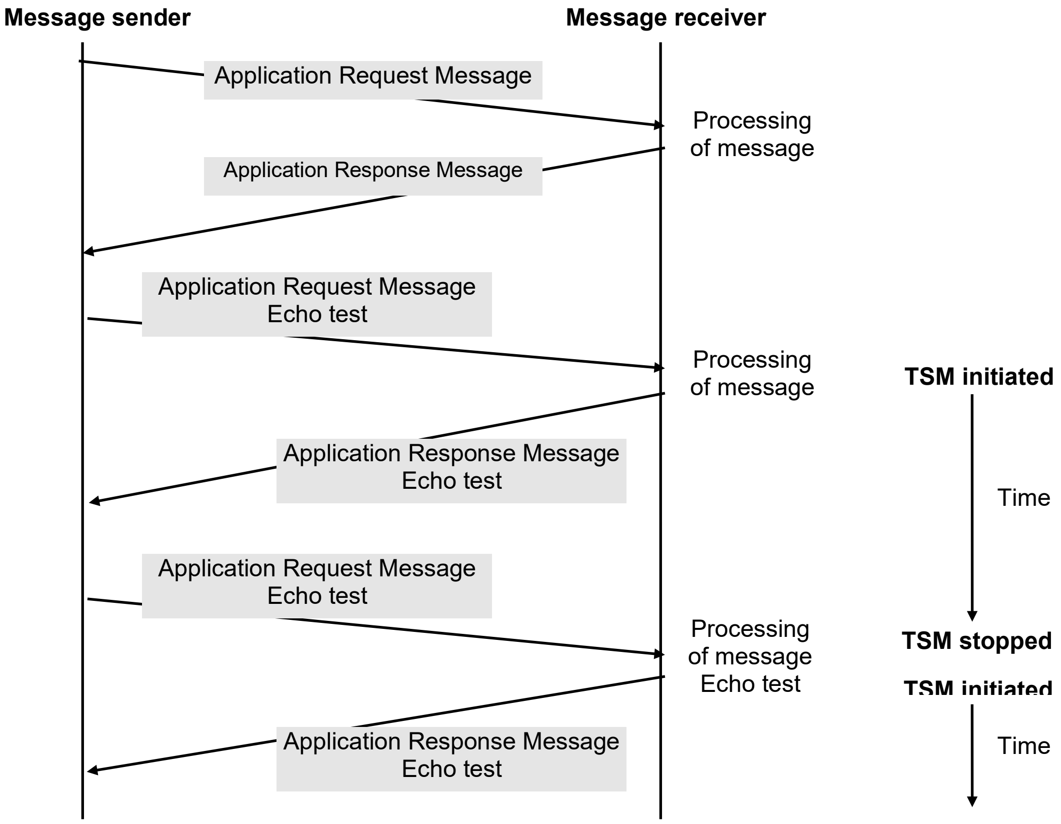
From a functional point of view, the TSM is a TSI whose value is higher than that of the TSI.
The TSI is activated upon receiving a message that does not require a response, but which requires another message or the sending of a response.
The purpose of the TSM is to monitor that activity over the line is properly maintained by echo test messages.

In transaction processing, the inactivity monitoring timer (TSI) and the maintained activity monitoring timer (TSM) have the same purpose (see the summary diagram below). As a result, they have the same meaning.

Meaning of a timeout:

* The sending system is no longer online as an echo-test message should have been received.

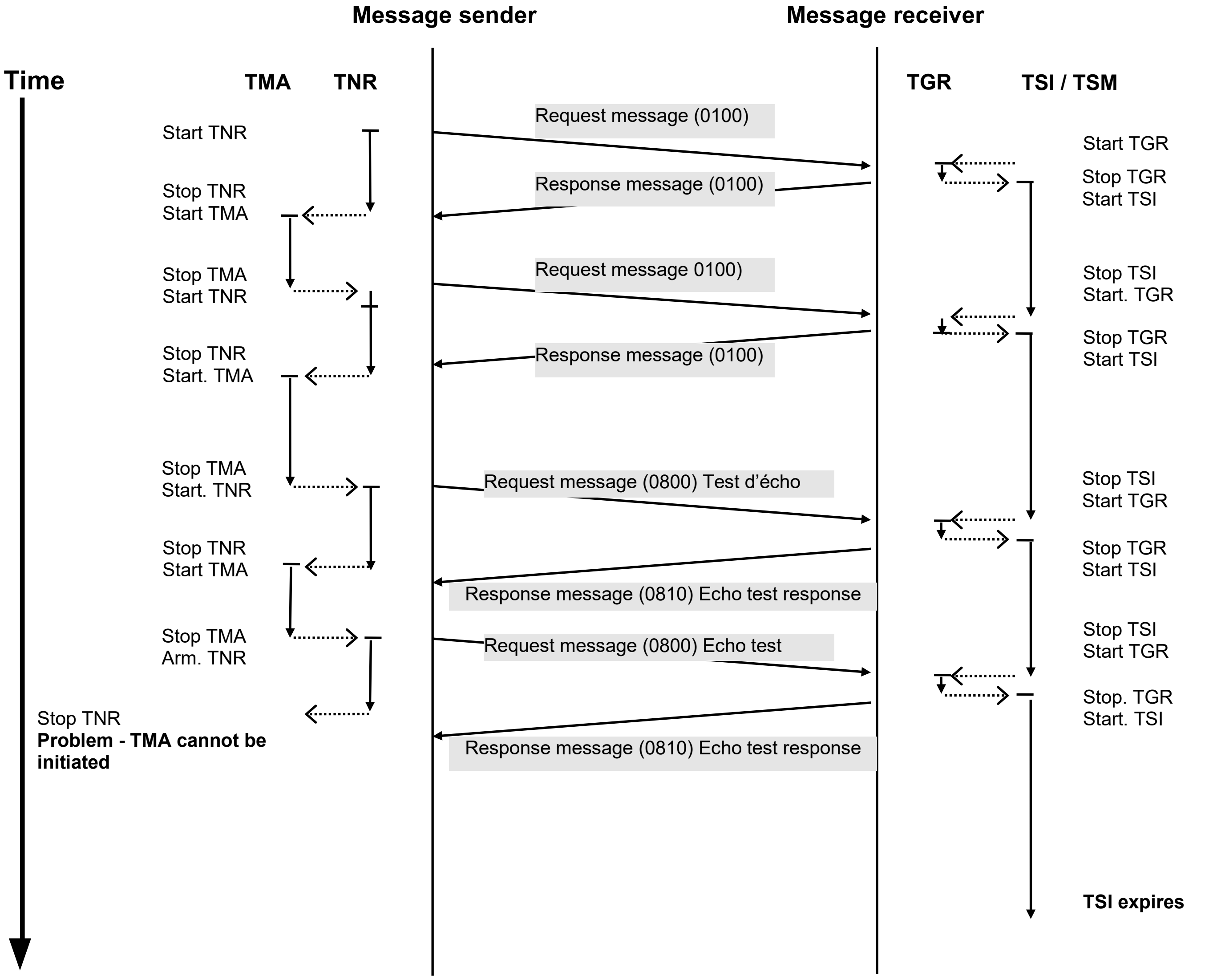
Maintained Activity Monitoring Timer (TSM)


Message sender
Message receiver
Application Request Message
Processing of message
Application Response Message
Application Request Message Echo test
Processing of message
TSM initiated
Application Response Message Echo test
Time
Application Request Message Echo test
Processing of message Echo test
TSM stopped
TSM initiated
Application Response Message Echo test
Time

5.6 EXAMPLES

Summary of TNR, TGR, TSI, TMA, TSM timers in transaction processing

In this context TSI and TSM have the same meaning



5.7 DEFAULT RECOMMENDATIONS

Timer	Negotiable	Minimum value	Maximum value	Recommended value	Constraint
TNR	No	-	-	50 sec	
TGR	No	-	-	30 sec	< TNR
TSI	Yes	2 min	30 min	13 min	
TMA	Yes	2 min	30 min	12 min	< TSI
TSM	No	-	-	15 min	> TSI

DATA FIELD DICTIONARY

TABLE OF CONTENTS

1. PREFACE

1.1. PURPOSE OF DOCUMENT

The Data Field Dictionary defines all the application data used by the protocols in compliance with the ISO 8583 (1987 version) standard.

It also specifies how the data is presented, i.e. the coding and format of the data fields.

Optional or mandatory use of data fields is not indicated in the Data Field Dictionary. This information is provided in the related reference documents.

1.2. TECHNICAL INFORMATION PROVIDED IN DOCUMENT

The Data Field Dictionary provides the following technical information:

- structure of data messages
- data coding rules
- data fields

It also indicates the message identifiers, fields, sub-fields and field values.

Important Note:

Transported data is subject to the rules defined in section 2.2, “DATA FORMAT AND CODING”. However, the final usage of the data element is described in the application.

2. DATA FIELD DICTIONARY

2.1. DESCRIPTION OF DATA MESSAGES

2.1.1. Message structure

The messages used by the CB2A AUTHORISATION protocol comply with the ISO 8583 standard.
Each message has one of the two following structures:

Identifier	bitmap	field i	......	field j	......	field k

where i, j and k range from 2 to 64

or

Identifier	bitmap	bitmap	field i	......	field j	......	field k

where i, j and k range from 2 to 128.

A message includes the following parts:

- message type identifier
- 1 or 2 bitmaps
- data fields that appear by ascending field number within the message

2.1.2. Message type identifier

The message type identifier is a numeric 4-byte field coded in BCD.
This field is mandatory.
The identifiers used by the CB2A Authorisation protocol are the following:

MTI[1]	Meaning
0100	Authorisation request
0110	Authorisation request response
0400	Reversal request
0401	Reversal request repeat
0410	Reversal request response
0800	Network management request
0810	Network management request response

[1]MTI = Message type identifier

2.1.3. Bitmap

Each bitmap contains 64 bits numbered from left to right.

Two bitmaps are defined. The first bitmap is mandatory, while the second is optional. The first bit of the first bitmap specifies the presence or absence of a second bitmap.

In each bitmap, a bit set to 1 indicates the presence of the associated field; a bit set to zero indicates its absence.

2.2. DATA FORMAT AND CODING

2.2.1. Notation conventions

The following tables list the notations used in the Data Fields Dictionary. These notations are used in the description of a field format and the value (or values) which are transported.

Notation	Description
a	alphabetic character ('A' to 'Z', 'a' to 'z')
n	numeric character ('0' to '9')
p	'space' character
s	special character (space included)
an	alphanumeric character
as	alphabetic or special character
ns	numeric or special character
ans	alphanumeric or special character
b	binary data
z	codes relating to magnetic track 2 and/or 3 data
AA	year (2 numeric characters)
MM	month (2 numeric characters)
JJ	day (2 numeric characters)
hh	hour (2 numeric characters)
mm	minutes (2 numeric characters)
ss	seconds (2 numeric characters)
x	"C" for credit, "D" for debit. Always associated with a numeric field which indicates a transaction amount. For example, x + n16 indicates credit or debit of an amount in 16 numeric characters. The amounts are associated with a specific meaning: – "D" indicates a "cardholder debit" in the acceptor/acquirer relationship. It refers to an " acquirer bank debit", which means a "credit" for the acceptor. "D" = Acceptor credit – "C" indicates a "cardholder credit" in the acceptor/acquirer relationship. It refers to an "acquirer bank credit", which means a "debit" for the acceptor. "C" = Acceptor debit

Table 1: Data type notations

Notation	Description
L	length of TLV (Type Length Value)
LL	coded on one byte and between 1 and 99 bytes
LLL	length coded on one byte and between 1 and 255 bytes
LL2	length coded on two bytes and between 1 and 999 bytes
3	fixed-length of 3 units(1)
...15	variable length up to 15 units(1)
3…15	variable length of 3 to 15 units(1)

Table 2: Data length notations

(1) A unit is defined by the field type or the data element.

2.2.2. Presentation conventions

The following conventions are used in CB2A Authorisation:

- For fields with a TLV structure, the notation (12)(3)(456) refers to type 12, 3-byte length, set to '456'.
- In a data coding example, the notation [12][34][56] represents the hexadecimal value of the transported bytes.

2.2.3. Data field coding

2.2.3.1. Data in "numeric" format (n)

These data fields are coded in DCB.

2.2.3.2. Data in "binary" format (b) and 'z' format (Track 2 data)

These data fields are coded in binary.

If "character" data elements are transported in a binary field, a character set must be defined. In this context, EMV usually uses a limited ASCII character set (ASCII 128). For Cartes Bancaires purposes, the extended ASCII character set is used for data coding.

For the network, there is no alphabet conversion for fields of this type.

2.2.3.3. Data elements in "character" format (a, an, as, ns, ans, …)

These data fields are coded in ASCII.

2.2.3.4. Summary table

The following table shows how the data in a given format is coded so that it can be transported inside a field in another format if necessary:

		Field format			
Data format		**Numeric** n	**Binary** b, ansb, …	**Characters** a, an, ns, …	**Magstripe** z
Numeric	n	BCD (1)		ASCII (2.1)	
Characters	a, an, as, ns, ans, …		ASCII (3)	ASCII (2.2)	
Signed numeric	x+n		ASCII + BCD (4)	ASCII (2.3)	
Binary	b, ansb, anscb, …		(5)	ASCII (6)	
Magstripe	z				(7)

(1) BCD coding in quartets:

Data format:	n12 (numeric, 12 positions)
Data value:	12345
Coding: (6 bytes)	`[00][00][00][01][23][45]`

(2) ASCII coding in bytes:

(2.1)	Data format:	n12 (numeric, 12 positions)
	Data value:	12345
	ASCII coding: (12 bytes)	`[30][30][30][30][30][30][30][31][32][33][34][35]`
(2.2)	Data format:	an12 (alphanumeric, 12 positions)
	Data value:	AGENCE2
	ASCII coding: (12 bytes)	`[41][47][45][4E][43][45][32][20][20][20][20][20]`
(2.3)	Data format:	x + n12 (signed numeric, 12 positions)
	Data value:	C12345
	ASCII coding: (13 bytes)	`[43][30][30][30][30][30][30][30][31][32][33][34][35]`

(3) ASCII coding in bytes:

This coding is for transporting alphanumeric data in a binary format field.
This is possible when transporting EMV data, in which case the EMV standard requires that these data be coded using a limited ASCII character set.
For this reason, and for Cartes Bancaires purposes, the extended ASCII character set is used.

Data format:	ans12 (alphanumeric, 12 positions)
Data value:	AGENCE 2
ASCII coding: (12 bytes)	**[41][47][45][4E][43][45][20][32][20][20][20][20]**

(4) Coding in ASCII (one byte) and in BCD (quartets):

This coding is for transporting alphabetic and numeric data in a binary format field.
For Cartes Bancaires purposes, the following values are used for coding alphabetic data: [43] for Credit, and [44] for Debit.
These values represent the characters "C" and "D" in ASCII format.

Data format:	x + n12 (signed numeric, 12 positions)
Data value:	C12345
ASCII coding: (7 bytes)	**[43][00][00][00][01][23][45]**

(5) Binary coding (bytes):

Data format:	b12 (binary, 12 positions)
Data value:	3CDE1245EF7684172048CBFF
Coding: (12 bytes)	**[3C][DE][12][45][EF][76][84][17][20][48][CB][FF]**

(6) Coding the data element's binary quartets in ASCII (bytes):

Data format:	b6 (binary, 6 positions)
Data value:	3CDE1245EF76
Characters sent	**"3","C","D","E","1","2","4","5","E","F","7","6"**
ASCII coding: (12 bytes)	**[33][43][44][45][31][32][34][35][45][46][37][36]**

(7) Coding of z-format data element in a z-format field:

Data format:	z12 (12 positions)
Data value:	45567D874 (where D is the separator)
Coding: (6 bytes)	**[00][04][55][67][D8][74]**

2.2.3.5. Data in "bitmap" format (excluding field-presence bitmap)

In compliance with standard ASN.1 ITU-T Rec. X.690 of July 2002, the bits of a byte are numbered from 8 to 1, where bit 8 is the "most significant bit" and bit 1 the "least significant bit".

Bits	8	7	6	5	4	3	2	1

Numbering of bits in one-byte "bitmap" data

Bits	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Numbering of bits in two-byte "bitmap" data

2.2.4. Rules for filling a non-significant data element based on the field format or type used

A non-significant data element is entirely filled with the pad character specific to its format unless its value is explicitly described.

2.2.5. Format for amounts

Amounts are expressed in the smallest unit of the currency (in cents for Euros) - see the list in ISO 4217.

2.2.6. Field Structure

2.2.6.1. Fixed-length fields

Fixed-length numeric fields are right-justified and left-filled with zeros if necessary. Binary fields occupy a whole number of bytes. Other fields are left-justified and right-filled with blanks.

Example: Coding the value '1000' in the "Transaction amount" field:
Field format: fixed, n12
Coding on 6 bytes: `[00][00][00][01][00][00]`
where 0000000 pad character,
10000 transaction amount.

2.2.6.2. Variable-length fields

Variable-length fields are preceded by one byte or 2 bytes indicating the field length. This length is coded in binary. Depending on the field type, a variable-length field can be from 1 to 255 or 999 bytes long, up to the maximum length of the field format.

Variable-length numeric "n" or "z" fields (such as Track 2 data) are right-justified, with a leading zero if the length is an odd number (pad character).

Examples:

Coding the value '9876543210123456789' in the "Primary Account Number (PAN)" field
Field format: variable LLVAR n…19
Coding on 11 bytes: `[13][09][87][65][43][21][01][23][45][67][89]`
where 13 length: 19 positions (13 in hex)
0 pad character
9876543210123456789 Primary Account Number in 19 positions

Coding the value '9876543210123456' in the "Primary Account Number (PAN)" field
Field format: variable LLVAR n…19
Coding on 9 bytes: `[10][98][76][54][32][10][12][34][56]`
where 10 length: 16 positions (10 in hex)
9876543210123456 Primary Account Number in 16 positions

2.2.6.3. Fields with a TLV (Type Length Value) structure

TLV fields are variable-length fields containing one or more data elements with a TLV structure. They are structured as follows:

Total field length	Data element 1	...	Data element n

The total field length, as for all variable-length fields, is coded in binary on 1 byte. It expresses the length of the data elements as a number of bytes.

A data element is structured as follows:
- "T": data type;
- "L": data length (1 to 255). This is not included in the data length calculation. It expresses the number of bytes able to transport the value "V" that follows.
- "V": value of the data element based on the number of characters defined by the length.

A TLV field therefore has the following structure:

Total length of field	Data element 1				Data element n		
	Type 1	Length 1	Value 1	…	Type n	Length n	Value n

Data elements in a TLV field can be placed in any order. They are not necessarily placed in ascending order of the type.

The types related to EMV data are always coded in 2 bytes. They are right-justified and left-filled with zeros if necessary.

Example: "9F35" ('terminal type') is the coding in 2 bytes of EMV tag "9F35".
"0082" (Application Interchange Profile') is the coding in 2 bytes of EMV tag "82".
Data element coding varies according to the type (character/binary) of the TLV field.

A. "Character" TLV fields

The data elements of a TLV "character" field have an "ans" format. As a result, they are coded in ASCII. Each data element is coded as follows:

- "T": 2 characters (2 bytes)
- "L": 2 characters (2 bytes); the length is right-justified and left-filled with zeros
- "V": the number of characters (bytes) is defined by the length

Example: coding of field 44 (TLV field, LLVAR ans…25)

Representation (14)$_{L}$(AA)$_{T1}$(4)$_{L1}$(0021)$_{V1}$(BD)$_{T2}$(2)$_{L2}$(15)$_{V2}$

L : 14 (total field length)
T1 : AA (incorrect field)
L1 : 4 (length of V1)
V1 : 0021 (value error in field 2)
T2 : BD (Banking Interface number)
L2 : 2 (length of V2)
V2 : 15 (Banking Interface number 15)

ASCII coding

[0E]$_{L}$
[41][41]$_{T1}$[30][34]$_{L1}$[30][30][32][31]$_{V1}$
[42][44]$_{T2}$[30][32]$_{L2}$[31][35]$_{V2}$

B. "Binary" TLV fields

Each data element is coded as follows:

-"T": 2 binary bytes
-"L": 1 binary byte (maximum length 255) or two binary bytes (maximum length 999),
-"V": the number of bytes is defined by the length. The binary format is implicit for each type. The description may specify several fixed-length data elements.

Example: coding of field 55 (TLV field, LLLVAR b…255)

Representation (11)$_{L}$(9C)$_{T1}$(1)$_{L1}$(00)$_{V1}$(9F37)$_{T2}$(4)$_{L2}$(F56BA536)$_{V2}$

L : 11 (total field length)
T1 : 9C (Transaction Type)
L1 : 1 (length of V1)
V1 : 00
T2 : 9F37 (Unpredictable Number)
L2 : 4 (length of V2)
V2 : F56BA536 (discriminating element)

Coding

[0B]$_{L}$
[00][9C]$_{T1}$[01]$_{L1}$[00]$_{V1}$
[9F][37]$_{T2}$[04]$_{L2}$[F5][6B][A5][36]$_{V2}$

2.2.6.4. Coding of types containing several data elements

Some types contain several data elements. There are two cases:

1. The type has a 'Structure' format. In this case, the coding and alignment rules specific to each of the data elements are applied. The data elements may have a different format.

Example 1: Field XX Format: b…255
Type: FFEE
Data format: Structure Number of bytes transported: 6

	Format	Value
Data element A	n1	1
Data element B	n3	123
Data element C	n5	456

Coding:

Data element A is n1, coded in 1 byte:	[01]
Data element B is n3, coded in 2 bytes:	[01][23]
Data element C is n5, coded in 3 bytes:	[00][04][56]

Therefore: $[FF][EE]_T$ $[06]_L$ $\underbrace{[01]}_{A}\underbrace{[01][23]}_{B}\underbrace{[00][04][56]}_{C}{}_V$

Example 2: Field XX Format: b…255
Type: FFEE
Data format: Structure Number of bytes transported: 5

	Format	Value
Data element A	n1	1
Data element B	b2	5F6
Data element C	n4	1999

Coding:

Data element A is n1, coded in 1 byte:	[01]
Data element B is b2, coded in 2 bytes:	[05][F6]
Data element C is n4, coded in 2 bytes:	[19][99]

Therefore: $[FF][EE]_T$ $[05]_L$ $\underbrace{[01]}_{A}\underbrace{[05][F6]}_{B}\underbrace{[19][99]}_{C}{}_V$

2. If the type does not have a 'Structure' format, coding and alignment rules must be applied. All data elements have an identical format.

Example: Field XX Format: b…255
Type: FFEE
Data format: n9 Number of bytes transported: 5

	Format	Value
Data element A	n1	1
Data element B	n3	123
Data element C	n5	456

Coding: As the type format is 'n9', the data is coded in 5 bytes. A quartet is attributed to each data element according to its format. In the example, as the format of the TLV type is numeric and contains an odd number of characters, the value of the type is right-justified and left-filled with a zero.

Therefore: $[FF][EE]_T$ $[05]_L$ $\underbrace{[01]}_{A}\underbrace{[12][30]}_{B}\underbrace{[04][56]}_{C}{}_V$

2.3. DATA FIELD DESCRIPTIONS

2.3.1. Alphabetical list

The table below presents an alphabetical list of the data elements used in the CB2A Authorisation protocol.
Each data element is shown with the field number used to transport it, and (when necessary) the sub-field for data transported in a TLV field structure.

Data element	Field/sub-field
3DS protocol major version	56 type 0022
3DS protocol version number	119 type 0022
Acceptance system card product code	56 type 0005
Acceptance system country code	59 type 0205
Acceptance system logical number	59 type 0203
Acceptor contract number	59 type 0202
Acquiring institution identification code	32
Additional amounts	54
Additional card reading capabilities	47 type 30
Additional data	56
Additional data - national	47
Additional electronic commerce data elements	59 type 0414
Additional electronic commerce transaction data	56 type 0046
Additional response data	44
Amount, authorised	55 type 9F02
Amount, other	55 type 9F03
Amount, transaction	4
Application Cryptogram (ARQC)	55 type 9F26
Application cryptogram verification results	44 type CB
Application Expiration Date	55 type 5F24
Application Identifier (AID)	55 type 9F06
Application Interchange Profile (AIP)	55 type 0082
Application selection indicator	56 type 0002
Application Selection Registered Proprietary Data	55 type 9F0A
Application Transaction Counter (ATC)	55 type 9F36
Application type identifier	112 type 03
Authentication amount	56 type 0038
Authentication date	56 type 0037
Authentication exemption status indicator	119 type 0017
Authentication merchant name	56 type 0036
Authorisation identification response	38
Authorisation identification response length	27
BDK (Base Derivation Key) name	48 type 0002
BDK (Base Derivation Key) version	48 type 0003
BIC	112 type 09
Bit Map Extended	1
Brand selected	56 type 0003
Card acceptor identification code	42
Card acceptor name/location	43
Card acceptor terminal identification	41
Card application type	55 type DF81
Card-on-file action	56 type 0029
Card security code	59 type 0300
Card security code verification results	59 type 0301
Card sequence number	23
Card type indicator	56 type 0018
Cardholder address	56 type 0006
Cardholder address checking information	44 type CC
Cardholder authentication method	59 type 0410
Cardholder authentication value	59 type 0401
Cardholder authentication value calculation method	59 type 0411
Cardholder authentication value processing information	59 type 0409

Data element	**Field/sub-field**
Cardholder postcode	56 type 0008
Cardholder total amount	59 type 0207
Cardholder verification method (CVM) results	55 type 9F34
Cardholder verification method used at POS	119 type 1022
CB2A specification date	47 type 33
Contactless device	55 type DF86
Counterparty last name and first name	112 type 07
Counterparty PAN	112 type 06
Cryptogram entry date and GMT time	56 type 0017
Cryptogram information data	55 type 9F27
Currency code, transaction	49
Data equivalent to ISO track 1 read in contactless mode	55 type 56
Data equivalent to ISO track 2 read in contactless mode	55 type DF6B
Date, expiration	14
Date, local transaction	13
Debit unique reference identifier	119 type 0047
Delivery address	56 type 0009
Digital wallet additional data	59 type 0417
Digital wallet name	59 type 0415
Electronic commerce data, initial transaction	59 type 0420
Electronic commerce indicator	59 type 0416
Electronic commerce authentication type	59 type 0407
ERT (Regulatory and Technical Environment)	59 type 0200
Exemption indicator	56 type 0033
Extended Electronic Commerce Indicator	119 type 0016
Extended message to the transaction initiator	119 type 00BC
Field conversion	44 type AC
Field conversion by acquirer (field 32) or forwarder (field 33)	47 type 20
File number	47 type 24
Final merchant identifier	56 type 0027
Forwarding institution identification code	33
FPAN	119 type 0011
Function code	59 type 0100
Funds transfer data	112
Funds transfer reason	112 type 08
IBAN	112 type 10
ICC processing results	55 type DF80
IDPA (Point of interaction identifier assigned by an acquirer)	47 type 97
IDSA (Acceptance system identifier assigned by an acquirer)	47 type A0
Incorrect field	44 type AA
Independent sales organisation	56 type 0024
Integrated circuit card system related data	55
IP address	56 type 0010
Issuer Action Code – Default	56 type 9F0D
Issuer Action Code – Denial	56 type 9F0E
Issuer Action Code - Online	56 type 9F0F
Issuer authentication data	55 type 0091
Issuer application data	55 type 9F10
Issuer proprietary data	55 type 9F7C
Issuer script results	55 type FF00
Issuer script template 1	55 type 0071
Issuer script template 2	55 type 0072
ITP PA (Point of interaction terminal application identifier)	59 type 0215
ITP SA (Acceptance system terminal application identifier)	59 type 0201
Kernel ID used	55 type DF68
KSN	48 type 0001
Language preference	56 type 5F2D
Last four digits of PAN	119 type 9F25
List of installed kernels	56 type 0040
Location category code	47 type 08
Marketplace identifier	56 type 0026
Merchant tokenisation indicator	119 type 0001
Merchant type	18
Message reason code	59 type 0101

Data element	Field/sub-field
Message to the transaction initiator	44 type BC
Mobile payment solution identifier	56 type 0012
Modified electronic commerce authentication type	59 type 0413
National data	59
Network management information code	70
nexo Acceptance System identifier	115 type 0002
nexo certificate	115 type 0003
nexo data	115
nexo PoS identifier	115 type 0001
Number of articles	56 type 0011
Optional services supported (acceptor domain)	59 type 0805
Order giver's account number at the organiser	112 type 05
Original data elements	90
Original transaction data	112 type 01
Original unique transaction identifier	47 type 99
Payment Account Reference	56 type 0056
Payment facilitator data	56 type 0001
Payment facilitator identifier	56 type 0025
Payment number	56 type 0031
Payment use case	56 type 0028
Payment validity date	56 type 0045
PIN data	52
PIN length	26
Point of interaction extended logical number	59 type 0216
Point of interaction information	47 type 31
Point of interaction logical number	59 type 0204
Point of service condition code	25
Point of service entry mode	22
Pre-authorisation duration	119 type 0208
Primary Account Number (PAN)	2
Processing code	3
Purchase identifier	119 type 0042
Purchase identifier type	119 type 0041
Reattempt conditions	119 type 0803
Reattempt frozen period	119 type 0802
Reattempt indicator	119 type 0801
Remote commerce acceptor identifier	119 type 0028
Replacement amounts	95
Resend counter	56 type 0020
Reserved for national use	119
Responding machine identifier	58
Response code	39
Responsibility transfer information	44 type CD
RTT (Terminal processing results)	55 type DF85
Reserved for national use	119
Retrieval reference number	37
Risk scoring service	59 type 0802
Scheme program merchant identifier	119 type 0009
Security Data	48
Security error	44 type AB
Security related control information	53
Serial number	56 type 0019
Service activation code	44 type AF
Service attribute	59 type 0800
SIRET	47 type 96
Systems trace audit number	11
TASA (Card acceptor application type)	59 type 020B
Telephone number	44 type BB
Terminal capabilities	55 type 9F33
Terminal Transaction Date	55 type 009A
Terminal Transaction Qualifiers (TTQ)	55 type 9F66
Terminal Type (Type de Terminal)	55 type 9F35
Terminal Verification Results (TVR)	55 type 0095
Three-domain secure components availability	119 type 0015

Data element	Field/sub-field
Three-domain secure results	59 type 0412
Three-domain secure results, others	59 type 0419
Time, local transaction	12
Token authentication verification value	119 type 0015
Token Requestor ID	119 type 9F19
Total number of payments	56 type 0032
Track 2 data	35
Track 2 equivalent data	55 type 0057
Track or equivalent data cryptogram processing information	44 type CA
Transaction eligible for token services	119 type 0359
Transaction identifier or cryptogram supplied by the acceptor	59 type 0400
Transaction type	55 type 009C
Transaction year	59 type 0102
Transmission date and time	7
Type of proof	56 type 0014
Type of transaction	56 type 0013
Unique transaction identifier	47 type 95
Unpredictable number	55 type 9F37
UUID container	56 type 0023
Wallet identifier	59 type 0418

2.3.2. List by field number

All fields of the ISO 8583 standard can be used in the CB2A Authorisation protocol, but only the significant fields are presented below. The table indicates whether or not the field is used in the CB2A Authorisation protocol.

No.	Type	Name	Format	
1		Bit Map Extended		
2		Primary Account Number (PAN)	LLVAR	n …19
3		Processing code		n 6
4		Amount, transaction		n 12
5		See ISO 8583 standard		n 12
6		See ISO 8583 standard		n 12
7		Transmission date and time	MMDDhhmmss	n 10
8		See ISO 8583 standard		n 8
9		See ISO 8583 standard		n 8
10		See ISO 8583 standard		n 8
11		Systems trace audit number		n 6
12		Time, local transaction	hhmmss	n 6
13		Date, local transaction	MMDD	n 4
14		Date, expiration	YYMM	n 4
15		See ISO 8583 standard		n 4
16		See ISO 8583 standard		n 4
17		See ISO 8583 standard		n 4
18		Merchant type		n 4
20		See ISO 8583 standard		n 3
21		See ISO 8583 standard		n 3
22		Point of service entry mode		n 3
23		Card sequence number		n 3
24		See ISO 8583 standard		n 3
25		Point of service condition code		n 2
26		PIN length		n 2
27		Authorisation identification response length		n 1
28		See ISO 8583 standard		x+n 8
29		See ISO 8583 standard		x+n 8
30		See ISO 8583 standard		x+n 8
31		See ISO 8583 standard		x+n 8
32		Acquiring institution identification code	LLVAR	n …11
33		Forwarding institution identification code	LLVAR	n …11
34		See ISO 8583 standard	LLVAR	ns …28
35		Track 2 data	LLVAR	z …37
36		See ISO 8583 standard	LLLVAR	z …104
37		Retrieval reference number		an 12

No.	Type	Name	Format	
38		Authorisation identification response		an 6
39		Response code		an 2
40		See ISO 8583 standard		an 3
41		Card acceptor terminal identification		ans 8
42		Card acceptor identification code		ans 15
43		Card acceptor name/location		ans 40
44		Additional response data	LLVAR	ans …25
	AA	Incorrect field		ans 4,6,8
	AB	Security error		ans 5
	AC	Field conversion		ans …21
	AF	Service activation code		ans 1
	BB	Telephone number		ans …21
	BC	Message to the transaction initiator		ans …21
	CA	Track or equivalent data cryptogram processing information		ans 1
	CB	Application cryptogram verification results		ans 1
	CC	Cardholder address checking information		ans 2
	CD	Responsibility transfer information		ans 1
45		See ISO 8583 standard	LLVAR	ans …76
46		See ISO 8583 standard	LLLVAR	ans …255
47		Additional data - national	LLLVAR	ans …255
	08	Location category code		ans …8
	20	Field conversion by acquirer (field 32) or forwarder (field 33)		ans …
	24	File number		anp 12
	30	Additional card reading capabilities		n 1
	31	Point of interaction information		n 1
	33	CB2A specification date		n 4
	95	Unique transaction identifier		ans ..50
	96	SIRET		ans 14
	97	IDPA (Point of interaction identifier assigned by an acquirer)		ans 8
	99	Original unique transaction identifier		ans..50
	A0	IDSA (Acceptance system identifier assigned by an acquirer)		ans 8
48		Security Data	LLLVAR	ansb …255
	0001	KSN		b10..12
	0002	BDK (Base Derivation Key) name		b2..15
	0003	BDK (Base Derivation Key) version		n..10
49		Currency code, transaction		n 3
50		See ISO 8583 standard		n 3
51		See ISO 8583 standard		n 3
52		PIN data		b 8..16
53		Security related control information		n 16
54		Additional amounts	LLLVAR	an …120
55		Integrated circuit card system related data	LLLVAR	b …255
	0056	Data equivalent to ISO track 1 read in contactless mode		ans …76
	0057	Track 2 equivalent data		b …19
	0071	Issuer Script Template 1		b …128
	0072	Issuer Script Template 2		b …128
	0082	Application Interchange Profile (AIP)		b 2
	0091	Issuer Authentication Data		b 8…16
	0095	Terminal Verification Results (TVR)		b 5
	009A	Terminal Transaction Date		n 6
	009C	Transaction type		n 2
	5F24	Application Expiration Date	YYMMDD	n 6
	9F02	Amount, authorised		n 12
	9F03	Amount, other		n 12
	9F06	Application identifier (AID)		b 5…16
	9F0A	Application Selection Registered Proprietary Data		b 4...32
	9F10	Issuer application data		b …32
	9F26	Application Cryptogram (ARQC)		b 8
	9F27	Cryptogram Information Data		b 1
	9F33	Terminal capabilities		b 3
	9F34	Cardholder verification method (CVM) results		b 3
	9F35	Terminal Type (Type de Terminal)		n 2
	9F36	Application Transaction Counter (ATC)		b 2

No.	Type	Name	Format	
	9F37	Unpredictable Number		b 4
	9F66	Terminal Transaction Qualifiers (TTQ)	structure	4
	9F6B	Data equivalent to ISO track 2 read in contactless mode		b …19
	9F7C	Issuer proprietary data		b …32
	DF68	Kernel ID used		b 1
	DF80	ICC processing results		n 2
	DF81	Card application type		n 1
	DF85	RTT (Terminal processing results)		b 5
	DF86	Contactless device		b …35
	FF00	Issuer script results		b …5
56		Additional data	LLLVAR	b …255
	0001	Payment facilitator data	structure	27
	0002	Application selection indicator		n2
	0003	Brand selected		b1
	0005	Acceptance system card product code		an3
	0006	Cardholder address		ansp..40
	0008	Cardholder postcode		ansp..10
	0009	Delivery address		ans80
	0010	IP address		ans4…45
	0011	Number of articles		n2
	0012	Mobile payment solution identifier		n3
	0013	Type of transaction		n2
	0014	Type of proof		n2
	0017	Cryptogram entry date and GMT time		n12
	0018	Card type indicator		n1
	0019	Serial number		ans..35
	0020	Resend counter		n1
	0022	3DS protocol major version		an1
	0023	UUID container		ans37
	0024	Independent sales organisation		ans15
	0025	Payment facilitator identifier		ans15
	0026	Marketplace identifier		ans15
	0027	Final merchant identifier		ans15
	0028	Payment use case		n2
	0029	Card-on-file action		an1
	0031	Payment number		n2
	0032	Total number of payments		n2
	0033	Exemption indicator		b2..3
	0036	Authentication merchant name		ans40
	0037	Authentication date		n14
	0038	Authentication amount		n12
	0040	List of installed kernels		b1..8
	0045	Payment validity date		n6
	0046	Additional electronic commerce transaction data	structure	126
	0056	Payment Account Reference		ans29
	5F2D	Language preference		an2
	9F0D	Issuer Action Code – Default		b5
	9F0E	Issuer Action Code – Denial		b5
	9F0F	Issuer Action Code - Online		b5
57		See ISO 8583 standard	LLLVAR	ans …255
58		Responding machine identifier	LLLVAR	ans …255
59		National data	LLLVAR	b …255
	0100	Function code		n 3
	0101	Message reason code		n 4
	0102	Transaction year		n 2
	0200	ERT (Regulatory and Technical Environment)		b 1
	0201	ITP SA (Acceptance system terminal application identifier)		n 12
	0202	Acceptor contract number		n 7
	0203	Acceptance system logical number		n 3
	0204	Point of interaction logical number		n 3
	0205	Acceptance system country code		n 3
	0207	Cardholder total amount		n 12
	020B	TASA (Card acceptor application type)		b 5…16
	0215	ITP PA (Point of interaction terminal application identifier)		n 12

No.	Type	Name	Format	
	0216	Point of interaction extended logical number		an 3
	0300	Card security code	structure	1, 3 or 4
	0301	Card security code verification results	structure	2
	0400	Transaction identifier or cryptogram supplied by the acceptor		b4…40
	0401	Cardholder authentication value		b 20..40
	0407	Electronic commerce transaction authentication type		n 2
	0409	Cardholder authentication value processing information		anp 1
	0410	Cardholder authentication method		ans 2
	0411	Cardholder authentication value calculation method		an 1
	0412	Three-domain secure results	structure	4
	0413	Modified electronic commerce authentication type		b 1
	0414	Additional electronic commerce data elements	structure	3..40
	0415	Digital wallet name		an 2
	0416	Electronic commerce indicator		an 2
	0417	Digital wallet additional data		an12..24
	0418	Wallet identifier		n6
	0419	Three-domain secure results, others	structure	10
	0420	Electronic commerce data, initial transaction	structure	22..58
	0800	Service attribute		n 2
	0802	Risk scoring service	structure	1..24
	0805	Optional services supported (acceptor domain)		b 2
60		See ISO 8583 standard	LLLVAR	ans …1
61		See ISO 8583 standard	LLLVAR	ans …3
62		Reserved for private use	LLLVAR	ans …255
63		Reserved for private use	LLLVAR	ans …255
64		See ISO 8583 standard		b 8
65		See ISO 8583 standard		b 11
66		See ISO 8583 standard		n 1
67		See ISO 8583 standard		n 2
68		See ISO 8583 standard		n 3
69		See ISO 8583 standard		n 3
70		Network management information code		n 3
71		See ISO 8583 standard		n 4
72		See ISO 8583 standard		n 4
73		See ISO 8583 standard		n 6
74		See ISO 8583 standard		n 10
75		See ISO 8583 standard		n 10
76		See ISO 8583 standard		n 10
77		See ISO 8583 standard		n 10
78		See ISO 8583 standard		n 10
79		See ISO 8583 standard		n 10
80		See ISO 8583 standard		n 10
81		See ISO 8583 standard		n 10
82		See ISO 8583 standard		n 12
83		See ISO 8583 standard		n 12
84		See ISO 8583 standard		n 12
85		See ISO 8583 standard		n 12
86		See ISO 8583 standard		n 16
87		See ISO 8583 standard		n 16
88		See ISO 8583 standard		n 16
89		See ISO 8583 standard		n 16
90		Original data elements		n 42
91		See ISO 8583 standard		an 1
92		See ISO 8583 standard		an 2
93		See ISO 8583 standard		an 5
94		See ISO 8583 standard		an 7
95		Replacement amounts		an 42
96		See ISO 8583 standard		b 8
97		See ISO 8583 standard		x+n 16
98		See ISO 8583 standard		ans 25
99		See ISO 8583 standard	LLVAR	n …11
100		See ISO 8583 standard	LLVAR	n …11
101		See ISO 8583 standard	LLVAR	ans …17
102		See ISO 8583 standard	LLVAR	ans …28

No.	Type	Name	Format	
103		See ISO 8583 standard	LLVAR	ans …28
104		See ISO 8583 standard	LLLVAR	ans …100
105		See ISO 8583 standard	LLLVAR	ans …255
106		See ISO 8583 standard	LLLVAR	ans …255
107		See ISO 8583 standard	LLLVAR	ans …255
108		See ISO 8583 standard	LLLVAR	ans …255
109		See ISO 8583 standard	LLLVAR	ans …255
110		See ISO 8583 standard	LLLVAR	ans …255
111		See ISO 8583 standard	LLLVAR	ans …255
112		Funds transfer data	LLLVAR	ans …255
	01	Original transaction data		ans 1..99
	03	Application type identifier		an 2
	05	Order giver's account number at the organiser		ans1..35
	06	Counterparty PAN		n..19
	07	Counterparty last name and first name		ans1..30
	08	Funds transfer reason		ans1..40
	09	BIC		ans1..11
	10	IBAN		an..34
113		See ISO 8583 standard	LLLVAR	ans …255
114		See ISO 8583 standard	LLLVAR	ans …255
115		nexo data	LLLVAR	b …255
	0001	nexo PoS identifier		ans..107
	0002	nexo Acceptance System identifier		ans..71
	0003	nexo certificate		ans..35
116		See ISO 8583 standard	LLLVAR	ans …255
117		See ISO 8583 standard	LLLVAR	ans …255
118		See ISO 8583 standard	LLLVAR	ans …255
119		Reserved for national use	LL2VAR	b…999
	0001	Merchant tokenisation indicator		an1
	0009	Scheme program merchant identifier		ans…8
	0011	FPAN		n9…19
	0013	Three-domain secure components availability		an1
	0015	Token authentication verification value		b4…40
	0016	Extended Electronic Commerce Indicator		n3
	0017	Authentication exemption status indicator		an1
	0022	3DS protocol version number		ans1…8
	0028	Remote commerce acceptor identifier		b…115
	0041	Purchase identifier type		an1
	0042	Purchase identifier		an32
	0047	Debit unique reference identifier		ans…50
	00BC	Extended message to the transaction initiator		ans…101
	0208	Pre-authorisation duration		n2
	0359	Transaction eligible for token services		an1
	0801	Reattempt indicator		n2
	0802	Reattempt frozen period		n4
	0803	Reattempt conditions		n6
	1022	Cardholder verification method used at POS		b1…4
	9F19	Token Requestor ID		an11
	9F25	Last four digits of PAN		n4
120		See ISO 8583 standard	LLLVAR	ans …255
121		See ISO 8583 standard	LLLVAR	ans …255
122		See ISO 8583 standard	LLLVAR	ans …255
123		See ISO 8583 standard	LLLVAR	ans …255
124		See ISO 8583 standard	LLLVAR	ans …255
125		See ISO 8583 standard	LLLVAR	ans …255
126		See ISO 8583 standard	LLLVAR	ans …255
127		See ISO 8583 standard	LLLVAR	ans …255
128		See ISO 8583 standard		b8

2.3.3. Definition of data fields used

This section defines the data fields used by the application protocols. These fields are a sub-set of those defined by ISO 8583 standard. The definition given here is more restrictive than that provided in the standard. The purpose is to simplify implementation and indicate the choices made relative to French and foreign bank cards.

Any type not defined in the CB2A Authorisation protocol is reserved for FrenchSys use, unless it is explicitly declared for private use in the dictionary.

The value of any data element not defined in the CB2A Authorisation protocol is reserved for FrenchSys use, unless it is declared explicitly for private use in the dictionary.
Any non-defined field in the CB2A Authorisation protocol, but defined in ISO 8583, can be used in agreements between users.

Basic principles for data fields

- **Any decodable* data field that is received and expected is processed in accordance with the specifications.**
- **Any decodable* data field that is received and not expected is not processed. It is not sent back and does not generate a chargeback.**
- **Any data field explicitly declared with a "mandatory absent" condition results in a chargeback, if received.**
- **Data elements that are received but not decodable* are rejected.**

* A data field is considered decodable if its structure is described in the dictionary and if it complies with the description.

- Fixed: data field format is described
- Variable without a TLV structure: data field format is described
- Variable with a TLV structure: data field has a TLV structure (the type is not necessarily described)

Field 2 **Format: LLVAR n ...19**

Primary Account Number

This field contains the Primary Account Number (PAN) related to the card.

Field 3 **Format: n6**

Processing code

❑ **Transaction description** ______ **n2**

Value	Description
00	Purchase of goods or services
10	Financial transaction without cash dispensing (e.g. bank transfer request)
11	Quasi-cash
14	Card capture
15	Authorisation to issue a certificate
17	Counter withdrawal
18 to 19	Reserved for private use
20	Credit (returns)
28	Quasi-cash refund
30	Available funds enquiry
36	Balance enquiry (copy)
37	Card return
41	Funds transfer, debit
42	Funds transfer, credit
90 to 99	Reserved for private use

❑ **Account type assigned to debit** ______ **n2**

Value	Description
00	Payment with no special features
33	Deferred clearing

❑ **Account type assigned to credit** ______ **n2**

Value	Description
00	Payment with no special features

Field 4 **Format: n12**

Amount, transaction

Transaction amount stated in the local currency of the acquirer or the transaction's originating location.

The amount is expressed in the smallest unit of the currency - see the list in ISO 4217.
The currency used is specified in field 49.

Field 7	**Format: n10 MMDDhhmmss**

Transmission date and time

Date and GMT time at which the message was sent. Once this has been set, this data element remains unchanged throughout the duration of the message.

Note: This is the date and time when the response was sent (not when the transaction began).

Field 11	**Format: n6**

Systems trace audit number

This field is used to reference the transaction in a unique manner and is managed by the initiator.
This transaction reference must be unique for an acquirer (field 32), acceptor (field 42), terminal ID (field 41), date (field 13) and time (field 12).

For an acceptance system application, field 11 must provide a unique reference for the transaction between two data capture sessions.

Field 12	**Format: n6 hhmmss**

Time, local transaction

Local time at which the transaction took place on an acceptor's premises. Once set, this data remains unchanged throughout the duration of the transaction.

Seconds are not printed on payment terminal receipts and are set to zero in field 12.

Field 13	**Format: n4 MMDD**

Date, local transaction

Local date on which the transaction took place on the card acceptor's premises. Once set, this data remains unchanged throughout the duration of the transaction.

Field 14	**Format: n4 AAMM**

Date, expiration

Card expiry date.
When present, this field must contain a significant value with YYMM structure.

Field 18	**Format: n4**

Merchant type

This code indicates the acceptor’s type of activity.

This code corresponds to the MCC (Merchant Category Code).

When present, this field must contain a significant value. The latest updates and values of this field are specified in Annex A of the ISO 18245 standard.

Field 22 Format: n3

Point of service entry mode

Values used:

□ **PAN entry mode** **quartets 1 and 2**

Value	Description
00	Not specified
01	Manual
02	Magstripe only (track 2 or track 1 data)
03	Barcode
04	Optical reader
05	Chip only (1)
07	Contactless using chip data
10	Card-on-File
81	Chip mode with fallback to magstripe (track 2) mode (2)
82	Provided by a server (Wallet)
83-89	Reserved for private use
91	Contactless using magstripe data
92-99	Reserved for private use

[1] The result(s) of attempt(s) to access the chip are present in field 55, type DF80.
[2] The result(s) of attempt(s) to access the chip can be present in field 55, type DF80, if they are available.

□ **PIN entry capability** **quartet 3**

Value	Description
0	Not specified
1	PIN entry
2	No PIN entry
8-9	Reserved for private use

PAN entry mode also specifies how the expiry date is entered.
PIN entry capability refers to the action performed for the current transaction.

Field 23 Format: n3

Card Sequence Number

Number used to distinguish between cards assigned to the same Primary Account Number (field 2).

Field 25 **Format: n2**

Point of service condition code

Any field 25 value not defined in the present dictionary can be used in agreements between users, providing that the value is compliant with ISO 8583.

Values:

Value	Description
00	Normal conditions
01	Customer not present
02	Unattented terminal able to retain card
03	Suspicious merchant
07	Telephone device request (via call center)
08	Mail/telephone order
10	Customer identity verified
11	Suspected fraud
12	Security reasons
15	Customer terminal (Home terminal)
27	Unattented terminal unable to retain card
52	Mail order
53	Telephone order
54-99	Reserved for private use

If there are several special conditions, it is recommended to give the highest priority to fraud or security description codes.

Priority should then be given to the most detailed description rather than a general description.

Field 26 **Format: n2**

PIN length

This data element specifies the maximum PIN length that can be input.

Possible values: 4 to 12.

Field 27 **Format: n1**

Authorisation identification response length

Maximum length of the authorisation number that the requester is able to process.

Field 32 **Format: LLVAR n…11**

Acquiring institution identification code

This field identifies the acquirer of the transaction, i.e. the institution presenting the transaction.

Field 32 contains the identifier of the acquirer bank.
The structure is the following:

❑ **Acquirer identifier** ________________ **n6**

❑ **Bank code** ________________ **n5**

Field 33 **Format: LLVAR n…11**

Forwarding institution identification code

Field 33 identifies the intermediate institutions between the acceptor and the acquirer.

Field 35 **Format: LLVAR z…37**

Track 2 data

Contains track 2 in compliance with the ISO 7813 standard.

Field 37 **Format: an12**

Retrieval reference number

Field 38 **Format: an6**

Authorisation identification response

Field 38 is defined only by the issuer in a response.

Field 39 **Format: an2**

Response code

This field contains the following:

- Request message: reason for the request
- Response message: result of the response to the request.

Any field 39 value not defined in the present dictionary can be used in agreements between users, providing that the value is compliant with ISO 8583.

The list of response codes that can be used is given below.

Value	Description
00	Approved or completed successfully
02	Refer to card issuer
03	Invalid merchant
04	Pick-up
05	Do not honour
07	Pick-up card, special condition
08	Honour with identification
10	Approved for partial amount
12	Invalid transaction
13	Invalid amount
14	Invalid card number (no such number)
15	No such issuer
17	Customer cancellation
20	Invalid response (error in server domain)
21	No action taken
25	Unable to locate record on file
30	Format error

Value	Description
31	Bank not supported by switch
32	Completed partially
33	Expired card
34	Suspected fraud
38	Allowable PIN tries exceeded
41	Lost card
43	Stolen card, pick-up
46	Business specific error
51	Not sufficient funds
54	Expired card
55	Incorrect PIN
56	No card record
57	Transaction not permitted to cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
60	Card acceptor contact acquirer
61	Exceeds withdrawal amount limit
62	Restricted card
63	Security violation
65	Exceeds withdrawal frequency limit
68	Response received too late
6P	Verification data failed
75	Allowable number of PIN tries exceeded
76	Card already in the exception file, previous record stored
77	Closed account
78	Blocked, first used transaction from new cardholder, and card not properly unblocked
82	Negative online CAM, dCVV, iCVV, or CVV results Or Offline PIN authentication interrupted
90	Cutoff is in process
91	Issuer or switch is inoperative
93	Transaction cannot be completed-Violation of Law
94	Duplicated transmission
96	System malfunction
97	General monitoring timeout
98	Server unavailable, network re-routing requested
99	Initiator domain incident
A0	Fallback in contact mode
A1	Soft decline (electronic commerce only)
A2	PIN request in single TAP mode
A3	New TAP with required authentication
A4	Misused TRA exemption
R0	Stop payment order
R1	Revocation of all e recurring payments for the card at the merchant
R3	Revocation of all recurring payments for the card

The values used for the different services (e.g. face-to-face payment, remote payment) and the associated actions (forcing, blocking, ...) are indicated in the services.

Field 41 **Format: ans8**

Card acceptor terminal identification

Transports the content of envelope 41 provided during a parameter downloading.

Field 42 **Format: ans15**

Card acceptor identification code

Transports the content of envelope 41 provided during a parameter downloading.

Field 43 **Format: ans40**

Card acceptor name/location

Field is structured as follows:

❑ **Name, town and region**____**ans38**

The data elements are separated by a backslash ("\").
As for every fixed-length "ans" field, the "name\town\region" structure is left-justified and right-filled with spaces.

❑ **Country** ____**ans2**

This data element is specified according to the alphabetic coding conventions of ISO 3166 (France: "FR").

Example:
a) DURAND\PARIS\07............................(23 spaces) .... FR
b) if town is unknown
DUMONT\\75002.........................(25 spaces) .... FR
c) if region is unknown
MERCIER\LYON\ ....(25 spaces) .... FR

Note: When this data is part of the envelope 43 provided during a parameter downloading, the acceptor system ignore the above description and return the content of the envelope 43 without modification.

Field 44 **Format: LLVAR ans 25**

Additional response data

Field 44 has a TLV (Value Length Type) structure.

• The structure of the data elements is the following:

❑ **Data type** ____**ans2**

Type	Description
AA	Incorrect field
AB	Security error
AC	Field conversion
AF	Service activation code
BB	Telephone number
BC	Message to the transaction initiator
CA	Track or equivalent data cryptogram processing information
CB	Application cryptogram verification results
CC	Cardholder address checking information
CD	Responsibility transfer information
RA-ZZ	Reserved for private use

❑ **Data length**____**ans2**

The two characters of the length are not counted in the data length. The length is right-justified and left-filled with a zero character.

❑ **Data value**

The data has the number of characters defined by the length.
There are different possible values for the data element. The value depends on the data element type.

The possible values for field 44 are indicated in the list of data element types.

Type = AA: Incorrect field

Data format: ans4, 6, 8 Number of bytes transported: 4, 6 or 8

The variable contains:

- The number of the incorrect field (3 characters)
- If it is a TLV field, may contain the type of the incorrect sub-field (2 or 4 characters). If it is a field including several consecutive sub-fields, may contain the position of the beginning of the incorrect sub-field (2 character)
- An error code:

1		Value error
2		Format error
3		Missing mandatory field

In some cases; Type AA can provide information on incorrect fields of response codes:

- If field 39=20 (security error in the server domain) and field 39=30 (format error): Type AA identifies the incorrect field (and maybe also the sub-field),
- If field 39=12 (invalid transaction): Type AA identifies field 001 (bitmap) to indicate that the transaction is not included. Field 003 (processing code) to indicate that the associated service is not open
- If field 39=13 (invalid amount): Type AA may indicate the invalid amount in the case of a reversal (field 4 or field 95),
- If field 39=25 (unable to locate record in file): in the case of a reversal, Type AA may indicate the field (and maybe sub-fields) which are preventing the association (field absent or incorrect),

Field 44 can contain several data elements related to incorrect fields.

Type = AB: Security error

Data format: ans5 Number of bytes transported: 5

Type = AC: Field conversion

Data format: ans…21 Number of bytes transported: …21.

Type AC provides information on field values that have been converted. It enables the transport of the former field value and the conversion initiator.

The variable contains the following:

- Conversion initiator (1 character)

0	e-rsb
1	Visa gateway
2	MasterCard gateway
9	Other

- Converted field number (3 characters)
- Orifinal value of converted field (n characters)

Field 44 can contain several data elements related to field conversion.

TYPE = AF: SERVICE ACTIVATION CODE

Data format: ans1 Number of bytes transported: 1

This data element is used to indicate a call trigger sent by an acquiring system to an acceptance system:

1	No call activation
2	Activate parameter downloading
3	Activate data capture
4	RFU

TYPE = BB: TELEPHONE NUMBER

Data format: ans…21 Number of bytes transported: …21

The variable contains:

- the country dialling code (3 characters and may be preceded by spaces)
- the correspondent's telephone number (including the regional dialling code)

Type BB can be used for an issuer call process in order to indicate the telephone number.

TYPE = BC: MESSAGE TO THE TRANSACTION INITIATOR

Data format: ans…21 Number of bytes transported: …21

The variable contains a message for the transaction initiator.

❑ **Control character____ans1**

1	Print
2	Display
3	Print and display
4	Print for cardholder only
5	Display for cardholder only
6	Print and display for the cardholder only
7	Print for acceptor only
8	Display for acceptor only
9	Print and display for acceptor only
A	Print for acceptor and cardholder
B	Display for acceptor and cardholder
C	Print and display for acceptor and cardholder
F	Reserved for private use

❑ **Response message ____ans…20**

TYPE = CA: TRACK OR EQUIVALENT DATA CRYPTOGRAM PROCESSING INFORMATION

Data format: ans1 Number of bytes transported: 1

TYPE = CB: APPLICATION CRYPTOGRAM VERIFICATION RESULTS

Data format: ans1 Number of bytes transported: 1

TYPE = CC: CARDHOLDER ADDRESS CHECKING INFORMATION

Data format: ans2 Number of bytes transported: 2

- **Nomenclature ans1**

Values	Description
0	CB2A

- **Result of control ans1**

Value	Label
A	Postcode and address fully match
B	Postcode and address partially match
C	Postcode and address do not match
D	Control was not performed or was not performed for all data elements

TYPE = CD: INFORMATION RELATING TO LIABILITY SHIFT

Data format: ans1 Number of bytes transported: 1

This data element can be used by the acquirer to inform the merchant of eligibility for the transfer of responsibility. The acquirer can use this data element to inform the merchant that it is eligible for a liability shift. The procedure for this data element is related to the specific requirements of each acquirer in relation to its merchants.

Values	Description
0	Unknown
1	Shift
2	No shift

Field 47 **Format: LLVAR ans …255**

Additional data – National

Field 47 has a TLV (Type Length Value) structure.

• The structure of the data elements is the following:

❑ **Data type ans2**

Within the scope of the CB2A Authorisation protocol, the possible values for the data element type are the following:

Type	Description	Repeatability
08	Location category code	
20	Field conversion by acquirer (field 32) or forwarder (field 33)	X
24	File number	
30	Additional card reading capabilities	
31	Point of interaction information	
33	CB2A specification date	
95	Unique transaction identifier	
96	SIRET	
97	IDPA (Point of interaction identifier assigned by an acquirer)	
99	Original unique transaction identifier	
A0	IDSA (Acceptance system identifier assigned by an acquirer)	

❑ **Data length ans2**

Two-character length is not included in the length of the variable. The length is right-justified and left-filled with a zero character.

❑ **Data value**

The number of characters of the variable is determined by the length.
The possible values of the variable are determined by the data element type.

• Content of the data elements depends on the type:

TYPE = 08: LOCATION CATEGORY CODE

Data format: ans…8 Number of bytes transported: …8

This data element is related to the sales unit. It is used to specify a Point of Sale's location (see SICB).

TYPE = 20: FIELD CONVERSION BY ACQUIRER (FIELD 32) OR FORWARDER (FIELD 33)

Data format: ans… Number of bytes transported: variable

The variable contains the following:

- Number of the converted field (3 characters)
- Original value of the converted field (n characters)

If a field has several conversions, only the first one is used for field 47, type 20.

Field 47 can contain several data elements related to field conversion (information about different fields).

TYPE = 24: FILE NUMBER

Data format: anp12 Number of bytes transported: 12

Serves as a reference for a reservation or a rental invoice identified as such by the archive manager (i.e. the acquirer, or the acceptor under the acquirer's responsibility). This field is identical for all authorisation requests related to the invoice.

TYPE = 30: ADDITIONAL CARD READING CAPABILITIES

Data format: n 1 Number of bytes transported: 1

Value	Description
1	Active contactless application

TYPE = 31: POINT OF INTERACTION INFORMATION

Data format: n 1 Number of bytes transported: 1

Value	Description
1	mPOS (smartphone/tablet with a PCI PTS dongle to read the card with PIN entry on the dongle)
2	SPoC (smartphone/tablet with a PCI PTS dongle to read the card with PIN entry on the device screen)
3	CPoC (smartphone/tablet without dongle, when the card is read in contactless mode using the NFC device and there is no PIN entry)
4	MPoC (smartphone/tablet without dongle, when the card is read in contactless mode with PIN entry on the device screen)

TYPE = 33: CB2A SPECIFICATION DATE

Data format: n 4 Number of bytes transported: 4

Release date of the CB2A specification in YYMM format

TYPE = 95: UNIQUE TRANSACTION IDENTIFIER

Data format: ans…50 Number of bytes transported: …50

❑ **Nomenclature______________________________________ an1**

The nomenclature value identifies the entity responsible for this encoding; it does not specify the scheme responsible for the transaction.

Values	Description
1	CB
2	MasterCard
3	Visa
4	Discover
5-9	Reserved for future use
A-Z	Reserved for future use

❑ **Unique transaction identifier ______________________________ ans..49**

The data element contains a transaction identifier generated by the authorisation system.

Note : it is the responsibility of the acquirer to send the data in the format that is accepted by the acceptor in the acceptor to acquirer protocol.

TYPE = 96: SIRET (COMPANY REGISTRATION NUMBER)

Data format: ans14 Number of bytes transported: 14

TYPE = 97: IDPA (POINT OF INTERACTION IDENTIFIER ASSIGNED BY AN ACQUIRER)

Data format: ans8 Number of bytes transported: 8

TYPE = 99: ORIGINAL UNIQUE TRANSACTION IDENTIFIER

Data format: ans…50 Number of bytes transported: …50

This data element contains the unique identifier of the transaction used as reference for linking.

Note that the first position of the data element contains the nomenclature.

TYPE = A0: IDSA (ACCEPTANCE SYSTEM IDENTIFIER ASSIGNED BY AN ACQUIRER)

Data format: ans8 Number of bytes transported: 8

Field 48 **Format: LLVAR ansb …255**

Security Data

This field is used to transport security data in messages.

The data elements transported in this field are coded in binary.

□ **Data type** **b2**

Type	Description	Repeatability
0001	KSN	
0002	BDK (Base Derivation Key) name	
0003	BDK (Base Derivation Key) version	

□ **Data element length** **b1**

The data element length is coded in binary (one byte) and is not included in the calculation of the data element length.

□ **Data element value**

The number of characters of the variable is determined by the length.
The possible values of the variable are determined by the data element type.

TYPE = 0001: KSN (KEY SERIAL NUMBER)

Data format: b10..12 Number of bytes transported: 10..12

If a DUKPT is used to encrypt the PIN, this field will contain a 10- or 12-byte KSN (Key Serial Number).

TYPE = 0002: BDK (BASE DERIVATION KEY) NAME

Data format: b2..15 Number of bytes transported: 2..15

The BDK Name data is used to transmit the identifier of the BDK key from which the PIN encryption key is derived. This identifier is formatted as follows:

Byte 1	BDK Key Identifier Type (see values below)
Bytes 2 to 15	Identifier of the BDK key according to the type indicated by octet 1

Byte 1 (BDK Key Identifier Type) of the Identifier field may be set as follows:

Value		**Description**
Values 00 to 7F Use reserved for CB2A specification	01	Identifier Type "DUKPT 2009" The identifier of the BDK key is 5 bytes long and corresponds to the Key Set Identifier (KSI) described in standard ANS X9.24-1: 2009. The Version field is not sent.
	02	Identifier Type "DUKPT 2017" The identifier of the BDK key is 4 bytes long and corresponds to the BDK ID described in standard ANSI X9.24-3: 2017. The Version field is not sent.
	03	Only Label The identifier consists of a series of ASCII characters (up to 14 characters). The Version field is not sent.
	04	Label and version The identifier consists of a series of ASCII characters (up to 14 characters). The Version field must be transmitted and be valued according to the YYYYMMDDhh (GMT) format.

Value		**Description**
	05	Format « OGDC CB » The Identifier of the key is 14 bytes (bytes 2 to 15 of the Identifier field). Its format is described in the document “FORMATS DE DISTRIBUTION ET D'INTRODUCTION DES CLES CB » The Version field is not sent.
	Autres valeurs	RFU
Values 80 to FF Owner's use	80 to FF	The use and content of bytes 2 to 15 of the Identifier field as well as the use or not of the Version field are defined bilaterally between the manufacturer and the manager of the BDK key.

TYPE = 0003: BDK (BASE DERIVATION KEY) VERSION

Data format: n10 Number of bytes transported: 5

Field 49 Format: n3

Currency code, transaction

Specifies the currency used to express the transaction amount defined in field 4. This is the local currency code of the acquirer or the transaction's originating location.
The codes are listed in the ISO 4217 standard document.
Note
the code for the Euro is 978.

Field 52 Format: b8…16

PIN data

This data element is coded in formats "0", "3" or "4" as defined in the ISO 9564 standard.

Field 53 Format: n16

Security related control information

Field 53 contains information that is required to use the security-related data contained in the message.

❑ **Not used______________________________ quartet 1**

❑ **Verifications used by the requester ______________________________ quartet 2**

In the absence of the Online PIN, only the “Verifications used by the requester” data element is used in the field 53. The values are the following:

0	PIN not controlled by the requester
1	PIN controlled and correct
2	PIN controlled and incorrect
3	PIN controlled and incorrect, maximum number of PIN entry tries reached

❑ **Not used______________________________ quartets 3 to 5**

❑ **PIN or key encryption mode______________________________ quartet 6**

❑ **PIN encryption type**

Values	Description
0	No encryption
2	Triple DES
3	DUKPT2009
4	DUKPT2017

❑ **PIN format ______________________________ quartets 7 and 8**

Values	Description
00	No PIN
01	ISO 9564-0 format
02	ISO 9564-3 format
03	ISO 9564-4 format

❑ **Encryption algorithm ______________________________ quartets 9 and 10**

Values	Description
00	No encryption
01	3DES
02	AES128
03	AES192
04	AES256

❑ **Not used______________________________ quartets 11 to 16**

Field 54 **Format: LLLVAR an … 120**

Additional amounts

This field contains up to 6 data elements. Each data element is composed of four fixed-length parts defined below.

❑ **Account type** **n2**

Values	Description
00	Payment with no special features (debit)
30	Credit transaction

❑ **Amount type** **n2**

Values	Description
43	Cumulative total of authorised amount
44	Tip amount
57	Original amount

An amount type can be found in several data elements.

❑ **Currency code** **n3**

The codes are listed in ISO 4217. The numeric list is used in this case.

❑ **Amount** **(x+n12) an13**

The 'x' in the format describes the type of amount (D or C).

Field 55 **Format: LLLVAR b …255**

Integrated circuit card system related data

Field 55 is used to transport all the data related to the integrated circuit (eg the data necessary for the acceptance of EMV cards).

In the case of EMV:

- data are transported in binary without transcoding,
- indicated data formats are those defined in the EMV specifications.

❑ **Data type** ____________________ **b2**

Type	Description	Repeatability
	EMV specific data	
0056	Data equivalent to ISO track 1 read in contactless mode	
0057	Track 2 equivalent data	
0071	Issuer Script Template 1	X
0072	Issuer Script Template 2	X
0082	Application Interchange Profile (AIP)	
0091	Issuer Authentication Data	
0095	Terminal Verification Results (TVR)	
009A	Terminal Transaction Date	
009C	Transaction type	
5F24	Application Expiration Date	
9F02	Amount, authorised	
9F03	Amount, other	
9F06	Application identifier (AID)	
9F0A	Application Selection Registered Proprietary Data	
9F10	Issuer application data	
9F1F	Track 1 Discretionary Data	
9F26	Application Cryptogram (ARQC)	
9F27	Cryptogram Information Data	
9F33	Terminal capabilities	
9F34	Cardholder verification method (CVM) results	
9F35	Terminal Type	
9F36	Application Transaction Counter (ATC)	
9F37	Unpredictable Number	
9F66	Terminal Transaction Qualifiers (TTQ)	
9F6B	Data equivalent to ISO track 2 read in contactless mode	
9F7C	Issuer proprietary data	
FF00	Issuer script results	X

Type	Description	Repeatability
	CB-specific data	
DF68	Kernel ID used	
DF80	ICC processing results	X
DF81	Card application type	
DF85	RTT (Terminal processing results)	
DF86	Contactless device	

❑ **Data element length** ____________________ **b1**

The data element length is coded in binary (one byte) and is not included in the calculation of the data element length.

❑ **Data element value**

The number of characters of the variable is determined by the length.
The possible values of the variable are determined by the data type.

TYPE = 0056: DATA EQUIVALENT TO ISO TRACK 1 READ IN CONTACTLESS MODE

Data format: ans…76 Number of bytes transported: …76

Contains the data elements related to track 1 equivalent data (as defined in ISO 7813) and contained in a contactless integrated circuit application.
Field separators are kept. The start and end delimiters and the LRC character must not be sent.
Field 55 type 0056 contains all track 1 equivalent data, as read in contactless mode.

TYPE = 0057: TRACK 2 EQUIVALENT DATA

Data format: b…19 Number of bytes transported: …19

Contient les éléments de données équivalents à la piste ISO2 telle que définie dans ISO/IEC 7813, excluant les caractères de début et de fin ainsi que le LRC.
Contains the data elements related to the track 2 equivalent data (as defined in ISO/IEC 7813), excluding start and end characters as well as the LRC.

TYPE = 0071: ISSUER SCRIPT TEMPLATE 1

Data format: b…128 Number of bytes transported: …128

Contains issuer-specific data elements sent to the integrated circuit **before** the **second** "Generate AC" command is executed.
This data element usually contains one or more 'Issuer Script Command' data elements (tag 86), each of which is used in the dialog between the terminal and the card.
IMPORTANT: This data is repeatable. However, the total length of all the occurrences of these data elements must not exceed 128 bytes. In this specific case, the length of an occurrence is not limited only to the length of the value but to the total length of the TLV structure, i.e.
number_of_occurrences * 3 (3 bytes for the tag and the length) + ∑value_length ≤ 128.

TYPE = 0072: ISSUER SCRIPT TEMPLATE 2

Data format: b…128 Number of bytes transported: …128

Contains issuer-specific data sent to the chip **after** the **second** "Generate AC" command is executed.
This data element can contain one or more 'Issuer Script Command' data elements (tag 86), each of which is used in the dialog between the terminal and the card.

IMPORTANT: This data element is repeatable. However, the total length of all the occurrences of these data elmeents must not exceed 128 bytes. In this specific case, the length of an occurrence is not limited only to the length of the value but to the total length of the TLV structure, i.e.
number_of_occurrences * 3 (3 bytes for the tag and the length) + ∑value_length ≤ 128.

TYPE = 0082: APPLICATION INTERCHANGE PROFILE (AIP)

Data format: b2 Number of bytes transported: 2

Contains the specific functions of the integrated circuit application (information supplied by the card).

TYPE = 0091: ISSUER AUTHENTICATION DATA

Data format: b8…16 Number of bytes transported: 8…16

Data sent to the card for issuer authentication.

TYPE = 0095: TERMINAL VERIFICATION RESULTS (TVR)

Data format: b5 Number of bytes transported: 5

Results of the different controls performed by the terminal.

TYPE = 009A: TERMINAL TRANSACTION DATE (EMV TAG 9A)

Data format: n6 (YYMMDD) Number of bytes transported: 3

Indicates the terminal local date on which the authorisation transaction was performed. Used for calculating the ARQC.

TYPE = 009C: TRANSACTION TYPE

Data format: n2 Number of bytes transported: 1

Contains the transaction type used for an Application Usage Control (AUC). EMV concept which corresponds to the Service Code. The correspondence between the private values of field 3 and their equivalent to set in the "transaction type" data element (field 55 type 009C) is as follows:

Field 03 - Private value		**Corresponding value- Field 55 type 009C**	
11	Quasi-cash	00	Purchase of goods or services
17	Manual cash	01	Withdrawal
28	Quasi-cash refund	20	Credit: returns
41	Funds transfer, debit	00	Purchase of goods or services
42	Funds transfer, credit	20	Credit: returns

TYPE = 5F24: APPLICATION EXPIRATION DATE

Data format: n6 (YYMMDD) Number of bytes transported: 3

Contains the application expiration date of the EMV card.

TYPE = 9F02: AMOUNT, AUTHORISED

Data format: n12 Number of bytes transported: 6

Indicates the amount that the terminal communicates to the card.

TYPE = 9F03: AMOUNT, OTHER

Data format: n12 Number of bytes transported: 6

This type can contain the secondary amount associated with a transaction, e.g. for Cashbacks.

TYPE = 9F06: APPLICATION IDENTIFIER (AID)

Data format: b5…16 Number of bytes transported: 5…16.

Contains the identifier of the card application (see ISO 7816-5).

TYPE = 9F0A: APPLICATION SELECTION REGISTERED PROPRIETARY DATA

Data format: b4…32 Number of bytes transported: 4…32

Contains the proprietary card data assigned by EMVCo to specific markets.
This data element comes from the card and contains TLVs. Can be greater than 32 bytes.
The terminal transports the first TLVs of the card data element up to the maximum size of the field.

TYPE = 9F10: ISSUER APPLICATION DATA (IAD)

Data format: b…32 Number of bytes transported: …32

Contains the data elements that the issuer wants to return in the authorisation messages.

TYPE = 9F1F: TRACK 1 DISCRETIONARY DATA

Data format: ans ..54 Number of bytes transported..54

TYPE = 9F26: APPLICATION CRYPTOGRAM (ARQC)

Data format: b8 Number of bytes transported: 8

Certificate returned by the integrated circuit in response to a cryptogram generation instruction. This certificate is used to authenticate the card.

TYPE = 9F27: CRYPTOGRAM INFORMATION DATA

Data format: b1 Number of bytes transported: 1

Code which specifies the type of certificate returned by the integrated circuit and the action to be performed by the terminal.

TYPE = 9F33: TERMINAL CAPABILITIES

Data format: b3 Number of bytes transported: 3

Specifies the terminal capabilities in a table.

TYPE = 9F34: CARDHOLDER VERIFICATION METHOD (CVM) RESULTS

Data format: b3 Number of bytes transported: 3

Specifies the results of the last cardholder authentication method.

TYPE = 9F35: TERMINAL TYPE

Data format: n2 Number of bytes transported: 1

Code which specifies the environment of an acceptance system, its communications capabilities and its operational controls.

TYPE = 9F36: APPLICATION TRANSACTION COUNTER (ATC)

Data format: b2 Number of bytes transported: 2

Specifies the transaction number processed by the card application. The counter is incremented by the integrated circuit.

TYPE = 9F37: UNPREDICTABLE NUMBER

Data format: b4	Number of bytes transported: 4

A unique variable associated with the generation of the ARQC application cryptogram (discriminating element).

TYPE = 9F66: TERMINAL TRANSACTION QUALIFIERS (TTQ)

Data format: structure	Number of bytes transported: 4

Terminal status during the transaction.

TYPE = 9F6B: DATA EQUIVALENT TO ISO TRACK 2 READ IN CONTACTLESS MODE

Data format: b...19	Number of bytes transported: ...19

Contains the track 2 equivalent data elements (as defined in ISO 7813) that are specified in a contactless integrated circuit application.

The field separators are kept. The start and end delimiters and the LRC character must not be sent.
Field 55 type 9F6B contains complete track 2 equivalent data exactly as it was read in contactless mode.
When this data contains an odd number of significant characters, it is right filled with a quartet filled with a 'F' hex value.

TYPE = 9F7C: ISSUER PROPRIETARY DATA

Data format: b..32	Number of bytes transported: 32

Contains data to be sent to the issuer.

TYPE = DF68: KERNEL ID USED

Data format: b1	Number of bytes transported: 1

Kernel identifier used to process the transaction.

TYPE = DF80: ICC PROCESSING RESULTS

Data format: n2 Number of bytes transported: 1

This variable specifies the results of the processing performed by the acceptor on the card's integrated circuit.

	MEANING
0x values: Basic processing	
00	Integrated circuit processing completed successfully
01	ICC reader out of order or disconnected
1x values: Valid response to chip reset controls not received	
10	No response to the reset

Field 55 can contain several data elements related to the results of processing performed on the integrated circuit.

TYPE = DF81: CARD APPLICATION TYPE

Data format: n1 Number of bytes transported: 1

2	EMV
3	Contactless integrated circuit – magstripe context

TYPE = DF85: RTT (TERMINAL PROCESSING RESULTS))

Data format: b5 Number of bytes transported: 5

Contains the result of the various controls performed by the terminal for a payment in contactless chip mode.

TYPE = DF86: CONTACTLESS DEVICE

Data format: b…35 Number of bytes transported: …35

Contains the Form Factor received by the terminal from the integrated circuit.
Structure of the data element:

- 2 bytes: tag containing the form factor
- 1 byte: length
- Up to 32 bytes: value

TYPE = FF00: ISSUER SCRIPT RESULTS

Data format: b...5 Number of bytes transported: ...5

Specifies the results of the issuer script processing.

Field 56 Format: LLLVAR b …255

Additional data

- ❑ **Data type ______________ b2**

Type	Description	Repeatability
	ISO 8583 (V93) standardised data	
0001	Payment facilitator data	
0002	Application selection indicator	
0003	Brand selected	
0005	Acceptance system card product code	
0006	Cardholder address	
0008	Cardholder postcode	
0009	Delivery address	
0010	IP address	
0011	Payment facilitator data	
0012	Mobile payment solution identifier	
0013	Type of transaction	
0014	Type of proof	
0017	Cryptogram entry date and GMT time	
0018	Card type indicator	
0019	Serial number	
0020	Resend counter	
0022	3DS protocol major version	
0023	UUID Container	X
0024	Independent sales organisation	
0025	Payment facilitator identifier	
0026	Marketplace identifier	
0027	Final merchant identifier	
0028	Payment use case	
0029	Card-on-file action	
0031	Payment number	
0032	Total number of payments	
0033	Exemption indicator	
0036	Authentication merchant name	
0037	Authentication date	
0038	Authentication amount	
0040	List of installed kernels	
0045	Payment validity date	
0046	Additional electronic commerce transaction data	
0056	Payment Account Reference	
5F2D	Language preference	X
9F0D	Issuer Action Code – Default	
9F0E	Issuer Action Code – Denial	
9F0F	Issuer Action code - Online	

- ❑ **Data element length ______________ b1**

  The data length is coded in binary (one byte) and is not included in the calculation of the data element length.

- ❑ **Data element value**

  The number of characters of the variable is determined by the length.
  The possible values of the variable are determined by the data type.

TYPE = 0001: PAYMENT FACILITATOR DATA

Data format: structure Number of bytes transported: 27

- ❑ **Payment Facilitator ID** ____ **n11**
- ❑ **Independent Sales Organisation ID** ____ **n11**
- ❑ **Sub-Merchant ID** ____ **ans15**

TYPE = 0002: APPLICATION SELECTION INDICATOR

Data format: n2 Number of bytes transported: 1

Data element used to specify whether the card application selection corresponds to the acquirer default selection or cardholder selection.

Value	Meaning
0	Selection by default
1	Cardholder selection

TYPE = 0003: BRAND SELECTED

Data format: b1 Number of bytes transported: 1

Indicates the brand selected by the cardholder.

Values	Description
00	CB
01	VISA
02	Vpay
03	Electron
04	MasterCard
05	Maestro
06	JCB
07	Discover
08	UPI
09	Amex
80-99	Reserved for private use

TYPE = 0005: ACCEPTANCE SYSTEM CARD PRODUCT CODE

Data format: an3 Number of bytes transported: 3

Card product identifier provided by the acceptance system.

TYPE = 0006: CARDHOLDER ADDRESS

Data format: ansp..40 Number of bytes transported: ..40

Cardholder address.

TYPE = 0008: CARDHOLDER POSTCODE

Data format: ansp..10 Number of bytes transported: ..10

Cardholder postcode.

TYPE = 0009: DELIVERY ADDRESS

Data format: ans80 Number of bytes transported: 80

Delivery address for the order.
The address has the following fields: number and street name, postcode and country. The fields are separated by asterisks.

TYPE = 0010: IP ADDRESS

Data format: ans4…45 Number of bytes transported: 4…45

Cardholder IP address.

The two address formats are the following:

- IPv4 is represented in decimal notation with four numbers between 0 and 255, separated by points. For example, 5.10.255.1
- IPv6 is represented by eight groups of four hexadecimal digits, each group representing 16 bits (two bytes). The groups are separated by colons (:).
  For example, IPv6: 2019: 0d8e: 113a: 1111: 0101: 8a2e: 0370: 7334

TYPE = 0011: NUMBER OF ARTICLES

Data format: n2 Number of bytes transported: 1

Number of articles in the cart.

TYPE = 0012: MOBILE PAYMENT SOLUTION IDENTIFIER

Data format: n3 Number of bytes transported: 2

Mobile payment solution identifier

❑ **Nomenclature** ________________________________ **n1**

Values	**Description**
0	CB
1-9	RFU

❑ **Identifier** ________________________________ **n2**

Values	**Description**
00	Apple Pay
01	Samsung Pay
02	Android Pay

Any other value can be used within the scope of agreements between users.

TYPE = 0013: TYPE OF TRANSACTION

Data format: n2 Number of bytes transported: 1

Type of transaction processed.

Values	Description
00	In-app payment
01	Browser-based payment

TYPE = 0014 : TYPE OF PROOF

Data format: n2 Number of bytes transported: 1

Type of proof generated by the payment solution.

Values	Description
00	EMV
01	Secured electronic commerce

TYPE = 0017: CRYPTOGRAM ENTRY DATE AND GMT TIME

Data format: n12(YYMMDDhhmmss) Number of bytes transported: 6

GMT date and GMT for card security code entry.

TYPE = 0018: CARD TYPE INDICATOR

Data format: n1 Number of bytes transported: 1

TYPE = 0019: SERIAL NUMBER

Data format: ans..35 Number of bytes transported: .35

Serial number of the acceptance system or point of acceptance.

TYPE = 0020: RESEND COUNTER

Data format: n1 Number of bytes transported: 1

Counter used for re-authorised messages.

TYPE = 0022: 3DS PROTOCOL MAJOR VERSION

Data format: an1 Number of bytes transported: 1

Values	Description
1	Version 3DS v1
2	Version 3DS v2

TYPE = 0023: UUID CONTAINER

Data format: ans37 Number of bytes transported: 37

- **Nomenclature________________________________ ans1**

Values	Description
1	DS Transaction ID
2	ACS Transaction ID
9	RFU
A-Z	RFU

- **UUID ________________________________ ans36**

TYPE = 0024: INDEPENDENT SALES ORGANIZATION

Data format: ans15 Number of bytes transported: 15

TYPE = 0025: PAYMENT FACILITATOR IDENTIFIER

Data format: ans15 Number of bytes transported: 15

TYPE = 0026: MARKETPLACE IDENTIFIER

Data format: ans15 Number of bytes transported: 15

TYPE = 0027: FINAL MERCHANT IDENTIFIER

Data format: ans15 Number of bytes transported: 15

TYPE = 0028: PAYMENT USE CASE

Data format: n2 Number of bytes transported: 1

Identification of remote payment use cases.

Values	Description
01	Single payment
02	Recurring subscription - Fixed amount and limited duration subscription
03	Instalment payment
04	Shipment payment
05	Recurring subscription - Other subscription
06	Reservation and rental payment
07	Pre-autorisation out of reservation and rental context
08-99	RFU

TYPE = 0029: CARD-ON-FILE ACTION

Data format: an1 Number of bytes transported: 1

Values	Description
1	Add card
2	Keep card

TYPE = 0031: PAYMENT NUMBER

Data format: n2 Number of bytes transported: 1

Payment number in progress.

TYPE = 0032: TOTAL NUMBER OF PAYMENTS

Data format: n2 Number of bytes transported: 1

Total number of payments planned.

TYPE = 0033: EXEMPTION INDICATOR

Data format: b2..3 Number of bytes transported: 2..3

Indicates the exemption cases(s) for the transaction related to strong cardholder authentication..

❑ **Byte 1** **b1**

Bit	Description
8	Issuer transaction risk analysis
7	Recurring operations with identical amounts and a specified duration
6	Delegated authentication
5	Authentication implementation is not technically possible
4	Low amount
3	Acceptor/acquirer transaction risk analysis
2	Trusted beneficiary
1	Secure corporate paymentprocess and protocol

❑ **Byte 2** **b1**

Bit	Description
5-8	RFU
4	Unattended terminal for transport fare and parking fee
3	Out of RTS SCA scope
2	Other cases
1	Specific scheme program exemption

❑ **RFU** **b1**

TYPE = 0036: AUTHENTICATION MERCHANT NAME

Data format: ans40 Number of bytes transported: 40

Name of the merchant presented for authentication.

TYPE = 0037: AUTHENTICATION DATE

Data format: n14(YYYYMMDDHHMMSS) Number of bytes transported: 7

Date and time of authentication.

TYPE = 0038: AUTHENTICATION AMOUNT

Data format: n12 Number of bytes transported: 6

Amount of authentication.

TYPE = 0040: LIST OF INSTALLED KERNELS

Data format: b1..8 Number of bytes transported: 1..8

The description of this list is provided here for information only. The reference description can be found in the functional documents.

- ❑ **Byte 1** **b1**

Value	Description
Bit 8	RFU
Bit 7	C7
Bit 6	C6
Bit 5	C5
Bit 4	C4
Bit 3	C3
Bit 2	C2
Bit 1	RFU

- ❑ **Byte 2** **b1**

Value	Description
Bit 8	RFU
Bit 7	RFU
Bit 6	RFU
Bit 5	RFU
Bit 4	RFU
Bit 3	C-PACE
Bit 2	WISE
Bit 1	PURE

- ❑ **Bytes 3 to 8** **b6**

Reserved for CN use.

TYPE = 0045: PAYMENT VALIDITY DATE

n6(YYMMDD) Number of bytes transported: 3

Validity date for a multiple payment.

TYPE = 0046: ADDITIONAL DATA – INITIAL TRANSACTION ELECTRONIC COMMERCE

Data format: structure Number of bytes transported: 126

Electronic commerce data for the initial transaction of a multiple payment. These data elements may be requested in transactions subsequent to the initial transaction.

- ❑ 3DS protocol major version ______ n2
- ❑ ACS transaction ID ______ ans36
- ❑ DS transaction ID ______ ans36
- ❑ Authentication merchant name ______ ans40
- ❑ Authentication date ______ n14
- ❑ Authentication amount ______ n12

TYPE = 0056: PAYMENT ACCOUNT REFERENCE

Data format: ans29 Number of bytes transported: 29

Payment Account Reference linked to the underlying PAN.

TYPE = 5F2D: LANGUAGE PREFERENCE

Data format: an2 Number of bytes transported: 2

Indicates a list of 1 to 4 language(s) order by preference.

TYPE = 9F0D: ISSUER ACTION CODE - DEFAULT

Data format: b5 Number of bytes transported: 5

Indicates the issuer default preference to reject a transaction that should have been online improved but that the terminal can not handle online.

TYPE = 9F0E: ISSUER ACTION CODE - DENIAL

Data format: b5 Number of bytes transported: 5

Indicates the issuer conditions to reject a transaction without trying an online connexion.

TYPE = 9F0F: ISSUER ACTION CODE - ONLINE

Data format: b5 Number of bytes transported: 5

Indicates the issuer conditions to accept a transaction online.

Field 58 **Format: LLLVAR ans …255**

Responding machine identifier

Field 58 is used in a response when an authorisation has been sent by the issuer or its representative and in network management messages.

Field 59 **Format: LLLVAR b …255**

National data

❑ **Data type ______ b2**

Type	Description	Repeatability
	ISO 8583 (V93) standardised data	
0100	Function code	
0101	Message reason code	X
0102	Transaction year	

Type	Description	Repeatability
	CB-specific data	
0200	Transaction regulatory and technical environment (ERT)	
0201	ITP SA (Acceptance system terminal application identifier)	
0202	Acceptor contract number	
0203	Acceptance system logical number	
0204	Point of interaction logical number	
0205	Acceptance system country code	
0207	Cardholder total amount	
020B	TASA (Card acceptor application type)	
0215	ITP PA (Point of interaction terminal application identifier)	
0216	Point of interaction extended logical number	

Type	Description	Repeatability
	Security data	
0300	Card security code	
0301	Card security code verification results	

Type	Description	Repeatability
	Electronic commerce data	
0400	Transaction identifier or cryptogram supplied by the acceptor	
0401	Cardholder authentication value	
0407	Electronic commerce transaction authentication type	
0409	Cardholder authentication valueprocessing information	
0410	Cardholder authentication method	
0411	Cardholder authentication value calculation method	
0412	Three-domain secure results	
0413	Modified electronic commerce authentication type	
0414	Additional electronic commerce data elements	
0415	Digital wallet name	
0416	Electronic commerce indicator	
0417	Digital wallet additional data	
0418	Wallet identifier	
0419	Three-domain secure results, others	
0420	Electronic commerce data elements, initial transaction	

Type	Description	Repeatability
	Data relating to payment for the reservation and rental of goods or services	
0800	Service attribute	

Type	Description	Repeatability
	Other	
0802	Risk scoring service	
0805	Optional services supported (acceptor)	

- ❑ **Data element length** ______________________________ **b1**

  The data element length is coded in binary (one byte) and is not included in the calculation of the data element length.

- ❑ **Data element value**

  The number of characters of the variable is determined by the length.
  The possible values of the variable are determined by the data type.

ISO 8583 (V93) STANDARD DATA

TYPE = 0100: FUNCTION CODE

Data format: n3 Number of bytes transported: 2

The function code specifies the purpose of a message within its message class.

Values 100 to 199 are used in authorization request messages:

100	Original authorisation – accurate amount
101	Original authorisation – estimated amount
102	Reauthorisation – accurate amount
103	Reauthorisation – estimated amount
104	Resubmission – accurate amount
105	Resubmission – estimated amount
106	Incremental authorisation – accurate amount
107	Incremental authorisation – estimated amount
108	Card Validity Check
163	Additional charges
164	No-show
165	Late operation
180-199	Reserved for private use

In the case of a "standard" authorisation request, the function code used is 100 (original authorisation – accurate amount).

TYPE = 0101: MESSAGE REASON CODE

Data format: n4 Number of bytes transported: 2

The message reason code provides the receiver with an authorisation or reversal request message, and the reason or the purpose of the message.

The following values comply with ISO 8583 V93 in relation to message reason code values.

Any other value compliant with the standard can be used within the scope of agreements between users.

Value	Description
Values 1500 to 1999 specify the reason why a request message (0100) was sent instead of an advice (0120).	
1503	Terminal random selection
1506	On line forced by card acceptor
1507	On line forced by card acceptance device to be updating
1508	On line forced by terminal
1509	On line forced by card issuer (service code)
1510	Over floor limit
1511	Merchant suspicious
1512	BIN not allowed
1513	Card not allowed
1651	Cumulative/cardholder/application
1652	BIN monitored
1653	Unknown BIN
1654	PAN monitored
1655	Pre-authorisation request
1656	Forced by issuer (flow control)
1657	Foreign currency
1658	Unknown transaction currency code
1659	Card refused
1660	Call following an ARQC issued by the card
1663	Bin refused
1664	Strictly online
1665	Offline with online capability
1671	Contactless chip transaction using magstripe data
1672	Card in SDA mode
1679	Provision for cumulative amounts
1680	Authorisation following issuer PIN request
1681	Suspected relay attack
1682	Relay attack detection processing
1683	Zero Amount Debt Recovery Transaction
1776-1999	Reserved for private use

Value	Description
	Values 4000 to 4499 indicate the reason why a reversal message (0400) was sent
4000	Customer cancellation
4007	Card acceptor device unable to complete transaction
4200	Cardholder decision
4201	Terminal decision
4202	Card decision
4203	Cardholder or terminal decision
4204	Acceptor decision
4351-4499	Reserved for private use

TYPE = 0102: TRANSACTION YEAR

Data format: n2 Number of bytes transported: 1

Year transaction was processed. This data element is returned as a complement to field 13.

CB SPECIFIC DATA

TYPE = 0200: ERT (REGULATORY AND TECHNICAL ENVIRONMENT)

Data format: b1 Number of bytes transported: 1

The following table shows all values that can be used in this type. Any values not listed may be considered as RFU (Reserved for future use):

Value	Description
- Face-to-face payment:	
10	Face to face payment
- Remote payment:	
20	Remote payment, manual entry via terminal
21	Remote payment, Telephone
22	Remote payment, Mail order
24	Internet, Cardholder Initiated Transaction
25	Remote payment, Television
27	Internet, subsequent transaction
28	Recurring payment via another form of order
- Telepayment	
30	Telepayment
- Unattended payment:	
41	Payment via a Category 1 unattended vending machine – Level 1: ADM
42	Payment via a Category 2.1 unattended vending machine – Level 1: ADM
43	Payment via an unattended terminal with differed payment
44	Reserved for future use
45	Payment via a Category 1 unattended vending machine – Level 2: SST
46	Payment via a Category 2.1 unattended vending machine – Level 2: SST
47	Payment via a Category 2.2 unattended vending machine – Level 2: SST
48	Payment via an unattended machine for specific activities (highways, car parks,etc)
49	Payment via a Category 1 unattended vending machine – Level 3: LAT
50	Payment via a Category 2.1 unattended vending machine – Level 3: LAT
51	Payment via a Category 2.2 unattended vending machine – Level 3: LAT
52	Reserved for future use
53	Reserved for future use
54	Payment via a Category 1 multi-service self-service banking terminal (ADM)
55	Payment via a Category 2.1 multi-service self-service banking terminal (ADM)
56	Payment via a Category 2.2 multi-service self-service banking terminal (ADM)
57	Payment via rental unattended vending machine l
58	Transport access network
59	Reserved for future use
- Quasi-cash payment	
60	Quasi-cash (corresponds to the standard case)
63	Quasi-cash, Television
64	Quasi-cash, Internet
65	Quasi-cash, Unattended vending machine
- Gateway-specific values	
75	Counter withdrawal
- Pre-authorisation:	
80	Pre-authorisation
- Private values:	
90-99	
- Funds transfer:	
B0	Funds transfer via mail or telephone
B1	Funds transfer via internet
B2	Face-to-face funds transfer
B3	Funds transfer via an unattended terminal

REFERENCE INFORMATION :

CB NATIONAL CLASSIFICATION OF UNATTENDED TERMINALS	
Category 1 unattended terminal	Transaction amount is known before the good or service is provided.
Category 2 – 1 unattended terminal	Transaction amount is not known until the completion of the transaction. Amount can generally be estimated either by the user or by the unattended terminal based on the user request.
Category 2 – 2 unattended terminal	Transaction amount is not known until the completion of the transaction. Amount cannot be estimated in advance.
INTERNATIONAL CLASSIFICATION	
Level 1 unattended unattended terminal	ADM: Zero floor limit authorisation and PIN control
Level 2 unattended terminal	SST: Zero floor limit authorisation but no PIN control
Level 3 unattended terminal	LAT: No authorisation request and no PIN control
Level 4 unattended terminal	In-flight commerce (not allowed for intra-regional transactions)

TYPE = 0201: ITP SA (ACCEPTANCE SYSTEM TERMINAL APPLICATION IDENTIFIER)

Data format: n12 Number of bytes transported: 6

Acceptance system terminal application identifier.

Manufacturer code	n3
Reference specifications version	n3
Terminal model reference	n3
iInterbank application software version	n3

TYPE = 0202: ACCEPTOR CONTRACT NUMBER

Data format: n7 Number of bytes transported: 4

TYPE = 0203: ACCEPTANCE SYSTEM LOGICAL NUMBER

Data format: n3 Number of bytes transported: 2

TYPE = 0204: POINT OF INTERCATION LOGICAL NUMBER

Data format: n3 Number of bytes transported: 2

TYPE = 0205: ACCEPTANCE SYSTEM COUNTRY CODE

Data format: n3 Number of bytes transported: 2

Country code of the card acceptor. Coding must comply ISO 3166 in which the code is represented by three numeric characters.

TYPE = 0207: CARDHOLDER TOTAL AMOUNT

Data format: n12 Number of bytes transported: 6

Cardholder information which contains the following for a given application: cumulative amount of all completed debit transactions, including transactions in progress (total amount expressed in the transaction currency or its counter-value). The amount is expressed in the currency of the transaction amount in progress.

TYPE = 020B: TASA (CARD ACCEPTOR APPLICATION TYPE)

Data format: b5…16 Number of bytes transported: 5…16

Identifies the card acceptor application that originated the message. Its structure is based on the AID in ISO 7816-5.
It includes the following:

❑ **Application supplier identifier** ____________________ **b5**

Values: any value compliant with ISO 7816-5.

❑ **Application type identifier** ____________________ **b…11**

Values: any value compliant with ISO 7816-5.

In the CB environment, the length of this field is 7.

For CB, the chosen values are:

- Application supplier registered identifier: **A000000042**
- Application type identifier: the values are limited to b2, and shown below:

Byte 1	
00	Not specified (2)
20	EMV/track 2 (1)
21	Wallets
40-80	Private values

Byte 2			
10	Face-to-face payment		
20	Remote payment	Manual entry via terminal	
21		Telephone	
22		Mail order	
24		Internet	
25		Television	
30	Telepayment	Not specified	
33		Television	
41	Payment via unattended terminal	Category 1	Level 1 ADM
42		Category 2.1	Level 1: ADM
43		Payment via an unattended terminal with mandatory cardholder authentication	
44		Reserved for future use	
45		Category 1	Level 2: SST
46		Category 2.1	Level 2: SST
47		Category 2.2	Level 2: SST
48		Payment via an unattended machine for specific markets (highways, parking,etc)	
49		Category 1	Level 3: LAT
50		Category 2.1	Level 3: LAT
51		Category 2.2	Level 3: LAT
52		Reserved for future use	
53		Reserved for future use	
54	Payment via multi-service banking ATM		
57	Payment via rental unattended vending machine		

Byte 2		
58	Transport access network	
60	Quasi-cash	Quasi-cash (standard case)
63		Quasi-cash Television
64		Quasi-cash, Internet
65		Quasi-cash unattended terminal vending machine
75	Withdrawal	Counter withdrawal
80	Pre-authorisation/Rental	
85-89		
90-99	Private values	
B0	Funds transfer	Funds transfer via mail or telephone
B1		Funds transfer via internet
B2		Face-to-face funds transfer
B3		Funds transfer via unattended terminal
B4-F9	RFU	

(1) For payments related to the reservation and rental of goods or services, value 20 is used when the application allows chip and magstripe data capture. May also be used for manual entry of cardholder data.

(2) For payments related to the reservation and rental of goods or services, value 00 is used when the application only allows manual entry of cardholder data.

TASA/ERT correspondence table

Card acceptor application type (TASA)		**Regulatory and Technical Environment (ERT)**	
Face-to-face payment			
10	Face-to-face payment	10	Face-to-face payment
Remote payment			
20	Remote payment: Manual entry via terminal	20	Remote payment, Manual entry via terminal
20	Remote payment: Manual entry via terminal	28	Recurring payment via another type of order
21	Remote payment: Telephone	21	Remote payment: Telephone
22	Remote payment: Mail order	22	Remote payment: Mail order
24	Remote payment: Internet	24	Internet, Cardholder Initiated Transacion
24	Remote payment: Internet	27	Internet, Subsequent Transaction
25	Remote payment: Television	25	Remote payment: Television
Telepayment			
30	Telepayment: not specified	30	Telepayment: not specified
33	Telepayment: television	33	Telepayment: television
Payment by unattended terminal			
41	Payment via a Category 1 unattended terminal - Level 1: ADM	41	Payment via a Category 1 unattended terminal - Level 1: ADM
42	Payment via a Category 2.1 unattended terminal – Level 1: ADM	42	Payment via a Category 2.1 unattended terminal – Level 1: ADM
43	Payment via an unattended terminal with differed payment	43	Payment via an unattended terminal with differed payment
45	Payment via a Category 2 unattended terminal – Level 1: SST	45	Payment via a Category 2 unattended terminal – Level 1: SST
46	Payment via a Category 2.1 unattended terminal – Level 2: SST	46	Payment via a Category 2.1 unattended terminal – Level 2: SST
47	Payment via a Category 2.2 unattended terminal – Level 2: SST	47	Payment via a Category 2.2 unattended terminal – Level 2: SST
48	Payment via an unattended machine for specific activities (highways, car parks, etc)	48	Payment via an unattended machine for specific activities (highways, car parks, etc)
49	Payment via a Category 1 unattended terminal	49	Payment via a Category 1 unattended terminal
50	Payment via a Category 2.1 unattended terminal – Level 3: LAT	50	Payment via a Category 2.1 unattended terminal – Level 3: LAT
51	Payment via a Category 2.2 unattended terminal – Level 3: LAT	51	Payment via a Category 2.2 unattended terminal – Level 3: LAT
54	Payment via a Category 1 multi-service banking ATM – Level 1: ADM	54	Payment via a Category 1 multi-service banking ATM – Level 1: ADM
54	Payment via a Category 1 multi-service banking ATM – Level 1: ADM	55	Payment via a Category 2.1 multi-service banking ATM – Level 1: ADM
54	Payment via a Category 1 multi-service banking ATM – Level 1: ADM	56	Payment via a Category 2.2 multi-service banking ATM – Level 1: ADM
57	Payment via rental unattended vending machine	57	Payment via rental unattended vending machine

Card acceptor application type (TASA)		Regulatory and Technical Environment (ERT)	
58	Transport access network	58	Transport access network
Quasi-cash			
60	Quasi-cash (standard case)	60	Quasi-cash (standard case)
63	Quasi-cash Television	63	Quasi-cash Television
64	Quasi-cash, Internet	64	Quasi-cash, Internet
65	Quasi-cash unattended terminal vending machine	65	Quasi-cash unattended terminal vending machine
Counter withdrawal			
75	Counter withdrawal	75	Counter withdrawal
Pre-authorisation			
80	Pre-authorisation	80	Pre-authorisation
Funds transfer			
B0	Funds transfer via mail or telephone	B0	Funds transfer via mail or telephone
B1	Funds transfer via internet	B1	Funds transfer via internet
B2	Face-to-face funds transfer	B2	Face-to-face funds transfer
B3	Funds transfer via unattended terminal	B3	Funds transfer via unattended terminal

TYPE = 0215: ITP PA (POINT OF INTERACTION TERMINAL APPLICATION IDENTIFIER)

Data format: n12 Number of bytes transported: 6

Point of acceptance terminal application identifier.

Manufacturer code	n3
Reference specifications version	n3
Terminal model reference	n3
iInterbank application software version	n3

TYPE = 0216: POINT OF INTERACTION EXTENDED LOGICAL NUMBER

Data format: an3 Number of bytes transported: 3

DATA RELATED SECURITY ASPECTS

TYPE = 0300: CARD SECURITY CODE

Data format: Structure Number of bytes transported: 1, 3 or 4

❑ **Information on card security code presence** ______ **n2**

00	Card security code (3 characters) not sent by the merchant
01	Card security code (3 characters) present
02	Card security code (3 characters) present on cardholder's card, but illegible (therefore not sent)
09	3 characters : cardholder informed merchant that no card security code is printed on card
10	Card security code (4 characters) not sent by the merchant
11	Card security code (4 characters) present
12	Card security code (4 characters) present on cardholder's card, but illegible (therefore not sent)
19	4 characters : cardholder informed merchant that no card security code is printed on card

❑ **Card security code value** ______ **n3…4**

Present only if the data element 'Information on presence of card security code ' is set to 01 or 11 (i.e. card security code is present).
The card security code is 3 characters long for CB cards and 4 for American Express cards.

❑ **Information on card security code verification** ______ **n1**

0	Card security code verification response code requested
1	Card security code verification response code requested and card security code verification results requested

TYPE = 0301: CARD SECURITY CODE VERFICATION RESULTS

Data format: Structure Number of bytes transported: 2

DATA RELATED TO ELECTRONIC COMMERCE

TYPE = 0400: TRANSACTION IDENTIFIER OR CRYPTOGRAM SUPPLIED BY THE ACCEPTOR

Data format: b4…40 Number of bytes transported: 4…40

Contains an unique reference for a secured electronic commerce transaction (This identifier is used in certain electronic commerce cryptogram calculation methods) or a cryptogram generated by the acceptance solution.

TYPE = 0401: CARDHOLDER AUTHENTICATION VALUE

Data format: b20..40 Number of bytes transported: 20..40

Contains the data elements related to the result of a secured electronic commerce or wallet transaction authentication.

TYPE = 0407: ELECTRONIC COMMERCE AUTHENTICATION TYPE

Data format: n2 Number of bytes transported: 1

Value	Description
09	No authentication cryptogram
20	Authentication cryptogram issued from a server
21	Authentication cryptogram issued from a Xpay or token cryptogram with authentication delegated to device

TYPE = 0409: CARDHOLDER AUTHENTICATION VALUE PROCESSING INFORMATION

Data format: anp1 Number of bytes transported: 1

TYPE = 0410: CARDHOLDER AUTHENTICATION METHOD

Data format: ans2 Number of bytes transported: 2

Contains the cardholder authentication method.

For CB transactions performed with a third-party Wallet, the data element contains the authentication method when the Wallet provides it for the transaction.

TYPE = 0411: CARDHOLDER AUTHENTICATION VALUE CALCULATION METHOD

Data format: an1 Number of bytes transported: 1

Contains the calculation method used by the issuer to make the electronic commerce cryptogram.

- For 3DS V1: Its value is identical to the 3D-Secure PARes message <TX><cavvAlgorithm> XML tag.
- For CB EMVCo 3DS: Its value is identical to the CB-AVALGO extension for Ares and RReq messages.
- W: Cryptogram generated by a wallet solution

TYPE = 0412: THREE-DOMAIN SECURE RESULTS

Data format: Structure Number of bytes transported: 4

Describes the result of exchanges using a secured remote payment architecture.

- **Nomenclature** **n1**

Value 0

- **Cardholder authentication** **an1**

For 3DS transactions, corresponds to the "Transaction Status" data element in the EMVCo 3DS specifications so this list below is likely to change according to EMVCo. **Therefore, any relevant value defined by EMV 3DS shall not be rejected by the recipient.**
Value E may be used for third party Wallet.

Values	Description
A	Proof of transit via ACS
E	Successful authentication, without cryptogram
I	Informational only
N	Unsuccessful authentication
U	Call made to ACS
Y	Successful authentication, with cryptogram
Blank	Timeout on ACS or no call to ACS

- **Registration control** **b2**

Bitmap of events related to cardholder registration (VERes and CRRes messages). This data element is only significant only with 3D Secure v1 in the CB nomenclature.

Values	Description
Bit 16-11	Reserved for CB use
Bit 10	Card absent from directory service cache (CRRes)
Bit 9	Card absent from MasterCard cache (CRRes)
Bit 8	Card absent from Visa cache (CRRes)
Bit 7	Card registered (VERes – 'Y' type)
Bit 6	Timeout or VERes - type 'U" when calling ACS
Bit 5	Timeout or VERes - type 'U' when calling Visa Directory Server
Bit 4	Timeout or VERes - type "U" when calling MasterCard Directory Server
Bit 3	Card not registered in ACS (VERes –type 'N')
Bit 2	Card not registered in MasterCard (VERes –type 'N')
Bit 1	Card not registered in Visa (VERes –type 'N')

TYPE = 0413: MODIFIED ELECTRONIC COMMERCE AUTHENTICATION TYPE

Data format: b1 Number of bytes transported: 1

Informs the acceptor and/or the CB acquirer that the security mode iniltially planned for the transaction has been changed.

Values	Description
09	No authentication cryptogrm
20	Authentication cryptogram issued from a server
21	Authentication cryptogram issued from a Xpay or token cryptogram with authentication delegated to device

TYPE = 0414: ADDITIONAL ELECTRONIC COMMERCE DATA ELEMENTS

Data format: Structure Number of bytes transported: 3..40

❑ **Nomenclature ____ an1**

Values	Description
3	CB

❑ **Type of additional data ____ an2**

Values	Description
In the CB nomenclature	
01	MasterPass
02	Paylib

❑ **Value of additional data ____ ans..37**

If "Nomenclature" = "3" and "Type of additional data" = "01", the format is as follows:

❑ **Wallet Program Data an3**

Value	Wallet identifier
101	MasterPass remote
102	MasterPass remote NFC Payment

If "Nomenclature" = "3" and "Type of additional data" = "02", the format is as follows:

❑ **Additional Authentication Method ____ an2**

Value that specifies the method used by Paylib to authenticate the transaction.

Values	Authentication method used
00	No authentication
01	Repeatable password (e.g. date of birth, password, postal code)
02	OTP via telephone (e.g. SMS, SVI, token)
03	OTP via secured software element (e.g. SEA)
04	OTP via secured hardware element (e.g. CAP, SIM)

❑ **Additional Authentication Reason Code ____ an2**

Reason for authentication request

Initial use	Risk management engine unavailable	Risk management engine requests additional strong authentication	No additional authentication requested	Value of field 'Additional Authentication Reason Code'
√			√	01
√		√		02
√	√			03
			√	11
		√		12
	√			13

TYPE = 0415: DIGITAL WALLET NAME

Data format: an2 Number of bytes transported: 2

The following table shows all values that can be used

Values	Description
03	MasterPass
04	Paylib

TYPE = 0416: ELECTRONIC COMMERCE INDICATOR

Data format: an2 Number of bytes transported: 2

Electronic Commerce Indicator based on secured architecture

TYPE = 0417: DIGITAL WALLET ADDITIONAL DATA

Data format: an12..24 Number of bytes transported: 12..24

The content of this data element is described in the functional specifications of the wallet.

- ❑ **Clearing transaction data ________ an12**
- ❑ **Additional data________ an..12**

TYPE = 0418: WALLET IDENTIFIER

Data format: n6 Number of bytes transported: 3

Identifier related to wallet approval.
The content of this data element is described in the functional specifications of the digital wallet.

- ❑ **Network ________ n2**
- ❑ **Technology ________ n2**
- ❑ **Brand ________ n2**

TYPE = 0419: THREE-DOMAIN SECURE RESULTS, OTHERS

Data format: Structure Number of bytes transported: 10

❑ **3DS authentication type** ________________ **an2**

Values	Description
CH	Challenge
FR	Frictionless
FD	Frictionless in stand-in mode

❑ **Merchant request for authentication** ________________ **n2**

For 3DS transactions, corresponds to the "3DS Requestor Challenge Indicator" data element in the EMVCo 3DS specifications so this list below is likely to change according to EMVCo. **Therefore, any relevant value defined by EMV 3DS shall not be rejected by the recipient.**

Values	Description
01	No preference – default value if the data element is absent or not set to a value
02	No authentication
03	Authentication requested
04	Authentication required
05	No authentication: transaction risk analysis already performed
06	No authentication: data share only
07	No authentication: SCA already performed
08	No authentication: whitelist
09	Authentication required

❑ **Transaction status reason** ________________ **n2**

Corresponds to the "Transaction Status Reason" data element in the EMVCo 3DS v2 specification. Provided in ARes or RReq messages.

Default value of "00" if the data element is absent or not set to a value.

❑ **Transaction cancellation indicator**________________ **n2**

Corresponds to the "Challenge Cancellation Indicator" data element in the EMVCo 3DS v2 specification. Provided in RReq messages.

Default value of "00" if the data element is absent or not set to a value.

❑ **CB 3DS score**________________ **anp2**

Corresponds to the "CB-SCORE" data element defined by CB as an extension to the ARes message in the EMVCo 3DS v2 protocol.

Padding characters (spaces) used by default if the data element is absent or not set to a value.

❑ **Reserved for future use** ________________ **an3**

TYPE = 0420: ELECTRONIC COMMERCE DATA, INITIAL TRANSACTION

Data format: structure Number of bytes transported: 22..58

Electronic commerce data from the initial transaction of a multiple payment. This data may be requested in the transactions subsequent to this initial transaction

- ❑ **Electronic commerce transaction authentication type ____ n2**
- ❑ **Cardholder authentication method ____ans2**
- ❑ **Carholder authentication value calculation method ____an1**
- ❑ **Result of using a secured remote payment architecture ____ ansb4**
- ❑ **Extension of result of using a secured payment architecture ____ ansb10**
- ❑ **Cardholder authentication value ____b4..40**
  When absent, data is filled with four bytes of zero.

DATA RELATED TO PAYMENT FOR THE RESERVATION AND RENTAL OF GOODS OR SERVICES

TYPE = 0800: SERVICE ATTRIBUTE

Data format: n2 Number of bytes transported: 1

Values	Description
1	No-show
2	Pre-authorisation
3	Additional pre-authorisation
5	Aggregation
6	Multiple payment, first payment
7	Multiple payment, other payment
11	Debt recovery

OTHER

TYPE = 0802: RISK SCORING SERVICE

Data format: structure Number of bytes transported: 1..24

❑ **Service identifier** **b1**

Values	Description
09	Risk scoring for the acquirer
90 to 99	Private risk scoring

❑ **Service data** **b..23**

Format for the data element related to the e-rsb risk scoring service (Service identifier = 09 and 0A):

❑ Notation service value **b1**

Values	Description
00-FF	e-rsb service reference

❑ Notation value **b2**

Values	Description
0000-FFFF	Note or score

❑ Notation reference value **b2**

Values	Description
0000-FFFF	Notation system reference

❑ Score reason value **b2**

Values	Description
0000-FFFF	Notation source or score reason

❑ **Action proposal** **b2**

Values	Description
0000-FFFF	Action proposal

❑ **Additional service data** **b12**

Values	Description
	Future uses

TYPE = 0805: OPTIONAL SERVICES SUPPORTED (ACCEPTOR DOMAIN)

Data format: b2 Number of bytes transported: 2

Bitmap describing the services supported by the acceptor. Several combinations of bits are possible. A bit is set if the service is supported.

Value	Description
Bits 16-5	Reserved for future use
Bit 4	Single TAP
Bit 3	Reversal
Bit 2	Reserved for future use
Bit 1	Partial authorisation

Field 70 Format: n3

Network management information code

In a 0800 message (network management message), the possible values of field 70 are:

Value	Description
001	Dialog opening (sign-on)
002	Dialog closure (sign-off)
301	Echo test

Field 90 Format: n42

Original data elements

Used with reversal requests to identify the original transaction (cancel or change authorisation).
All field elements must be set.

□ **Message identifier____________________ quartets 1 to 4**

Value	Description
0100	The reversal is related to an authorisation request message

□ **System trace audit number ____________________ quartets 5 to 10**

Value: field 11 of the original authorisation request.

□ **Authorisation transmission date and time ____________________ quartets 11 to 20**

Value: field 7 of the original authorisation request.

□ **Authorisation acquiring institution identifier ____________________ quartets 21 to 31**

Value: field 32 of the original authorisation request, left-filled with zeros.

□ **Reserved for future use ____________________ quartets 32 to 42**

Value: zeros.

Field 95 **Format: an42**

Replacement amounts

Specifies the amount actually provided to the cardholder in a reversal transaction.

❑ **New amount______________________________________an12**

❑ **Reserved for future use ________________________________an30**

This amount is expressed in the currency specified in field 49.

Field 112 **Format: LLLVAR ans …255**

Funds transfer data

This field contains all data required in funds transfer management.

❑ **Data type _______________________________________an2**

Type	Description
01	Original transaction data
03	Application type identifier
05	Payer/account number
06	Counterparty PAN
07	Counterparty last name and first name
08	Funds transfer reason
09	BIC
10	IBAN

❑ **Data element length _________________________________ n2**

❑ **Data element value**

TYPE = 01: ORIGINAL TRANSACTION DATA

Data format: ans1..99 Number of bytes transported: 1..99

Information about the person or entity that initiated the funds transfer.

❑ **Nomenclature ____________________________________ an1**

Values	Description
3	CB

❑ **Origin reference ________________________________ ans..98**

TYPE = 03: APPLICATION TYPE IDENTIFIER TRANSACTION

Data format: an2 Number of bytes transported: 2

Specifies the type of application that initiated the funds transfer transaction.

Values	Description
CB nomenclature	
CC	Card to card transfer
DE	Electronic purse account unloading
EB	B2B collaborative economy
EC	B2C collaborative economy
PA	Payment for business-to-individual services
PG	Payment of winnings
RA	Refund for purchases not paid by card
RE	Funds transfer via funds receiver

TYPE = 05: PAYER/ACCOUNT NUMBER

Data format: ans1..35 Number of bytes transported: 1..35

TYPE = 06: COUNTERPARTY PAN

Data format: n..19 Number of bytes transported: 19

Specifies the PAN of the PAN counterparty in field 2 in a card-to-card transfer transaction.

TYPE = 07: COUNTERPARTY LAST NAME AND FIRST NAME

Data format: ans1..30 Number of bytes transported: 1..30

TYPE = 08: FUNDS TRANSFER REASON

Data format: ans1..40 Number of bytes transported: 1.40

TYPE = 09: BIC (BANK IDENTIFIER CODE)

Data format: ans1..11 Number of bytes transported: 1..11

International identifier of bank.

TYPE = 10: IBAN

Data format: an …34 Number of bytes transported: …34

IBAN of the payer.

IBAN complies with ISO 13616.

- ❑ **Country code _____________________________ an2**

  Alphabetic code compliant with ISO 3166.

- ❑ **Control character_____________________________ an2**

  Check digits calculated in compliance with paragraph 6 of ISO 13616.

- ❑ **BBAN _____________________________ an…30**

  This is specific to each banking institution and uniquely identifies a customer's account in a financial institution. The BBAN is the same length for each country. In France, it corresponds to the "RIB" (23 characters).

  The IBAN of an account managed by a banking institution whose country code is "FR" (France) is 27 characters long. The structure of a BBAN or RIB data for an account held in France is:

  Domiciliary bank code: an 5

  Branch code: an 5

  Bank account number: an 11

  Check digits ('RIB key'): an 2

Field 115 **Format: LLLVAR b …255**

nexo data

- ❑ **Data type ___ b2**

Type	Description	Repeatability
0001	nexo PoS identifier	
0002	nexo Acceptance System identifier	
0003	nexo certificate	

- ❑ **Data element length ___ b1**
- ❑ **Data element value**

TYPE = 0001: NEXO POS IDENTIFIER

Data format: ans..107 Number of bytes transported: ..107

Identification of the nexo terminal.
This field includes nexo data elements from the nexo server (POIComponent = "TERM"): "Identification.ProviderIdentification", "Identification.Identification" and "Identification.SerialNumber", each separated by an anti-slash ("\").

TYPE = 0002: NEXO ACCEPTANCE SYSTEM IDENTIFIER

Data format: ans..71 Number of bytes transported:..71

Identification of the nexo terminal in the case of an integrated/distributed system.
This field includes nexo data elements from the nexo server (POIComponent = "SERV"): "Identification.ProviderIdentification" and "Identification.Identification", each separated by an anti-slash ("\").

TYPE = 0003: NEXO CERTIFICATE

Data format: ans..35 Number of bytes transported:..35

Identification of the nexo solution.
Reference of the nexo certificate assigned to the solution
This field contains the nexo data element "Assessment.Number" of the nexo application (POIComponent = "APLI").

Field 119 Format: LL2VAR b…999

Reserved for national use

- ❑ **Data type** b2

Type	Description	Repeatability
0001	Merchant tokenisation indicator	
0009	Scheme program merchant identifier	
0011	FPAN	
0013	Three-domain secure components availability	
0015	Token authentication verification value	
0016	Extended Electronic Commerce Indicator	
0017	Authentication exemption status indicator	
0022	3DS protocol version number	
0028	Remote commerce acceptor identifier	
0041	Purchase identifier type	
0042	Purchase identifier	
0047	Debit unique reference identifier	
00BC	Extended message to the transaction initiator	
0208	Pre-authorisation duration	
0359	Transaction eligible for token services	
0801	Reattempt indicator	
0802	Reattempt frozen period	
0803	Reattempt conditions	
1022	Cardholder verification method used at POS	
9F19	Token Requestor ID	
9F25	Last four digits of PAN	
1022	Cardholder verification method used at POS	

- ❑ **Data element length** n2
- ❑ **Data element value**

TYPE = 0001: MERCHANT TOKENISATION INDICATOR

Data format: an1 Number of bytes transported: 1

Value	Meaning
1	Card-On-File tokenisation

TYPE = 0009: SCHEME PROGRAM MERCHANT IDENTIFIER

Data format: ans…8 Number of bytes transported: …8

Merchant identifier for the transaction scheme program

TYPE = 0011 : FPAN

Data format: n9…19 Number of bytes transported: 5…10

Primary Account Number associated to the token for tokenised transactions.

TYPE = 0013: THREE-DOMAIN SECURE COMPONENTS AVAILABILITY

Data format: an1 Number of bytes transported: 1

Value	Description
1	3DS server unavailable

TYPE = 0015: TOKEN AUTHENTICATION VERIFICATION VALUE

Data format: b4…40 Number of bytes transported: 4…40

Token cryptogram that contains uniquely generated data to enable validation of the uthorised use of the Payment Token.

TYPE = 0016: EXTENDED ELECTRONIC COMMERCE INDICATOR

Data format: n3 Number of bytes transported: 2

SLI (Security Level Indicator) in electronic commerce.

TYPE = 0017: AUTHENTICATION EXEMPTION STATUS INDICATOR

Data format: an1 Number of bytes transported: 1

Indicates the status of the exemption.

TYPE = 0022: 3DS PROTOCOL VERSION NUMBER

Data format: ans1…8 Number of bytes transported: 1…8

Corresponds to the ‘Message version number’ data element in the EMVCo 3DS specifications.
Default value of ‘0’ if the data element is absent or not set to a value.
Examples: 2.0.0, 2.1.0, 2.2.0

TYPE = 0028: REMOTE COMMERCE ACCEPTOR INDICATOR

Data format: b…115 Number of bytes transported: …115

This identifier may consist of part of merchant business website URL or reverse domain name which allows to perform the dynamic linking validation.

TYPE = 0041: PURCHASE IDENTIFIER TYPE

Data format: an1 Number of bytes transported: 1

The following list is provided for example. Refer to schemes' rules:

Type	Meaning
0	Free text
1	Order number
3	Rental agreement number
4	Hotel folio number
5	Invoice number

TYPE = 0042: PURCHASE IDENTIFIER

Data format: an32 Number of bytes transported: 32

Allows to uniquely identify a payment agreement using the same PAN or token under the same merchant and the same payment use case.

TYPE = 0047: DEBIT UNIQUE REFERENCE IDENTIFIER

Data format: ans…50 Number of bytes transported: …50

Identifier of the debit transaction to which a credit transaction is associated. This debit is an authorized debit which can have been made in remote payment or in another payment method.

TYPE = 00BC: EXTENDED MESSAGE TO THE TRANSACTION INITIATOR

Data format: ans1…101 Number of bytes transported: …101

- ❑ **Control character ____ ans1**

Values	Description
0	Reserved
1	Print
2	Display
3	Print and display
4	Print for cardholder only
5	Display for cardholder only
6	Print and display for the cardholder only
7	Print for acceptor only
8	Display for acceptor only
9	Print and display for the acceptor only
A	Print for the acceptor and the cardholder
B	Display for the acceptor and the cardholder
C	Print and display for the acceptor and the cardholder
F	Reserved for private use

- ❑ **Response message ____ ans…100**

TYPE = 0208: PRE-AUTHORISATION DURATION

Data format: n 2 Number of bytes transported: 1

This indicates for how many days the pre-authorisation is valid.

TYPE = 0359: TRANSACTION ELIGIBLE FOR TOKEN SERVICES

Data format: an1 Number of bytes transported: 1

Allows the scheme to indicate whether the transaction is eligible for its token services.

TYPE = 0801: REATTEMPT INDICATOR

Data format: n 2 Number of bytes transported: 1

Use by acquirers to communicate to merchants the procedure to follow when an authorisation request is declined.

Values	Description
01	Obtain new information before the next transaction
02	Try again later
03	Never try again

TYPE = 0802: REATTEMPT FROZEN PERIOD

Data format: n 4 Number of bytes transported: 2

Number of hours where reattempt is not allowed

TYPE = 0803: REATTEMPT CONDITIONS

Data format: n 6 Number of bytes transported: 3

❑ **Reattempt allowed duration**____ **n4**

❑ **Maximum number of reattempts**____________________________________ **n2**

TYPE = 9F19: TOKEN REQUESTOR ID

Data format: an 11 Number of bytes transported: 11

Identifies each unique combination of Token Requestor and Token Domain(s) for a given Token Service Provider:

- Positions 1-3: Token Service Provider Code, unique to each Token Service Provider
- Positions 4-11: assigned by the Token Service Provider for each Token Requestor and Token Domain

TYPE = 9F25: LAST FOUR DIGITS OF PAN

Data format: n 4 Number of bytes transported: 2

Last four digits of PAN

TYPE = 1022: CARDHOLDER VERIFICATION METHOD USED AT POS

Data format: b1…4 Number of bytes transported: 1…4

Lists the value attributed to each bit of the 16 bits (two characters) which indicate the cardholder verification method used by the POS.

☐ **Byte 1____ b1**

b8	b7	b6	b5	b4	b3	b2	b1	Description
x								1 = Consumer device CVM
	0							Reserved for future use
		x						1 = Offline PIN encrypted
			x					1 = Offline PIN in clear
				x				1 = Online PIN
					x			1 = Signature
						x		1 = No CVM
							x	1 = Unknown

☐ **Reserved for future use____ b3**

NETWORK MANAGEMENT

TABLE OF CONTENTS

1. INTRODUCTION

The Network Management Service includes three types of network management requests. All these requests are dedicated exclusively to terminals/devices used by Big Retailers.

- Sign-On
- Sign-Off
- Echo test

The message type identifier (0800/0810) by itself cannot identify these different messages. The value for field 70 (Network Management Code) is used to identify the transaction.

Request messages (0800) are only initiated by Big Retailer equipment. Response messages (0810) are always returned by the Acquiring System.

SPECIFIC INFORMATION RELATED TO BIG RETAILERS

Big Retailers are merchants which produce large flows of authorisation transactions. Due to these high volumes and for reasons related to Service Quality and scaling, Acquiring Systems can set up dedicated TRANSPAC connections.

These dedicated connections are referred to as “reserved” and are different from the standard connections used for *CB2A Authorisation/EMA and CB2A Authorisation/Non-EMA* terminals.

For such reserved connections, Big Retailer and Acquirer Systems can use the following network management specifications:

Echo Test	(Application level)
Sign-on/Sign-off	(Application level)
NRT, IMT and AMT Timers	(CBcom - Pseudo-session level)

Note: All the above specifications are optional.

1.1. SIGN-ON/SIGN-OFF TRANSACTION

The Sign-On transaction is used to open a dialog at the application layer.
The Sign-Off transaction is used to close a dialog at the application layer.

Between the above two transactions, a dialog is established during which authorisation and echo test transactions can be exchanged.

In addition to the sign-on function, these messages transport data enabling mutual identification of the parties.

Message type identifier:

- request message = network management request: 0800
- response message = network management request response: 0810

The network management code (field 70) is used to identify the message:

- sign-on transaction: field 70 = 001
- sign-off transaction: field 70 = 002

1.2. ECHO TEST TRANSACTION

Big Retailer equipment uses the echo activity to ensure the availability of the point of access and the connection to it.

This network management transaction includes the following messages:

- 0800 'echo test' request sent by the "Big Retailer" equipment
- 0810 'echo test' request response message returned by the acquirer system

Value '301' in field 70 (network management code) identifies the transaction.

After the Acquirer system receives an echo request message (0800), it replies with a response message (0810) including a response code (field 39). Value '00' indicates that the service is provided.

When a response (0810) is received with a field 39 value different from '00', the "Big Retailer" equipment must disconnect.

If there is no response within a specified period of time (see CBcom, TNR timer), the acceptance system can re-send the request or disconnect.

2. RESPONSE CODES

A response code (field 39) returned in a response message triggers action or processing by the receiving system.
Only the common and significant response codes are presented in the tables below.

2.1. RESPONSE CODES FOR A SIGN-ON/SIGN-OFF TRANSACTION

No.	Description
00	Approved or completed successfully
12	Invalid transaction
30	Format error
31	Unknown acquiring institution identification code
90	Temporary system shutdown
96	System malfunction

Refer to the relevant specifications in the Reference Manuals (MPE, MPA) for further information about the actions to take.

2.2. RESPONSE CODES FOR AN ECHO TEST TRANSACTION

No.	Description
00	Approved or completed successfully
12	Invalid transaction
30	Format error
31	Unknown acquiring institution identification code
58	Transaction not permitted for terminal
90	Temporary system shutdown
96	System malfunction

Refer to the relevant specifications in the Reference Manuals (MPE, MPA) for further information about the actions to take.

3. MESSAGE DESCRIPTIONS

Table legends

The term "transaction” refers to a set of "requests/responses".
The term "message" refers either to a request or to a response.

Field presence conditions

X	Mandatory
C	Conditional: the condition making this field mandatory is stated in a note (nn); in all other cases, the field is optional
F	Optional
.	The field may be present, but it is not processed by the receiving system.

Non-applicable - Field is not defined in the standard.

Field contents

S	Message-specific value
Q	Value is equal to request value
QI	Value is equal to initial request value
RI	Value is equal to initial response value

Note

- All fields undefined in the CB2A Authorisation protocol, but which comply with ISO 8583 (v87) can be used.
- The condition "mandatory if available" means that the data element must be transported by the protocol when provided by the application

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Echo test request : **0800** **B:** Response to echo test request : **0810**

N°	**Définition**	**A**	**B**
1	Bit Map, extended	X	X
7	Transmission date and time	XS	XS
11	Systems trace audit number	XS	XQ
32	Acquiring institution identification code	F	FQ
33	Forwarding institution identification code	C(21)	CQ(9)
39	Response code	.	XS
41	Card acceptor terminal identification	C(35)	FQ
42	Card acceptor identification code	F	CQ(9)
44	Additional response data	.	C(2)
AA	Incorrect field	.	C(19)
BB	Telephone number	.	FS
BC	Message to the transaction initiator	.	FS
58	Responding machine identifier	.	FS
70	Network management information code	X	XQ

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Sign-on / Sign-off : **0800**	**B:** Response to Sign-on / Sign-off : **0810**

N°	Définition	A	B
1	Bit Map, extended	X	X
7	Transmission date and time	XS	XS
11	Systems trace audit number	XS	XQ
32	Acquiring institution identification code	F	FQ
33	Forwarding institution identification code	C(21)	CQ(9)
39	Response code	.	XS
41	Card acceptor terminal identification	C(35)	FQ
42	Card acceptor identification code	C(15)	CQ(9)
44	Additional response data	.	C(2)
AA	Incorrect field	.	C(19)
BB	Telephone number	.	FS
BC	Message to the transaction initiator	.	FS
47	Additional data - national	C(2)	C(2)
96	SIRET	C(29)	FQ
A0	IDSA (card acceptor terminal identifier)	C(29)	FQ
58	Responding machine identifier	.	F
59	National data	C(2)	C(2)
0202	Acceptor contract number	C(15)	FQ
0203	Acceptance system logical number	C(15)	XQ
70	Network management information code	XS	XQ

N°	COMMENTAIRES
2	See list of types
9	Mandatory if present in the request, otherwise absent
15	Mandatory if "forwarding institution identifier" is absent
19	Mandatory if "response code"=30, optional if "response code"=12
21	Mandatory in case of one or more intermediaries between Acceptor and Acquirer, otherwise absent
29	Mandatory if available, otherwise absent
35	Mandatory if parameters downloaded

FACE-TO-FACE PAYMENT
UNATTENDED PAYMENT

TABLE OF CONTENTS

1. INTRODUCTION

The present volume describes the following:

- Face-to-face payments
- Standard unattended payment
- Payments on multiservice banking ATMs
- Payments on rental terminals
- Face-to-face payments for the reservation and rental of goods or services

1.1. OVERVIEW

The purpose of this service is to:

- request a debit or credit payment authorisation without online PIN verification
- obtain a response to this authorisation request (approval or reason for decline)
- reverse a previously granted authorisation to inform the issuer of the final transaction amount
- obtain a response to this reversal request.

Message type identifier:

- request message = authorisation request: 0100
- response message = authorisation request response: 0110
- request message = authorisation reversal request: 0400
- request message = authorisation reversal repeat request: 0401
- response message = authorisation reversal request response: 0410

2. RESPONSE CODES

A response code (field 39) returned in a response message generates an action by the receiver.

Only significant and commonly used response codes are presented in the tables below.

2.1. RESPONSE CODES FOR A FACE-TO-FACE PAYMENT AUTHORISATION REQUEST

No.	Description
00	Successful approval/completion
02	Refer to card issuer
03	Invalid merchant
04	Pickup
05	Do not honour
07	Pickup card, special conditions
08	Honour with cardholder identification
10	Approved for partial amount
12	Invalid transaction
13	Invalid amount
14	Invalid card number (no such number)
15	No such issuer
17	Customer cancellation
19	Re-enter transaction
20	Invalid response (error in server domain)
30	Format error
31	Bank not supported by switch
33	Expired card
34	Suspected fraud
38	Allowable PIN tries exceeded
41	Lost card
43	Stolen card, pick-up
46	Business specific error
51	not sufficient funds
54	Expired card
55	Incorrect PIN
56	No card record
57	Transaction not permitted to cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
60	Card acceptor contact acquirer
62	Restricted card
63	Security violation
68	Response received too late
6P	Verification data failed
75	Allowable number of PIN-entries exceeded
77	Closed account
78	Blocked, first used or special condition—new cardholder not activated or card is temporarily blocked
82	Negative online CAM, dCVV, iCVV, or CVV results Or Offline PIN authentication interrupted
91	Issuer or switch is inoperative
93	Transaction cannot be completed-Violation of law
94	Duplicate transmission
96	System malfunction
97	General monitoring timeout
98	Server inaccessible (set by the server)
A0	Fallback in contact mode
A2	PIN request in single TAP mode
A3	New TAP with required authentication

For information about the actions to be taken, refer to the specifications in MPE (Electronic Payment Manual).

2.2. RESPONSE CODES FOR AN UNATTENDED PAYMENT AUTHORISATION REQUEST

No.	Description
00	Successful approval/completion
02	Refer to card issuer
03	Invalid merchant
04	Pickup
05	Do not honour
07	Pickup card, special condition
08	Honour with cardholder identification
10	Approved for partial amount
12	Invalid transaction
13	Invalid amount
14	Invalid card number (no such number)
15	No such issuer
20	Invalid response (error in server domain)
30	Format error
31	Bank not supported by switch
33	Expired card
34	Suspected fraud
38	Allowable PIN tries exceeded
41	Lost card
43	Stolen card, pick-up
46	Business specific error
51	not sufficient funds
54	Expired card
55	Incorrect PIN
56	No card record
57	Transaction not permitted to cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
60	Card acceptor contact acquirer
61	Exceeds withdrawal amount limit
62	Restricted card
63	Security violation
68	Response received too late
6P	Verification data failed
75	Allowable number of PIN-entries exceeded
77	Closed account
78	Blocked, first used or special condition—new cardholder not activated or card is temporarily blocked
82	Negative online CAM, dCVV, iCVV, or CVV results Or Offline PIN authentication interrupted
91	Issuer or switch is inoperative
93	Transaction cannot be completed-Violation of law
94	Duplicate transmission
96	System malfunction
97	General monitoring timeout
98	Server inaccessible (set by the server)
A0	Fallback in contact mode

For information about the actions to be taken, refer to the specifications in MPE (Electronic Payment Manual).

2.3. RESPONSE CODES FOR A FACE-TO-FACE/UNATTENDED PAYMENT REVERSAL REQUEST

No.	Description
00	Successful approval/completion
17	Customer cancellation
21	No action taken

No.	Description
32	Partial completion (ISO 8583)
99	Malfunction

2.4. RESPONSE CODES FOR A RESPONSE TO A REVERSAL REQUEST RELATED TO FACE-TO-FACE/UNATTENDED PAYMENT

No.	Description
03	Invalid merchant
12	Invalid transaction
13	Invalid amount
14	Invalid card number (no such number)
15	No such issuer
20	Invalid response (error in server domain)
25	Unable to locate record in file
30	Format error
31	Bank not supported by switch
56	No card record
63	Security violation
90	Cutoff
91	Issuer or switch is inoperative
94	Duplicate transmission
96	System malfunction
97	General monitoring timeout
98	Server inaccessible (set by the server)

3. REQUIREMENTS RELATED TO PAYMENT FOR THE RESERVATION AND RENTAL OF GOODS OR SERVICES

3.1. AUTHORISATION REQUEST TRANSACTION FOR FACE-TO-FACE PAYMENT

The purpose of this transaction is to request an authorisation for face-to-face payment.

The response to this authorisation request provides approval or the reason for decline.

Typical values:

- field 22 position 1 and 2 (PAN entry mode) <> 01
- field 56 type 0028 (Payment use case) = 06 ‘Reservation and rental payment’ or 07 ‘Pre-authorisation out of reservation and rental’
- field 59 type 0100 (Function code) = 101 ‘Original authorisation – estimated amount’
- field 59 type 0101 (Reason code) = 1655 ‘Pre-authorisation request’
- field 59 type 0200 (ERT*) = 80
- field 59 type 0800 (service attribute) = 2 ‘Pre-authorisation’

*Regulatory and Technical Environment (ERT)

3.2. AUTHORISATION REQUEST TRANSACTION FOR UNATTENDED PAYMENT

The purpose of this transaction is to request an authorisation for unattended payment.

The response to this authorisation request provides approval or the reason for decline.

Typical values:

- field 22 position 1 and 2 (PAN entry mode <> 01 and <> 10
- field 56 type 0028 (Payment use case) = 06 ‘Reservation and rental payment’ or 07 ‘Pre-authorisation out of reservation and rental’
- field 59 type 0100 (Function code) = 101 ‘Original authorisation – estimated amount’
- field 59 type 0101 (Reason code) = 1655 ‘Pre-authorisation request’
- field 59 type 0200 (ERT*) = 57
- field 59 type 0800 (service attribute) = 2 ‘Pre-authorisation’

*Regulatory and Technical Environment (ERT)

4. REQUIREMENTS RELATED TO CONTACTLESS PAYMENT

4.1. EMV ICC CONTACTLESS TRANSACTIONS

Typical values:

- field 22 position 1 and 2 (Point of service entry mode) = 07
- field 55 type DF81 (Card application type) = 2
- field 55 type DF85 (Result of terminal processing) is completed

4.2. CONTACTLESS CHIP TRANSACTIONS USING MAGSTRIPE DATA

Typical values:

- field 22 position 1 and 2 (Point of service entry mode) = 91
- field 55 type DF81 (Card application type) = 3
- field 55 type 0056 (Track 1 equivalent data read in contactless mode) set if track 1 data was read
- field 55 type 9F6B (Track 2 equivalent data read in contactless mode) set if track 2 data was read
- field 59 type 0101 (Message reason code) = 1671

5. REQUIREMENTS RELATED TO REVERSALS AND PARTIAL AUTHORISATIONS

Partial authorisation is performed in two steps:

- Indication in the authorisation request message that the merchant terminal supports partial authorisations (bit no. 1 in field 59 type 0805)
- Partial authorisation granted by the issuer

For unattended payments - as the transaction amount is not known before the goods have been distributed, terminals must perform a reversal as soon as the actual amount is known in order to update the cardholder's payment limit.
Bit no. 3 in field 59 type 0805 is used to indicate that the acceptance system is performing the reversal.

5.1. INFORMATION ON DATA ELEMENT VALUES

5.1.1. Fields 4, 54 and 95

Field		Authorisation		Reversal	
No.	Field name	Request	Response	Request	Response
4	Transaction amount	Authorisation amount Condition: X	Authorised amount Condition: X	Authorised amount Condition: X	Authorised amount Condition: XQ
54-57	Original amount		Authorisation amount Condition: mandatory for partial authorisations		
95	Replacement amount			Final transaction amount Condition: X	Final transaction amount Condition: FQ

5.1.2. Field 3 in 0400/0401 messages

The value of field 3 is equal to that of the initial request.

5.1.3. Field 4 in 0110 messages

- For full authorisations, the value must be equal to the value in the request.
- For partial authorisations (field 39=10), the value must be equal to the authorised amount.

5.1.4. Field 4 in 0400 messages

- For full authorisations, the value must be equal to the value in the request.
- For partial authorisations (field 39=10), the value must be equal to the authorised amount
- If there is no response to the authorisation request, the value must be equal to the value in the request

5.1.5. Field 54 in 0110 messages

- For full authorisations, this field is absent.
- For partial authorisations (field 39=10), the value of the "amount" of field 54 must be equal to the value of field 4 of the request.

5.1.6. Field 95 in 0400 messages

- When the final transaction amount is equal to the authorised amount (reversal with no effect), the value must be equal to the value of field 4 (transaction amount).
- When the final transaction amount is equal to zero (full reversal), the value of this field must be equal to zero.

6. REQUIREMENTS RELATED TO CARD VALIDITY CHECK

The purpose of this transaction is to request information about a cardholder PAN (Primary Account Number).

Message type identifier:

- Request: 0100
- Response: 0110

Typical values:

- field 59 type 100 (Function code) set to 108 (Card Validity Check)
- field 4 (Amount) set to 0

Note: a field 59 type 0418 (Wallet Identifier) set indicates **a wallet registration**.

7. MESSAGE DESCRIPTIONS

How to read the tables:

The term "transaction" refers to a request/response.
The term "message" refers to either a request or to a response.

Data field presence conditions

X	Mandatory
C	Conditional: the condition making this field mandatory is stated in a note (nn); in all other cases, the field is optional
F	Optional
.	The field may be present, but it is not processed by the receiver

Field values

S	Message-specific value
Q	Value is equal to request value
QI	Value is equal to initial request value
RI	Value is equal to initial response value

Note:

- All fields undefined in CB2A Authorisation can be used, providing they are compliant with ISO 8583 (v87).
- The condition “Mandatory if available” means that the data element must be transported by the protocol when provided by the application.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment autho. req. (EMV chip and contactless EMV chip) : **0100**	**B:** Payment autho. request (magn. stripe and contactless magn. stripe) : **0100**
C: Resp. to payment autho. req. (contact and contactless) : **0110**	

N°	Définition	A	B	C
1	Bit Map, extended	C(1)	C(1)	C(1)
2	Primary Account Number	X	X	XQ
3	Processing code	X	X	XQ
4	Amount, transaction	X	X	X
7	Transmission date and time	C(117)	C(117)	.
11	Systems trace audit number	XS	XS	XQ
12	Time, local transaction	XS	XS	FQ
13	Date, local transaction	XS	XS	FQ
14	Date, expiration	.	X	FQ
18	Merchant type	X	X	FQ
22	Point of service entry mode	X	X	FQ
23	Card sequence number	C(84)	.	CQ(84)
25	Point of service condition code	X	X	FQ
26	Pin length	C(30)	C(30)	FQ
27	Authorisation identification response length	C(7)	C(7)	.
32	Acquiring institution identification code	X	X	XQ
33	Forwarding institution identification code	C(21)	C(21)	FQ
35	Track 2 data	C(12)	C(128)	.
37	Retrieval reference number	F	F	C(79)
38	Authorisation identification response	.	.	C(10)
39	Response code	.	.	XS
41	Card acceptor terminal identification	X	X	XQ
42	Card acceptor identification code	X	X	XQ
43	Card acceptor name/location	C(63)	C(63)	FQ
44	Additional response data	.	.	C(2)
AA	Incorrect field	.	.	C(69)
AB	Security error	.	.	C(12)
AC	Field conversion	.	.	F
AF	Service activation code	.	.	F
BB	Telephone number	.	.	F
BC	Message to the transaction initiator	.	.	F
CA	Track or equivalent data cryptogram processing information	.	.	C(12)
CB	Application cryptogram verification results	.	.	C(12)
CD	Information related to liability shift	.	.	F
47	Additional data - national	C(2)	C(2)	C(2)
08	Location category code	C(63)	C(63)	FQ
24	File number	C(145)	C(145)	CQ(145)
30	Additional card reading capabilities	C(3)	C(3)	FQ
31	Point of interaction information	C(3)	C(3)	FQ
33	CB2A specification date	C(3)	C(3)	.
95	Unique transaction identifier	.	.	C(3)
96	SIRET	C(63)	C(63)	FQ

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment autho. req. (EMV chip and contactless EMV chip) : **0100**	**B:** Payment autho. request (magn. stripe and contactless magn. stripe) : **0100**
C: Resp. to payment autho. req. (contact and contactless) : **0110**	

N°	**Définition**	**A**	**B**	**C**
97	IDPA	C(63)	C(63)	FQ
99	Original unique transaction identifier	C(3)	C(3)	F
A0	IDSA (card acceptor terminal identifier)	C(63)	C(63)	FQ
48	Security Data	C(2)	C(2)	.
0001	KSN	C(31)	C(31)	.
0002	BDK name	C(29)	C(29)	.
0003	BDK version	C(154)	C(154)	.
49	Currency code, transaction	X	X	XQ
52	PIN data	C(32)	C(32)	C(12)
53	Security related control information	X	X	X
54	Additionnal amounts	C(118)	C(118)	C(118)
43	Cumulative total authorised amount	C(150)	.	CQ(150)
44	Tip amount	C(119)	C(119)	CQI
57	Original amount	.	.	C(115)
55	Integrated circuit card system related data	C(2)	C(2)	C(2)
0056	Data equivalent to ISO track 1 read in contactless mode	C(48)	C(48)	.
0057	Track 2 equivalent data	C(165)	C(48)	.
0071	Issuer Script Template 1	.	.	C(24)
0072	Issuer Script Template 2	.	.	C(24)
0082	Application Interchange Profile (AIP)	X	C(48)	.
0091	Issuer Authentication Data	.	.	C(24)
0095	Terminal Verification Results (TVR)	C(160)	.	.
009A	Terminal Transaction Date	C(138)	.	.
009C	Transaction type	X	.	.
5F24	Application expiration date	X	.	FQ
9F02	Amount, authorized	C(135)	.	.
9F06	Application Identifier (AID)	X	C(48)	.
9F0A	Application selection registered proprietary data	C(84)	C(84)	.
9F10	Issuer application data	C(85)	C(85)	.
9F1F	Track 1 Discretionary Data	C(48)	C(48)	.
9F26	Application Cryptogram	C(160)	.	.
9F27	Cryptogram Information Data (CID)	C(160)	.	.
9F33	Terminal capabilities	X	C(101)	.
9F34	Cardholder Verification Method Results	C(29)	.	.
9F35	Terminal type	C(3)	C(3)	.
9F36	Application Transaction Counter (ATC)	C(160)	.	.
9F37	Unpredictable Number	C(160)	.	.
9F66	Terminal transaction qualifiers (TTQ)	C(48)	.	.
9F6B	Data equivalent to ISO track 2 read in contactless mode	.	C(48)	.
9F7C	Issuer Proprietary Data	C(48)	.	.
DF68	Kernel ID used	C(48)	C(48)	.
DF80	ICC processing results	C(127)	C(29)	FQ

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment autho. req. (EMV chip and contactless EMV chip) : **0100**	**B:** Payment autho. request (magn. stripe and contactless magn. stripe) : **0100**
C: Resp. to payment autho. req. (contact and contactless) : **0110**	

N°	**Définition**	**A**	**B**	**C**
DF81	Card application type	X	C(49)	FQ
DF85	RTT (Terminal processing results)	C(48)	.	.
DF86	Contactless device	C(3)	C(3)	.
56	Additional data	C(2)	C(2)	C(2)
0001	Payment facilitator data	C(3)	C(3)	.
0002	Application selection indicator	C(3)	C(3)	.
0003	Brand selected	C(3)	C(3)	.
0019	Serial number	C(3)	C(3)	.
0020	Resend counter	C(3)	.	.
0024	Independent sales organisation	C(3)	C(3)	.
0025	Payment facilitator identifier	C(3)	C(3)	.
0026	Market place identifier	C(3)	C(3)	.
0027	Final merchant identifier	C(3)	C(3)	.
0028	Payment use case	C(63)	C(63)	.
0040	List of installed kernels	C(3)	C(3)	.
0056	Payment Account Reference	.	.	C(108)
5F2D	Language preference	C(153)	.	.
9F0D	Issuer Action Code - Default	C(153)	.	.
9F0E	Issuer Action Code - Denial	C(153)	.	.
9F0F	Issuer Action Code - Online	C(153)	.	.
59	National data	C(2)	C(2)	C(2)
0100	Function code	C(47)	C(47)	FQ
0101	Message reason code	X	X	FQ
0102	Transaction year	XS	XS	CQ(95)
0200	ERT (Regulatory and Technical Environment)	X	X	FQ
0201	ITP SA (Acceptance system terminal application identifier)	X	X	FQ
0202	Acceptor contract number	X	X	FQ
0203	Acceptance system logical number	X	X	FQ
0204	Point of interaction logical number	C(151)	C(22)	FQ
0205	Acceptance system country code	C(63)	C(63)	FQ
0207	Cardholder total amount	C(5)	C(5)	FQ
020B	TASA (Card acceptor application type)	X	X	FQ
0215	ITP PA (Point of interaction terminal application identifier)	C(3)	C(3)	FQ
0216	Point of interaction extended logical number	C(152)	.	FQ
0800	Service attribute	C(46)	C(46)	FQ
0805	Optional services supported (acceptor domain)	C(3)	C(3)	.
112	Funds transfer data	C(2)	C(2)	.
01	Original transaction data	C(94)	C(94)	.
03	Application type identifier	C(94)	C(94)	.
08	funds transfer reason	C(147)	.	.
10	IBAN	C(147)	.	.
115	nexo data	C(2)	C(2)	.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment autho. req. (EMV chip and contactless EMV chip) : **0100**	**B:** Payment autho. request (magn. stripe and contactless magn. stripe) : **0100**
C: Resp. to payment autho. req. (contact and contactless) : **0110**	

N°	**Définition**	**A**	**B**	**C**
0001	nexo PoS identifier	C(3)	C(3)	.
0002	nexo Acceptance System identifier	C(3)	C(3)	.
0003	nexo certificate	C(3)	C(3)	.
119	Reserved for national use	C(2)	C(2)	C(2)
0011	FPAN	.	.	C(3)
0022	3DS protocol version number	.	.	FQ
0047	Debit unique reference identifier	C(156)	C(156)	F
00BC	Extended message to the transaction initiator	.	.	F
0208	Pre-authorisation duration	C(63)	C(63)	.
0801	Reattempt indicator	.	.	C(3)
0802	Reattempt frozen period	.	.	C(161)
0803	Reattempt conditions	.	.	C(162)
1022	Cardholder verification method used at POS	C(3)	C(3)	FQ

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Proximity wallets payment authorization request : **0100**	**B:** Response to proximity wallets payment autho. request : **0110**

N°	**Définition**	**A**	**B**
1	Bit Map, extended	C(1)	C(1)
2	Primary Account Number	X	XQ
3	Processing code	X	XQ
4	Amount, transaction	X	X
7	Transmission date and time	C(117)	.
11	Systems trace audit number	XS	XQ
12	Time, local transaction	XS	FQ
13	Date, local transaction	XS	FQ
14	Date, expiration	X	FQ
18	Merchant type	X	FQ
22	Point of service entry mode	X	FQ
25	Point of service condition code	X	FQ
27	Authorisation identification response length	C(7)	.
32	Acquiring institution identification code	X	XQ
33	Forwarding institution identification code	C(21)	FQ
35	Track 2 data	C(12)	.
37	Retrieval reference number	F	C(79)
38	Authorisation identification response	.	C(10)
39	Response code	.	XS
41	Card acceptor terminal identification	X	XQ
42	Card acceptor identification code	X	XQ
43	Card acceptor name/location	C(63)	FQ
44	Additional response data	.	C(2)
AA	Incorrect field	.	C(69)
AB	Security error	.	C(12)
AC	Field conversion	.	F
AF	Service activation code	.	F
BB	Telephone number	.	F
BC	Message to the transaction initiator	.	F
CA	Track or equivalent data cryptogram processing information	.	C(12)
CB	Application cryptogram verification results	.	C(12)
CD	Information related to liability shift	.	F
47	Additional data - national	C(2)	C(2)
08	Location category code	C(63)	FQ
24	File number	C(145)	CQ(145)
30	Additional card reading capabilities	C(3)	FQ
31	Point of interaction information	C(3)	FQ
33	CB2A specification date	C(3)	.
95	Unique transaction identifier	.	C(3)
96	SIRET	C(63)	FQ
97	IDPA	C(63)	FQ
99	Original unique transaction identifier	C(3)	F

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Proximity wallets payment authorization request : **0100** **B:** Response to proximity wallets payment autho. request : **0110**

N°	Définition	A	B
A0	IDSA (card acceptor terminal identifier)	C(63)	FQ
49	Currency code, transaction	X	XQ
53	Security related control information	X	X
54	Additionnal amounts	C(118)	C(118)
43	Cumulative total authorised amount	C(150)	CQ(150)
57	Original amount	.	C(115)
56	Additional data	C(2)	C(2)
0001	Payment facilitator data	C(3)	.
0002	Application selection indicator	C(3)	.
0003	Brand selected	C(3)	.
0019	Serial number	C(3)	.
0020	Resend counter	C(3)	.
0024	Independent sales organisation	C(3)	.
0025	Payment facilitator identifier	C(3)	.
0026	Market place identifier	C(3)	.
0027	Final merchant identifier	C(3)	.
0056	Payment Account Reference	.	C(108)
5F2D	Language preference	C(153)	.
9F0D	Issuer Action Code - Default	C(153)	.
9F0E	Issuer Action Code - Denial	C(153)	.
9F0F	Issuer Action Code - Online	C(153)	.
59	National data	C(2)	C(2)
0100	Function code	C(47)	FQ
0101	Message reason code	X	FQ
0102	Transaction year	XS	CQ(95)
0200	ERT (Regulatory and Technical Environment)	X	FQ
0201	ITP SA (Acceptance system terminal application identifier)	X	FQ
0202	Acceptor contract number	X	FQ
0203	Acceptance system logical number	X	FQ
0204	Point of interaction logical number	C(151)	FQ
0205	Acceptance system country code	C(63)	FQ
0207	Cardholder total amount	C(5)	FQ
020B	TASA (Card acceptor application type)	X	FQ
0215	ITP PA (Point of interaction terminal application identifier)	C(3)	FQ
0216	Point of interaction extended logical number	C(152)	FQ
0401	Cardholder authentication value	C(5)	.
0409	Cardholder authentication value processing information	.	X
0411	Cardholder authentication value calculation method	C(5)	.
0417	Digital wallet additional data	C(3)	.
0418	Wallet identifier	X	.
0800	Service attribute	C(46)	FQ
0805	Optional services supported (acceptor domain)	C(3)	.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Proximity wallets payment authorization request : **0100**	**B:** Response to proximity wallets payment autho. request : **0110**

N°	**Définition**	**A**	**B**
112	Funds transfer data	C(2)	.
01	Original transaction data	C(94)	.
03	Application type identifier	C(94)	.
08	funds transfer reason	C(147)	.
10	IBAN	C(147)	.
115	nexo data	C(2)	.
0001	nexo PoS identifier	C(3)	.
0002	nexo Acceptance System identifier	C(3)	.
0003	nexo certificate	C(3)	.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment reversal request : **0400/0401**	**B:** Response to payment reversal request : **0410**

N°	Définition	A	B
1	Bit Map, extended	C(1)	C(1)
2	Primary Account Number	XQI	XQ
3	Processing code	XQI	XQ
4	Amount, transaction	X	XQ
7	Transmission date and time	XS	FS
11	Systems trace audit number	XS	XQ
12	Time, local transaction	XS	FQ
13	Date, local transaction	XS	FQ
14	Date, expiration	CQI(104)	FQ
18	Merchant type	XQI	FQ
22	Point of service entry mode	XQI	FQ
23	Card sequence number	CQI(104)	CQ(9)
25	Point of service condition code	XQI	FQ
32	Acquiring institution identification code	XQI	XQ
33	Forwarding institution identification code	C(21)	FQ
37	Retrieval reference number	CRI(116)	FQ
38	Authorisation identification response	CRI(10)	.
39	Response code	XS	XS
41	Card acceptor terminal identification	XQI	XQ
42	Card acceptor identification code	XQI	XQ
43	Card acceptor name/location	CQI(104)	FQ
44	Additional response data	.	C(2)
AA	Incorrect field	.	C(106)
AB	Security error	.	C(12)
AC	Field conversion	.	F
AF	Service activation code	.	F
BC	Message to the transaction initiator	.	F
47	Additional data - national	C(2)	C(2)
08	Location category code	CQI(104)	FQ
24	File number	CQI(104)	CQ(9)
30	Additional card reading capabilities	CQI(104)	FQ
31	Point of interaction information	CQI(104)	FQ
33	CB2A specification date	CQI(104)	.
95	Unique transaction identifier	CRI(116)	FQ
96	SIRET	CQI(104)	FQ
97	IDPA	CQI(104)	FQ
99	Original unique transaction identifier	CQI(104)	.
A0	IDSA (card acceptor terminal identifier)	CQI(104)	FQ
49	Currency code, transaction	XQI	XQ
52	PIN data	C(12)	.
53	Security related control information	XS	XS
55	Integrated circuit card system related data	C(2)	C(2)

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment reversal request : **0400/0401** **B:** Response to payment reversal request : **0410**

N°	**Définition**	**A**	**B**
0056	Data equivalent to ISO track 1 read in contactless mode	CQI(104)	.
0095	Terminal Verification Results (TVR)	C(104)	.
5F24	Application expiration date	CQI(104)	.
9F02	Amount, authorized	CQI(104)	.
9F06	Application Identifier (AID)	CQI(104)	.
9F0A	Application selection registered proprietary data	CQI(104)	.
9F10	Issuer application data	C(104)	.
9F1F	Track 1 Discretionary Data	C(3)	.
9F33	Terminal capabilities	CQI(104)	.
9F35	Terminal type	CQI(104)	.
9F36	Application Transaction Counter (ATC)	CQI(104)	.
9F66	Terminal transaction qualifiers (TTQ)	CQI(104)	.
9F7C	Issuer Proprietary Data	CQI(104)	.
DF68	Kernel ID used	CQI(104)	.
DF81	Card application type	CQI(104)	FQ
DF85	RTT (Terminal processing results)	C(104)	.
DF86	Contactless device	C(104)	.
FF00	Issuer script results	C(29)	.
56	Additional data	C(2)	C(2)
0001	Payment facilitator data	CQI(104)	.
0003	Brand selected	CQI(104)	.
0019	Serial number	CQI(104)	.
0020	Resend counter	CQI(104)	.
0024	Independent sales organisation	CQI(104)	.
0025	Payment facilitator identifier	CQI(104)	.
0026	Market place identifier	CQI(104)	.
0027	Final merchant identifier	CQI(104)	.
0040	List of installed kernels	CQI(104)	.
0056	Payment Account Reference	C(108)	C(108)
5F2D	Language preference	CQI(104)	.
9F0D	Issuer Action Code - Default	CQI(104)	.
9F0E	Issuer Action Code - Denial	CQI(104)	.
9F0F	Issuer Action Code - Online	CQI(104)	.
59	National data	C(2)	C(2)
0100	Function code	CQI(104)	.
0101	Message reason code	XS	FQ
0102	Transaction year	XS	FQ
0200	ERT (Regulatory and Technical Environment)	XQI	FQ
0201	ITP SA (Acceptance system terminal application identifier)	XQI	.
0202	Acceptor contract number	XQI	FQ
0203	Acceptance system logical number	XQI	FQ
0204	Point of interaction logical number	CQI(104)	.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment reversal request : **0400/0401** **B:** Response to payment reversal request : **0410**

N°	Définition	A	B
0205	Acceptance system country code	CQI(104)	.
0207	Cardholder total amount	CQI(104)	.
020B	TASA (Card acceptor application type)	XQI	.
0215	ITP PA (Point of interaction terminal application identifier)	CQI(104)	.
0216	Point of interaction extended logical number	CQI(104)	.
0417	Digital wallet additional data	CQI(104)	.
0418	Wallet identifier	CQI(104)	.
90	Original data elements	XS	FQ
95	Replacement amounts	XS	FQ
112	Funds transfer data	C(2)	.
01	Original transaction data	C(94)	.
03	Application type identifier	C(94)	.
08	funds transfer reason	CQI(104)	.
10	IBAN	CQI(104)	.
115	nexo data	C(2)	.
0001	nexo PoS identifier	CQI(104)	.
0002	nexo Acceptance System identifier	CQI(104)	.
0003	nexo certificate	CQI(104)	.
119	Reserved for national use	C(2)	C(2)
0047	Debit unique reference identifier	CQI(104)	.
00BC	Extended message to the transaction initiator	.	F

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Authorization request (via voice authorization center) : **0100** **B:** Response to authorization request via call center : **0110**

N°	Définition	A	B
1	Bit Map, extended	C(1)	C(1)
2	Primary Account Number	X	XQ
3	Processing code	X	XQ
4	Amount, transaction	X	XQ
7	Transmission date and time	FS	FS
11	Systems trace audit number	XS	XQ
12	Time, local transaction	XS	FQ
13	Date, local transaction	XS	FQ
14	Date, expiration	X	FQ
18	Merchant type	X	FQ
22	Point of service entry mode	X	FQ
23	Card sequence number	.	CQ(84)
25	Point of service condition code	X	FQ
27	Authorisation identification response length	C(7)	.
32	Acquiring institution identification code	X	XQ
33	Forwarding institution identification code	C(21)	FQ
35	Track 2 data	C(12)	.
37	Retrieval reference number	F	C(79)
38	Authorisation identification response	.	C(10)
39	Response code	.	XS
41	Card acceptor terminal identification	X	XQ
42	Card acceptor identification code	X	XQ
43	Card acceptor name/location	F	FQ
44	Additional response data	.	C(2)
AA	Incorrect field	.	C(69)
AB	Security error	.	C(12)
AC	Field conversion	.	F
AF	Service activation code	.	F
BB	Telephone number	.	F
BC	Message to the transaction initiator	.	F
CA	Track or equivalent data cryptogram processing information	.	C(12)
CB	Application cryptogram verification results	.	C(12)
47	Additional data - national	C(2)	C(2)
08	Location category code	C(63)	FQ
33	CB2A specification date	C(3)	.
96	SIRET	C(63)	FQ
97	IDPA	C(63)	FQ
A0	IDSA (card acceptor terminal identifier)	C(63)	FQ
49	Currency code, transaction	X	XQ
53	Security related control information	X	X
55	Integrated circuit card system related data	.	C(2)
0071	Issuer Script Template 1	.	C(24)

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Authorization request (via voice authorization center) : **0100** **B:** Response to authorization request via call center : **0110**

N°	**Définition**	**A**	**B**
0072	Issuer Script Template 2	.	C(24)
0091	Issuer Authentication Data	.	C(24)
5F24	Application expiration date	.	FQ
DF80	ICC processing results	.	FQ
DF81	Card application type	.	FQ
59	National data	C(2)	C(2)
0100	Function code	C(47)	FQ
0101	Message reason code	X	FQ
0102	Transaction year	XS	CQ(95)
0200	ERT (Regulatory and Technical Environment)	X	FQ
0201	ITP SA (Acceptance system terminal application identifier)	X	FQ
0202	Acceptor contract number	X	FQ
0203	Acceptance system logical number	X	FQ
0204	Point of interaction logical number	C(22)	FQ
0205	Acceptance system country code	C(63)	FQ
0207	Cardholder total amount	X	FQ
020B	TASA (Card acceptor application type)	X	FQ
0300	Card security code	C(11)	.

N°	COMMENTAIRES
1	Mandatory if one of fields 65 to 128 is present
2	See list of types
3	Mandatory if available
5	Mandatory for debit transaction
7	Mandatory if Acceptor cannot receive "Authorisation, identification response" up to six digits
9	Mandatory if present in the request, otherwise absent
10	Mandatory if authorisation granted, otherwise optional
11	Mandatory if transaction is made via a call center
12	Must be absent
21	Mandatory in case of one or more intermediaries between Acceptor and Acquirer, otherwise absent
22	Mandatory for a clustered or concentrated system, otherwise absent
24	Mandatory if EMV transaction or contactless EMV transaction and if provided by Issuer, otherwise absent
29	Mandatory if available, otherwise absent
30	Mandatory if PIN is present, otherwise absen
31	Mandatory if DUKPT used to encrypt the PIN
32	Mandatory if remote PIN verification, otherwise absent
46	Mandatory if needed to identifiy the corresponding service
47	Mandatory for debit transaction in case of a pre-authorisation, additional invoice, cumulative amount or unattended terminal with network access
48	Mandatory if available for a contactless transaction
49	Mandatory for contactless transactions, otherwise absent
63	Mandatory if data element was provided to the system (parameters downloading), otherwise absent
69	Mandatory if "response code"=30, optional if "response code"=12, 13 or 20, otherwise absent
79	Mandatory in the response if present in the request (identical value to request), or if managed by the Acquirer, otherwise absent
84	Mandatory if present in card application, otherwise absent
85	Mandatory for a debit transaction if present in the card application, mandatory if available for a credit transaction
94	Mandatory for a funds transfer transaction
95	Mandatory if field 13 is present, otherwise absent
101	Mandatory for contactless transactions or if pre-authorisation
104	Mandatory if present in the initial request
106	Mandatory if response code = 30
108	May be present. Presence conditions are specific to each scheme.
115	Mandatory for partial authorisation
116	Mandatory if present in the initial response
117	Mandatory if reversals management capability
118	Mandatory if at least one of the following amount types is present
119	Mandatory for transaction with tip
127	Mandatory for a contact transaction, mandatory if available for a contactless transaction
128	Mandatory for a contact transaction, must be absent for a contactless transaction
135	Mandatory if the amount used for calculating the certificate is not available in other data elements of the message
138	Mandatory if the date used for calculating the certificate is not available in other data elements of the message
145	Mandatory for a debit transaction in case of a pre-authorisation, additional invoice, cumulative amount or unattended terminal with network access; mandatory if available for an Original Credit
147	Mandatory if available for an Original Credit
150	Mandatory if a cumulative authorisation is calculated for an unattended terminal with network access otherwise mandatory if available
151	Mandatory for a clustered or concentrated system and if field 59 type 0216 is absent, otherwise absent
152	Mandatory for a clustered or concentrated system and if field 59 type 0204 is absent, otherwise absent

N°	COMMENTAIRES
153	Mandatory if available for a contactless transaction if required by the used scheme
154	Mandatory if required by the BDK key identifier type (byte 1 of field 48 type 0002), otherwise absent
156	Mandatory if available for a credit transaction
160	Mandatory for a debit transaction, mandatory if available for a contactless credit transaction
161	Mandatory if field 119 type 0801 is present and field 119 type 0803 is absent
162	Mandatory if field 119 type 0801 is present and field 119 type 0802 is absent
165	Mandatory if present in the card application and if function code not equal to 104 and 105 (resubmission), otherwise absent

REMOTE PAYMENT

SECURED ELECTRONIC COMMERCE

TABLE OF CONTENTS

1. INTRODUCTION

The present volume describes the following:

- Non-secure remote payment
- Secured electronic commerce
- Recurring payment
- Remote payment for the reservation and rental of goods or services

The purpose of this service is to:

- request a debit or credit authorisation related to remote payment
- obtain a response to this authorisation request (approval or reason for decline)
- reverse an authorisation previously granted to inform the issuer of the final transaction amount
- obtain the response to this reversal request.

Message type identifier:

- request message = authorisation request: 0100
- response message = authorisation request response: 0110
- request message = authorisation reversal request: 0400
- request message = authorisation reversal repeat request: 0401
- response message = authorisation reversal request response: 0410

2. RESPONSE CODES

A response code (field 39) returned in a response message generates an action by the receiver.

Only significant and commonly used response codes are presented in the tables below.

2.1. RESPONSE CODES FOR A REMOTE PAYMENT AUTHORISATION REQUEST

No.	Description
00	Successful approval/completion
02	Refer to card issuer
03	Invalid merchant
04	Pickup
05	Do not honour
07	Pickup card, special conditions
08	Honour with cardholder identification
10	Approved for partial amount
12	Invalid transaction
13	Invalid amount
14	Invalid card number (no such number)
15	No such issuer
20	Invalid response (error in server domain)
30	Format error
31	Bank not supported by switch
33	Expired card
34	Suspected fraud
41	Lost card
43	Stolen card
46	Business specific error
51	Insufficient funds or credit limit exceeded
54	Expired card
56	No card record
57	Transaction not permitted to cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
60	Card acceptor contact acquirer
62	Restricted card
63	Security violation
68	Response received too late
6P	Verification data failed
77	Closed account
78	Blocked, first used or special condition—new cardholder not activated or card is temporarily blocked
91	Issuer or switch is inoperative
93	Transaction cannot be completed-Violation of law
94	Duplicate transmission
96	System malfunction
97	General monitoring timeout
98	Server inaccessible (set by the server)
A1	Soft decline (electronic commerce only)
A4	Misused TRA exemption
R0	Stop payment order
R1	Revocation of all the recurring payments for card
R3	Revocation of all recurring payments for card

For information about the actions to be taken, refer to the specifications in MPE (Electronic Payment Manual).

2.2. RESPONSE CODES FOR A REMOTE PAYMENT REVERSAL REQUEST

No.	**Description**
00	Successful approval/completion
17	Customer cancellation
21	No action taken (unable to back out prior transaction)
32	Partial completion (ISO 8583)
99	Malfunction

2.3. RESPONSE CODES FOR A RESPONSE TO A REMOTE PAYMENT REVERSAL REQUEST

No.	Description
03	Invalid merchant or service provider
12	Invalid transaction
13	Invalid amount
14	Invalid PAN
15	No such issuer
20	Invalid response (error in server domain)
25	Unable to locate record in file
30	Format error
31	Unknown acquiring institution identification code
56	No card record
63	Security rules violation
90	Temporary system failure
91	Card issuer or network inaccessible/ Issuer unavailable or switch inoperative
94	Duplicate transmission
96	System malfunction
97	General monitoring timeout
98	Server inaccessible (set by the server)

3. REQUIREMENTS RELATED TO PAYMENTS FOR THE RESERVATION AND RENTAL OF GOODS AND SERVICES

3.1. AUTHORISATION REQUEST TRANSACTION RELATED TO REMOTE PAYMENT

The purpose of this transaction is to request an authorisation for remote payment.

The response to this authorisation request provides approval or the reason for decline.

Message type identifier:

- Request: 0100
- Response: 0110

Typical values for transactions with manual entry on an attended terminal:

Initial pre-authorisation :

- field 22 positions 1 and 2 (PAN entry mode) = 01 ‘Manual’
- field 56 type 0028 (Payment use case) = 06 ‘Reservation and rental payment’ or 07 ‘Pre-authorisation out of reservation and rental’
- field 59 type 0100 (Function code) = 101 (initial authorisation - estimated amount)
- field 59 type 0101 (Reason code) = 1655
- field 59 type 0200 (ERT*) = 80
- field 59 type 0800 (service attribute) = 2 ‘Pre-authorisation’

Additional charges :

- field 22 positions 1 and 2 (PAN entry mode) = 01 ‘Manual’
- field 56 type 0028 (Payment use case) = 06 ‘Reservation and rental payment’ or 07 ‘Pre-authorisation out of reservation and rental’
- field 59 type 0100 (Function code) = 163 (additional charges)
- field 59 type 0200 (ERT*) = 80
- field 59 type 0800 (service attribute) = 3 ‘Additional pre-authorisation’
- field 47 type 24 (file number) must be equal to that of the initial request
- field 47 type 99 (Original unique transaction identifier) must be equal to field 47 type 95 sentby the issuer in the response to the pre-authorisation request.

Typical values for additional charges on an unattended terminal:

- field 22 positions 1 and 2 (PAN entry mode) = 10 ‘Card on File’
- field 56 type 0028 (Payment use case) = 07 ‘Pre-authorisation out of reservation and rental’
- field 59 type 0100 (Function code) = 163 (additional charges)
- field 59 type 0200 (ERT*) = 57
- field 59 type 0800 (service attribute) = 3 ‘Additional pre-authorisation’
- field 47 type 24 (file number) must be equal to that of the initial request
- field 47 type 99 (Original unique transaction identifier) must be equal to field 47 type 95 sentby the issuer in the response to the pre-authorisation request.

Typical values for secured electronic commerce:

Initial pre-authorisation :

- field 56 type 0028 (Payment use case) = 06 ‘Reservation and rental payment’
- field 59 type 0100 (Function code) = 101 (initial authorisation - estimated amount)
- field 59 type 0101 (Reason code) = 1655
- field 59 type 0200 (ERT*) = 24

Additional charges :

- field 56 type 0028 (Payment use case) = 06 ‘Reservation and rental payment’
- field 59 type 0100 (Function code) = 163 (additional charges)
- field 59 type 0200 (ERT*) = 27
- field 47 type 24 (file number) must be equal to that of the initial request
- field 47 type 99 (Original unique transaction identifier) must be equal to field 47 type 95 sent by the issuer in the response to the pre-authorisation request.

* Regulatory and Technical Environment (ERT)

3.2. INFORMATION REQUEST

The purpose of this transaction is to request information about a PAN.

Message type identifier:

- Request: 0100
- Response: 0110

Typical values:

- field 4 (Amount) = 0
- field 59 type 0100 (Function code) = 108 (information request)
- field 59 type 0101 (Reason code) = 1655
- field 59 type 0200 (ERT*) = 80
- field 59 type 0800 (service attribute) = 2
  *Regulatory and Technical Environment (ERT)

4. REQUIREMENTS RELATED TO MULTIPLE PAYMENT

1. Cardholder Initiated Transactions

- **Except for mobile payment solutions based on EMV data elements,** an Internet Cardholder Initiated Transaction (ERT* = 24) must include the data elements listed below, **subject to the presence condition**.

  * ERT = Regulatory and Technical Environment

Data	**CB2A Authorisation field**
Cumulative total authorised amount	Field 54 type amount type 43
3DS protocol major version	Field 56 type 0022
Cryptogram entry date and GMT time	Field 56 type 0017
DS transaction ID	Field 56 type 0023 data element UUID applies to nomenclature 1
ACS transaction ID	Field 56 type 0023 data element UUID applies to nomenclature 2
Payment use case	Field 56 type 0028
Service attribute	Field 59 type 0800
Card-on-file action	Field 56 type 0029
Payment number	Field 56 type 0031
Total number of payments	Field 56 type 0032
Exemption indicator	Field 56 type 0033
Authentication merchant name	Field 56 type 0036
Authentication date	Field 56 type 0037
Authentication amount	Field 56 type 0038
Payment validity date	Field 56 type 0045
Function code	Field 59 type 0100
Card security code	Field 59 type 0300
Transaction identifier or cryptogram provided by the acceptor	Field 59 type 0400
Cardholder authentication value	Field 59 type 0401
Electronic commerce transaction authentication type	Field 59 type 0407
Cardholder authentication method used by the issuer	Field 59 type 0410
Electronic commerce cryptogram calculation method	Field 59 type 0411
Three-domain secure results	Field 59 type 0412
Additional electronic commerce data elements	Field 59 type 0414
Digital wallet name	Field 59 type 0415
Electronic commerce indicator	Field 59 type 0416
Digital wallet additional data	Field 59 type 0417
Wallet identifier	Field 59 type 0418
Three-domain secure results, others	Field 59 type 0419

- “Recurring payment transactions not made in secured electronic commerce mode” (ERT* = 28) do not contain neither specific electronic commerce data elements nor payment case identification data.

  *Regulatory and Technical Environment (ERT)

2. Subsequent Transactions

- Transactions subsequent to an initial electronic commerce transaction (ERT* = 27) must include the data elements listed below, **subject to the presence condition**.

  * ERT = Regulatory and Technical Environment

Data	**CB2A Authorisation field**	**CB2A Authorisation settings**
Original unique transaction identifier	Field 47 type 99	Same value as in field 47 type 95 of the initial transaction response
Debit unique transaction identifier	Field 119 type 0047	Same value as in field 47 type 95 of the initial debit transaction response
Cumulative total authorised amount	Field 54 type amount 43	Transaction specific value
Payment use case	Field 56 type 0028	Same value as in field 56 type 0028 of the initial transaction
Card-on-file action	Field 56 type 0029	Absent
Payment number	Field 56 type 0031	Transaction specific value
Total number of payments	Field 56 type 0032	Same value as in field 56 type 0032 of the initial transaction
Exemption indicator	Field 56 type 0033	Transaction specific value
Payment validity date	Field 56 type 0045	Same value as in field 56 type 0045 of the initial transaction
DS transaction ID	56 type 0023 data element UUID applies to nomenclature 1 of the initial transaction	Transaction specific value for 3RI MIT
	Field 56 type 0046/ DS transaction ID	Copy of field 56 type 0023 data element UUID applies to nomenclature 1 of the initial transaction (*)
ACS transaction ID	56 type 0023 data element UUID applies to nomenclature 2 of the initial transaction	Transaction specific value for 3RI MIT
	Field 56 type 0046/ ACS transaction ID	Copy of field 56 type 0023 data element UUID applies to nomenclature 2 of the initial transaction (*)
Authentication merchant name	Field 56 type 0036	Transaction specific value for 3RI MIT
	Field 56 type 0046/ Merchant name	Copy of field 56 type 0036 of the initial transaction (*)
Authentication date	Field 56 type 0037	Transaction specific value for 3RI MIT
	Field 56 type 0046/ Authentication date	Copy of field 56 type 0037 of the initial transaction (*)
Authentication amount	Field 56 type 0038	Transaction specific value for 3RI MIT
	Field 56 type 0046/ Authentication amount	Copy of field 56 type 0038 of the initial transaction (*)
Cardholder authentication value of the current transaction	Field 59 type 0401	Transaction specific value for 3RI MIT, otherwise absent
Electronic commerce transaction authentication type of the current transaction	Field 59 type 0407	Transaction specific value for 3RI MIT, otherwise absent
Cardholder authentication method used by the issuer of the current transaction	Field 59 type 0410	Absent
Electronic commerce cryptogram calculation method of the current transaction	Field 59 type 0411	Absent
Three-domain secure results of the current transaction	Field 59 type 0412	Transaction specific value for 3RI MIT, otherwise absent
Three-domain secure results, others of the current transaction	Field 59 type 0419	Transaction specific value for 3RI MIT, otherwise absent

Cardholder authentication value of the initial transaction	Field 59 type 0420/ Cardholder authentication value	Copy of field 59 type 0401 of the initial transaction(*)
Electronic commerce authentication type of the initial transaction	Field 59 type 0420/ Electronic commerce transaction authentication type	Copy of field 59 type 0407 of the initial transaction(*)
Cardholder authentication method of the initial transaction	Field 59 type 0420/ Cardholder authentication method	Copy of field 59 type 0410 de la transaction initiale(*)
Electronic commerce cryptogram calculation method of the initial transaction	Field 59 type 0420/ Cardholder authentication value calculation method	Copy of field 59 type 0411 of the initial transaction(*)
Result of using the secure remote payment architecture of the initial transaction	Field 59 type 0420/ Result of using a secured remote payment architecture	Copy of field 59 type 0412 of the initial transaction(*)
Extension of the result of the secure payment architecture of the initial transaction	Field 59 type 0420/ Extension of result of using a secured payment architecture	Copy of field 59 type 0419 of the initial transaction(*)

(*) If a data element is not significant, it is filled with the pad character specific to the format of the data element.

- “Recurring payment transactions not made in secured electronic commerce mode” (ERT* = 28) do not contain neither specific electronic commerce data elements nor payment case identification data.

* ERT = Regulatory and Technical Environment

5. REQUIREMENTS RELATED TO REVERSALS AND PARTIAL AUTHORISATIONS

Partial authorisation is performed in two steps:

- Indication in the authorisation request message that the merchant terminal supports partial authorisations (bit no. 1 in field 59 type 0805)
- Partial authorisation granted by the issuer

5.1. INFORMATION ON DATA ELEMENT VALUES

5.1.1. Fields 4 and 95

Field		Authorisation		Reversal	
No.	Field name	Request	Response.	Request	Response.
4	Transaction amount	Authorisation amount Condition: X	Authorised amount Condition: X	Authorised amount Condition: X	Authorised amount Condition: XQ
95	Replacement amount			Final transaction amount Condition: X	Final transaction amount Condition: FQ

5.1.2. Field 3 in 0400/0401 messages

The value of field 3 is equal to that of the initial request.

5.1.3. Field 4 in 0110 messages

- For full authorisations, the value must be equal to the value in the request.
- For partial authorisations (field 39=10), the value must be equal to the authorised amount.

5.1.4. Field 4 in 0400 messages

- The value must be equal to that of the request.
- If there is no response to the authorisation request, the value must be equal to the value in the request.

5.1.5. Field 95 in 0400 messages

- When the final transaction amount is equal to the authorised amount (reversal with no effect), the value must be equal to the value of field 4 (transaction amount).
- When the final transaction amount is equal to zero (full reversal), the value of this field must be equal to zero.

6. REQUIREMENTS RELATED TO CARD VALIDITY CHECK

The purpose of this transaction is to request information about a cardholder PAN (Primary Account Number).

Message type identifier:

- Request: 0100
- Response: 0110

Typical values:

- field 4 (Amount) = 0
- field 59 type 0100 (Function code) = 108 (card validity check)

The following specific values indicate a wallet registration:

- field 59 type 100 (Function code) set to 108 (card validity check)
- field 4 (Amount) set to 0
- field 59 type 0418 (Wallet Identifier) set to the identifier

The following specific values indicate a card validity check before shipment:

- field 59 type 100 set to 108
- field 4 set to 0
- field 56 type 0028 (Payment use case) = 04 (Shipment payment)

7. REQUIREMENTS RELATED TO AGGREGATED TRANSACTIONS

The purpose of this transaction is to request a pre-authorisation for a maximum amount. The transaction is then completed when the actual amount of the purchases is known or when the maximum amount is reached.

Message type identifier:

- Request: 0100
- Response: 0110

Typical values:

- field 59 type 0100 (Function code) = 101 (estimated amount)
- field 59 type 0101 (Message reason code) = 1679 (Provision for cumulative amounts)
- field 59 type 0800 (Service attribute) = ‘5’ (Cumulative invoice)

8. MESSAGE DESCRIPTIONS

<u>How to read the tables:</u>

The term "transaction" refers to a request/response.
The term "message" refers to either a request or to a response.

<u>Data field presence conditions</u>

X	Mandatory
C	Conditional: the condition making this field mandatory is stated in a note (nn); in all other cases, the field is optional
F	Optional
.	The field may be present, but it is not processed by the receiver

Non-applicable - Field is not defined in the standard.
.

<u>Field values</u>

S	Message-specific value
Q	Value is equal to request value
QI	Value is equal to initial request value
RI	Value is equal to initial response value

<u>Note:</u>

- All fields undefined in CB2A Authorisation can be used, providing they are compliant with ISO 8583 (v87).
- The condition “Mandatory if available” means that the data element must be transported by the protocol when provided by the application.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Authorisation request : **0100** **B:** Response to authorization request : **0110**

N°	Définition	A	B
1	Bit Map, extended	C(1)	C(1)
2	Primary Account Number	XS	XQ
3	Processing code	XS	XQ
4	Amount, transaction	XS	XQ
7	Transmission date and time	C(117)	.
11	Systems trace audit number	XS	XQ
12	Time, local transaction	XS	FQ
13	Date, local transaction	XS	FQ
14	Date, expiration	XS	FQ
18	Merchant type	XS	FQ
22	Point of service entry mode	XS	FQ
23	Card sequence number	C(141)	CQ(141)
25	Point of service condition code	XS	FQ
27	Authorisation identification response length	C(7)	.
32	Acquiring institution identification code	XS	XQ
33	Forwarding institution identification code	C(21)	FQ
37	Retrieval reference number	C(23)	C(79)
38	Authorisation identification response	.	C(10)
39	Response code	.	XS
41	Card acceptor terminal identification	XS	XQ
42	Card acceptor identification code	XS	XQ
43	Card acceptor name/location	C(159)	.
44	Additional response data	.	C(2)
AA	Incorrect field	.	C(69)
AB	Security error	.	C(12)
AC	Field conversion	.	FS
AF	Service activation code	.	FS
BB	Telephone number	.	FS
BC	Message to the transaction initiator	.	FS
CA	Track or equivalent data cryptogram processing information	.	C(12)
CB	Application cryptogram verification results	.	C(12)
CC	Cardholder address checking information	.	C(3)
CD	Information related to liability shift	.	F
47	Additional data - national	C(2)	C(2)
08	Location category code	C(63)	FQ
24	File number	C(146)	CQ(146)
33	CB2A specification date	C(3)	.
95	Unique transaction identifier	.	C(3)
96	SIRET	C(63)	FQ
97	IDPA	C(63)	FQ
99	Original unique transaction identifier	C(3)	F
A0	IDSA (card acceptor terminal identifier)	C(63)	FQ

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Authorisation request : **0100**	**B:** Response to authorization request : **0110**

N°	**Définition**	**A**	**B**
49	Currency code, transaction	XS	XQ
53	Security related control information	XS	XS
54	Additionnal amounts	C(118)	.
43	Cumulative total authorised amount	C(3)	.
55	Integrated circuit card system related data	C(2)	.
0082	Application Interchange Profile (AIP)	C(148)	.
0095	Terminal Verification Results (TVR)	C(148)	.
009A	Terminal Transaction Date	C(139)	.
009C	Transaction type	C(148)	.
9F02	Amount, authorized	C(140)	.
9F10	Issuer application data	C(148)	.
9F26	Application Cryptogram	C(136)	.
9F27	Cryptogram Information Data (CID)	C(148)	.
9F33	Terminal capabilities	C(4)	.
9F36	Application Transaction Counter (ATC)	C(148)	.
9F37	Unpredictable Number	C(148)	.
56	Additional data	C(2)	C(2)
0001	Payment facilitator data	C(3)	.
0002	Application selection indicator	C(3)	.
0003	Brand selected	C(3)	.
0005	Acceptance system card product code	C(3)	.
0006	Cardholder address	C(3)	.
0008	Cardholder postcode	C(3)	.
0009	Delivery address	C(3)	.
0010	IP address	C(3)	.
0011	Number of articles	C(3)	.
0012	Mobile payment solution identifier	C(137)	.
0013	Type of transaction	C(137)	.
0014	Type of proof	C(137)	.
0017	Cryptogram entry date and GMT time	C(3)	.
0018	Card type indicator	.	C(12)
0019	Serial number	C(3)	.
0020	Resend counter	C(158)	.
0022	3DS protocol major version	C(155)	.
0023	UUID container	C(103)	.
0024	Independent sales organisation	C(3)	.
0025	Payment facilitator identifier	C(3)	.
0026	Market place identifier	C(3)	.
0027	Final merchant identifier	C(3)	.
0028	Payment use case	C(3)	.
0029	Card-on-file action	C(3)	.
0031	Payment number	C(3)	.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Authorisation request : **0100**	**B:** Response to authorization request : **0110**

N°	**Définition**	**A**	**B**
0032	Total number of payments	C(3)	.
0033	Exemption indicator	C(3)	.
0036	Merchant name	C(157)	.
0037	Authentication date	C(157)	.
0038	Authentication amount	C(157)	.
0045	Payment validity date	C(3)	.
0046	Additional data - initial transaction electronic commerce	C(3)	.
0056	Payment Account Reference	.	C(108)
59	National data	C(2)	C(2)
0100	Function code	C(98)	FQ
0101	Message reason code	XS	FQ
0102	Transaction year	XS	CQ(95)
0200	ERT (Regulatory and Technical Environment)	XS	FQ
0201	ITP SA (Acceptance system terminal application identifier)	XS	FQ
0202	Acceptor contract number	X	FQ
0203	Acceptance system logical number	XS	FQ
0204	Point of interaction logical number	C(22)	FQ
0205	Acceptance system country code	C(148)	.
0207	Cardholder total amount	C(6)	FQ
020B	TASA (Card acceptor application type)	X	FQ
0215	ITP PA (Point of interaction terminal application identifier)	C(3)	FQ
0300	Card security code	C(130)	C(12)
0301	Card security code verification result	.	C(12)
0400	Transaction identifier or cryptogram supplied by the acceptor	C(99)	.
0401	Cardholder authentication value	C(122)	.
0407	Electronic commerce authentication type	C(17)	.
0409	Cardholder authentication value processing information	.	C(12)
0410	Cardholder authentication method	C(3)	.
0411	Cardholder authentication value calculation method	C(29)	.
0412	Three-domain secure results	C(102)	.
0413	Modified electronic commerce authentication type	.	C(29)
0414	Additional electronic commerce data elements	C(133)	.
0415	Digital wallet name	C(125)	.
0416	Electronic commerce indicator	C(29)	C(163)
0417	Digital wallet additional data	C(132)	.
0418	Wallet identifier	C(134)	.
0419	Three-domain secure results, others	C(149)	FQ
0420	Data related to initial electronic commerce transaction	C(3)	.
0800	Service attribute	C(46)	FQ
0802	Risk scoring service	.	C(3)
0805	Optional services supported (acceptor domain)	C(3)	.
112	Funds transfer data	C(2)	.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Authorisation request : **0100**	**B:** Response to authorization request : **0110**

N°	Définition	A	B
01	Original transaction data	C(94)	.
03	Application type identifier	C(94)	.
05	Payer account number	C(142)	.
06	Counterparty PAN	C(142)	.
07	Counterparty last name and first name	C(144)	.
08	funds transfer reason	C(147)	.
09	BIC	F	.
10	IBAN	C(147)	.
115	nexo data	C(2)	.
0001	nexo PoS identifier	C(3)	.
0002	nexo Acceptance System identifier	C(3)	.
0003	nexo certificate	C(3)	.
119	Reserved for national use	C(2)	C(2)
0001	Merchant tokenisation indicator	C(3)	.
0009	Scheme program merchant identifier	C(3)	.
0013	Three-domain secure components availability	C(3)	.
0015	Token authentication verification value	C(3)	.
0016	Extended Electronic Commerce Indicator	.	C(163)
0017	Authentication exemption status indicator	.	C(164)
0022	3DS protocol version number	C(155)	.
0028	Remote commerce acceptor identifier	C(163)	.
0041	Purchase identifier type	C(29)	.
0042	Purchase identifier	C(29)	.
0047	Debit unique reference identifier	C(156)	F
00BC	Extended message to the transaction initiator	.	F
0208	Pre-authorisation duration	C(63)	.
0359	Transaction eligible for token services	.	C(164)
0801	Reattempt indicator	.	C(3)
0802	Reattempt frozen period	.	C(161)
0803	Reattempt conditions	.	C(162)
9F19	Token Requestor ID	C(3)	.
9F25	Last four digits of PAN	.	C(3)

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment reversal request : **0400/0401** **B:** Response to payment reversal request : **0410**

N°	Définition	A	B
1	Bit Map, extended	C(1)	C(1)
2	Primary Account Number	XQI	XQ
3	Processing code	XQI	XQ
4	Amount, transaction	X	XQ
7	Transmission date and time	XS	FS
11	Systems trace audit number	XS	XQ
12	Time, local transaction	XS	FQ
13	Date, local transaction	XS	FQ
14	Date, expiration	XQI	FQ
18	Merchant type	XQI	FQ
22	Point of service entry mode	XQI	FQ
23	Card sequence number	FQI	.
25	Point of service condition code	XQI	FQ
32	Acquiring institution identification code	XQI	XQ
33	Forwarding institution identification code	C(21)	FQ
37	Retrieval reference number	CRI(116)	FQ
38	Authorisation identification response	CRI(10)	.
39	Response code	XS	XS
41	Card acceptor terminal identification	XQI	XQ
42	Card acceptor identification code	XQI	XQ
43	Card acceptor name/location	CQI(104)	.
44	Additional response data	.	C(2)
AA	Incorrect field	.	C(106)
AB	Security error	.	C(12)
AC	Field conversion	.	F
AF	Service activation code	.	F
BC	Message to the transaction initiator	.	F
47	Additional data - national	C(2)	C(2)
08	Location category code	CQI(104)	FQ
24	File number	CQI(104)	FQ
33	CB2A specification date	CQI(104)	.
95	Unique transaction identifier	CRI(116)	FQ
96	SIRET	CQI(104)	FQ
97	IDPA	CQI(104)	FQ
99	Original unique transaction identifier	CQI(104)	.
A0	IDSA (card acceptor terminal identifier)	CQI(104)	FQ
49	Currency code, transaction	XQI	XQ
53	Security related control information	XS	XS
55	Integrated circuit card system related data	C(2)	.
0082	Application Interchange Profile (AIP)	FQI	.
0095	Terminal Verification Results (TVR)	FQI	.
009A	Terminal Transaction Date	FQI	.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment reversal request : **0400/0401** **B:** Response to payment reversal request : **0410**

N°	**Définition**	**A**	**B**
009C	Transaction type	FQI	.
9F02	Amount, authorized	FQI	.
9F10	Issuer application data	FQI	.
9F26	Application Cryptogram	FQI	.
9F27	Cryptogram Information Data (CID)	FQI	.
9F33	Terminal capabilities	CQI(104)	.
9F36	Application Transaction Counter (ATC)	FQI	.
9F37	Unpredictable Number	FQI	.
56	Additional data	C(2)	C(2)
0001	Payment facilitator data	CQI(104)	.
0003	Brand selected	CQI(104)	.
0005	Acceptance system card product code	CQI(104)	.
0012	Mobile payment solution identifier	CQI(104)	.
0019	Serial number	CQI(104)	.
0020	Resend counter	CQI(104)	.
0024	Independent sales organisation	CQI(104)	.
0025	Payment facilitator identifier	CQI(104)	.
0026	Market place identifier	CQI(104)	.
0027	Final merchant identifier	CQI(104)	.
0056	Payment Account Reference	C(108)	C(108)
59	National data	C(2)	C(2)
0100	Function code	CQI(104)	.
0101	Message reason code	XS	FQ
0102	Transaction year	XS	FQ
0200	ERT (Regulatory and Technical Environment)	XQI	FQ
0201	ITP SA (Acceptance system terminal application identifier)	XQI	.
0202	Acceptor contract number	XQI	FQ
0203	Acceptance system logical number	XQI	FQ
0204	Point of interaction logical number	CQI(104)	.
0205	Acceptance system country code	FQI	.
0207	Cardholder total amount	CQI(104)	.
020B	TASA (Card acceptor application type)	XQI	.
0215	ITP PA (Point of interaction terminal application identifier)	CQI(104)	.
0400	Transaction identifier or cryptogram supplied by the acceptor	CQI(104)	.
0401	Cardholder authentication value	CQI(104)	.
0407	Electronic commerce authentication type	CQI(104)	.
0411	Cardholder authentication value calculation method	CQI(104)	.
0412	Three-domain secure results	CQI(104)	.
0414	Additional electronic commerce data elements	CQI(104)	.
0415	Digital wallet name	CQI(104)	.
0416	Electronic commerce indicator	CQI(104)	.
0417	Digital wallet additional data	CQI(104)	.

X: Mandatory C: Conditional F: Optional .: Non-processed field S: Message specific value Q: Same value as in the initial request QI: Same value as in the initial request RI: Same value as in the initial response

A: Payment reversal request : **0400/0401** **B:** Response to payment reversal request : **0410**

N°	**Définition**	**A**	**B**
0418	Wallet identifier	CQI(104)	.
0419	Three-domain secure results, others	CQI(104)	.
0800	Service attribute	CQI(104)	.
90	Original data elements	XS	FQ
95	Replacement amounts	XS	FQ
112	Funds transfer data	C(2)	.
01	Original transaction data	CQI(104)	.
03	Application type identifier	CQI(104)	.
05	Payer account number	CQI(104)	.
06	Counterparty PAN	CQI(104)	.
07	Counterparty last name and first name	CQI(104)	.
08	funds transfer reason	CQI(104)	.
09	BIC	FQI	.
10	IBAN	CQI(104)	.
115	nexo data	C(2)	.
0001	nexo PoS identifier	CQI(104)	.
0002	nexo Acceptance System identifier	CQI(104)	.
0003	nexo certificate	CQI(104)	.
119	Reserved for national use	C(2)	C(2)
0047	Debit unique reference identifier	CQI(104)	.
00BC	Extended message to the transaction initiator	.	F

N°	COMMENTAIRES
1	Mandatory if one of fields 65 to 128 is present
2	See list of types
3	Mandatory if available
4	Mandatory if application type identifier = 20xx
6	Mandatory for debit transaction, mandatory if available for refund
7	Mandatory if Acceptor cannot receive "Authorisation, identification response" up to six digits
10	Mandatory if authorisation granted, otherwise optional
12	Must be absent
17	Mandatory for an electronic commerce debit transaction, mandatory if available for a refund,
21	Mandatory in case of one or more intermediaries between Acceptor and Acquirer, otherwise absent
22	Mandatory for a clustered or concentrated system, otherwise absent
23	Mandatory in case of pre-authorisation; if managed by the Acquirer; identical value for all related transactions
29	Mandatory if available, otherwise absent
46	Mandatory if needed to identifiy the corresponding service
63	Mandatory if data element was provided to the system (parameters downloading), otherwise absent
69	Mandatory if "response code"=30, optional if "response code"=12, 13 or 20, otherwise absent
79	Mandatory in the response if present in the request (identical value to request), or if managed by the Acquirer, otherwise absent
94	Mandatory for a funds transfer transaction
95	Mandatory if field 13 is present, otherwise absent
98	Mandatory for a debit transaction in case of a pre-authorisation, additional invoice, no-show transaction or cumulative amount, mandatory if available for a refund transaction
99	Mandatory if available and if field 59 type 0407 = 20
102	Mandatory for a debit transaction if e-commerce transaction security type = 20, mandatory if available for a refund,
103	Mandatory if available for CB 3DS v2 transaction
104	Mandatory if present in the initial request
106	Mandatory if response code = 30
108	May be present. Presence conditions are specific to each scheme.
116	Mandatory if present in the initial response
117	Mandatory if reversals management capability
118	Mandatory if at least one of the following amount types is present
122	Mandatory for all "3DS debit transactions authenticated with proof or certified authentication attempt"; mandatory for a debit transaction using an open wallet; otherwise absent
125	Mandatory if a digital wallet is used and if field 59 type 0418 is absent
130	Mandatory unless additional invoice
132	Mandatory if available for a digital wallet and if field 59 type 0418 is set, otherwise absent
133	Mandatory if field 59 type 0415 is set
134	Mandatory if a digital wallet is used and if field 59 type 0415 is absent, otherwise absent
136	Mandatory for a secured e-commerce debit transaction executed in EMV mode, otherwise absent
137	Mandatory if available and if a mobile payment solution is used, otherwise absent
139	Mandatory for a secured e-commerce debit transaction carried out in EMV mode and if the date used for calculating the certificate is not available in other data elements of the message, mandatory if available for a credit transaction, otherwise absent
140	Mandatory for a secured e-commerce debit transaction executed in EMV mode and if the date used for calculating the certificate is not available in other data elements of the message; mandatory if available for a credit transaction, otherwise absent
141	Mandatory if available for secured e-commerce transactions executed in EMV mode, otherwise absent
142	Mandatory for a card-to-card funds transfer
144	mandatory if available for a card-to-card funds transfer or an Original Credit
146	Mandatory for debit transaction in case of a pre-authorisation, additional invoice, cumulative amount; mandatory for a card-to-card

N°	COMMENTAIRES
	funds transfer or Original Credit; mandatory if available for an unattended terminal with network access; mandatory if available for a credit
147	Mandatory if available for an Original Credit
148	Mandatory for a secured electronic commerce debit transaction executed in EMV mode; mandatory if available for a credit transaction, otherwise absent
149	Mandatory if a 3DS v2 architecture is used
155	Mandatory if 3DS authentication
156	Mandatory if available for a credit transaction
157	Mandatory if provided by the implemented authentication solution
158	Mandatory for resubmission
159	Mandatory for a card-to-card funds transfer or if data element was provided to the system (parameters downloading), otherwise absent
161	Mandatory if field 119 type 0801 is present and field 119 type 0803 is absent
162	Mandatory if field 119 type 0801 is present and field 119 type 0802 is absent
163	Mandatory for some international schemes
164	May be sent by some international schemes