2AP Authorisation

Acceptor to Acquirer Protocol
(CB2A)

VOLUME 0 - INTRODUCTION

Version 1.6.6 - September 2025

TERMS OF USE

INTELLECTUAL PROPERTY RIGHTS

The intellectual property rights, including third-party's intellectual property rights, vested in these technical specifications are granted under a license of use. Any communication, distribution, reproduction, use or representation of this document, beyond the scope of the rights granted by FrenchSys, and by whatever means, is prohibited without the prior agreement of FrenchSys.

Trademarks, trade names or company names, logos and images referenced herein are used for identification or illustrative purpose only and remain the property of their respective owners.

DISCLAIMER AND LIMITATION OF LIABILITY

BY CONSULTING OR BY USING THIS SPECIFICATION, YOU AGREE ON YOUR BEHALF AND ON BEHALF OF EACH ENTITY AND PERSON ON BEHALF OF WHOM YOU ACT, TO BE LEGALLY BOUND BY THE TERMS OF USE DETAILED BELOW.

Whilst FrenchSys has used its best endeavors to make sure that the information, data, and other materials contained in this Specification are accurate and complete, and whilst this Specification aims to be in accordance with the relevant applicable laws, regulations, and directives, FrenchSys does not accept any liability for any error, omission, or non-conformance. Your use of this Specification and the information, data and other materials contained therein is at your own risk.

This Specification and the information, data and other materials contained therein are provided to you "AS IS", "WHERE IS" and "WITH ALL FAULTS", without warranty of any kind, and are not intended to provide, and do not constitute regulatory or legal advice to any individual or entity. It remains your sole responsibility to ensure that your use of this Specification, and the information, data and other materials contained therein are fully compliant to the relevant applicable laws, regulations, and directives in force.

FrenchSys will not be liable for any damages whatsoever (including, without limitation, incidental, consequential, indirect, or punitive damages, lost profits, or damages resulting from lost data or business interruption) resulting from your use of or inability to use this Specification and the information, data and other materials contained therein.

You agree to hold harmless FrenchSys from and against any and all claims, actions or demands, including costs and attorney's fees, arising from or in connection with your use of this Specification.

REVISION HISTORY

Version	Date	Content
1.6.6	September 2025	First version

Note: *This version has been generated through a different tool compared to previous versions, and may have some small presentation differences. However, if despite our best efforts, you spot any inconsistency, please contact us.*

Table of contents

1 OVERVIEW OF DOCUMENT

2AP 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
- Volume 3.4: Manual cash disbursment

2 PRESENTATION OF DOCUMENT

2.1 PREFACE

The present version includes all 2AP 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
- Manual cash disbursement
- 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 LIST OF CHANGES IN THIS VERSION

- XXXX - V1.0 - Editorial changes and fixes
- 1985 - V1.0 - Update of data for clearing
- 1986 - V1.0 - Authentication data quality indicator
- 1987 - V1.0 - Digital currency indicator
- 1988 - V1.0 - Response codes alignment
- 1989 - V1.0 - ‘Additional funds transfer data’ becomes ‘Industry specific data’
- 1990 - V1.0 - New CB2A Addendum for funds transfer
- 1991 - V1.0 - New additional amount type for AFT in CB2A common part
- 1992 - V1.0 - Payment facilitator address in CB2A common part
- 1993 - V1.0 - New data elements for AFT
- 1995 - V1.0 - New dataset format
- 1996 - V1.0 - New field for fleet data
- 1997 - V1.0 - New CB2A Addendum for fleet data
- 2006 - V1.0 - Merchant street address
- 2007 - V1.0 - New additional amount type for fleet in CB2A common part
- 2011 - V1.0 - Manual cash disbursement
- 2014 - V1.0 - Kernel 8 integration
- 2015 - V1.0 - New reason code for transit
- 2023 - V1.0 - New 3DS Challenge Indicator values
- 2039 - V1.0 - Paylib sunset

XXXX - V1.0 - EDITORIAL CHANGES AND FIXES

Context

Fixing typos and minor errors

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 59: National data *LLLVAR b...255*

...

⇨ ***TYPE = 0100: FUNCTION CODE*** *n3*

Value	Description
163	~~Additional charges~~ Delayed charges

⇨ ***TYPE = 0800: SERVICE ATTRIBUTE*** *n2*

Value	Description
03	~~Additional charges~~ Delayed charges

1985 - V1.0 - UPDATE OF DATA FOR CLEARING

Context

Visa references:

- Enhancements to global processing alignment GTLIG October 2024 - §1.2
- Requirement to support maximum processing data GTLIG October 2024 - § 3.20

A new field 119 type 1001 has been integrated in CB2A version 1.6.5 to save data from authorisation responses. It's completed with:

- the applied product platform
- the applied account type from
- the extended of clearing delay indicator

sent by Visa in authorisation responses.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 119: Reserved for national use *LL2VAR b...999*

...

⇨ ***TYPE = 1001: RESPONSE DATA FOR CLEARING*** *structure*

...

❑ **Applied product platform** _____ **an2**

❑ **Applied account type from** _____ **an2**

❑ **Extended authorisation indicator** _____ **an1**

❑ **Reserved for future use** _____ ~~**b0…14**~~ **b0…9**

1986 - V1.0 - AUTHENTICATION DATA QUALITY INDICATOR

Context

Reference: Changes to support secure data quality requirements GTLIG October 2024

Visa has created an indicator to inform merchants that the transaction has sufficient authentication data or not.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 119: Reserved for national use *LL2VAR b...999*

...

☐ **Data type** _____ **b2**

Value	Description
0040	Authentication data quality indicator

⇨ ***0040: AUTHENTICATION DATA QUALITY INDICATOR*** *an1*

This subfield indicates whether the transaction meets authentication data quality requirements.

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.1: Authorisation request and response

***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: Auth request: **0100**	**B**: Auth response: **0110**

N°	Definition	A	B
119 type 0040	Authentication data quality indicator	.	C (3)

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.3: Comments

N°	Comments
3	Mandatory if available

1987 - V1.0 - DIGITAL CURRENCY INDICATOR

Context

Visa reference: requirements to support digital currency transactions and ramp provider program GTLIG April 2025 - § 3.4

Visa created an indicator to identify transactions related to digital currency. It needs to be added in CB2A.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 119: Reserved for national use *LL2VAR b...999*

...

❑ **Data type** _____ **b2**

Value	Description
0035	Special condition indicator

⇨ ***0035: SPECIAL CONDITION INDICATOR*** *n1*

This subfield identifies the purchase of digital currency.

Value	Description
1	Purchase of Central Bank Digital Currency (CBDC) or Tokenized Deposits
2	Purchase of Stablecoin (Fiat-backed)
3	Purchase of Blockchain Native Token/Coin
4	Purchase of Non-Fungible Token (NFT)
7	Purchase of Cryptocurrency
8	Quasi-Cash
9	Payment on an existing debt

Volume 3.2 - Face-to-face payment – Unattended payment, section 6.1: Authorisation request and response

***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: Auth request EMV: **0100** **B**: Auth request Magstripe: **0100** **C**: Auth response: **0110**

N°	Definition	A	B	C
119 type 0035	Special condition indicator	C (3)	C (3)	.

Volume 3.2 - Face-to-face payment – Unattended payment, section 6.3: Reversal request and response

***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: Reversal request: **0400/0401**	**B**: Reversal response: **0410**

N°	Definition	A	B
119 type 0035	Special condition indicator	C (3)	.

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.1: Authorisation request and response

***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: Auth request: **0100**	**B**: Auth response: **0110**

N°	Definition	A	B
119 type 0035	Special condition indicator	C (3)	.

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.2: Reversal request and response

***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: Reversal request: **0400/0401**	**B**: Reversal response: **0410**

N°	Definition	A	B
119 type 0035	Special condition indicator	C (3)	.

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.3: Comments

N°	Comments
3	Mandatory if available

1988 - V1.0 - RESPONSE CODES ALIGNMENT

Context

Visa reference: changes to authorization response code GTLIG April 2025 - § 2.11

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

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 39: Response code *an2*

Value	Description
19	Re-enter transaction
39	No such account type
40	Requested function not supported
47	Restricted card
5C	Transaction not supported/blocked by issuer
64	Transaction does not fulfil Anti-Money Laundering requirement
79	Life cycle
80	Approved transaction without financial impact
83	Fraud/security
8P	Policy
9G	Blocked by cardholder/contact cardholder
62	~~Restricted card~~ Card invalid in region or country
82	~~Negative online CAM, dCVV, iCVV, or CVV results Or Offline PIN authentication interrupted~~ Incorrect CVV, dCVV, iCVV
93	~~Transaction cannot be completed-Violation of Law~~ Transaction cannot be completed - Violation of Law
96	~~System malfunction~~ System malfunction, no rerouting requested
A0	~~Fallback in contact mode~~ Fallback in EMV contact mode
A1	~~Soft decline, 3DS with challenge required (electronic commerce only)~~ Soft decline (electronic commerce only), 3DS with challenge required

Volume 3.2 - Face-to-face payment – Unattended payment, changed section 2.1: Response codes for a face-to-face payment authorisation request

See in document

Volume 3.2 - Face-to-face payment – Unattended payment, changed section 2.2: Response codes for an unattented payment authorisation request

See in document

Volume 3.2 - Face-to-face payment – Unattended payment, changed section 2.4: Response codes for a response to a reversal request related to a face-to-face payment authorisation request

See in document

Volume 3.3 - Remote payment – Secured electronic commerce, changed section 2.1: Response codes for a remote payment authorisation request

See in document

Volume 3.3 - Remote payment – Secured electronic commerce, changed section 2.2: Response codes for a remote payment reversal request

See in document

Volume 3.3 - Remote payment – Secured electronic commerce, changed section 2.3: Response codes for a response to a remote payment reversal request

See in document

1989 - V1.0 - 'ADDITIONAL FUNDS TRANSFER DATA' BECOMES 'INDUSTRY SPECIFIC DATA'

Context

The CB2A field 118 is renamed and will be used for data elements without functional description which will be added in specific addenda.

This year, all fields added for debit funds transfer in CB2A 1.6.5 are moved to a funds transfer dedicated addendum. Furthermore, all additional data elements requested by Visa this year are described in change sheets of this addendum.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

118: ~~Additional funds transfer data~~ Industry-specific data *LL2VAR b...999*

❑ ~~**Data type**~~ _____ ~~**b2**~~

⇨ ~~***0001 : AFT - Nomenclature***~~ ~~*an 1*~~

~~Indicates the network involved in the coding of data in the field.~~

⇨ ~~***1000 : Unique Transfer Reference***~~ ~~*ans 1...35*~~

~~Contains a unique reference to identify the funds transfer transaction.~~

⇨ ~~***1001 : AFT - Application Type Identifier***~~ ~~*an 1...3*~~

~~Identifies the type of application that initiated the transaction. Refer to each scheme rules.~~

⇨ ~~***1002 : Source of the funds***~~ ~~*n 2*~~

~~Source of the funds.~~

⇨ ~~***1003 : Transfer reason***~~ ~~*ans 1...35*~~

~~Reason for the transfer.~~

⇨ ~~***1004 : Label or message***~~ ~~*ans 1...65*~~

~~Text or a message.~~

⇨ ~~***1005 : Customer language***~~ ~~*ans 2...3*~~

~~Language used by the customer.~~

⇨ ~~***1006 : Customer language message***~~ ~~*b 1...50*~~

~~Message in the customer's language.~~

⇨ ~~**1007 : AGREEMENT ID**~~ ~~ans4~~

⇨ ~~**2000 : PAYER/PARTICIPANT IDENTIFIER**~~ ~~ans 1…35~~

~~Payer's participant identifier at the Payer side.~~

⇨ ~~**2001 : PAYER/PAN**~~ ~~n…19~~

~~Payer's PAN. Note : When the PAN has an odd number of positions, the first position is equal to 0 and that the first useful position is the second one.~~

⇨ ~~**2002 : PAYER/FIRST NAME**~~ ~~ans 1…35~~

~~Payer's first name.~~

⇨ ~~**2003 : PAYER/MIDDLE NAME**~~ ~~ans 1…35~~

~~Payer's middle name.~~

⇨ ~~**2004 : PAYER/LAST NAME**~~ ~~ans 1…35~~

~~Payer's last name.~~

⇨ ~~**2005 : PAYER/ADDRESS**~~ ~~ans 1…50~~

~~Payer's address.~~

⇨ ~~**2006 : PAYER/POSTCODE**~~ ~~ans 1…10~~

~~Payer's postal code.~~

⇨ ~~**2007 : PAYER/CITY**~~ ~~ans 1…25~~

~~Payer's city.~~

⇨ ~~**2008 : PAYER/STATE OR PROVINCE**~~ ~~ans 2…3~~

~~Payer's state or province.~~

⇨ ~~**2009 : PAYER/COUNTRY**~~ ~~ans 3~~

~~Payer's country.~~

⇨ ~~**2010 : PAYER/PHONE**~~ ~~ans 1…20~~

~~Payer's phone number.~~

~~⇨ **2011 : PAYER/BIRTH DATE** n 8~~

~~Payer's birth date (MMDDYYYY format).~~

~~⇨ **2012 : PAYER/BIC** ans 1…11~~

~~International Bank Identifier Code for the Payer's bank account.~~

~~⇨ **2013 : PAYER/IBAN** an…34~~

~~International Bank Account Number for the Payer's bank account.~~

~~⇨ **2014 : PAYER/ACCOUNT NUMBER** an 1…35~~

~~Payer's account number.~~

~~⇨ **2015 : PAYER/IDENTITY DOCUMENT** ans…4~~

~~Type of identity document used to identify the Payer.~~

~~⇨ **2016 : PAYER/ID NUMBER** ans…35~~

~~Number of the identity document used to identify the Payer.~~

~~⇨ **2017 : PAYER/ID COUNTRY CODE** ans 3~~

~~Issuing country code of the identity document used to identify the Payer.~~

~~⇨ **2018 : PAYER/NATIONALITY** ans 3~~

~~Nationality of the Payer.~~

~~⇨ **2019 : PAYER/ACCOUNT NUMBER TYPE** n2~~

~~Account number type of the payer.~~

~~⇨ **2020 : PAYER/IDENTITY SUB TYPE** an 2~~

~~⇨ **2021 : PAYER/ACCOUNT IDENTIFIER VALUE** ans34~~

~~⇨ **2022 : PAYER/ACCOUNT IDENTIFIER TYPE CODE** an2~~

~~⇨ **3001 : PAYEE/PAN** n…19~~

~~Payee's PAN. Note : When the PAN has an odd number of positions, the first position is equal to 0 and that the first useful position is the second one.~~

~~⇨ **3002 : PAYEE/FIRST NAME** ans 1…35~~

~~Payee's first name.~~

~~⇨ **3003 : PAYEE/MIDDLE NAME** ans 1…35~~

~~Payee's middle name.~~

~~⇨ **3004 : PAYEE/LAST NAME** ans 1…35~~

~~Payee's last name.~~

~~⇨ **3005 : PAYEE/ADDRESS** ans 1…50~~

~~Payee's address.~~

~~⇨ **3006 : PAYEE/POSTCODE** ans 1…10~~

~~Payee's postal code.~~

~~⇨ **3007 : PAYEE/CITY** ans 1…25~~

~~Payee's city.~~

~~⇨ **3008 : PAYEE/STATE OR PROVINCE** ans 2…3~~

~~Payee's state or province.~~

~~⇨ **3009 : PAYEE/COUNTRY** ans 3~~

~~Payee's country.~~

~~⇨ **3010 : PAYEE/PHONE** ans 1…20~~

~~Payee's phone number.~~

~~⇨ **3011 : PAYEE/BIRTH DATE** n 8~~

~~Payee's birth date (MMDDYYYY format).~~

~~⇨ **3012 : PAYEE/BIC** ans 1…11~~

~~International Bank Identifier Code for the payee's bank account.~~

~~⇨ **3014 : PAYEE/ACCOUNT NUMBER** an 1.35~~

~~Payee's account number.~~

~~⇨ **3015 : PAYEE/IDENTITY DOCUMENT** ans…4~~

~~Type of identity document used to identify the payee.~~

~~⇨ **3016 : PAYEE/ID NUMBER** ans…35~~

~~Number of the identity document used to identify the payee.~~

~~⇨ **3017 : PAYEE/ID COUNTRY CODE** ans 3~~

~~Issuing country code of the identity document used to identify the payee.~~

~~⇨ **3018 : PAYEE/NATIONALITY** ans 3~~

~~Nationality of the payee.~~

~~⇨ **3019 : PAYEE/ACCOUNT NUMBER TYPE** n2~~

~~Account number type of the payee.~~

~~⇨ **3020 : PAYEE/IDENTITY SUB TYPE** an 2~~

~~⇨ **3021 : PAYEE/ACCOUNT IDENTIFIER VALUE** ans34~~

~~⇨ **3022 : PAYEE/ACCOUNT IDENTIFIER TYPE CODE** an2~~

~~⇨ **3023 : PAYEE/TOKEN AUTHENTICATION FACTOR A** b1~~

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.1: Authorisation request and response

***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: Auth request: **0100**	**B**: Auth response: **0110**

N°	Definition	A	B
~~118 type 0001~~	~~Nomenclature~~	~~C (108)~~	~~.~~

N°	Definition	A	B
~~118 type 1000~~	~~Unique Transfer Reference~~	~~C (108)~~	~~-~~
~~118 type 1001~~	~~Application Type Identifier~~	~~C (108)~~	~~-~~
~~118 type 1002~~	~~Source of the funds~~	~~C (108)~~	~~-~~
~~118 type 1003~~	~~Transfer reason~~	~~C (108)~~	~~-~~
~~118 type 1004~~	~~Label or message~~	~~C (108)~~	~~-~~
~~118 type 1005~~	~~Customer language~~	~~C (108)~~	~~-~~
~~118 type 1006~~	~~Customer language message~~	~~C (108)~~	~~-~~
~~118 type 1007~~	~~Agreement ID~~	.	~~-~~
~~118 type 2000~~	~~Payer/Participant identifier~~	~~C (108)~~	~~-~~
~~118 type 2001~~	~~Payer/PAN~~	~~C (108)~~	~~-~~
~~118 type 2002~~	~~Payer/First name~~	~~C (108)~~	~~-~~
~~118 type 2003~~	~~Payer/Middle name~~	~~C (108)~~	~~-~~
~~118 type 2004~~	~~Payer/Last name~~	~~C (108)~~	~~-~~
~~118 type 2005~~	~~Payer/Address~~	~~C (108)~~	~~-~~
~~118 type 2006~~	~~Payer/Postcode~~	~~C (108)~~	~~-~~
~~118 type 2007~~	~~Payer/City~~	~~C (108)~~	~~-~~
~~118 type 2009~~	~~Payer/Country~~	~~C (108)~~	~~-~~
~~118 type 2010~~	~~Payer/Phone~~	~~C (108)~~	~~-~~
~~118 type 2011~~	~~Payer/Birth date~~	~~C (108)~~	~~-~~
~~118 type 2012~~	~~Payer/BIC~~	~~C (108)~~	~~-~~
~~118 type 2013~~	~~Payer/IBAN~~	~~C (108)~~	~~-~~
~~118 type 2015~~	~~Payer/Identity document~~	~~C (108)~~	~~-~~
~~118 type 2016~~	~~Payer/ID number~~	~~C (108)~~	~~-~~
~~118 type 2017~~	~~Payer/ID country code~~	~~C (108)~~	~~-~~
~~118 type 2018~~	~~Payer/Nationality~~	~~C (108)~~	~~-~~
~~118 type 2019~~	~~Payer/Account Number Type~~	~~C (108)~~	~~-~~
~~118 type 2020~~	~~Payer/Identity Sub Type~~	~~C (108)~~	~~-~~
~~118 type 2021~~	~~Payer/Account Identifier value~~	~~C (108)~~	~~-~~
~~118 type 2022~~	~~Payer/Account Identifier type code~~	~~C (108)~~	~~-~~
~~118 type 3001~~	~~Payee/PAN~~	~~C (108)~~	~~-~~
~~118 type 3002~~	~~Payee/First name~~	~~C (108)~~	~~-~~
~~118 type 3003~~	~~Payee/Middle name~~	~~C (108)~~	~~-~~
~~118 type 3004~~	~~Payee/Last name~~	~~C (108)~~	~~-~~
~~118 type 3005~~	~~Payee/Address~~	~~C (108)~~	~~-~~
~~118 type 3006~~	~~Payee/Postcode~~	~~C (108)~~	~~-~~
~~118 type 3007~~	~~Payee/City~~	~~C (108)~~	~~-~~
~~118 type 3008~~	~~Payee/State or province~~	~~C (108)~~	~~-~~
~~118 type 3009~~	~~Payee/Country~~	~~C (108)~~	~~-~~
~~118 type 3010~~	~~Payee/Phone~~	~~C (108)~~	~~-~~
~~118 type 3011~~	~~Payee/Birth date~~	~~C (108)~~	~~-~~
~~118 type 3012~~	~~Payee/BIC~~	~~C (108)~~	~~-~~

N°	Definition	A	B
~~118 type 3014~~	~~Payee/Account number~~	~~C (108)~~	~~-~~
~~118 type 3015~~	~~Payee/Identity document~~	~~C (108)~~	~~-~~
~~118 type 3016~~	~~Payee/ID number~~	~~C (108)~~	~~-~~
~~118 type 3017~~	~~Payee/ID country code~~	~~C (108)~~	~~-~~
~~118 type 3018~~	~~Payee/Nationality~~	~~C (108)~~	~~-~~
~~118 type 3019~~	~~Payee/Account Number Type~~	~~C (108)~~	~~-~~
~~118 type 3020~~	~~Payee/Identity Sub Type~~	~~C (108)~~	~~-~~
~~118 type 3021~~	~~Payee/Account Identifier value~~	~~C (108)~~	~~-~~
~~118 type 3022~~	~~Payee/Account Identifier type code~~	~~C (108)~~	~~-~~
~~118 type 3023~~	~~Payee/Token authentication factor A~~	~~C (108)~~	~~-~~

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.3: Comments

N°	Comments
108	May be present. Presence conditions are specific to each scheme.

1990 - V1.0 - NEW CB2A ADDENDUM FOR FUNDS TRANSFER

Context

In the common part of CB2A Authorisation, field 118 is renamed (refer to change sheet 1989).

All data elements dedicated for funds transfer are moved in a dedicated addendum.

For further details, please refer to this addendum.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

118: Industry-specific data *LL2VAR b...999*

Addendum - Funds Transfer, created section 1: Overview of document

See in document

Addendum - Funds Transfer, created section 2: Change sheets applicable to CB2A/2AP 1.6.5

See in document

Addendum - Funds Transfer, created section 3: Data fields dictionary for Funds transfer for international schemes

See in document

Addendum - Funds Transfer, created section 3.1: Alphabetical list

See in document

Addendum - Funds Transfer, created section 3.2: List by field number

See in document

Addendum - Funds Transfer, created section 3.3: Definition of data fields used

See in document

Addendum - Funds Transfer, created section 4: Messages description of remote funds transfers

See in document

Addendum - Funds Transfer, created section 4.1: Authorisation request and response

See in document

Addendum - Funds Transfer, created section 4.2: Reversal request and response

See in document

Addendum - Funds Transfer, created section 4.3: comments

See in document

1991 - V1.0 - NEW ADDITIONAL AMOUNT TYPE FOR AFT IN CB2A COMMON PART

Context

An occurrence of additional amount is used by Visa to convey the sender's AFT Foreign Exchange Markup Fee as assessed by the acquirer, service provider, or merchant (if applicable).

It’s added in CB2A and may be used only in CB2A funds transfer addendum.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 54: Additional amounts *LLLVAR an...120*

...

❑ **Amount type** _____ **n2**

Value	Description
95	Transfer service

1992 - V1.0 - PAYMENT FACILITATOR ADDRESS IN CB2A COMMON PART

Context

Visa requests the Payment Facilitator address to be integrated in CB2A in funds transfer exchanges.

This new data element is integrated in the common CB2A dictionary. It is described with further detail in CB2A funds transfer addendum.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

113: Payment Facilitator address *LL2VAR b...999*

Refer to Funds transfer addendum

1993 - V1.0 - NEW DATA ELEMENTS FOR AFT

Context

Visa references:

- Changes to support new data requirements in Visa Direct transaction GTLIG October 2024 - §3.2
- AFT data elements and processing rules

Visa requires additional information and the payment facilitator address in funds transfer authorization requests.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 113: Payment Facilitator address *LL2VAR b...999*

...

Field 118: Industry-specific data *LL2VAR b...999*

...

Addendum - Funds Transfer, section 4.1: Authorisation request and response

***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**: Authorisation response: **0110**

N°	Definition	A	B
113	Payment Facilitator address	C (2)	C (2)
113 type 0019	Payment Facilitator name	C (177)	.
113 type 0028	Payment Facilitator street address	C (177)	.
113 type 0029	Payment Facilitator city name	C (177)	.
113 type 0030	Payment Facilitator state/province code	C (177)	.
113 type 0031	Payment Facilitator postal code	C (177)	.
113 type 0032	Payment Facilitator country code	C (177)	.
118	Industry-specific data	C (2)	C (2)
~~118 type 1007~~	~~Agreement ID~~	.	C (108)
118 type 0019	Visa risk assessment data risk score	.	C (177)
~~118 type 0001~~	~~Nomenclature~~	C (108)	.
~~118 type 1000~~	~~Unique Transfer Reference~~	C (108)	.
~~118 type 1001~~	~~Application Type Identifier~~	C (108)	.
~~118 type 1002~~	~~Source of the funds~~	C (108)	.
~~118 type 1003~~	~~Transfer reason~~	C (108)	.
~~118 type 1004~~	~~Label or message~~	C (108)	.
~~118 type 1005~~	~~Customer language~~	C (108)	.
~~118 type 1006~~	~~Customer language message~~	C (108)	.

N°	Definition	A	B
~~118 type 2000~~	~~Payer/Participant identifier~~	C (108)	.
~~118 type 2001~~	~~Payer/PAN~~	C (108)	.
~~118 type 2002~~	~~Payer/First name~~	C (108)	.
~~118 type 2003~~	~~Payer/Middle name~~	C (108)	.
~~118 type 2004~~	~~Payer/Last name~~	C (108)	.
~~118 type 2005~~	~~Payer/Address~~	C (108)	.
~~118 type 2006~~	~~Payer/Postcode~~	C (108)	.
~~118 type 2007~~	~~Payer/City~~	C (108)	.
~~118 type 2008~~	~~Payer/State or province~~	C (108)	.
~~118 type 2009~~	~~Payer/Country~~	C (108)	.
~~118 type 2010~~	~~Payer/Phone~~	C (108)	.
~~118 type 2011~~	~~Payer/Birth date~~	C (108)	.
~~118 type 2012~~	~~Payer/BIC~~	C (108)	.
~~118 type 2013~~	~~Payer/IBAN~~	C (108)	.
~~118 type 2015~~	~~Payer/Identity document~~	C (108)	.
~~118 type 2016~~	~~Payer/ID number~~	C (108)	.
~~118 type 2017~~	~~Payer/ID country code~~	C (108)	.
~~118 type 2018~~	~~Payer/Nationality~~	C (108)	.
~~118 type 2019~~	~~Payer/Account Number Type~~	C (108)	.
~~118 type 2020~~	~~Payer/Identity Sub Type~~	C (108)	.
~~118 type 2021~~	~~Payer/Account Identifier value~~	C (108)	.
~~118 type 2022~~	~~Payer/Account Identifier type code~~	C (108)	.
~~118 type 3001~~	~~Payee/PAN~~	C (108)	.
~~118 type 3002~~	~~Payee/First name~~	C (108)	.
~~118 type 3003~~	~~Payee/Middle name~~	C (108)	.
~~118 type 3004~~	~~Payee/Last name~~	C (108)	.
~~118 type 3005~~	~~Payee/Address~~	C (108)	.
~~118 type 3006~~	~~Payee/Postcode~~	C (108)	.
~~118 type 3007~~	~~Payee/City~~	C (108)	.
~~118 type 3008~~	~~Payee/State or province~~	C (108)	.
~~118 type 3009~~	~~Payee/Country~~	C (108)	.
~~118 type 3010~~	~~Payee/Phone~~	C (108)	.
~~118 type 3011~~	~~Payee/Birth date~~	C (108)	.
~~118 type 3012~~	~~Payee/BIC~~	C (108)	.
~~118 type 3014~~	~~Payee/Account number~~	C (108)	.
~~118 type 3015~~	~~Payee/Identity document~~	C (108)	.
~~118 type 3016~~	~~Payee/ID number~~	C (108)	.
~~118 type 3017~~	~~Payee/ID country code~~	C (108)	.
~~118 type 3018~~	~~Payee/Nationality~~	C (108)	.
~~118 type 3019~~	~~Payee/Account Number Type~~	C (108)	.
~~118 type 3020~~	~~Payee/Identity Sub Type~~	C (108)	.

N°	Definition	A	B
~~118 type 3021~~	~~Payee/Account Identifier value~~	C (108)	.
~~118 type 3022~~	~~Payee/Account Identifier type code~~	C (108)	.
~~118 type 3023~~	~~Payee/Token authentication factor A~~	C (108)	.
~~118 type 2014~~	~~Payer/Account Number~~	C (108)	.
118 type 0018	Acceptor legal business name	C (108)	.
118 type 0201	National POS geographical data	C (108)	.
118 type 4012	Account owner nationality	C (177)	.
118 type 4013	Account owner country of birth	C (177)	.
118 type 4014	Account owner occupation	C (177)	.
118 type 4015	Account owner date of birth	C (177)	.
118 type 4016	Account owner email address personal	C (177)	.
118 type 4017	Account Owner Address Line 1	C (177)	.
118 type 4018	Account Owner Address Line 2	C (177)	.
118 type 4019	Account Owner Street Name	C (177)	.
118 type 4020	Account Owner Postal Code	C (177)	.
118 type 4021	Account Owner City Name	C (177)	.
118 type 4022	Account Owner Country Subdivision Code, Major	C (177)	.
118 type 4023	Account Owner Country	C (177)	.
118 type 4024	Account owner building	C (177)	.
118 type 4025	Account Owner Country Subdivision Code, Minor	C (177)	.

Addendum - Funds Transfer, section 4.3: comments

N°	Comments
2	See list of types
108	May be present. Presence conditions are specific to each scheme.
177	May be set for Visa funds transfer

1995 - V1.0 - NEW DATASET FORMAT

Context

To facilitate the integration of new data elements, a new format is created.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

104: Transaction specific data *LL2VAR b…999 (Datasets)*

Refer to Fleet addendum

Volume 2 - Data Fields Dictionary, created section 2.2.6.4: Dataset format

The format named ‘LL2VAR Dataset’ identifies a TLV field containing all subfields also defined with a TLV structure.

In this case, all subfields have a Dataset format with the following structure:

Total length of field	Dataset 1	…	Dataset n

Dataset 1								
Dataset 1 identifier	Dataset 1 length	Dataset 1 value = data elements of Dataset 1						
		Tag 1	Length 1	Value 1	…	Tag n	Length n	Value n

1996 - V1.0 - NEW FIELD FOR FLEET DATA

Context

A CB2A field is used for fleet data. It's integrated in the common CB2A dictionary. It's described with further detail in CB2A fleet addendum.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

104: Transaction specific data *LL2VAR b...999 (Datasets)*

Refer to Fleet addendum

1997 - V1.0 - NEW CB2A ADDENDUM FOR FLEET DATA

Context

Visa references:

- Request 14 Changes to Type of Purchase Field in Fuel Transactions (§3.13 GTLIG Oct 24),
- Request 25 Changes to Support Value Added Tax Documentation Indicators in Fleet Transactions (§9.3.3 GTLIG April 25),
- Request 32 Changes to Support Visa Fleet Merchant Discount Program in Europe and U.S. Regions (§4.9 GTLIG April 25)
- Request 42: Details and Use Case Examples for Visa Fleet

Creation of the Fleet data addendum that contains Visa specific data and the fleet data requested by Mastercard.

Visa data are created in CB2A Authorisation fields 104 and 118.

Please refer to this document.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

104: Transaction specific data *LL2VAR b...999 (Datasets)*

Refer to Fleet addendum

118: Industry-specific data *LL2VAR b...999*

Addendum - Fleet, created section 1: Overview of document

See in document

Addendum - Fleet, created section 2: Data fields dictionary for Funds transfer for international schemes

See in document

Addendum - Fleet, created section 2.1: Alphabetical list

See in document

Addendum - Fleet, created section 2.2: List by field number

See in document

Addendum - Fleet, created section 2.3: Definition of data fields used

See in document

Addendum - Fleet, created section 3: Messages description specific to fleet data

See in document

Addendum - Fleet, created section 3.1: Authorisation request and response

See in document

Addendum - Fleet, created section 3.2: Reversal request and response

See in document

Addendum - Fleet, created section 3.3: comments

See in document

2006 - V1.0 - MERCHANT STREET ADDRESS

Context

Merchant street address is requested by Visa in funds transfer and fleet data. This data is added in CB2A Authorisation common part.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 119: Reserved for national use *LL2VAR b...999*

...

❑ **Data type** _____ **b2**

Value	Description
0200	Merchant street address

⇨ ***0200: MERCHANT STREET ADDRESS*** *ans...99*

Volume 3.2 - Face-to-face payment – Unattended payment, section 6.1: Authorisation request and response

***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: Auth request EMV: **0100** **B**: Auth request Magstripe: **0100** **C**: Auth response: **0110**

N°	Definition	A	B	C
119 type 0200	Merchant street address	C (3)	C (3)	.

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.1: Authorisation request and response

***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: Auth request: **0100** **B**: Auth response: **0110**

N°	Definition	A	B
119 type 0200	Merchant street address	C (3)	.

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.3: Comments

N°	Comments
3	Mandatory if available

2007 - V1.0 - NEW ADDITIONAL AMOUNT TYPE FOR FLEET IN CB2A COMMON PART

Context

An occurrence of additional amount is used by Visa to convey some additional amounts associated with fleet cards :

- 4P - Additional transaction fee 1 for EV purposes
- 4Q - Additional transaction fee 2 for EV purposes
- 4G - Total Discount Amount for discount purposes

Equivalent amounts types are added in CB2A Authorisation common part.

4P and 4Q are already integrated in CBAE with Amount type values 88 and 89.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 54: Additional amounts *LLLVAR an...120*

...

❑ **Amount type** _____ **n2**

Value	Description
87	Total Discount Amount for discount purposes
88	Additional transaction fee 1
89	Additional transaction fee 2

Volume 3.2 - Face-to-face payment – Unattended payment, section 6.1: Authorisation request and response

***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: Auth request EMV: **0100** **B**: Auth request Magstripe: **0100** **C**: Auth response: **0110**

N°	Definition	A	B	C
54 type 87	Total Discount Amount for discount purposes	C (179)	C (179)	.
54 type 88	Additional transaction fee 1	C (179)	C (179)	.
54 type 89	Additional transaction fee 2	C (179)	C (179)	.

Volume 3.2 - Face-to-face payment – Unattended payment, section 6.3: Reversal request and response

***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: Reversal request: **0400/0401** **B**: Reversal response: **0410**

N°	Definition	A	B
54 type 87	Total Discount Amount for discount purposes	C (179)	.

N°	Definition	A	B
54 type 88	Additional transaction fee 1	C (179)	.
54 type 89	Additional transaction fee 2	C (179)	.
54	Additional amounts	C (118)	C (118)

Volume 3.2 - Face-to-face payment – Unattended payment, section 6.5: Comments

N°	Comments
118	Mandatory if at least one of the following amount types is present
179	May be present for Visa fleet

2011 - V1.0 - MANUAL CASH DISBURSEMENT

Context

A scheme opens a new service to allow a merchant to propose cash withdrawal in its shop. The service is opened for contact and contactless transactions.

The details of the location category code are added in the data dictionary and a new value “Manual cash disbursement’ is created to identify the new service.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 47: Additional data – National *LLVAR ans…255*

...

⇨ ***08: LOCATION CATEGORY CODE*** *ans…8*

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

This data element is related to the sales unit. It is used to specify a Point of Sale’s location.

Value	Description
VA	Agency sale
VB	On board sale
PR	Counter sale
RG	Manual cash at counter
RM	Manual cash in shop

Volume 3.4 - Manual Cash Disbursement , created section 1: Introduction

See in document

Volume 3.4 - Manual Cash Disbursement , created section 1.1: Overview

See in document

Volume 3.4 - Manual Cash Disbursement , created section 2: Response codes

See in document

Volume 3.4 - Manual Cash Disbursement , created section 2.1: Response codes for a manual cash disbursement authorisation request

See in document

Volume 3.4 - Manual Cash Disbursement , created section 2.2: Response codes for a manual cash disbursement reversal request

See in document

Volume 3.4 - Manual Cash Disbursement , created section 2.3: Response codes for a response to a reversal request related to a manual cash disbursment

See in document

Volume 3.4 - Manual Cash Disbursement , created section 3: Requirements related to contactless payment

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4: Requirements related to reversals

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4.1: Information on data element values

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4.1.1: Field 47 type 08 in all messages

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4.1.2: Fields 4 and 95

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4.1.3: Field 3 in 0400/0401 messages

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4.1.4: Field 4 in 0110 messages

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4.1.5: Field 4 in 0400 messages

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4.1.6: Field 54 in 0110 messages

See in document

Volume 3.4 - Manual Cash Disbursement , created section 4.1.7: Field 95 in 0400 messages

See in document

Volume 3.4 - Manual Cash Disbursement , created section 5: Messages description of remote funds transfers

See in document

Volume 3.4 - Manual Cash Disbursement , created section 5.1: Authorisation request and response

See in document

Volume 3.4 - Manual Cash Disbursement , created section 5.3: Comments

See in document

2014 - V1.0 - KERNEL 8 INTEGRATION

Context

A new EMV tag may be sent to the issuer for Kernel 8.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 55: Integrated circuit card system related data *LLLVAR b...255*

...

❑ **Data type** _____ **b2**

Value	Description
9F81	Card authenticated application data

⇨ ***9F81: CARD AUTHENTICATED APPLICATION DATA*** *b...128*

Volume 3.2 - Face-to-face payment – Unattended payment, section 6.1: Authorisation request and response

***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: Auth request EMV: **0100** **B**: Auth request Magstripe: **0100** **C**: Auth response: **0110**

N°	Definition	A	B	C
55 type 9F81	Card authenticated application data	C (3)	.	.

Volume 3.2 - Face-to-face payment – Unattended payment, section 6.5: Comments

N°	Comments
3	Mandatory if available

2015 - V1.0 - NEW REASON CODE FOR TRANSIT

Context

Alignment with Mobility Payments Manual 2025 : a new reason code is created.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 59: National data *LLLVAR b...255*

...

⇨ ***TYPE = 0101: MESSAGE REASON CODE*** *n4*

Value	Description
1676	High amount transaction

2023 - V1.0 - NEW 3DS CHALLENGE INDICATOR VALUES

Context

EMV 3DS 2.3.1.1 introduces new values for the "3DS Requestor Challenge Indicator" field. Those values are integrated into 2AP.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 59: National data *LLLVAR b...255*

...

⇨ ***TYPE = 0419: THREE-DOMAIN SECURE RESULTS OTHERS*** *Structure*

...

❑ **Merchant request for authentication** _____ **n2**

Value	Description
02	~~No authentication~~ No authentication requested
10	No authentication requested (low value exemption)
11	No authentication requested (Secure corporate payment exemption)
12	Authentication requested (Device Binding prompt requested if challenge required)
13	Authentication requested (Issuer requested)
14	Authentication requested (Merchant-initiated transactions)

2039 - V1.0 - PAYLIB SUNSET

Context

Paylib is removed from protocols.

Implementation

Volume 2 - Data Fields Dictionary, section 2.3.3: Definition of data fields used

Field 59: National data *LLLVAR b...255*

...

⇨ ~~***0414 : ADDITIONAL ELECTRONIC COMMERCE DATA ELEMENTS***~~ ~~*Structure*~~

❑ ~~**Nomenclature**~~ _____ ~~**an1**~~

~~Value 3~~

❑ ~~**Type of additional data**~~ _____ ~~**an2**~~

❑ ~~**Value of additional data**~~ _____ ~~**ans...37**~~

❑ ~~**Additional Authentication Method**~~ _____ ~~**an2**~~

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

❑ ~~**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'~~
~~X~~			~~X~~	~~01~~
~~X~~		~~X~~		~~02~~
~~X~~	~~X~~			~~03~~
			~~X~~	~~11~~
		~~X~~		~~12~~
	~~X~~			~~13~~

⇨ ~~***0415 : DIGITAL WALLET NAME***~~ ~~*an2*~~

~~The following table shows all values that can be used~~

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.1: Authorisation request and response

***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: Auth request: **0100**	**B**: Auth response: **0110**

N°	Definition	A	B
~~59 type 0414~~	~~Additional electronic commerce data elements~~	~~C~~	~~.~~
~~59 type 0415~~	~~Digital wallet name~~	~~C~~	~~.~~

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.2: Reversal request and response

***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: Reversal request: **0400/0401**	**B**: Reversal response: **0410**

N°	Definition	A	B
~~59 type 0414~~	~~Additional electronic commerce data elements~~	~~CQI~~	~~.~~
~~59 type 0415~~	~~Digital wallet name~~	~~CQI~~	~~.~~

Volume 3.3 - Remote payment – Secured electronic commerce, section 6.3: Comments

N°	Comments
~~125~~	~~Mandatory if a digital wallet is used and if field 59 type 0418 is 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~~ Mandatory if a digital wallet is used, otherwise absent

END OF DOCUMENT

2AP Authorisation

Acceptor to Acquirer Protocol
(CB2A)

VOLUME 1 - GENERAL PRINCIPLES

Version 1.6.6 - September 2025

Table of contents

1 INTRODUCTION

The present volume contains the following information:

- Purpose of the authorisation protocol
- General principles and role of CB2A/FP-2A Authorisation
- Examples of standard exchanges

2 PURPOSE OF AUTHORISATION PROTOCOL

The 2AP 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 2AP AUTHORISATION PROTOCOL

The 2AP Authorisation protocol and CP (ex 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:

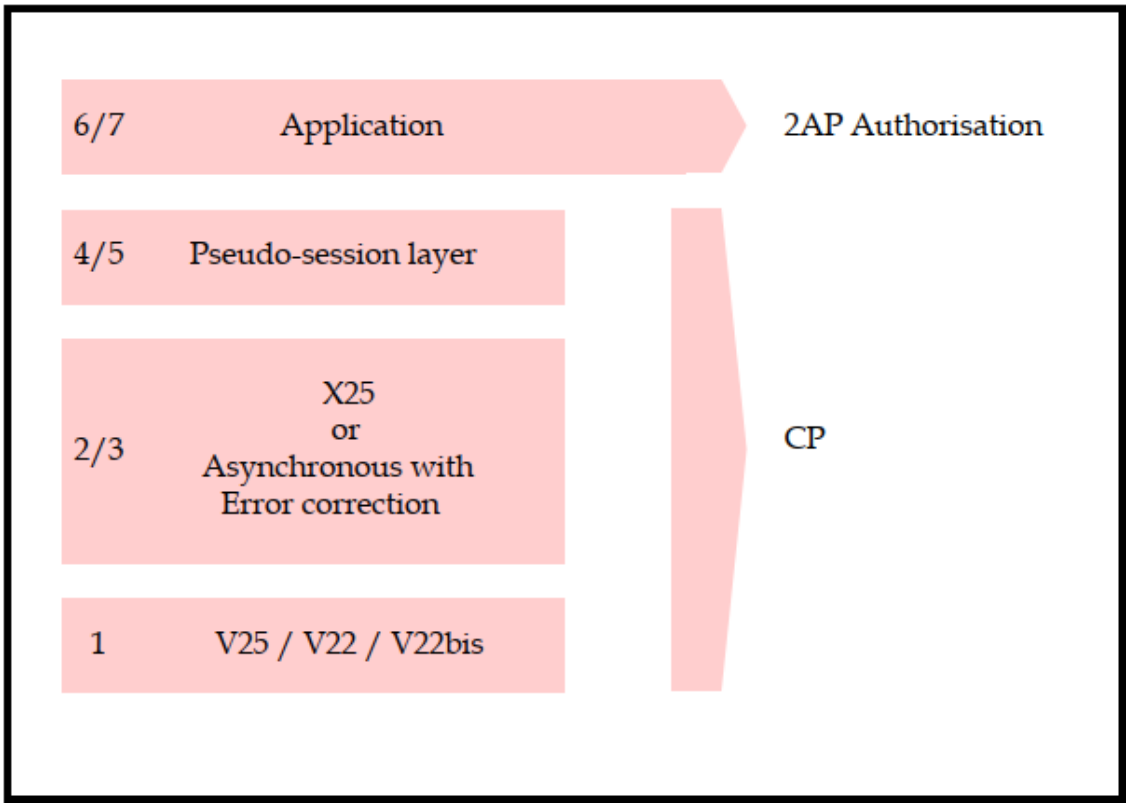


Figure: 2AP / OSI reference model

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 electronic payment software has been installed.

This definition includes stand-alone terminals, Online systems (Terminal + Server), systems with electronic payment software, 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 REQUEST

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.

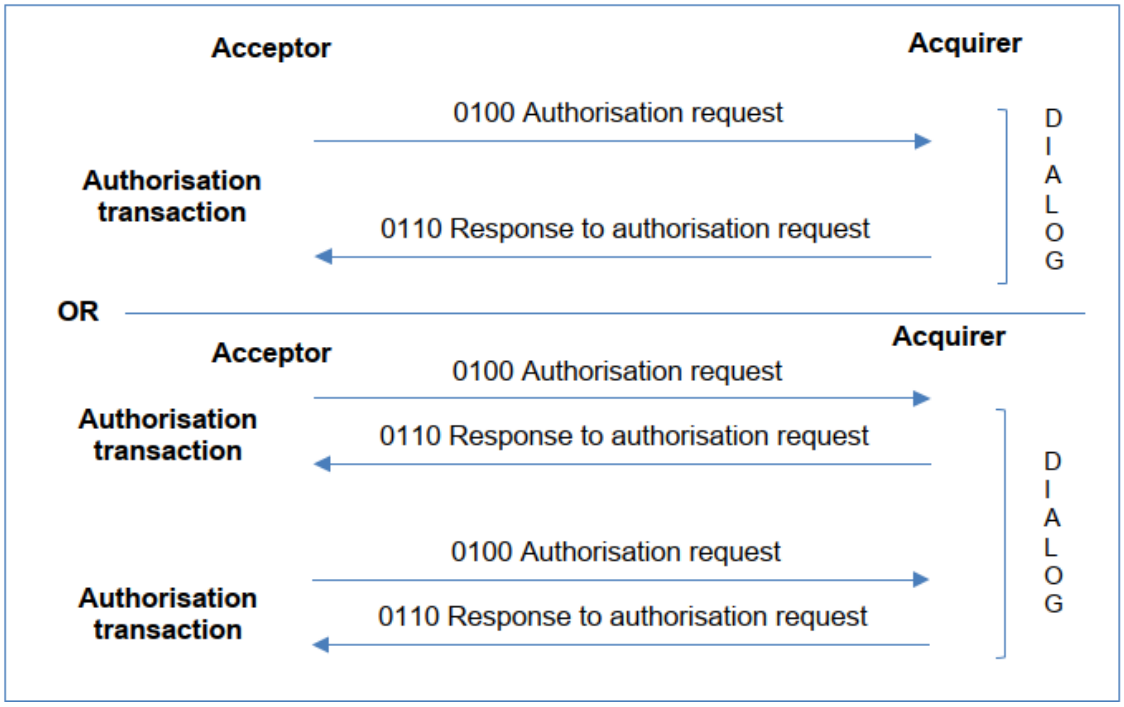


Figure: Authorisation - Dialog without network management

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.

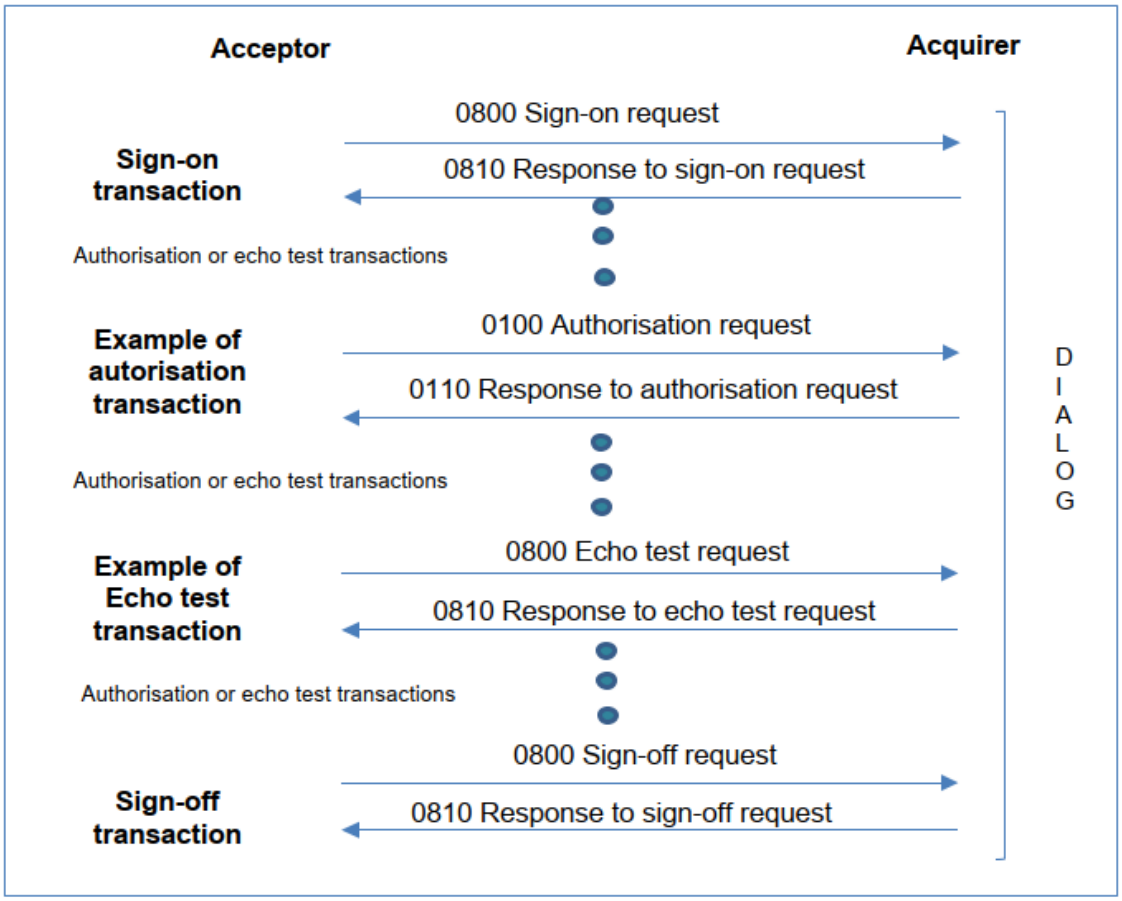


Figure: Authorisation - Dialog with network management

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.

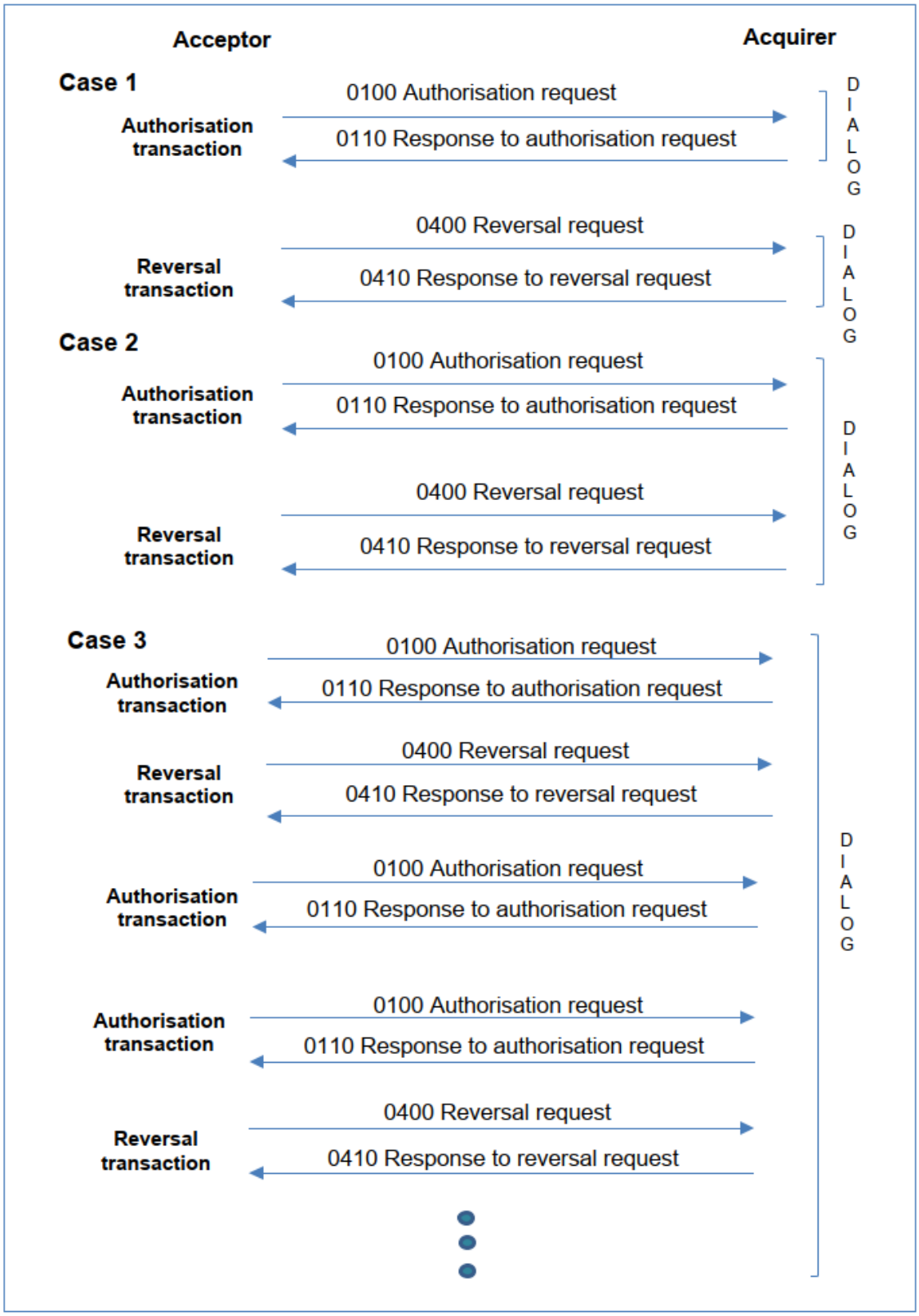


Figure: Reversal - Dialog without network management

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.

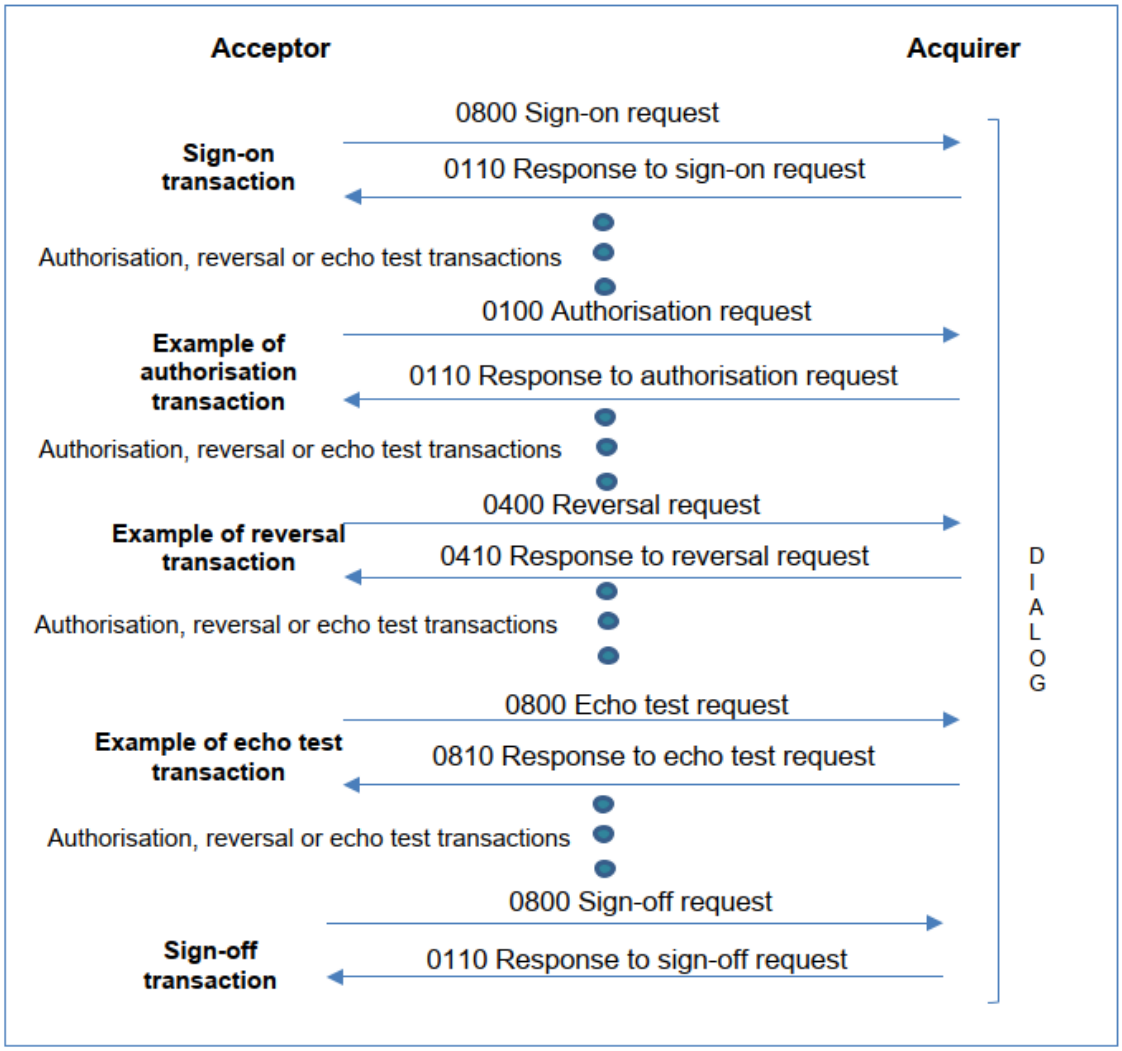


Figure: Reversal - Dialog with network management

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).

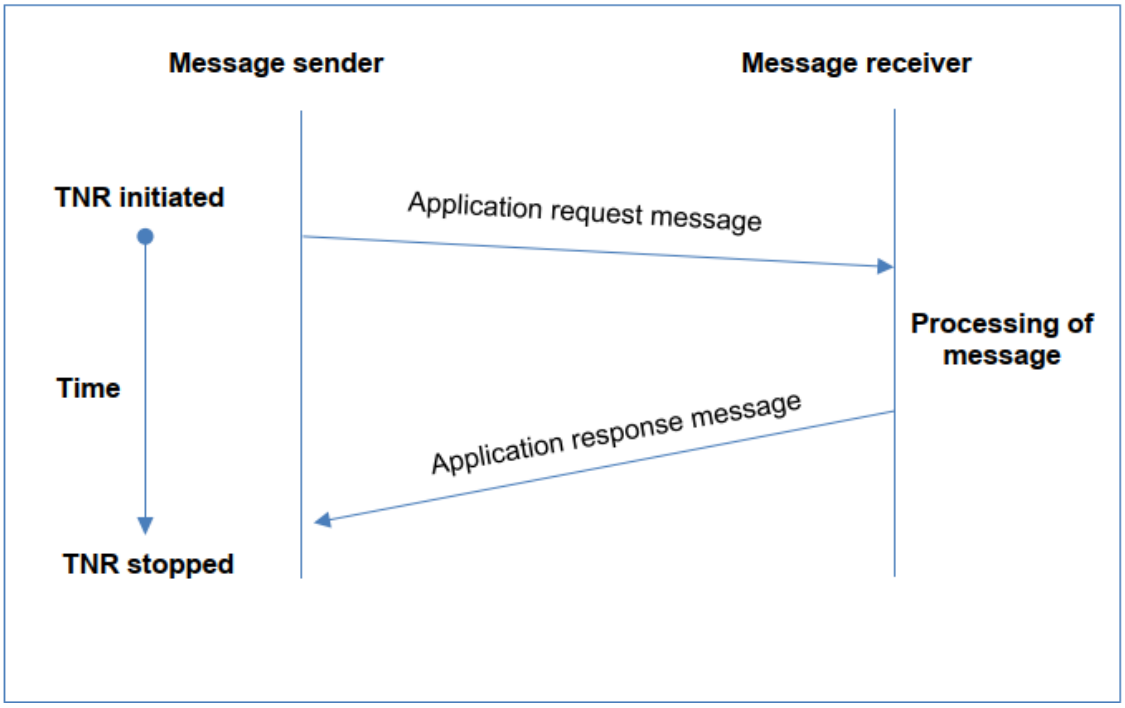


Figure: Non Response Timer (TNR)

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)

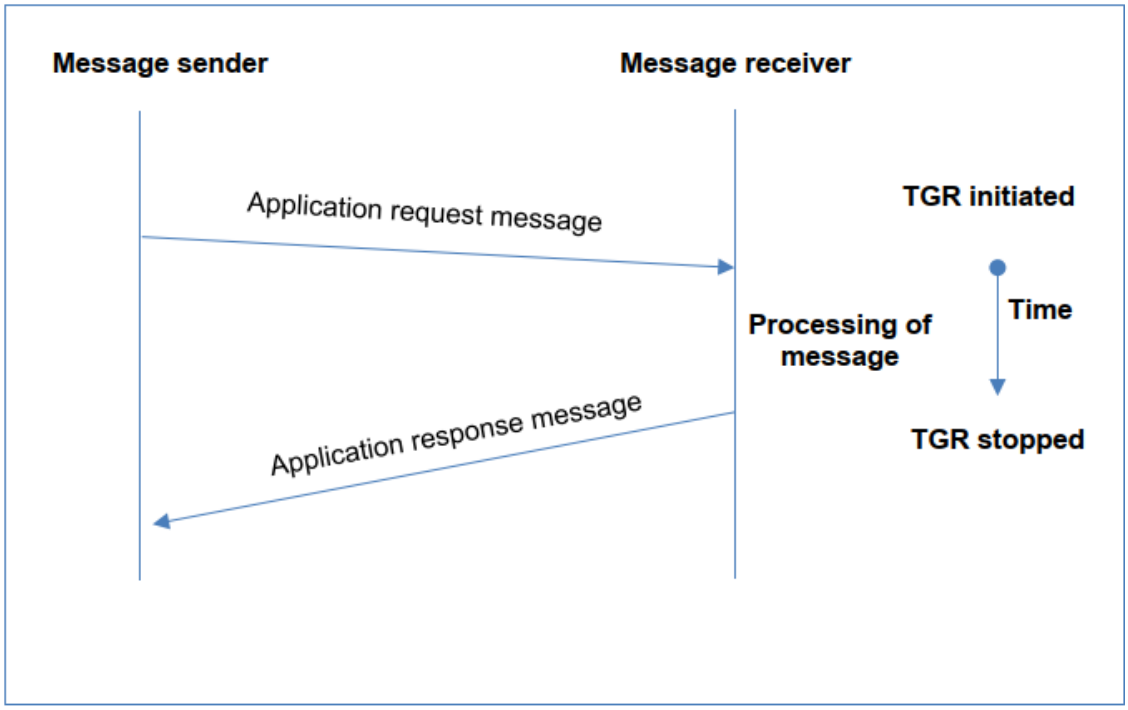


Figure: Guarantee Response Timer (TGR)

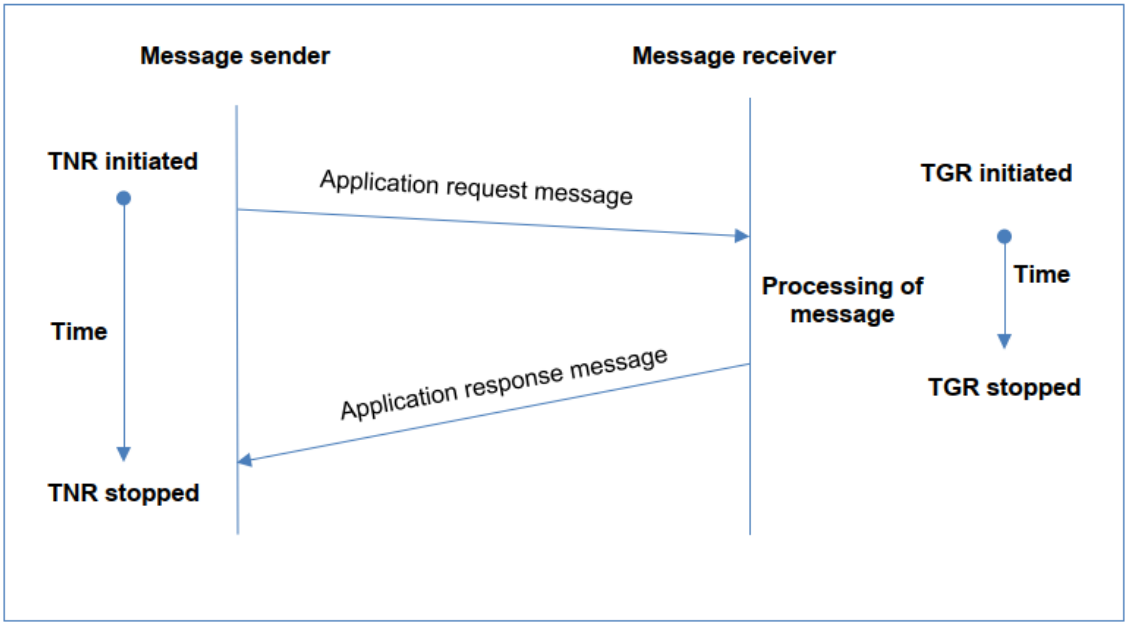


Figure: Combination of TNR and TGR

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 is sent (TSI timer timeout).

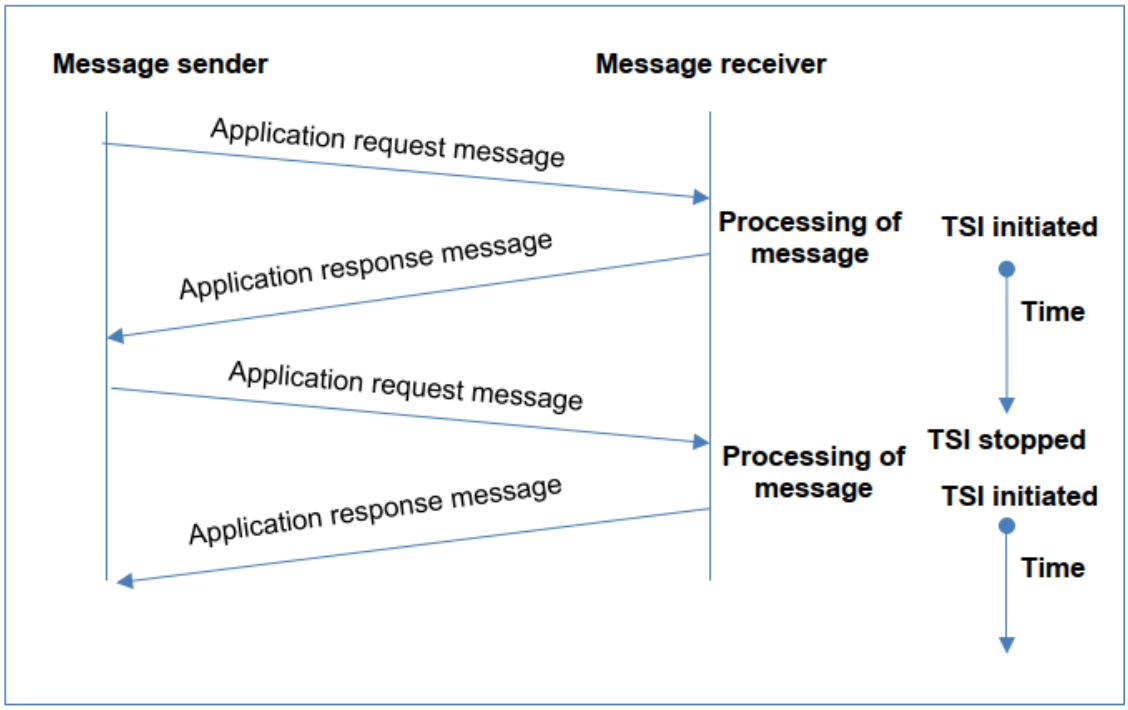


Figure: Inactivity Monitoring Timer (TSI)

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).

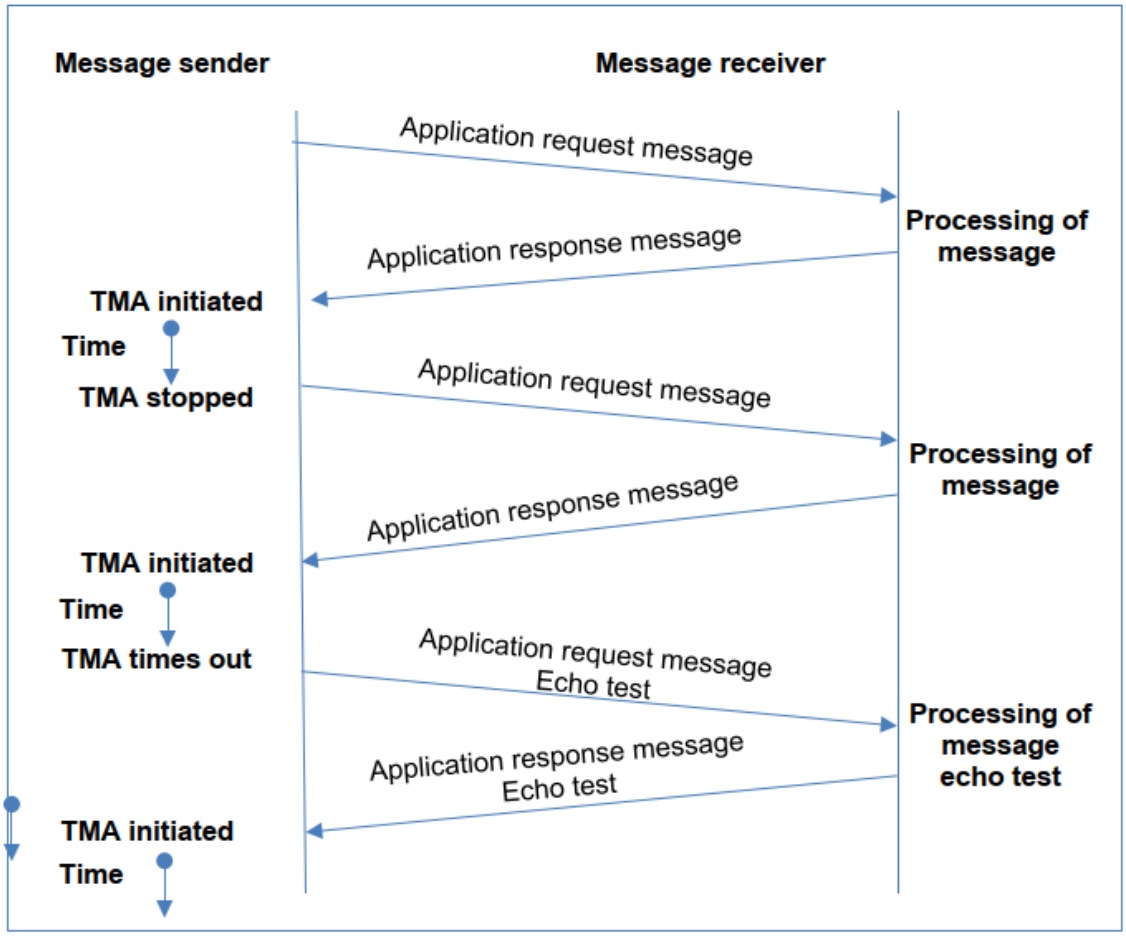


Figure: Maintained Activity Timer (TMA)

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.

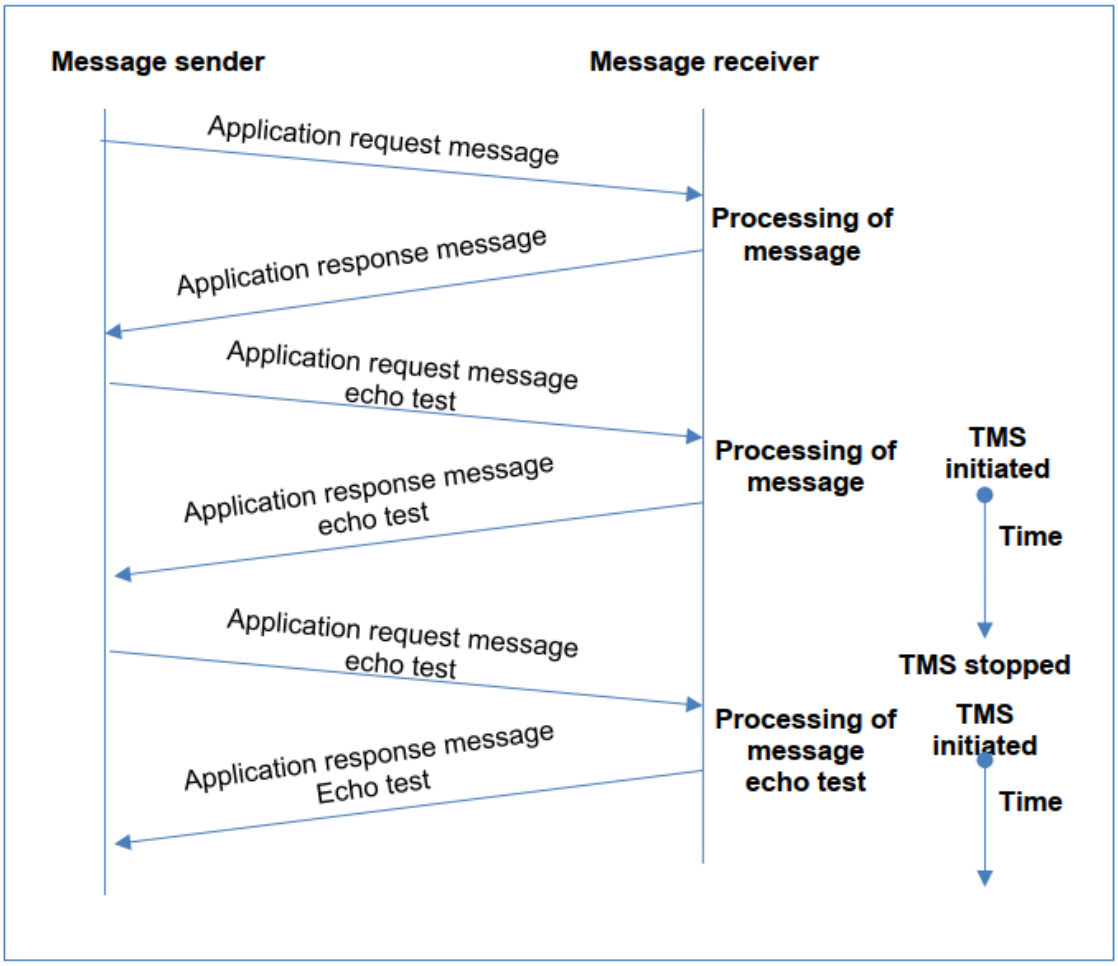


Figure: Maintained Activity Monitoring Timer (TSA)

5.6 EXAMPLES

In this context, TSI and TSM have the same meaning.

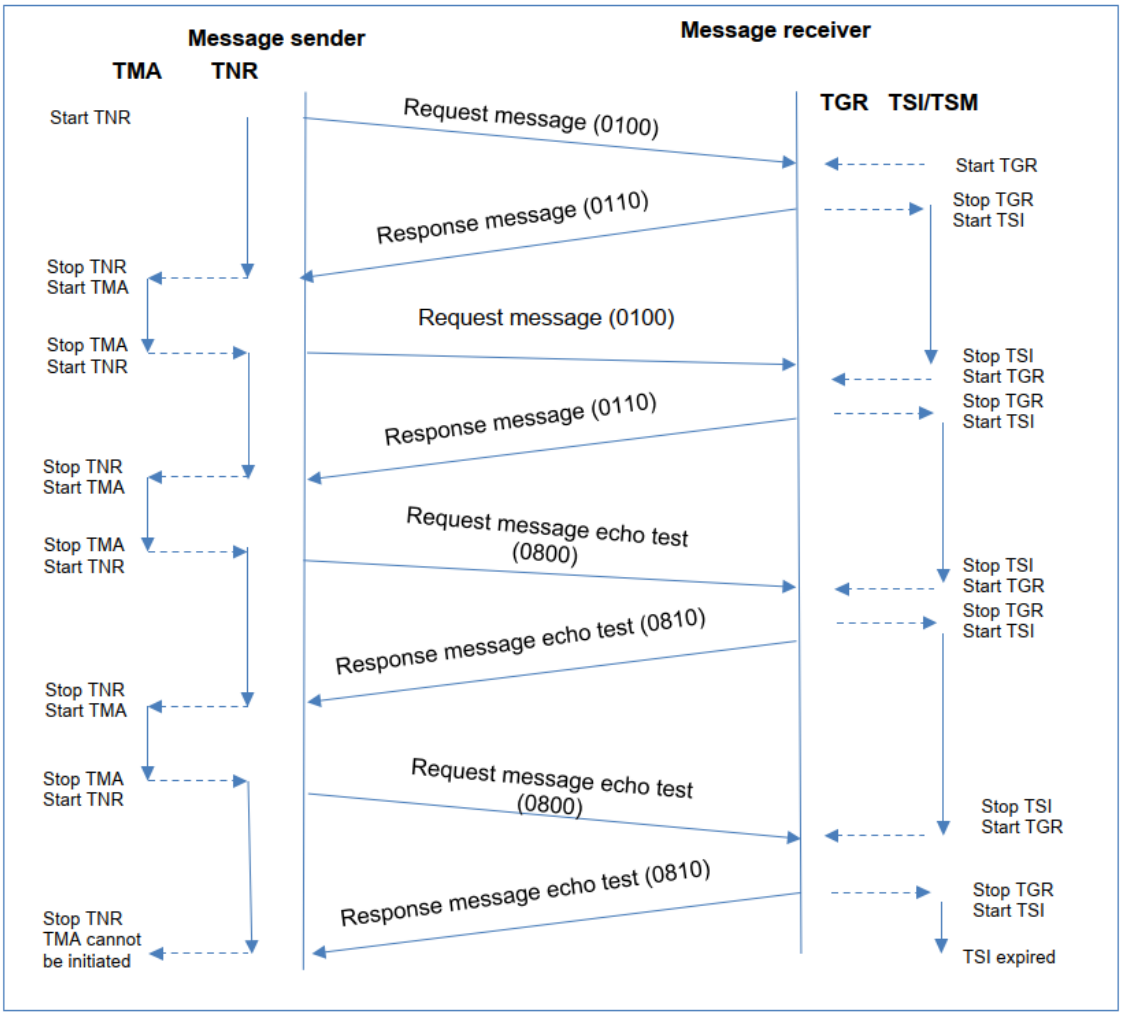


Figure: Summary of TNR, TGR, TSI, TMA, TSM timers in transaction processing

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

END OF DOCUMENT

2AP Authorisation

Acceptor to Acquirer Protocol
(CB2A)

VOLUME 2 - DATA FIELDS DICTIONARY

Version 1.6.6 - September 2025

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 2AP 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 2AP Authorisation protocol are the following:

MTI (Message Type Identifier)	Description
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

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
YY	year (2 numeric characters)
MM	month (2 numeric characters)
DD	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
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)

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

2.2.2 Presentation 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.

The following conventions are used in 2AP 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:

Data format	Field 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, abscb		(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.

2.2.6.3.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

2.2.6.3.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 Dataset format

The format named 'LL2VAR Dataset' identifies a TLV field containing all subfields also defined with a TLV structure.

In this case, all subfields have a Dataset format with the following structure:

Total length of field	Dataset 1	…	Dataset n

Dataset 1								
Dataset 1 identifier	Dataset 1 length	Dataset 1 value = data elements of Dataset 1						
		Tag 1	Length 1	Value 1	…	Tag n	Length n	Value n

2.2.6.5 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 [01][01][23][00][04][56]V

A B C

Example 2:

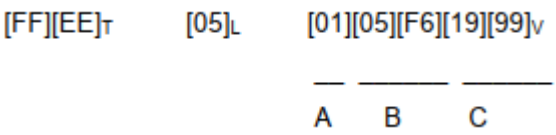
- Field XX
  - Format: b…255
- Type: FFEE
  - Data format: Structure
  - Number of bytes transported: 5

	Format	Value
Data element A	n1	1
Data element B	b2	15F6
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 3 bytes: [19][99]

Therefore:



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:

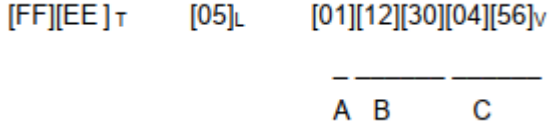
- Field XX
  - Format: b…255
- Type: FFEE
  - Data format: n9
  - Number of bytes transported: 5

	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:



2.3 DATA FIELD DESCRIPTIONS

2.3.1 Alphabetical list

The table below presents an alphabetical list of the data elements used in the 2AP 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
2AP specification date	47 type 33
3DS protocol major version	56 type 0022
3DS protocol version number	119 type 0022
Acceptance system card product code	56 type 0005
Acceptance System Components Identifier (ex ITP SA)	59 type 0201
Acceptance system country code	59 type 0205
Acceptance system logical number	59 type 0203
Acceptor additional contact information	119 type 1106
Acceptor advice code	119 type 0801
Acceptor contract number	59 type 0202
Acceptor customer service phone number	119 type 1104
Acceptor phone number	119 type 1105
Acceptor URL address	122
Account name match decision	123 type 0026
Account name request result	123 type 0025
Account name verification type	123 type 0021
Account owner	123 type 0024
Acquiring institution identification code	32
Additional amounts	54
Additional card reading capabilities	47 type 30
Additional data	56
Additional data initial transaction	56 type 0046
Additional data – National	47
Additional response data	44
Amount authorised	55 type 9F02
Amount other	55 type 9F03
Amount, cardholder billing	6
Amount, transaction	4
Amount, transaction fee	28
Application Cryptogram (ARQC)	55 type 9F26
Application cryptogram verification results	44 type CB
Application Expiration Date	55 type 5F24

Data element	Field/Sub-field
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 transaction	112 type 03
Authentication amount	56 type 0038
Authentication data quality indicator	119 type 0040
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 (Bank Identifier Code)	112 type 09
Brand selected	56 type 0003
Card acceptor identification code	42
Card acceptor name/location	43
Card acceptor terminal identification	41
Card Application Identifier (AID)	55 type 9F06
Card application type	55 type DF81
Card authenticated application data	55 type 9F81
Card product identifier	47 type 98
Card Security Code	59 type 0300
Card security code verfication results	59 type 0301
Card Sequence Number	23
Card type indicator	56 type 0018
Card-on-file action	56 type 0029
Cardholder address	123 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
Cardholder postcode	123 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

Data element	Field/Sub-field
Conversion rate, cardholder billing	10
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, cardholder billing	51
Currency code, transaction	49
Customer related data	123
Data equivalent to ISO track 1 read in contactless mode	55 type 0056
Data equivalent to ISO track 2 read in contactless mode	55 type 9F6B
Date, expiration	14
Date, local transaction	13
Debit unique reference identifier	119 type 0047
Delivery address	123 type 0009
Device information	55 type DF86
Digital wallet additional data	59 type 0417
Electronic commerce authentication type	59 type 0407
Electronic commerce data initial transaction	59 type 0420
Electronic commerce indicator	59 type 0416
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
FPAN expiry date	119 type 0012
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

Data element	Field/Sub-field
Independent sales organization	56 type 0024
Industry-specific data	118
Information relating to liability shift	44 type CD
Integrated circuit card system related data	55
IP address	123 type 0010
Issuer Action Code - Default	56 type 9F0D
Issuer Action Code - Denial	56 type 9F0E
Issuer Action Code - Online	56 type 9F0F
Issuer Application Data (IAD)	55 type 9F10
Issuer Authentication Data	55 type 0091
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
Kernel ID used	55 type DF68
Kernel identifier - Terminal	55 type 0096
KSN (Key Serial Number)	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
Maximum clearing date	119 type 0083
Merchant payment gateway ID	119 type 0204
Merchant scheme tokenisation indicator	119 type 0001
Merchant street address	119 type 0200
Merchant type	18
Message reason code	59 type 0101
Message to the transaction initiator	44 type BC
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

Data element	Field/Sub-field
Original data elements	90
Original transaction data	112 type 01
Original unique transaction identifier	47 type 99
Other email address	123 type 0032
Other email address verification result	123 type 0034
Other phone number	123 type 0031
Other phone number verification result	123 type 0033
Payer/account number	112 type 05
Payment Account Reference	56 type 0056
Payment by link indicator	119 type 0050
Payment Facilitator address	113
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
POI card input capabilities	119 type 1003
POI Components Identifier (ex ITP PA)	59 type 0215
POI display and print capabilities	119 type 1004
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	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
Recurring - Details	119 type 1118
Recurring Indian cards	119 type 1119
Remote commerce acceptor indicator	119 type 0028
Replacement amounts	95
Resend counter	56 type 0020

Data element	Field/Sub-field
Reserved for national use	119
Responding machine identifier	58
Response code	39
Response data for clearing	119 type 1001
Retrieval reference number	37
Risk scoring service	59 type 0802
RTT (Terminal processing results))	55 type DF85
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
Service location address	119 type 1113
SIRET (company registration number)	47 type 96
Special condition indicator	119 type 0035
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 (EMV tag 9A)	55 type 009A
Terminal Transaction Qualifiers (TTQ)	55 type 9F66
Terminal Type	55 type 9F35
Terminal Verification Results (TVR)	55 type 0095
Three-domain secure components availability	119 type 0013
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
Tokenised payment solution identifier	56 type 0012
Total number of payments	56 type 0032
Track 1 Discretionary Data	55 type 9F1F
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

Data element	Field/Sub-field
Transaction identifier or cryptogram supplied by the acceptor	59 type 0400
Transaction specific data	104
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 2AP Authorisation protocol, but only the significant fields are presented below. The table indicates whether or not the field is used in the 2AP Authorisation protocol.

Nr	Type	Name	Format
2		Primary Account Number	LLVAR n…19
3		Processing code	n6
4		Amount, transaction	n12
6		Amount, cardholder billing	n12
7		Transmission date and time	n10 MMDDhhmmss
10		Conversion rate, cardholder billing	n8
11		Systems trace audit number	n6
12		Time, local transaction	n6 hhmmss
13		Date, local transaction	n4 MMDD
14		Date, expiration	n4 YYMM
18		Merchant type	n4
22		Point of service entry mode	n3
23		Card Sequence Number	n3
25		Point of service condition code	n2
26		PIN length	n2
27		Authorisation identification response length	n1
28		Amount, transaction fee	an9
32		Acquiring institution identification code	LLVAR n…11
33		Forwarding institution identification code	LLVAR n…11
35		Track 2 data	LLVAR z…37
37		Retrieval reference number	an12
38		Authorisation identification response	an6

Nr	Type	Name	Format
39		Response code	an2
41		Card acceptor terminal identification	ans8
42		Card acceptor identification code	ans15
43		Card acceptor name/location	ans40
44		Additional response data	LLVAR ans 25
	AA	Incorrect field	ans4, 6, 8
	AB	Security error	ans5
	AC	Field conversion	ans…21
	AF	Service activation code	ans1
	BB	Telephone number	ans…21
	BC	Message to the transaction initiator	ans…21
	CA	Track or equivalent data cryptogram processing information	ans1
	CB	Application cryptogram verification results	ans1
	CC	Cardholder address checking information	ans2
	CD	Information relating to liability shift	ans1
47		Additional data – National	LLVAR ans…255
	08	Location category code	ans…8
	20	Field conversion by acquirer (field 32) or forwarder (field 33)	ans…
	24	File number	anp12
	30	Additional card reading capabilities	n 1
	31	Point of interaction information	n 1
	33	2AP specification date	n 4
	95	Unique transaction identifier	ans…50
	96	SIRET (company registration number)	ans14
	97	IDPA (point of interaction identifier assigned by an acquirer)	ans8
	98	Card product identifier	ans2…10
	99	Original unique transaction identifier	ans…50
	A0	IDSA (acceptance system identifier assigned by an acquirer)	ans8
48		Security Data	LLVAR ansb…255
	0001	KSN (Key Serial Number)	b10…12
	0002	BDK (Base Derivation Key) name	b2…15
	0003	BDK (Base Derivation Key) version	n10
49		Currency code, transaction	n3
51		Currency code, cardholder billing	n3
52		PIN data	b8…16
53		Security related control information	n16
54		Additional amounts	LLLVAR an…120
55		Integrated circuit card system related data	LLLVAR b…255

Nr	Type	Name	Format
	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)	b2
	0091	Issuer Authentication Data	b8…16
	0095	Terminal Verification Results (TVR)	b5
	0096	Kernel identifier - Terminal	b1…8
	009A	Terminal transaction date (EMV tag 9A)	n6 (YYMMDD)
	009C	Transaction Type	n2
	5F24	Application Expiration Date	n6 (YYMMDD)
	9F02	Amount authorised	n12
	9F03	Amount other	n12
	9F06	Card Application Identifier (AID)	b5…16
	9F0A	Application Selection Registered Proprietary Data	b4…32
	9F10	Issuer Application Data (IAD)	b…32
	9F1F	Track 1 Discretionary Data	ans…54
	9F26	Application Cryptogram (ARQC)	b8
	9F27	Cryptogram Information Data	b1
	9F33	Terminal capabilities	b3
	9F34	Cardholder verification method (CVM) results	b3
	9F35	Terminal Type	n2
	9F36	Application Transaction Counter (ATC)	b2
	9F37	Unpredictable Number	b4
	9F66	Terminal Transaction Qualifiers (TTQ)	structure
	9F6B	Data equivalent to ISO track 2 read in contactless mode	b…19
	9F7C	Issuer proprietary data	b…32
	9F81	Card authenticated application data	b…128
	DF68	Kernel ID used	b1
	DF80	ICC processing results	n2
	DF81	Card application type	n1
	DF85	RTT (Terminal processing results))	b5
	DF86	Device information	b…35
	FF00	Issuer script results	b…5
56		Additional data	LLLVAR b…255
	0001	Payment Facilitator Data	structure
	0002	Application selection indicator	n2
	0003	Brand selected	b1

Nr	Type	Name	Format
	0005	Acceptance system card product code	an3
	0011	Number of articles	n2
	0012	Tokenised payment solution identifier	n3
	0013	Type of transaction	n2
	0014	Type of proof	n2
	0017	Cryptogram entry date and GMT time	n12(YYMMDDhhmmss)
	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 organization	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(YYYYMMDDHHMMSS)
	0038	Authentication amount	n12
	0040	List of installed kernels	b8
	0045	Payment validity date	n6(YYMMDD)
	0046	Additional data initial transaction	structure
	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
58		Responding machine identifier	LLLVAR ans…255
59		National data	LLLVAR b…255
	0100	Function code	n3
	0101	Message reason code	n4
	0102	Transaction year	n2
	0200	ERT (Regulatory and technical environment)	b1
	0201	Acceptance System Components Identifier (ex ITP SA)	n12

Nr	Type	Name	Format
	0202	Acceptor contract number	n7
	0203	Acceptance system logical number	n3
	0204	Point of interaction logical number	n3
	0205	Acceptance system country code	n3
	0207	Cardholder total amount	n12
	020B	TASA (Card acceptor application type)	b5…16
	0215	POI Components Identifier (ex ITP PA)	n12
	0216	Point of interaction extended logical number	an3
	0300	Card Security Code	Structure
	0301	Card security code verfication results	Structure
	0400	Transaction identifier or cryptogram supplied by the acceptor	b4…40
	0401	Cardholder authentication value	b20…40
	0407	Electronic commerce authentication type	n2
	0409	Cardholder authentication value processing information	anp1
	0410	Cardholder authentication method	ans2
	0411	Cardholder authentication value calculation method	an1
	0412	Three-domain secure results	Structure
	0413	Modified electronic commerce authentication type	b1
	0416	Electronic commerce indicator	an2
	0417	Digital wallet additional data	an12…24
	0418	Wallet identifier	n6
	0419	Three-domain secure results others	Structure
	0420	Electronic commerce data initial transaction	structure
	0800	Service attribute	n2
	0802	Risk scoring service	structure
	0805	Optional services supported (acceptor domain)	b2
70		Network management information code	n3
90		Original data elements	n42
95		Replacement amounts	an42
104		Transaction specific data	LL2VAR b…999 (Datasets)
112		Funds transfer data	LLLVAR ans…255
	01	Original transaction data	ans1…99
	03	Application type identifier transaction	an2
	05	Payer/account number	ans 1…35
	06	Counterparty PAN	n…19
	07	Counterparty last name and first name	ans1…30
	08	Funds transfer reason	ans1…40
	09	BIC (Bank Identifier Code)	ans1…11

Nr	Type	Name	Format
	10	IBAN	an…34
113		Payment Facilitator address	LL2VAR b…999
115		nexo data	LLLVAR b…255
	0001	nexo PoS identifier	ans…107
	0002	nexo Acceptance System identifier	ans…71
	0003	nexo certificate	ans…35
118		Industry-specific data	LL2VAR b…999
119		Reserved for national use	LL2VAR b…999
	0001	Merchant scheme tokenisation indicator	an1
	0009	Scheme program merchant identifier	ans…8
	0011	FPAN	n9…19
	0012	FPAN expiry date	n4
	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 indicator	b…115
	0035	Special condition indicator	n1
	0040	Authentication data quality indicator	an1
	0041	Purchase identifier type	an1
	0042	Purchase identifier	an32
	0047	Debit unique reference identifier	ans…50
	0050	Payment by link indicator	an1
	0083	Maximum clearing date	n4
	00BC	Extended message to the transaction initiator	ans1…101
	0200	Merchant street address	ans…99
	0204	Merchant payment gateway ID	n11
	0208	Pre-authorisation duration	n 2
	0359	Transaction eligible for token services	an1
	0801	Acceptor advice code	n 2
	0802	Reattempt frozen period	n 4
	0803	Reattempt conditions	n 6
	1001	Response data for clearing	structure
	1003	POI card input capabilities	b2
	1004	POI display and print capabilities	structure
	1022	Cardholder verification method used at POS	b1…4
	1104	Acceptor customer service phone number	ans…16

Nr	Type	Name	Format
	1105	Acceptor phone number	ans…16
	1106	Acceptor additional contact information	ans…25
	1113	Service location address	ans29
	1118	Recurring - Details	an2
	1119	Recurring Indian cards	Structure
	9F19	Token Requestor ID	an 11
	9F25	Last four digits of PAN	n 4
122		Acceptor URL address	LLLVAR ans…255
123		Customer related data	LL2VAR b…999
	0006	Cardholder address	ansp…40
	0008	Cardholder postcode	ansp…10
	0009	Delivery address	ans80
	0010	IP address	ans4…45
	0021	Account name verification type	an2
	0024	Account owner	ans105
	0025	Account name request result	an2
	0026	Account name match decision	an8
	0031	Other phone number	ans16
	0032	Other email address	ans99
	0033	Other phone number verification result	an1
	0034	Other email address verification result	an1

2.3.2.1 List of ISO8583 and reserved fields

Nr	Type	Name	Format
5		See ISO8583 standard	n12
8		See ISO8583 standard	n8
9		See ISO8583 standard	n8
15		See ISO8583 standard	n4
16		See ISO8583 standard	n4
17		See ISO8583 standard	n4
20		See ISO8583 standard	n3
21		See ISO8583 standard	n3
24		See ISO8583 standard	n3
29		See ISO8583 standard	x+n8
30		See ISO8583 standard	x+n8
31		See ISO8583 standard	x+n8
34		See ISO8583 standard	LLVAR ns…28
36		See ISO8583 standard	LLLVAR z…104

Nr	Type	Name	Format
40		See ISO8583 standard	an3
45		See ISO8583 standard	LLLVAR ans…76
46		See ISO8583 standard	LLLVAR ans…255
50		See ISO8583 standard	n3
57		See ISO8583 standard	LLLVAR ans…255
60		See ISO8583 standard	LLLVAR ans…1
61		See ISO8583 standard	LLLVAR ans…3
62		Reserved for private use	LLLVAR ans…255
63		Reserved for private use	LLLVAR ans…255
64		See ISO8583 standard	b8
65		See ISO8583 standard	b11
66		See ISO8583 standard	n1
67		See ISO8583 standard	n2
68		See ISO8583 standard	n3
69		See ISO8583 standard	n3
71		See ISO8583 standard	n4
72		See ISO8583 standard	n4
73		See ISO8583 standard	n6
74		See ISO8583 standard	n10
75		See ISO8583 standard	n10
76		See ISO8583 standard	n10
77		See ISO8583 standard	n10
78		See ISO8583 standard	n10
79		See ISO8583 standard	n10
80		See ISO8583 standard	n10
81		See ISO8583 standard	n10
82		See ISO8583 standard	n12
83		See ISO8583 standard	n12
84		See ISO8583 standard	n12
85		See ISO8583 standard	n12
86		See ISO8583 standard	n16
87		See ISO8583 standard	n16
88		See ISO8583 standard	n16
89		See ISO8583 standard	n16
91		See ISO8583 standard	an1
92		See ISO8583 standard	an2
93		See ISO8583 standard	an5
94		See ISO8583 standard	an7

Nr	Type	Name	Format
96		See ISO8583 standard	b8
97		See ISO8583 standard	x+n16
98		See ISO8583 standard	ans25
99		See ISO8583 standard	LLVAR n…11
100		See ISO8583 standard	LLVAR n…11
101		See ISO8583 standard	LLVAR ans…17
102		See ISO8583 standard	LLVAR ans…28
103		See ISO8583 standard	LLVAR ans…28
105		See ISO8583 standard	LLLVAR ans…255
106		See ISO8583 standard	LLLVAR ans…255
107		See ISO8583 standard	LLLVAR ans…255
108		See ISO8583 standard	LLLVAR ans…255
109		See ISO8583 standard	LLLVAR ans…255
110		See ISO8583 standard	LLLVAR ans…255
111		See ISO8583 standard	LLLVAR ans…255
114		See ISO8583 standard	LLLVAR ans…255
116		See ISO8583 standard	LLLVAR ans…255
117		See ISO8583 standard	LLLVAR ans…255
120		See ISO8583 standard	LLLVAR ans…255
121		See ISO8583 standard	LLLVAR ans…255
124		See ISO8583 standard	LLLVAR ans…255
125		See ISO8583 standard	LLLVAR ans…255
126		See ISO8583 standard	LLLVAR ans…255
127		See ISO8583 standard	LLLVAR ans…255
128		See ISO8583 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 2AP 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 2AP Authorisation protocol is reserved for FrenchSys use, unless it is declared explicitly for private use in the dictionary. Any non-defined field in the 2AP 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: Primary Account Number

Format: LLVAR n...19

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

Field 3: Processing code

Format: n6

❑ **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 - 19	Reserved for private use
20	Credit (returns)
28	Quasi-cash refund
30	Available funds enquiry
36	Balance enquiry (copy)
37	Card return
39	VMAAS eligibility inquiry
41	Funds transfer, debit
42	Funds transfer, credit
90 - 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: Amount, transaction

Format: n12

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 6: Amount, cardholder billing

Format: n12

Amount billed to the cardholder, stated in the currency of the cardholder account country.

This amount is stated in the smallest units of the currency specified in field 51.

Field 7: Transmission date and time

Format: n10 MMDDhhmmss

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 10: Conversion rate, cardholder billing

Format: n8

Factor used to convert values between the transaction amount and the amount billed to the cardholder.

The transaction amount (field 4) is multiplied by the cardholder billing conversion rate to obtain the cardholder billing amount (field 6).

Field 11: Systems trace audit number

Format: n6

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: Time, local transaction

Format: n6 hhmmss

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: Date, local transaction

Format: n4 MMDD

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: Date, expiration

Format: n4 YYMM

Card expiry date.

When present, this field must contain a significant value with YYMM structure or 0000 (for cards without validity date).

Field 18: Merchant type *Format: n4*

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: Point of service entry mode *Format: n3*

❑ **PAN entry mode** _____ **quartets 1 and 2**

PAN entry mode also specifies how the expiry date is entered.

- (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.

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

❑ **PIN entry mode** _____ **quartet 3**

PIN entry mode refers to the action performed for the current transaction.

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

Field 23: Card Sequence Number *Format: n3*

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

Field 25: Point of service condition code

Format: n2

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. 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.

Value	Description
00	Normal conditions
01	Customer not present
02	Unattended 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	Unattended terminal unable to retain card
52	Mail order
53	Telephone order
54 - 99	Reserved for private use

Field 26: PIN length

Format: n2

This data element specifies the maximum PIN length that can be input. Possible values: 4 to 12.

Field 27: Authorisation identification response length

Format: n1

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

Field 28: Amount, transaction fee

Format: an9

This field contains a signed amount (structure:x+n8).

Field 32: Acquiring institution identification code

Format: LLVAR n…11

This field identifies the acquirer of the transaction, i.e. the institution presenting the transaction. Field 32 contains the identifier of the acquirer bank.

❑ **Acquirer identifier** _____ **n6**

❑ **Bank identifier** _____ **n5**

Field 33: Forwarding institution identification code

Format: LLVAR n...11

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

Field 35: Track 2 data

Format: LLVAR z...37

Contains track 2 in compliance with the ISO 7813 standard.

Field 37: Retrieval reference number

Format: an12

This data element is left to the discretion of the acceptor - acquirer relation. Once it has been defined, it can no longer be changed during the entire process (i.e. acceptance, authorisation, data capture).

Field 38: Authorisation identification response

Format: an6

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

Field 39: Response code

Format: an2

- 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 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.

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
19	Re-enter transaction
20	Invalid response (error in server domain)
21	No action taken

Value	Description
25	Unable to locate record on file
30	Format error
31	Bank not supported by switch
32	Completed partially
33	Expired card
34	Suspected fraud
38	Allowable PIN tries exceeded
39	No such account type
40	Requested function not supported
41	Lost card
43	Stolen card, pick-up
46	Business specific error
47	Restricted card
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
5C	Transaction not supported/blocked by issuer
60	Card acceptor contact acquirer
61	Exceeds withdrawal amount limit
62	Card invalid in region or country
63	Security violation
64	Transaction does not fulfil Anti-Money Laundering requirement
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
79	Life cycle
80	Approved transaction without financial impact
82	Incorrect CVV, dCVV, iCVV
83	Fraud/security
8P	Policy

Value	Description
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, no rerouting requested
97	General monitoring timeout
98	Server unavailable, network re-routing requested
99	Initiator domain incident
9G	Blocked by cardholder/contact cardholder
A0	Fallback in EMV contact mode
A1	Soft decline (electronic commerce only), 3DS with challenge required
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
Z5	Valid account but amount is not supported

Field 41: Card acceptor terminal identification

Format: ans8

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

Field 42: Card acceptor identification code

Format: ans15

Transports the content of envelope 42 provided during a parameter downloading.

Field 43: Card acceptor name/location

Format: ans40

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 ignores the above description and returns the content of the envelope 43 without modification.

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").

Field 44: Additional response data

Format: LLVAR ans 25

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

❑ **Data type** **ans2**

Value	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*** *Format: ans4, 6, 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 (see values below)

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.

Value	Description
1	Value error
2	Format error
3	Missing mandatory field

⇨ ***TYPE = AB: SECURITY ERROR*** *Format: ans5*

⇨ ***TYPE = AC: FIELD CONVERSION*** *Format: ans…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.

❑ **Conversion initiator** _____ **ans1**

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

❑ **Converted field number** _____ **ans3**

❑ **Original value of converted field** _____ **ans…17**

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

⇨ ***TYPE = AF: SERVICE ACTIVATION CODE*** *Format: ans1*

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

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

⇨ ***TYPE = BB: TELEPHONE NUMBER*** *Format: ans…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*** *Format: ans…21*

The variable contains a message for the transaction initiator.

❑ **Control character** **ans1**

Value	Description
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*** *Format: ans1*

⇨ ***TYPE = CB: APPLICATION CRYPTOGRAM VERIFICATION RESULTS*** *Format: ans1*

⇨ ***TYPE = CC: CARDHOLDER ADDRESS CHECKING INFORMATION*** *Format: ans2*

❑ **Nomenclature** **ans1**

Value	Description
0	2AP

❑ **Result of control** **ans1**

Value	Description
A	Postcode and address fully match
B	Postcode and address partially match
C	Postcode and address do not match

Value	Description
D	Control was not performed or was not performed for all data elements
R	Retry (indeterminate outcome)

⇨ ***TYPE = CD: INFORMATION RELATING TO LIABILITY SHIFT*** *Format: ans1*

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.

Value	Description
0	Unknown
1	Shift
2	No shift

Field 47: Additional data – National *Format: LLVAR ans...255*

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

❑ **Data type** _____ **ans2**

Value	Description
08	Location category code
20	Field conversion by acquirer (field 32) or forwarder (field 33)
24	File number
30	Additional card reading capabilities
31	Point of interaction information
33	2AP specification date
95	Unique transaction identifier
96	SIRET
97	IDPA (Point of interaction identifier assigned by an acquirer)
98	Card product identifier
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 — Format: ans…8

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

Value	Description
PR	Counter sale
RG	Manual cash at counter
RM	Manual cash in shop
VA	Agency sale
VB	On board sale

⇨ TYPE = 20: FIELD CONVERSION BY ACQUIRER (FIELD 32) OR FORWARDER (FIELD 33) — Format: ans…

- 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 — Format: anp12

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 — Format: n 1

Value	Description
1	Active contactless application

⇨ TYPE = 31: POINT OF INTERACTION INFORMATION — Format: n 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: 2AP SPECIFICATION DATE — Format: n 4

Release date of the 2AP specification in YYMM format

⇨ ***TYPE = 95: UNIQUE TRANSACTION IDENTIFIER*** *Format: ans…50*

❑ **Nomenclature** **an1**

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

Value	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)*** *Format: ans14*

⇨ ***TYPE = 97: IDPA (POINT OF INTERACTION IDENTIFIER ASSIGNED BY AN ACQUIRER)*** *Format: ans8*

⇨ ***TYPE = 98: CARD PRODUCT IDENTIFIER*** *Format: ans2…10*

❑ **Nomenclature** **an1**

❑ **Product code** **ans1…9**

Depends on the network source

⇨ ***TYPE = 99: ORIGINAL UNIQUE TRANSACTION IDENTIFIER*** *Format: ans…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)*** *Format: ans8*

Field 48: Security Data *Format: LLVAR ansb…255*

This field is used to transport security data in messages. The data elements transported in this field are coded in binary.

❑ **Data type** **b2**

Value	Description
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)*** *Format: b10…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*** *Format: b2…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

Value	Description
Use reserved for 2AP 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.
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.
06 - 7F	RFU
Private use	
80 - 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*** *Format: n10*

Field 49: Currency code, transaction *Format: n3*

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 51: Currency code, cardholder billing *Format: n3*

Specifies the currency used to express the amount defined in field 6. This is the currency code of the cardholder account's country.

The codes are listed in the ISO 4217 standard document.

Field 52: PIN data *Format: b8...16*

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

Field 53: Security related control information *Format: n16*

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.

Value	Description
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

Value	Description
0	No encryption

Value	Description
2	Triple DES
3	DUKPT2009
4	DUKPT2017

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

Value	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**

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

❑ **Not used** _____ **quartets 11 to 16**

Field 54: Additional amounts

Format: LLLVAR an...120

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

❑ **Account type** _____ **n2**

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

❑ **Amount type** _____ **n2**

An amount type can be found in several data elements.

Value	Description
43	Cumulative total of authorised amount
44	Tip amount
57	Original amount
60	POI Amount before DCC conversion

Value	Description
87	Total Discount Amount for discount purposes
88	Additional transaction fee 1
89	Additional transaction fee 2
90	Amount, anticipated
95	Transfer service

❑ **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: Integrated circuit card system related data *Format: LLLVAR b…255*

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**

Value	Description
0056	Data equivalent to ISO track 1 read in contactless mode
0057	Track 2 equivalent data
0071	Issuer Script Template 1
0072	Issuer Script Template 2
0082	Application Interchange Profile (AIP)
0091	Issuer Authentication Data
0095	Terminal Verification Results (TVR)
0096	Kernel identifier - Terminal
009A	Terminal Transaction Date
009C	Transaction type
5F24	Application Expiration Date
9F02	Amount, authorised
9F03	Amount, other
9F06	Card 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

Value	Description
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
9F81	Card authenticated application data
DF3F	Card data storage
DF68	Kernel ID used
DF80	ICC processing results
DF81	Card application type
DF85	RTT (Terminal processing results)
DF86	Device information
FF00	Issuer script results

❑ **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*** *Format: ans…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*** *Format: b…19*

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*** *Format: b…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 — *Format: b…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 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 = 0082: APPLICATION INTERCHANGE PROFILE (AIP) — *Format: b2*

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

⇨ TYPE = 0091: ISSUER AUTHENTICATION DATA — *Format: b8…16*

Data sent to the card for issuer authentication.

⇨ TYPE = 0095: TERMINAL VERIFICATION RESULTS (TVR) — *Format: b5*

Results of the different controls performed by the terminal.

⇨ TYPE = 0096: KERNEL IDENTIFIER - TERMINAL — *Format: b1…8*

⇨ TYPE = 009A: TERMINAL TRANSACTION DATE (EMV TAG 9A) — *Format: n6 (YYMMDD)*

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

⇨ TYPE = 009C: TRANSACTION TYPE — *Format: n2*

Contains the transaction type used for an Application Usage Control (AUC). This data is scheme specific and equivalences exist between tag 9C and the processing code.

⇨ TYPE = 5F24: APPLICATION EXPIRATION DATE — *Format: n6 (YYMMDD)*

Contains the application expiration date of the EMV card.

⇨ TYPE = 9F02: AMOUNT AUTHORISED — *Format: n12*

Indicates the amount that the terminal communicates to the card.

⇨ TYPE = 9F03: AMOUNT OTHER — *Format: n12*

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

⇨ TYPE = 9F06: CARD APPLICATION IDENTIFIER (AID) — *Format: b5…16*

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

⇨ ***TYPE = 9F0A: APPLICATION SELECTION REGISTERED PROPRIETARY DATA*** *Format: b4…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)*** *Format: b…32*

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

⇨ ***TYPE = 9F1F: TRACK 1 DISCRETIONARY DATA*** *Format: ans…54*

⇨ ***TYPE = 9F26: APPLICATION CRYPTOGRAM (ARQC)*** *Format: b8*

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*** *Format: b1*

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*** *Format: b3*

Specifies the terminal capabilities in a table.

⇨ ***TYPE = 9F34: CARDHOLDER VERIFICATION METHOD (CVM) RESULTS*** *Format: b3*

Specifies the results of the last cardholder authentication method.

⇨ ***TYPE = 9F35: TERMINAL TYPE*** *Format: n2*

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

⇨ ***TYPE = 9F36: APPLICATION TRANSACTION COUNTER (ATC)*** *Format: b2*

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

⇨ ***TYPE = 9F37: UNPREDICTABLE NUMBER*** *Format: b4*

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

⇨ ***TYPE = 9F66: TERMINAL TRANSACTION QUALIFIERS (TTQ)*** *Format: structure*

Terminal status during the transaction.

⇨ ***TYPE = 9F6B: DATA EQUIVALENT TO ISO TRACK 2 READ IN CONTACTLESS MODE*** *Format: b…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*** *Format: b…32*

Contains data to be sent to the issuer.

⇨ ***TYPE = 9F81: CARD AUTHENTICATED APPLICATION DATA*** *Format: b…128*

⇨ ***TYPE = DF68: KERNEL ID USED*** *Format: b1*

Kernel identifier used to process the transaction.

⇨ ***TYPE = DF80: ICC PROCESSING RESULTS*** *Format: n2*

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

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

Value	Description
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

⇨ ***TYPE = DF81: CARD APPLICATION TYPE*** *Format: n1*

Value	Description
2	EMV
3	Contactless integrated circuit – magstripe context

⇨ ***TYPE = DF85: RTT (TERMINAL PROCESSING RESULTS))*** *Format: b5*

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

⇨ ***TYPE = DF86: DEVICE INFORMATION*** *Format: b…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*** *Format: b…5*

Specifies the results of the issuer script processing.

Field 56: Additional data — *Format: LLLVAR b…255*

❑ **Data type** **b2**

Value	Description
0001	Payment facilitator data
0002	Application selection indicator
0003	Brand selected
0005	Acceptance system card product code
0011	Number of articles
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
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

Value	Description
0046	Additional data – Initial transaction
0056	Payment Account Reference
5F2D	Language preference
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*** *Format: structure*

❑ **Payment Facilitator ID** _____ **n11**

❑ **Independent Sales Organisation ID** _____ **n11**

❑ **Sub-Merchant ID** _____ **ans15**

⇨ ***TYPE = 0002: APPLICATION SELECTION INDICATOR*** *Format: n2*

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

Value	Description
00	Selection by default
01	Cardholder selection

⇨ ***TYPE = 0003: BRAND SELECTED*** *Format: b1*

Indicates the brand selected by the cardholder.

Value	Description
00	CB
01	VISA
02	Vpay
03	Electron
04	MasterCard
05	Maestro
06	JCB

Value	Description
07	Discover
08	UPI
09	Amex
80 - 99	Reserved for private use

⇨ *TYPE = 0005: ACCEPTANCE SYSTEM CARD PRODUCT CODE* — *Format: an3*

⇨ *TYPE = 0011: NUMBER OF ARTICLES* — *Format: n2*

Number of articles in the cart.

⇨ *TYPE = 0012: TOKENISED PAYMENT SOLUTION IDENTIFIER* — *Format: n3*

❑ **Nomenclature** **n1**

Value	Description
0	CB
1 - 9	RFU

❑ **Identifier** **n2**

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

Value	Description
00	Apple Pay
01	Samsung Pay
02	Google Pay
03	Garmin Pay
11	Click-to-Pay

⇨ *TYPE = 0013: TYPE OF TRANSACTION* — *Format: n2*

Type of transaction processed.

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

⇨ *TYPE = 0014: TYPE OF PROOF* — *Format: n2*

Type of proof generated by the payment solution.

Value	Description
00	EMV
01	Secured electronic commerce

⇨ TYPE = 0017: CRYPTOGRAM ENTRY DATE AND GMT TIME — Format: n12(YYMMDDhhmmss)

GMT date and GMT for card security code entry.

⇨ TYPE = 0018: CARD TYPE INDICATOR — Format: n1

⇨ TYPE = 0019: SERIAL NUMBER — Format: ans…35

Serial number of the acceptance system or point of acceptance.

⇨ TYPE = 0020: RESEND COUNTER — Format: n1

Counter used for re-authorised messages.

⇨ TYPE = 0022: 3DS PROTOCOL MAJOR VERSION — Format: an1

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

⇨ TYPE = 0023: UUID CONTAINER — Format: ans37

❑ **Nomenclature** _____ **ans1**

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

❑ **UUID** _____ **ans36**

⇨ TYPE = 0024: INDEPENDENT SALES ORGANIZATION — Format: ans15

⇨ TYPE = 0025: PAYMENT FACILITATOR IDENTIFIER — Format: ans15

⇨ TYPE = 0026: MARKETPLACE IDENTIFIER — Format: ans15

⇨ TYPE = 0027: FINAL MERCHANT IDENTIFIER — Format: ans15

⇨ TYPE = 0028: PAYMENT USE CASE — Format: n2

Identification of remote payment use cases.

Value	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-authorisation out of reservation and rental context
08	Deposit-refund system
09 - 89	RFU
90	Non payment card validity check
91 - 99	RFU

⇨ ***TYPE = 0029: CARD-ON-FILE ACTION*** *Format: an1*

Value	Description
1	Add card
2	Keep card

⇨ ***TYPE = 0031: PAYMENT NUMBER*** *Format: n2*

Payment number in progress.

⇨ ***TYPE = 0032: TOTAL NUMBER OF PAYMENTS*** *Format: n2*

Total number of payments planned.

⇨ ***TYPE = 0033: EXEMPTION INDICATOR*** *Format: b2…3*

❑ **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** **b…1**

⇨ ***TYPE = 0036: AUTHENTICATION MERCHANT NAME*** *Format: ans40*

Name of the merchant presented for authentication.

⇨ ***TYPE = 0037: AUTHENTICATION DATE*** *Format: n14(YYYYMMDDHHMMSS)*

Date and time of authentication.

⇨ ***TYPE = 0038: AUTHENTICATION AMOUNT*** *Format: n12*

Amount of authentication.

⇨ ***TYPE = 0040: LIST OF INSTALLED KERNELS*** *Format: b8*

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

❑ **Byte 1** **b1**

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

❑ **Byte 2** **b1**

Bit	Description
8	RFU
7	RFU
6	RFU
5	RFU
4	RFU

Bit	Description
3	C-PACE
2	WISE
1	PURE

❑ **Byte 3 to 8** _____ **b6**

Reserved for CN use.

⇨ ***TYPE = 0045: PAYMENT VALIDITY DATE*** *Format: n6(YYMMDD)*

Validity date for a multiple payment.

⇨ ***TYPE = 0046: ADDITIONAL DATA INITIAL TRANSACTION*** *Format: structure*

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**

When absent (for instance, for a face-to-face CIT), data is filled with zero.

❑ **ACS transaction ID** _____ **ans36**

When absent (for instance, for a face-to-face CIT), data is filled with spaces.

❑ **DS transaction ID** _____ **ans36**

When absent (for instance, for a face-to-face CIT), data is filled with spaces.

❑ **Authentication merchant name** _____ **ans40**

❑ **Authentication date** _____ **n14**

❑ **Authentication amount** _____ **n12**

⇨ ***TYPE = 0056: PAYMENT ACCOUNT REFERENCE*** *Format: ans29*

Payment Account Reference linked to the underlying PAN.

⇨ ***TYPE = 5F2D: LANGUAGE PREFERENCE*** *Format: an2*

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

⇨ ***TYPE = 9F0D: ISSUER ACTION CODE - DEFAULT*** *Format: b5*

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*** *Format: b5*

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

⇨ ***TYPE = 9F0F: ISSUER ACTION CODE - ONLINE*** *Format: b5*

Indicates the issuer conditions to accept a transaction online.

Field 58: Responding machine identifier

Format: LLLVAR ans...255

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: National data

Format: LLLVAR b...255

❑ **Data type** _____ **b2**

Value	Description
ISO 8583 (V93) standardised data	
0100	Function code
0101	Message reason code
0102	Transaction year
French specific data	
0200	Transaction regulatory and technical environment (ERT)
0201	Acceptance System Components Identifier (ex ITP SA)
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	POI Components Identifier (ex ITP PA)
0216	Point of interaction extended logical number
Security data	
0300	Card security code
0301	Card security code verification results
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 value processing 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

Value	Description
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
Other data	
0800	Service attribute
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.

⇨ ***TYPE = 0100: FUNCTION CODE*** *Format: n3*

The function code specifies the purpose of a message within its message class. Values 100 to 199 are used in authorization request messages: In the case of a "standard" authorisation request, the function code used is 100 (original authorisation –accurate amount).

Value	Description
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	Delayed charges
164	No-show
165	Late operation
180 - 199	Reserved for private use

⇨ ***TYPE = 0101: MESSAGE REASON CODE*** *Format: n4*

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
1675	Deferred authorisation
1676	High amount transaction
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
1684	PAR to send to the Acceptor

Value	Description
1776 - 1999	Reserved for private use
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* *Format: n2*

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

⇨ *TYPE = 0200: ERT (REGULATORY AND TECHNICAL ENVIRONMENT)* *Format: b1*

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): Reference information for unattended terminals

Value	Description
French national classification	
Category 1	Transaction amount is known before the good or service is provided.
Category 2 – 1	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	Transaction amount is not known until the completion of the transaction. Amount cannot be estimated in advance.
International classification	
Level 1 unattended	ADM: Zero floor limit authorisation and PIN control
Level 2	SST: Zero floor limit authorisation but no PIN control
Level 3	LAT: No authorisation request and no PIN control
Level 4	In-flight commerce (not allowed for intra-regional transactions)

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

Value	Description
25	Remote payment, Television
Acceptor Initiated Transaction	
27	AIT (after Internet or face-to-face or unattended payment CIT)
28	AIT (other cases)
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 I
58	Open Payment
59	Single Ticket Transaction
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	

Value	Description
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

⇨ TYPE = 0201: ACCEPTANCE SYSTEM COMPONENTS IDENTIFIER (EX ITP SA) — Format: n12

Acceptance system terminal application identifier.

Information	Format
Manufacturer code	n3
Reference specifications version	n3
Terminal model reference	n3
Interbank application software version	n3

⇨ TYPE = 0202: ACCEPTOR CONTRACT NUMBER — Format: n7

⇨ TYPE = 0203: ACCEPTANCE SYSTEM LOGICAL NUMBER — Format: n3

⇨ TYPE = 0204: POINT OF INTERACTION LOGICAL NUMBER — Format: n3

⇨ TYPE = 0205: ACCEPTANCE SYSTEM COUNTRY CODE — Format: n3

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 — Format: n12

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) — Format: b5…16

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

❑ **Application supplier identifier** _____ **b5**

Values:

- any value compliant with ISO 7816-5.
- For CB: **A000000042**

❑ **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: shown below:

(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.

Byte 2 value	Description		
10	Face-to-face payment		
20	Remote payment	Manual entry via terminal	
21		Telephone order	
22		Mail order	
24		Internet	
25		Television	
28		Recurring payment via another type of order	
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		

58	Open Payment		
59	Single Ticket Transaction		
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		
85-99	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		

TASA/ERT correspondence table

TASA		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	Remote payment: manual entry 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 Transaction
24	Remote payment: Internet	27	Internet, subsequent transaction
25	Remote payment: Television	25	Remote payment: Television
28	Recurring payment via another type of order	28	Recurring payment via another type of order
28	Recurring payment via another type of order	21	Remote payment: Telephone
28	Recurring payment via another type of order	22	Remote payment: Mail order
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

TASA		ERT	
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	48	Payment via an unattended machine for specific activities
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
58	Open Payment	58	Open Payment
59	Single Ticket Transaction	59	Single Ticket Transaction
Quasi-cash			
60	Quasi-cash (standard case)	60	Not specified
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

Bit	Description
40 - 80	Private values
21	Wallets

Bit	Description
20	EMV/track 2 (1)

⇨ TYPE = 0215: POI COMPONENTS IDENTIFIER (EX ITP PA) — Format: n12

Point of acceptance terminal application identifier.

Information	Format
Manufacturer code	n3
Reference specifications version	n3
Terminal model reference	n3
Interbank application software version	n3

⇨ TYPE = 0216: POINT OF INTERACTION EXTENDED LOGICAL NUMBER — Format: an3

⇨ TYPE = 0300: CARD SECURITY CODE — Format: Structure

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

Value	Description
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**

Value	Description
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 — Format: Structure

⇨ TYPE = 0400: TRANSACTION IDENTIFIER OR CRYPTOGRAM SUPPLIED BY THE ACCEPTOR — *Format: b4…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 — *Format: b20…40*

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

⇨ TYPE = 0407: ELECTRONIC COMMERCE AUTHENTICATION TYPE — *Format: n2*

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 — *Format: anp1*

⇨ TYPE = 0410: CARDHOLDER AUTHENTICATION METHOD — *Format: ans2*

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 — *Format: an1*

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 — *Format: Structure*

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

❑ **Nomenclature** **n1**

Value	Description
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.

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

⇨ *TYPE = 0413: MODIFIED ELECTRONIC COMMERCE AUTHENTICATION TYPE* — *Format: b1*

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

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 = 0416: ELECTRONIC COMMERCE INDICATOR* — *Format: an2*

Electronic Commerce Indicator based on secured architecture

⇨ *TYPE = 0417: DIGITAL WALLET ADDITIONAL DATA* — *Format: an12…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* — *Format: n6*

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

- ❑ **Network** _____ **n2**
- ❑ **Technology** _____ **n**
- ❑ **Brand** _____ **n2**

⇨ *TYPE = 0419: THREE-DOMAIN SECURE RESULTS OTHERS* — *Format: Structure*

- ❑ **3DS authentication type** _____ **an2**

Value	Description
CH	Challenge
FR	Frictionless

❑ **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.

Value	Description
01	No preference – default value if the data element is absent or not set to a value
02	No authentication requested
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
10	No authentication requested (low value exemption)
11	No authentication requested (Secure corporate payment exemption)
12	Authentication requested (Device Binding prompt requested if challenge required)
13	Authentication requested (Issuer requested)
14	Authentication requested (Merchant-initiated transactions)

❑ **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*** *Format: structure*

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**

When absent, data is filled with zero.

❑ **Cardholder authentication method** **ans2**

When absent, data is filled with 2 spaces.

❑ **Cardholder authentication value calculation method** **an1**

When absent, data is filled with one space.

❑ **Result of using a secured remote payment architecture** **ansb4**

When absent, data is filled with one space.

❑ **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.

⇨ ***TYPE = 0800: SERVICE ATTRIBUTE*** *Format: n2*

Value	Description
01	No-show
02	Pre-authorisation
03	Delayed charges
04	Acceptor Initiated Transaction following a face-to-face or an unattended CIT
05	Aggregation
06	Multiple payment, first payment
07	Acceptor Initiated Transaction following an internet CIT
11	Debt recovery

⇨ ***TYPE = 0802: RISK SCORING SERVICE*** *Format: structure*

❑ **Service identifier** **b1**

Value	Description
09	Risk scoring for the acquirer
90 - 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**

Value	Description
00 - FF	e-rsb service reference

❑ **Notation value** **b2**

Value	Description
0000 - FFFF	Note or score

❑ **Notation reference value** **b2**

Value	Description
0000 - FFFF	Notation system reference

❑ **Score reason value** **b2**

Value	Description
0000 - FFFF	Notation source or score reason

❑ **Action proposal** **b2**

Value	Description
0000 - FFFF	Action proposal

❑ **Additional service data** **b12**

Reserved for future use

⇨ ***TYPE = 0805: OPTIONAL SERVICES SUPPORTED (ACCEPTOR DOMAIN)*** *Format: b2*

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

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

Field 70: Network management information code *Format: n3*

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: Original data elements *Format: n42*

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: Replacement amounts

Format: an42

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

❑ **New amount** _____ **an12**

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

❑ **Reserved for future use** _____ **an30**

Field 104: Transaction specific data

Format: LL2VAR b…999 (Datasets)

Refer to Fleet addendum

Field 112: Funds transfer data

Format: LLLVAR ans…255

This field contains all data required in funds transfer management.

❑ **Data type** _____ **an2**

Value	Description
01	Original transaction data
03	Application type identifier
05	Payer/account number
06	Counterparty PAN
07	Counterparty last name and first name

Value	Description
08	Funds transfer reason
09	BIC
10	IBAN

❑ **Data element length** _____ **n2**

❑ **Data element value** _____

⇨ ***TYPE = 01: ORIGINAL TRANSACTION DATA*** *Format: ans1…99*

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

❑ **Nomenclature** _____ **an1**

Value 3

❑ **Origin reference** _____ **ans…98**

⇨ ***TYPE = 03: APPLICATION TYPE IDENTIFIER TRANSACTION*** *Format: an2*

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

Value	Description
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*** *Format: ans 1…35*

⇨ ***TYPE = 06: COUNTERPARTY PAN*** *Format: n…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*** *Format: ans1…30*

⇨ ***TYPE = 08: FUNDS TRANSFER REASON*** *Format: ans1…40*

⇨ ***TYPE = 09: BIC (BANK IDENTIFIER CODE)*** *Format: ans1…11*

International identifier of bank.

⇨ ***TYPE = 10: IBAN*** *Format: an…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: o Domiciliary bank code: an 5 o Branch code: an 5 o Bank account number: an 11 o Check digits ('RIB key'): an 2

Field 113: Payment Facilitator address *Format: LL2VAR b…999*

Refer to Funds transfer addendum

Field 115: nexo data *Format: LLLVAR b…255*

❑ **Data type** **b2**

Value	Description
0001	nexo PoS identifier
0002	nexo Acceptance System identifier
0003	nexo certificate

❑ **Data element length** **b1**

❑ **Data element value**

⇨ ***TYPE = 0001: NEXO POS IDENTIFIER*** *Format: ans…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*** *Format: ans…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*** *Format: ans…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 118: Industry-specific data

Format: LL2VAR b...999

Field 119: Reserved for national use

Format: LL2VAR b...999

❑ **Data type** _____ **b2**

Value	Description
0001	Merchant tokenisation indicator
0009	Scheme program merchant identifier
0011	FPAN
0012	FPAN expiry date
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
0035	Special condition indicator
0040	Authentication data quality indicator
0041	Purchase identifier type
0042	Purchase identifier
0047	Debit unique reference identifier
0050	Payment by link indicator
0083	Maximum clearing date
00BC	Extended message to the transaction initiator
0200	Merchant street address
0204	Merchant payment gateway ID
0208	Pre-authorisation duration
0359	Transaction eligible for token services
0801	Acceptor advice code
0802	Reattempt frozen period
0803	Reattempt conditions
1001	Response data for clearing
1003	POI card input capabilities
1004	POI display and print capabilities
1022	Cardholder verification method used at POS
1104	Acceptor customer service phone number

Value	Description
1105	Acceptor phone number
1106	Acceptor additional contact information
1113	Service location address
1118	Recurring - Details
1119	Recurring – Indian cards
9F19	Token Requestor ID
9F25	Last four digits of PAN

❑ **Data element length** _____ **b2**

❑ **Data element value** _____

⇨ ***TYPE = 0001: MERCHANT SCHEME TOKENISATION INDICATOR*** *Format: an1*

Value	Description
1	Card-On-File tokenisation

⇨ ***TYPE = 0009: SCHEME PROGRAM MERCHANT IDENTIFIER*** *Format: ans…8*

Merchant identifier for the transaction scheme program

⇨ ***TYPE = 0011: FPAN*** *Format: n9…19*

Primary Account Number associated to the token for tokenised transactions.

⇨ ***TYPE = 0012: FPAN EXPIRY DATE*** *Format: n4*

Expiration date of the Primary Account Number associated to the token for tokenised transactions.

⇨ ***TYPE = 0013: THREE-DOMAIN SECURE COMPONENTS AVAILABILITY*** *Format: an1*

Value	Description
1	3DS server unavailable

⇨ ***TYPE = 0015: TOKEN AUTHENTICATION VERIFICATION VALUE*** *Format: b4…40*

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

⇨ ***TYPE = 0016: EXTENDED ELECTRONIC COMMERCE INDICATOR*** *Format: n3*

SLI (Security Level Indicator) in electronic commerce.

⇨ ***TYPE = 0017: AUTHENTICATION EXEMPTION STATUS INDICATOR*** *Format: an1*

Indicates the status of the exemption.

⇨ ***TYPE = 0022: 3DS PROTOCOL VERSION NUMBER*** *Format: ans1…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*** *Format: b…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 = 0035: SPECIAL CONDITION INDICATOR*** *Format: n1*

This subfield identifies the purchase of digital currency.

Value	Description
1	Purchase of Central Bank Digital Currency (CBDC) or Tokenized Deposits
2	Purchase of Stablecoin (Fiat-backed)
3	Purchase of Blockchain Native Token/Coin
4	Purchase of Non-Fungible Token (NFT)
7	Purchase of Cryptocurrency
8	Quasi-Cash
9	Payment on an existing debt

⇨ ***TYPE = 0040: AUTHENTICATION DATA QUALITY INDICATOR*** *Format: an1*

This subfield indicates whether the transaction meets authentication data quality requirements.

⇨ ***TYPE = 0041: PURCHASE IDENTIFIER TYPE*** *Format: an1*

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

Value	Description
0	Free text
1	Order number
3	Rental agreement number
4	Hotel folio number
5	Invoice number

⇨ ***TYPE = 0042: PURCHASE IDENTIFIER*** *Format: an32*

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*** *Format: ans…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 = 0050: PAYMENT BY LINK INDICATOR*** *Format: an1*

Value	Description
1	Payment by link

⇨ ***TYPE = 0083: MAXIMUM CLEARING DATE*** *Format: n4*

Date the scheme's rules require the transaction to be cleared. Julian date: format YDDD with Y from 0 to 9 and DDD from 001 to 366.

⇨ ***TYPE = 00BC: EXTENDED MESSAGE TO THE TRANSACTION INITIATOR*** *Format: ans1…101*

❑ **Control character** _____ **ans1**

Value	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 = 0200: MERCHANT STREET ADDRESS*** *Format: ans…99*

⇨ ***TYPE = 0204: MERCHANT PAYMENT GATEWAY ID*** *Format: n11*

Identify the payment gateway that ultimately sends the transaction data to the Acquirer.

⇨ ***TYPE = 0208: PRE-AUTHORISATION DURATION*** *Format: n 2*

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

⇨ TYPE = 0359: TRANSACTION ELIGIBLE FOR TOKEN SERVICES — *Format: an1*

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

⇨ TYPE = 0801: ACCEPTOR ADVICE CODE — *Format: n 2*

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

Value	Description
01	Obtain new information before the next transaction
02	Try again later
03	Never try again
04	Do not store the card number in Card-On-File

⇨ TYPE = 0802: REATTEMPT FROZEN PERIOD — *Format: n 4*

Number of hours where reattempt is not allowed

⇨ TYPE = 0803: REATTEMPT CONDITIONS — *Format: n 6*

- ❑ **Reattempt allowed duration** _____ **n4**
- ❑ **Maximum number of reattempts** _____ **n2**

⇨ TYPE = 1001: RESPONSE DATA FOR CLEARING — *Format: structure*

- ❑ **Account funding source** _____ **an1**
- ❑ **Applied Authorization Characteristics Indicator** _____ **an1**
- ❑ **Applied Market-Specific Data Identifier** _____ **an1**
- ❑ **Program Downgrade Reason Code** _____ **an2**
- ❑ **Validation code** _____ **an4**
- ❑ **Expense threshold** _____ **an1**
- ❑ **Merchant program - Merchant Verification Value** _____ **n10**
- ❑ **Applied cardholder ID method** _____ **an1**
- ❑ **Applied product platform** _____ **an2**
- ❑ **Applied account type from** _____ **an2**
- ❑ **Extended authorisation indicator** _____ **an1**
- ❑ **Reserved for future use** _____ **b0…9**

⇨ TYPE = 1003: POI CARD INPUT CAPABILITIES — *Format: b2*

- ❑ **Byte 1** _____ **b1**

Bit	Description
8	Reserved for future use
7	1 = No terminal
6	1 = Magstripe reader
5	1 = Contactless chip card reader - EMV chip context
4	1 = Contactless chip card reader – magnetic stripe context
3	1 = Contact chip card reader
2	1 = Keypad input
1	Reserved for future use

❑ **Byte 2: reserved for future use** _____ **b1**

⇨ ***TYPE = 1004: POI DISPLAY AND PRINT CAPABILITIES*** *Format: structure*

❑ **Cardholder display capabilities** _____

- ❑ **Number of lines** _____ **n4**
- ❑ **Line width** _____ **n4**
- ❑ **Reserved for future use** _____ **b6**

❑ **Merchant display capabilities** _____

- ❑ **Number of lines** _____ **n4**
- ❑ **Line width** _____ **n4**
- ❑ **Reserved for future use** _____ **b6**

❑ **Cardholder print capabilities** _____

- ❑ **Format** _____ **b1**

Bit	Description
8	Other receipt format
7	Reserved for future use
6	Reserved for future use
5	Reserved for future use
4	1 = External system (
3	1 = email
2	1 = SMS
1	1 = Paper

- ❑ **Paper line width (only for paper format)** _____ **n4**
- ❑ **Reserved for future use** _____ **b6**

❑ **Merchant print capabilities** _____

- ❑ **Format** _____ **b1**

Bit	Description
8	Other receipt format
7	Reserved for future use
6	Reserved for future use
5	Reserved for future use
4	1 = External system (
3	1 = email
2	1 = SMS
1	1 = Paper

- ❑ **Line width (only for paper format)** _____ **n4**
- ❑ **Reserved for future use** _____ **b6**

❑ **Reserved for future use** _____ **b…12**

⇨ ***TYPE = 1022: CARDHOLDER VERIFICATION METHOD USED AT POS*** *Format: b1…4*

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

Bit	Description
8	1 = Consumer device CVM
7	Reserved for future use
6	1 = Offline PIN encrypted
5	1 = Offline PIN in clear
4	1 = Online PIN
3	1 = Signature
2	1 = No CVM
1	1 = Unknown

⇨ ***TYPE = 1104: ACCEPTOR CUSTOMER SERVICE PHONE NUMBER*** *Format: ans…16*

⇨ ***TYPE = 1105: ACCEPTOR PHONE NUMBER*** *Format: ans…16*

⇨ ***TYPE = 1106: ACCEPTOR ADDITIONAL CONTACT INFORMATION*** *Format: ans…25*

⇨ ***TYPE = 1113: SERVICE LOCATION ADDRESS*** *Format: ans29*

- ❑ **Service location city name** _____ **ans13**
- ❑ **Service location country code** _____ **ans3**
- ❑ **Service location subdivision code** _____ **ans3**
- ❑ **Service location postal code** _____ **ans10**

⇨ ***TYPE = 1118: RECURRING - DETAILS*** *Format: an2*

❑ **Recurring – Frequency type** _____ **an1**

Value	Description
F	Fixed
V	Variable

❑ **Recurring – Amount type** _____ **an1**

Value	Description
F	Fixed
V	Variable

⇨ ***TYPE = 1119: RECURRING INDIAN CARDS*** *Format: Structure*

❑ **Recurring frequency** _____ **an2**

Value	Description
01	Daily
02	Twice weekly
03	Weekly
04	Ten days
05	Fortnightly
06	Monthly
07	Every two months
08	Trimester
09	Quarterly
10	Twice yearly
11	Annually
12	Unscheduled

❑ **Registration reference number** _____ **an35**

❑ **Maximum recurring payment amount** _____ **n12**

❑ **Validation indicator** _____ **an1**

Value	Description
0	Not validated
1	Validated

⇨ ***TYPE = 9F19: TOKEN REQUESTOR ID*** *Format: an 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*** *Format: n 4*

Last four digits of PAN

Field 122: Acceptor URL address *Format: LLLVAR ans…255*

Acceptor website address

Field 123: Customer related data *Format: LL2VAR b…999*

❑ **Data type** _____ **b2**

Value	Description
0006	Cardholder address
0008	Cardholder postcode
0009	Delivery address
0010	IP address
0021	Account name verification type
0024	Account Owner
0025	Account Name Request Result
0026	Account Name Match Decision
0031	Other phone number
0032	Other email address
0033	Other phone number verification result
0034	Other email address verification result

❑ **Data element length** _____ **b2**

❑ **Data element value** _____

⇨ ***TYPE = 0006: CARDHOLDER ADDRESS*** *Format: ansp…40*

Cardholder address.

⇨ ***TYPE = 0008: CARDHOLDER POSTCODE*** *Format: ansp…10*

Cardholder postcode.

⇨ ***TYPE = 0009: DELIVERY ADDRESS*** *Format: ans80*

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 — Format: ans4…45

Cardholder IP address. 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 = 0021: ACCOUNT NAME VERIFICATION TYPE — Format: an2

Value	Description
10	Funds transfer - Payee account owner name inquiry
11	Funds transfer - Payer account owner name inquiry

⇨ TYPE = 0024: ACCOUNT OWNER — Format: ans105

- ❑ **Name, Given** _____ **ans35**
- ❑ **Name, Middle** _____ **ans35**
- ❑ **Name, Last** _____ **ans35**

⇨ TYPE = 0025: ACCOUNT NAME REQUEST RESULT — Format: an2

Value	Description
MP	Name match performed
NP	Name match not performed
NS	Name match not supported

⇨ TYPE = 0026: ACCOUNT NAME MATCH DECISION — Format: an8

- ❑ **Full name account match decision** _____ **an2**

Value	Description
MA	Full match
NO	No match
PA	Partial match

- ❑ **Last name account match decision** _____ **an2**

Value	Description
MA	Full match
NO	No match
PA	Partial match

- ❑ **Middle name account match decision** _____ **an2**

Value	Description
MA	Full match
NO	No match
PA	Partial match

❑ **First name account match decision** _____ **an2**

Value	Description
MA	Full match
NO	No match
PA	Partial match

⇨ ***TYPE = 0031: OTHER PHONE NUMBER*** *Format: ans16*

⇨ ***TYPE = 0032: OTHER EMAIL ADDRESS*** *Format: ans99*

⇨ ***TYPE = 0033: OTHER PHONE NUMBER VERIFICATION RESULT*** *Format: an1*

Value	Description
1	Verified
2	Failed
3	Not performed

⇨ ***TYPE = 0034: OTHER EMAIL ADDRESS VERIFICATION RESULT*** *Format: an1*

Value	Description
1	Verified
2	Failed
3	Not performed

END OF DOCUMENT

2AP Authorisation

Acceptor to Acquirer Protocol
(CB2A)

VOLUME 3.1 - NETWORK MANAGEMENT

Version 1.6.6 - September 2025

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.

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 2AP Authorisation/EMA and 2AP 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)
- TNR, TSI and TMA Timers (CP (ex 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 CP (ex 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

Value	Meaning
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 (APM (ex MPE), UPM (ex MPA)) for further information about the actions to take.

2.2 RESPONSE CODES FOR AN ECHO TEST TRANSACTION

Value	Meaning
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 (APM (ex MPE), UPM (ex MPA)) for further information about the actions to take.

3 MESSAGES DESCRIPTION

How to read the tables

The term "transaction" refers to a set of "requests/responses".

The term "message" refers either to 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 receiving system.
- **Non-applicable** - Field is not defined in the standard.

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 the 2AP 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

3.1 ECHO TEST REQUEST AND RESPONSE

***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**: Echo test response: **0810**

N°	Definition	A	B
MTI	MTI	X	X
Bitmap	1st bitmap	X	X
1	2nd bitmap	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

N°	Definition	A	B
58	Responding machine identifier	.	FS
70	Network management information code	X	XQ

3.2 SIGN-ON, SIGN-OFF AND RESPONSE

***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 request: **0800**	**B**: Sign-On response: **0810**

N°	Definition	A	B
MTI	MTI	X	X
Bitmap	1st bitmap	X	X
1	2nd bitmap	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 (company registration number)	C (29)	FQ
A0	IDSA (acceptance system identifier assigned by an acquirer)	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

3.3 COMMENTS

N°	Comments
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

END OF DOCUMENT

2AP Authorisation

Acceptor to Acquirer Protocol
(CB2A)

VOLUME 3.2 - FACE-TO-FACE PAYMENT – UNATTENDED PAYMENT

Version 1.6.6 - September 2025

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

Value	Meaning
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
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
39	No such account type
40	Requested function not supported
41	Lost card
43	Stolen card, pick-up
46	Business specific error
47	Restricted card
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
5C	Transaction not supported/blocked by issuer
60	Card acceptor contact acquirer
62	Card invalid in region or country
63	Security violation
64	Transaction does not fulfil Anti-Money Laundering requirement
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	Incorrect CVV, dCVV, iCVV
91	Issuer or switch is inoperative
93	Transaction cannot be completed - Violation of law
94	Duplicate transmission
96	System malfunction, no rerouting requested
97	General monitoring timeout
98	Server inaccessible (set by the server)
9G	Blocked by cardholder/contact cardholder
A0	Fallback in EMV 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 APM (Attended Payment Manual).

2.2 RESPONSE CODES FOR AN UNATTENTED PAYMENT AUTHORISATION REQUEST

Value	Meaning
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

Value	Meaning
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
39	No such account type
40	Requested function not supported
41	Lost card
43	Stolen card, pick-up
46	Business specific error
47	Restricted card
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
5C	Transaction not supported/blocked by issuer
60	Card acceptor contact acquirer
61	Exceeds withdrawal amount limit
62	Card invalid in region or country
63	Security violation
64	Transaction does not fulfil Anti-Money Laundering requirement
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	Incorrect CVV, dCVV, iCVV
91	Issuer or switch is inoperative
93	Transaction cannot be completed - Violation of law
94	Duplicate transmission
96	System malfunction, no rerouting requested
97	General monitoring timeout
98	Server inaccessible (set by the server)

Value	Meaning
9G	Blocked by cardholder/contact cardholder
A0	Fallback in EMV 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 UPM (Unattented Payment Manual).

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

Value	Meaning
00	Successful approval/completion
17	Customer cancellation
21	No action taken
32	Partial completion (ISO 8583)
99	Malfunction

2.4 RESPONSE CODES FOR A RESPONSE TO A REVERSAL REQUEST RELATED TO A FACE-TO-FACE PAYMENT AUTHORISATION REQUEST

Value	Meaning
00	Successful approval/completion
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
80	Approved transaction without financial impact
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 CONTACTLESS PAYMENT

3.1 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

3.2 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

4 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.

4.1 INFORMATION ON DATA ELEMENT VALUES

4.1.1 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

4.1.2 Field 3 in 0400/0401 messages

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

4.1.3 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.

4.1.4 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.

4.1.5 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.

4.1.6 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.

5 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: 010
- 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.

6 MESSAGES DESCRIPTION

How to read the tables

The term "transaction" refers to a set of "requests/responses".

The term "message" refers either to 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 receiving system.
- **Non-applicable** - Field is not defined in the standard.

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 the 2AP 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

6.1 AUTHORISATION REQUEST AND RESPONSE

***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: Auth request EMV: **0100**	**B**: Auth request Magstripe: **0100**	**C**: Auth response: **0110**

N°	Definition	A	B	C
MTI	MTI	X	X	X
Bitmap	1st bitmap	X	X	X
1	2nd bitmap	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
6	Amount, cardholder billing	C (100)	C (100)	FQ
7	Transmission date and time	C (117)	C (117)	.
10	Conversion rate, cardholder billing	C (100)	C (100)	FQ
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

N°	Definition	A	B	C
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	C (23)	C (23)	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 relating 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	2AP specification date	C (3)	C (3)	.
95	Unique transaction identifier	.	.	C (3)
96	SIRET (company registration number)	C (63)	C (63)	FQ
97	IDPA (point of interaction identifier assigned by an acquirer)	C (63)	C (63)	FQ
98	Card product identifier	.	.	C (164)
99	Original unique transaction identifier	C (3)	C (3)	F
A0	IDSA (acceptance system identifier assigned by an acquirer)	C (63)	C (63)	FQ
48	Security Data	C (2)	C (2)	.
0001	KSN (Key Serial Number)	C (31)	C (31)	.
0002	BDK (Base Derivation Key) name	C (29)	C (29)	.
0003	BDK (Base Derivation Key) version	C (154)	C (154)	.
49	Currency code, transaction	X	X	XQ

N°	Definition	A	B	C
51	Currency code, cardholder billing	C (100)	C (100)	FQ
52	PIN data	C (32)	C (32)	C (12)
53	Security related control information	X	X	X
54	Additional amounts	C (118)	C (118)	C (118)
43	Cumulative total of authorised amount	C (150)	.	CQ (150)
44	Tip amount	C (119)	C (119)	CQI
57	Original amount	.	.	C (115)
60	POI Amount before DCC conversion	C (100)	C (100)	FQ
87	Total Discount Amount for discount purposes	C (179)	C (179)	.
88	Additional transaction fee 1	C (179)	C (179)	.
89	Additional transaction fee 2	C (179)	C (179)	.
90	Amount, anticipated	C (174)	C (174)	.
55	Integrated circuit card system related data	C (2)	C (2)	CQ (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 (173)	.	.
0096	Kernel identifier - Terminal	C (29)	.	.
009A	Terminal transaction date (EMV tag 9A)	C (138)	.	.
009C	Transaction Type	X	.	.
5F24	Application Expiration Date	X	.	FQ
9F02	Amount authorised	C (135)	.	.
9F06	Card Application Identifier (AID)	X	C (48)	.
9F0A	Application Selection Registered Proprietary Data	C (84)	C (84)	.
9F10	Issuer Application Data (IAD)	C (85)	C (85)	.
9F1F	Track 1 Discretionary Data	C (48)	C (48)	.
9F26	Application Cryptogram (ARQC)	C (173)	.	.
9F27	Cryptogram Information Data	C (173)	.	.
9F33	Terminal capabilities	X	C (101)	.
9F34	Cardholder verification method (CVM) results	C (29)	.	.
9F35	Terminal Type	C (3)	C (3)	.
9F36	Application Transaction Counter (ATC)	C (173)	.	.
9F37	Unpredictable Number	C (173)	.	.
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)	.	.
9F81	Card authenticated application data	C (3)	.	.
DF68	Kernel ID used	C (48)	C (48)	.

N°	Definition	A	B	C
DF80	ICC processing results	C (127)	C (29)	FQ
DF81	Card application type	X	C (49)	FQ
DF85	RTT (Terminal processing results))	C (48)	.	.
DF86	Device information	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 organization	C (3)	C (3)	.
0025	Payment facilitator identifier	C (3)	C (3)	.
0026	Marketplace identifier	C (3)	C (3)	.
0027	Final merchant identifier	C (3)	C (3)	.
0028	Payment use case	C (176)	C (176)	.
0031	Payment number	C (175)		
0032	Total number of payments	C (175)		
0040	List of installed kernels	C (3)	C (3)	.
0045	Payment validity date	C (175)		
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	Acceptance System Components Identifier (ex ITP SA)	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	POI Components Identifier (ex ITP PA)	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)	.

N°	Definition	A	B	C
01	Original transaction data	C (94)	C (94)	.
03	Application type identifier transaction	C (94)	C (94)	.
08	Funds transfer reason	C (147)	.	.
10	IBAN	C (147)	.	.
115	nexo data	C (2)	C (2)	.
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)
0012	FPAN expiry date	.	.	C (3)
0022	3DS protocol version number	.	.	FQ
0035	Special condition indicator	C (3)	C (3)	.
0047	Debit unique reference identifier	C (156)	C (156)	F
0083	Maximum clearing date	.	.	C (3)
00BC	Extended message to the transaction initiator	.	.	F
0200	Merchant street address	C (3)	C (3)	.
0208	Pre-authorisation duration	C (63)	C (63)	.
0801	Acceptor advice code	.	.	C (3)
0802	Reattempt frozen period	.	.	C (161)
0803	Reattempt conditions	.	.	C (162)
1001	Response data for clearing	.	.	C (3)
1003	POI card input capabilities	C (29)	C (29)	.
1004	POI display and print capabilities	C (29)	C (29)	.
1022	Cardholder verification method used at POS	C (3)	C (3)	FQ
1104	Acceptor customer service phone number	C (3)	C (3)	.
1105	Acceptor phone number	C (3)	C (3)	.
1106	Acceptor additional contact information	C (3)	C (3)	.
1113	Service location address	C (166)	C (166)	.
1118	Recurring - Details	C (3)	C (3)	.

6.2 PROXIMITY WALLET - AUTHORISATION REQUEST AND RESPONSE

***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: Auth request Wallet: **0100**	**B**: Auth response Wallet: **0110**

N°	Definition	A	B
MTI	MTI	X	X
Bitmap	1st bitmap	X	X
1	2nd bitmap	C (1)	C (1)
2	Primary Account Number	X	XQ
3	Processing code	X	XQ

N°	Definition	A	B
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	C (23)	FQ
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 relating 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	2AP specification date	C (3)	.
95	Unique transaction identifier	.	C (3)
96	SIRET (company registration number)	C (63)	FQ
97	IDPA (point of interaction identifier assigned by an acquirer)	C (63)	FQ
99	Original unique transaction identifier	C (3)	F
A0	IDSA (acceptance system identifier assigned by an acquirer)	C (63)	FQ
49	Currency code, transaction	X	XQ

N°	Definition	A	B
53	Security related control information	X	X
54	Additional amounts	C (118)	C (118)
43	Cumulative total of 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 organization	C (3)	.
0025	Payment facilitator identifier	C (3)	.
0026	Marketplace 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	Acceptance System Components Identifier (ex ITP SA)	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	POI Components Identifier (ex ITP PA)	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)	.
112	Funds transfer data	C (2)	.

N°	Definition	A	B
01	Original transaction data	C (94)	.
03	Application type identifier transaction	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)	.

6.3 REVERSAL REQUEST AND RESPONSE

***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: Reversal request: **0400/0401** **B**: Reversal response: **0410**

N°	Definition	A	B
MTI	MTI	X	X
Bitmap	1st bitmap	X	X
1	2nd bitmap	C (1)	C (1)
2	Primary Account Number	XQI	XQ
3	Processing code	XQI	XQ
4	Amount, transaction	X	XQ
6	Amount, cardholder billing	C (100)	FQ
7	Transmission date and time	XS	FS
10	Conversion rate, cardholder billing	C (100)	FQ
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
35	Track 2 data	C (3)	.
37	Retrieval reference number	C (23)	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)

N°	Definition	A	B
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	2AP specification date	CQI (104)	.
95	Unique transaction identifier	CRI (116)	FQ
96	SIRET (company registration number)	CQI (104)	FQ
97	IDPA (point of interaction identifier assigned by an acquirer)	CQI (104)	FQ
99	Original unique transaction identifier	CQI (104)	.
A0	IDSA (acceptance system identifier assigned by an acquirer)	CQI (104)	FQ
49	Currency code, transaction	XQI	XQ
51	Currency code, cardholder billing	C (100)	FQ
52	PIN data	C (12)	.
53	Security related control information	XS	XS
54	Additional amounts	C (118)	C (118)
87	Total Discount Amount for discount purposes	C (179)	.
88	Additional transaction fee 1	C (179)	.
89	Additional transaction fee 2	C (179)	.
55	Integrated circuit card system related data	C (2)	C (2)
0056	Data equivalent to ISO track 1 read in contactless mode	CQI (104)	.
0057	Track 2 equivalent data	C (3)	.
0082	Application Interchange Profile (AIP)	C (104)	.
0095	Terminal Verification Results (TVR)	C (104)	.
009A	Terminal transaction date (EMV tag 9A)	C (104)	.
009C	Transaction Type	C (104)	.
5F24	Application Expiration Date	CQI (104)	.
9F02	Amount authorised	CQI (104)	.
9F06	Card Application Identifier (AID)	CQI (104)	.
9F0A	Application Selection Registered Proprietary Data	CQI (104)	.
9F10	Issuer Application Data (IAD)	C (104)	.
9F1F	Track 1 Discretionary Data	C (3)	.
9F26	Application Cryptogram (ARQC)	C (104)	.
9F27	Cryptogram Information Data	C (104)	.
9F33	Terminal capabilities	C (104)	.
9F35	Terminal Type	CQI (104)	.

N°	Definition	A	B
9F36	Application Transaction Counter (ATC)	C (104)	.
9F37	Unpredictable Number	C (104)	.
9F66	Terminal Transaction Qualifiers (TTQ)	C (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	Device information	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 organization	CQI (104)	.
0025	Payment facilitator identifier	CQI (104)	.
0026	Marketplace 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	Acceptance System Components Identifier (ex ITP SA)	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	CQI (104)	.
0207	Cardholder total amount	CQI (104)	.
020B	TASA (Card acceptor application type)	XQI	.
0215	POI Components Identifier (ex ITP PA)	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

N°	Definition	A	B
95	Replacement amounts	XS	FQ
112	Funds transfer data	C (2)	.
01	Original transaction data	C (94)	.
03	Application type identifier transaction	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)
0035	Special condition indicator	C (3)	.
0047	Debit unique reference identifier	CQI (104)	.
00BC	Extended message to the transaction initiator	.	F

6.4 CALL CENTER - AUTHORISATION REQUEST AND RESPONSE

***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: Auth request call center: **0100**	**B**: Auth response call center: **0110**

N°	Definition	A	B
MTI	MTI	X	X
Bitmap	1st bitmap	X	X
1	2nd bitmap	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	C (23)	CQ (79)
38	Authorisation identification response	.	C (10)

N°	Definition	A	B
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	2AP specification date	C (3)	.
96	SIRET (company registration number)	C (63)	FQ
97	IDPA (point of interaction identifier assigned by an acquirer)	C (63)	FQ
A0	IDSA (acceptance system identifier assigned by an acquirer)	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)
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	Acceptance System Components Identifier (ex ITP SA)	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)	.

6.5 COMMENTS

N°	Comments
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
23	Mandatory if managed by the Acceptor
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 absent
31	Mandatory if DUKPT used to encrypt the PIN
32	Mandatory if remote PIN verification, otherwise absent
46	Mandatory if needed to identify the corresponding service
47	Mandatory for debit transaction in case of pre-authorisation, additional charges, aggregated payments or transit, mandatory for a card validity check
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
100	May be used by a private Dynamic Currency Conversion application
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

N°	Comments
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, mandatory for the first transaction of a multiple payment, mandatory for mobility
145	Mandatory for a debit transaction when (service attribute = 2-Pre-authorisation or 3-Additional charges, or 5-Aggregation) or ERT = 58; 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
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
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
164	May be sent by some international schemes
165	Mandatory if present in the card application and if function code not equal to 104 and 105 (resubmission), otherwise absent
166	May by set when the sale location is different from the merchant store location; otherwise absent
173	Mandatory for a debit transaction, mandatory if available for a credit transaction
174	May be present for a card validity check, otherwise absent
175	May be present for a multiple payment
176	Mandatory if data element was provided to the system (parameters downloading), mandatory for a multiple payment, otherwise absent
179	May be present for Visa fleet

END OF DOCUMENT

2AP Authorisation

Acceptor to Acquirer Protocol
(CB2A)

VOLUME 3.3 - REMOTE PAYMENT – SECURED ELECTRONIC COMMERCE

Version 1.6.6 - September 2025

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

Value	Meaning
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
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
39	No such account type
40	Requested function not supported
41	Lost card
43	Stolen card
46	Business specific error
47	Restricted card
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
5C	Transaction not supported/blocked by issuer
60	Card acceptor contact acquirer

62	Card invalid in region or country
63	Security violation
64	Transaction does not fulfil Anti-Money Laundering requirement
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
79	Life cycle
83	Fraud/security
8P	Policy
91	Issuer or switch is inoperative
93	Transaction cannot be completed - Violation of law
94	Duplicate transmission
96	System malfunction, no rerouting requested
97	General monitoring timeout
98	Server inaccessible (set by the server)
9G	Blocked by cardholder/contact cardholder
A1	Soft decline (electronic commerce only), 3DS with challenge required
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
Z5	Valid account but amount is not supported

For information about the actions to be taken, refer to the specifications in SEcoM (ex MPADS).

2.2 RESPONSE CODES FOR A REMOTE PAYMENT REVERSAL REQUEST

Value	Meaning
00	Successful approval/completion
17	Customer cancellation
21	No action taken (unable to back out prior transaction)
32	Partial completion (ISO 8583)
99	Initiator domain incident

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

Value	Meaning
00	Successful approval/completion
03	Invalid merchant or service provider
12	Invalid transaction
13	Invalid amount

Value	Meaning
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
80	Approved transaction without financial impact
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 REVERSALES 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

3.1 INFORMATION ON DATA ELEMENT VALUES

3.1.1 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

3.1.2 Field 3 in 0400/0401 messages

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

3.1.3 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.

3.1.4 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.

3.1.5 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.

4 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) set to 0
- field 59 type 100 (Function code) set to 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 10
- field 4 set to 0
- field 56 type 0028 (Payment use case) = 04 (Shipment payment)

5 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)

6 MESSAGES DESCRIPTION

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 2AP 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.

6.1 AUTHORISATION REQUEST AND RESPONSE

***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: Auth request: **0100**	**B**: Auth response: **0110**

N°	Definition	A	B
MTI	MTI	X	X
Bitmap	1st bitmap	X	X
1	2nd bitmap	C (1)	C (1)
2	Primary Account Number	XS	XQ
3	Processing code	XS	XQ
4	Amount, transaction	XS	XQ
6	Amount, cardholder billing	C (100)	FQ
7	Transmission date and time	C (117)	.
10	Conversion rate, cardholder billing	C (100)	FQ
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)

N°	Definition	A	B
25	Point of service condition code	XS	FQ
27	Authorisation identification response length	C (7)	.
28	Amount, transaction fee	C (29)	.
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 relating 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	2AP specification date	C (3)	.
95	Unique transaction identifier	.	C (3)
96	SIRET (company registration number)	C (63)	FQ
97	IDPA (point of interaction identifier assigned by an acquirer)	C (63)	FQ
98	Card product identifier	.	C (164)
99	Original unique transaction identifier	C (3)	F
A0	IDSA (acceptance system identifier assigned by an acquirer)	C (63)	FQ
49	Currency code, transaction	XS	XQ
51	Currency code, cardholder billing	C (100)	FQ
53	Security related control information	XS	X
54	Additional amounts	C (118)	.
43	Cumulative total of authorised amount	C (3)	.
60	POI Amount before DCC conversion	C (100)	FQ
90	Amount, anticipated	C (174)	.
95	Transfer service	C (177)	.
55	Integrated circuit card system related data	C (2)	.

N°	Definition	A	B
0082	Application Interchange Profile (AIP)	C (148)	.
0095	Terminal Verification Results (TVR)	C (148)	.
009A	Terminal transaction date (EMV tag 9A)	C (139)	.
009C	Transaction Type	C (148)	.
9F02	Amount authorised	C (140)	.
9F10	Issuer Application Data (IAD)	C (148)	.
9F26	Application Cryptogram (ARQC)	C (136)	.
9F27	Cryptogram Information Data	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)	.
0011	Number of articles	C (3)	.
0012	Tokenised 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 organization	C (3)	.
0025	Payment facilitator identifier	C (3)	.
0026	Marketplace 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)	.
0032	Total number of payments	C (3)	.
0033	Exemption indicator	C (3)	.
0036	Authentication 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	C (3)	.
0056	Payment Account Reference	.	C (108)

N°	Definition	A	B
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	Acceptance System Components Identifier (ex ITP SA)	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	POI Components Identifier (ex ITP PA)	C (3)	FQ
0300	Card Security Code	X	C (12)
0301	Card security code verfication results	.	C (12)
0400	Transaction identifier or cryptogram supplied by the acceptor	C (12)	.
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)
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	Electronic commerce data initial 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)	.
01	Original transaction data	C (94)	.
03	Application type identifier transaction	C (94)	.
05	Payer/account number	C (108)	.
06	Counterparty PAN	C (142)	.
07	Counterparty last name and first name	C (144)	.
08	Funds transfer reason	C (147)	.
09	BIC (Bank Identifier Code)	F	.
10	IBAN	C (147)	.
115	nexo data	C (2)	.

N°	Definition	A	B
0001	nexo PoS identifier	C (3)	.
0002	nexo Acceptance System identifier	C (3)	.
0003	nexo certificate	C (3)	.
118	Industry-specific data	C (2)	.
119	Reserved for national use	C (2)	C (2)
0001	Merchant scheme 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 indicator	C (163)	.
0035	Special condition indicator	C (3)	.
0040	Authentication data quality indicator	.	C (3)
0041	Purchase identifier type	C (29)	.
0042	Purchase identifier	C (29)	.
0047	Debit unique reference identifier	C (156)	F
0050	Payment by link indicator	C (3)	.
0083	Maximum clearing date	.	C (3)
00BC	Extended message to the transaction initiator	.	F
0200	Merchant street address	C (3)	.
0204	Merchant payment gateway ID	C (3)	.
0208	Pre-authorisation duration	C (63)	.
0359	Transaction eligible for token services	.	C (164)
0801	Acceptor advice code	.	C (3)
0802	Reattempt frozen period	.	C (161)
0803	Reattempt conditions	.	C (162)
1001	Response data for clearing	.	C (3)
1022	Cardholder verification method used at POS	C (3)	.
1104	Acceptor customer service phone number	C (3)	.
1105	Acceptor phone number	C (3)	.
1106	Acceptor additional contact information	C (3)	.
1113	Service location address	C (166)	.
1118	Recurring - Details	C (3)	.
1119	Recurring Indian cards	C (3)	.
9F19	Token Requestor ID	C (3)	.
9F25	Last four digits of PAN	.	C (3)
122	Acceptor URL address	C (3)	C (2)
123	Customer related data	.	C (2)
0006	Cardholder address	C (3)	.

N°	Definition	A	B
0008	Cardholder postcode	C (3)	.
0009	Delivery address	C (3)	.
0010	IP address	C (3)	.
0021	Account name verification type	C (171)	.
0024	Account owner	C (169)	.
0025	Account name request result	.	C (170)
0026	Account name match decision	.	C (170)
0031	Other phone number	C (172)	.
0032	Other email address	C (172)	.
0033	Other phone number verification result	.	C (172)
0034	Other email address verification result	.	C (172)

6.2 REVERSAL REQUEST AND RESPONSE

***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: Reversal request: **0400/0401** **B**: Reversal response: **0410**

N°	Definition	A	B
MTI	MTI	X	X
Bitmap	1st bitmap	X	X
1	2nd bitmap	C (1)	C (1)
2	Primary Account Number	XQI	XQ
3	Processing code	XQI	XQ
4	Amount, transaction	X	XQ
6	Amount, cardholder billing	C (100)	FQ
7	Transmission date and time	XS	FS
10	Conversion rate, cardholder billing	C (100)	FQ
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	C (23)	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

N°	Definition	A	B
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	2AP specification date	CQI (104)	.
95	Unique transaction identifier	CRI (116)	FQ
96	SIRET (company registration number)	CQI (104)	FQ
97	IDPA (point of interaction identifier assigned by an acquirer)	CQI (104)	FQ
99	Original unique transaction identifier	CQI (104)	.
A0	IDSA (acceptance system identifier assigned by an acquirer)	CQI (104)	FQ
49	Currency code, transaction	XQI	XQ
51	Currency code, cardholder billing	C (100)	FQ
53	Security related control information	XS	XS
54	Additional amounts	C (118)	.
95	Transfer service	C (177)	.
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 (EMV tag 9A)	FQI	.
009C	Transaction Type	FQI	.
9F02	Amount authorised	FQI	.
9F10	Issuer Application Data (IAD)	FQI	.
9F26	Application Cryptogram (ARQC)	FQI	.
9F27	Cryptogram Information Data	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	Tokenised payment solution identifier	CQI (104)	.
0019	Serial number	CQI (104)	.
0020	Resend counter	CQI (104)	.
0024	Independent sales organization	CQI (104)	.

N°	Definition	A	B
0025	Payment facilitator identifier	CQI (104)	.
0026	Marketplace 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	Acceptance System Components Identifier (ex ITP SA)	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	POI Components Identifier (ex ITP PA)	CQI (104)	.
0400	Transaction identifier or cryptogram supplied by the acceptor	C (12)	.
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)	.
0416	Electronic commerce indicator	CQI (104)	.
0417	Digital wallet additional data	CQI (104)	.
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 transaction	CQI (104)	.
06	Counterparty PAN	CQI (104)	.
07	Counterparty last name and first name	CQI (104)	.
08	Funds transfer reason	CQI (104)	.
09	BIC (Bank Identifier Code)	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)	.

N°	Definition	A	B
119	Reserved for national use	C (2)	C (2)
0035	Special condition indicator	C (3)	.
0047	Debit unique reference identifier	CQI (104)	.
00BC	Extended message to the transaction initiator	.	F
1119	Recurring Indian cards	C (3)	.

6.3 COMMENTS

N°	Comments
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 CIT, mandatory for MIT with 3RI authentication, mandatory if available for a CIT 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 if managed by the Acceptor
29	Mandatory if available, otherwise absent
46	Mandatory if needed to identify 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 pre-authorisation, incremental authorisation, additional charges, no-show transaction or aggregated payments ; mandatory for a card validity check ; mandatory if available for a refund transaction
100	May be used by a private Dynamic Currency Conversion application
102	Mandatory for a debit transaction if EMV 3DS was used, 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

N°	Comments
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
132	Mandatory if available for a digital wallet and if field 59 type 0418 is set, otherwise absent
134	Mandatory if a digital wallet is used, otherwise absent
136	Mandatory for a secured e-commerce debit transaction executed in EMV mode, otherwise absent
137	Mandatory if available and if a tokenised 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 a debit transaction when (service attribute = 2-Pre-authorisation or 3-Additional charges or 5-Aggregation); mandatory for a card-to-card funds transfer or Original Credit; mandatory if available for a refund
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
166	May by set when the sale location is different from the merchant store location; otherwise absent
169	Mandatory for the account name inquiry service
170	Can be set for the account name inquiry service
171	Mandatory for the account name inquiry service in funds transfer context
172	Mandatory for the Account Verification Request service
174	May be present for a card validity check, otherwise absent
177	May be set for Visa funds transfer

END OF DOCUMENT

2AP Authorisation

Acceptor to Acquirer Protocol
(CB2A)

VOLUME 3.4 - MANUAL CASH DISBURSEMENT

Version 1.6.6 - September 2025

Table of contents

1 INTRODUCTION

The present volume describes manual cash disbursements.

This service allow a merchant / agent to propose cash withdrawal in its shop/premises.

The service is only opened for EMV contact and contactless transactions.

Manual Cash Disbursement characteristics:

- ERT = 75
- Transaction Type
  - 17 in contact mode
  - 01 (kernel 3) ou 17 (kernel 2 et CPACE) in contactless mode
- Processing code = 17
- Location category code = RM ou RG

1.1 OVERVIEW

The purpose of this service is to:

- request a debit authorisation obtain a response to this authorisation
- request (approval or reason for decline)
- reverse a previously granted authorisation
- 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 MANUAL CASH DISBURSEMENT AUTHORISATION REQUEST

Value	Meaning
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

Value	Meaning
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 A MANUAL CASH DISBURSEMENT REVERSAL REQUEST

Value	Meaning
00	Successful approval/completion
17	Customer cancellation
21	No action taken
32	Partial completion (ISO 8583)
99	Malfunction

2.3 RESPONSE CODES FOR A RESPONSE TO A REVERSAL REQUEST RELATED TO A MANUAL CASH DISBURSMENT

Value	Meaning
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

Value	Meaning
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 CONTACTLESS PAYMENT

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 REQUIREMENTS RELATED TO REVERSALS

Bit no. 3 in field 59 type 0805 is used to indicate that the acceptance system is performing the reversal.

4.1 INFORMATION ON DATA ELEMENT VALUES

4.1.1 Field 47 type 08 in all messages

Cash manual disbursements are identified by a field 47 type 08 'Location Category Code' = RG or RM.

4.1.2 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

4.1.3 Field 3 in 0400/0401 messages

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

4.1.4 Field 4 in 0110 messages

The value must be equal to the value in the request.

4.1.5 Field 4 in 0400 messages

The value must be equal to the value in the request.

4.1.6 Field 54 in 0110 messages

This field is absent.

4.1.7 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.

5 MESSAGES DESCRIPTION OF REMOTE FUNDS TRANSFERS

How to read the tables

The term "transaction" refers to a set of "requests/responses".

The term "message" refers either to 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 receiving system.
- **Non-applicable** - Field is not defined in the standard.

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 the 2AP 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

5.1 AUTHORISATION REQUEST AND RESPONSE

***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: Manual cash disbursement: **0100**	**B**: Response to manual cash disbursement: **0110**

N°	Definition	A	B
2	Primary Account Number	X	XQ
3	Processing code	X	XQ
4	Amount, transaction	X	X
6	Amount, cardholder billing	C (100)	FQ
7	Transmission date and time	C (117)	.
10	Conversion rate, cardholder billing	C (100)	FQ
11	Systems trace audit number	XS	XQ
12	Time, local transaction	XS	FQ
13	Date, local transaction	XS	FQ
14	Date, expiration	.	FQ
18	Merchant type	X	FQ
22	Point of service entry mode	X	FQ
23	Card Sequence Number	C (84)	(84)
25	Point of service condition code	X	FQ

N°	Definition	A	B
26	PIN length	C (30)	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	C (23)	(79)
38	Authorisation identification response	.	(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	.	(2)
AA	Incorrect field	.	(69)
AB	Security error	.	(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	.	(12)
CB	Application cryptogram verification results	.	(12)
CD	Information relating to liability shift	.	F
47	Additional data – National	C (2)	(2)
08	Location category code	X	XQ
30	Additional card reading capabilities	C (3)	FQ
31	Point of interaction information	C (3)	FQ
33	2AP specification date	C (3)	.
95	Unique transaction identifier	.	(3)
96	SIRET (company registration number)	C (63)	FQ
97	IDPA (point of interaction identifier assigned by an acquirer)	C (63)	FQ
98	Card product identifier	.	(164)
99	Original unique transaction identifier	C (3)	F
A0	IDSA (acceptance system identifier assigned by an acquirer)	C (63)	FQ
48	Security Data	C (2)	.
0001	KSN (Key Serial Number)	C (31)	.
0002	BDK (Base Derivation Key) name	C (29)	.
0003	BDK (Base Derivation Key) version	C (154)	.
49	Currency code, transaction	X	XQ
51	Currency code, cardholder billing	C (100)	FQ
52	PIN data	C (32)	(12)
53	Security related control information	X	X
57	Original amount	.	C (115)

N°	Definition	A	B
55	Integrated circuit card system related data	C (2)	(2)
0056	Data equivalent to ISO track 1 read in contactless mode	C (48)	.
0057	Track 2 equivalent data	C (165)	.
0071	Issuer Script Template 1	.	(24)
0072	Issuer Script Template 2	.	(24)
0082	Application Interchange Profile (AIP)	X	.
0091	Issuer Authentication Data	.	(24)
0095	Terminal Verification Results (TVR)	C (160)	.
0096	Kernel identifier - Terminal	C (29)	.
009A	Terminal transaction date (EMV tag 9A)	C (138)	.
009C	Transaction Type	X	.
5F24	Application Expiration Date	X	FQ
9F02	Amount authorised	C (135)	.
9F06	Card Application Identifier (AID)	X	.
9F0A	Application Selection Registered Proprietary Data	C (84)	.
9F10	Issuer Application Data (IAD)	C (85)	.
9F1F	Track 1 Discretionary Data	C (48)	.
9F26	Application Cryptogram (ARQC)	C (173)	.
9F27	Cryptogram Information Data	C (160)	.
9F33	Terminal capabilities	X	.
9F34	Cardholder verification method (CVM) results	C (29)	.
9F35	Terminal Type	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	.	.
9F7C	Issuer proprietary data	C (48)	.
DF68	Kernel ID used	C (48)	.
DF80	ICC processing results	C (127)	F
DF81	Card application type	X	FQ
DF85	RTT (Terminal processing results))	C (48)	.
DF86	Device information	C (3)	.
56	Additional data	C (2)	(2)
0001	Payment Facilitator Data	C (3)	.
0002	Application selection indicator	C (3)	.
0019	Serial number	C (3)	.
0024	Independent sales organization	C (3)	.
0025	Payment facilitator identifier	C (3)	.
0026	Marketplace identifier	C (3)	.
0027	Final merchant identifier	C (3)	.
0040	List of installed kernels	C (3)	.

N°	Definition	A	B
0056	Payment Account Reference	.	(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)	(2)
0101	Message reason code	X	FQ
0200	ERT (Regulatory and technical environment)	X	FQ
0201	Acceptance System Components Identifier (ex ITP SA)	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	X	FQ
020B	TASA (Card acceptor application type)	X	FQ
0215	POI Components Identifier (ex ITP PA)	C (3)	FQ
0216	Point of interaction extended logical number	C (152)	FQ
0805	Optional services supported (acceptor domain)	C (3)	.
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)	(2)
0011	FPAN	.	(3)
0012	FPAN expiry date	.	(3)
00BC	Extended message to the transaction initiator	.	F
1003	POI card input capabilities	C (29)	.
1004	POI display and print capabilities	C (29)	.
1022	Cardholder verification method used at POS	C (3)	FQ
1104	Acceptor customer service phone number	C (3)	.
1105	Acceptor phone number	C (3)	.
1106	Acceptor additional contact information	C (3)	.
1113	Service location address	C (166)	.

5.2 REVERSAL REQUEST AND RESPONSE

***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: **0100**	**B**: Response to payment reversal request: **0110**

N°	Definition	A	B
1	2nd bitmap	C (1)	C (1)
2	Primary Account Number	XQI	XQ

N°	Definition	A	B
3	Processing code	XQI	XQ
4	Amount, transaction	X	XQ
6	Amount, cardholder billing	CQ (100)	FQ
7	Transmission date and time	XS	FS
10	Conversion rate, cardholder billing	CQ (100)	FQ
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)	C (9)
25	Point of service condition code	XQI	FQ
32	Acquiring institution identification code	XQI	XQ
33	Forwarding institution identification code	CQ (21)	FQ
35	Track 2 data	C (3)	.
37	Retrieval reference number	CQ (23)	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	XQI	FQ
30	Additional card reading capabilities	CQI (104)	FQ
31	Point of interaction information	CQI (104)	FQ
33	2AP specification date	CQI (104)	.
95	Unique transaction identifier	CQ (116)	FQ
96	SIRET (company registration number)	CQI (104)	FQ
97	IDPA (point of interaction identifier assigned by an acquirer)	CQI (104)	FQ
99	Original unique transaction identifier	CQI (104)	.
A0	IDSA (acceptance system identifier assigned by an acquirer)	CQI (104)	FQ
49	Currency code, transaction	XQI	XQ
51	Currency code, cardholder billing	CQ (100)	FQ
52	PIN data	C (12)	.

N°	Definition	A	B
53	Security related control information	XS	XS
55	Integrated circuit card system related data	C (2)	C (2)
0056	Data equivalent to ISO track 1 read in contactless mode	CQI (104)	.
0057	Track 2 equivalent data	C (3)	.
0095	Terminal Verification Results (TVR)	C (104)	.
5F24	Application Expiration Date	CQI (104)	.
9F02	Amount authorised	CQI (104)	.
9F06	Card Application Identifier (AID)	CQI (104)	.
9F0A	Application Selection Registered Proprietary Data	CQI (104)	.
9F10	Issuer Application Data (IAD)	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	Device information	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)	.
0024	Independent sales organization	CQI (104)	.
0025	Payment facilitator identifier	CQI (104)	.
0026	Marketplace 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)
0101	Message reason code	XS	FQ
0102	Transaction year	XS	FQ
0200	ERT (Regulatory and technical environment)	XQI	FQ
0201	Acceptance System Components Identifier (ex ITP SA)	XQI	.
0202	Acceptor contract number	XQI	FQ

N°	Definition	A	B
0203	Acceptance system logical number	XQI	FQ
0204	Point of interaction logical number	CQI (104)	.
0205	Acceptance system country code	CQI (104)	.
0207	Cardholder total amount	CQI (104)	.
020B	TASA (Card acceptor application type)	XQI	.
0215	POI Components Identifier (ex ITP PA)	CQI (104)	.
0216	Point of interaction extended logical number	CQI (104)	.
90	Original data elements	XS	FQ
95	Replacement amounts	XS	FQ
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)
00BC	Extended message to the transaction initiator	.	F

5.3 COMMENTS

N°	Comments
1	Mandatory if one of fields 65 to 128 is present
2	See list of types
3	Mandatory if available
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
12	Must be absent
21	Mandatory in case of one or more intermediaries between Acceptor and Acquirer, otherwise absent
23	Mandatory if managed by the Acceptor
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 absent
31	Mandatory if DUKPT used to encrypt the PIN
32	Mandatory if remote PIN verification, otherwise absent
48	Mandatory if available for a contactless transaction
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

N°	Comments
85	Mandatory for a debit transaction if present in the card application, mandatory if available for a credit transaction
100	May be used by a private Dynamic Currency Conversion application
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
127	Mandatory for a contact transaction, mandatory if available 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, mandatory for the first transaction of a multiple payment, mandatory for mobility
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
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
160	Mandatory for a debit transaction, mandatory if available for a contactless credit transaction
164	May be sent by some international schemes
165	Mandatory if present in the card application and if function code not equal to 104 and 105 (resubmission), otherwise absent
166	May by set when the sale location is different from the merchant store location; otherwise absent
173	Mandatory for a debit transaction, mandatory if available for a credit transaction

END OF DOCUMENT