

ISO:8583 Specifications

i2c Reference Guide

* + 1. | Standard

Confidential © i2c Inc. All rights reserved.



*Published by i2c Inc. Copyright © 2024 i2c Inc. Version: 24.3.1 | Standard*

*Revision Date: May 16th, 2024*

*All rights reserved. No part of the contents of this document can be reproduced or transmitted in any form or by any means without the written permission of i2c Inc. i2c has made every effort during the preparation of this document to ensure the accuracy of the information provided here. However, the information contained in this document comes without warranty, either expressed or implied. i2c will not be liable for any damage, cost, or alleged cost, arising either directly or indirectly on account of this document. Other product and company names mentioned herein may be the trademarks of their respective owners.*

Table of Contents

[Summary of Changes 7](#_bookmark0)

[PART 1 – Message Structure 12](#_bookmark1)

[ISO 8583 Protocol Format 12](#_bookmark2)

[Message Length 12](#_bookmark3)

[Message Type Identifier (MTI) 12](#_bookmark4)

[Message Bitmaps 12](#_bookmark5)

[Message Data Elements 14](#_bookmark6)

[PART 2 – Message Layouts 15](#_bookmark7)

[PART 3 – Co-operative Auth Model 19](#_bookmark8)

[Block Diagram 19](#_bookmark9)

[Connectivity Message Flows 20](#_bookmark10)

[Sign-On Message 20](#_bookmark11)

[Sign-Off Message 20](#_bookmark12)

[Echo/Health Check Message 20](#_bookmark13)

[Transaction Flows 21](#_bookmark14)

[Authorized by Auth-Host Processor 21](#_bookmark15)

[Declined by Auth-Host Processor 22](#_bookmark16)

[Exceptions Processing Flows 23](#_bookmark17)

[Fail at i2c Pre-Processing 23](#_bookmark18)

[Stand-in Processing 24](#_bookmark19)

[Post Processing Failure 26](#_bookmark20)

[PART 4 – Data Elements Definition 29](#_bookmark21)

[Legends for Attributes Acronyms 29](#_bookmark22)

[Data Elements Details 30](#_bookmark23)

[DE – 002 – PRIMARY ACCOUNT NUMBER 30](#_bookmark24)

[DE – 003 – PROCESSING CODE 30](#_bookmark25)

[DE – 004 – AMOUNT, TRANSACTION 30](#_bookmark26)

[DE – 005 – AMOUNT, SETTLEMENT 30](#_bookmark27)

[DE – 006 – AMOUNT, CARDHOLDER BILLING 30](#_bookmark28)

[DE – 007 – TRANSMISSION DATE AND TIME 31](#_bookmark29)

[DE – 009 – CONVERSION RATE, SETTLEMENT 32](#_bookmark30)

[DE – 010 – CONVERSION RATE, CARDHOLDER BILLING 32](#_bookmark31)

[DE – 011 – SYSTEM TRACE AUDIT NUMBER 32](#_bookmark32)

[DE – 012 – TIME, LOCAL TRANSACTION 32](#_bookmark33)

[DE – 013 – DATE, LOCAL TRANSACTION .................................................... 32  [DE – 014 – DATE, EXPIRATION 33](#_bookmark35)](#_bookmark34)

[DE – 015 – DATE, SETTLEMENT 33](#_bookmark36)

[DE – 018 – MERCHANT TYPE 33](#_bookmark37)

[DE – 022 – POINT-OF-SERVICE ENTRY MODE CODE 33](#_bookmark38)

[DE – 023 – PAN SEQUENCE NUMBER 33](#_bookmark39)

[DE – 025 – POINT-OF-SERVICE CONDITION CODE 34](#_bookmark40)

[DE – 026 – POINT-OF-SERVICE PIN CAPTURE CODE 34](#_bookmark41)

[DE – 028 – AMOUNT, TRANSACTION FEE 34](#_bookmark42)

[DE – 029 – AMOUNT SETTLEMENT FEE 34](#_bookmark43)

[DE – 032 – ACQUIRING INSTITUTION IDENTIFICATION CODE 34](#_bookmark44)

[DE – 033 – FORWARDING INSTITUTION IDENTIFICATION CODE 35](#_bookmark45)

[DE – 037 – RETRIEVAL REFERENCE NUMBER 35](#_bookmark46)

[DE – 038 – AUTHORIZATION IDENTIFICATION RESPONSE 35](#_bookmark47)

[DE – 039 – RESPONSE CODE 35](#_bookmark48)

[DE – 041 – CARD ACCEPTOR TERMINAL IDENTIFICATION 35](#_bookmark49)

[DE – 042 – CARD ACCEPTOR IDENTIFICATION CODE 35](#_bookmark50)

[DE – 043 – CARD ACCEPTOR NAME/LOCATION 36](#_bookmark51)

[DE – 048 – ADDITIONAL PROCESSING DATA 36](#_bookmark52)

[DE – 049 – CURRENCY CODE, TRANSACTION 36](#_bookmark53)

[DE – 050 – CURRENCY CODE, SETTLEMENT 36](#_bookmark54)

[DE – 051 – CURRENCY CODE, CARDHOLDER BILLING 36](#_bookmark55)

[DE – 054 – ADDITIONAL AMOUNTS 36](#_bookmark56)

[DE – 057 – AUTHORIZATION LIFE CYCLE 37](#_bookmark57)

[DE – 059 – GEOGRAPHIC DATA 37](#_bookmark58)

[DE – 061 – POINT-OF-SERVICE (POS) DATA 38](#_bookmark59)

[DE – 063 – NETWORK DATA 38](#_bookmark60)

[DE – 065 – SECONDARY BITMAP DATA 38](#_bookmark61)

[DE – 070 – NETWORK MANAGEMENT INFORMATION CODE 38](#_bookmark62)

[DE – 080 – DISPUTE ACTION INFORMATION 39](#_bookmark63)

[DE – 090 – ORIGINAL DATA ELEMENTS 39](#_bookmark64)

[DE – 102 – ACCOUNT IDENTIFICATION 1 40](#_bookmark65)

[DE – 108 – RECEIVER/SENDER DATA 40](#_bookmark66)

[DE – 110 – MINI STATEMENT DATA 41](#_bookmark68)

[DE – 111 – ADDITIONAL DATA 42](#_bookmark69)

[DE – 123 – VERIFICATION DATA 43](#_bookmark70)

[DE – 125 – SUPPORTING INFORMATION 43](#_bookmark71)

[PART 5 – Appendices 45](#_bookmark72)

[Appendix A – Message Matching Criteria 45](#_bookmark73)

[Matching Criteria for Clearing Message with Corresponding Authorization (01xx with 022x](#_bookmark74) [Matching) 45](#_bookmark74)

[Matching Criteria for Reversal Message with Corresponding Original Message (01xx/02xx with](#_bookmark75) [042x Matching) 45](#_bookmark75)

[Appendix B – Authorization Expiration Time 46](#_bookmark76)

[Appendix C – Data Elements Detailed Definitions 47](#_bookmark77)

[Data Element 003 – Processing Codes Table 47](#_bookmark78)

[Data Element 022 – POS Entry Mode Codes Table 49](#_bookmark79)

[Data Element 025 – POS Condition Codes Table 51](#_bookmark80)

[Data Element 026 – POS PIN Capture Codes Table 53](#_bookmark81)

[Data Element 039 – Response Codes Table 53](#_bookmark82)

[Data Element 043 – Card Acceptor Name/Location 56](#_bookmark83)

[Data Element 048 – Additional Processing Data 58](#_bookmark85)

[Data Element 054 – Additional Amounts Codes Table 60](#_bookmark86)

[Data Element 061 – Point-of-Service Data Codes Table 62](#_bookmark87)

[Data Element 108 – Receiver/Sender Data Table 71](#_bookmark88)

[Data Element 111 – Additional Data Table 75](#_bookmark89)

[Data Element 125 - SUPPORTING INFORMATION 90](#_bookmark92)

[Data Element 109 – Advice Reason Code Table 117](#_bookmark94)

[Appendix D – Sample Messages 122](#_bookmark95)

[Sample Network Request/Response Messages (0800, 0810) 122](#_bookmark96)

[Sample Authorization Request/Response Messages (0100, 0110) 124](#_bookmark97)

[Sample Authorization Advice Request/Response Messages (0120, 0130) 126](#_bookmark98)

[Sample Financial Request/Response Messages (0200, 0210) 128](#_bookmark99)

[Sample Financial Advice Request/Response Messages (0220, 0230) 130](#_bookmark100)

[Sample Reversal Request/Response Messages (0420, 0430) 132](#_bookmark101)

[Sample Token Notification Message (0620, 0320) 134](#_bookmark102)

[Sample DE-111 – Additional Data 135](#_bookmark103)

[Appendix E – Possible Values of New Sub-fields in DE-111 138](#_bookmark105)

[Stand In Trans Indicator 138](#_bookmark106)

[Token Type 138](#_bookmark107)

[Token Status 138](#_bookmark108)

[Token Device Type 139](#_bookmark109)

[Token Authorization Request Indicator 139](#_bookmark110)

[Token Notification Type 140](#_bookmark111)

[Chargeback Flag (Data Element 111.45) 140](#_bookmark112)

[On-behalf Service (Data Element 111.46) 140](#_bookmark113)

[Fraud Scoring Data (Data Element 111.47) 141](#_bookmark114)

[Appendix F – Token Activation / OTP Notification Message Identification 143](#_bookmark115)

[Appendix G – Token Provisioning – Send OTP Request 143](#_bookmark116)

[Appendix H – Token Transactions Flow 144](#_bookmark117)

[Appendix I – Token Creation Green/Red/Yellow Path Identification from Issue Perspective 145](#_bookmark118)

[Appendix J – Message Type Identifiers 146](#_bookmark119)

[Appendix K – Anticipated Amount Transaction 146](#_bookmark120)

# Summary of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Released On** | **Description of Change** | **Where to Look** |
| 24.3.1 | May 16th, 2023 | Updated description in Appendix A – Message Matching Criteria | Refer to: [Matching Criteria for](#_bookmark75) [Reversal Message with](#_bookmark75) [Corresponding Original Message](#_bookmark75) [(01xx/02xx with 042x Matching)](#_bookmark75) |
| 23.2.2 | August 31st, 2023 | Updated tag length value of Decline Reasons from ‘03’ to ‘02’ in DE – 080 – DISPUTE ACTION INFORMATION | Refer to: [DE – 080 – DISPUTE](#_bookmark63) [ACTION INFORMATION](#_bookmark63) |
| 23.2.2 | August 1st, 2023 | Added new processing codes to DE 003 – Processing Codes Table | Refer to: [Data Element 003 –](#_bookmark78) [Processing Codes Table](#_bookmark78) |
| 23.2.1 | February 08th, 2023 | Added DE 80 – Dispute Action Information  Added Dispute Decline Reasons in Appendix D  Added 80 – Dispute Action Information in “Message Layouts” section | Refer to: [DE – 080 – DISPUTE](#_bookmark63) [ACTION INFORMATION](#_bookmark63)  Refer to: [Data Element 80 Dispute](#_bookmark104) [Action Information Tag 05 Decline](#_bookmark104) [Reasons](#_bookmark104)  Refer to: [PART 2 – Message Layouts](#_bookmark7) |
| 22.09.1 | September 21st, 2022 | Added a Token Status D | Refer to: [Appendix E – Possible](#_bookmark108) [Values of New Sub-fields in DE-111](#_bookmark108) |
| 22.06.1 | May 26th, 2022 | Incremental Authorization Indicator Support Added for Efund/FIS | Refer to: [Data Element 111 –](#_bookmark89) [Additional Data Table](#_bookmark89) |
| 22.05.1 | April 1st, 2022 | Segregation of ‘GV’ response code for status inquiry / Account verification transactions in case of declined due to invalid card status (‘SX’) or expiry (‘EX’). Token Authorization Request - TAR red path response code updated as ‘TR’ from ‘TX’ | Refer to: [Data Element 039 –](#_bookmark82) [Response Codes Table](#_bookmark82) |
| 21.12.2 | December 08th, 2021 | Support Added for Sender Data for Visa. | Refer to:  [DE – 108 – Receiver/Sender Data](#_bookmark66) |
| 21.12.1 | November 30th, 2021 | Support added for Fiserv based auth- hosts | Refer to: [Fiserv DE 43](#_bookmark51) [Fiserv DE 90](#_bookmark63) [Fiserv DE 109](#_bookmark67) [Fiserv DE 111](#_bookmark68) |
| 21.10.1 | October 11th, 2021 | Addition of new Token Device Type Addition of new Dataset in DE 125 for Visa | Refer to:  Token Device Type Data Element 125 |
| 21.09.1 | September 7th, 2021 | Addition of new Field for Mastercard | Refer to:  Data Element 108 |

|  |  |  |  |
| --- | --- | --- | --- |
| 21.08.2 | August 25th, 2021 | Addition of new fields 33 and 90 | Refer to:  Data Element 33  Data Element 90 |
| 21.08 | August 15th, 2021 | Addition of new Field 59 for Mastercard and Visa | Refer to:  Data Element 59 |
| 21.07 | July 15th, 2021 | Field 125 and Field 111 updated | Refer to:  Data Element 125 – Discover Data Element 111 |
| 21.06 | June 1st, 2021 | Field 125 updated | Refer to:  Data Element 125 - Discover |
| 21.06 | March 30th, 2021 | Addition of Transaction types | Refer to:  [Data Element 3](#_bookmark25) |
| 21.06 | March 30th, 2021 | Addition of a Field 125 for Discover. | Refer to:  Data Element 125 - Discover |
| 21.06 | March 30th, 2021 | Addition of a Field 111 for Discover. | Refer to:  Data Element 111 - Discover |
| 21.06 | March 30th, 2021 | Addition of a Field 109 for Discover. | Refer to:  Data Element 109 |
| 21.05 | May 4th, 2021 | Updated description for DE 111.47 (MasterCard Format) to show that it is in TLV format. | Refer to:  Fraud Scoring Data (Data Element 111.47) |
| 21.04 | April 13th, 2021 | Updated part 3. Added co-operative auth model. Improved explanations of message ﬂows | Refer to: Part-3 |
| 21.04 | March 23rd, 2021 | 3DS Related Data Added | Refer to:  Data Element 111 |
| 21.03 | March 9th, 2021 | Updated PART 2 – Message Layouts for DE02 | Refer to: Message Layouts |
| 20.12 | November 26th, 2020 | Fee chunks for excess usage fee | Refer to:  DE54 chunk 46-47 |
| 20.11.2 | November 10th, 2020 | Description of DE57 updated | Refer to:  Data Element 57 |
| 20.11.1 | November 2nd, 2020 | Value of POS Entry Mode (29) updated | Refer to:  POS Entry Mode Codes Table |
| 20.10.2 | October 9th, 2020 | Expire Pre Auth Reversal Message Indicator | Refer to:  Data Element 048 |

|  |  |  |  |
| --- | --- | --- | --- |
| 20.10.1 | September 30th, 2020 | Token Device Bound Fields Added | Refer to:  [Data Element 111](#_bookmark69) |
| 20.9.1 | September 01st, 2020 | STAR Access Support Added | Refer to:  [Data Element 048.](#_bookmark52)  [Additional Amounts Codes Table](#_bookmark86) [Data Element 63](#_bookmark60)  [Data Element 109](#_bookmark67) [Data Element 111](#_bookmark69) |
| 20.7.1 | July 25th, 2020 | Incremental Authorizations and Multi- Clearing Transactions related indicators added for MC DMS based Clients | Refer to:  [Data Element 048.](#_bookmark52) [Data Element 109](#_bookmark67) [Data Element 111](#_bookmark69) |
| 20.5.1 | May 04th, 2020 | Application Transaction Counter (ATC) support added in 48.8 and new response code ‘AI’ introduced | Refer to:  [Data Element 048.](#_bookmark52) [Response Codes](#_bookmark82) |
| 20.3.1 | March 18th, 2020 | Over Limit Fee and Over Payment Fee chunks 07 and 08 added | Refer to [Additional Amounts Codes](#_bookmark56) [Table](#_bookmark56) |
| 20.2.1 | January 31st, 2020 | UnionPay Support Added, Update some values for DE61 | Refer to: [UnionPay DE111](#_bookmark91) [UnionPay DE125](#_bookmark93) [Field 61](#_bookmark59) |
| 20.1.1 | December 23rd, 2019 | Default timeout value added | Refer to Timeout Communication Exception Flows |
| 19.9.1.1 | September 17th, 2019 | New Field 109 Added , DE54 chunk 06 added | Refer to [Field 109](#_bookmark67) |
| 19.8.1.2 | September 12th, 2019 | Addition of:  New DE-007 added in Token Provisioning – Send OTP Request (0600) | Refer to: [Appendix G](#_bookmark116) |
| 19.8.1.1 | August 16th, 2019 | Addition of:  Modified MTI 0100 – Token Provisioning – Send OTP Request to MTI 0600 Administrative request  Appendix-G modified, New field 02 added in request. Field 111 modified DE-25 POS Condition code modified from 59 to 66 | Refer to: [Appendix G](#_bookmark116) |
| 19.7.1 | July 16th, 2019 | Addition of:  New MTI 0100 – Token Provisioning – Send OTP Request  New sub-fields 111.47 & 111.48. Appendix-G. | Refer to: [Message Layouts](#_bookmark7)  [Sub Elements of DE 111](#_bookmark89) [Appendix G](#_bookmark116) |
| 19.7.1 | June 25th, 2019 | Addition of new sub-fields 48.7 & 48.8. | Refer to [Data Element 048.](#_bookmark52) |

|  |  |  |  |
| --- | --- | --- | --- |
| 19.4.1 | April 18th, 2019 | Description change for DE-07 | Refer to [Data Element 07](#_bookmark29) |
| 19.4.1 | April 18th, 2019 | Addition of new response code value 99 | Refer to [Response Codes.](#_bookmark82) |
| 19.4.1 | April 18th, 2019 | Addition of a new sub-field 48.4, 48.5,  48.6 in DE-048. | Refer to [Data Element 048.](#_bookmark52) |
| 19.4.1 | April 10th, 2019 | Addition of a new sub-field 48.3 in DE- 048. | Refer to [Data Element 048.](#_bookmark52) |
| 19.4.1 | April 10th, 2019 | Addition of a new Response Code value 1A – Strong Customer Authentication Required in DE-39 | Refer to [Response Codes](#_bookmark82) section. |
| 19.4.1 | April 10th, 2019 | Addition of new Field 110 – Mini Statement Data. | Refer to [DE – 110.](#_bookmark68) |
| 19.4.1 | April 10th, 2019 | Addition of new process code value 34 (ATM Mini Statement) in Field 3— Processing Code, position 1–2. | Refer to [Processing Codes.](#_bookmark25) |
| 19.2.1 | March 1st, 2019 | Conditional new Field-048 (Additional Processing Data) added in the ISO specifications. | Refer to [Data Element – 048](#_bookmark52) |
| 19.1.1 | January 10th, 2019 | Description added of Sub field DE 111 and DE125 | DE 111 Mastercard Format:Sub Field 111.4, 111.18, 111.19, 125.6 |
| 18.7.1 | July 5th, 2018 | Addition of new sub field in DE 111 On- behalf Service, Fraud Scoring Data | DE 111 Mastercard Format: Sub Field 111.46, 111.47 |
| 18.7.1 | July 5th, 2018 | Addition of new sub field in DE 111 Chargeback flag | DE 111 Visa Format: Sub Field 111.46 DE 111 Mastercard Format: Sub Field 111.45  DE 111 Efund Format: Sub Field 111.11  DE 111 Star Format: Sub Field 111.4 |
| 18.6.1 | June 20th, 2018 | Addition of new code in:  Appendix H, Token Event Notification Section.  Token Notification Type. | DE 111 Token Notification Type |
| 18.5.1 | May 21st, 2018 | Addition of new sub field in DE 111 i.e. 111.45 | DE 111 Visa Format Sub Field 111.45 |
| 18.5.1 | April 26th, 2018 | Addition of new sub field in DE 111 i.e. 111.44 | DE 111 MasterCard Format Sub Field 111.44 |
| 18.5.1 | April 26th, 2018 | Text updated | Appendix F, Appendix H |
| 18.7.1 | July 4th, 2018 | Addition of new sub-field 111.47 (Fraud Scoring Data) | See section [Sub Elements of DE-111](#_bookmark90) [when DE-63.7 = ‘MASTERCARD’](#_bookmark90) |
| 18.7.1 | July 4th, 2018 | Addition of new sub-field 111.46 (On- behalf Service) | See section [Sub Elements of DE-111](#_bookmark90) [when DE-63.7 = ‘MASTERCARD’](#_bookmark90) |
| 18.7.1 | July 4th, 2018 | Addition of new sub-field 111.45 (Chargeback flag) | See section [Sub Elements of DE-111](#_bookmark90) [when DE-63.7 = ‘MASTERCARD’](#_bookmark90) |

# PART 1 – Message Structure

## ISO 8583 Protocol Format

|  |  |  |  |
| --- | --- | --- | --- |
| **Message Length** | **Message Type Identifier (MTI)** | **Bitmaps (Primary & Secondary)** | **Data Elements** |
| 2 or 4 Bytes | 4 Bytes | 8 Bytes each | Variable |

##### Message Length

The message length is the first 2 or 4 bytes of the message. The number of bytes which contains message length depends on the type of field configuration. Below are the two possible configurations:

**ASCII format** – The message length will be represented in 4-bytes ASCII format where the first 4 bytes of the message represents length. For example, for a 68 bytes message, the message length will be like 0068.

**Bytes format** – The first 2 bytes of the message will represent message length. The length will be in packed hexadecimal format.

The message length will not include the length of bytes used to represent message length, which means Message Length = Length MTI + Length Bitmaps + Length Data Elements

For the **bytes format**, below pseudo code can be used to extract message length:

var msg = message\_received\_at\_socket;

var msgLenBytes = msg[0,1]; // the first 2 bytes

var msgLenBinary = binary((int)msg[0]) + binary((int)msg[1]); var msgLen = convertToInteger(msgLenBinary);

##### Message Type Identifier (MTI)

The n-4 ASCII representation of the Message, called MTI. It is the first mandatory data element in ISO 8583 message and specifies general message category (e.g., financial or reversal).

Refer to [Appendix J](#_bookmark119) for the list of supported message type identifiers.

#### Message Bitmaps

The data elements transmitted in the message are not fixed; bitmaps specify which data elements are present and which are not. The length of a bitmap can be of 8 or 16 bytes (64 binary values) depending upon the format of message i.e. ASCII format or Bytes format.

* + - 1. **ASCII format** – A bitmap will be comprised of 16 unpacked hexadecimal digits where each digit will represent 4 bits.
      2. **Bytes format** – A bitmap will be represented in 8-bytes packed hexadecimal format. Each byte will contain 2 hexadecimal digits i.e. 8 binary value.

Each bitmap will contain 64 bits where each bit represents the presence of data element on that bit number. i2c’s ISO 8583 specification can contain two bitmaps i.e. Primary (mandatory) & Secondary (optional). The detail of each bitmap is described below.

##### Primary Bitmap

Every message includes the Primary Bitmap. It is of 8 Bytes (64 bits) length, positioned after the message type identifier. Except for the first bit, each bit of the primary bitmap is associated with the corresponding data element, starting from 2 to 64. Each bit indicates the presence or absence of its associated data element.

* + - * + If a bit is 0, the data element associated with the bit is not present.
        + If a bit is 1, the data element associated with the bit is present in the message.

For example:

The first bit of the Primary Bitmap indicates the presence of Secondary Bitmap. If the first bit is 1, a Secondary Bitmap follows this Bitmap.

##### Secondary Bitmap

Like the Primary Bitmap, Secondary Bitmap is also of 8 Bytes (64 bits) length, positioned after primary bitmap in the i2c message. Except for the first bit, each bit of the secondary bitmap is associated with the corresponding data element, starting from 66 to 128. Each bit indicates the presence or absence of its associated data element.

* + - * + If a bit is 0, the data element associated with the bit is not present.
        + If a bit is 1, the data element associated with the bit is present in the message.

For example:

The first bit of the Secondary Bitmap indicates the presence of a Third Bitmap. If the first bit is 1, a Third Bitmap follows this Bitmap. This bit will always be 0.

##### Third Bitmap

The third bitmap is reserved for future use.

## Message Data Elements

The Message Data Elements section explains the available fields along with their formats that can be a part of the i2c message.

# PART 2 – Message Layouts

C = Conditional, CE = Conditional Echo, M = Mandatory, ME = Mandatory Echo, Blank Space = Not Available or Not Required

\* For Non-PCI Compliant Auth-Host, secure data elements like PIN, CVV1, and CVV2 etc. will not be sent.

**0100/0110\* –** Token Send OTP Request

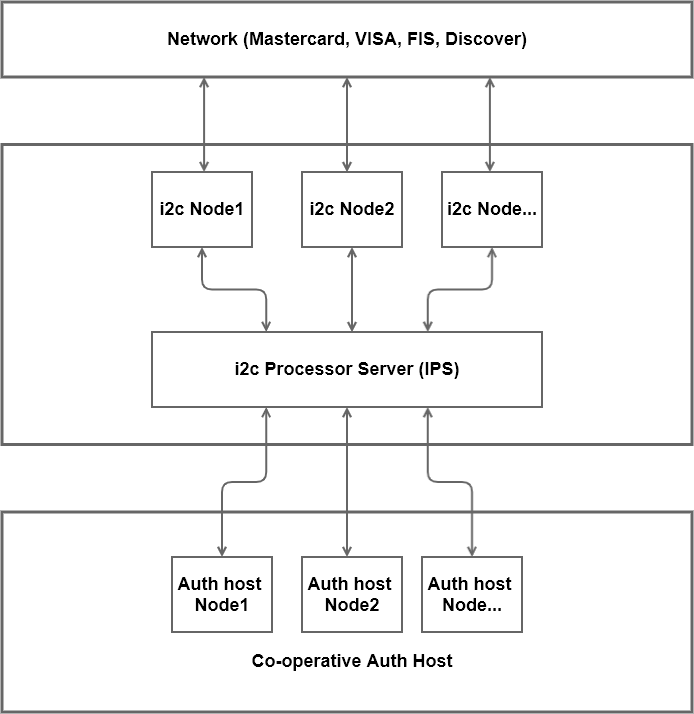
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Field** | **Description** | **010**  **0** | **011**  **0** | **011**  **0\*** | **011**  **0\*** | **012**  **0** | **013**  **0** | **020**  **0** | **021**  **0** | **022**  **0** | **023**  **0** | **042**  **0** | **043**  **0** | **080**  **0** | **081**  **0** | **030**  **2** | **031**  **2** | **062**  **0** | **06**  **30** |
| 2 | Primary Account Number | ME | ME | ME | ME | ME | ME | ME | ME | ME | ME | ME | ME |  |  | ME | ME | ME | ME |
| 3 | Processing Code | ME | ME |  |  | ME | ME | ME | ME | ME | ME | ME | ME |  |  |  |  |  |  |
| 4 | Transaction Amount | ME | C |  |  | ME | C | C | C | C | C | ME | C |  |  |  |  |  |  |
| 5 | Settlement Amount | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 6 | Cardholder Billing Amount | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 7 | Transmissio n Date/Time | ME | ME | M | ME | ME | ME | ME | ME | ME | ME | ME | ME | ME | ME | CE | CE | ME | ME |
| 9 | Settlement Conversion Rate | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 10 | Conversion Rate | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 11 | Trace Number | ME | ME | M | ME | ME | ME | ME | ME | ME | ME | ME | ME | ME | ME | CE | CE | ME | ME |
| 12 | Local Time | C | C |  |  | C | C | ME | C | C | C | C | C |  |  |  |  |  |  |
| 13 | Local Date | C | C |  |  | C | C | ME | C | C | C | C | C |  |  |  |  |  |  |
| 14 | Date, Expiration | CE |  |  |  | CE |  | CE |  | CE |  | CE |  |  |  |  | CE | CE |  |
| 15 | Date, Settlement | C | C |  |  | C | C | ME | ME | ME | ME | C | C |  |  |  | C | C | C |
| 18 | Merchant Category Code (MCC) | C |  | M | ME | C |  | C |  | C |  | C |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Field** | **Description** | **010**  **0** | **011**  **0** | **011**  **0\*** | **011**  **0\*** | **012**  **0** | **013**  **0** | **020**  **0** | **021**  **0** | **022**  **0** | **023**  **0** | **042**  **0** | **043**  **0** | **080**  **0** | **081**  **0** | **030**  **2** | **031**  **2** | **062**  **0** | **06**  **30** |
| 22 | Point of Service Entry Mode Code | C |  | M | ME | C |  | C |  | C |  | C |  |  |  |  |  |  |  |
| 25 | POS  Condition Code | C | C | M | ME | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 26 | POS PIN  Capture Code | C |  |  |  | C |  | C |  | C |  |  |  |  |  |  |  |  |  |
| 28 | Amount, Transaction Fee | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 29 | Amount, Settlement Fee | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 32 | Acquirer Institution Identification Code | ME | ME | M | ME | ME | CE | ME | ME | CE | CE | ME | CE |  |  |  |  |  |  |
| 37 | Retrieval Reference | CE | CE | M | ME | CE | CE | CE | CE | CE | CE | CE | CE |  |  | CE | CE | CE | CE |
| 38 | Auth-ID Code | CE | CE |  |  | CE |  | CE | CE | CE |  | CE | CE |  |  |  |  |  |  |
| 39 | Response Code | C | ME | C | M | C | ME | C | C | C | ME | C | C | C | C |  | ME | C | C |
| 41 | Card Acceptor Terminal ID | CE | CE | M | ME | CE | CE | CE | CE | CE | CE | CE | CE |  |  |  |  |  |  |
| 42 | Card Acceptor ID Code | C | C | M | ME | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 43 | Card Acceptor Name/Locati on | C |  |  |  | C |  | ME |  | C |  | C | C |  |  |  |  |  |  |
| 48 | Additional Processing Data | C |  |  |  | C |  | C |  | C |  |  |  |  |  |  |  |  |  |
| 49 | Currency Code, Currency | ME | ME |  |  | ME | C | C | C | C | C | ME | C |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Field** | **Description** | **010**  **0** | **011**  **0** | **011**  **0\*** | **011**  **0\*** | **012**  **0** | **013**  **0** | **020**  **0** | **021**  **0** | **022**  **0** | **023**  **0** | **042**  **0** | **043**  **0** | **080**  **0** | **081**  **0** | **030**  **2** | **031**  **2** | **062**  **0** | **06**  **30** |
| 50 | Currency Code, Settlement | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 51 | Currency Code, Card- Holder Billing | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 54 | Additional Amounts | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 57 | Authorizatio n Life Cycle | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 61 | Point-of- Service (POS) Data | C | C |  |  | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 63 | Network Data | ME | C |  |  | ME | C | ME | C | ME | C | ME | C |  |  | C | C | ME | ME |
| 65 | Tertiary Bitmap | C | C | C | C | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 70 | Network Managemen t Information Code |  |  |  |  |  |  |  |  |  |  |  |  | ME | ME |  |  | C | C |
| 80 | Dispute Action Information |  |  |  |  | C | C |  |  | C | C | C | C |  |  |  |  |  |  |
| 102 | Account Identification 1 | C | C | C | C | C | C | C | C | C | C | C | C |  |  |  |  |  |  |
| 110 | Mini Statement Data |  | C |  |  |  |  |  | C |  |  |  |  |  |  |  |  |  |  |
| 111 | Additional Data, Private Acquirer | C | C | M | C | C | C | C | C | C | C | C | C |  |  | ME | ME | ME | ME |
| 123 | Verification Data | C | C |  |  | C |  | C | C | C |  | C |  |  |  |  |  |  |  |
| 125 | Supporting Information | C | C | C |  |  |  |  |  |  |  |  |  |  |  |  |  | ME | ME |

# PART 3 – Co-operative Auth Model

## Block Diagram

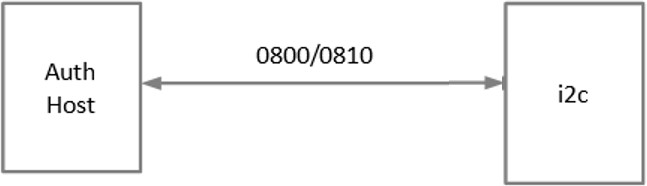


## Connectivity Message Flows

i2c will establish connection with Auth host. In case of disconnection, i2c will retry to establish connection.

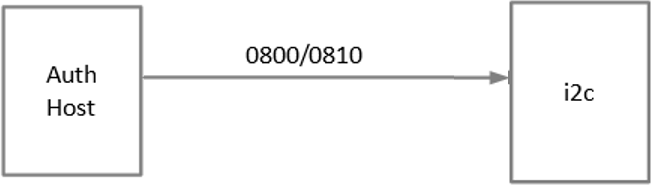
##### Sign-On Message

Once connection is established, i2c will send sign on. Sign on must be successful before sending transaction to auth host.



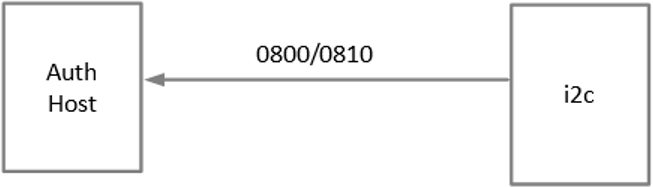
##### Sign-Off Message

Auth host can initiate Sign-off message to not receive further transactions. Once Sign-off is performed by Auth host, Sign-on is expected by Auth host to resume transaction processing.



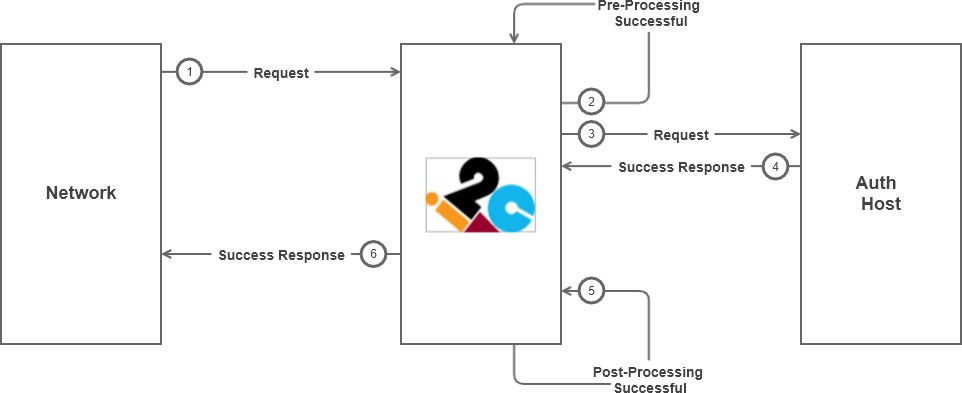
##### Echo/Health Check Message

Echo messages are sent on socket after defined intervals in-case there is no transaction in defined time- frame. Echo messages are sent by i2c to auth host.



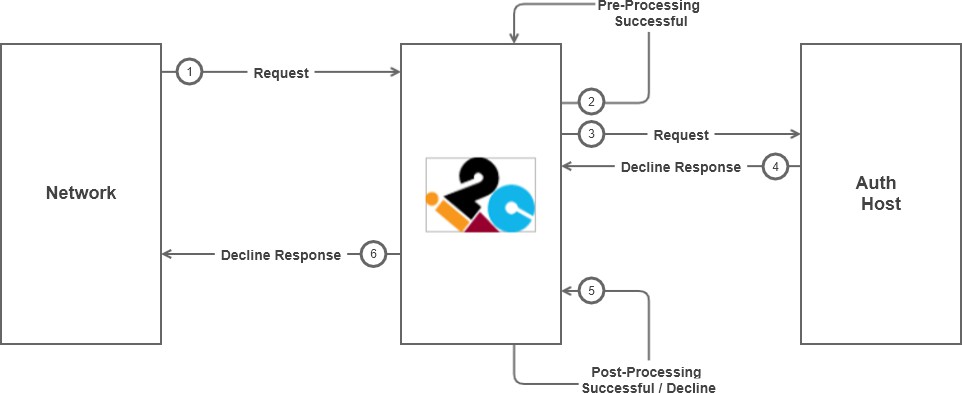
## Transaction Flows

##### Authorized by Auth-Host Processor



|  |  |
| --- | --- |
| **Step** | **Description** |
| 1 | Network initiates a transaction request/(0xx0) message to i2c |
| 2 | Pre-processing process is executed at i2c prior to sending transaction to auth host. |
| 3 | i2c forwards the Financial Transaction Request message to the auth host |
| 4 | The auth host generates a success response(0X10/0X30) and sends it to i2c. |
| 5 | Post-processing process is executed at i2c prior to sending response to network. |
| 6 | i2c generates a success response (0x10/0x30) message and sends it to network. |

##### Declined by Auth-Host Processor

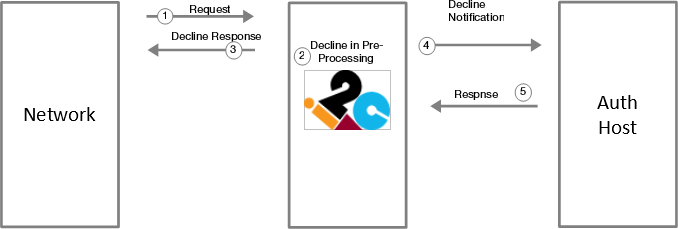


|  |  |
| --- | --- |
| **Step** | **Description** |
| 1 | Network initiates a transaction request/(0xx0) message to i2c |
| 2 | Pre-processing process is executed at i2c prior to sending transaction to auth host. |
| 3 | i2c forwards the Financial Transaction Request message to the auth host |
| 4 | The auth host generates a decline response (0X10/0X30) and sends it to i2c. |
| 5 | Post-processing process is executed at i2c prior to sending response to network. |
| 6 | i2c generates a decline response (0x10/0x30) message and sends it to network. |

## Exceptions Processing Flows

##### Fail at i2c Pre-Processing

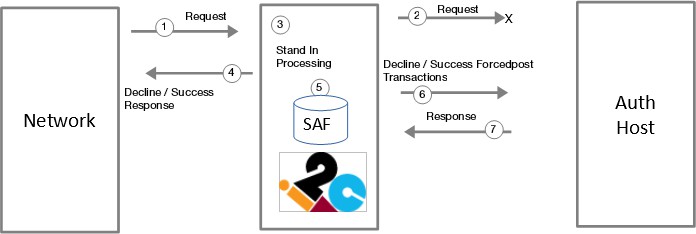
If a transaction fails pre-processing at i2c, then only a configurable notification will be sent to the auth host processor. The Decline response to the network will be sent (for non-force post transactions).



|  |  |
| --- | --- |
| **Step** | **Description** |
| 1 | Network initiates a transaction request/(0xx0) message to i2c |
| 2 | Transaction failed at i2c in pre-processing |
| 3 | i2c generates a decline response (0x10/0x30) message and sends it to network. |
| 4 | i2c will send a decline notification to auth host |
| 5 | Auth host generates a transaction request response(0x10/0x30) message and sends it to i2c. |

##### Stand-in Processing Auth Host Down

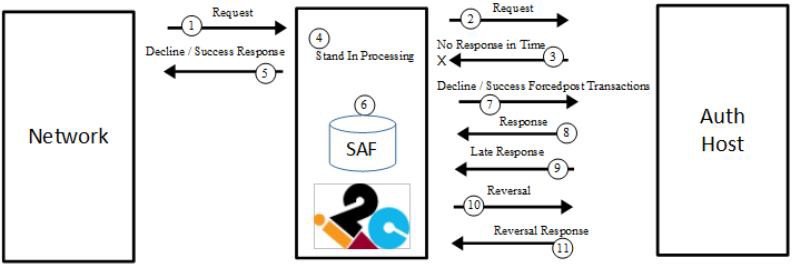
If there occurs an exception in sending the request message to the auth host due to non- availability of auth host, then either a decline notification or a forced post notification will be sent to the auth host based on auth host configuration with i2c.



|  |  |
| --- | --- |
| **Stage** | **Description** |
| 1 | Network initiates a transaction request/(0xx0) message to i2c |
| 2 | i2c initiates a Financial Transaction Request message, but unable to send this to auth host because of network communication failure. |
| 3 | i2c will perform Stand In processing.  Stand-in processing is configurable (Allowed/Not Allowed). |
| 4.1 | If auth host has configuration with i2c to decline transaction in its non-availability, then i2c sends a decline response (0x10/0x30) message to network. |
| 4.2 | If auth host has configuration with i2c to process transaction in its non-availability, then i2c sends a success response (0x10/0x30) message to network.  Stand-in limits are configurable for POS and ATM transactions.  Unit of accumulative limit is down time of auth host. For example, $100 is configured as stand-in limit then i2c will not allow transactions once approved transactions accumulative amount is reached $100 within down time of auth host.  Once auth is up again, accumulation counter is reset.  Note : Stand-in limit works only incase, system of record is auth host. |
| 5 | i2c stores decline / forced post notification to be sent to auth host in SAF (Store & Forward). |
| 6 | SAF mechanism will forward notifications to auth host when it is available for communication. |
| 7 | Auth host generates a transaction request response (0x10/0x30) message and sends it to i2c. |

##### Auth Host Time-Out

If a transaction is successful at i2c in pre-processing but no response is received from the auth host at all or till the specific time, then either a decline notification or a forced post notification will be sent to the auth host based on auth host configuration with i2c.



|  |  |
| --- | --- |
| **Step** | **Description** |
| 1 | Network initiates a transaction request/(0xx0) message to i2c |
| 2 | i2c initiates a Financial Transaction Request message & sent this to auth host. |
| 3 | No response from auth host in time. |
| 4 | i2c performs Stand In processing. Stand-in processing is configurable (Allowed / Not Allowed). |
| 5.1 | If auth host has configuration with i2c to decline transaction for timeout response, then i2c sends a decline response (0x10/0x30) message to network. |
| 5.2 | If auth host has configuration with i2c to process transaction for timeout response, then i2c sends a success response (0x10/0x30) message to network.  Stand-in limits are configurable for POS and ATM transactions.  Unit of accumulative limit is down time of auth host. For example, $100 is configured as stand-in limit then i2c will not allow transactions once approved transactions accumulative amount is reached $100 within down time of auth host. Accumulation is reset once auth host is up.  Note : Stand-in limit works only incase, system of record is auth host. |
| 6 | i2c store decline / forced post notification to be sent to auth host in SAF (Store & Forward). |
| 7 | SAF mechanism will forward notifications to auth host. |
| 8 | Auth host generates a transaction request response (0x10/0x30) message and sends it to i2c. |
| 9 | Auth host generates a transaction request response (0x10/0x30) message and sends it to i2c after specified time. (Late response) |
| 10 | If auth host late response is successful, then i2c generates a reversal to auth host only if 5.2 case is executed at step 6. |
| 11 | The auth host generates reversal response (0X10/0X30) message and sends it to i2c. |

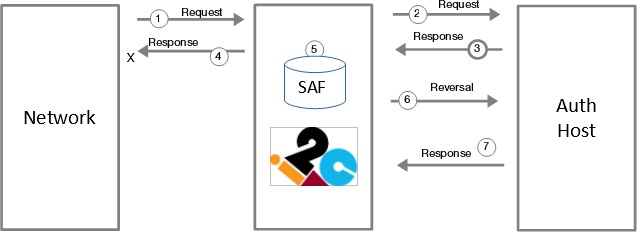
##### Post Processing Failure

**Fail at i2c in Response to Network**

If a transaction is successful in i2c in pre-processing, by auth host processor and in post- processing at i2c, but failed to send the response to the socket for network, then an auto reversal at i2c as well as initiate a reversal at the auth host processor side.

If a transaction is successful in i2c in pre-processing, by auth host processor and in post- processing at i2c, but the response sent to the switch was rejected with a format error, then the switch will send the reversal to i2c and a reversal will be initiated at i2c as well as at auth host processor.

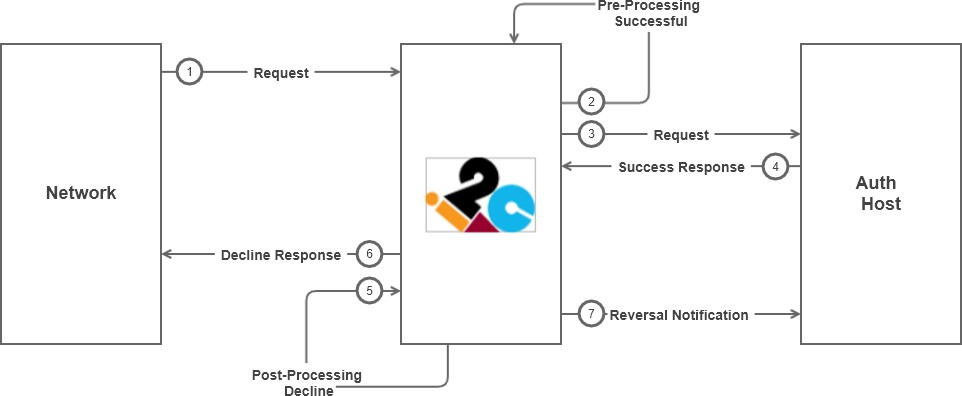
If a transaction is successful in i2c in pre-processing, by auth host processor and in post- processing at i2c, but the response sent to the switch was rejected due to timeout at i2c, then the switch will send the reversal to i2c and a reversal will be initiated at i2c as well as at auth host processor.



|  |  |
| --- | --- |
| **Step** | **Description** |
| 1 | Network initiates a transaction request/(0xx0) message to i2c |
| 2 | i2c forwards the Financial Transaction Request message to the auth host |
| 3 | Auth host generates a success transaction request response(0X10/0X30) message and sends it to i2c. |
| 4 | i2c generates a response (0x10/0x30) message and sends it to network, but it cannot be delivered to network because of network communication failure or i2c decline in post processing. |
| 5 | i2c reverse transaction & store reversal to be sent to auth host in SAF. |
| 6 | SAF mechanism will forward reversal to auth host. |
| 7 | The auth host generates a transaction reversal response (0X10/0X30) message and sends it to i2c. |

##### Fail at i2c due to business rules / services

Services that are executed after sending authorization request to auth host are called post processing services. For example, fraud and ADS services.



|  |  |
| --- | --- |
| **Step** | **Description** |
| 1 | Network initiates a transaction request/(0xx0) message to i2c. |
| 2,3 | i2c forwards the Financial Transaction Request message to the auth host. |
| 4 | Auth host generates a success transaction request response(0X10/0X30) message and sends it to i2c. |
| 5 | Post processing is failed at i2c side due to services like (Fraud, ADS, …). |
| 6 | i2c generates a decline response (0x10/0x30) message and sends it to network. |
| 7 | i2c sends reverse notification to auth host to reverse the financial impact on its side. |

##### Fail at i2c in Parsing Response

If some exception occurs in parsing the response message from the auth host, then this (non- forced post) transaction will be considered & processed as a timed-out transaction at the auth host. For forced post transaction, it will be looped in and resent to the auth host until a successful response is received from the auth host.

# PART 4 – Data Elements Definition

## Legends for Attributes Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| n | Numeric digits only. For example, n 6 in DE-11: System Trace Audit Number indicates the  data of fixed, definite length of 6 Numeric digits. |
| an | Alphabetic and Numeric characters only. |
| ns | Numeric and Special characters only. |
| ans | Alphabetic, Numeric and Special Characters. |
| x | Indicates a Debit or Credit. For example, x + n 8 in DE-28: Amount, Transaction Fee means prefix C or D and 8 digits of amount, transaction.  C indicates Credit (a positive amount).  D indicates Debit (a negative amount). |
| b | Data in Bytes (Binary String) Format. |
| LLVAR | Variable Length that follows from 01 – 99, appended at the start of the Data Element's value to identify the actual length of the value present. For example, n.. 19 in DE-2: Primary Account Number indicates variable length up to a maximum of 19 characters as its actual value may vary from 16 to 19 characters.  NOTE: In LLVAR format, the length identified is the number of characters to read after the first 2 positions to get the data element's value. |
| LLLVAR | Variable Length that follows from 001 – 999, appended at the start of the Data Element's value to identify the actual length of the value present. For example, ans... 060 in DE-60: Advice Reason Code indicates variable length up to a maximum of 60 alphanumeric and special characters.  NOTE: In LLLVAR format, the actual length is added in first 3 positions that gives number of characters to read after these positions to get the data element's value. |

## Data Elements Details

### DE – 002 – PRIMARY ACCOUNT NUMBER

**Format**: LLVAR

**Attributes**: n..19

**Description**: A series of digits used to identify a customer account or relationship. This can be 16 to 19 digits card number or card reference number.

***Note:*** *For Non-PCI Compliant auth-host, the card reference number will be sent instead of card number.*

### DE – 003 – PROCESSING CODE

**Attributes:** an 6

**Description:** A series of digits used to describe the effect of a transaction on the customer account and identify the accounts affected.

Positions 1–2, Transaction Type: A 2-digit code identifying the customer transaction type, or the center function being processed.

Positions 3–4, Account Type (From): A 2-digit code identifying the cardholder account type affected for cardholder account debits and inquiries, and the "from" account type for cardholder account transfer transactions.

Positions 5–6, Account Type (To): A 2-digit code identifying the cardholder account type affected for cardholder account credits and the "to" account type for cardholder account transfer transactions.

Refer to the [Processing Codes Table](#_bookmark78) for a list of valid processing codes.

### DE – 004 – AMOUNT, TRANSACTION

**Attributes:** n 12

**Description:** Funds requested by the cardholder in the local currency of the acquirer or source location of the transaction, exclusive of transaction fee amount.

### DE – 005 – AMOUNT, SETTLEMENT

**Attributes:** n 12

**Description:** Funds to be transferred between the acquirer and issuer. This amount equals the transaction amount in the currency of settlement.

### DE – 006 – AMOUNT, CARDHOLDER BILLING

**Attributes:** n 12

**Description:** The amount billed to the cardholder in the currency of the cardholder account, exclusive of cardholder billing fees. It will always contain the fee amount in addition to transaction amount in cardholder billing currency i.e. DE 51.

### DE – 007 – TRANSMISSION DATE AND TIME

**Attributes:** n 10

**Format:** MMddhhmmss

**Description:** The date and time the message entered into the data interchange system. Greenwich Mean Time (GMT) can be used as timezone, forwarded data is unaltered

### DE – 009 – CONVERSION RATE, SETTLEMENT

##### Attributes: n 8

**Description:** The factor used in the conversion from the transaction to settlement amount. The transaction amount is multiplied by the settlement conversion rate to determine the settlement amount.

This data element is in the format ABBBBBBB, where:

A = the decimal position from the right

B = the actual conversion factor

### DE – 010 – CONVERSION RATE, CARDHOLDER BILLING

##### Attributes: n 8

**Description:** The factor used in the conversion from the transaction to cardholder billing amount. The transaction amount is multiplied by the cardholder billing conversion rate to determine the cardholder billing amount.

This data element is in the format ABBBBBBB, where:

A = the decimal position from the right

B = the actual conversion factor

### DE – 011 – SYSTEM TRACE AUDIT NUMBER

##### Attributes: n 6

**Description:** A number assigned by the message initiator to uniquely identify a transaction. The trace number remains unchanged for all messages throughout the life of the transaction.

For Token Authorization Request, (MTI = 01xx and TAR Indicator = 1), this field is Conditional. See

DE – 111, Additional Data Details for TAR indicator.

### DE – 012 – TIME, LOCAL TRANSACTION

**Attributes**: n 6

**Format:** hhmmss

**Description:** The local time at which the transaction takes place at the point of the card acceptor location. This time must remain unchanged throughout the life of the transaction.

### DE – 013 – DATE, LOCAL TRANSACTION

##### Attributes: n 4

**Format:** MMdd

**Description:** The local month and day on which the transaction takes place at the card acceptor location. This date must remain the same throughout

the life of the transaction.

### DE – 014 – DATE, EXPIRATION

##### Attributes: n 4

**Format:** yymm

**Description:** The year and month after which the card expires.

### DE – 015 – DATE, SETTLEMENT

##### Attributes: n 4

**Format:** MMdd

Description: The month and day funds are transferred between the acquirer and issuer or any intermediate network facility.

### DE – 018 – MERCHANT TYPE

##### Attributes: n 4

**Description:** The classification of the merchant’s type of business product or service.

For Token OTP Notification Request, its value will be 7299 (Miscellaneous personal services—Not elsewhere classified). See Appendix F for OTP Notification Request Identification.

### DE – 022 – POINT-OF-SERVICE ENTRY MODE CODE

##### Attributes: n 3

**Description:** Two numeric to indicate the method by which the primary account number was entered into the system and one numeric to indicate PIN entry capabilities.

Positions 1–2, PAN and Date Entry Mode: A 2-digit code that identifies the actual method used to enter the cardholder account number and card expiration date.

For Token OTP Notification Request, its value will be 01 (Manual key entry). See Appendix F for OTP Notification Request Identification.

Position 3, PIN Entry Capability: A 1-digit code that identifies the capability of terminal to capture PINs. This code does not necessarily mean that a PIN was entered or is included in this message. Refer to POS Entry Mode Codes Table for the complete list of valid codes.

### DE – 023 – PAN SEQUENCE NUMBER

##### Attributes: n 3

**Description:** DE 23 (Card Sequence Number) distinguishes among separate cards having the same PAN or DE 34 (Primary Account Number [PAN] Extended). Issuers mayencode chip cards with Card Sequence Numbers. Acquirers with chip-reading capability may pass this information encoded on the chip in DE 23 of Financial Transaction/0200 messages.

##### Values:

Valid values for Card Sequence Number are in the range 000–099.

### DE – 025 – POINT-OF-SERVICE CONDITION CODE

##### Attributes: n 2

**Description:** An identification of the condition under which the transaction takes place at the point- of-service.

For Token OTP Notification Request, its value will be 66 (E-commerce request through public network). See [Appendix F](#_bookmark115) for OTP Notification Request Identification.

Refer to [POS Condition Codes Table](#_bookmark80) for the complete list of valid codes.

### DE – 026 – POINT-OF-SERVICE PIN CAPTURE CODE

##### Attributes: n 2

Description: A code indicating the technique and/or maximum number of PIN characters accepted by the point-of-service device used to construct the PIN data.

Refer to POS PIN Capture Codes Table for the complete list of valid codes.

### DE – 028 – AMOUNT, TRANSACTION FEE

**Attributes:** x + n 8

**Description:** The fee charged (for example, by the acquirer) for transaction activity in the currency of the transaction amount. This fee can be a surcharge, rebate, or transaction fee.

Transaction fee must be represented in numeric 8 digits while the x represents the Credit or Debit sign where,

C = Credit amount

D or 0 = Debit amount

### DE – 029 – AMOUNT SETTLEMENT FEE

**Attributes:** x + n 8

**Description:** The fee transferred between the acquirer and the issuer equal to the transaction fee amount in the currency of the settlement amount. This amount must be the same value in the response as in the request. The value is a debit for a fee and a credit for a rebate.

Settlement fee must be represented in numeric 8 digits while the x represents the Credit or Debit sign where,

C = Credit amount

D or 0 = Debit amount

### DE – 032 – ACQUIRING INSTITUTION IDENTIFICATION CODE

**Format**: LLVAR

**Attributes**: n 11

**Description**: A code identifying the acquiring institution (for example, merchant bank) or its agent. This can be any uniquely identifying number agreed upon by the network.

For Token OTP Notification Request, its value will be 746922. See [Appendix F](#_bookmark115) for OTP Notification Request Identification.

### DE – 033 – FORWARDING INSTITUTION IDENTIFICATION CODE

**Format**: LLVAR

**Attributes**: n… 11

**Description**: DE 33 (Forwarding Institution Identification Code) identifies the institution forwarding a Request or Advice message in an interchange system if not the same institution as specified in the DE 32 (Acquiring Institution Identification Code).

### DE – 037 – RETRIEVAL REFERENCE NUMBER

**Attributes:** an 12

**Description:** This field contains a number that is used with other data elements as a key to identify and track all messages related to a given cardholder transaction; that is, to a given transaction set. For x8xx messages, retrieval reference number can be generated using following format:

|  |  |
| --- | --- |
| **Position** | **Data** |
| 1-4 | The yddd equivalent of the field 7 date |
| 5-6 | The hours from the time in field 7 |
| 7-12 | The value from field 11 |

### DE – 038 – AUTHORIZATION IDENTIFICATION RESPONSE

**Attributes:** an 6

**Description:** Field 38 contains the authorization code provided by the issuer when a transaction is approved or a “no reason to decline” code provided for successful verification.

### DE – 039 – RESPONSE CODE

**Attributes**: an 2

**Description:** A code that defines the disposition of a message. When the response code is 30, then Additional Response Data (bit 044) contains the bit number in error.

Refer to Response Codes Table for the complete list of valid codes.

### DE – 041 – CARD ACCEPTOR TERMINAL IDENTIFICATION

**Attributes:** an 8

**Description:** A unique code identifying a terminal at the card acceptor location.

For Token OTP Notification Request, its value will be 11111111. See Appendix F for OTP Notification Request Identification.

### DE – 042 – CARD ACCEPTOR IDENTIFICATION CODE

**Attributes:** an 15

**Description:** A code identifying the card acceptor that defines the point of the transaction in both local and interchange environments.

For Token OTP Notification Request, its value will be 111111111111111. See [Appendix F](#_bookmark115) for OTP Notification Request Identification.

### DE – 043 – CARD ACCEPTOR NAME/LOCATION

**Usage**: Usage 1: For existing clients; Usage 2: For new clients

**Attributes:** an 43 (Usage 1); an 70 (Usage 2)

**Description:** This field contains the name and location of the card acceptor (merchant), including the city name, state and country code.

For details, please refer to [DE – 43 – Card Acceptor Name/Location](#_bookmark83).

### DE – 048 – ADDITIONAL PROCESSING DATA

**Format**: LLLVAR

**Attributes**: ans... 255

**Description**: This data element is reserved for communicating the results of i2c processing for example Issuer Script Command sent in case of EMV transactions or any other processing data. This field is applicable for x1xx, x2xx & x4xx transactions.

For details of sub-fields, please refer to [DE – 48, Additional Processing Details](#_bookmark84).

### DE – 049 – CURRENCY CODE, TRANSACTION

##### Attributes: n 3

**Description:** The local currency of the acquirer or source location of the transaction. Currency used in transaction amount and transaction fee amount.

For Token Authorization Request, (MTI = 01xx and TAR Indicator = 1), this field is Conditional. See DE – 111, Additional Data Details for TAR indicator.

### DE – 050 – CURRENCY CODE, SETTLEMENT

##### Attributes: n 3

**Description:** A code defining the currency of the settlement amount and the settlement fee amount.

### DE – 051 – CURRENCY CODE, CARDHOLDER BILLING

##### Attributes: n 3

**Description:** A code defining the currency of the cardholder billing amount and the cardholder billing fee amount.

### DE – 054 – ADDITIONAL AMOUNTS

**Format**: LLLVAR

**Attributes**: ans... 120

**Description**: This field contains additional amounts like additional fees, card balances, etc. which applies to the transaction.

The field will be formatted in chunks of 20 bytes each, where chunk represents one amount to be communicated. This means maximum of 6 amounts can be communicated in this field. Each chunk (20-bytes) will be formatted as follows:

**Positions 1–2, Account Type:** This 2-digit code (field 54.1) identifies the account type. **Positions 3–4, Amount Type:** This 2-digit code (field 54.2) describes the use of the amount. **Positions 5–7, Currency Code:** This 3-digit code (field 54.3) defines the currency used in positions 9–20.

**Position 8, Amount, Sign:** This 1-digit code (field 54.4) defines the value of the amount as either positive or negative, where C = Positive balance & D = Negative balance.

**Positions 9–20, Amount:** This 12-character amount (field 54.5) is right-justified and contains leading zeros. The amount also includes an implied decimal relative to the currency code specified in positions 5–7.

Refer to Additional Amounts Codes Table for the complete list of valid account / amount types. Refer to Additional Amounts Business Use Cases table.

### DE – 057 – AUTHORIZATION LIFE CYCLE

**Format**: LLLVAR

**Attributes**: an 003

**Description:** The ANSI X9.2-1988 standard defines this data element as the Authorization Life Cycle, a value in calendar days, hours, or minutes that identifies the time for which an acquirer is requesting guarantee of funds.

This data element is subdivided into the following two sub-elements:

**Position 1, Life Cycle Indicator (n 1):** It indicates the type of time interval in effect for a pre- authorization. Possible values are:

1 = Calendar days

2 = Hours

3 = Minutes

**Position 2-3, Life cycle (n 2):** It is the time interval in effect for a pre-authorization.

##### DE – 059 – GEOGRAPHIC DATA

**Format**: LLLVAR

**Attribute**: ans… 018

**Description**: This field contains geographic information about POS location

|  |  |  |
| --- | --- | --- |
| **Position** | **Attribute** | **Description** |
| 1-10 | ans 10 | Merchant Postal code |

|  |  |  |
| --- | --- | --- |
| 11-18 | ans 18 | Reserved for future |

### DE – 061 – POINT-OF-SERVICE (POS) DATA

**Format**: LLLVAR

**Attributes**: ans... 019

**Description:** The ANSI X9.2-1988 standard defines this data element as the National Point-Of- Service Condition Code, a series of codes intended to identify terminal class, presentation data, and security condition.

Refer to Point-of-Service (POS) Data Table for the complete list of valid i2c POS Codes.

### DE – 063 – NETWORK DATA

**Format**: LLLVAR

**Attributes**: ans... 070

**Description:** DE 63 (Network Data) is generated by the Authorization Platform for each originating message routed through the network. The receiver must retain the data element and use it in any response or acknowledgment message associated with the originating message. The Sub-Fields of DE-63 are as follows:

|  |  |  |
| --- | --- | --- |
| **Position** | **Attribute** | **Description** |
| 1-4 | an 4 | Acquirer Network ID |
| 5-8 | an 4 | Issuer Network ID |
| 9-24 | an 16 | Transaction Identifier/Access Transaction Sequence Number |
| 25-33 | an 9 | Bank Net Reference Number |
| 34 | an 1 | Interchange Rate Indicator |
| 35-58 | n 24 | Acquirer Reference Number |
| 59-70 | an 12 | Network Type |

**Note:** All sub-fields are right justified space filled. If data in any of the sub-field is not present, it must be space filled.

For Token Authorization Request, (MTI = 01xx and TAR Indicator = 1), this field is Conditional. See

[DE – 111, Additional Data Details](#_bookmark89) for TAR indicator.

### DE – 065 – SECONDARY BITMAP DATA

**Attributes:** b 64

**Description:** A series of 64 bits used to identify the presence (denoted by 1) or absence (denoted by a 0) of data elements 66 through 128.

### DE – 070 – NETWORK MANAGEMENT INFORMATION CODE

##### Attributes: n 3

**Description:** Used to identify network status.

|  |  |
| --- | --- |
| **Code** | **Description** |
| 081 | Sign On Code |
| 082 | Sign Off Code |
| 301 | Echo/Health Check Code |

### DE – 080 – DISPUTE ACTION INFORMATION

**Format**: LLLVAR

**Attributes**: ans... 999

This is a field is setup in Tag, Length, Value (TLV) format which contain information about the Dispute Actions transactions. It contains multiple tags. The description for each of the tag is given below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tag** | **Length** | **Value** | **Format** | **Content** |
| '01’ | '02’ | Dispute Trans ID | N | It is a unique identifier in our system against a dispute. |
| '02’ | '02’ | Dispute Amount | N | The claimed dispute Amount by Card holder. |
| '03’ | '02’ | Credit Type | AN | This is applicable only for the Credit transactions. This tag will not be available for debit transactions.  Credit Type Possible value are:   * Admin Credit: Administratively Credit is given to Cardholder. * Network: Network has accepted the claim and send the charge-back.   None: where settlement of funds is already completed between merchant and card holder. |
| '04’ | '02’ | Agent ID | AN | The ID of the chargeback analyst. |
| '05’ | '02’ | Decline Reasons | AN | The reasons on the basis of which the claim does not fulfills. The tag will contain the comma separated list of reason ids.  Details against each ID can be seen in [Data Element 80](#_bookmark104) [Dispute Action Information Tag 05 Decline Reasons.](#_bookmark104) |
| '06’ | '02’ | CH Loss Date | Date | The date on which cardholder faces the loss. [YYYYMMDD] |

### DE – 090 – ORIGINAL DATA ELEMENTS

**Usages**: Usage 1: For existing clients; Usage 2: For new clients

**Attributes**: n 42 (Usage 1); n 44 (Usage 2)

**Description**: DE 90 (Original Data Elements) are data elements contained in an original message that may identify a transaction for correction or reversal. Below is detail for field sub elements:

**\*\*Usage-1 Details (For existing clients):**

|  |  |  |
| --- | --- | --- |
| **Position** | **Type** | **Element** |
| 1 – 4 | n - 4 | Message Type Identifier |
| 5 - 10 | n - 6 | System trace audit no |
| 11 – 20 | n - 10 | Transmission date time |
| 21 - 31 | n – 11 | Acquirer Institution Id |
| 32 - 42 | n - 11 | Forwarding Institution ID Code |

**\*\*Usage-2 Details (For existing clients):**

|  |  |  |
| --- | --- | --- |
| **Position** | **Type** | **Element** |
| 1 – 4 | n - 4 | Message Type Identifier |
| 5 - 10 | n - 6 | System trace audit no |
| 11 – 22 | n - 12 | Transmission date time |
| 23 - 33 | n – 11 | Acquirer Institution Id |
| 34 - 44 | n - 11 | Forwarding Institution ID Code |

### DE – 102 – ACCOUNT IDENTIFICATION 1

**Format**: LLVAR

**Attributes**: ans.. 28

**Description**: A series of digits used to identify a customer account or relationship Id.

Account identification 1 identifies the account involved for a single account transaction. In the case of transfers, Account Identification 1 identifies the From account in a transaction.

### DE – 108 – RECEIVER/SENDER DATA

**Format:** LLLVAR

**Attributes:** ans... 999

**When DE-63.7 = ‘VISA’:** DE 108 (Additional Transaction Reference Data) provides the capability for the acquirers to send sender data required in 0200 and 0100 original credit transactions.

Refer to [details](#_bookmark88) for the complete list of sender data fields with sub elements.

**When DE-63.7 = ‘MASTERCARD’:** DE 108 (Additional Transaction Reference Data) provides the capability for the acquirers to send sender, receiver, and transaction level data to the issuer in funding transfer transactions and MoneySend payment transactions. DE 108 provides the

capability to acquirers to send to the issuer data for Mastercard™ Merchant Presented QR payment transactions and Mastercard Merchant Presented QR funding transactions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub Element** | **Length Field** | **Representation** | **Element** |
| 01 | 3 | ans...322; LLLVAR | Receiver Data |
| 02 | 3 | ans...322; LLLVAR | Sender Data |
| 03 | 3 | ans...138; LLLVAR | Transaction reference Data |
| 04 | 3 | ans...61; LLLVAR | Language Description |
| 05 | 3 | ans...99; LLLVAR | Digital Account Info |
| 06 | 3 | ans...237; LLLVAR | QR Dynamic Code Data |

### DE – 109 – ADVICE REASON CODE

**Format**: LLLVAR, Fixed Format

**Attributes**: ans 999

This data element is reserved by ISO for private definition and use. i2c defines this data element as Additional Data, which contains additional information for Visa®, MasterCard®, FIS®, Discover®, and Fiserv format.

This contains data in fixed length sub-fields. The number and contents of sub-fields varies according to different networks, based on the value of DE-63.7 (Network Type).

Refer to Advice Reason Code for the complete list of network specific additional data fields for Fixed Format.

### DE – 110 – MINI STATEMENT DATA

**Format**: LLLVAR

**Attributes**: an 360

**Description**: This field is required in responses (0110/0210) of 0100/0200 ATM Mini Statement requests.

Issuers that choose to support the new mini statement requests, must be able to receive the new transaction type value 34 (ATM Mini Statement) carried in existing Field 3, positions 1–2 and must be able to send Field 110 in the 0110/0210 responses.

The field will be formatted just like Field-54 where data of each transaction will be formatted in a chunk of 36-bytes. This means maximum of 10 transactions (i.e. 10 chunks of 36 bytes each) can be communicated in this field.

Each chunk (36-bytes) will be formatted as follows:

**Positions 1–8** will contain an 8-digit transaction date in yyyymmdd format.

**Positions 9–23** will contain a 15-character alphanumeric transaction description that is left-justified with trailing spaces.

**Position 24** will contain a 1-digit code prefix that defines whether the transaction amount is credit or debit, where, C (Credit) & D (Debit).

**Positions 25–36** will contain a 12-character amount that is right-justified and contains leading zeros. The amount also includes an implied decimal relative to the cardholder billing currency code.

### DE – 111 – ADDITIONAL DATA

**Format**: LLLVAR, Fixed Format

**Attributes**: ans... 999

**Description**: This data element is reserved by ISO for private definition and use. i2c defines this data element as *Additional Data*, which contains additional information for Visa®, MasterCard®, FIS® , Discover® , Star®, UnionPay®, and Fiserv format.

This contains data in fixed length sub-fields. The number and contents of sub-fields varies according to different networks, based on the value of DE-63.7 (Network Type).

* Sub Field/s for Token Authorization Request (TAR 0100)
* Token Authorization Request (TAR) Indicator
* Sub Field/s for Token Financial Transactions (01XX, 02XX,04XX)
* Token Device Id
* Token Device No
* Token Device Name
* Token Device Type
* Token ID
* Token Type
* Token Status
* Sub Field/s for Token OTP Request (0100)
  + Token OTP Code
  + Token OTP Expiry Date Time
* Sub Field/s for Token PAN Management (0302)
  + Replacement PAN
  + Replacement PAN Expiration Date
* Sub Field/s for Token Life Cycle (0620)
  + Token Notification Type

Refer to Additional Data Table for the complete list of network specific additional data fields for Fixed Format.

### DE – 123 – VERIFICATION DATA

**Format**: LLLVAR

**Attributes**: ans... 255

**Description:** It is an i2c-defined private-use field that contains information used for certain types of verification data, including selected portions of the cardholder’s postal code and street address. All merchants whose acquirers subscribe to the i2c Address Verification Service may request postal code and street address verification for a cardholder.

The field has two sub-fields which are described below:

|  |  |  |
| --- | --- | --- |
| **Positio**  **n** | **Data** | **Description** |
| 1-9 | Postal code | This value is the 5-digit postal code (left-justified with 4  positions of right-space-fill), or 9-digit postal code. |
| 10-29 | Cardholder street address | This sub-field contains up to 20 characters of street address. The acquirer converts spelled-out numbers to  digits, left-justified with right space-fill. |

### DE – 125 – SUPPORTING INFORMATION

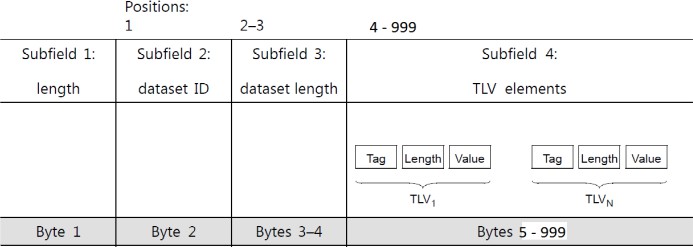
**Format**: LLLVAR, BER-TLV Format for Visa (DE-63.7 = VISA) LLLVAR, Fixed Format for MasterCard (DE-63.7 = MASTERCARD) **Attributes**: ans 999

**Description:** It is an i2c-defined private-use field that contains supporting information used for certain types of transactions, including Token Authorization Transactions (TAR) and Administrative Advice Messages. All merchants whose acquirers subscribe to the i2c Tokenization Service may request supporting information of a transaction.

Refer to Supporting Information Table for the complete list of data fields for BER-TLV and Fixed Format.

##### BER-TLV Format for Visa

For VISA, this field allows for multiple data-sets in TLV format. Each data-set can have multiple TLV sub-fields. The format is shown below:



In the Basic Encoding Rules (BER), the Tag-Length-Value (TLV) format is an ISO convention that treats field content as data-sets.

**Length Sub-field:** This one-byte binary sub-field contains the number of bytes following the length sub-field. The maximum value is 255.

**Position 1, Dataset ID:** This one-byte binary sub-field contains a hexadecimal value that identifies the TLV data that follows. Following are the valid values:

Dataset Value Hex 68, Token Data Dataset Value Hex 01, Token Device Dataset Value Hex 02, Wallet Provider

Dataset Value Hex 40, Terms and Conditions

**Positions 2–3, Dataset Length:** This 2-byte binary sub-field specifies the total length of the TLV fields present in the dataset. The length is variable, depending on the data that follows.

**Positions 4–999, TLV Elements:** Each sub-field of a dataset has a defined tag, length, and value. The tag is used in conjunction with the dataset ID value. The dataset sub-fields can be present in any order with other TLV sub-fields.

# PART 5 – Appendices

## Appendix A – Message Matching Criteria

#### Matching Criteria for Clearing Message with Corresponding Authorization (01xx with 022x Matching)

|  |  |  |
| --- | --- | --- |
| **Criteria #** | **Message Type** | **Criteria Fields** |
| 1 | 0100/0220 | DE-002, Transaction Identifier |
| 2 | 0100/0220 | DE-002, DE-038 |
| 3 | 0100/0220 | DE-002, DE-037 |
| 4 | 0100/0220 | DE-002, DE-111.31 |

#### Matching Criteria for Reversal Message with Corresponding Original Message (01xx/02xx with 042x Matching)

|  |  |  |
| --- | --- | --- |
| **Criteria #** | **Message Type** | **Criteria Fields** |
| 1 | 0420 | DE-002, Transaction Identifier |
| 2 | 0420 | DE-002, DE-011, DE-012, DE-032 and DE-037 |
| 3 | 0420 | DE-002, DE-011, DE-032 and DE-037 |
| 4 | 0420 | DE-002, Banknet Reference No. |
| 5 | 0420 | DE-002, DE-038 |

**Transaction Identifier:** A number which remains unique throughout a transaction life cycle. The value is received in DE63.3 (Transaction Identifier) DE111.7 (for MASTERCARD)

## Appendix B – Authorization Expiration Time

In authorization (01xx), funds are held for a configurable time period. Possible configuration can be:

* Auth Expiry Days for Electronic PAN entry Mode
* Auth Expiry Days for Manual PAN entry Mode
* Auth Expiry Days according to Merchant Cat Code

If a particular authorization (01xx) is not settled by merchant within time, then funds are released, and a reversal will be sent to the auth host by i2c for this authorization.

## Appendix C – Data Elements Detailed Definitions

#### Data Element 003 – Processing Codes Table

|  |  |
| --- | --- |
| **Positions 1–2: Transaction Type** | |
| **Code** | **Definition** |
| 00 | Purchase |
| 01 | Withdrawal |
| 02 | Debit Adjustment |
| 03 | Guarantee with Conversion (POS Check Service) (Future Use) |
| 04 | Verification with Conversion (POS Check Service) (Future Use) |
| 06 | Traveler Check |
| 09 | Purchase with Cash Back |
| 10 | Account Funding |
| 11 | Quasi-Cash Transaction–Debit or Internet Gambling Transaction |
| 13 | Funds Withdrawal for Electronic Purse / Address Verification with a goods or services Authorization for Recurring Billing (Recurring Payments) |
| 14 | Recurring Billing (Recurring Payments) – goods or services |
| 15 | Installment Payment – goods or Services |
| 17 | Cash Disbursement |
| 18 | Deferred Goods and Services / Scrip Issue / Conversion Only (POS Check Service) / Card Account Verification |
| 19 | Debit Fee Collection / Deferred Goods and Services With Cash Disbursement |
| 20 | Credit Return (of goods) / Credit Transaction / Credit Voucher or Merchandise / Return Authorization (U.S. Only) / Purchase Return/Refund |
| 21 | Deposit |
| 22 | Credit Adjustment |
| 23 | Check Deposit Guarantee |
| 24 | Check Deposit |
| 25 | Envelope-less Cash Deposit |
| 26 | Original Credit |
| 28 | Prepaid Activation and Load Prepaid Load / Payment Transaction |
| 29 | Credit Funds Disbursement / Primary Credit |
| 30 | Available Funds Inquiry / Commercial Deposit |
| 31 | Balance Inquiry |
| 33 | Account Updater Code / Account Verification (Future Use) |
| 34 | ATM Mini Statement |

|  |  |
| --- | --- |
| 39 | Eligibility Inquiry / Generic Balance Inquiry (Future Use) |
| 40 | Cardholder Account Transfer |
| 50 | Bill Payment / Payment to Another Party |
| 53 | Payment (U.S. only) |
| 54 | Payment Debit (P2P) |
| 55 | Payment from Third Party |
| 56 | Payment Credit (P2P) |
| 58 | Payment from Account to Credit/Loan |
| 59 | Payment Enclosed |
| 72 | Prepaid Activation |
| 91 | PIN Unblock |
| 92 | PIN Change |
| PV | PV Credit Transaction |
| PD | PV Debit Transaction |
| CB | CHARGEBACK CREDIT |
| Q2 | SPECIAL CREDIT 2 |

|  |  |
| --- | --- |
| **Positions 3–4: Account Type (From)** | |
| **Code** | **Definition** |
| 00 | Default Account (Not specified or Not applicable) |
| 10 | Savings Account |
| 20 | Checking Account |
| 30 | Credit Card Account |
| 38 | Credit Line Account |
| 39 | Corporate Account |
| 40 | Universal Account |
| 50 | Money Market Investment Account |
| 60 | Stored Value /Prepaid account |
| 90 | Revolving Loan Account |
| 35 | Deferred debit account |
| 36 | Charge account |

|  |  |
| --- | --- |
| **Positions 5–6: Account Type (To)** | |
| **Code** | **Definition** |
| 00 | Default Account (Not specified or Not applicable) |
| 10 | Savings Account |
| 20 | Checking Account |
| 30 | Credit Card Account |
| 38 | Credit Line Account |
| 40 | Universal Account |
| 50 | Money Market Investment Account |
| 58 | IRA Investment Account |
| 90 | Revolving Loan Account |
| 91 | Installment Loan Account |
| 92 | Real Estate Loan Account |

#### Data Element 022 – POS Entry Mode Codes Table

|  |  |
| --- | --- |
| **Position 1–2: PAN and Date Entry Mode** | |
| **Code** | **Definition** |
| 00 | Unspecified |
| 01 | Manual |
| 02 | Magnetic stripe |
| 03 | Bar code / Consumer-presented QRC, chip information excluded |
| 04 | OCR / Consumer-presented QR Code (QRC), chip information included |
| 05 | Integrated circuit card |
| 06 | Manual (key-entered) |
| 07 | Contact-less via Chip rules |
| 08 | Reserved for ISO use |
| 09 | PAN entry via electronic commerce, including remote chip |

|  |  |
| --- | --- |
| 10 | From file |
| 11 | Full magnetic stripe read (optionally supported) |
| 12 | Contactless via magnetic stripe rules |
| 13 | Integrated circuit card, CVV data may be unreliable |
| 14 | PAN auto-entry via chip PayPass mapping |
| 15 | Contactless M/Chip PayPass Mapping |
| 16 | PAN manual entry via e-commerce |
| 17 | Contactless input PayPass Mapping Service |
| 18 | Store-and-forward |
| 19 | MICR Reader (POS Check Service); U.S. Only |
| 20 | Store-and-forward resubmission |
| 21 | Electronic Commerce |
| 22 | Radio Frequency Identification Indicator |
| 23 | Mobile Commerce (mCommerce) |
| 24 | Voice Authorizations |
| 25 | Voice Response Unit (VRU) |
| 26 | Batch Authorizations |
| 27 | Batch Authorization Cash Access |
| 28 | Biometrics |
| 29 | Credentials on File |
| 30-60 | Reserved for ISO use |
| 61-78 | Reserved for national use |
| 79 | Chip card or chip-capable terminal was unable to process the transaction using the data on the chip or magnetic stripe, the PAN was entered manually, or the Acquirer is not certified to process the value 80. |
| 80 | Chip card or chip-capable terminal was unable to process the transaction using the data on the chip, the PAN was entered via magnetic stripe. The full track data was read from the data encoded on the card and transmitted within the authorization request on Track-2 Data (DE 35) or Track-1 Data (DE 45) without alteration or truncation. |

|  |  |
| --- | --- |
| 81-89 | Reserved for private use |
| 90 | PAN auto-entry via magnetic stripe—the full track data has been read from the data encoded on the card and transmitted within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation. |
| 91 | PAN auto-entry via contact-less magnetic stripe—the full track data has been read from the data on the card and transmitted within the authorization request in DE 35 (Track 2 Data) or DE 45 (Track 1 Data) without alteration or truncation. |
| 92 | PAN Auto Entry via Server (issuer, acquirer, or third-party vendor system) |
| 93 | Merchant-presented QR code, chip information included |
| 94 | Merchant-presented QR code, chip information excluded |
| 95 | Visa only. Chip card with unreliable Card Verification Value (CVV) data. |
| 96-99 | Reserved for private use |

|  |  |
| --- | --- |
| **Position 3: PIN Entry Capability** | |
| **Code** | **Definition** |
| 0 | Unspecified |
| 1 | PIN entry capability |
| 2 | No PIN entry capability |
| 3 | Terminal has PIN entry capability, but PIN pad is out of service |
| 4-5 | Reserved for ISO use |
| 6 | PIN pad inoperative |
| 7 | Reserved for national use |
| 8 | Reserved for private use |
| 9 | PIN verified by terminal device |

#### Data Element 025 – POS Condition Codes Table

|  |  |
| --- | --- |
| **Data Element 025 – Point-of-Service Condition Codes** | |
| **Code** | **Definition** |
| 00 | Normal presentment |

|  |  |
| --- | --- |
| 01 | Customer not present |
| 02 | ATM Transactions |
| 03 | Merchant suspicious |
| 04 | Electronic card register interface |
| 05 | Customer present, card not present |
| 06 | Pre-Authorized request |
| 07 | Telephone device/mobile phone request |
| 08 | Mail and/or telephone order |
| 09 | Security alert |
| 10 | Customer identity verified |
| 11 | Suspected fraud |
| 12 | Security reasons |
| 15 | Customer terminal (home terminal) |
| 16 | Administration terminal |
| 17 | Chargeback (validation request or advice) |
| 27 | Unattended terminal unable to retain card |
| 28-39 | Reserved for ISO use |
| 40 | Customer not present, standing order/recurring payment |
| 41-50 | Reserved for national use |
| 51 | Point of Sale (POS) |
| 52 | CVV verified and valid |
| 53 | CVV verified and invalid |
| 54 | Non-Secure/Security unknown electronic commerce transaction |
| 55 | Secure electronic transaction with cardholder certificate |
| 56 | Secure electronic transaction without cardholder certificate |
| 57 | Channel-encrypted electronic commerce transaction |
| 58 | Secure electronic transaction containing a digital signature |

|  |  |
| --- | --- |
| 59 | Deferred billing |
| 60 | Internet PIN debit transaction |
| 61 | Reserved for private use |
| 62 | Account Verification w/o Auth; product eligibility inquiry without authorization |
| 63 | POS Check original full financial transaction or adjustment; |
| 64 | Chargeback reversal |
| 65 | Request for telecode verification without authorization |
| 66 | Electronic commerce request by public network |
| 67-70 | Reserved for private use |
| 71 | Card present, magnetic stripe cannot be read (key-entered) |
| 72 | Unattended terminal able to retain card |
| 73-99 | Reserved for private use |

#### Data Element 026 – POS PIN Capture Codes Table

|  |  |
| --- | --- |
| **Data Element 026 – Point-of-Service PIN Capture Codes** | |
| **Code** | **Definition** |
| 00-04 | Invalid |
| 05-12 | Indicates the maximum number of PIN characters that the terminal can accept |
| 13-99 | Reserved |

#### Data Element 039 – Response Codes Table

|  |  |
| --- | --- |
| **Data Element 039 – Response Codes** | |
| **Code** | **Definition** |
| 00 | Approved |
| 01 | Refer to Card Issuer |
| 02 | Refer to Card Issuer, Special Condition |
| 03 | Invalid Merchant |
| 04 | Lost/Stolen Card |
| 05 | Do not Honor |
| 06 | Error |

|  |  |
| --- | --- |
| 07 | Pick-up Card, Special Condition |
| 08 | Honor with Identification |
| 10 | Approved – Partial Amount |
| 12 | Invalid Transaction |
| 13 | Invalid Amount |
| 14 | Invalid Card Number |
| 15 | Invalid Issuer |
| 17 | Customer Cancellation, Reversal |
| 27 | Issuer File Update Field Edit Error |
| 30 | Format Error |
| 31 | Bank Not Supported by Switch (Future Use) |
| 32 | Partial Reversal |
| 33 | Expired Card, Pick-up |
| 34 | Suspect Fraud |
| 39 | No Credit Account (Future Use) |
| 40 | Requested Function Not Supported |
| 41 | Lost Card Not Captured |
| 42 | No universal account |
| 43 | Stolen Card, Pick-up |
| 51 | Insufficient Funds |
| 52 | No Checking Account (Future Use) |
| 53 | No Savings Account (Future Use) |
| 54 | Expired Card |
| 55 | Invalid PIN |
| 56 | No Card Account |
| 57 | Transaction not Permitted to Cardholder |
| 58 | Transaction not Permitted to Acquirer/Terminal |
| 59 | Suspected Fraud |
| 61 | Exceeds Withdrawal Amount Limit |
| 62 | Restricted Card |
| 63 | Decline Error in Decryption of PIN Block / Security Violation |
| 64 | Original Amount Incorrect, Reversal |
| 65 | Exceeds Withdrawal Frequency Limit |
| 68 | Response Received Late |

|  |  |
| --- | --- |
| 70 | Invalid Transaction; Contact Card Issuer |
| 71 | PIN Change Decline |
| 75 | Allowed Number of PIN Tries Exceeded |
| 76 | Invalid/Nonexistent “To” Account Specified (Future Use) |
| 77 | Invalid/Nonexistent “From” Account Specified (Future Use) |
| 78 | Invalid/Nonexistent Account Specified (General) (Future Use) |
| 79 | Key Exchange Validation Failed |
| 80 | System not Available (Future Use) |
| 81 | Invalid Transaction (PIN Block Format Error) |
| 82 | Time Out Issuer |
| 84 | Invalid Authorization Life Cycle |
| 85 | Approved – Account Verification |
| 86 | PIN Validation Not Possible or Invalid PVK/ZPK/Offset/PVV |
| 87 | Approved – Purchase Only |
| 88 | Invalid Transaction (CVC1/CVV2/CID/iCVV Format Error) |
| 89 | Bad CVC1/iCVV/Expiry Date |
| 91 | Issuer or Switch Inoperative |
| 92 | Unable to Route Transaction |
| 93 | Transaction Cannot be Completed |
| 94 | Duplicate Transmission |
| 96 | Refer to Card Issuer / System Error |
| 97 | Already Activated Card |
| 99 | Approve Transaction in Super Green Path |
| AT | Auth-Host Timed Out |
| CD | Cryptogram Decline |
| CN | Invalid Currency |
| DN | Duplicate Record Found Against Name and DOB / Auth-Host Down |
| EX | Status inquiry / Account Verification declined due to invalid Card Expiry |
| E7 | Bad CVV2/CID/Expiry Date |
| GA | General AVS Decline |
| GC | General Card Decline |
| GV | General CVV2 Decline |
| PA | Card is Pre-Active |
| PF | Purse Found with Invalid Status |

|  |  |
| --- | --- |
| PI | PIN Change Fail Invalid Data |
| PL | Bad PIN (Invalid PIN Block Length) |
| SA | Inactive Card |
| SD | Account Closed |
| SX | Status inquiry / Account Verification declined due to invalid Card Status |
| TM | Card Technology Mismatch |
| TR | Token Provisioning / Authorization Request declined with Red Path |
| X1 | Bad AVS |
| 1A | Strong Customer Authentication Required |
| AI | ATC Validation Failed (Authorization Host must set response code AI in case of ATC validation failure at authorization host side) |
| X6 | Valid account but amount not supported |

\*\*For any forced post message 0x2x, auth host must respond with approved response code i.e. “00”

##### Data Element 043 – Card Acceptor Name/Location

\*\*Usage-1 Details (For existing clients):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-43 – Card Acceptor Name/Location (Usage-1)** | | | | |
| **Sub Field No.** | **Field Name** | **Description** | **Positio n** | **Format (ASCII)** |
| 43.1 | Address | Merchant’s Street Address | 1-25 | 25 AN |
| 43.2 | City | Merchant’s City Name | 26-38 | 13 AN |
| 43.3 | State | Merchant’s State | 39-40 | 2 AN |
| 43.4 | Country | Merchant’s Country Code | 41-43 | 3 AN |

\*\*Usage-2 Details (For new clients):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-43 – Card Acceptor Name/Location (Usage-2)** | | | | |
| **Sub Field No.** | **Field Name** | **Description** | **Positio n** | **Format (ASCII)** |
| 43.1 | Address | Merchant’s Street Address | 1-25 | 25 AN |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 43.2 | City | Merchant’s City Name | 26-40 | 15 AN |
| 43.3 | State | Merchant’s State | 41-42 | 2 AN |
| 43.4 | Country | Merchant’s Country Code | 43-45 | 3 AN |
| 43.5 | Card Acceptor Name | Merchant’s Name | 46-70 | 25 AN |

\*\* Note: In case of Usage-2, Card Acceptor Name will be sent to Auth-Host if only received from network as mostly it is sent by network in Address field (43.1). In this case, field-43.5 will consist of ALL spaces.

Currently, it is only supported by FISERV.

#### Data Element 048 – Additional Processing Data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-48 – Additional Processing Data** | | | | |
| **Sub Field No.** | **Field Name** | **Description** | **Position** | **Format (ASCII)** |
| 48.1 | EMV – Issuer Script Command Identifiers | The identifiers of the Issuer Script Commands sent in the response as a result of EMV processing.  Below are the supported Script Command Identifiers:   * **01** – PIN Change * **02** – PIN Unblock   The field will be left-justified space-filled. If multiple script commands are sent in a transaction, this field will contain all script commands identifiers. For example, if both PIN Change (01) & PIN Unblock (02) scripts are sent, this sub-field will be formatted as: '0102 '. | 1-12 | 12 AN |
| 48.2 | EMV – Result of Issuer Script Commands sent in Previous Transaction | The status of the EMV Issuer Script Commands sent in the previous transaction. It will tell that whether the issuer script sent in response was successfully executed on the card or not. Possible values are:   * **(space)** – Pending * **P** – Passed * **F** – Failed | 13 | 1 AN |
| 48.3 | Transaction Processing Indicator | The indicator which described the purpose or type of processing performed on a transaction.  The field is a 2 byte alphanumeric which can hold below list of possible values:   * **PC** – The indicator identifies a Pending Credit Financial Advice (0220). The credit will be posted to the card account against the credit authorization. * **HC** – The indicator represents a debit authorization advice (0120) which is to hold the credit given in 0220 credit financial advice. | 14-15 | 2 AN |
| 48.4 | Card Status Validation Result Code | This field will identify the result of the Card Status Validation Service. Refer to the table below for the possible result code values. | 16 | 1 AN |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 48.5 | Card Expiry Validation Result Code | This field will describe the result of the Card Expiry Validation Service. Possible result code values are:   * 1 – Expired Card | 17 | 1 N |
| 48.6 | Card Balance Indicator | This field will indicate the state of the card balance (in case of insufficient funds). Possible result code values are:   * 0 – Card has zero balance * 1 – Card has positive balance * 2 – Card has negative balance | 18 | 1 N |
| 48.7 | Message Reason Code | This field is used in reversals (04xx) to indicate the response code of original transaction.  This code will be used in reversals initiated by i2c as a result of processing failure of authorizations which are already approved by the Authorization Host.  The key possible values includes:  **03** – Invalid merchant  **05** – System malfunction  **57** – Transaction not permitted to cardholder  **59** – Suspected Fraud / Limits Violation  Other possible values may include all values of Field 39. | 19-20 | 2 AN |
| 48.8 | Application Transaction Counter (ATC) | It will contain 5 digit ATC value. Default Value 00000. | 21-25 | 5 N |
| 48.9 | Process Mode | It will contain process mode. Possible Values:   * SMS * DMS * AXS (Represents STAR Access network) | 26-28 | 3 AN |
| 48.10 | Expire Pre Auth Reversal Message Indicator. | This will only applicable for Reversal messages x4xx. Possible values:   * Y * N   Value Y represent that the respective x4xx is the reversal messages of Pre  Authorization transaction automatically generated by i2c System to expire the authorization for which no clearing / completion message receive from network after N number of configured days. | 29-33 | 1 N |

|  |  |
| --- | --- |
| **Card Status Result Codes** | |
| **Card Status** | **Result Code** |
| Already Active Card | 1 |
| Pick Up – No Fraud | 2 |
| Pick Up – Fraud Account | 3 |
| Restricted Card | 4 |
| Lost Card | 5 |
| Stolen Card | 6 |
| Inactive Card | 7 |
| Suspected Card | 8 |
| Pre-active Card | 9 |
| Closed Card | A |

#### Data Element 054 – Additional Amounts Codes Table

|  |  |
| --- | --- |
| **Data Element 054 – Positions 1–2: Account Type** | |
| **Code** | **Definition** |
| 00 | Not Specified or Default Account |
| 10 | Savings Account |
| 20 | Checking Account |
| 30 | Credit Card Account |
| 40 | Universal Account |

|  |  |
| --- | --- |
| **Data Element 054 – Positions 3–4: Amount Type** | |
| **Code** | **Definition** |
| 00 | Unknown |
| 01 | Ledger Balance |
| 02 | Available Balance |
| 03 | Amount Owing |
| 04 | Amount Due |
| 05 | Account Available Credit |
| 06 | Amount Currency Conversion Assessment |
| 07 | Over Limit Fee |

|  |  |
| --- | --- |
| 08 | Over Payment Fee |
| 10 | Healthcare Eligibility Amount |
| 11 | Prescription Eligibility Amount |
| 16 | Credit Line |
| 17 | Prepaid Online Bill Pay Fee Amount or POS balance/ATM overdraft protection balance |
| 18 | Beginning Balance |
| 20 | Amount Remaining this Cycle |
| 40 | Amount Cash Back |
| 41 | Amount Goods and Services |
| 42  44 | Amount Surcharge Amount, anticipated |
| 56 | Hold Amount |
| 57 | Original Amount or Pre-Authorized Amount |
| 58 | Authorized Amount (StarAccess) |
| 59 | Floor Limit |
| 72 | Fee Amount: Added in Card-Holder Billing Amount i.e. DE 06. |
| 80 | Co-pay Amount |
| 90 | Available Credit or Check Amount |
| 91 | Credit Limit or Original amount/Tip or Gratuity for Service |
| 93 | Cash Deposit Amount |
| 94 | Check Deposit Amount |
| 95 | Foreign Exchange Fee |
| 96 | Merchant Local Currency/Cash Benefit Amount |
| 98 | Courtesy Amount |
| 99 | Original Cash Back Amount |
| 73 | Interchange Fee |
| 43 | Total Authorization Amount (in case of Incremental Authorization total accumulative amount) |
| 46 | ATM Excess Usage Fee |
| 47 | Currency Conversion Excess Usage Fee |

#### Data Element 061 – Point-of-Service Data Codes Table

|  |  |
| --- | --- |
| **Data Element 061 – Position 1 (Attendance Indicator)** | |
| **Code** | **Definition** |
| 0 | Attended |
| 1 | Unattended |
| 2 | No terminal used (voice/audio response unit [ARU] authorization) |
| 9 | Unknown/data not available |
| R | Reserved for National or Private Use |

|  |  |
| --- | --- |
| **Data Element 061 – Position 2 (Operator Indicator)** | |
| **Code** | **Definition** |
| 0 | Customer-operated |
| 1 | Card acceptor-operated |
| 2 | Administrative |

|  |  |
| --- | --- |
| **Data Element 061 – Position 3 (Terminal Location Indicator)** | |
| **Code** | **Definition** |
| 0 | On premise |
| 1 | Off premise |
| 2 | On premises of cardholder (Home PC) |
| 3 | No terminal used |
| 4 | On premises of card acceptor facility [Card-Holder terminal including Home PC, mobile phone, PDA] |
| 6 | Off cardholder premised, unattended |
| 9 | Unknown data not available |

|  |  |
| --- | --- |
| **Data Element 061 – Position 4 (Cardholder Presence Indicator)** | |
| **Code** | **Definition** |
| 0 | Customer present |

|  |  |
| --- | --- |
| 1 | Customer not present |
| 2 | Mail/Facsimile order (customer not present) |
| 3 | Telephone order |
| 4 | Customer not present, standing order/recurring payment |
| 5 | Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDS]) |
| 8 | Pre-Authorized purchase |
| 9 | Unknown data not available |
| S | Installment Payment |
| R | Reserved |
| A | CardHolder not present Stand-In Authorization |

|  |  |
| --- | --- |
| **Data Element 061 – Position 5 (Card Presence Indicator)** | |
| **Code** | **Definition** |
| 0 | Card present |
| 1 | Card not present |
| 8 | Pre-Authorized purchase |
| 9 | Unknown / data not available |
| R | Reserved |
| 2 | Amex contactless Transaction |
| 3 | Digital Wallet – Conatctless Initiated |
| 4 | Digital Wallet – Application Initiated |
| 5 | Issuer Originated Payments |

|  |  |
| --- | --- |
| **Data Element 061 – Position 6 (Card Retention Indicator)** | |
| **Code** | **Definition** |
| 0 | Device does not have card retention capability |
| 1 | Device has card retention capability |
| 9 | Unknown data not available |

|  |  |
| --- | --- |
| **Data Element 061 – Position 7 (Transaction Status Indicator)** | |
| **Code** | **Definition** |

|  |  |
| --- | --- |
| 0 | Original presentment |
| 1 | First representment |
| 2 | Second representment |
| 3 | Third representment |
| 4 | Previously authorized request |
| 5 | Resubmission |
| 6 | Merchant-approved Purchase |
| 7 | Time Based Payment Authorization Request or CDC inquiry request |
| 8 | Pre-authorization request/Card Validation/Account Status Check |
| 9 | Debit MasterCard Stand-In |
| A | Purchase with Cash back |
| B | Single transaction of a mail/phone order |
| C | Recurring transaction |
| D | Installment payment |
| E | Unknown classification |
| F | Secure electronic commerce transaction |
| G | Non-authenticated security transaction at a 3-D Secure-capable merchant, and merchant attempted to authenticate the cardholder using 3-D Secure |
| H | Non-authenticated Security Transaction |
| I | Non-secure transaction |
| J | Not Applicable |
| K | Account Status Inquiry Service |
| L | Non-SET trans from SET-enabled merchant |
| M | Secure Code Phone Order |
| N | ATC Update |
| R | Reserved |

|  |  |
| --- | --- |
| **Data Element 061 – Position 8 (Transaction Security Indicator)** | |
| **Code** | **Definition** |
| 0 | No security concern |
| 1 | Suspected fraud |
| 2 | Identification verified |
| 3 | Electronic commerce transaction with digital signature |
| 4 | Non-secure/Security unknown electronic commerce transaction |

|  |  |
| --- | --- |
| 5 | Secure electronic transaction with cardholder certificate |
| 7 | Channel-encrypted electronic commerce transaction |
| 8 | CVV validated and valid |
| 9 | CVV validated and invalid |
| A | Cardholder verified by Biometrics |
| B | Unknown |
| C | Chip Transaction Indicator present |
| D | Acquirer indicates that Card Authentication may not be reliable. |
| E | V.I.P. indicates acquirer inactive for Card Authentication. |
| F | V.I.P. indicates issuer inactive for Card Authentication. |
| R | Reserved |

|  |  |  |
| --- | --- | --- |
| **Data Element 061 – Position 9-10 (Terminal Type Indicator)** | |  |
| **Code** | **Definition** |
| 00 | Administrative terminal |  |
| 01 | POS terminal |  |
| 02 | ATM |  |
| 03 | Home terminal |  |
| 04 | ECR |  |
| 05 | Dial terminal/Call Center Operator |  |
| 06 | Fuel machine/ Travelers Check Machine |  |
| 07 | Fuel Machine |  |
| 08 | POS script machine |  |
| 09 | Coupon machine |  |
| 10 | Ticket machine |  |
| 11 | Franchise teller/Point of Banking terminal |  |
| 12 | Personal banking |  |
| 13 | Public utility |  |
| 14 | Vending |  |
| 15 | Self-service |  |
| 16 | Authorization |  |
| 17 | Payment |  |
| 18 | VRU |  |
| 19 | Smart phone |  |

|  |  |  |
| --- | --- | --- |
| 20 | Interactive television |  |
| 21 | Personal Digital Assistant (PDA)/Mobile Device |  |
| 22 | Screen phone |  |
| 23 | Electronic commerce |  |
| 24 | Transponder (IBM-only) / MICR terminals at POS (Tandem-only) |  |
| 26 | Off Premise |  |
| 27 | Not a CAT transaction |  |
| 28 | Authorized Level 1 CAT: automated dispensing machine with PIN or ATM |  |
| 29 | Authorized Level 3 CAT: limited amount terminal |  |
| 30 | Authorized Level 4 CAT: In-flight Commerce |  |
| 31 | Unspecified |  |
| 32 | Reserved |  |
| 33 | Unattended customer terminal |  |
| 34 | Travelers Check Machine |  |
| 35 | MICR terminal at teller |  |
| 36 | Internet Terminal |  |
| 37 | POS terminal allows partial pre-authorizations |  |
| 38 | Multimedia Terminal |  |
| 39 | Manual Transactions at Bank Counter |  |
| 40 | Personal Computer |  |
| 41 | Mobile Phone |  |
| 42 | I type fixed phone (Telephone without PIN pad) |  |
| 43 | II type fixed phone |  |
| 44 | Wireless POS |  |
| 45 | CDRS |  |
| 46 | Merchant’s Terminal |  |
| 47 | Setup Box |  |
| 48 | Batch File Processing System |  |
| 49 | Authorized Level 2 CAT |  |
| 99 | Unknown |  |
| **Data Element 061 – Position 11 (Terminal Input Capability Indicator)** | | |
| **Code** | **Definition** | |
| 00 | Unknown | |
| 01 | Manual, no terminal | |
| 02 | Magnetic stripe | |

|  |  |
| --- | --- |
| 03 | Bar code |
| 04 | OCR |
| 05 | ICC |
| 06 | File |
| 07 | Contact-less read capability via Mag stripe rules |
| 08 | Contact-less read capability via Chip rules |
| 09 | Mag stripe reader and key entry/Terminal does not read card data |
| 10 | Mag stripe reader and key entry and EMV-Compatible ICC reader |
| 11 | Contact-less M/Chip (Proximity Chip) Terminal supports PayPass M/Chip and PayPass mag-stripe transactions. The terminal also may support contact transactions; however, this  value must only be used for Contact-Less Transactions. |
| 12 | EMV specification (compatible chip reader) and magnetic stripe reader. This terminal can  also support contact-less transactions; however, these values must only be used for contact transactions. |
| 13 | Key entry only |
| 14 | EMV specification (compatible chip reader) only. This terminal can also support contact- less transactions; however, this value must only be used for contact transactions. |
| 15 | MICR read (POS Check Service), U.S. Only |
| 16 | MICR read and image-capable (POS Check Service), U.S. Only |
| 17 | Terminal does not read card data |
| 18 | Radio Frequency Identification (RFID) |
| 19 | Secure Electronic Transaction (SET) with certificate |
| 20 | SET without certificate |
| 21 | Channel-encrypted Electronic Commerce Transaction (SSL) |
| 22 | Non-secure Electronic Commerce Transaction |
| 23 | Mobile Device |
| 24 | F (No Value) |
| 25 | Secure Cardless Entry |

|  |  |
| --- | --- |
| **Data Element 061 – Position 13 (Chip Condition Codes)** | |
| **Code** | **Definition** |
| 0 | Not applicable to fallback transactions. |
| 1 | This value applies to fallback transactions. Transaction was initiated from a magnetic stripe with a service code beginning with 2 or 6 and the last read at VSDC terminal was a successful chip read or was not a chip transaction. |
| 2 | This value applies to fallback transactions. Transaction was initiated at a chip-capable |



|  |  |
| --- | --- |
|  | terminal from a magnetic stripe that contains service code 2 or 6, and the previous  transaction initiated by that terminal was an unsuccessful chip read. |

|  |  |
| --- | --- |
| **Data Element 061 – Position 14 (Special Condition Indicator)** | |
| **Code** | **Definition** |
| 0 | Default Value |
| 9 | Payment on existing debt |
| 1 | Electronic Commerce with security |
| 2 | Electronic Commerce without security |
| 4 | In-Flight Transaction |
| 7 | Purchase of Cryptocurrency |
| 8 | Quasi Cash |

|  |  |
| --- | --- |
| **Data Element 061 – Position 15 (Chip Transaction Indicator)** | |
| **Code** | **Definition** |
| 0 | Not applicable; subsequent sub-fields are present When an Early Data option acquirer, or a Full Data option acquirer, submits Early Data, field 60.6 must contain zero (0) or be excluded from the message. |
| 1 | This value is sent by acquirers using either the standard third bitmap or field 55 to submit chip data. |
| 2 | This value is sent by acquirers using the expanded third bitmap for their chip data. The value 2 applies only to acquirers; V.I.P. changes it to 1 before the request is forwarded to the issuer. |
| 3 | V.I.P. (not the acquirer) inserts this code and downgrades the transaction by dropping chip data section. |
| 4 | V.I.P inserts this code based on the presence of a Visa issued token. |

|  |  |
| --- | --- |
| **Data Element 061 – Position 16 (Cardholder ID Method Indicator)** | |
| **Code** | **Definition** |
| 0 | Not specified |
| 1 | Signature |
| 2 | PIN |
| 3 | Unattended terminal, no PIN pad |
| 4 | Mail/Telephone/Electronic Commerce |

|  |  |
| --- | --- |
| 5 | TransQPS Action (Quick payment Service), I will pay without signature |
| 10 | Biometric |
| 11 | Offline PIN |
| 12 | Pattern Recognition |
| 13 | Device Code / Other |

|  |  |
| --- | --- |
| **Data Element 061 – Position 17 (Chip Card Authentication Reliability Indicator)** | |
| **Code** | **Definition** |
| 0 | Not specified |
| 1 | Acquirer indicates that Card Authentication may not be reliable |
| 2 | Switch indicates acquirer inactive for Card Authentication. |
| 3 | Switch indicates issuer inactive for Card Authentication. |
| 4 | Switch Center indicates that the transaction has used Token Service provided by the network itself. |

|  |  |
| --- | --- |
| **Data Element 061 – Position 18 (Mail/Phone/Electronic Commerce and Payment Indicator)** | |
| **Code** | **Definition** |
| 0 | Not Applicable |
| 1 | Unknown/Unspecified |
| 2 | Not an e-commerce transaction |
| 3 | Single transaction of a mail/phone order |
| 4 | Recurring transaction |
| 5 | Installment payment |
| 6 | Secure electronic commerce transaction |
| 7 | Non-authenticated security transaction at a 3-D Secure-capable merchant, and merchant attempted to authenticate the cardholder using 3-D Secure |
| 8 | Non-authenticated Security Transaction |
| 9 | Non-secure transaction |
| A | In-App Authentication |
| B | Electronic commerce transaction with digital signature |
| C | Secure electronic transaction with cardholder certificate |
| D | Secure electronic transaction without cardholder certificate |

|  |  |
| --- | --- |
| **Data Element 061 – Position 19 (Interactive Mode Identifier)** | |
| **Code** | **Definition** |
| 0 | Default |
| 1 | Internet |
| 2 | Text Message (SMS) |
| 3 | Voice (IVR) |
| 4-9 | Reserved |
| K | Failed CUPSecure safe authentication, and does not adopt the security technology of encryption. |
| E | Channel-encrypted electronic commerce transaction |
| F | UnionPay safe entry mode authentication conducted, and cardholder security information is input successfully |
| G | Certification of Issuer SAA direct authentication authorization conducted, and the SAA authentication authorization is successful |
| H | Authentication of Issuer SA direct status verification conducted, and the cardholder status verification is successful |
| I | Tried to conduct the issuer direct status verification |
| J | Failed CUPSecure safe authentication, but adopt the security technology of channel |
| L | Issuer Authentication Mode in card-no-present self-service transactions |
| M | Issuer Non-Authentication Mode in card-no-present self-service transaction |
| N | Static UCAF Value (Switch assigned static AAV) |
| O | Issuer Risk based Decision |
| P | Aquirer Risk based Decision |
| Q-Z | Reserved |

**Data Element 108 – Receiver/Sender Data Table DE 108 – TLV Fields Details when DE-63.7 = ‘VISA’:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-108 when DE-63.7 = ‘VISA’** | | | | |
| **Tag** | **Length** | **Value** | **Format** | **Content of Sub-Element** |
| 01 | 16 | Sender Reference Number | AN | Contains a transaction reference number that is provided by the originator or acquirer and can be used to uniquely identify the entity funding the transaction. |
| 02 | 34 | Sender Account Number | AN | Contains the account number of the entity funding the transaction. |
| 03 | 30 | Sender Name | AN | Contains the name of the entity funding the transaction. |
| 04 | 35 | Sender Address | AN | Contains the address of the entity funding the transaction. |
| 05 | 25 | Sender City | AN | Contains the city of the entity funding the transaction. |
| 06 | 2 | Sender State | AN | Contains the geographical state or province of the entity funding the transaction.  Sender State is required when Sender Country in Tag 07 contains **124** (Canada) or **840** (U.S.). This field is optional otherwise. |
| 07 | 3 | Sender Country | AN | Contains the country of the entity funding the transaction.  **Format**: 3-digit ISO country code. |
| 08 | 2 | Source of Funds | AN | Indicates the method used by the sender to fund an OCT.  The tag is required in all domestic and cross- bordermoney transfer OCTs destined to U.S. recipient issuers.  Values are:  **01** = Visa credit **02** = Visa debit **03** = Visa prepaid **04** = Cash  **05** = Debit/deposit access accounts other than those linked to a Visa card (includes checking / savings accounts and proprietary debit/ Automated Teller Machine (ATM) cards)  **06** = Credit accounts other than those linked to a Visa card (includes credit cards and proprietary credit lines) |
| 09 | 20 | Claim Code | AN | **Visa Mobile Prepaid (VMP) Transaction**: Tag contains the third-party request reference number. VMP transactions are supported for certain countries in the AP, CEMEA, and LAC regions only. For a |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | given transaction, the issuer, acquirer, and merchant must be within the same country. |
| 0A | 30 | Recipient Name | AN | Contains the name of the entity receiving the funds. |
| 0B | 20 | Confirmation Number | AN |  |
| 0C | 25 | Recipient City | AN | Contains the city of the entity receiving the funds. |
| 0D | 3 | Recipient Country | N |  |
| 0E | 3 | Proprietary Account Type | AN | Contains the country of the entity receiving the funds.  **Format**: 3-digit ISO country code. |
| 0F | 12 | Proprietary Amount | N |  |
| 10 | 5-10 | Sender postal Code | AN | Contains the postal code of the entity funding the transaction. |

**DE 108 - Sub Field 01 Details when DE-63.7 = ‘MASTERCARD’**:

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub Element 01 of DE-108 [Receiver/Recipient Data] when DE-63.7 = ‘MASTERCARD’** | | | |
| **Sub Field No.** | **Sub Field Name** | **Sub Field Length** | **Data Representation** |
| 01 | First Name | 2 | ans…35; LLVAR |
| 02 | Middle Name | 2 | ans-1 |
| 03 | Last Name | 2 | ans…35; LLVAR |
| 04 | Street Address | 2 | ans…50; LLVAR |
| 05 | City | 2 | ans…25; LLVAR |
| 06 | State/Province Code | 2 | ans…3; LLVAR |
| 07 | Country | 2 | ans-3 |
| 08 | Postal Code | 2 | ans…10; LLVAR |
| 09 | Phone Number | 2 | ans…20; LLVAR |
| 10 | Date of Birth | 2 | n-8 |
| 11 | Account Number | 2 | n…20; LLVAR |
| 12 | Identification Type | 2 | n-2 |
| 13 | Identification Number | 2 | ans…25; LLVAR |
| 14 | Identification Country Code | 2 | ans-3 |
| 15 | Identification Expiration Date | 2 | n-8 |
| 16 | Nationality | 2 | ans-3 |
| 17 | Country of Birth | 2 | ans-3 |
| 18 | Account Type | 2 | n-2 |

**DE 108 - Sub Field 02 Details when DE-63.7 = ‘MASTERCARD’:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub Element 02 of DE-108 [Sender Data] when DE-63.7 = ‘MASTERCARD’** | | | |
| **Sub Field No.** | **Sub Field Name** | **Sub Field Length** | **Data Representation** |
| 01 | First Name | 2 | ans…35; LLVAR |
| 02 | Middle Name | 2 | ans-1 |
| 03 | Last Name | 2 | ans…35; LLVAR |
| 04 | Street Address | 2 | ans…50; LLVAR |
| 05 | City | 2 | ans…25; LLVAR |
| 06 | State/Province Code | 2 | ans…3; LLVAR |
| 07 | Country | 2 | ans-3 |
| 08 | Postal Code | 2 | ans…10; LLVAR |
| 09 | Phone Number | 2 | ans…20; LLVAR |
| 10 | Date of Birth | 2 | n-8 |
| 11 | Account Number | 2 | n…20; LLVAR |
| 12 | Identification Type | 2 | n-2 |
| 13 | Identification Number | 2 | ans…25; LLVAR |
| 14 | Identification Country Code | 2 | ans-3 |
| 15 | Identification Expiration Date | 2 | n-8 |
| 16 | Nationality | 2 | ans-3 |
| 17 | Country of Birth | 2 | ans-3 |
| 18 | Account Type | 2 | n-2 |

**DE 108 - Sub Field 03 Details when DE-63.7 = ‘MASTERCARD’:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub Element 03 of DE-108 [Transaction Reference Data] when DE-63.7 = ‘MASTERCARD’** | | | |
| **Sub Field No.** | **Sub Field Name** | **Sub Field Length** | **Data Representation** |
| 01 | Unique Transaction reference | 2 | ans…19; LLVAR |
| 02 | Additional Message | 2 | ans…65; LLVAR |
| 03 | Funding Source | 2 | n…2 |
| 04 | Participation ID | 2 | ans…30; LLVAR |
| 05 | Transaction Purpose (Possible Values are listed in below table ) | 2 | n…2 |

**DE108.03.05: Possible Values for Transaction Purpose when DE-63.7 = ‘MASTERCARD’**

|  |  |
| --- | --- |
| **Possible value** | |
| **Value** | **Definition** |
| 00 | Family Support |
| 01 | Regular Labor Transfers (expatriates) |
| 02 | Travel & Tourism |
| 03 | Education |
| 04 | Hospitalization & Medical Treatment |
| 05 | Emergency Need |
| 06 | Savings |
| 07 | Gifts |
| 08 | Others |
| 09 | Salary |
| 10 - 15 | Reserved |

**DE 108 - Sub Field 04 Details when DE-63.7 = ‘MASTERCARD’:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub Element 04 of DE-108 [Language Description] when DE-63.7 = ‘MASTERCARD’** | | | |
| **Sub Field No.** | **Sub Field Name** | **Sub Field Length** | **Data Representation** |
| 01 | Language Identification | 2 | ans…2 |
| 02 | Language Data | 2 | b…50; LLVAR |

**DE 108 - Sub Field 05 Details when DE-63.7 = ‘MASTERCARD’:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub Element 05 of DE-108 [Digital Account Information] when DE-63.7 = ‘MASTERCARD’** | | | |
| **Sub Field No.** | **Sub Field Name** | **Sub Field Length** | **Data Representation** |
| 01 | Digital Account reference Number | 2 | n…19; LLVAR |
| 02 | Mastercard Merchant Presented QR Receiving Account Number | 2 | ans…34; LLVAR |

##### Data Element 111 – Additional Data Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Elements of DE-111 when DE-63.7 = ‘VISA’** | | | | |
| **Sub Field No.** | **Sub Field Name** | **Visa Bit No.** | **Position** | **Format (ASCII)** |
| 111.1 | Authorization characteristics indicator | 62.1 | 1 | 1 AN |
| 111.2 | Transaction identifier | 62.2 | 2-16 | 15 N |
| 111.3 | Validation code | 62.3 | 17-20 | 4 AN |
| 111.4 | Market-specific data indicator 2 | 62.4 | 21 | 1 AN |
| 111.5 | Duration | 62.5 | 22-23 | 2 N |
| 111.6 | Purchase identifier | 62.7 | 24-49 | 26 AN |
| 111.7 | Date; auto rental check-out, lodging check-in | 62.8 | 50-55 | 6 N |
| 111.8 | No show indicator | 62.9 | 56 | 1 AN |
| 111.9 | Extra charges | 62.10 | 57-62 | 6 N |
| 111.10 | Multiple clearing sequence number | 62.11 | 63-64 | 2 N |
| 111.11 | Multiple clearing sequence count | 62.12 | 65-66 | 2 N |
| 111.12 | Restricted ticket indicator | 62.13 | 67 | 1 AN |
| 111.13 | Total amount authorized | 62.14 | 68-79 | 12 N |
| 111.14 | Requested payment service | 62.15 | 80 | 1 AN |
| 111.15 | Chargeback rights indicator | 62.16 | 81-82 | 2 AN |
| 111.16 | Electronic commerce goods indicator | 62.19 | 83-84 | 2 AN |
| 111.17 | Merchant verification value | 62.20 | 85-94 | 10 N |
| 111.18 | Online risk assessment risk score and reason codes | 62.21 | 95-98 | 4 AN |
| 111.19 | Online risk assessment condition codes | 62.22 | 99-104 | 6 AN |
| 111.20 | Card-level results | 62.23 | 105-106 | 2 AN |
| 111.21 | Network ID | 63.1 | 107-110 | 4 N |
| 111.22 | Message reason code | 63.3 | 111-114 | 4 N |
| 111.23 | STIP/Switch reason code | 63.4 | 115-118 | 4 N |
| 111.24 | Visa acquirer’s business id | 63.8 | 119-126 | 8 N |
| 111.25 | Fraud data | 63.9 | 127-140 | 14 ANS |
| 111.26 | Reimbursement attribute | 63.11 | 141 | 1 ANS |
| 111.27 | Merchant volume indicator | 63.18 | 142-143 | 2 N |
| 111.28 | Fee program indicator | 63.19 | 144-146 | 3 AN |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 111.29 | Charge indicator | 63.21 | 147 | 1 ANS |
| 111.30 | Stand In Trans Indicator ([Possible Values](#_bookmark106)) |  | 148 | 1 N |
| 111.31 | Transaction Unique Identifier |  | 149-154 | 6 AN |
| 111.32 | Token Device Id | 125.03 | 155-218 | 64 AN |
| 111.33 | Token Device No | 125.04 | 219-233 | 15 N |
| 111.34 | Token Device Name | 125.05 | 234-253 | 20 AN |
| 111.35 | Token Device Type ([Possible Values](#_bookmark109)) | 125-01 | 254-255 | 2 AN |
| 111.36 | Token ID | 123.01 | 256-274 | 19 AN |
| 111.37 | Token Type ([Possible Values](#_bookmark107)) | 123.07 | 275-276 | 2 AN |
| 111.38 | Token Status ([Possible Values](#_bookmark108)) | 123.08 | 277 | 1 AN |
| 111.39 | Token Authorization Request (TAR) Indicator ([Possible Values](#_bookmark110)) |  | 278 | 1 N |
| 111.40 | Token Notification Type ([Possible Values](#_bookmark111)) |  | 279-282 | 4 N |
| 111.41 | Token OTP Code (spaced padded on left) | 43.1 | 283-590 | 8 AN |
| 111.42 | Token OTP Expiry Date Time (Format: YYMMDDhhmm) | NA | 291-300 | 10 N |
| 111.43 | Replacement PAN | 127.41  tag 01 | 301-319 | 19 AN |
| 111.44 | Replacement PAN Expiration Date (Format: YYMM) | 127.41  tag 02 | 320-323 | 4 N |
| 111.45 | Partial Authorization Indicator | 60.10 | 324 | 1N |
| 111.46 | Chargeback Flag |  | 325 | 1AN |
| 111.47\* | Cardholder Verification Method Identifier |  | 326 | 1 N |
| 111.48\* | Cardholder Verification Method Value |  | 327-390 | 64 AN |
| 111.49 | Bound Device Index | 123.80 | 391-392 | 2 AN |
| 111.50\* | Token User Identifier | 123.81 | 393-403 | 11AN |
| 111.51\* | Token User Application Type | 123.82 | 404-405 | 2 AN |
| 111.52 | 3D Secure Indicator | 126.20 | 406 | 1 ANS |
| 111.53 | CAVV Result Code | 44.13 | 407 | 1 ANS |
| 111.54 | E-Commerce and payment indicator | 60.8 | 408-409 | 2 N |
| 111.55 | E-Commerce Security Indicator | 63.6 | 410 | 1 ANS |
| 111.56 | CAVV Data | 126.9 | 411-451 | 40 AN |
| 111.57 | Wallet Type |  | 451-455 | 5 AN |

**111.47 – Cardholder Verification Method Identifier**

The cardholder verification method identifier represents the verification method selected by the cardholder during the token provision process when a Yellow path is opted and OTP (One-Time Password) is selected as a step-up authentication method.

The possible values can be:

* Cell Phone
* Email

##### 111.48 – Cardholder Verification Method Value

This field will contain the content of the selected cardholder verification method. For example, if value 1 i.e., Cell Phone is selected in Field 111.47, then this field will contain the cardholder’s phone number on which on which OTP has to be sent. Similarly, if value 2 i.e., Email is selected in Field 111.47, then will contain cardholder’s email address on which email has to be sent.

##### 111.49- Bound Device Index

This field will contain the index number from the Visa database where the device ID is stored. The value will be a one-byte hexadecimal value in the range of **01**–**63** (Decimal 1–99).

##### 111.51- Token User Application Type

This field will contain the application type of the token user. This entity can be the merchant, a marketplace, or a check out host. The application type is one of the following valid values:

* **00** (Unknown)
* **01** (Web)
* **02** (Mobile web)
* **03** (Mobile application)
* **04** (Marketplace application)
* **05** (Voice application)
* **06** (Biometric application)
* **07**–**FF** (Reserved)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-111 when DE-63.7 = ‘MASTERCARD’** | | | | |
| **Sub Field**  **No.** | **Field Name** | **MC Bit No.** | **Position** | **Format**  **(ASCII)** |
| 111.1 | Account category | 48.38 | 1 | 1 AN |
| 111.2 | Electronic commerce  merchant/cardholder certificate serial number | 48.40 | 2-41 | 40 AN |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 111.3 | Electronic commerce certificate qualifying  information | 48.41 | 42-136 | 95 ANS |
| 111.4\* | Electronic commerce indicators | 48.42 | 137-143 | 7 N |
| 111.5 | Universal cardholder authentication field  (UCAF) | 48.43 | 144-175 | 32 ANS |
| 111.6 | Mobile Program Indicators | 48.48 | 176-248 | 73ANS |
| 111.7 | Original Switch Serial Number | 48.59 | 249-257 | 9 N |
| 111.8 | POS Data, extended condition codes\* | 48.61 | 258-262 | 5 N |
| 111.9 | Trace ID | 48.63 | 263-277 | 15 ANS |
| 111.10 | Transit program | 48.64 | 278-281 | 4 N |
| 111.11 | Implied decimal | 48.70 | 282-286 | 5 N |
| 111.12 | Issuer chip authentication | 48.72 | 287-302 | 16 AN |
| 111.13 | MasterCard electronic transaction  indicator | 48.76 | 303 | 1 A |
| 111.14 | Payment transaction type indicator | 48.77 | 304-306 | 3 AN |
| 111.15 | Chip CVR/TVR bit error results listing | 48.79 | 307-356 | 50 AN |
| 111.16 | PIN Service code | 48.80 | 357-358 | 2 A |
| 111.17 | Maestro PIN-less program indicator | 48.81 | 359 | 1 AN |
| 111.18\* | Address verification service request | 48.82 | 360-361 | 2 N |
| 111.19\* | Address verification service response | 48.83 | 362 | 1 N |
| 111.20 | Merchant advice code | 48.84 | 363-364 | 2 AN |
| 111.21 | Card validation code result | 48.87 | 365 | 1 AN |
| 111.22 | Magnetic stripe compliance status  indicator | 48.88 | 366 | 1 AN |
| 111.23 | Magnetic stripe compliance error indicator | 48.89 | 367 | 1 AN |
| 111.24 | CVC 2 Value | 48.92 | 368-370 | 3 N |
| 111.25 | Program participation indicator | 48.94 | 371-398 | 28 ANS |
| 111.26 | MasterCard promotion code | 48.95 | 399-404 | 6 AN |
| 111.27 | MasterCard corporate fleet card id/driver  number | 48.98 | 405-410 | 6 N |
| 111.28 | MasterCard corporate fleet card vehicle  number | 48.99 | 411-425 | 15 AN |
| 111.29 | Stand In Trans Indicator ([Possible Values](#_bookmark106)) |  | 426 | 1 N |
| 111.30 | Transaction Unique Identifier |  | 427-432 | 6 AN |
| 111.31 | Token Device Id | NA | 433-496 | 64 AN |
| 111.32 | Token Device No | 124.191 | 497-511 | 15 N |
| 111.33 | Token Device Name | 120.92 | 512-531 | 20 AN |
| 111.34 | Token Device Type ([Possible Values](#_bookmark109)) | NA | 532-533 | 2 AN |
| 111.35 | Token ID | 120.1 Or  120.24 Or  48.33 tag 02 | 534-552 | 19 AN |
| 111.36 | Token Type ([Possible Values](#_bookmark107)) | 120.253 Or  124.195 | 553-554 | 2 AN |
| 111.37 | Token Status ([Possible Values](#_bookmark108)) |  | 555 | 1 AN |
| 111.38 | Token Authorization Request (TAR) |  | 556 | 1 N |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Indicator ([Possible Values](#_bookmark110)) |  |  |  |
| 111.39 | Token Notification Type ([Possible Values](#_bookmark111)) |  | 557-560 | 4 N |
| 111.40 | Token OTP Code (spaced padded on left) | 120.38 | 561-568 | 8 AN |
| 111.41 | Token OTP Expiry Date Time (Format:  YYMMDDhhmm) | 120.46 | 569-578 | 10 N |
| 111.42 | Replacement PAN | NA | 579-597 | 19 AN |
| 111.43 | Replacement PAN Expiration Date  (Format: YYMM) | NA | 598-601 | 4 N |
| 111.44\* | Customer’s Activation Code  DistributionMethod Preference | 120.6 | 602-766 | 165 ANS |
| 111.45 | Chargeback flag (For details, see  [Appendix-E](#_bookmark105)) |  | 767 | 1AN |
| 111.46 | On-behalf Service (OBS) (For details, see  [Appendix-E](#_bookmark105)) | 48.71 | 768-807 | 40 ANS |
| 111.47 | Fraud Scoring Data (For details, see  [Appendix-E](#_bookmark105)) | 48.75 | 808-839 | 32 AN |
| 111.48\* | Incremental Authorization Indicator |  | 840 | 1AN |
| 111.49 | Final Auth Indicator | 48.61 | 841 | 1 N |
| 111.50 | Issuer Transaction Transformation Flag |  | 842 | 1 N |
| 111.51 | Network Billing Amount | 6 | 843-854 | 12 N |
| 111.52 | Network Billing Exchange Rate | 10 | 855-862 | 8 N |
| 111.53 | On Demand Acquirer ID |  | 863-866 | 4 N |
| 111.54 | File Update Code | 91 | 867 | 1 AN |
| 111.55 | File Name | 101 | 868-884 | 17 ANS |
| 111.56 | Primary Account Card Sequence Number | 120 | 885-887 | 3 ANS |

##### POS Data, extended condition codes:

Sub field – 1: Partial Approval Terminal Support Indicator

Sub field – 2: Purchase Amount Only Terminal Support Indicator Sub field – 3: Real time Substantiation Indicator

Sub field – 4: Reserved for Future Use Sub field – 5: Final Authorization Indicators

##### \* Electronic Commerce Indicators

Contains the electronic commerce indicators representing the security level and cardholder authentication associated with the transaction. This subfield must be present in all Authorization Request/0100 messages

for electronic commerce transactions. This subfield consists of further three sub-fields SF1, SF2 and SF3. SF1 and SF2 have length 3-N with 3 different positions & SF3 has length 1-N. Each position has possible values.

##### Possible Values of Position 1 of SF1:

0 = Reserved for existing Mastercard Europe/Visa definitions

1 = Reserved for future use

2 = Chanel

3-8 = Reserved for future use 9 = None (no security protocol)

##### Possible Values of Position 2 of SF1:

0 = Reserved for future use

1 = Cardholder certificate not used

2 = Processed through Masterpass

4 = Digital Secure Remote Payment Transaction 5–9 = Reserved for future use

##### Possible Values of Position 3 of SF1:

0 = UCAF data collection is not supported by the merchant

1 = UCAF data collection is supported by the merchant, and UCAF data should be available

2 = Issuer Authenticated

3 = UCAF data collection is supported by the merchant.

4 = Reserved for future use

5 = Issuer risk based decisioning

6 = Merchant Risk Based Decisioning

7 = Partial shipment or recurring payment. Liability will depend on the original UCAF values provided and matching with the initial transaction.

Subelement 111.4, subfields 2 and 3 are only present in the Financial Transaction Request, Response/0210 message provided by Mastercard to the acquirer if an Security Level Indicator (SLI) downgrade occurred.

Issuers will not see subfields 2 or 3 in the Financial Transaction Request/0200 messages.

##### 111.18\* (Address Verification Service Request)

Indicates that verification of the cardholder billing address is requested in the authorization message and this field must be present in authorization request message whenever cardholder address verification is required.

##### Possible Values:

52 = AVS and Authorization Request/0100

##### 111.19\* (Address Verification Service Response)

Contains the AVS verification response code in the Authorization Request Response message.

##### Possible Values:

**A =** Address matches, postal code does not.

**B =** Visa only. Street address match. Postal code not verified because of incompatible formats. (Acquirer sent both street address and postal code.)

**C =** Visa only. Street address and postal code not verified because of incompatible formats. (Acquirer sent both street address and postal code.)

**D =** Visa only. Street address and postal code match.

**F =** Visa only. Street address and postal code match. Applies to U.K. only.

**G =** Visa only. Non-AVS participant outside the U.S.; address not verified for international transaction.

**I =** Visa only. Address information not verified for international transaction.

**M =** Visa only. Street addresses and postal code match.

**N =** Neither address nor postal code matches.

**P =** Visa only. Postal codes match. Street address not verified because of incompatible formats. (Acquirer sent both street address and postal code.)

**R =** Retry, system unable to process.

**S =** AVS currently not supported.

**U =** No data from issuer/Authorization Platform

**W =** For U.S. addresses, nine-digit postal code matches, address does not; for address outside the U.S., postal code matches, address does not.

**X =** For U.S. addresses, nine-digit postal code and address matches; for addresses outside the U.S., postal code and address match.

**Y =** For U.S. addresses, five-digit postal code and address matches.

**Z =** For U.S. addresses, five-digit postal code matches, address does not.

##### 111.44\*

There will be only one method contained within this field. This field will only be present if the cardholder provides a choice.

Activation Code Distribution Method Type (n-1)

Possible Values are:

**1** = Masked mobile phone number

**2** = Masked email address

**3** = Automated call center phone number

**4** = Call center phone number

**5** = Website

**6** = Mobile application

**7** = Masked voice call phone number

Activation Code Distribution Method Value (ans…164) See below examples:

###### “1(###) ### 4567”

1 = Masked mobile phone number

The “1” will be followed by the masked mobile phone number. “**2a\*\*\***[**d@anymail.com**](mailto:d@anymail.com)**”**

2 = Masked email address

The “2” will be followed by the consumer’s masked email address (the issuer will mask according to their own format).

###### “3(555) 123 4567”

3 = Automated call center phone number

The “3” will be followed by the phone number. This phone number is not masked. “4(555) 123 8901”

4 = Call center phone number

The “4” will be followed by the phone number. This phone number is not masked. “[5http://www.anybank.com](http://www.anybank.com/)”

5 = Website

The “5” will be followed by the issuer’s website URL. “6com.anybank.mobileapp”

6 = Mobile app

The “6” will be followed by the issuer’s mobile app information, the content of which depends upon the mobile device operating system.

“7(###) ### 2345”

7 = Masked voice call phone number

The “7” will be followed by the masked voice call phone number.

##### 111.48\*: Incremental authorization Indicator

Possible Values: Y/N

[will be received in Authorization messages (x1xx) only, If Incremental Auth then → ‘Y’, else → ‘N’]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-111 when DE-63.7 = ‘EFUNDS’** | | | | |
| **Sub Field No.** | **Field Name** | **FIS Bit**  **No.** | **Position** | **Format**  **(ASCII)** |
| 111.1 | Partial Authorization Indicator | 63.40 | 1 | 1 AN |
| 111.2 | Stand In Trans Indicator ([Possible Values](#_bookmark106)) |  | 2 | 1 N |
| 111.3 | Transaction Unique Identifier |  | 3-8 | 6 AN |
| 111.4 | Token Device Id | NA | 9-72 | 64 AN |
| 111.5 | Token Device No | NA | 73-87 | 15 N |
| 111.6 | Token Device Name | NA | 88-107 | 20 AN |
| 111.7 | Token Device Type ([Possible Values](#_bookmark109)) |  | 108-109 | 2 AN |
| 111.8 | Token ID | NA | 110-128 | 19 AN |
| 111.9 | Token Type ([Possible Values](#_bookmark107)) |  | 129-130 | 2 AN |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 111.10 | Token Status ([Possible Values](#_bookmark108)) |  | 131 | 1 AN |
| TBD | Token Authorization Request (TAR) Indicator  ([Possible Values](#_bookmark110)) |  | TBD | 1 N |
| TBD | Token Notification Type ([Possible Values](#_bookmark111)) |  | TBD | 4 N |
| TBD | Token OTP Code (spaced padded on left) | NA | TBD | 8 AN |
| TBD | Token OTP Expiry Date Time (Format:  YYMMDDhhmm) | NA | TBD | 10 N |
| TBD | Replacement PAN | NA | TBD | 19 AN |
| TBD | Replacement PAN Expiration Date (Format:  YYMM) | NA | TBD | 4 N |
| 111.11 | Chargeback flag |  | 132 | 1AN |
| 111.12 | Incremental Authorization Flag | 60 | 133 | 1AN |
| 111.13 | Multi-Clearing Sequence | 124 | 134 | 2N |
| 111.14 | Multi-Clearing Count | 124 | 136 | 2N |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-111 when DE-63.7 = ‘STAR’** | | | | |
| **Sub Field No.** | **Field Name** | **STAR**  **Bit No.** | **Position** | **Format (ASCII)** |
| 111.1 | Partial Authorization/Approval Indicator | 63.7 | 1 | 1 AN |
| 111.2 | Stand In Trans Indicator |  | 2 | 1 N |
| 111.3 | Transaction Unique Identifier |  | 3-8 | 6 AN |
| 111.4 | Chargeback flag |  | 9 | 1 AN |
| 111.5\* | Incremental Authorization | 110.2 | 10 | 1 AN |
| 111.6\* | Multiple Transaction Sequence | 110.6 | 11-13 | 3 N |
| 111.7\* | Multiple Transaction Count | 110.7 | 14-16 | 3 N |
| 111.8 | Pseduo-Terminal Id | 63.1 | 17-22 | 6 AN |
| 111.9 | Interchange Program Identifier | 104.2 | 23-25 | 3 N |
| 111.10 | STAR® Verification Value | 104.3 | 26-35 | 10 AN |
| 111.11 | Market Indicator | 104.4 | 36 | 1 AN |
| 111.12 | Merchant Aggregation Indicator | 104.5 | 37 | 1 AN |
| 111.13 | Transaction Aggregation Indicator | 104.6 | 38 | 1 AN |
| 111.14 | Money/Funds Transfer/Prepaid Load Definition | 104.7 | 39 | 1 AN |
| 111.15\* | Transaction Description | 104.8 | 40-41 | 2 AN |
| 111.16 | Purchase Identifier | 110.3 | 42-67 | 26 AN |
| 111.17\* | STAR® Predictive Fraud Score | 110  Tag SF | 68-70 | 3 N |
| 111.18\* | STAR® Predictive Fraud Reason Code | 110  Tag SF | 71-72 | 2 AN |

##### \*: Incremental authorization Indicator

Possible Values: Y/N

[will be received in Authorization messages (x1xx) only, If Incremental Auth then → ‘Y’, else → ‘N’]

##### \*: Multiple Transaction Sequence

If there are multiple completions, the number of completion that this record represents.

##### \*: Multiple Transaction Count

Indicates the total number of completions expected in a multi-clearing scenario.

##### 111.15\*: Transaction Description

Possible values and their corresponding detail for this field:

|  |  |
| --- | --- |
| **AA** | Account to Account |
| **BB** | Business to Business |
| **BP** | Business to Person |
| **OG** | Online gambling (winnings) – for future  use |
| **PP** | Person to Person |

##### \*: Predictive Fraud Score

Represents a score ranging from **000 to 999**. The higher the value, more likely it is to be a fraudulent transaction.

##### \*: Predictive Fraud Reason Code

Reflects the reason code that supports the STAR predictive fraud score value.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-111 when DE-63.7 = ‘UNIONPAY’** | | | | |
| **Sub Field No.** | **Field Name** | **UnionPay Bit No.** | **Position** | **Format (ASCII)** |
| 111.1 | Minor Unit of Transaction Currency | 60.3.3 | 1-3 | 3 AN |
| 111.2 | Partial Authorization Indicator | 60.3.4 | 4 | 1 AN |
| 111.3 | Transaction Medium | 60.3.6 | 5 | 1 AN |
| 111.4 | IC card application type | 60.3.7 | 6 | 1 AN |
| 111.5 | Account Attribute | 60.3.8 | 7-8 | 2 AN |
| 111.6 | Card Level | 60.3.9 | 9 | 1 AN |
| 111.7 | Card Product | 60.3.10 | 10-11 | 2 AN |
| 111.8 | Transaction Cancellation Indicator |  | 12 | 1 AN |
| 111.9 | Original MTI of Cancellation Transaction |  | 13-16 | 4 AN |
| 111.10 | OTP Code (spaced padded on left) |  | 17-26 | 10 AN |
| 111.11 | Token OTP Expiry Date Time (Format: |  | 27-36 | 10 AN |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | YYMMDDhhmm) |  |  |  |
| 111.12 | OTP Business Type |  | 37 | 1 AN |
| 111.13 | ID Number | 61.1 | 38-59 | 22 AN |
| 111.14 | CVN Rsult Code | 61.2 | 60 | 1 AN |
| 111.15 | PVV Result Code | 61.3 | 61 | 1 AN |
| 111.16 | CVN2 Result Code | 61.4.3 | 62 | 1 AN |
| 111.17 | ARQC Authentication Result | 61.5 | 63 | 1 AN |
| 111.18 | Card-Holder Mobile Number | 61.6.AM.9.2 | 64-83 | 20 AN |
| 111.19 | OTP Generate and Send Indicator |  | 84 | 1 AN |

##### \* (Transaction Cancellation Indicator)

This field will contain 1 char transaction cancellation indicators with possible values:

* + - 0 → Transaction is a not cancellation transaction.
    - 1 → Transaction is a cancellation advice of an earlier approved transaction.
    - 2 → Transaction is a reversal of cancellation advice.

This indicator is only applicable for reversal 0220 and 0420 transactions. It will indicate if a transaction is cancellation or cancellation reversal transaction.

Union Pay has a unique functionality where they can cancel any previously sent ISO pre-authorization or financial message e.g. 01XX and 02XX.

For authorization host i2c will send cancellation/cancellation reversal transactions with MTI 0220/0420 and 20 transaction type along with flag in DE- 111.8 transaction cancellation indicator and DE 111.9 Original MTI of Cancellation Transaction.

If a cancellation of 01xx transaction is received to authorization host than they should cancel pre- authorization and release funds, and for cancellations of 02xx transactions they should credit their respective systems.

If a reversal of cancellation of 01xx transaction is received to authorization host than they should reacquire funds for said amount, and for reversal of cancellation of 02xx transactions they should reverse earlier credited 0220 transactions.

##### 111.3\* (Transaction Medium)

This field will contain 1 char transaction medium indicators with possible values:

* 0 → Unknown
* 1 → Magnetic stripe card transaction
* 2 → Chip card transaction via chip
* 3 → Magstripe transaction of chip and magstripe hybrid card
* 4 → Virtual card transaction
* 5 → QRC-based transaction
* 6 → Biological traits transaction
* 7 → Card-not-present transaction

**NOTE**: This field is used for identification on QR Code based transactions. For QR code transaction transaction medium must be 5 and Pan Entry mode must be in 03,04,93,94.

##### OTP Generation Indicator

This field indicates whether to generate and send generated OTP to card holder. Possible values:

* + - 0 → Do not generate or match OTP
    - 1 → Generate OTP
    - 2 → Match OTP

##### 111.12 OTP Business Type

This field determine business type of OTP is used in this transaction. Below are given values:

* 0 → No OTP present
* 1 → E-Commerce OTP
* 2 → QR Transaction OTP
* 3 → Digital Wallet Tokenization OTP (Reversed for Future)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-111 when DE-63.7 = ‘DISCOVER’** | | | | |
| **Sub Field No.** | **Field Name** | **Discover Bit No.** | **Position** | **Format (ASCII)** |
| 111.1 | Transaction Status Indicator | 61.7 | 1 | 1 ANS |
| 111.2 | Transaction Identifier | 48.11 | 2-16 | 15 ANS |
| 111.3 | Chargeback flag |  | 17 | 1 AN |
| 111.4 | Stand In Trans Indicator |  | 18 | 1 N |
| 111.5 | Transaction Unique Identifier |  | 19-24 | 6 N |
| 111.6 | Partial Authorization/Approval Indicator | 61.2 | 25 | 1 N |
| 111.7 | Incremental Authorization | 61.7 | 26 | 1 N |

##### Partial Authorization/Approval Indicator

|  |  |
| --- | --- |
| **Position 2: Partial Approval Indicator** | |
| **Code** | **Definition** |
| 0 | Partial Approval Not Supported |
| 1 | Partial Approval Supported: Merchandise can be partially approved  Cash Over can be partially approved |
| 2 | Partial Approval Supported: Merchandise can be partially approved  Cash Over must be fully approved or declined |
| 3 | Partial Approval Supported:  Merchandise must be fully approved or declined Cash Over can be partially approved |
| 4 | Partial Approval Supported:  Merchandise must be fully approved or declined Cash Over must be fully approved or declined |

**Incremental Authorization:**

This field indicates whether the auth is incremental one or not. If value in “I” then value 1 will be send to Authhost otherwise 0.

|  |  |
| --- | --- |
| **Position 7: POS Transaction Status Indicator** | |
| **Code** | **Definition** |
| 0 | Normal Request (original presentment) |
| 4 | Pre-authorized Request |
| A | Re-authorize for Full Amount |
| D | Delayed Card Sale |
| E | Resubmission of Card Sale |
| G | Transit Aggregated Transaction |
| I | Incremental Authorization |

|  |  |
| --- | --- |
| N | No-Show Charge |
| P | Partial Shipment |
| R | Recurring Payment |
| S | Installment Payment |
| U | Unscheduled Payment |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-111 when DE-63.7 = ‘FISERV’** | | | | |
| **Sub Field No.** | **Field Name** | **Fiserv Bit No.** | **Position** | **Format (ASCII)** |
| 111.1 | Stand-In Transaction Indicator | N/A | 1 | 1 ANS |
| 111.2 | Transaction Unique Identifier | N/A | 2-7 | 6 ANS |

#### Data Element 125 - [SUPPORTING INFORMATION](#_bookmark71)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-125 when DE-63.7 = ‘VISA’** | | | | |
| **Tag** | **Length** | **Value** | **Format** | **Content of Sub-Element** |
| ***Dataset ID: 68, Token Data*** | | | | |
| 1F31 | 4 | Elapsed Time To Live | N | This tag contains the elapsed time in hours since the current limited-use key (LUK) is provisioned on the device. |
| 1F32 | 3 | Count of Number of Transactions | N | This tag contains the cumulative count of transactions for the current limited-use key (LUK). |
| 1F33 | 7 | Cumulative Transaction Amount | N | This tag contains the cumulative total of transaction amounts in USD for the current limited-use key (LUK). |
| 01 | 13–19 | Token | AN | Ignore this tag. It is already included in DE 111. |
| 02 | 2 | Token Assurance Level | AN | Reserved for future use. This field contains spaces. |
| 03 | 11 | Token Requestor ID | N | This tag contains the token requestor ID. |
| 04 | Up to 19 | Primary Account Number, Account Range | ANS | Ignore this tag. It is already included in DE 02. |
| 05 | Up to 32 | Token Reference ID | AN | This tag contains the token reference ID. |
| 06 | 4 | Token Expiration | N | This tag will contain the token expiration date. The |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Date |  | date is in yymm format, where yy = year (00–99) and mm = month (01–12). |
| 07 | 2 | Token Type | AN | Ignore this tag. It is already included in DE 111. |
| 08 | 1 | Token Status | AN | Ignore this tag. It is already included in DE 111. |
| 0A | 1 | Last Updated By | AN | This tag is present in the response when the token is located. |
| 0B | 32 | PAN Reference ID | ANS | This tag contains a unique reference ID generated by Visa for the card account number.  This tag is required in 0302 Token File Inquiry Messages if Field 2—Primary Account Number is not present. |
| 1A | 6–8 | Activation Code | AN | Ignore this tag. It is already included in DE 111. |
| 1B | 12 | Activation Code Expiry Date/Time | N, BCD | Ignore this tag. It is already included in DE 111. |
| 1C | 2 | Activation Code Verification Attempts | N, BCD | This tag contains the number of attempts to verify the current activation code. |
| 1D | 2 | Number of Activation Codes Issued | N, BCD | This tag contains the total number of token activation codes issued. |
| 10 | 2 | Visa Token Score | N | This tag contains the degree of risk associated with the token. The valid values are from 01–99. |
| 11 | 2 | Visa Token Decisioning | AN | This tag contains the results of the token provisioning decision. The valid values are: 00 = Provision and activate.  05 = Do not provision.  85 = Provision inactive state  – requires further consumer authentication before activation. |
| 12 | 2 | Number of Active Tokens | N | This tag contains the number of device tokens currently active for this PAN. |
| 13 | 2 | Number of Inactive Tokens | N | This tag contains the number of device tokens currently inactive (device tokens that have not been activated) for this PAN. |
| 14 | 2 | Number of Suspended Tokens | N | This tag contains the number of device tokens that were activated but are suspended for payments for this PAN. |
| 1E | 6 | Token Activation Date/Time | TLV | Token activation date and time in yymmddhhmmss format expressed in GMT. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 80 | 1 | Bound Device Index | TLV | Index number from the Visa database where the device ID is stored. Value can be 01-63 (in hexadecimal format). (Decimal 1-99). |
| 81 | 1-11 | Token User Identifier | TLV | Contains unique value that identifies the token user. Token user is an entity that initiates a payment request.  Applicable for e-commerce transactions (device and Card-on-File token types). |
| 82 | 1 | Token User Application Type | TLV | Application type of token user. Entities can be a merchant, a marketplace, or a check out host. Application types:  00 = Unknown  01 = Web  02 = Mobile web  03 = Mobile application  04 = Marketplace application  05 = Voice application  06 = Biometric application 07-FF = Reserved |
| 83 | 1 | Token Authentication Factor A | TLV | Authentication factor used by token requestors and merchants to authenticate cardholder at time of transaction.  Applicable for e-commerce transactions (device and Card-on-File token types).  Authentication Values:  00 = No authentication method acquired  01 = Username/password  02 = Passcode or password  Consumer Device Cardholder Verifi cation Method (CDCVM):  10 = Passcode  11 = Password  12 = Pattern  13 = Biometric fingerprint  14 = Biometric facial recognition  15 = Biometric iris recognition  16 = Biometric voice recognition  17 = Behavioral biometric One Time Passcode (OTP):  18 = Device unlocked (CDCVM unknown)  30 = Short message system (SMS)  31 = Email  32 = Hardware token without user verification |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | 33 = Hardware token with user verifi cation  34 = Soft token  35 = Any other method  40 = Knowledge based authentication  41 = Out of band (OOB) authentication  42 = Local authentication Fast Identity Online (FIDO):  50 = Possession only. No user verifi cation.  51 = With user verification (biometric)  52 = With user verification (passcode/password) 60 = SE based token: cryptogram generated from a SE device for a davice-bound token was provided, establishes possession factor.  61 = Device bound token: device bound token (token reference) was provided by token requestor along with proof of device used for binding token, establishes possession factor.  In Europe, token user identifier may be used to support dynamic linking requirements of PSD2/RTS. |
| 84 | 1 | Token Authentication Factor B | TLV | Authentication factor used by token requestors and merchants to authenticate cardholder at time of transaction.  Applicable for e-commerce transactions (device and Card-on-File token types).  Authentication Values:  00 = No authentication method acquired  01 = Username/password  02 = Passcode or password  Consumer Device Cardholder Verifi cation Method (CDCVM):  10 = Passcode  11 = Password  12 = Pattern  13 = Biometric fingerprint  14 = Biometric facial recognition  15 = Biometric iris recognition  16 = Biometric voice recognition  17 = Behavioral biometric One Time Passcode (OTP):  18 = Device unlocked (CDCVM unknown)  30 = Short message system (SMS)  31 = Email  32 = Hardware token without user verification  33 = Hardware token with user verifi cation  34 = Soft token |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | 35 = Any other method  40 = Knowledge based authentication  41 = Out of band (OOB) authentication  42 = Local authentication Fast Identity Online (FIDO):  50 = Possession only. No user verifi cation.  51 = With user verification (biometric)  52 = With user verification (passcode/password) 60 = SE based token: cryptogram generated from a SE device for a davice-bound token was provided, establishes possession factor.  61 = Device bound token: device bound token (token reference) was provided by token requestor along with proof of device used for binding token, establishes possession factor.  In Europe, token user identifier may be used to support dynamic linking requirements of PSD2/RTS. |
| 85 | 3 | Token Authentication Amount | TLV | Payment amount made visible by the token requestor to consumer at time of purchase. Applicable for e-commerce transactions (device and Card-on-File token types).  In Europe, token user identifier may be used to support dynamic linking requirements of PSD2/RTS. |
| 86 | 6 | Token requestor – token service provider ID | TLV | Unique value that identifies the service provider for a token requestor. A token service provider is the integration partner for token requestors for provisioning and cryptogram requests.  Applicable for e-commerce and Card-on-File transactions. |
| ***Dataset ID: 01, Token Device*** | | |  |  |
| 01 | 2 | Device Type | TLV | Ignore this tag. It is already included in DE 111. |
| 02 | 3 | Device Language Code | TLV | This tag contains a three-character language code that conforms with ISO 639 standards.  An example would be eng (English). |
| 03 | Up to 48 | Device ID | TLV | Ignore this tag. It is already included in DE 111. |
| 04 | Up to 15 | Device Number | TLV | Ignore this tag. It is already included in DE 111. |
| 05 | 16 | Device Name | TLV | Ignore this tag. It is already included in DE 111. |
| 06 | Up to 25 | Device Location | TLV | This tag contains the obfuscated geographic location of the device or the coarse location of the device.  Location is latitude/longitude with up to 4 digits of precision; for instance  +37.7799/-122.4290. Precision is rounded off to a |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 07 |  |  |  | less granular level e.g. +37/-122 or +37.78/-122.43. |  |
| 15 | IP Address | TLV | This tag contains the IP address of the device at the time of the provisioning request.  The value will be in the format: 255.255.255.255. Each octet (255)  may be 1–3 digits in length. |  |
| ***Dataset ID: 02, Wallet Provider*** | | | | | |
| 03 | 1 | Wallet Provider Risk Assessment | TLV | This tag contains one of the following valid values:  0 = Unconditionally approved.  1 = Conditionally approved with further verification.  2 = Not approved. | |
| 04 | 10 | Wallet Provider Risk Assessment Version | TLV | This tag contains the Wallet Provider Risk Assessment Version. | |
| 05 | 2 | Wallet Provider Device Score | TLV | This tag contains the value of 1–5, with 5 being the most trusted. | |
| 06 | 2 | Wallet Provider Account Score | TLV | This tag contains the value of 1–5, with 5 being the most trusted. | |
| 07 | 30 | Wallet Provider Reason Codes | TLV | This tag contains up to 15 reason codes of 2 bytes each. The valid values are:  **01** = Cardholders’ wallet account is too new relative to launch.  **02** = Cardholders’ wallet account is too new relative to provisioning request.  **03** = Cardholders’ wallet account/card pair is newer than date threshold.  **04** = Changes made to account data within the date threshold.  **05** = Suspicious transactions linked to this account. **06** = Account has not had activity in the last year. **07** = Suspended cards in the secure element.  **08** = Device was put in lost mode in the last 7 days for longer than the duration threshold.  **09** = The number of provisioning attempts on this device in 24 hours exceeds threshold.  **0A** = There have been more than the threshold number of different cards attempted at provisioning to this phone in 24 hours.  **0B** = The card provisioning request contains a distinct name in excess of the permitted threshold. **0C** = The device score is less than 3.  **0D** = The account score is less than 4. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | **0E** = Device provisioning location outside of the cardholder’s wallet account home country.  **0G** = Suspect fraud. |
| 08 | 2 | PAN Source | TLV | This tag contains one of the following valid values:  **01** = Key-entered.  **02** = On file.  **03** = Mobile banking app. |
| 09 | 32 | Wallet Account ID | TLV | This tag contains the Wallet Account ID. |
| 0A | Up to 32 | Wallet Account E- mail Address | TLV | This tag contains the Wallet Account E-mail Address. |
| ***Dataset ID: 40, Terms and Conditions*** | | | | |
| 01 | 64 | Terms and Conditions Verification | AN | This field contains the terms and conditions data when field 63.3 contains message reason code 3700. |
| 02 | 32 | Issuer Terms and Conditions Date/Time | AN | This field contains the date and time. |
| ***Dataset ID: 58, Original Token Data*** | | | | |
| 80 | 13-19 | Original Token | AN | This field contains the original token number used for provisioning of a new token. |
| 81 | 2 | Original Token Assurance Level | AN | This field contains the Assurance Level of original token. |
| 82 | 11 | Original Token Requestor ID | N | This field contains the original token Requestor ID. |
| 83 | Upto 32 | Original Token Ref ID | AN | This field contains the original token ref ID. |
| 84 | 2 | Original Token Type | AN | This field will contain the token type of the source token used for provisioning a new token.  Valid values are:   * 01 (ECOM/COF (e-commerce/card on file)) * 02 (SE (secure element)) * 03 (CBP (cloud-based payment)) * 05 (E-commerce enabler) |
| 85 | 2 | Original Device Type | AN | This field will contain the device type of the source token used for provisioning a new token.  Valid values are:   * 00 (Unknown) * 01 (Mobile phone) * 02 (Tablet) * 03 (Watch) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | * 04 (Mobile phone or tablet) * 05 (Personal computer) * 06 (Household device) * 07 (Wearable device) * 08 (Automobile device) |
| 86 | Upto 48 | Original Device ID | ANS | This field will contain the device ID of the source token used for provisioning a new token. |
| 01 | 3 | PAN Issued Date | TLV | This tag contains the PAN Issued Date. |
| 02 | 3 | PAN Activation Date | TLV | This tag contains the date of activation of the card. |
| ***Dataset ID: 67, Token Verification Result Code*** | | | | |
| 08 | 1 | Token Verification Result Code | TLV | * 1 = TAVV cryptogram failed validation * 2 = TAVV cryptogram passed validation * 3 = DTVV or Visa-defined format cryptogram passed validation * 4 = DTVV or Visa-defined format cryptogram passed validation   The TAVV-only cryptogram option is applicable for token transactions without 3DS data |
| **Dataset ID: 41, Replacement PAN Data** | | | | |
| 01 | 13-19 | Replacement PAN | TLV | This field is required when the PAN contained in Field 2—Primary Account Number is being replaced with a new PAN. |
| 02 | 4 | Replacement PAN Expiration Date | TLV | This field contains the expiration date of the new PAN in tag 01 or updatedexpiration date of the  existing PAN. Format = yymm. |
| **Dataset ID: 56, Device Parameter** | | | | |
| 01 | 24 | Device IMEI | TLV | This tag will contain the hardware ID of the device. NOTE  This field will be included in the 0600 Token notification online request message when  Field 63.3—Message Reason Code contains the  value of 3700 (Token create). |
| 02 | 1 | OS ID | TLV | This tag contains the ID of Operating System during Provisioning. |
| 03 | 1 | Provisioning attempts on the device | TLV | This tag will contain the number of provisioning attempts on the device within the last 24 hours. |
| 04 | 1 | Account-To-Device | TLV | This tag will contain the number of days the device |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Bounding Age |  | was used by this account. |
| 05 | 2 | Device Country | TLV | This tag will contain the two-character alpha ISO country code of the device at the time of provisioning. |
| 06 | 1 | Token Protection Method | TLV | This tag will describe how the tokens are protected on the device. Valid values are:   * 1 (Software) * 2 (Transaction execution environment (TEE)) * 3 (Secure element (SE)) * 4 (Cloud) |
| 07 | 1 | Presentation Type | TLV | This tag will contain the token presentment mode. Valid values are:   * 1 (Near field communication (NFC)—Host card emulation (HCE)—or secure element (SE)) * 2 (Magnetic secure transmission) * 3 (QR–Consumer device) * 4 (QR–Consumer cloud) |
| 08 | 24 | Device Serial Number | TLV | This tag will contain the serial number of the mobile device. |
| 09 | 1 | Location Source | TLV | This tag will contain the source used to identify the consumer’s location. Valid values are:   * 1 (WiFi) * 2 (Cellular) * 3 (GPS) * 4 (Other) |
| 0A | 5 | Device TimeZone | TLV | This tag will contain the device time zone. |
| 0B | 1 | Device TimeZone Setting | TLV | This tag will indicate how the time zone setting was obtained. Valid values are:   * 1 (Network set) * 2 (Consumer set) |
| 0C | 24 | Device Bluetooth Media Access Control | TLV | This tag will contain the MAC address for Bluetooth. |
| 0D | 1 | OS Type | TLV | This tag will indicate the operating system running on the device. Valid values are:   * 1 (Android) * 2 (iOS) * 3 (Windows) * 4 (Blackberry) * 5 (Tizen) * 6 (Other) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dataset ID: 57, Wallet Parameter** | | | | |
| 01 | 2 | Wallet Provider PAN Age | TLV | This tag will contain the number of days that the user’s PAN has been on file for the user. |
| 02 | 2 | User Account Age | TLV | This tag will contain the number of days since the user account for this user exists. |
| 03 | 2 | Wallet Account Age | TLV | This tag will contain the number of days since the  user created the wallet account or started using the account. |
| 04 | 2 | Days Since Last Activity | TLV | This tag will contain the number of days since the last activity on the account. |
| 05 | 2 | Number Of Transactions, Last 12 months | TLV | This tag will contain the number of transactions on this account within the last 12 months. |
| 06 | 2 | Days Since Last Account Change | TLV | This tag will contain the number of days since account settings were changed. |
| 07 | 1 | Suspended Cards in Account | TLV | This tag will contain the number of cards suspended on the account |
| 08 | 2 | Wallet Account Country | TLV | This tag will contain the two-character alpha ISO country code of the account holder |
| 09 | 1 | Number Of Active Tokens | TLV | This tag will contain the number of active tokens  on this account |
| 0A | 1 | Number Of Devices With Active Token | TLV | This tag will contain the number of devices for this user with the same token. |
| 0B | 1 | Number Of Active Tokens on All Devices | TLV | This tag will contain the number of active tokens for this user across all devices |
| 0C | 1 | Consumer Entry Mode | TLV | This tag will indicate how the card information was entered on the device. Valid values are:   * 1 (Key-entered) * 2 (Camera captured) * 3 (Unknown) |
| 80 | 2 | Wallet Account Email Address Age | TLV | Number of days email address exists (0000 - 9999). |
| 81 | 1 | Wallet Provider Phone Score | TLV | Value between 1 - 5, where 1 is least trusted and 5 is most trusted. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-125 when DE-63.7 = ‘MASTERCARD’** | | | | |
| **Sub Field No.** | **Field Name** | **MC Bit No.** | **Position** | **Format (ASCII)** |
| 125.1 | Token Expiration Date |  | 1-4 | 4 N |
| 125.2 | Token Service Provider Identification |  | 5-5 | 1 A |
| 125.3 | Token Assurance Level |  | 6-7 | 2 N |
| 125.4 | Token Requestor ID |  | 8-18 | 11 N |
| 125.5 | Contactless Usage |  | 19-19 | 1 N |
| 125.6\* | Card on File Electronic Commerce Usage |  | 20-20 | 1 N |
| 125.7 | Mobile/Digital Wallet Electronic Commerce Usage |  | 21-21 | 1 N |
| 125.8 | Correlation ID |  | 22-35 | 14 AN |
| 125.9 | Number of Active Tokens for the Primary Account Number |  | 36-37 | 2 ANS |
| 125.10 | Issuer Product Configuration ID |  | 38-47 | 10 ANS |
| 125.11 | Consumer Language |  | 48-49 | 2 A |
| 125.12 | Final Tokenization Decision |  | 50-50 | 1 ANS |
| 125.13 | Final Tokenization Decision Indicator |  | 51-51 | 1 ANS |
| 125.14 | T&C Identifier |  | 52-83 | 32 ANS |
| 125.15 | T&C Date and Time |  | 84-93 | 10 ANS |
| 125.16 | Number of Activation Attempts |  | 94-94 | 1 ANS |
| 125.17 | Token Unique Reference |  | 95-142 | 48 ANS |
| 125.18 | Primary Account Number Unique Reference |  | 143-190 | 48 ANS |
| 125.19 | Tokenization Event Indicator |  | 191-191 | 1 N |
| 125.20 | Tokenization Event Reason Code |  | 192-193 | 2 AN |
| 125.21 | Event Requestor |  | 194-194 | 1 ANS |
| 125.22 | Primary Account Number Source |  | 195-195 | 1 AN |
| 125.23 | Payment Application Instance |  | 196-243 | 48 ANS |
| 125.24 | Device Source IP Address |  | 244-255 | 12 ANS |
| 125.25 | Wallet Service Provider Account ID Hash |  | 256-319 | 64 ANS |
| 125.26 | Cardholder Name |  | 320-346 | 27 ANS |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 125.27 | Wallet Service Provider Tokenization Recommendation |  | 347-347 | 1 AN |
| 125.28 | Wallet Service Provider Tokenization Recommendation Standard Version |  | 348-349 | 2 AN |
| 125.29 | Wallet Service Provider Device Score |  | 350-350 | 1 N |
| 125.30 | Wallet Service Provider Account Score |  | 351-351 | 1 N |
| 125.31 | Wallet Service Provider Tokenization Recommendation Reason Codes |  | 352-357 | 6 ANS |
| 125.32 | Device Location |  | 358-366 | 9 ANS |

**\*Tlv Fields of DE-125 when DE-63.7 = ‘MASTERCARD’**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tag Length Value**  **Dataset ID: 01, Wallet Program Data**  Wallet Identifier  01 3  02 2 Token Transaction Identifiers | | | **Format** | **Content of Sub-Element** |
| TLV  TLV | The Wallet Identifier is added for MDES transactions when it is available, which  identifies the wallet through which the MDES token was initiated.  103 - Apple Pay  216 - Google Pay  217 - Samsung Pay  327 - Merchant tokenization program  This subelement will contain, when available, the calculated Token Transaction  Identifier to identify the transaction. Token Transaction Identifier is to be retained  and used to provide the transaction details associated with an original purchase  and subsequent reversal messages. The Token Transaction Identifier is only sent to  issuers participating in the Mastercard Digital Enablement Service. |
| **Dataset ID: 02, PAN Mapping File Information** | | | | |
| 01 | 1 | Account Number Indicator | TLV | (Account Number Indicator) indicates the type of PAN mapping account.  **C** → Mastercard Digital Enablement Service secure element token  **E** → Embossed account number provided by issuer  **F** → Mastercard Digital Enablement Service static token **H** → Mastercard Digital Enablement Service cloud-based payments token  **L** → Pay with rewards loyalty program operator [LPO] card |

1. 19 Account Number PAN

Expiration Date

TLV This Subfield contains the PAN mapping account number.

This Subfield contains the expiration date of the PAN Mapping File Information.

* + **Acquirer Message** = contains the expiration date when
* the issuer provided one for a PAN mapping record added to the MCC106 MDES PAN Mapping File
* A transit transaction response contains MCC 4111, 4131, 4784, and 7523, or

1. 4

Token Assurance

TLV

– The Mastercard Digital Enablement Service was applied.

* **Issuer Message** = contains Contactless card/device expiration date, or virtual card expiration date, or Mastercard Digital

Enablement Service token expiration date, only if acquirer provided in DE 14

* **Issuer and acquirer response message** = contains embossed Expiration date in response to transit transactions

This Subfield contains a value indicating the

1. 2
2. 11

Level TLV

Token Requester ID

TLV

confidence level of the token to PAN/cardholder binding.

This Subfield contains the ID assigned by the Token Service Provider to the Token Requestor.

- *Contains the ID assigned by the Token Service Provider to the Token Requestor. The Token Requestor ID is optional for all token types.*

1. 19 PAN Account Range

TLV This Subfield contains the PAN Account Range.

1. 2 Storage Technology TLV (Storage Technology) describes the Storage

Technology of a requested or created token.

1. 3

Payment Account

Data TLV

(Payment Account Data) contains unique, non- financial reference information associated with the PAN or token used to initiate the transaction.

***Dataset ID: 03 Token Related Data***



Token Expiration Date

01

TLV

Expiration date that is embossed, encoded, or both on the card that represents the cardholder primary account number (primary account number).

Format: YYMM

1. Token Service Provider Identification (TCN)
2. Token Assurance Level

TLV M = Mastercard Digital Enablement Service

TLV Assurance level assigned to the token (value between 00 and 99).

1. Contactless Usage TLV Contains value indicating if the token is

permitted for use in contactless transactions.

Values:

* + 0 = Token is not permitted for use in contactless transactions
  + 1 = Token is permitted for use in contactless transactions

Card on file electronic commerce usage

05

TLV

Contains value indicating if the token is permitted for use in card on file electronic commerce transactions.

Values:

* 0 = Token is not permitted for use in Card on File electronic commerce transactions
* 1 = Token is permitted for use in card on file electronic commerce transactions

1. Mobile / digital wallet electronic commerce usage

Number of active tokens for the PAN

TLV Contains value indicating if the token is permitted for use in mobile/digital wallet electronic commerce transactions.

Values:

* + 0 = Token is not permitted for use in mobile/digital wallet electronic commerce transactions
  + 1 = Token is permitted for use in mobile/ digital wallet electronic commerce transactions

Number of active or suspended tokens for the primary account number digitized to consumer devices. Space-filled when token

1. TLV

present in DE 48, subelement 33, subfield 2 (Account Number) in an 0100 Tokenization Complete Notification message is provisioned to a server. Presence of this field is conditional

1. Issuer product configuration id



TLV The unique product configuration identifier applied to the token, as provided by the issuer, identifying a particular set of card art, texts, and other product related data, that were provided during the issuer enablement or maintenance process.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 09 |  |  |  | Presence of this field is conditional. |
|  | Consumer language | TLV | Language preference selected by the consumer. Presence of this field is conditional. |
| 0A |  | Final Tokenization Decision | TLV | The final tokenization decision that was used in the tokenization of the card.   * 1 = Approve * 2 = Approve but requires additional authentication   Presence of this field is conditional. |
| 0B |  | Final Tokenization Decision Indicator | TLV | The element of the Service that was responsible for determining the final tokenization decision:   * 1 = Tokenization Eligibility Response * 2 = Tokenization Authorization Response * 3 = Issuer pre-defined tokenization rules * 4 = Mobile Application   Presence of this field is conditional. |
| 0C |  | T&C Identifier | TLV | Identifier associated with the version of terms and conditions accepted by the consumer. Presence of this field is  conditional. |
| 0D |  | T&C Date And Time | TLV | Date and time that the consumer accepted the terms and conditions of the Service, specified in UTC units.  Format: YYMMDDhhmm |
| 0E |  | Number Of Activation Attempts | TLV | Number of activation code entry attempts  by the cardholder. Space-filled when DE124, SF14 (Token Type) value is F. Presence of this field is conditional. |
| 1A |  | Token Unique Reference (TCN) | TLV | Service-allocated unique reference to the token. |
| 1B |  | PAN Unique Reference | TLV | Service-allocated unique reference to the tokenized Primary Account Number at the wallet level. |
| 1C | Tokenization Event Indicator | TLV | Value indicating the event that has occurred on the Mastercard Digital Enablement Service for the token  3 = Deactivate  4 = Deleted from consumer device  6 = Suspend  7 = Resume  8 = Tokenization Exception Event  9 = Replacement |

1D Tokenization Event Reason Code

Event Requestor

TLV If the Tokenization Event Indicator contains value 8 (Tokenization Exception Event), this field contains a value indicating the event reason. If the Tokenization Event Indicator contains a value of 3 (Deactivate), 6 (Suspend), or 7 (Resume), this field will not be present.

* + 00 = Activation code retries exceeded
  + 01 = Activation code expired or invalidated
  + 02 = Activation code entered incorrectly by cardholder

If the Tokenization Event Indicator contains a value of 3 (Deactivate), 6 (Suspend), or 7 (Resume), this field will contain a value indicating the party that requested the event. If the Tokenization Event Indicator contains a value of 8 (Tokenization Exception Event) this field will be space filled.

* + 0 = Indicates the Tokenization Event was requested by the Wallet Provider or Token Requestor
  + 1 = Indicates the Tokenization Event was requested by the Funding Account issuer
  + 2 = Indicates the Tokenization Event was requested by the Cardholder

1E TLV

* 3 = Indicates the Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Validation security (applicable to Tokenization Event Indicator value of 6 (Suspend), or 7 (Resume) only)
* 4 = Indicates the Tokenization Event was requested in relation to a systematic event triggered by Mobile PIN Change Validation security (applicable to Tokenization Event Indicator value of 6 (Suspend), or 7 (Resume) only)
* 5 = Reserved for future use
* 6 = Reserved for future use
* 7 = Reserved for future use
* 8 = Reserved for future use
* 9 = Reserved for future use

***Dataset ID: 04, PAN Mapping File Information***



01 Primary Account TLV Identifies the method which the cardholder is

|  |  |  |  |
| --- | --- | --- | --- |
|  | Number Score |  | attempting to tokenize a primary account number with one of the following values:  1 = Card on file  2 = Card added manually  3 = Card added via application |
| 02 | Payment Application Instance ID | TLV | Identifier associated with the payment application installed onto a device. |
| 03 | Device Source IP Address | TLV | Variable length IP address. Each octet of the IP address is converted to hex, and joined into one string, with the order maintained. |
| 04 | Wallet Provider Account ID Hash | TLV | When provided by the Wallet Provider, the issuer may use this hash value to match against known identifiers for the cardholder; for example, their email addresses on file. If the hash values match, this may aid an issuer’s digitization decision by providing additional factors to help verify that the Wallet Provider account holder is indeed their cardholder, or to differentiate between primary and secondary cardholders. |
| 05 | Cardholder name | TLV | This field may be present and contain the name of the cardholder. The format is either LASTNAME/FIRSTNAME with the names delimited by a slash “/” (Example: SMITH/JOE) or the format is FIRSTNAME LASTNAME (Example: JOE SMITH).  If the cardholder’s name is longer than 27 positions, the data will be truncated to the maximum length of 27. |
| 06 | Wallet provider Tokenization Recommendation | TLV | Tokenization decision suggested by the Wallet Provider. One of the following values:  0 = Decline  1 = Approve  2 = Require additional authentication |
| 07 | Wallet provider Tokenization Recommendation Standard Version | TLV | The version of the standards the Wallet Provider is using to determine the suggested tokenization recommendation. |
| 08 | Wallet Provider Device Score | TLV | Score assigned by Wallet Provider for the device. Value between 1 and 5. |

|  |  |  |  |
| --- | --- | --- | --- |
| 09 | Wallet Provider Account Score | TLV | Score assigned by Wallet Provider for the primary account number. Value between 1 and 5. |
| 0A | Wallet Provider Tokenization Reccomendation Reason Codes | TLV | Code indicating the specific reason the Wallet Provider is suggesting the tokenization recommendation.  The data of this field is a hex-encoded bitmap, whereby each bit corresponds to a specific Reason Code.  The bitmap is big-endian with the least significant bit corresponding to Reason Code 01, with the next least significant bit corresponding to Reason Code 02, and so on. For example, if Reason Codes 01, 05, and 16 were encoded, the bitmap would be 0000000010000000000100001 and the hex  value of this field would be 008011.  If the Wallet Provider has no reason, this field will contain spaces. |
| 0B | Device Location | TLV | Latitude and longitude where the device the consumer is attempting to tokenize a card onto is located.  Device Location Latitude – an-4; hexadecimal encoded degrees with 2 decimal places Device Location Longitude – an-4; hexadecimal encoded degrees with 2 decimal places Device Location Lat/Long Sector – n-1 – one of the following values:  1 = Latitude = N, Longitude = W  2 = Latitude = N, Longitude = E  3 = Latitude = S, Longitude = W  4 = Latitude = S, Longitude = E  This field will contain spaces if the Wallet Provider has not provided this information. |

##### 125.6\* (Card on File Electronic Commerce Usage)

Contains value indicating if the token is permitted for use in card on file electronic commerce transactions.

##### Possible Values:

0 = Token is not permitted for use in Card on File electronic commerce transactions.

1 = Token is permitted for use in Card on File electronic commerce transactions.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE-125 when DE-63.7 = ‘UNIONPAY’** | | | | |
| Tag | Length | Value | Format | Content of Sub-Element |
| ***Dataset ID: QR, Token Data*** | | | | |
| 01 | 3 | QRC Use Case Indicator | ANS | Valid values:  100- Consumer-presented QRC, purchase transaction. 210- Merchant-presented QRC, purchase transaction.  211- Merchant-presented QRC, purchase transaction, debit card only. Example: purchasing financial products.  220- Merchant-presented QRC, ATM cash withdrawal.  212- Merchant-presented QRC, purchase transaction in small businesses.  231- P2P QRC-based Payment, primary credit transaction.  232- P2P QRC-based Payment, account funding transaction, |
| 02 | 20 | QRC Voucher Number | ANS | Generated by UnionPay system. The payment index is unique permanently. It is used to locate a transaction. |
| 03 | 34 | C2B Payment Code | ANS | The information contained in the Consumer- presented QRC. |
| 04 | 11 | Wallet ID 1 | ANS | Assigned by UPI. It indicates the Wallet ID of payer. |
| 05 | 11 | Wallet ID 2 | ANS | Assigned by UPI. It indicates the Wallet ID of payee. |

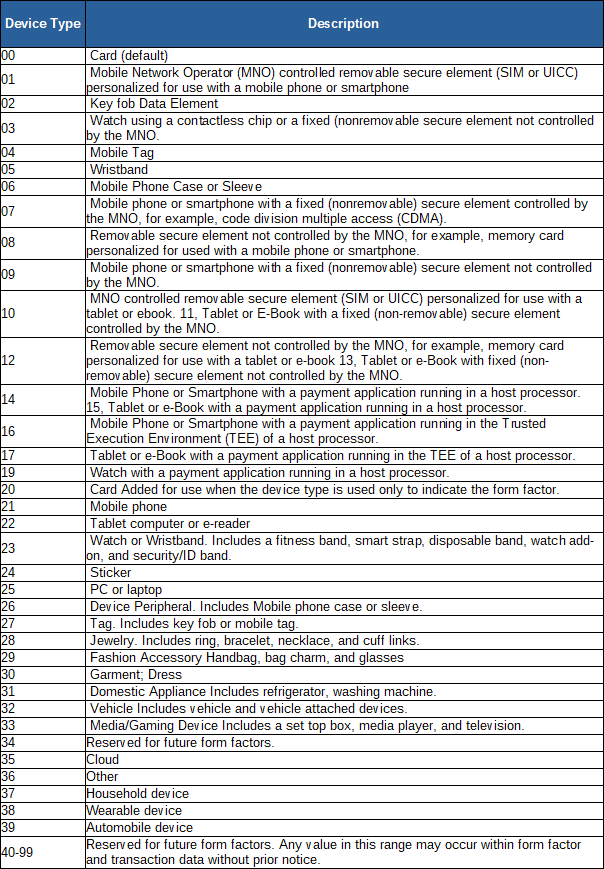
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Sub Elements of DE 125 when DE63.7 = ‘DISCOVER’** | | | | | | |  |
| Sub Field No | Field Name | Discover Bit No | Data set | TAG | Format | Values | |
| 125.1 | Token Requestor ID | 106 | 61 | 02 | 16 AN | This tag will contain the ID of Token  Requestor.  This tag may not be present to all Merchant / Acquirers. | |
| 125.2 | Token Assurance | 106 | 61 | 03 | 2 AN | This tag will contain a | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Level |  |  |  |  | value that indicates the confidence level of the Payment Token to PAN Cardholder binding.  Contact your Discover Account Executive for further clarification on the use of this field. |
| 125.3 | PAN Data | 106 | 61 | 04 | 19 AN | Contains Primary Account data for the tokenized Account. Acquirers and Merchant Processors must not forward PAN data to Merchants.  This tag may not be present to all Merchant / Acquirers.  Contact your Discover Network Account Executive for further clarification on the use of this field. |
| 125.4 | Payment Token Number | 106 | 61 | 05 | 19 AN | This is the Payment Token number. |
| 125.5 | Token Expiry Date | 106 | 61 | 06 | 4 AN | The expiration date of the Payment Token. Format  = YYMM. |
| 125.6 | PAN Expiration Date | 106 | 61 | 13 | 4 AN | The PAN expiration date for the Primary Account Number. Format = YYMM |
| 125.7 | Token Network Transaction Identifier | 106 | 61 | 14 | 64 AN | This tag will contain a unique Transaction ID generated by Discover Digital Platform. |
| 125.8 | Token ID | 106 | 61 | 18 | 64 AN | Service-allocated unique reference to the token. |
| 125.9 | Token Domain Type | 106 | 61 | 20 | 2 AN | Contains a value indicating the type of Payment Token present.  01 ECOM/COF- E-  Commerce/Card-on-File 02Secure Element 03HCE / Cloud-Based Payment  04CBP (Cloud Based |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Payment) |
| 125.10 | Device Type | 106 | 62 | 01 | 2 AN | This tag contains the device type.  Possible values:  125.10 Possible values of device types 92 |
| 125.11 | Device ID | 106 | 62 | 06 | 64 AN | A stable persistent hardware identifier of the device (e.g. the secure element identifier (SEID) provided by the digital wallet). |
| 125.12 | Full Phone Number | 106 | 62 | 08 | 20 AN | A full phone number, if provided by the digital wallet. |
| 125.13 | Device Name | 106 | 62 | 10 | 64 ANS | Commercial name (model) of the device, as defined by the device provider |
| 125.14 | Device Location | 106 | 62 | 12 | 35 ANS | This tag contains the geographic location of the device. Location is latitude/longitude rounded to nearest whole digit; for example, +37/-  121. May present when function code is 641 |
| 125.15 | Device IP Address | 106 | 62 | 13 | 35 ANS | This tag contains the IP address of the device at the time of the provisioning request. May present when function code is 641. This value will be in the format: 255.255.255.255. Each  octet (255) may be 1–3 digits in length. (align with V+ data in Field 63) |
| 125.16 | Account Risk | 106 | 63 | 05 | 2 AN | A value of 01–05, with a value of 05 as the most trusted |
| 125.17 | Device Risk | 106 | 63 | 04 | 2 AN | A value of 01–05, with a value of 05 as the most trusted |
| 125.18 | Risk Reason | NA | NA | NA | 3 N | Identified risk reason code for identifying provision risk color |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 125.19 | Phone no. (Last 4) | NA | NA | NA | 4 N | User phone number if available (Last) |
| 125.20 | Provisioning Risk | NA | NA | NA | 10 AN | Risk rating based on experience with the customer and device being provisioned. Possible values are GREEN YELLOW ORANGE RED |
| 125.21 | Token Notification Type | NA | NA | NA | 4 N | Specific operation that needs to performed on the Token associated with the tokenId |
| 125.22 | Correlation Id | NA | NA | NA | 64 ANS | This is a value that is returned by the Issuer. This allows the Issuer to tie together Verify Card calls with Provision Credential calls as these happen asynchronously. |
| 125.23 | OTP | NA | NA | NA | 8 AN | OTP code entered by user / received from network |
| 125.24 | Cardholder Verification Method Identifier | NA | NA | NA | 1 N |  |
| 125.25 | Cardholder Verification Method Value | NA | NA | NA | 64 AN |  |
| 125.26 | Token Authorization Request (TAR) Indicator | NA | NA | NA | 1 N | If 1 it means the request is Token authorization request. |
| 125.27 | Billing Address | NA | NA | NA | 128 ANS | Full Billing Address of the Cardholder |
| 125.28 | Billing Zip | NA | NA | NA | 24 ANS | Full postal code of the Customer |
| 125.9 | Token Status | NA | NA | NA | 1 N | Token Status |
| 125.30 | Replacement DPAN Expiry | NA | NA | NA | 4 ANS | Replacement DPAN Expiry |
| 125.31 | Replacement PAN | NA | NA | NA | 19 ANS | Replacement PAN |
| 125.32 | Wallet Type | NA | NA | NA | 5 AN | Token Wallet Type |

**125.10 Possible values of device types**



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tag Length Value Format Content of Sub-Element**    ***Dataset ID: 01, Request Header***  Request ID A unique reference for Request. This should be  1-64 TLV freshly generated by the client for every API Call.  This enables easier troubleshooting of issues  between the MPP and the NWP  1-64 Session ID TLV This is a Unique Identifier created by the MPP to  represent a provisioning attempt for an Account on a device. It is used to tie together the activity across   1. the different APIs up until the point that there has   been a successful provisioning. Required for following APIs only Account Eligibility Verify Card Provision Credentials   * + OOB Contact Channels   + OOB Contact Channel   + OOB Authentication   + OOB Authentication Validation  1. 16 Program ID TLV This tag contains the cumulative count of   transactions for the current limited-use key (LUK).This is a unique identifier that identifies the product and the institution participating in the scheme. The value to be sent will be provided by NWP.  ***Dataset ID: 02, User Context***   1. 1-100 Wallet ID TLV The Wallet ID passed in the request 02 1-64 Device ID TLV The Device ID passed in the request 03 1-100 User ID TLV The User ID passed in the request   **Dataset ID: 03, Account Eligibility Context** | | | | |
| 01 | 1-64 | Terms & Condition ID | TLV | The identifier for the version of the terms and conditions that are to be accepted by the user during this provision cycle. The actual T&Cs are retrieved by calling the Resource API. |
| 02 | 1-64 | Terms & Condition Accepted Date | TLV | This Tag Contains the Terms and Condition Accepted Date |
| 03 | 19 | PAN | TLV | The Primary Account Number representing the Account that is to be boarded onto the wallet. |
| 04 | 4 | PAN ID | TLV |  |
| 05 | 3 | Expiry Date | TLV | The Expiry Date of the card in format *MMYY.* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 06 | 1-64 | CardHolder Name | TLV | Full name of the Cardholder. The Cardholder name can contain special characters such as diacritic marks (umlauts, cedillas, accents) or Emoji characters so it is difficult to restrict the values on this. The transport will validate that it is a UTF-8 character. |
| 07 | 128 | Billing Address | TLV | Full Billing Address of the Cardholder |
| 08 | 24 | Billing Postal Code | TLV | Full Billing Zip of the Customer |
| 09 | 20 | Source | TLV | This indicates which method was used to capture the user information that is being sent. "add-device" - Provision a companion device using the details of a previously provisioned device "in-app" - This is set when the provision Request is initiated from Card Mobile app "on- file" - This is set when the account is already present "restore" – This is set when is provision is initiated as a result of restore of previously provisioned pan. E.g., a new device registered with wallet account with previously digitalized pan. "user-input" – User manually |
| 0A | 1 | Capture Method | TLV | Capture Method   * Camera * Manual |
| **Dataset ID: 04, Device Context** | | | | |
| 01 | 1-64 | device bluetooth mac | TLV | Device bluetooth MAC address (e.g., 00-16-68 or 00-16-68-2B-40-90 or 00:16:68:2B:40:90 or  0016682B4090 or 00.16.68.2B.40.90) |
| 02 | 1-64 | device brand | TLV | Brand of the device. Eg. "Google" for nexus devices  ,"Samsung" for Samsung devices |
| 03 | 2 | device country | TLV | Country where the device was purchased (iso 3166- 1 alpha-2) |
| 04 | 64 | device id type | TLV | Type of the device id from which it is sources. E.g., TEE |
| 05 | 15-32 | device ip | TLV | IP Address of the device |
| 06 | 1-64 | device manufacturer | TLV | Mobile Manufacturer (Google, Samsung etc) |
| 07 | 1-64 | device model | TLV | Device Model (Galaxy 56,LG, G4, HTC etc) |
| 08 | 1-100 | device name | TLV | User Assigned Device Name |
| 09 | 1-64 | device os build | TLV | Device OS build version (9.3.2, 4.1.1. etc) |
| 10 | 1-64 | device os type | TLV | Device OS type (Android, Windows, Symbian etc) |
| 11 | 1-32 | device os version | TLV | Mobile operating system version (Android 4.4.2, Kitkat 5.0.3, etc...) |
| 12 | 1-32 | device time zone | TLV | Device time zone. example: "GMT-08:00" |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 13 | 4-35 | device time zone settings | TLV | true if user lets timezone be set timezone Network, false if user set own timezone. |
| 14 | 1-3 | device type | TLV | Type of device  1 – Mobile  2 – Tablet  3 – Watch 2  5 – Phone\_Tablet  6 – PC/Mac  7 - Cloud  99 – Other |
| 15 | 1-20 | device user id | TLV | Device User ID |
| 16 | 2-4 | imei | TLV | Last 2 or 4 digits. Issuer app can query for IMEI / MEID through standard android API. Issuer can then compare their independently derived knowledge of the IMEI/MEID to the last 2 or 4 characters that are sent. Customer service can use IMEI last 2 or 4 characters in support scenarios to verify they are speaking with the holder of the device, and to disambiguate a device. |
| 17 | 10 | language | TLV | Code for identifying the device language. Based on IEFT BCP 47. If not provided, this will be defaulted to en-US. |
| 18 | 1-16 | latitude | TLV | Coordinates (latitude) of the device when it is being provisioned |
| 19 | 1-64 | location source | TLV | Source from which location of the device is identified e.g., WiFi, Cellular, GPS |
| 20 | 1-16 | longitude | TLV | Coordinates (longitude) of the device when it is being provisioned |
| 21 | 5-64 | parent device id | TLV | A stable persistent hardware identifier of the parent device that survives factory resets (e.g., Device id of the phone when watch is provisioned) |
| 22 | 4 | phone number | TLV | User phone number if available (Last) |
| 23 | 2-4 | serial number | TLV | The last 2 to 4 digits of the device Serial number |
| **Dataset ID: 05, User Provision Context** | | | | |
| 01 | 1-300 | email address | TLV | Device profile email Address. This will be obfuscated if supplied. |
| 02 | 1-4 | email address age | TLV | Age of profile email id in weeks |
| 03 | 2 | email address country | TLV | Country of device at time of provisioning (iso 3166-1 alpha-2) |
| 04 | 1-64 | hashed email address | TLV | Hashed Email Address / Account Id |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dataset ID: 06, Risk Context** | | | | |
| 01 | 1 | account risk | TLV | MPP risk rating based on experience with the customer account. Numeric score from 1-5. 1 – Highest Risk, Lowest Confidence.  5 – Lowest Risk, Highest Confidence. |
| 02 | 1 | device risk | TLV | MPP risk rating based on experience with the device being provisioned. Numeric score from 1-5.  1 – Highest Risk, Lowest Confidence. 5 – Lowest Risk, Highest Confidence. |
| 03 | 1-10 | provisioning risk | TLV | MPP risk rating based on experience with the customer and device being provisioned. Possible values are  GREEN YELLOW ORANGE RED |
| 04 | 1-2 | age of device usage by account | TLV | Number of weeks since the device was used by the wallet account. Max value is 99. |
| 05 | 1-2 | age of last account activity | TLV | Number of weeks since last activity by the wallet account (provision, refresh, lifecycle events from the wallet account across Networks/Issuers). Max value is 99. |
| 06 | 1-2 | age of last account change | TLV | Number of weeks since the last change to the wallet account. Max value is 99. |
| 07 | 1-4 | age of tokenized card | TLV | Number of weeks since another card from the same issuer was tokenized on a device. Max value is 9999. |
| 08 | 1-4 | age of wallet account | TLV | Age of user’s financial relationship with mobile platform (in weeks) |
| 09 | 1-4 | card on file tenure | TLV | Age of card on file (in weeks). Applicable only for card-on file use cases |
| 0A | 2 | country during provision | TLV | Country of device at time of provisioning (iso 3166-1 alpha-2) |
| 0B | 1-3 | number of tokens account | TLV | Number of Tokens for the wallet account across devices. Max value is 999. |
| 0C | 1-3 | number of tokens device | TLV | Number of Tokens on physical device. |
| 0D | 1-2 | suspended tokens in account | TLV | Number of suspended Tokens in the wallet account. Max value is 99. |
| 0E | 1-2 | total provisioning | TLV | Number of provisioning attempts on the device for |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | attempts |  | the last 24 hours. Max value is 99. |
| 11 | 1-4 | total transaction count for year | TLV | Total number of transaction count by the wallet account in the past 12 months (at the account level across devices, Networks, partners etc). Max value is 9999. |
| 12 | 1-3 | risk reason code | TLV | MPP identified risk reason code for identifying provision risk color. |
| **Dataset ID: 06, Token Context** | | | | |
| 01 | 12-19 | token | TLV | The tokenized Account Number representing the Account that is to be boarded onto the wallet. This is the Account Number that will used for tokenized Transactions. |
| 02 | 4 | Token expiry Date | TLV | The expiry Date of the Token in format MMYY. |
| 03 | 32-64 | Token id | TLV | This is an opaque identifier for the Token in the wallet associated with the programId. |
| 04 | 2 | Token type | TLV | A classification of the type of Token being passed 01 - Card on File (individual Merchant)  04 – CBP (Cloud Based Payment) |
| 05 | 1-32 | Selected channel identifier | TLV | Unique identifier of the out-of-band contact channel selected by the user. This is the value of one of the identifiers returned in the getOOBContactChannels Response. |

# Data Element 109 – Advice Reason Code Table

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sub Elements of DE 109 when DE63.7 = ‘MASTERCARD’ and 48.9 = ‘SMS’** | | | | | | | | |
| **Sub Field No** | | **Field Name** | **MC Bit No** | | | **Position** | | **Format** |
| 109.1 | | Message Reason Code | 60.1 | | | 1-3 | | 3N |
| 109.2 | | Message Reason Code Detail | 60.2 | | | 4-7 | | 4N |
| 109.3 | | Detail Text | 60.3 | | | 8-60 | | 53 ANS |
| 109.4 | | Additional Text | 60.4 | | | 61-100 | | 40 AN |
| **Sub Elements of DE 109 when DE63.7 = ‘MASTERCARD’ and 48.9 = ‘DMS’** | | | | | | | | |
| **Sub Field No** | **Field Name** | | | **MC Bit No** | **Position** | | **Format** | |
| 109.1\* | Message Reason Code | | | N/A | 1-7 | | 7N | |

##### \*: Multi-Clearing Indicators

* + - Multi-Clearing → ‘**1403’** (If Field 109 **contains** value ‘1403’, It is a multi-clearing)
    - Final Clearing → ‘**1404’** (If field 109 **contains** value ‘1404’, it is the last clearing in multiclearing cycle)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE 109 when DE63.7 = ‘STAR’ and 48.9 = ‘AXS’** | | | | |
| **Sub Field No** | **Field Name** | **STAR Bit**  **No** | **Position** | **Format** |
| 109.1\* | Advice/Reversal Reason Code | 60 | 1-6 | AN-6 |

##### 109.1\*

Represents the advice/reversal reason code. Issuers may use specific advice reason codes to notify acquirer of the reason for a decline on a recurring payment authorization.

|  |  |
| --- | --- |
| **Position 1-2:** Indicates which reason code is present | * **80** = Reversal Reason present * **40** = Advice Reason present * **C0** = Both reversal and advice reason subfields are present. |
| **Position 3-4:** Depending upon the previous field, this field contains either a valid advice/reversal reason code. | * **RR** (A valid reversal reason code) * **AA** (A valid advice reason code) |
| **Position 5-6:** Present only if the first two positions contain ‘C0’, then reversal code is present at position 3-4 and advice reason code in at these two positions. | * **C0RRAA** (where RR is reversal reason code & AA is advice reason code) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE 109 when DE63.7 = ‘DISCOVER’** | | | | |
| Sub Field No | Field Name | DISCOVER Bit No | Position | Format |
| 109.1 | Message Reason Code | 25 | 1-2 | 2 N |

Possible values with description:

|  |  |  |
| --- | --- | --- |
| **Reversal Reason Codes** | | |
| Code | Definition | |
| 00 | Customer Cancellation | |
| 01 | Unspecified; No Action Taken | |
| 02 | Suspected Malfunction | |
| 03 | Format Error; No Action Taken | |
| 04 | Completed Partially | |
| 05 | Original Amount Incorrect | |
| 06 | Response Received Too Late | |
| 07 | Card Acceptor Device (POS Device) Unable to Complete Transaction | |
| 13 | Unable to Deliver Message to Point of Sale (POS) | |
| 14 | Suspected Malfunction/Card Retained | |
| 16 | Suspected Malfunction/Track 3 Not Updated | |
| 17 | Suspected Malfunction/No Cash Dispensed | |
| 18 | Timed-Out at Taking Money/No Cash Dispensed | |
| 19 | Timed-Out at Taking Card/Card Retained and No Cash Dispensed | |
| 20 | Invalid Response; No Action Taken | |
| 21 | Timed-Out Waiting for Response | |
| 22 | Invalid Card Product Code | |
| 51 | Return (of goods or services) | |
| 52 | Credit Adjustment | |
| **Advice Reason Codes** | |  |
| Code | Definition |  |
| 62 | Invalid Card Product Code |  |
| 63 | Merchant is not in Inclusion Table |  |
| 64 | Reserved |  |
| 65 | Reserved |  |
| 66 | Issuer unavailable |  |
| 67 | Issuer’s rules failed |  |
| 68 | AVS verification failed |  |
| 69 | Reserved |  |
| 70 | Mobile Passcode not verified |  |
| 71 | Mobile Transaction Amount exceeds stand-in limit |  |

|  |  |  |
| --- | --- | --- |
| 72 | Network Declined: Suspected Fraud |  |
| 73 | Automated Fuel Dispenser - final Card Sale amount |  |
| 74 | Host Capture - final Card Sale amount |  |

|  |  |
| --- | --- |
| **Administrative Transaction Request Reason Codes** | |
| Code | Definition |
| 80 | Instant Credit Support – Consumer |
| 81 | Application Status – Consumer |
| 82 | Authorized User Inquiry – Consumer |
| 83 | Account Inquiry – Consumer |
| 84 | Account Maintenance – Consumer |
| 90 | Instant Credit Support - Business |
| 91 | Application Status – Business |
| 92 | Authorized User Inquiry – Business |
| 93 | Mobile Passcode not verified Account Inquiry – Business |
| 94 | Account Maintenance – Business |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sub Elements of DE 109 when DE63.7 = ‘FISERV’** | | | | |
| Sub Field No | Field Name | FISERV Bit No | Position | Format |
| 109.1 | Message Reason Code | 25 | 1-4 | 4N |

Possible values of Field-109 with description for FISERV:

|  |  |
| --- | --- |
| **Advice Reason Codes (For 01xx and 02xx messages)** | |
| Code | Definition |
| 1000 | Stand-in processing at the card issuer's option |
| 1001 | Stand-in because card issuer was signed off |
| 1002 | Stand-in because card issuer timed out on original request |
| 1003 | Stand-in because card issuer was unavailable |
| 1004 | Terminal processed |
| 1005 | ICC processed |
| 1006 | Under floor limit |
| 1007 | Stand-in processing at the acquirer's option |

|  |  |
| --- | --- |
| 1008 | Credit adjustment |
| 1376 | Default value |

|  |  |
| --- | --- |
| **Advice Reason Codes (For 04xx messages)** | |
| **Code** | **Definition** |
| 4000 | Customer/Merchant cancellation |
| 4001 | Unspecified |
| 4002 | Suspected malfunction |
| 4003 | Format error; no action taken |
| 4004 | Completed partially (under dispense) |
| 4005 | Original amount incorrect |
| 4006 | Response received too late (late response reversal) |
| 4007 | Card acceptor device unable to complete transaction |
| 4013 | Unable to deliver message to point of service |
| 4014 | Acquirer denial suspect fraud |
| 4021 | Time out waiting for response (early reversal) |

## Appendix D – Sample Messages

#### Sample Network Request/Response Messages (0800, 0810)

##### Request Message [0800] (ASCII format)

00670800822000000800000004000000000000000409111530088001909916088001081

Where,

Message length (4-bytes): 0067 MTI (4-bytes): 0800

Bitmaps (32 bytes): 82200000080000000400000000000000

Data Elements (31 bytes): 0409111530088001909916088001081

###### Parsed Data Elements:

DE 007 = 0409111530

DE 011 = 088001

DE 037 = 909916088001

DE 070 = 081

##### Response Message [0810] (ASCII format)

00690810822000000A0000000400000000000000040911153008800190991608800100081

Where,

Message length (4-bytes): 0069 MTI (4-bytes): 0810

Bitmaps (32 bytes): 822000000A0000000400000000000000

Data Elements (33 bytes): 040911153008800190991608800100081

###### Parsed Data Elements:

DE 007 = 0409111530

DE 011 = 088001

DE 037 = 909916088001

DE 039 = 00

DE 070 = 081

##### Request Message [0800] (Bytes format)

###### Request Message (represented in Hex):

00333038303082200000080000000400000000000000303232363039323635363038383030313930353731

34303838303031303831

Where,

Message length (2-bytes): 0033 (51 bytes)

MTI (4-bytes): 30383030 (0800)

Bitmaps (16 bytes): 82200000080000000400000000000000

Data Elements (31 bytes): 30323236303932363536303838303031393035373134303838303031303831

###### Parsed Data Elements:

DE 007 = 0226092656

DE 011 = 088001

DE 037 = 905714088001

DE 070 = 081

**Response Message [0810] (Bytes format)**

###### Request Message (represented in Hex):

003530383130822000000A00000004000000000000003032323630393236353630383830303139

30353731343038383030313030303831

Where,

Message length (2-bytes): 0035 (53 bytes)

MTI (4-bytes): 30383130 (0810)

Bitmaps (16 bytes): 822000000A0000000400000000000000

Data Elements (33 bytes): 303232363039323635363038383030313930353731343038383030313030303831

###### Parsed Data Elements:

DE 007 = 0226092656

DE 011 = 088001

DE 037 = 905714088001

DE 039 = 00

DE 070 = 081

#### Sample Authorization Request/Response Messages (0100, 0110)

##### Request Message [0100] (represented in Hex):

01F830313030F67A449108E0A40A000000000402000031353130303139343836383733363536343030303

03030303030303030303530303030303030303030303530313030303132323133323931383631303032303

03030313633373231383239313830313232303132323535343139303230304430303030303030303036303

0303030303830323231333031363337325445524D4944303143415244204143434550544F5220204143515

549524552204E414D4520202020202020202020202043495459204E414D45202020204341555341383430

38343030323030303732383430443030303030303030303130303031363030303030303030303430323030

30303037303030303220202020313233343536313233343536313233202020202020202020202030202020

20202020202020202020202020202020202020205649534120202020202020203135313030313934383638

37333635363431353420313233343536313233343536313233202020202030302020202020202020202020

20202020202020202020202020202030303030303020303030303030303030302030303030303030303030

30302020202020303030303030303030302020202020202020202020203030303230303030303030303030

30303030303020202020202020202020202020202030302020202030373638383932

###### Parsed Message [0100]:

DE-2 [100194868736564]

DE-3 [000000]

DE-4 [000000050000]

DE-6 [000000050100]

DE-7 [0122132918]

DE-10 [61002000]

DE-11 [016372]

DE-12 [182918]

DE-13 [0122]

DE-15 [0122]

DE-18 [5541]

DE-22 [902]

DE-25 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016372] DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR]

DE-43 [ACQUIRER NAME CITY NAME CAUSA] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA]

DE-102 [100194868736564]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0768892]

##### Response Message [0110] (represented in Hex):

01CE30313130F67A00910EC0A40A00000000040200003135313030313934383638373336353634303030

30303030303030303030353030303030303030303030353031303030313232313332393138363130303230

30303031363337323138323931383031323230313232303044303030303030303030363030303030303830

3232313330313633373230303132343535315445524D4944303143415244204143434550544F5220203834

30383430303230303037323834304430303030303030303031303030313630303030303030303034303230

30303030373030303032202020203132333435363132333435363132332020202020202020202020302020

20202020202020202020202020202020202020202056495341202020202020202031353130303139343836

38373336353634313534203132333435363132333435363132332020202020303020202020202020202020

20202020202020202020202020202020303030303030203030303030303030303020303030303030303030



30303020202020203030303030303030303020202020202020202020202030303032303030303030303030

3030303030303020202020202020202020202020202030302020202030373638383932

###### Parsed Message [0110]:

DE-2 [100194868736564]

DE-3 [000000]

DE-4 [000000050000]

DE-6 [000000050100]

DE-7 [0122132918]

DE-10 [61002000]

DE-11 [016372]

DE-12 [182918]

DE-13 [0122]

DE-15 [0122]

DE-25 [00]

DE-28 [D00000000] DE-32 [000000

DE-37 [802213016372]

DE-38 [001245]

DE-39 [51]

DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA]

DE-102 [100194868736564]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0768892]



#### Sample Authorization Advice Request/Response Messages (0120, 0130)

##### Request Message [0120 (represented in Hex):

01FA30313230F67A44D108E0A40A000000000402000031353130303139343836383733363536343030303

03030303030303030303530303030303030303030303530313030303132323133333330303631303032303

03030313633373431383333303030313232303132323535343139303230303030443030303030303030303

63030303030303830323231333031363337345445524D4944303143415244204143434550544F522020414

3515549524552204E414D4520202020202020202020202043495459204E414D4520202020434155534138

34303834303032303030373238343044303030303030303030313030303136303030303030303030343032

30303030303730303030322020202031323334353631323334353631323320202020202020202020203020

20202020202020202020202020202020202020202020564953412020202020202020313531303031393438

36383733363536343135342031323334353631323334353631323320202020203030202020202020202020

20202020202020202020202020202020203030303030302030303030303030303030203030303030303030

30303030202020202030303030303030303030202020202020202020202020303030323030303030303030

303030303030303020202020202020202020202020202030302020202030393834373037

###### Parsed Message [0120]:

DE-2 [100194868736564]

DE-3 [000000]

DE-4 [000000050000]

DE-6 [000000050100]

DE-7 [0122133300]

DE-10 [61002000]

DE-11 [016374]

DE-12 [183300]

DE-13 [0122]

DE-15 [0122]

DE-18 [5541]

DE-22 [902]

DE-25 [00]

DE-26 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016374] DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR]

DE-43 [ACQUIRER NAME CITY NAME CAUSA] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA]

DE-102 [100194868736564]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0984707]

##### Response Message [0130] (represented in Hex):

01C830313330F67A00910AC0A40A000000000402000031353130303139343836383733363536343030303

03030303030303030303530303030303030303030303530313030303132323133333330303631303032303

03030313633373431383333303030313232303132323030443030303030303030303630303030303038303

232313330313633373435315445524D4944303143415244204143434550544F52202038343038343030323

03030373238343044303030303030303030313030303136303030303030303030343032303030303037303

03030322020202031323334353631323334353631323320202020202020202020203020202020202020202

02020202020202020202020202020564953412020202020202020313531303031393438363837333635363



43135342031323334353631323334353631323320202020203030202020202020202020202020202020202

02020202020202020203030303030302030303030303030303030203030303030303030303030302020202

02030303030303030303030202020202020202020202020303030323030303030303030303030303030303

020202020202020202020202020202030302020202030393834373037

###### Parsed Message [0130]:

DE-2 [100194868736564]

DE-3 [000000]

DE-4 [000000050000]

DE-6 [000000050100]

DE-7 [0122133300]

DE-10 [61002000]

DE-11 [016374]

DE-12 [183300]

DE-13 [0122]

DE-15 [0122]

DE-25 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016374]

DE-39 [51]

DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR ] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA ]

DE-102 [100194868736564]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0984707]



#### Sample Financial Request/Response Messages (0200, 0210)

##### Request Message [0200] (represented in Hex):

01FA30323030F67A44D108E0A40A000000000402000031353130303139343836383733363635343030303

03030303030303030303530303030303030303030303530313030303132323133333134313631303032303

03030313633373331383331343130313232303132323535343139303230303030443030303030303030303

63030303030303830323231333031363337335445524D4944303143415244204143434550544F522020414

3515549524552204E414D4520202020202020202020202043495459204E414D4520202020434155534138

34303834303032303030373238343044303030303030303030313030303136303030303030303030343032

30303030303730303030322020202031323334353631323334353631323320202020202020202020203020

20202020202020202020202020202020202020202020564953412020202020202020313531303031393438

36383733363635343135342031323334353631323334353631323320202020203030202020202020202020

20202020202020202020202020202020203030303030302030303030303030303030203030303030303030

30303030202020202030303030303030303030202020202020202020202020303030323030303030303030

303030303030303020202020202020202020202020202030302020202030393035343430

###### Parsed Message [0200]:

DE-2 [100194868736654]

DE-3 [000000]

DE-4 [000000050000]

DE-6 [000000050100]

DE-7 [0122133141]

DE-10 [61002000]

DE-11 [016373]

DE-12 [183141]

DE-13 [0122]

DE-15 [0122]

DE-18 [5541]

DE-22 [902]

DE-25 [00]

DE-26 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016373] DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR ]

DE-43 [ACQUIRER NAME CITY NAME CAUSA] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA ]

DE-102 [100194868736654]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0905440]

##### Response Message [0210] (represented in Hex):

01D230323130F67A40910EC0A40A000000000402000031353130303139343836383733363635343030303

03030303030303030303530303030303030303030303530313030303132323133333134313631303032303

03030313633373331383331343130313232303132323535343130304430303030303030303036303030303

03038303232313330313633373330303132343535315445524D4944303143415244204143434550544F522

02038343038343030323030303732383430443030303030303030303130303031363030303030303030303

43032303030303037303030303220202020313233343536313233343536313233202020202020202020202

03020202020202020202020202020202020202020202020205649534120202020202020203135313030313

93438363837333636353431353420313233343536313233343536313233202020202030302020202020202



02020202020202020202020202020202020202030303030303020303030303030303030302030303030303

03030303030302020202020303030303030303030302020202020202020202020203030303230303030303

03030303030303030303020202020202020202020202020202030302020202030393035343430

###### Parsed Message [0210]:

DE-2 [100194868736654]

DE-3 [000000]

DE-4 [000000050000]

DE-6 [000000050100]

DE-7 [0122133141]

DE-10 [61002000]

DE-11 [016373]

DE-12 [183141]

DE-13 [0122]

DE-15 [0122]

DE-18 [5541]

DE-25 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016373]

DE-38 [001245]

DE-39 [51]

DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR ] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA ]

DE-102 [100194868736654]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0905440]



#### Sample Financial Advice Request/Response Messages (0220, 0230)

##### Request Message [0220] (represented in Hex):

01FA30323230F67A44D108E0A40A000000000402000031353130303139343836383733363635343030303

03030303030303030303530303030303030303030303530313030303132323133333335373631303032303

03030313633373531383333353730313232303132323535343139303230303030443030303030303030303

63030303030303830323231333031363337355445524D4944303143415244204143434550544F522020414

3515549524552204E414D4520202020202020202020202043495459204E414D4520202020434155534138

34303834303032303030373238343044303030303030303030313030303136303030303030303030343032

30303030303730303030322020202031323334353631323334353631323320202020202020202020203020

20202020202020202020202020202020202020202020564953412020202020202020313531303031393438

36383733363635343135342031323334353631323334353631323320202020203030202020202020202020

20202020202020202020202020202020203030303030302030303030303030303030203030303030303030

30303030202020202030303030303030303030202020202020202020202020303030323030303030303030

303030303030303020202020202020202020202020202030302020202030202020202020

###### Parsed Message [0220]:

DE-2 [100194868736654]

DE-3 [000000]

DE-4 [000000050000]

DE-6 [000000050100]

DE-7 [0122133357]

DE-10 [61002000]

DE-11 [016375]

DE-12 [183357]

DE-13 [0122]

DE-15 [0122]

DE-18 [5541]

DE-22 [902]

DE-25 [00]

DE-26 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016375] DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR ]

DE-43 [ACQUIRER NAME CITY NAME CAUSA] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA ]

DE-102 [100194868736654]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0 ]

##### Response Message [0230] (represented in Hex):

01CE30323330F67A00910EC0A40A00000000040200003135313030313934383638373336363534303030

30303030303030303030353030303030303030303030353031303030313232313333333537363130303230

30303031363337353138333335373031323230313232303044303030303030303030363030303030303830

3232313330313633373530303132343535315445524D4944303143415244204143434550544F5220203834

30383430303230303037323834304430303030303030303031303030313630303030303030303034303230

30303030373030303032202020203132333435363132333435363132332020202020202020202020302020

20202020202020202020202020202020202020202056495341202020202020202031353130303139343836

38373336363534313534203132333435363132333435363132332020202020303020202020202020202020



20202020202020202020202020202020303030303030203030303030303030303020303030303030303030

30303020202020203030303030303030303020202020202020202020202030303032303030303030303030

3030303030303020202020202020202020202020202030302020202030202020202020

###### Parsed Message [0230]:

DE-2 [100194868736654]

DE-3 [000000]

DE-4 [000000050000]

DE-6 [000000050100]

DE-7 [0122133357]

DE-10 [61002000]

DE-11 [016375]

DE-12 [183357]

DE-13 [0122]

DE-15 [0122]

DE-25 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016375]

DE-38 [001245]

DE-39 [51]

DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR ] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA ]

DE-102 [100194868736654]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0 ]



#### Sample Reversal Request/Response Messages (0420, 0430)

##### Request Message [0420] (represented in Hex):

01FA30343230F67A44910AE0A40A000000000402000031353130303139343836383733363736383030303

03030303030303030303230303030303030303030303230313030303132323133343434333631303035303

03030313633383031383434343330313232303132323535343139303230304430303030303030303036303

03030303038303232313330313633383030305445524D4944303143415244204143434550544F522020414

3515549524552204E414D4520202020202020202020202043495459204E414D4520202020434155534138

34303834303032303030373238343044303030303030303030313030303136303030303030303030343032

30303030303730303030322020202031323334353631323334353631323320202020202020202020203020

20202020202020202020202020202020202020202020564953412020202020202020313531303031393438

36383733363736383135342031323334353631323334353631323320202020203030202020202020202020

20202020202020202020202020202020203030303030302030303030303030303030203030303030303030

30303030202020202030303030303030303030202020202020202020202020303030323030303030303030

303030303030303020202020202020202020202020202030302020202030363836343931

###### Parsed Message [0420]:

DE-2 [100194868736768]

DE-3 [000000]

DE-4 [000000020000]

DE-6 [000000020100]

DE-7 [0122134443]

DE-10 [61005000]

DE-11 [016380]

DE-12 [184443]

DE-13 [0122]

DE-15 [0122]

DE-18 [5541]

DE-22 [902]

DE-25 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016380]

DE-39 [00]

DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR ]

DE-43 [ACQUIRER NAME CITY NAME CAUSA] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA ]

DE-102 [100194868736768]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0686491]

##### Response Message [0430] (represented in Hex):

01F930343330F67A00910EE0A40A000000000402000031353130303139343836383733363736383030303

03030303030303030303230303030303030303030303230313030303132323133343434333631303035303

03030313633383031383434343330313232303132323030443030303030303030303630303030303038303

232313330313633383030303132343530305445524D4944303143415244204143434550544F52202041435

15549524552204E414D4520202020202020202020202043495459204E414D452020202043415553413834

30383430303230303037323834304430303030303030303031303030313630303030303030303034303230

30303030373030303032202020203132333435363132333435363132332020202020202020202020302020

20202020202020202020202020202020202020202056495341202020202020202031353130303139343836



38373336373638313534203132333435363132333435363132332020202020303020202020202020202020

20202020202020202020202020202020303030303030203030303030303030303020303030303030303030

30303020202020203030303030303030303020202020202020202020202030303032303030303030303030

3030303030303020202020202020202020202020202030302020202030363836343931

###### Parsed Message [0430]:

DE-2 [100194868736768]

DE-3 [000000]

DE-4 [000000020000]

DE-6 [000000020100]

DE-7 [0122134443]

DE-10 [61005000]

DE-11 [016380]

DE-12 [184443]

DE-13 [0122]

DE-15 [0122]

DE-25 [00]

DE-28 [D00000000] DE-32 [000000]

DE-37 [802213016380]

DE-38 [001245]

DE-39 [00]

DE-41 [TERMID01]

DE-42 [CARD ACCEPTOR ]

DE-43 [ACQUIRER NAME CITY NAME CAUSA] DE-49 [840]

DE-51 [840]

DE-54 [0072840D000000000100] DE-61 [0000000004020000]

DE-63 [0002 123456123456123 0 VISA ]

DE-102 [100194868736768]

DE-111 [ 123456123456123 00 000000 0000000000 000000000000 0000000000 00020000000000000000

00 0686491]

#### Sample Token Notification Message (0620, 0320)

##### Request Message [0620] (represented in Hex):

03D230363230C22000000A000002040000000002000831353130303134313738383635323631353038323

93132353834343031323630363632343231323031323630363030303730303030322020202020202020202

02020202020202020202020202020202020202020302020202020202020202020202020202020202020202

02056495341202020202020202038393033323320303030303030303030303030303030202020202030302

02020202020202020202020202020202020202020202020202030303030303020303030303030303030302

03030303030303030303030302020202020303030303030303030302020202020202020202020203030303

23337313130303030303030303030303020202020202020202020202020205A30302020202030202020202

02031323334353637383931323334353637383931323334353637383931323334353637383931323334353

637383931323320202020202020202020202020202020353535353030303030303030303030693263204D6 F62696C65202020202020202020203031343036333237313132373030303131383030305A5A4130343330 30202020202020202030303030303030303030202020202020202020202020202020202020203030303035

30360200590220F1F2F3F4F5F6F7F8F9F1F2F3F4F5F6F7F8F9F1F2F3F4F5F6F7F8F9F1F2F3F4F50706F

0F5F0F9F0C30601F30920F7F8F9F7F8F9F7F9F8F7F7F8F9F7F8F9F7F9F8F7F7F8F9F7F8F9F7F9F8F7F

7F80301F70802F0F10A01F80100730203C5D5C7070EF5F54BF2F5F54BF2F5F54BF2F5F50404F5F5F5F

50B01F206084EF3F76160F1F2F10102F0F10901F70330F1F2F3F4F5F6F7F8F9F1F2F3F4F5F6F7F8F9F1 F2F3F4F5F6F7F8F9F1F2F3F4F5F6F7F8F9F1F2F3F4F5F6F7F8F9F1F2F30801F50A01F8050A89F28340 D496828993856800DE0202F2F21F3102F7F21D02F4F41B0CF7F7F7F7F7F7F7F7F7F7F7F71401F40702 E9E91F3203F6F0F01F3305F1F0F0F0F00409F0F0F0F0F0F0F0F0F01102F8F80B19E56060F0F0F0F0F0F 0F0F0F0F0F0F0F0F0F0F0F1F2F3F4F5F60604F2F3F1F20110F4F0F6F3F2F7F1F1F2F7F0F0F0F1F1F813

01F20C20F0F1F2F3F4F5F6F7F8F9F0F1F2F3F4F5F6F7F8F9F0F1F2F3F4F5F6F7F8F9F0F1030BF4F0F0 F0F0F0F0F0F0F5F50801C11001F90A01F01C02F5F51A06F6F6F6F6F6F61201F30520F1F2F3F4F5F6F7 F8F9F1F2F3F4F5F6F7F8F9F1F2F3F4F5F6F7F8F9F1F2F3F4F5400044021AD496956B40F0F740D683A3 40F2F0F2F040F1F07AF2F57AF2F1F70126E38889A2C689859384E6899393C39695A3818995E3859994A

2C19584C396958489A3899695A2

##### Request Message [0302] (represented in Hex):

01D130333032C2200000080000020000000000020000313635333837353731303030303034363939303833

30313633383539393731303034366465763136393731303034303730303030322020202020202020202020

20202020202020202020202020202020202020302020202020202020202020202020202020202020202020

56495341202020202020202033323320303030303030303030303030303030202020202030302020202020

20202020202020202020202020202020202020202030303030303020303030303030303030302030303030

30303030303030302020202020303030303030303030302020202020202020202020203030303230303030

30303030303030303030303020202020202020202020202020202030302020202030202020202020202020

20202020202020202020202020202020202020202020202020202020202020202020202020202020202020

20202020202020202020202020202020202030303030303030303030303030303020202020202020202020

20202020202020202020202030303030303030303030303030303030303030202020303030303020202020

20202020303030303030303030303435323031303939303030303030313920202032303132

#### Sample DE-111 – Additional Data

##### Sample DE-111 (Fixed Format) for Visa

325Y0000000000000010000H0700000000000000000000000000000000000000000000000000000000A00 D 01234567890000000000A 0002000090011234567800000000000000000101S0 000000000000000

00000 0000000000 00000

##### Sample DE-111 for MasterCard

767Z400502010 0103210 0101102010031300112345678900412000000000010 00000000000000MD

0000010101 010000000 C01 N52001 YA000 000000123456 0679847 000000000000000 00000

0000000000 0000

**Data Element 80 Dispute Action Information Tag 05 Decline Reasons**

|  |  |  |
| --- | --- | --- |
| **Reject Reason ID** | **Reject Reason Title** | **Reject Reason Description** |
| **1** | Authenticated via OTP (UCAF) | The disputed transaction(s) was/were authenticated via OTP, indicating the transactions were validated from profile registered phone number or email  address |
| **2** | Authenticated via CHIP | The disputed transaction(s) was/were authenticated  with CHIP, indicating your card was physically used to perform these disputed transactions |
| **3** | Authenticated via CHIP & PIN | The disputed transaction(s) was/were authenticated with CHIP and PIN or Chip read transactions indicating your card was physically used to perform  disputed transaction(s) |
| **4** | CVV Code Used | The disputed transaction(s) was/were authenticated with CVV code indicating your card information was  used to perform disputed transaction(s) |
| **5** | Web Account Created After OTP Authentication | The web account was created after authentication with OTP indicating the account creation was validated from profile registered phone number or  email address |
| **6** | No Balance Inquiry | No Balance Inquiry was observed prior to disputed  charge |
| **7** | No Decline/Bad PIN | No Decline/Bad PIN was observed prior to disputed  charge |
| **8** | No PIN Reset | No Reset PIN was observed prior to disputed  charge |
| **9** | No NSF Declines | No NSF was observed after the disputed charge |
| **10** | No Declines after Card Reported | No declined transactions observed after the card  was reported |
| **11** | No Declines after Card Reissue Request | No declined transactions observed after the card re-  issue request was initiated |
| **12** | PIN Authenticated via Registered  Phone/Email | Reset/Setup PIN was authenticated from profile  registered phone number or email address |
| **13** | Trans Reviewed by CH through Web | The transaction(s) & other details were reviewed by cardholder through Web Account in disputed date  range |
| **14** | Trans Reviewed by CH through Mobile | The transaction(s) & other details were reviewed by cardholder through Mobile App in disputed date  range |
| **15** | Trans Reviewed by CH through IVR | The transactions & other details were reviewed by  cardholder through IVR in disputed date range |
| **16** | Disputed Trans made on DD Date | The disputed transaction(s) were made on the same  day the Direct Deposit was received |
| **17** | Valid Presentment Received | The re-presentment document(s) received from the merchant was/were reviewed and found valid to  decline this dispute |
| **18** | ATM Provided Proof | The ATM provided proof of successful withdrawal(s) |
| **19** | Merch Successfully Delivered | The services/merchandise were successfully  delivered to the profile address |
| **20** | Merchant History | The account history has non-disputed transaction(s) |

|  |  |  |
| --- | --- | --- |
|  |  | of the same merchant that were made prior to the  disputed transaction(s) |
| **21** | Family Fraud | A potential Family Fraud case according to the  information analyzed in the merchant documents |
| **22** | Normal Spending Trend | The recent spending trend on the card is observed  as normal |
| **23** | PIN Changed with Registered Phone | The same phone number which is available on  cardholder profile was used to change PIN |
| **24** | Merch Docs have Same Last Name | The merchant re-presentment document(s) show  the same last name which is on cardholder profile |
| **25** | Reported After 120 Days | The disputed transaction(s) are reported after 120  days of transaction date(s) |
| **26** | Trans made within 7-mile Radius | The disputed transaction(s) were made within 7-mile  radius from the profile address |
| **27** | Cancel by Cardholder | The cardholder himself/herself called the customer support and requested for cancellation of reported  dispute. |
| **28** | Credit Issued by Merchant/Credit  Adjustment by Merchant | The merchant has issued the credit and no further  action required for reported dispute. |
| **29** | No Chargeback Rights | No Chargeback Rights |
| **30** | Valid Document Received (via email) | The merchant has sent documentation via email/fax  to show proof of charge |
| **31** | Card Activated via Registered Phone | The card was activated using the registered number  on the account |
| **32** | Card Still in Use (Lost/Stolen) | The card is reported as lost/stolen but is still in use |
| **33** | AVS Match | The Address on the merchant documents is a full  match to the registered address |
| **34** | Cancellation of Services Failed | Based on merchant documents cancellation of the  product/service was failed |
| **35** | The card in Possession not Lost/Stolen | The card has not been reported as lost/stolen and is  in possession |
| **36** | No Evidence of Double Charge | No evidence of a double charge is observed |
| **37** | Cardholder Unauthorized Dispute  Pattern | A pattern of multiple Unauthorized disputes filed is  observed |
| **38** | Additional CP Transaction not Disputed  (Lost/Stolen) | There are additional card present transactions in the  same time frame that are left undisputed |
| **39** | Claim Filed in Error | The dispute was incorrectly filed |
| **40** | Friendly Fraud | A potential Friendly Fraud case according to the  information analyzed |

## Appendix E – Possible Values of New Sub-fields in DE-111

#### Stand In Trans Indicator

* 0 (Default Value)
* 1 (AuthHost Timed Out)
* 2 (AuthHost Down)

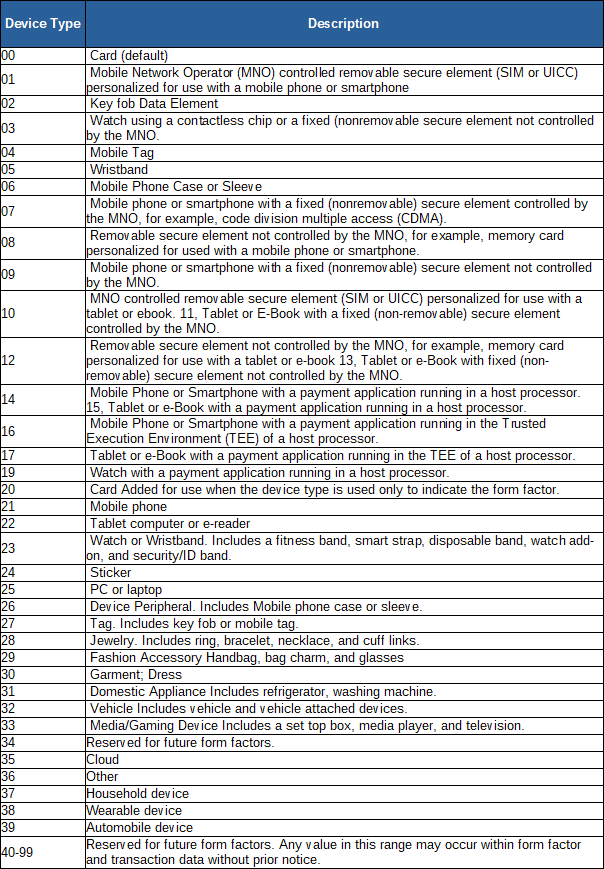
#### Token Type

* 01 (ECOM/COF- E-Commerce/Card-on-File)
* 02 (Secure Element)
* 03 (Cloud-Based Payment)
* 05 (E-Commerce Enabler)

#### Token Status

* B (Active for payment)
* I (Inactive for payment (not yet active))
* S (Temporarily suspended for payments)
* F (Permanently deactivated for payments)
* D (Discard for payment)

#### Token Device Type



#### Token Authorization Request Indicator

* 0 (Not a TAR Request)
* 1 (TAR Request)

#### Token Notification Type

* 4300 (Token Completion Notification: Green Path)
* 4301 (Token Completion Notification: Yellow Path)
* 4302 (Token Completion Notification: Yellow Path Call Center)
* 4304 (Token Completion Notification: Red Path)
* 4305 (Token Creation Only Notification)
* 4401 (Token Event Notification: Deactivate Token)
* 4402 (Token Event Notification: Suspend Token)
* 4403 (Token Event Notification: Resume Token)
* 4306 (Token Event Notification: Token Data Update / Token Expiration Update)
* 4307 (Token Event Notification: Exception / Invalid OTP)

#### Chargeback Flag (Data Element 111.45)

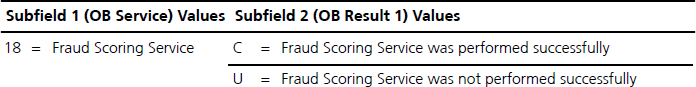
* 0 Chargeback Transaction
* 1 Chargeback Cancellation Transaction
* 2 Representment Transaction
* 3 Representment Reversal Transaction
* 4 2nd Chargeback Transaction
* 5 2nd Chargeback Cancellation Transaction
* 6 Arbitration Transaction
* 7 Arbitration Reversal Transaction
* 8 Chargeback Preauth Transaction
* 9 2nd Chargeback Preauth Transaction
* A Chargeback Preauth Cancellation Transaction
* B 2nd Chargeback Preauth Cancellation Transaction
* C Chargeback Special Adjustment Transaction
* D Chargeback Adjustment
* E Chargeback Adjustment Reversal

##### On-behalf Service (Data Element 111.46)

Data Element 111.46 is mapped to Mastercard Data Element 48, Sub-element 71. This sub-element identifies the type of Mastercard on-behalf service performed on the transaction. There are 3 sub-fields of this sub-element.

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Field Name** | **Subfield Length** | **Description** |
| 1 | On-behalf Service Indicator | 2 | It contains the on-behalf service indicator. (see below the list of possible on-behalf service indicators) |
| 2 | On-behalf Result 1 | 1 | It indicates the results of the service processing. |
| 3 | On-behalf Result 2 | 1 | It contains the on-behalf result 2 indicator value. |

Below are the possible results for Fraud Scoring On-behalf Service:



##### Fraud Scoring Data (Data Element 111.47)

Data Element 111.47 is mapped to Mastercard Data Element 48, Subelement 75. Mastercard fraud scoring solution provides customers & issuers an opportunity to enroll in Expert Monitoring Real time Fraud Scoring Service & Fraud Rules Manager respectively to assess the fraud scoring of a financial transactions.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Field Name** | **Subfield ID** | **Subfield Length** | **Description** |
| 1 | Fraud Assessment Score | 01 | 03 | Fraud Scoring System provides the risk score of 000-999 where 000 indicates the least likely fraudulent transaction and 999 indicates the most likely fraudulent transaction. |
| 2 | Score Reason Code | 02 | 02 | Fraud Scoring System provides the Score Reason Code, an alphanumeric code identifying the data used to derive the fraud score.  **Score | Reason Code Description XX** | Suspicious transaction   1. | Four or more swiped transactions on a self- service terminal in the past two days 2. | Suspicious activity during the past three days |
| 3 | Rules Score | 03 | 03 | Fraud Rule Manager Service provides the rule adjusted score of 000–999, where 000 indicates the least likely fraudulent transaction and 999 indicates the most likely fraudulent transaction. |
| 4 | Rule Reason Code 1 | 04 | 02 | Fraud Rule Manager Service provides the Rule Reason Code, an alphanumeric code that identifies the data used to derive the Rule Adjusted Score. |
| 5 | Rule Reason Code 2 | 05 | 02 | Fraud Rule Manager Service provides the Rule Reason Code, an alphanumeric code that identifies the data used to derive the Rule Adjusted Score. |

Data received in this field will be in TLV (Tag-Length-Value) format. Sample data: 0103049020208

This will be parsed as follows: Tag:01, Length:03, Value: 049 Tag:02, Length:02, Value: 08

## Appendix F – Token Activation / OTP Notification Message Identification

Token Activation / OTP Notification message can be identified with following fields, in addition to OTP code in DE 111:

MTI = 0120, Filed 32 = 746922, Field 41 = 11111111, Field 42 = 111111111111111.

## Appendix G – Token Provisioning – Send OTP Request

Administrative request (Token Provisioning – Send OTP) Request message will contain following mandatory information:

MTI = 0600

Field 02 = PRIMARY ACCOUNT NUMBER Field 07 = LOCAL TRANSMISSION DATE TIME

Field 18 = 7299

Field 22 = 01

Field 25 = 66

Field 32 = 746922

Field 41 = 11111111

Field 42 = 111111111111111

Field 63 = VISA [switchType at position 59 –> total length 70]

Field 111 = Contains OTP, OTP Expiry DateTime, Cardholder Verification Method Identifier & Value OTP Expiry Date Time (Value will be in GMT)

Expected response codes in DE39 in response. Success = 00

Format Error = 30 Transaction not allowed = 57 System malfunction = 96 Refer to Card Issuer = 01

## Appendix H – Token Transactions Flow

|  |
| --- |
| **Token Messages** |
| Message with **MTI 0100** with **TAR** indicator in DE 111. |
| **Token Activation Message** with **MTI 0120** with Access Code (OTP) and Code Expiry in DE 111. [Optional only if TAR qualifies for yellow path] |
| **Token Complete Notification** with MTI 0620 with indication in DE 111. Token Notification Type with following values:  4300 (Green Path)  4301 (Yellow Path OTP)  4302 (Yellow Path Call Center) 4304 (Red Path)  4305 (Token Creation Only) |
| **Token Event Notification** with MTI 0620 with indication in DE 111. Token Notification Type with following values:  4401 (Token Deactivate F) 4402 (Token Suspend S) 4403 (Token Resume B)  4306 (Token Data Update / Token Expiration Update) |
| PAN replacement message (in case of PAN reissued with new number) with MTI 0302 with indication in DE 111.  Replacement PAN (New PAN)  Replacement PAN Expiration Date |

## Appendix I – Token Creation Green/Red/Yellow Path Identification from Issue Perspective

##### Green Path:

TAR Message with DE 39 = 00.

##### Yellow Path:

TAR Message with DE 39 = 85.

##### Red Path:

TAR Message with DE 39 = 05.

## Appendix J – Message Type Identifiers

|  |  |
| --- | --- |
| **MTI** | **Description** |
| 0100 | Authorization Request |
| 0110 | Authorization Response |
| 0100 | Token Provisioning – Send OTP Request |
| 0110 | Token Provisioning – Send OTP Response |
| 0120 | Token OTP Notification |
| 0130 | Token OTP Notification Response |
| 0120 | Advice Authorization Request |
| 0130 | Authorization Advice Response |
| 0200 | Financial Transaction Request |
| 0210 | Financial Transaction Response |
| 0220 | Financial Transaction Advice |
| 0230 | Financial Transaction Response |
| 0302 | File Update Request |
| 0312 | File Update Request Response |
| 0420 | Reversal Advice |
| 0430 | Reversal Advice Response |
| 0600 | Administrative Request |
| 0620 | Administrative Advice |
| 0630 | Administrative Advice Response |
| 0800 | Network Management Request (Mandatory for TCP/IP Communication) |
| 0810 | Network Management Response (Mandatory for TCP/IP Communication) |

100 Redwood Shores Parkway, Suite 100, Redwood City, CA 94065 +1-650-593-5400 | [connect@i2cinc.com](mailto:connect@i2cinc.com) [www.i2cinc.com](http://www.i2cinc.com/)

## Appendix K – Anticipated Amount Transaction

Anticipated amount verification transactions are Account verification transactions with anticipated amount which is used to confirm the account has availability to accept purchases.

Host which are system of records or have balance maintained at their end must confirm the anticipated amount, and sending the appropriate response code. Host must not hold funds during the processing of an anticipated amount verification transaction.

A new amount type code 44 is used to identify anticipated amounts in Field 54.

When both the account and anticipated amount are validated by the host, the response message will contain the existing value of 00 (Approved) in Field 39—Response Code.

When only the account is validated, the response message will contain one of the following values in Field 39—Response Code:

* 85 (Approved – Account Verification)
* X6 (Valid account but amount not supported) Anticipated Amount verification transactions Identification:
* A 0100 Account verification request
* Field 4—Amount, Transaction contains all zeros
* Field 25—Point-of-Service Condition Code contains the existing value of **62** (Account Verification w/o Auth; product eligibility inquiry without authorization)
* Field 54—Additional Amounts contains an anticipated amount type code.
* Field 63.7 = “VISA”.