

ISO 8583 is a widely used international standard for the interchange of electronic financial transaction messages, particularly for card-based payments (credit, debit, ATM). It defines a message format that allows various systems (POS terminals, ATMs, payment processors, banks) to communicate effectively and securely.

An ISO 8583 message is generally composed of three main parts:

1. **Message Type Indicator (MTI):** This is a four-digit numeric code that defines the overall purpose and function of the message. It indicates:
 - **Version of ISO 8583:** (e.g., 1987, 1993, 2003)
 - **Message Class:** (e.g., authorization, financial transaction, administrative)
 - **Message Function:** (e.g., request, response, advice)
 - **Message Origin:** (e.g., acquirer, issuer, network)
2. **Bitmaps:** These are indicators of which data elements are present in the current message.
 - **Primary Bitmap:** A 64-bit field (or 8-byte packed) that indicates the presence of data elements 1-64.
 - **Secondary Bitmap:** If present, indicated by the first bit of the primary bitmap, it's another 64-bit field for data elements 65-128.
 - **Tertiary Bitmap:** Less commonly used, it would indicate data elements 129-192.
3. **Data Elements (DEs):** These are the actual fields that contain the detailed transaction information. ISO 8583 defines up to 128 primary data elements (and 192 in extended versions), though not all are used in every transaction. Each data element has a defined format (e.g., numeric, alphanumeric, binary) and length (fixed or variable).

Here are some of the *key and commonly used* ISO 8583 Data Elements:

- **DE 2: Primary Account Number (PAN):** The cardholder's account number (e.g., credit card number).
- **DE 3: Processing Code:** Defines the type of transaction being performed (e.g., purchase, cash advance, refund, balance inquiry). This is typically a 6-digit code.
- **DE 4: Transaction Amount:** The monetary value of the transaction.
- **DE 7: Transmission Date and Time:** The date and time when the message was transmitted.

- **DE 11: System Trace Audit Number (STAN):** A unique number assigned by the originating system to identify the transaction.
- **DE 12: Local Transaction Time:** The time of the transaction at the terminal/point of sale.
- **DE 13: Local Transaction Date:** The date of the transaction at the terminal/point of sale.
- **DE 15: Settlement Date:** The date when the transaction is expected to be settled.
- **DE 22: Point of Service (POS) Entry Mode:** Indicates how the card data was captured (e.g., magnetic stripe, EMV chip, manual entry).
- **DE 32: Acquiring Institution Identification Code:** Identifies the financial institution that initiated the transaction (the acquirer).
- **DE 37: Retrieval Reference Number:** A unique reference number for the transaction, often used for reconciliation.
- **DE 38: Authorization Identification Response:** The authorization code returned by the issuer for an approved transaction.
- **DE 39: Response Code:** A crucial field indicating the status of the transaction (e.g., "00" for approved, "05" for declined, "51" for insufficient funds).
- **DE 41: Card Acceptor Terminal Identification:** Identifies the terminal where the transaction took place.
- **DE 42: Card Acceptor ID Code:** Identifies the merchant or location where the card was accepted.
- **DE 43: Card Acceptor Name/Location:** The name and location of the merchant.
- **DE 49: Currency Code, Transaction:** The currency of the transaction amount.
- **DE 52: Personal Identification Number (PIN) Data:** Encrypted PIN block if a PIN was entered.
- **DE 53: Security Related Control Information:** Contains various security elements, including encryption details.
- **DE 54: Additional Amounts:** Used for cashback amounts, original amounts in reversals, etc.
- **DE 55: Integrated Circuit Card (ICC) Data (EMV Data):** Contains EMV-specific data for chip card transactions.

- **DE 60: Reserved for National Use (often for transaction-specific data):** Used by national networks for specific purposes (e.g., batch number, transaction type extension).
- **DE 61: Reserved for National Use (often for original transaction data):** Similar to DE 60, but often used to carry data from the original transaction for reversals or follow-ups.
- **DE 62: Reserved for Private Use:** Can be used for custom data by specific implementations.
- **DE 102/103: Account Identification 1/2:** Used for source and destination account numbers in fund transfers.

It's important to note that while ISO 8583 provides a standard framework, different payment networks and financial institutions often have their own variations and specific usage of these data elements, along with their own proprietary data elements within the "private use" fields. Therefore, detailed specifications are usually required when implementing ISO 8583 for a particular system or network.

Sources

explain Each data element with example

You're asking for a detailed explanation of each key ISO 8583 data element, along with examples. This is a comprehensive request, so let's break down the most commonly used and important data elements.

Keep in mind that the *exact* format and content of each data element can vary slightly depending on the specific version of ISO 8583 (e.g., 1987, 1993, 2003) and the particular network's implementation. However, the core purpose remains consistent.

Let's begin with the Message Type Indicator (MTI) and Bitmaps, as they precede the Data Elements.

Message Type Indicator (MTI)

The MTI is a 4-digit numeric field that sets the context for the entire message.

Format: NNNN (4 numeric digits)

Example: 0100

Breakdown of the MTI (e.g., for 0100):

- **First Digit (Version):**
 - 0xxx: ISO 8583:1987

- 1xxx: ISO 8583:1993
- 2xxx: ISO 8583:2003
- *Example:* 0 means ISO 8583:1987 standard.
- **Second Digit (Message Class):** Defines the general purpose.
 - x1xx: Authorization (e.g., purchase, refund request)
 - x2xx: Financial (e.g., actual funds movement like a cash withdrawal, goods/services purchase)
 - x3xx: File Actions (e.g., batch upload/download)
 - x4xx: Reversal/Chargeback
 - x8xx: Network Management (e.g., logon, key exchange)
 - *Example:* 1 means an Authorization message.
- **Third Digit (Message Function):** Defines the specific action.
 - xx0x: Request (e.g., "I want to authorize this transaction")
 - xx1x: Request Response (e.g., "The authorization request was approved/declined")
 - xx2x: Advice (e.g., "This transaction happened, please update your records")
 - xx3x: Advice Response
 - *Example:* 0 means it's a Request.
- **Fourth Digit (Message Origin/Originator):** Indicates who originated the message.
 - xxx0: Acquirer (Point of Sale/ATM initiating the transaction)
 - xxx1: Issuer (Bank holding the cardholder's account)
 - xxx2: Card Acceptor
 - xxx5: Interchange/Network
 - *Example:* 0 means it's an Acquirer message.

Common MTI Examples:

- **0100:** Authorization Request (e.g., a merchant requests approval for a credit card purchase).

- **0110:** Authorization Request Response (e.g., the issuer responds with "approved" or "declined").
 - **0200:** Financial Transaction Request (e.g., an ATM cash withdrawal request, where funds are immediately disbursed).
 - **0210:** Financial Transaction Request Response.
 - **0400:** Reversal Request (e.g., canceling a previous authorization).
 - **0410:** Reversal Request Response.
 - **0800:** Network Management Request (e.g., a terminal sending a "logon" message to the host).
 - **0810:** Network Management Request Response.
-

Bitmaps (Primary, Secondary, Tertiary)

Bitmaps are essential because they tell the receiving system *which* data elements are present in the message. This makes the message flexible and avoids sending empty fields.

- **Primary Bitmap (DE 1):** Always present. It's an 8-byte (64-bit) field. Each bit corresponds to a data element from 1 to 64. If the bit is '1', the corresponding data element is present. If '0', it's absent.
- **Secondary Bitmap (DE 65):** If the first bit (bit 1) of the Primary Bitmap is '1', then a Secondary Bitmap is present. This is another 8-byte field that indicates the presence of data elements from 65 to 128.
- **Tertiary Bitmap (DE 129):** Less common. If bit 1 of the Secondary Bitmap is '1', a Tertiary Bitmap (for DEs 129-192) is present.

Format: Binary (often transmitted as hexadecimal characters). Each '1' bit indicates presence, '0' indicates absence.

Example: Let's say the Primary Bitmap (raw hex) is 7000000000000000.

To decode this: 70 in binary is 0111 0000. 00 in binary is 0000 0000. ...and so on for the remaining 6 bytes.

If we look at 0111 0000:

- Bit 1: 0 (DE 1 - Secondary Bitmap - Absent)
- Bit 2: 1 (DE 2 - Primary Account Number - Present)
- Bit 3: 1 (DE 3 - Processing Code - Present)

- Bit 4: 1 (DE 4 - Amount, Transaction - Present)
- Bit 5-8: 0 (DE 5-8 - Absent)

So, this bitmap indicates that DEs 2, 3, and 4 are present in the message.

Key ISO 8583 Data Elements (with Examples)

Here's a breakdown of commonly used data elements:

DE 2: Primary Account Number (PAN)

- **Description:** The cardholder's account number (e.g., credit card, debit card number).
- **Format:** Up to 19 digits. Variable length (LLVAR - Length indicator followed by variable data). The length indicator is usually 2 digits.
- **Example:** 1643123456789012345 (16-digit card number prefixed by '16' for length) or just the raw 4312345678901234. (The length encoding LLVAR means the actual data sent would be 164312345678901234).

DE 3: Processing Code

- **Description:** A 6-digit code defining the type of transaction. The first two digits specify the transaction type, the next two the account type from, and the last two the account type to.
- **Format:** N6 (6 numeric digits)
- **Examples:**
 - 000000: Purchase (from default account to default account)
 - 010000: Cash Advance
 - 200000: Refund/Credit
 - 300000: Balance Inquiry
 - 001000: Purchase from Savings
 - 000010: Purchase to Credit Card

DE 4: Amount, Transaction

- **Description:** The monetary value of the transaction. Usually implicitly decimal (e.g., 2 decimal places).
- **Format:** N12 (12 numeric digits, right-justified, zero-filled).

- **Example:**
 - For \$12.50: 000000001250
 - For \$100.00: 000000010000

DE 5: Amount, Settlement

- **Description:** The amount of the transaction in the settlement currency. This might differ from DE 4 if currency conversion occurs.
- **Format:** N12
- **Example:** If a USD transaction of \$100 is settled in EUR at an exchange rate, this might be 000000008500 (for 85.00 EUR).

DE 6: Amount, Cardholder Billing

- **Description:** The amount charged to the cardholder's account in their billing currency.
- **Format:** N12
- **Example:** If a USD transaction of \$100 is charged to a UK cardholder, this might be 000000007500 (for 75.00 GBP).

DE 7: Transmission Date and Time

- **Description:** The date and time when the message was transmitted to the next host, in Coordinated Universal Time (UTC/GMT).
- **Format:** N10 (MMDDhhmmss - Month, Day, Hour, Minute, Second)
- **Example:** 0716173609 (July 16, 17:36:09)

DE 11: System Trace Audit Number (STAN)

- **Description:** A unique sequential number assigned by the originating system to identify a transaction from its inception to completion. It's crucial for matching requests with responses and for reconciliation.
- **Format:** N6 (6 numeric digits)
- **Example:** 000123, 123456

DE 12: Time, Local Transaction

- **Description:** The time the transaction occurred at the Point of Sale (POS) terminal or ATM.
- **Format:** N6 (hhmmss - Hour, Minute, Second)

- **Example:** 173000 (5:30:00 PM)

DE 13: Date, Local Transaction

- **Description:** The date the transaction occurred at the POS terminal or ATM.
- **Format:** N4 (MMDD - Month, Day)
- **Example:** 0716 (July 16)

DE 15: Date, Settlement

- **Description:** The date when the transaction is expected to be settled (funds actually transferred between institutions).
- **Format:** N4 (MMDD)
- **Example:** 0717 (July 17, for settlement the next day)

DE 18: Merchant Type

- **Description:** A 4-digit code identifying the category of the merchant (Merchant Category Code - MCC).
- **Format:** N4
- **Example:** 5411 (Supermarkets), 5812 (Restaurants), 4111 (Local Commuter Transport)

DE 22: Point of Service (POS) Entry Mode

- **Description:** A 2 or 3-digit code indicating how the cardholder's account number and PIN were captured at the POS.
- **Format:** N2 or N3
- **Examples:**
 - 01: Manual Entry
 - 02: Magnetic Stripe Read
 - 05: EMV Chip Read (online)
 - 07: Contactless Chip
 - 90: Magnetic Stripe (ISO track 1/2) - for 1987 version usually
 - 91: Integrated Circuit Card (ICC) - for 1987 version usually

DE 25: Point of Service (POS) Condition Code

- **Description:** A 2-digit code describing the conditions under which the transaction took place.
- **Format:** N2
- **Examples:**
 - 00: Normal transaction
 - 01: Card present, PIN required
 - 06: Card not present, mail/telephone order
 - 08: Cardholder present, unattended terminal

DE 32: Acquiring Institution Identification Code

- **Description:** Identifies the financial institution that owns the POS terminal or ATM (the acquirer). Usually, the bank identification number (BIN).
- **Format:** LLVAR up to N11 (2-digit length + up to 11 numeric digits)
- **Example:** 06123456 (6-digit BIN prefixed by '06' for length)

DE 37: Retrieval Reference Number

- **Description:** A unique transaction identifier generated by the acquirer/terminal for tracking and retrieval. Often includes date/time or STAN.
- **Format:** AN12 (12 alphanumeric characters)
- **Example:** 519712345678 (where 5197 might be date/time and 12345678 a sequence)

DE 38: Authorization Identification Response

- **Description:** The authorization code returned by the issuer for an approved transaction. This is the crucial approval code.
- **Format:** AN6 (6 alphanumeric characters)
- **Example:** A1B2C3, 001234, APPROVED

DE 39: Response Code

- **Description:** A 2-digit (or 3-digit) code indicating the disposition of a transaction (approved, declined, error, etc.). This is *the* most important field for understanding the outcome.
- **Format:** AN2 or AN3
- **Examples (Common):**

- 00: Approved
- 01: Refer to Card Issuer
- 05: Do Not Honor (Generic decline)
- 12: Invalid Transaction
- 14: Invalid Card Number
- 41: Lost Card, Pick Up
- 51: Insufficient Funds
- 54: Expired Card
- 62: Invalid Transaction (often for invalid processing code)
- 91: Issuer or Switch Inoperative

DE 41: Card Acceptor Terminal Identification

- **Description:** A unique identifier for the specific POS terminal or ATM where the transaction occurred.
- **Format:** ANS8 (8 alphanumeric and special characters)
- **Example:** POS00001, ATM_CHENNA

DE 42: Card Acceptor Identification Code

- **Description:** Identifies the merchant or organization that owns the terminal. This is often the merchant ID.
- **Format:** ANS15 (15 alphanumeric and special characters)
- **Example:** ABCSTORE1234567, MYHOTEL00000001

DE 43: Card Acceptor Name/Location

- **Description:** The name and location of the merchant or card acceptor, typically printed on receipts.
- **Format:** ANS40 or ANS99 (variable length up to 40 or 99 characters).
- **Example:** STARBUCKS COFFEE NEW YORK NY

DE 48: Additional Data - Private Use / Reserved

- **Description:** A variable-length field often used by networks for specific data elements not covered by other ISO fields. Can contain sub-elements.
- **Format:** LLLVAR (3-digit length indicator + variable data).

- **Example:** Could contain loyalty points, merchant-specific discount codes, etc. The content is highly proprietary.

DE 49: Currency Code, Transaction

- **Description:** The numeric ISO 4217 currency code for the transaction amount (DE 4).
- **Format:** N3 (3 numeric digits)
- **Examples:**
 - 840: USD (United States Dollar)
 - 978: EUR (Euro)
 - 356: INR (Indian Rupee)

DE 52: Personal Identification Number (PIN) Data

- **Description:** The encrypted PIN block entered by the cardholder. This is always encrypted using strong cryptographic methods.
- **Format:** B8 (8 bytes binary data, often represented as 16 hex characters)
- **Example:** A1B2C3D4E5F67890 (hex representation of the encrypted PIN block)

DE 53: Security Related Control Information

- **Description:** Contains various security-related elements, such as key identifiers, encryption methods, and message authentication codes (MACs).
- **Format:** B16 (16 bytes binary data, often 32 hex characters) or LLVAR
- **Example:** This would be a complex binary structure specific to the security architecture.

DE 54: Additional Amounts

- **Description:** Used for various additional amounts related to the transaction, such as cashback amount, tip amount, original transaction amount (for reversals), fees, etc. Can contain sub-elements.
- **Format:** LLLVAR (3-digit length indicator + variable data). Typically consists of a series of fixed-length sub-fields for different amount types.
- **Example:** If a purchase was \$50 and cashback was \$20: 040C00000000002000 (hypothetical format: Type Code + Account Type + Amount)

DE 55: Integrated Circuit Card (ICC) Data - EMV Data

- **Description:** This is a critical field for EMV (chip card) transactions. It contains all the data exchanged between the card chip and the terminal during the transaction, formatted as Tag-Length-Value (TLV).
- **Format:** LLLVAR (3-digit length indicator + variable binary data)
- **Example:** 060904008000 (length 06, Tag 9F04, Length 04, Value 008000)
 - This field is highly complex and contains numerous EMV tags like 9F26 (Application Cryptogram), 9F36 (Application Transaction Counter), 95 (Terminal Verification Results), etc.

DE 60: Reserved for National Use / Transaction Specific Data

- **Description:** This field is widely used by national payment networks (e.g., Visa, Mastercard, RuPay) to carry specific transaction-related information that isn't standardized in other fields. This is often where things like batch numbers, original transaction types for reversals, or specific product codes reside. Can contain sub-elements.
- **Format:** LLLVAR (3-digit length indicator + variable data)
- **Example:** Could contain Batch Number and Transaction Sub-type.

DE 61: Reserved for National Use / Issuer Specific Data

- **Description:** Similar to DE 60, but often used for more issuer-specific data or data related to the *original* transaction in the case of follow-up messages (e.g., the original MTI, STAN, or amounts for a reversal).
- **Format:** LLLVAR
- **Example:** If it's a reversal, DE 61 might contain the MTI, STAN, and date of the original transaction.

DE 62: Reserved for Private Use / Additional Data

- **Description:** Another general-purpose field for private or proprietary data elements defined by specific institutions or networks.
- **Format:** LLLVAR
- **Example:** A bank might use this for internal customer reference numbers or specific fraud indicators.

DE 63: Reserved for Private Use / Additional Data (often for security/MACs)

- **Description:** Often used for security information, such as Message Authentication Codes (MACs) to ensure message integrity, or additional proprietary data.

- **Format:** LLLVAR
- **Example:** MAC data.

DE 102: Account Identification 1 (Source Account)

- **Description:** In fund transfer messages, this identifies the source account number.
- **Format:** LLVAR (Length indicator + variable alphanumeric data)
- **Example:** 109876543210 (10-digit account number, prefixed by '10' for length)

DE 103: Account Identification 2 (Destination Account)

- **Description:** In fund transfer messages, this identifies the destination account number.
- **Format:** LLVAR
- **Example:** 101234567890 (10-digit account number, prefixed by '10' for length)

Important Considerations:

- **Fixed vs. Variable Length:** Some fields have a fixed length (e.g., DE 3 is always 6 digits). Others are variable and indicated by a length prefix (e.g., LLVAR for 2-digit length, LLLVAR for 3-digit length).
- **Data Type:** 'N' for Numeric, 'AN' for Alphanumeric, 'ANS' for Alphanumeric Special characters, 'B' for Binary.
- **Justification and Padding:** Numeric fields are typically right-justified and zero-padded. Alphanumeric fields are usually left-justified and space-padded.
- **Network-Specific Implementations:** While the core definitions are standard, each payment network (Visa, Mastercard, Amex, RuPay, Discover, etc.) publishes its own implementation guides that detail which DEs they use, their specific formats, and any custom usage of the "reserved" fields (DE 60-63, 100+).

Understanding these key data elements is fundamental to working with and interpreting ISO 8583 messages in the financial industry.