EHI Guide (JSON version)

Version: 5.1

31 March 2026

Publication number: JSON EHI-5.1-3/31/2026

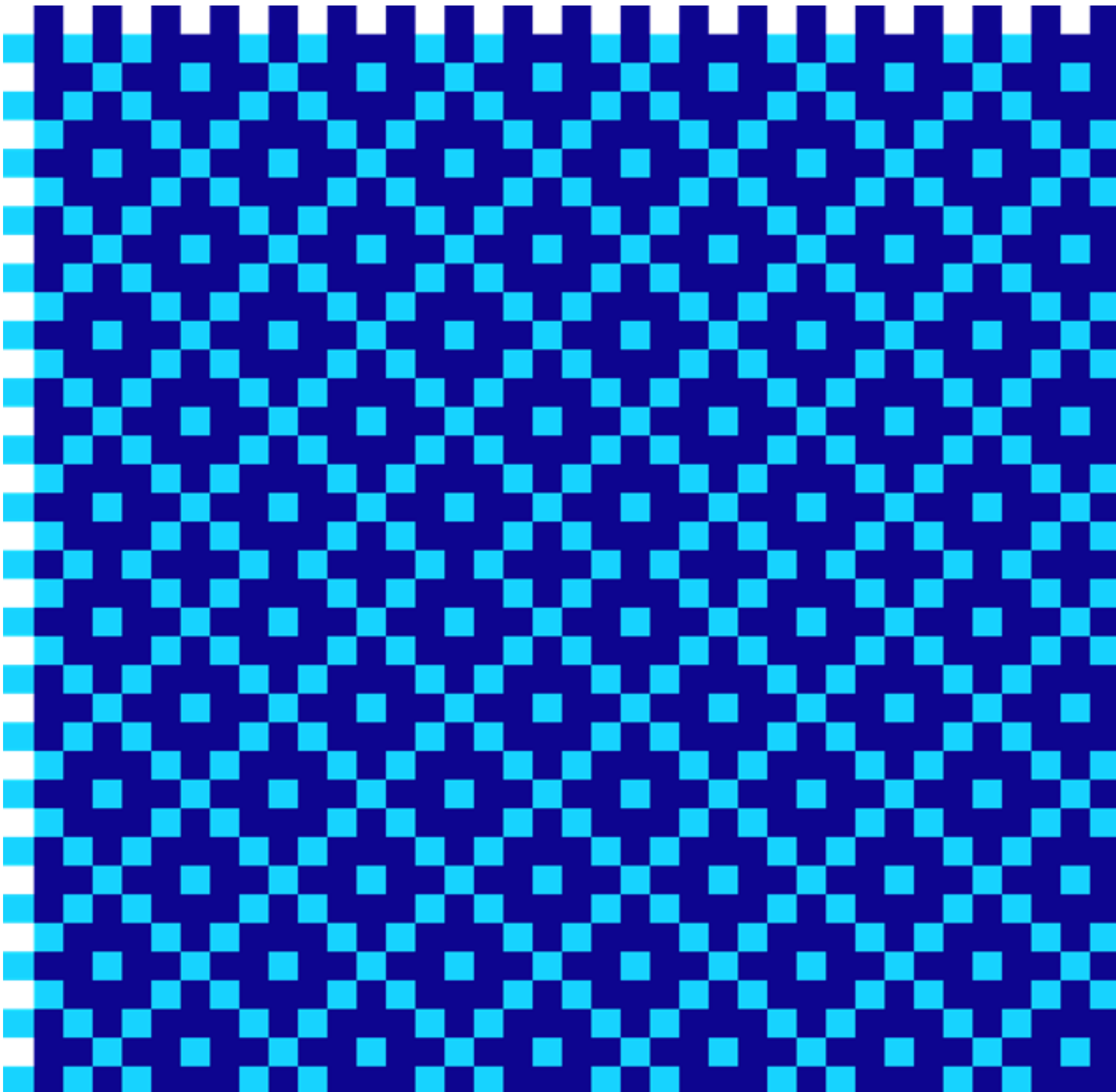
For the latest technical documentation, see the Documentation Portal.

Thredd, Kingsbourne House, 229-231 High Holborn, London, WC1V 7DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

© Thredd 2026



Copyright

© Thredd 2026

The material contained on this website is copyrighted and owned by Thredd Ltd together with any other intellectual property in such material.

The material contained in this guide is copyrighted and owned by Thredd Ltd together with any other intellectual property in such material.

Except for personal and non-commercial use, no part of this guide may be copied, republished, performed in public, broadcast, uploaded, transmitted, distributed, modified or dealt with in any manner at all, without the prior written permission of Thredd Ltd., and, then, only in such a way that the source and intellectual property rights are acknowledged.

To the maximum extent permitted by law, Thredd Ltd shall not be liable to any person or organisation, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained on this website.

To the maximum extent permitted by law, Thredd Ltd shall not be liable to any person or organisation, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained in this guide.

The information in these materials is subject to change without notice and Thredd Ltd. assumes no responsibility for any errors.

About this Guide

This guide describes the Thredd External Host Interface (EHI) and provides technical specifications on how to integrate your systems to EHI.

The guide provides details of how to receive and respond to EHI messages in JSON format.

Document Scope

You should read this guide if you are using EHI for payment transaction authorisation and/or subscription to the EHI real-time payment transaction data feed.

Target Audience

This guide is aimed at developers who need to integrate their applications to Thredd, using EHI.

What's Changed?

If you want to find out what's changed since the previous release, see the Document History section.

For a list of EHI fields available with each of the supported EHI versions, see EHI Versions.

How to use this Guide

If you are new to EHI and want to understand how EHI works, we suggest you start with following topics: Overview, EHI Operating Modes and typical Transaction Flow Scenarios. See also the other topics in the Getting Started section, including our Best Practise for Customer Implementations.

If you are an experienced EHI developer or want to find out how to process EHI messages, see Processing EHI Transactions.

To view message examples for different types of transactions, see Example Messages.

Conventions used in this Guide

When reading the tables in this guide, note the following information may be provided.

Element	Description
Usage	• **Omitted** - can be omitted (fields not included) or included with an empty value (e.g., `"Bill_Ccy": ""`) • **Optional** - can be omitted (fields not included) or included with an empty value. Can be present (e.g., `"Bill_Ccy":"0"`) • **Mandatory** - field must be present. For example: `"Bill_Ccy": "978"`
Key	The field name. Please pay particular attention to the capitalisation and spelling. Where a field name is used within text, this is formatted as in the following example: `Bill_Ccy` or `Bill_Ccy` (when used in a table note).
Data Types	The type of field data type supported. For details, including minimum and maximum lengths, see Data Types.

Related Documents

Refer to the table below for a list of other relevant documents that should be used together with this guide.

Document	Description
Web Services Guide	Provides details of the Thredd Web Services API.

Document	Description
Cards API Documentation	For customers using the Thredd REST-based Cards API, see the Cards API Docs Website.
Thredd Portal Guide	Describes how to use the Thredd Portal to manage your cards and transactions.
Smart Client Guide	Describes how to use the legacy Thredd Smart Client desktop application to manage your account.
Chargeback Guide	Describes the chargeback process and options for managing chargebacks.
Transaction XML Reporting Guide	Describes the transaction XML report sent to Program Managers.
3D Secure Guide	Describes the Thredd 3D Secure service.
Card Transaction System Guide	Describes how to submit card test transactions in the UAT environment.

Tip: For the latest technical documentation, see the Documentation Portal.

SECTION 1: GETTING STARTED

You should read this section if you are new to the ExternaL Host Interface (EHI) and want to understand how it works and how EHI is configured.

Topics covered in this section:

- About this Guide
- Overview
- EHI Operating Modes
- EHI Connection and Messages
- Card Payment Networks
- Transaction Flow Scenarios
- EHI Data Feeds
- Transaction Types
- EHI Version Control
- EHI Configuration Options
- Integration Steps

Tip: To find out how to integrate your external host system to EHI, see Processing EHI Transactions.

Tip: If you are upgrading your EHI version and want to understand what has changed, see Document History.

1.1 Overview

The External Host Interface (EHI) offers a way to exchange transactional data between the Thredd processing system and the Program Manager's externally hosted systems. All transaction data processed by Thredd is transferred to the external host system via EHI in real time. EHI provides two main functions:

- A real-time transaction notification data feed
- Payment authorisation control

Note: Thredd supports Visa, Mastercard and Discover networks, as well as smaller networks that use the Mastercard Network Exchange (MNE), such as STAR and Pulse[1] . EHI provides a single, unified message format, which enables your systems to receive and process messages using a single integration to Thredd. For more information, see Card Payment Networks.

1.1.1 Real-time Transactional Data Feed

Thredd receives global real-time card and payment-related notifications from the card schemes (Visa and Mastercard networks). These notifications are merged into a single Thredd message format which your systems can process. The real-time notifications are sent via a secure connection to the external host URL endpoint you have requested for your programme. These include notifications for: *Authorisations*, *Presentments*, *Financial* messages, *Load* and *Balance Transfers* and *Expired Cards*. For details see Transaction Types.

Your systems should respond with an acknowledgement of receipt of the message.

The EHI data feed can be used to ensure you can provide your cardholders with real-time information.

For more information on the fields and attributes included in the data feeds, see EHI Data Feeds.

Note: In addition to the real-time data feed, Thredd also provides daily batch XML reports, via sFTP. You can use this data to support your payment reconciliations. See the *XML Transaction Reports Specifications*.

1.1.2 Payment Authorisation Control

The payment authorisation process is initiated when a cardholder makes a purchase with a merchant , who then seeks authorisation for the card payment via their acquirer. See the figure below.

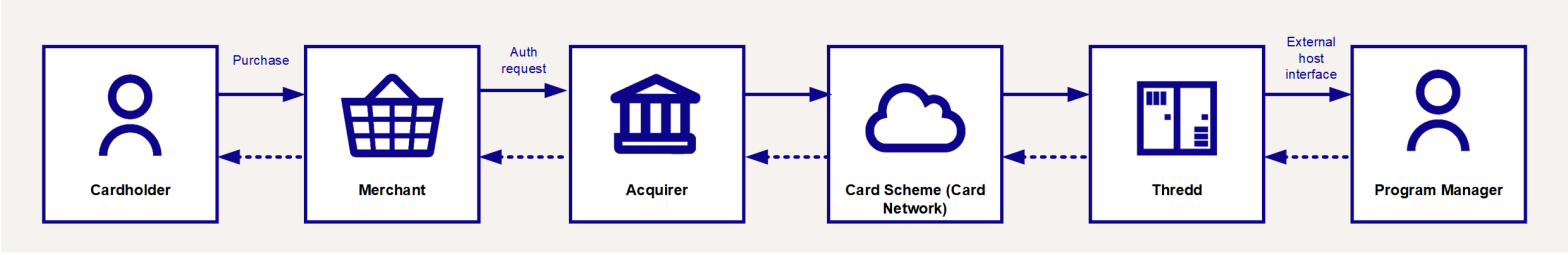


Figure 1: Parties involved in the payment authorisation process

When a payment authorisation request is received from the card schemes, Thredd first performs conventional transaction-related card and cardholder checks, such as EMV data, PIN, CVV2, velocity checks, fraud checks and card product checks.

Your EHI setup option determines whether Thredd or your systems manage the payment authorisation. For example:

- **Gateway Processing (Mode 1)**: Your systems maintain the card balance. You make the authorisation decision and respond to Thredd to indicate whether the transaction can be approved or declined.
- **Cooperative Processing (Mode 2)**: Thredd maintains the card balance. Thredd approves or declines and sends to you the transaction. This enables you to overrule any approved decision.
- **Full Service Processing (Mode 3)**: Thredd maintains the card balance. Thredd makes the authorisation decision and provides you with the response.
- **Gateway Processing with STIP (Mode 4)**: Your systems maintain the card balance. You perform authorisation. Thredd delivers Stand-In Processing (STIP) if your systems are unavailable.

Thredd provides other flexible mode options, where a combination of Thredd and external host authorisation can be used. See EHI Operating Modes.

---

[1] Contact your account manager for information on Discover network availability and restrictions. Mastercard Network Exchange enables smaller networks to use Mastercard as a routing platform for payments.

Thredd will process your response and respond to the card scheme (Mastercard or Visa). The authorisation decision process is in real time.

1.2 EHI Version Control

The currently supported EHI versions are 3.x, 4.x and 5.x.

Thredd creates new EHI versions for new functionality as required by scheme and regulatory changes and/or client enhancements. These are available to all customers.

We distinguish between the following versions:

- *Major versions*: add significant functionality (e.g. MDES). Examples of major version numbers are: 3.0, 4.0, 5.0, and so on.
- *Minor versions*: add minimal functionality (e.g. new field). Examples of minor version numbers are: 4.1, 4.2, 4.3, 5.1. and so on.
- *Document versions*: reflect guide update. Examples of document version numbers are: 4.0.1, 4.0.2, 4.0.3. and so on.

We send notifications out to you whenever there is a new release. To upgrade your EHI version, contact your Thredd account manager or Thredd implementation manager.

1.2.1 Adding New Fields

When Thredd needs to add new fields, we increase the minor version. We keep a record of which EHI version requires which fields. When you connect to the EHI, the system looks up your current EHI version and sends you only the fields that are associated with that version.

Note: If we add new values to an existing field, you receive the new values (that is, the EHI version protects which fields you receive, not the values inside existing fields.)

For a list of EHI fields available with each of the supported EHI versions, see EHI Versions.

1.2.2 Upgrading your EHI Version

Thredd recommends that you upgrade your EHI version to one of the currently supported versions. Versions 3 onwards provide access to ThreddNet, with enhanced EHI features such as load balancing, a streamlined service architecture, support for multiple external host endpoints, faster response times and reduced connection timeouts.

Decommissioning of old EHI Versions

If you are on an older version of EHI, prior to 3.x, we recommend you upgrade. Older versions that are no longer supported may be decommissioned in the future.

1.2.3 Best Practise for Customer Implementations

- Regularly upgrade to ensure you are on a supported EHI version. You should develop EHI integration with an awareness that older, unsupported versions are no longer being tested.
- Ignore all fields you are not expecting, and do not treat this as an error. This will mean that you can upgrade to a new EHI version, without making any changes on your side.
- In order to use any new EHI fields and functionality you may need to update your systems. For details of new fields that have been added to a release, see EHI Versions. For details of additional changes, see the Documentation History.

1.3 EHI Operating Modes

For authorisation types of transactions, the external host interface can operate in one of five supported modes. See the table below:

Setup type	Mode	Who Authorises?	Who Maintains the Balance?	Thredd Authorisation Stand-In	Details
Gateway Processing	1	External Host	External Host	No	Your systems maintain the balance and perform authorisation.
Cooperative Processing	2	Thredd	Thredd / External Host	Yes	Thredd maintains the balance and performs authorisation. You can override an approval decision. In Approval with Load your systems can update the Thredd-maintained balance.
Full Service Processing	3	Thredd	Thredd	No	Thredd maintains the balance and performs authorisation. You receive a read-only response.
Gateway Processing with STIP	4	External Host	External Host	Yes	Your systems maintain the balance and perform authorisation. Thredd provides Stand-In authorisation if the external host is unavailable.

Each mode is described in more detail below.

Tip: Not sure which mode you need? To find the right mode for your business, try our EHI Mode Selector Wizard.

1.3.1 Gateway Processing (Mode 1) - External Host Maintains Balances

You manage the cardholder balances and approve or decline a payment authorisation request.

Your system should always calculate the total balance impact of the transaction, for example billing amount and fees, when determining whether to approve the transaction. (See Calculating the Total Cost.)

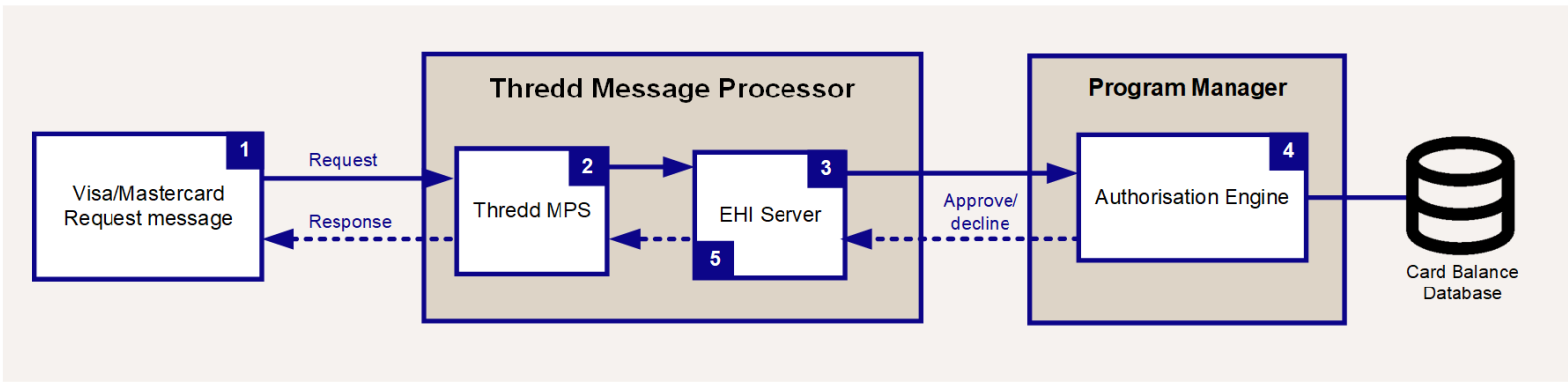


Figure 2: Gateway Processing (Mode 1) - external host approves transaction

1. The card scheme (Visa or Mastercard) sends an authorisation request.
2. The Thredd Message Processing System (MPS) performs checks such as authentication, validation and fraud protection[1], as well as checks based on your product configuration. (This results in a decline if the checks fail. In this case Thredd sends an advice only to the Program Manager and no authorisation decision is required.)
3. The EHI server sends the request to the external host URL endpoint configured for the Program Manager.

[1]Fraud protection is based on whether you are using Thredd's real-time Fraud Transaction Monitoring service. If a rule is triggered it can decline the card transaction.

4. The external host (i.e., Program Manager's systems) then decides whether to approve or decline the transaction, by checking details of the balance held on the card.
5. The EHI server waits for a response from the external host. The response must be received within the allowed time period (see EHI Configuration Options) or the transaction is declined. When received, this is forwarded to the card scheme.

1.3.2 Cooperative Processing (Mode 2) - Thredd Maintains Balances

Thredd performs all types of checks (card, cardholder and balance). But the external host can overrule the Thredd decision and advise to decline the transaction.

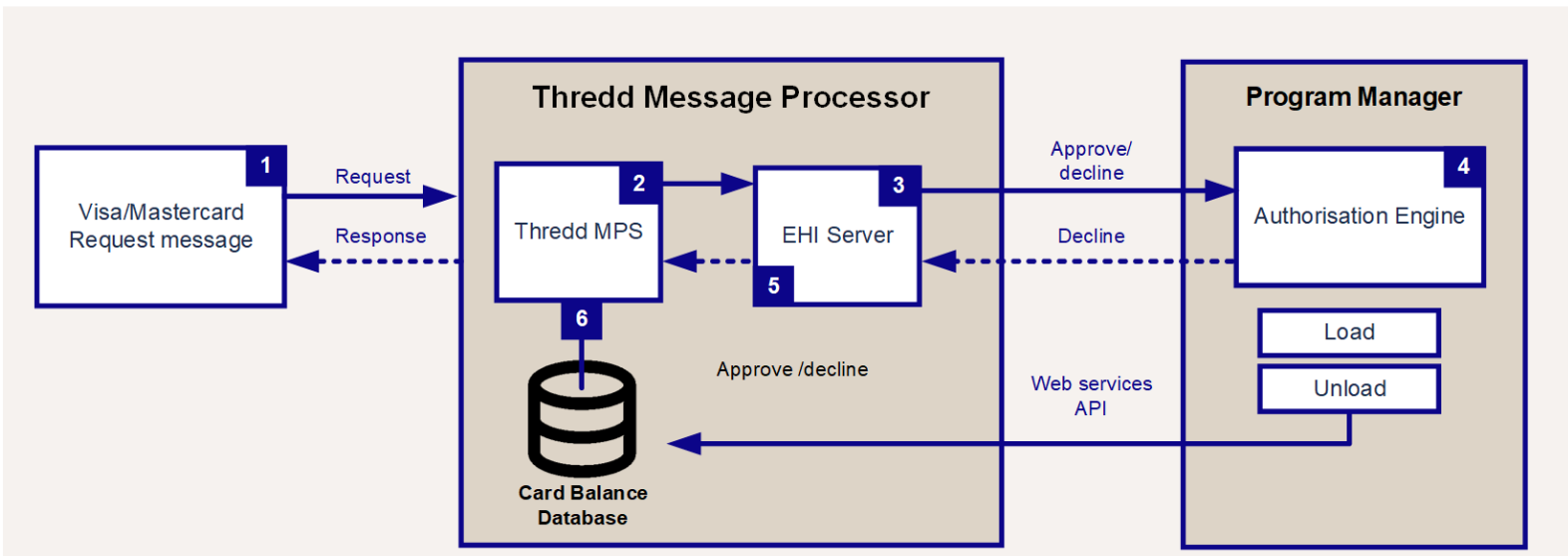


Figure 3: Cooperative Processing (Mode 2) - Thredd approves in first instance

1. The card scheme (Visa or Mastercard) sends an authorisation request.
2. The Thredd Message Processing System (MPS) performs checks such as authentication, validation and fraud protection, as well as checks based on your product configuration.
3. Thredd decides whether to approve or decline the transaction, based on the balance details held by Thredd.
4. The EHI server sends the Thredd response (approve or decline) to the external host URL endpoint configured for the Program Manager.
    - If declined, you can overrule the Thredd decision only for a balance decline (where *Approve with Load* is enabled)[2].
    - If approved, you can decide whether to overrule the Thredd decision and decline the transaction.
    - You can approve for a partial amount if the transaction satisfies the conditions for partial amount approval.
5. The approve or decline response is sent to the card scheme.

Since Thredd maintains the balance, we update the balance as part of the payment transaction life-cycle.

Note: In Mode 2, you can override a Thredd decline code of 51 (Insufficient Funds) with another decline code by passing this in the `ResponseStatus` field of your EHI response. Adding a different decline code is useful for passing to a cardholder a more specific decline reason. However, note that if the Thredd response status is not 51 (Insufficient Funds), then any response status from your end is ignored and the original Thredd response status (as provided in the `Status_Code` field) is preserved.

Stand In

In Mode 2 EHI supports authorisation *Stand-In* where Thredd can fully approve transactions at times where there is no connection to the external host. If *Stand In* is enabled and there is no response from the external host during the allocated time-out period, Thredd approves or declines the transaction, based on Thredd data (such as available balance, card usage rules and risk settings). 'On behalf' approved transactions have the `Authorised by Thredd` flag set to '*Yes*' and when delivered to the external host, Thredd only requires an acknowledgement response.

---

[2] In mode 2 - Approval with Load you can override a balance decline, where Thredd declined because the Thredd held balance indicated insufficient available funds to cover the authorisation; in this case, you should follow up the override by loading the amount to the card, to update the Thredd held balance.

Approval with Load

Your external host systems can approve a card transaction with a simultaneous instruction to Thredd for loading an amount to the card (in order to update the Thredd-maintained card balance ledger).
If this is required and the product is enabled with the *Approval with Load* option, the response message of the approved transaction must contain the '*0A*' response code and the amount to load. The load is done before the transaction amount is debited from the current balance.

Your external host systems should take into account the total balance impact of the transaction (billing amount, fees and padding) when determining whether to approve the transaction. (See Calculating the Total Cost.)

Note: Multi-currency FX cards do not support *Approval with load*.

Note: For clients using Master Virtual Cards (MVCs). MVC setup is restricted to the *Separate Balance* option, which supports loading funds to a single MVC card during the authorisation approval and load process. A *Shared Balance* setup, where funds are automatically transferred between primary and secondary cards, is not supported. For more information, see the Master Virtual Cards Guide: MVC Setup Options.

Note: The Card Schemes (Mastercard and Visa) must approve any *Approve with Load* programmes.

1.3.3 Full Service Processing (Mode 3) - Read-only Data Subscription

Thredd manages the card transaction request and approves or declines. The external host interface is used only as a transaction data feed from the Thredd system to the Program Manager's system.

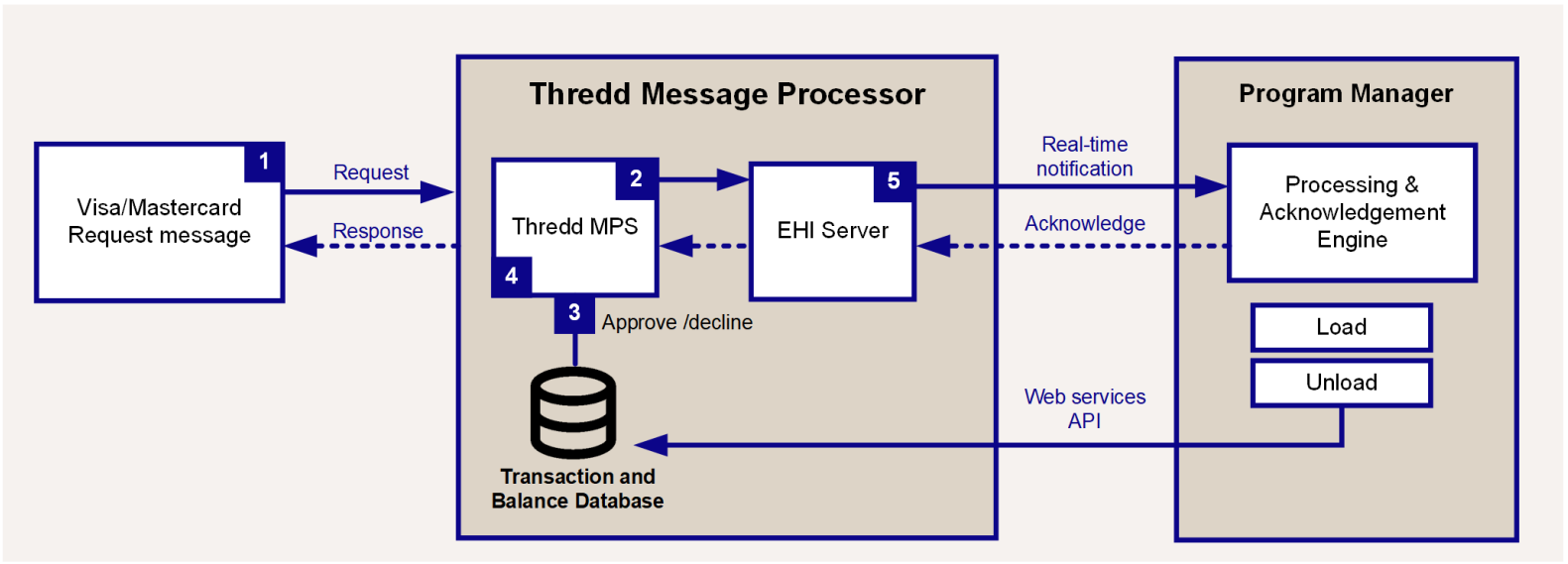


Figure 4: Full Service Processing (Mode 3) - Thredd approves and external host receives data subscription service only

1. The card scheme (Visa or Mastercard) sends an authorisation request.
2. The Thredd Message Processing System (MPS) performs checks such as authentication, validation and fraud protection, as well as checks based on your product configuration.
3. Thredd decides whether to approve or decline the transaction, based on the balance details held by Thredd. Thredd updates the balance.
4. The approve or decline response is sent to the card scheme.
5. The EHI server sends an advice with the transaction outcome, including the latest card balance, to the external host URL endpoint configured for the Program Manager.

1.3.4 Gateway Processing with STIP (Mode 4) – External Host Maintains Balance (with Thredd Stand-in)

EHI Mode 4 is as EHI Mode 1 (where you approve the transaction), except that the external host can maintain the Thredd stand-in balances. If the external host cannot be contacted, then Thredd approves or declines using the current Thredd stand-in balance. The Thredd stand-in balances can be updated by any of the below options:

- EHI response messages (see `Update_Balance` field).
- Balance Update Web Service (see `ws_BalanceUpdate` in the *Web Services Guide*).

- STIP Balance Update endpoint (see the API Hub documentation).

In EHI Mode 4, all transactions (authorisations and financials) updates the Thredd stand-in balance.

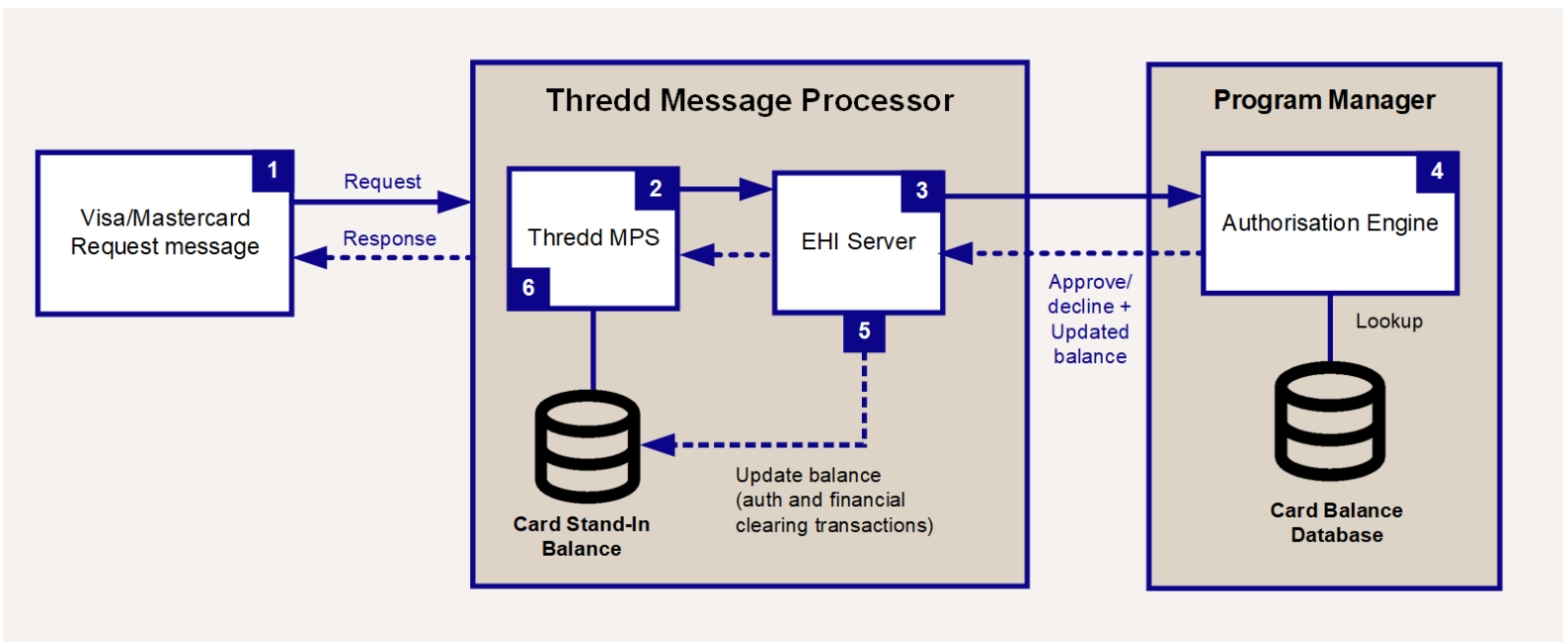


Figure 5: Gateway Processing with STIP (Mode 4) - External host approves, but Thredd can stand in if external host is not available

1. The card scheme (Visa or Mastercard) sends an authorisation request.
2. The Thredd Message Processing System (MPS) performs checks such as authentication, validation and fraud protection, as well as checks based on your product configuration. This result in a decline if the checks fail. In this case Thredd send an advice only to the Program Manager and no authorisation decision is required.
3. The EHI server sends the card transaction request to the external host URL endpoint configured for the Program Manager.
4. The external host (or the Program Manager's systems) decides whether to approve or decline the transaction, by checking details of the balance held on the card.
5. The EHI server waits for a response from the external host. If EHI receives an approve or decline response, the response is returned to the card scheme.
6. If no response is received, then Thredd does stand-in authorisation on behalf of the Program Manager and sends this to the card scheme.

1.4 EHI Connection and Messages

The External Host Interface messaging system is based on RESTful principles. The API accepts JSON-encoded request bodies and returns JSON-encoded responses. The API uses standard HTTP Response codes and verbs. All requests to the API must be made over HTTPS.

See the figure below, illustrating the Thredd system components and typical message flow.

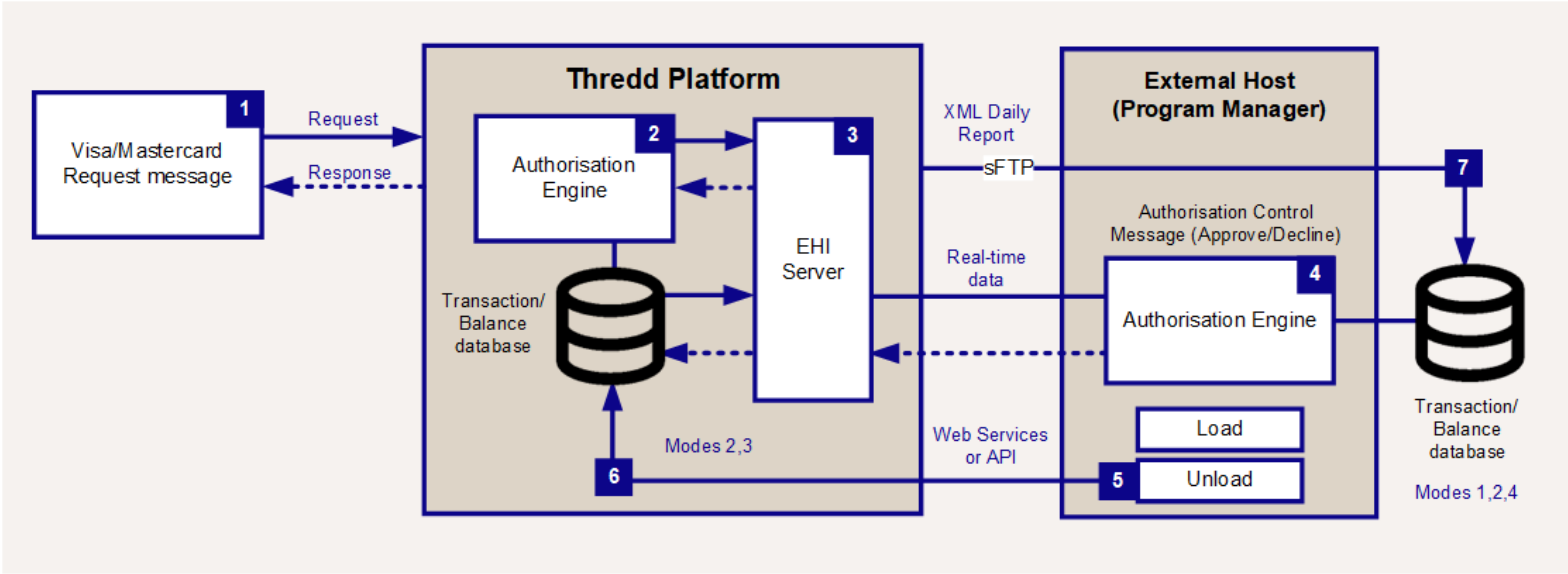


Figure 6: Thredd System Components and External Host Interface Message Flow

Below is a generic summary of this process, which may differ depending on your EHI mode. For more information, see EHI Operating Modes.

1. The card scheme (Visa or Mastercard) sends real-time payment authorisation requests, as well as batch clearing file and financial transaction notifications to Thredd.
2. The Thredd Message Processing System (MPS) performs authentication, validation, velocity controls, fraud protection and product configuration checks.
3. The EHI server sends the card transaction requests and any financial notifications to the external host URL endpoint configured for your programme.
4. Depending on your EHI mode, Thredd may be involved in the card transaction approval decision. For example, in EHI mode 1 (Gateway Processing), mode 4 (Gateway Processing with STIP) the external host (i.e., Program Manager's systems) decides whether to approve or decline the transaction, by checking details of the balance held on the card. In EHI mode 3 (Full Service Processing) Thredd makes the approval decision.
5. The EHI server waits for an approve or decline response or a financial message acknowledgement from the external host. When received, this is processed. Card transaction decline or approve responses are forwarded to the card scheme.
6. Where Thredd maintains the balance on the card, the Program Manager can perform load and unload transactions via the Thredd web services, to update the balance (for details, refer to the *Web Services Guide*).
7. In addition to the real-time data feed, Thredd also provides a daily batch XML transactional data feed via sFTP. You can use this data to support your payment reconciliation process.

Note: Due to the real-time nature of authorisation or online financial requests, in EHI modes where your systems need to process the request, they must respond within the configured time limit for a request (see EHI Configuration Options) or the transaction will be declined.

1.4.1 Types of EHI Messages

EHI sends the following types of messages to the external host (Program Manager's systems):

- **Real-time authorisation requests** - which require an immediate approve or decline decision and response. If not responded to in time, Thredd or the Card Scheme may provide Stand-In Processing (STIP)
- **Real-time reversal requests** - which require an immediate acknowledgement
- **Real-time advices** - which require an immediate acknowledgement (e.g, authorisation advices)
- **Financial notifications** - such as presentments and chargebacks. These require an acknowledgement. An additional response status is optional.
- **Cut off messages** (optional) - batch report showing all messages you should have received in a defined period. See Cut Off Messages.

For most message types, EHI waits for an acknowledgement from the external host to confirm that the message has been received. If no response is received, EHI resends the message. See Processing EHI Transactions.

For details of the fields included in each type of transaction, see EHI Data Feeds.

1.4.2 Transmission Control Protocol (TCP) Connection

For each message sent via the EHI, the following occurs:

1. The EHI makes a TCP connection to the external host URL configured for your program. Thredd is always the TCP client, the external host (your system) is always the TCP server.
2. Using the HTTP POST method, EHI sends an HTTP message to this TCP connection with the SOAP XML message as the message body. The message body is XML encoded to the UTF-8 format. See https://www.w3.org/TR/REC-xml for specifications.
3. The response from your system must be a valid HTTP response with the HTTP response body containing the valid XML response data.
4. In the production environment EHI uses Thredd's Trust Framework, which leverages the **Mutual Transport Layer** (**mTLS**) protocol. .

1.4.3 mTLS Connection

EHI uses Thredd's Secure Connectivity Framework, which leverages the **Mutual Transport Layer** (**mTLS**) protocol. You will need to set up your mTLS termination point to validate the mTLS Transport Certificates. For more information, see the Connecting to Thredd Guide.

1.5 Card Payment Networks

Thredd supports cards enabled for use on Visa, Mastercard and Discover networks, as well as smaller networks that use the Mastercard Network Exchange (MNE), such as STAR and Pulse[1]. These global card payment networks are operated by Card Scheme organisations, which regulate and manage activity on their networks. The payment networks are open to financial institutions and processors, and allow cardholders to pay with Scheme-issued cards and merchants to accept card payments in their businesses worldwide. Thredd operates on the card Issuing side, acting as the gateway between the Card Schemes and the card issuers/Program Managers.

The payment networks are highly standardised and strictly regulated, so interested parties must be certified to be able to participate. Thredd is a certified *Issuer Processor*, which enables us to process various types of card payment transactions from the payment networks we support. Thredd transforms messages from payment networks and other sources into a simplified and unique internal format, available via EHI. Integrating to EHI enables you receive all Thredd supported payment network messages.

EHI content is evolving with the changes introduced by the Card Schemes via periodical releases and ad-hoc announcements. Thredd provides you with notifications of these changes and new EHI version releases.

1.5.1 Card Payment (Network) Transactions

In regions which support the Dual Message System (e.g., UK, Europe and Australia) there are two main steps in a typical card payment transaction:

Step 1: Request for Authorisation

The card scheme sends an authorisation request to Thredd. Thredd receives the authorisation request via the network and responds in realtime after checks done by Thredd and your systems. The result may be approval or decline.

- An approved authorisation does not move any funds, but only blocks/unblocks the authorised amount. Approved authorisations are normally cleared later by financial message to finalise the transaction. If the financial message does not arrive in a defined period, the block is removed.
- Some messages such as balance enquiries are also Authorisation messages, but there are no complementary financial messages for those messages.

Step 2: Financial/Clearing Message

The card scheme sends a financial (or clearing) message to Thredd. Most common financial messages are presentments, which mostly match with an authorisation received previously. Financial messages require a change to the actual balance of the cardholder account. If there is a linked authorisation, financial message must clear the blocking applied for the matching authorisation.

Note that the authorisation amount and financial amount may differ, and blocked amount actual balance mechanisms should ideally be managed independently.

In the life-cycle of a transaction, there may be several financial messages. These messages include chargebacks for disputed financial transactions and reversals of presentments and chargebacks. The figure below lists possible message types and their phases and orders in a transaction life cycle.

---

1 Please contact your account manager for information on Discover network availability and restrictions. Mastercard Network Exchange enables smaller networks to use Mastercard as a routing platform for payments.

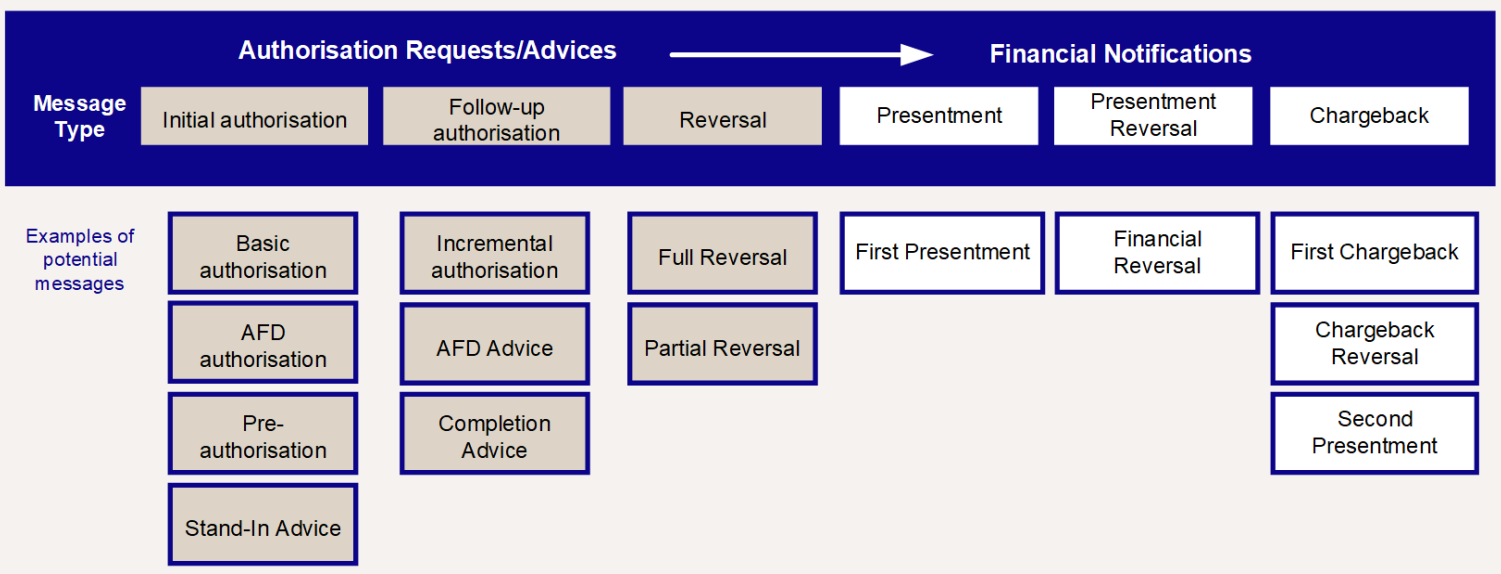


Figure 7: Examples of typical authorisation and financial messages - Dual Message Systems

Most transaction life-cycles consist of a single authorisation and first presentment. However, there are more complex combinations that needs to be supported by EHI. For more information on the transaction types and the steps in processing, see Transaction Flow Scenarios - Dual Message Systems.

1.5.2 Non-Card-Network Transactions

These are transactions that are not originated via the payment networks we support, but by another means, such as Web Services and BACS, CHAPS or Faster Payments. Examples include: load of funds into an account, payments to an account via Faster Payments or card expiry notifications.

1.6 Transaction Flow Scenarios

This section provides examples of typical transaction flows with Message Transaction IDs (MTIDs) for Dual Message systems. This provides a flavour of the type of messages you can expect to receive from the Thredd system.

1.6.1 Authorisations

Authorisation is the stage in a transaction life-cycle where a merchant requests approval for a card payment amount. If the authorisation is approved, the amount is ring-fenced on the card. Typically, the merchant then has 7-10 days to request the transfer of the authorised funds (although this can be up to 28 days for certain merchant category codes). For additional information see What are Authorisations and how do they work?

Authorisation with Approve

The following scenario illustrates a typical approve journey for EHI modes 1, 2 and 4 (Gateway and Cooperative Processing).

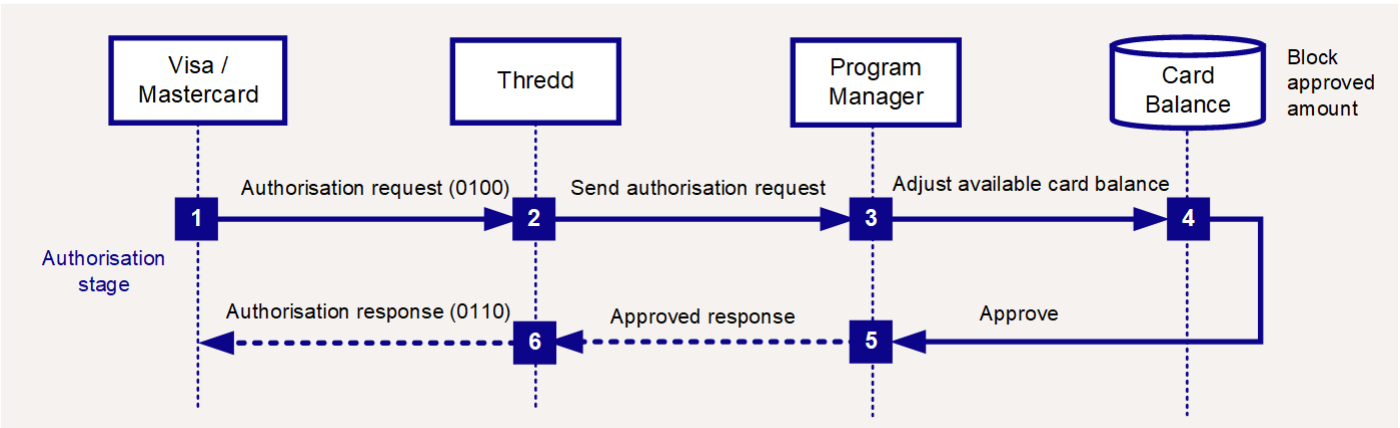


Figure 8: Authorisation Flow - Approve

1. The scheme sends an 0100 authorisation request to Thredd.
2. Thredd carries out validation checks and sends the request to the external host (Program Manager).
3. The Program Manager approves the request.
4. The Program Manager blocks the approved amount (including fees) on the card and reduces the available balance.
5. The Program Manager returns an approved response:

   "Responsestatus": "00" and *"Acknowledgement": "1"*.*
6. Thredd responds to the scheme with an 0110 message (with response status 00 indicating an approval).

* Responsestatus = 00 indicates the request is approved; Acknowledgement = 1 informs Thredd that the message was received and Thredd does not need to resend.

Partial Amount Approval

Partial amount approval is allowed for authorisation requests that have a response code status of 10 and where Thredd_POS_Capability position 1 (partial approval support indicator) is 1. This feature is available for all EHI modes. You can use the Bill_Amt_Approved field to return the partially approved amount. See GetTransaction Message Fields: Bill_Amt_Approved.

Authorisation Resulting in a Decline

The following scenario illustrates a typical decline journey for EHI modes 1, 2 and 4 (Gateway and Cooperative Processing).

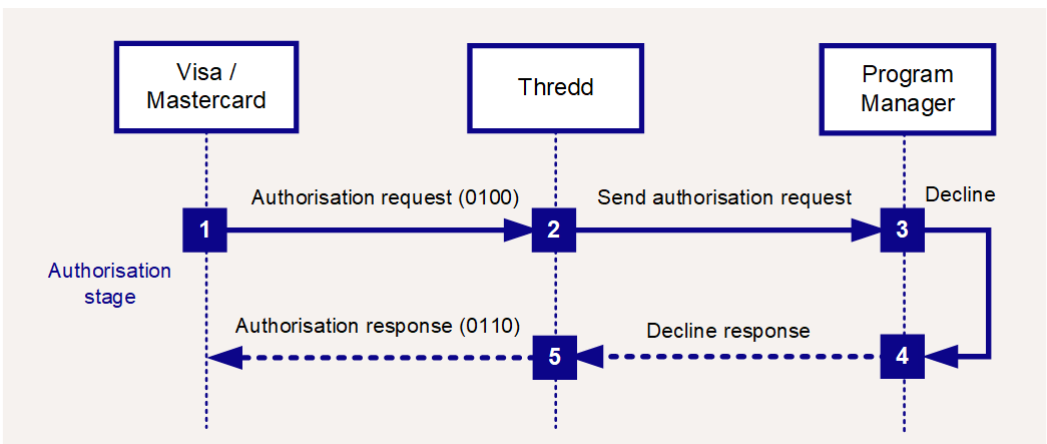


Figure 9: Authorisation Flow - Decline

1. The scheme sends an 0100 authorisation request to Thredd.
2. Thredd carries out validation checks and sends the request to the external host (Program Manager).
3. The Program Manager declines the request.
4. The Program Manager returns a declined response, for example:

   *"Responsestatus": "05" and "Acknowledgement": "1".**
5. Thredd responds to the scheme with an 0110 message (with an appropriate response status, e.g. 05, indicating a decline).

* Responsestatus = 05 indicates Do not honour. You can return any suitable decline response code. See Response Codes.

Acknowledgement = 1 informs Thredd that the message was received and Thredd does not need to resend.

Authorisation Reversal (network)

This type of transaction occurs when the merchant, acquirer or card scheme requests a reversal of the original authorisation. This should result in the amount previously ring-fenced on the card being unblocked.

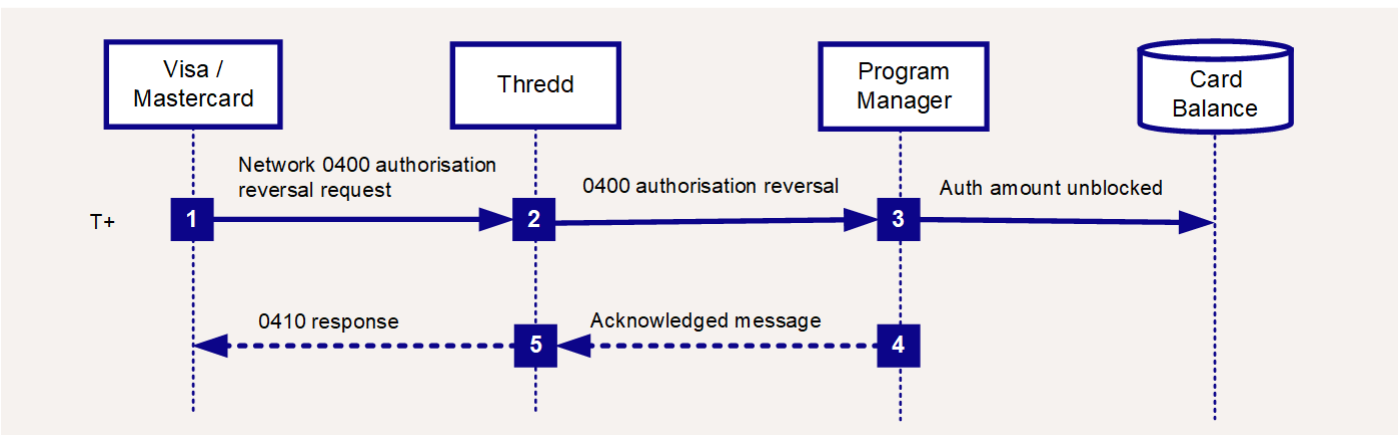


Figure 10: Authorisation Reversal Flow

1. The scheme sends an 0400 authorisation reversal request to Thredd.
2. Thredd sends the request to the external host (Program Manager).
3. Thredd responds to the scheme with an 0410 message.
4. The Program Manager matches the reversal message to the original authorisation message. See Transaction Matching.
   The Program Manager unblocks the authorised amount and updates the cardholder's available balance.
5. The Program Manager acknowledges the message: *acknowledgement = 1.*

Authorisation Reversal (non-network)

If no presentment (request to settle the amount previously authorised) is received within the Thredd hanging filter period, Thredd automatically reverses the authorisation.

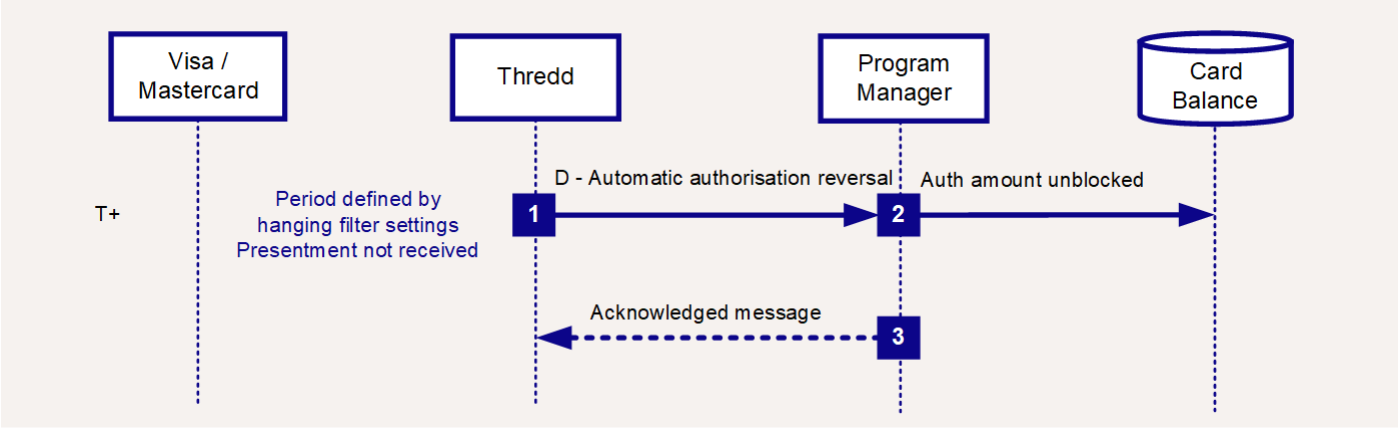


Figure 11: Authorisation Reversal Flow

1. If no presentment is received within the time period set by the hanging filter, EHI sends a financial reversal message to the external host (Program Manager).
2. The Program Manager matches the reversal message to the original authorisation. See Transaction Matching.
3. The Program Manager unblocks the authorised amount and updates the cardholder's available balance.
4. The Program Manager acknowledges the message: *acknowledgement = 1.*

Incremental Authorisation

An incremental authorisation is an additional authorisation, following a previous transaction authorisation, which is used to request an additional amount for the same product or service purchased by the cardholder. See What is an incremental authorisation and how do I identify it?

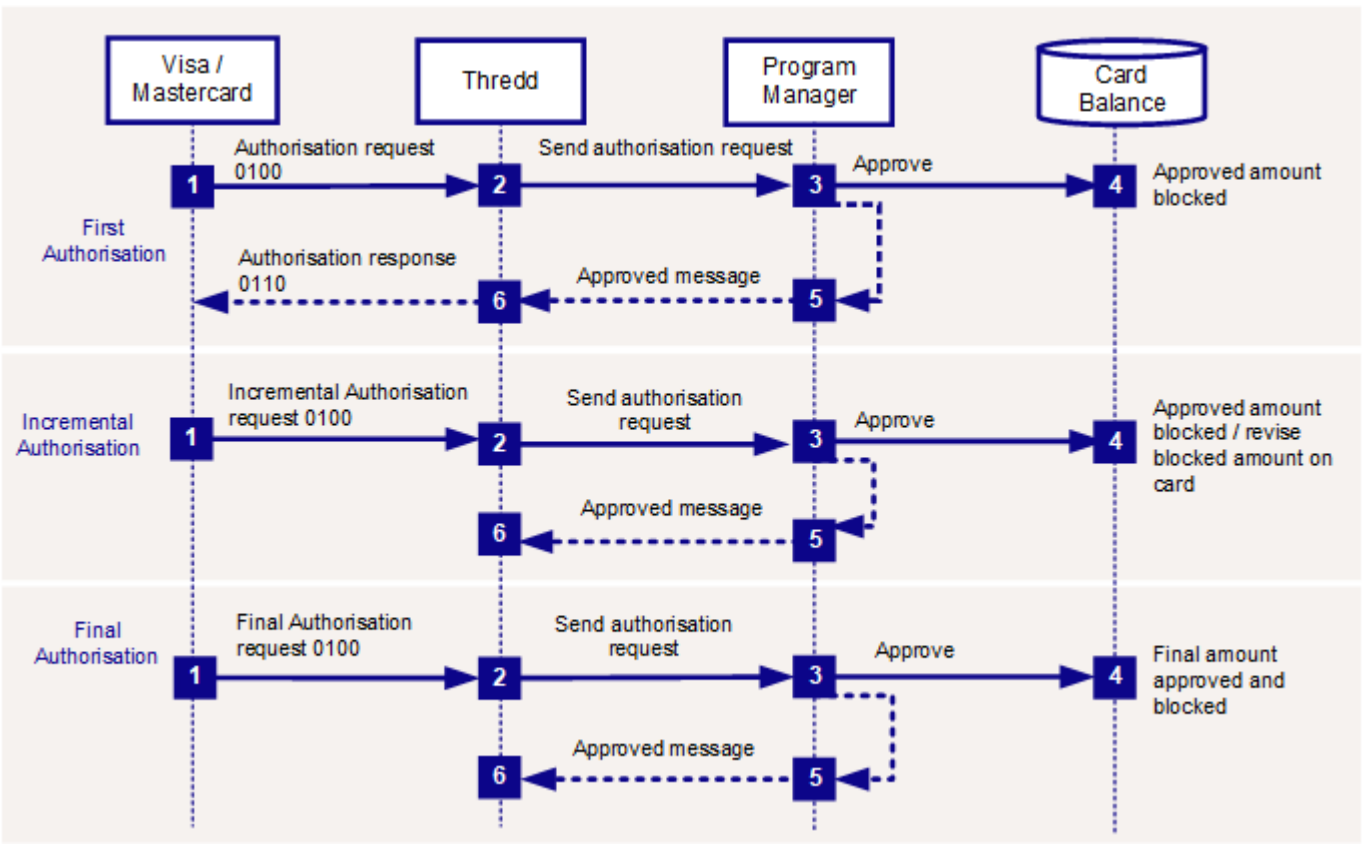


Figure 12: Incremental Authorisation Reversal Flow

- A request for the first authorisation is received, and follows the steps of a normal authorisation. See Authorisation with Approve.
- When you receive the incremental authorisation (`auth_type` = P or 0), where you maintain the card balance and approve, you should block the additional amount.
- If you receive the final authorisation (`auth_type` = F), where you maintain the card balance and approve, you should revise the amount blocked on the card based on the final amount.

You will receive a single financial presentment, which includes the sum of all incremental authorisations.

AFD Authorisations

Automated Fuel Dispensers (AFD) are unattended terminals at fuel stations that allow cardholders to purchase fuel without requiring an attendant. Authorisations from AFDs work slightly differently to other types of authorisations. The initial amount authorised may be followed by an authorisation completion advice for either a higher or a lower amount. In EHI modes where you maintain the card balance, you should return an authorisation decision (approve or decline) and then update the blocked amount on the card, to reflect the new authorised amount.

Note: AFD transactions (MCC 5542) are blocked by default on the Thredd platform. This will result in an automatic decline for AFD authorisations. To enable AFD transactions, contact your account manager or implementation manager.

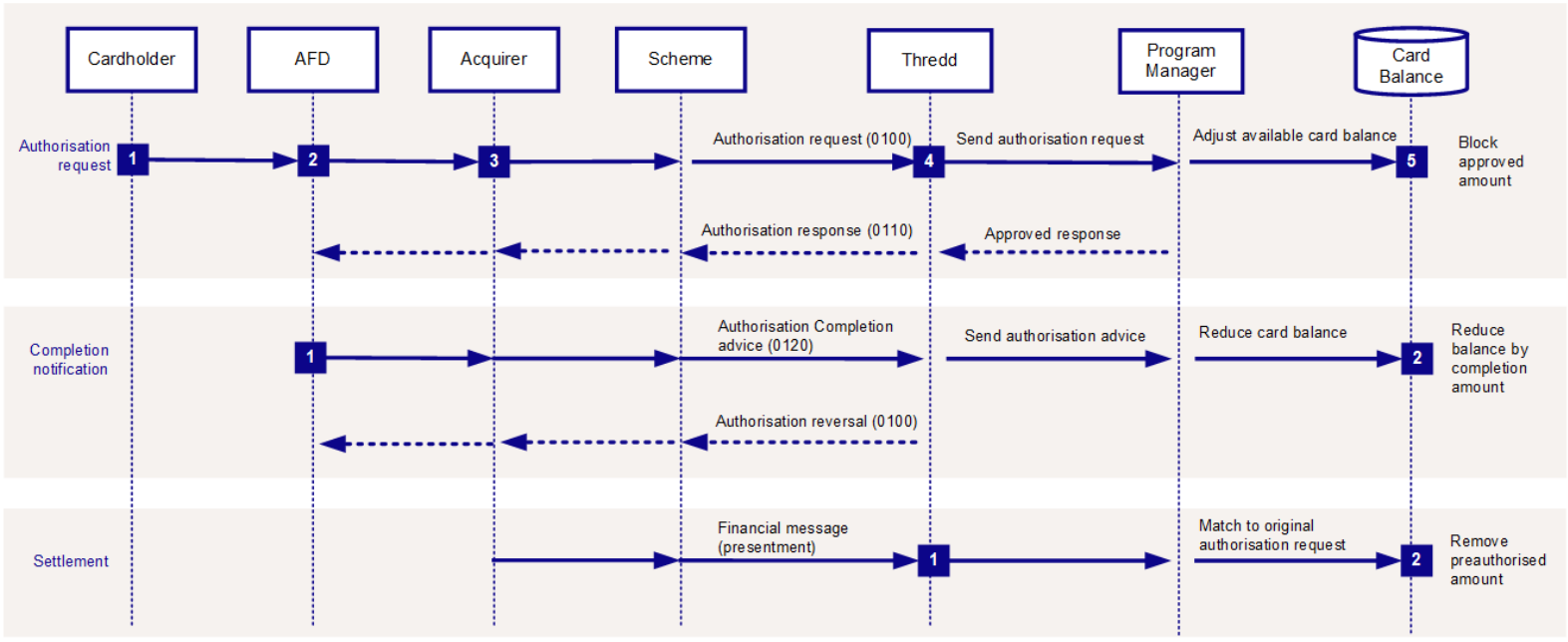


Figure 13: AFD Authorisation and Settlement Flow

Note: The general AFD process described in this section may differ, depending on the fuel dispenser.

Scenario 1: Maximum preauthorisation example

Step 1: Authorisation Request

1. The cardholder inserts or taps their card at an Automated Fuel Dispenser (AFD).
2. The AFD requests either a pre-set fixed preauthorisation amount or a maximum preauthorisation amount (e.g., 100.00 GBP).
3. The Acquirer sends an authorisation request message. The message may contain a partial authorisation indicator, which allows a partial approval response from the issuer to be returned.
4. Thredd or the Program Manager approves or declines the preauthorisation amount. An approval will either be for the full requested amount or, if the issuer supports partial authorisation, an amount based on the cardholder's available funds if less than the amount of the authorisation request.
5. If approved, then Thredd or the Program Manager blocks the approved amount on the card and reduces the available balance (e.g., by 100 GBP).

Step 2: Authorisation Confirmation Advice

1. The fuel is dispensed and costs 90 GBP. The AFD confirms the amount with the Acquirer. The Acquirer sends a completion advice for 90 GBP to Thredd.
2. Thredd or the Program Manager deducts this amount (90 GBP) from the card's actual balance.
3. Thredd generates a partial authorisation reversal for -10 GBP (`Txn_Type` = D, Credit) linked to the original preauthorisation (reducing the full authorised amount from 100 GBP to 90 GBP).

Step 3: Settlement and Reconciliation

1. Thredd or the Program Manager receives the clearing file and matches the financial transaction (presentment) to the original authorisation.
2. Thredd or the Program Manager removes the authorisation amount of 90 GBP. The card now has an authorisation for 90 GBP and a financial message of 90 GBP.

Scenario 2: Nominal preauthorisation example

Step 1: Authorisation Request

1. The cardholder inserts or taps their card at an Automated Fuel Dispenser (AFD).
2. The AFD requests an authorisation for a nominal amount (e.g., 1.00 USD).
3. The Acquirer sends a preauthorisation request message, indicating that the actual maximum amount expected is higher (e.g., 100 USD chargeback protection amount).
4. Thredd or the Program Manager approves or declines the preauthorisation, treating the nominal amount request as a request for the maximum predetermined amount (e.g., 100 USD) to hold funds for the transaction, even though the request amount is 1 USD. Thredd/The Program Manager may partially approve an amount based on available funds (e.g., approving 50 USD out of 100 USD if the account balance is limited).
5. The authorisation response sent back to the merchant reflects the approved amount, which may be less than the maximum or nominal amount requested, indicating a partial approval if applicable.

Step 2: Authorisation Confirmation Advice

1. The fuel is dispensed and costs 90 USD. The AFD confirms the amount with the Acquirer. The Acquirer sends a completion advice for 90 USD to Thredd.
2. Thredd or the Program Manager deducts this amount (90 USD) from the card's actual balance.
3. Thredd generates a partial authorisation reversal for -10 USD (`Txn_Type` = D, Credit) linked to the original preauthorisation (reducing the full authorised amount from 100 USD to 90 USD).

Step 3: Settlement and Reconciliation

1. Thredd or the Program Manager receives the clearing file and matches the financial transaction (presentment) to the original authorisation.
2. Thredd or the Program Manager removes the authorisation amount of 90 GBP. The card now has an authorisation for 90 USD and a financial message of 90 USD.

Refund

A refund transaction occurs when a merchant refunds money to the cardholder, typically relating to a previously processed transaction. The merchant/acquirer submits a request for a *partial* or a *full* refund of a previously paid amount. This is typically processed as an 0100 Authorisation request for a negative billed amount, with the DE3 processing code of *20*. This 2-digit code is displayed in the Thredd (`Proc_Code`) transaction field.

Note: It is not recommended to update the available balance until the linked financial notification is received. You must make information about any pending refund transactions available to cardholders.

1.6.2 Financials

Thredd receives batch clearing files containing financial transactions (presentments) for authorisations that need settlement. Typically the authorisations happened the previous day. Thredd processes the clearing files and sends a separate notification via EHI for each presentment transaction. For additional information see What are Presentments and how do they work?

First Presentment

First presentment occurs when the merchant sends a request to take either part or all of the amount previously authorised on the card[1]. This can happen at the same time as the authorisation request or in some cases it can be much later. The Program Manager should attempt to match the presentment to the original authorisation request.

[1] You should be aware that in some cases it is possible for merchants to submit a presentment for more than the authorised amount. This is permitted for certain Merchant Category Codes (MCC), but it may also indicate a fraudulent transaction.

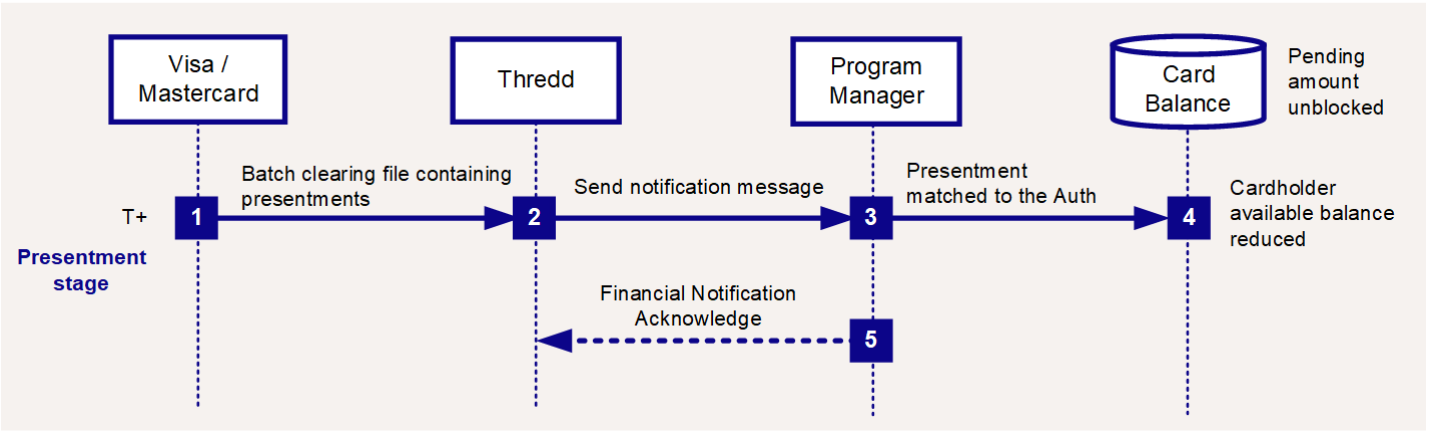


Figure 14: Presenment Flow

1. The scheme sends a batch clearing file to Thredd.
2. Thredd processes the file and sends a notification message per presentment, via EHI, to the external host (Program Manager).
3. The Program Manager matches the presentment to the original authorisation. See Transaction Matching.
4. The Program Manager unblocks the pending amount and reduces the cardholder's available balance.
5. The Program Manager acknowledges the message: *acknowledgement= 1.*

First Presentment for an Offline Transaction

In an offline transaction, Thredd has not received a previous authorisation transaction, so when a financial presentment message is received from the card schemes, we are unable to match to an 0100 authorisation transaction. In this case, Thredd creates a new authorisation transaction and sends this to the Program Manager, followed by the linked presentment message.

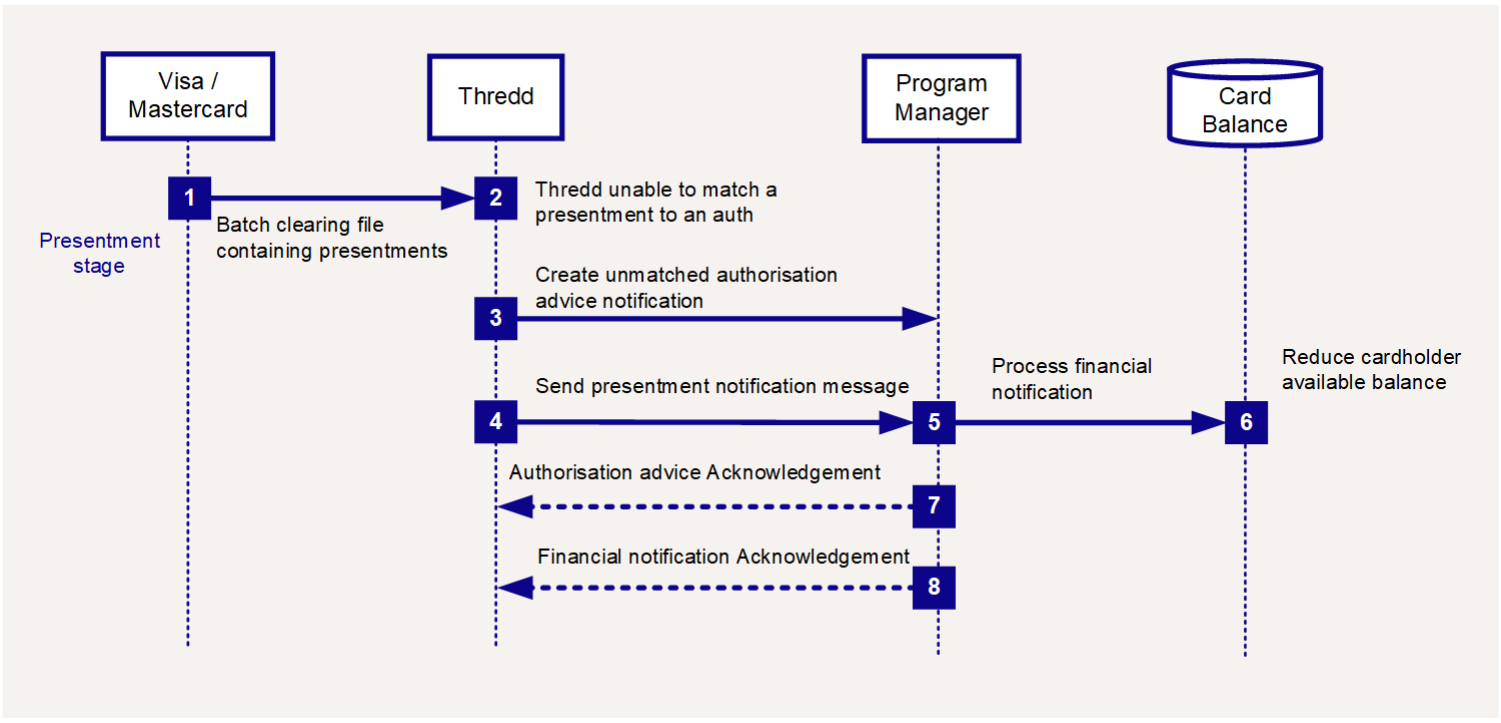


Figure 15: Offline Transaction - Presentment Flow

1. The scheme sends a batch clearing file to Thredd.
2. Thredd carries out validation checks. Since this is an offline transaction, Thredd will not be able to match to an existing 0100 authorisation.
3. Thredd creates an Unmatched Authorisation Advice Notification and sends it the external host (Program Manager).
4. Thredd sends a presentment notification to the Program Manager.
5. The Program Manager processes the financial notification (matching it to the Unmatched Authorisation Advice Notification).
6. The Program Manager reduces the cardholder's available balance by the amount of the presentment.
7. The Program Manager acknowledges the authorisation message: *acknowledgement= 1.*
8. The Program Manager returns a financial notification acknowledgement:*acknowledgement= 1.*

Incremental Presentment

An incremental presentment may occur when a merchant requests an authorisation for a specific amount, but then submits multiple presentments for different partial amounts. An incremental presentment has one authorisation and multiple presentment files. The final presentment total usually equals the total of the original authorised amount. For more information, see What are incremental presentments and how do I handle them?

Financial Reversal

A financial reversal occurs when the acquirer cancels all or part of a prior transaction (which may be a purchase, refund, cashback, cash, PIN change, or any other transaction type).

For example, if the acquirer has already taken the funds and are aware of a processing error (e.g., double charging), they can submit an 1240 Financial Reversal. You must return any deducted amounts back to the card.

Note: For a financial reversal, if the card has subsequently been lost, stolen or replaced, then the card record will be in a blocked and inactive/archived status, and you will not be able to update the card status or process transactions on the card. You should have a process in place to provide the reversed funds to your customer (e.g., move money to another account belonging to your customer).

1.6.3 Chargebacks

A chargeback is a mechanism available to cardholders who dispute a transaction on the card and want part or all of a card payment returned. The chargeback is always issued by the card issuer or Program Manager. The creation of chargebacks is outside of the EHI flow; you can create a chargeback using either the Visa or Mastercard online Dispute Management portals or the Thredd Smart Client. For more information, refer to the *Thredd Chargeback Guide*.

Chargeback and Second Presentment

A chargeback can only be created for a transaction that has a linked presentment. The Program Manager or card issuer creates the chargeback request, which is sent to the card scheme (Visa or Mastercard). This triggers the process described below.

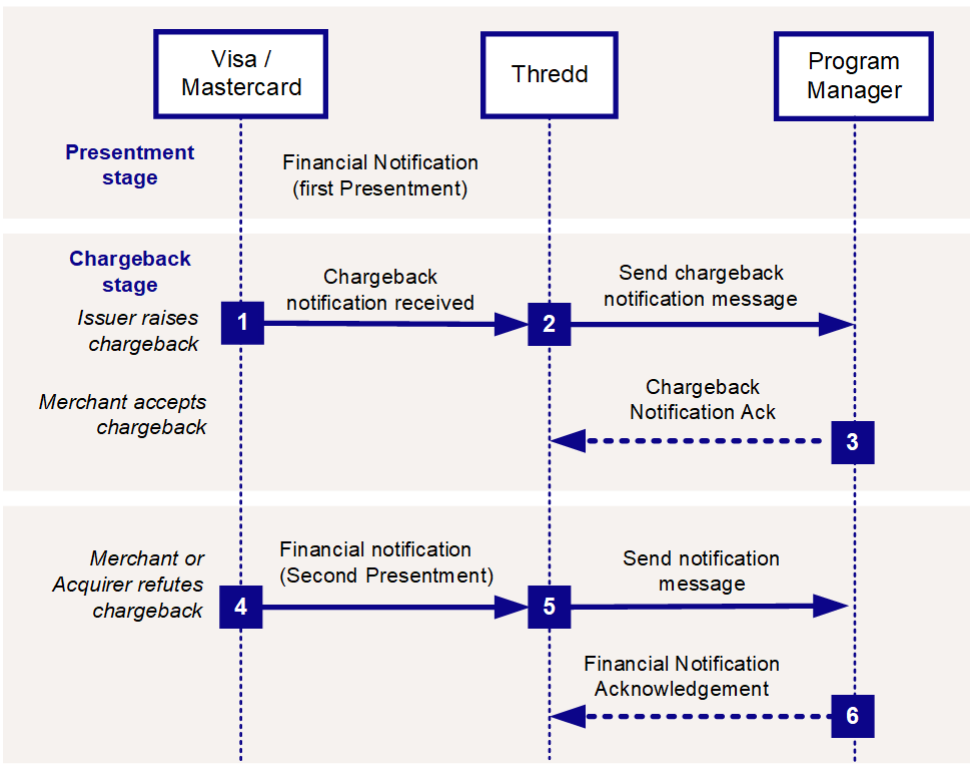


Figure 16: Chargeback Transaction Flow

1. Thredd receives a chargeback notification from the card scheme (Visa or Mastercard).
2. Thredd sends the chargeback notification message to the external host (Program Manager).
3. The Program Manager returns a chargeback notification acknowledgement.

4. If the merchant or acquirer accepts the chargeback, no further EHI messages are sent. (The Program Manager receives additional transaction notifications via the card scheme's dispute management portal or via Smart Client.)
5. If the merchant or acquirer does not accept the chargeback, Thredd receives a second presentment notification from the card scheme.
6. Thredd sends the second presentment notification message to the Program Manager.
7. The Program Manager returns a notification acknowledgement.

Note: When a chargeback is raised, you should always return the disputed amount to the cardholder within the time period prescribed by the card scheme and issuer regulations relevant to your region.

1.7 Transaction Types

EHI sends the following transaction type messages to the external host:

Message Type	Description	How to Process	How you should respond
Authorisation	A request message to approve or decline a payment. Authorisation type transactions include normal authorisation requests and authorisation reversals. An authorisation request message should result in blocking the approved amount on the card to cover a later financial message which is expected to follow.	Gateway or Cooperative Processing (modes 1, 2 and 4): Approve or decline. If approved and you maintain the balance, block the approved amount on the customer's card.	Gateway or Cooperative Processing (modes 1, 2 and 4): Return a decision (approve or decline) and an acknowledgement. Full Service Processing (mode 3): Return an acknowledgement.
Financial	A notification message which Thredd generates based on the batch clearing files received from the card schemes. Financial type transactions include: First Presentment, Financial Reversal, Second Presentment, Chargeback, Chargeback Reversal and Fees.	Match to an existing authorisation or financial. Gateway or Cooperative Processing (modes 1, 2 and 4): Update the card balance	Return an acknowledgement.
Load	A notification that the customer's card balance has been credited (via a Web Service, Cards API, Thredd Portal or Smart Client).	Full Service Processing (mode 3): just acknowledge Gateway Processing (modes 1 and 4): not applicable Cooperative Processing (mode 2): Only applicable if Thredd maintains the balance.	Return an acknowledgement.
Unload	A notification that the customer's card balance has been debited (via a Web Service, Cards API, Thredd Portal or Smart Client).	Full Service Processing (mode 3): just acknowledge Gateway Processing (modes 1 and 4): not applicable Cooperative Processing (mode 2): Only applicable if Thredd maintains the balance.	Return an acknowledgement.
Payment	A notification of a payment originating from a non-card network entity (e.g. Faster Payment or direct debit), paying funds into or out of the customer's card. **Note**: Only relevant to Agency Banking transactions.	Full Service Processing (mode 3): just acknowledge Gateway Processing (modes 1 and 4): acknowledge and process (update balance) Cooperative Processing (mode 2): Please check with your Implementation Manager.	Return an acknowledgement.
Balance Adjustment	A notification that the customer's balance has been updated (via a Web Service, Cards API, Thredd Portal or Smart Client). This can be either a credit or debit.	Full Service Processing (mode 3): just acknowledge Gateway Processing (modes 1 and 4): not applicable Cooperative Processing (mode 2): Only applicable if Thredd maintains the balance.	Return an acknowledgement.
Card Expiry	A notification that the customer's card has expired. Thredd	Just acknowledge. You can decide whether to renew the card (using	Return an acknowledgement.

Message Type	Description	How to Process	How you should respond
	generates this based on the expiry date configured for the card.	the Thredd API)	

1.8 EHI Data Feeds

The EHI can be used as a source of read-only transactional data. For each transaction that Thredd processed, the EHI sends a notification message to your external host system (i.e., to the external host URL endpoint you have requested for your programme). The notification message contains all key attributes of the processed transaction. As with the authorisation advice, the notifications are sent to the external host in real time.

The sections below list the most important fields for each type of message. For details of all the fields in the GetTransaction message, see GetTransaction Messages. For details of the fields in the Cut Off message, see Cut Off Message.

1.8.1 GetTransaction message: Real-time transactional data feed fields

Data that is passed to the external host in transaction messages includes the following fields:

Actual Balance (ActBal)	Available Balance (Avl_Bal)	Billing Amount (Bill_Amt)
Billing Currency (Bill_Ccy)	Blocked Amount (BlkAmt)	Customer Reference (Cust_Ref)
FX Padding (FX_Pad)	Fixed Fee (Fee_Fixed)	Rate Fee (Fee_Rate)
Merchant Category Code (MCC_Code)	Padding (FX_Pad)	Note (Note)
Settlement Amount (Settle_Amt)	Settlement Currency (Settle_Ccy)	Token (Token)
Transaction Link ID (Trans_link)	Transaction Amount (Txn_Amt)	Transaction Currency (Txn_CCy)
Transaction Country (Txn_Ctry)	Transaction Description (Txn_Desc)	Transaction ID (TXn_ID)
Transaction Date (Txn_Thredd_Date)	Transaction Status (Txn_Stat_Code)	Transaction Type (Txn_Type)
Status Code (Status_Code)	Processing Code (Proc_Code)	

1.8.2 GetTransaction message: Authorisation, presentment and financial transactions fields

Authorisation, presentment and online financial transactions include the following additional attributes:

Transmission Date and Time (TXN_Time_DE07)	Local Transaction Date and Time (POS_Time_DE12)	Acquiring Institution ID (Acquirer_id_DE32)
Authorisation Code (Auth_Code_DE38)	POS Terminal ID (POS_Termnl_DE41)	Merchant ID (Merch_Net_id)
Merchant Name (Merch_Name)	Card Network Reference (Traceid_Message)	Response Code (Responsestatus)
Point-of-Service (POS) Data (POS_Data_DE22)	MCC Code (MCC_Code)	MCC Description (MCC_Desc)

1.8.3 Cut off message fields

In addition to the real-time transaction data feed, you can opt to receive cut off messages (Cut_Off) at predefined intervals which contain the following data:

Product ID (ProductID)	Cut off Date (CutoffDate)	Authorisations Acknowledged (Auths_Acknowledged)

Authorisations Not Acknowledged (Auths_NotAcknowledged)	Financials Acknowledged (Financials_Acknowledged)	Financials Not Acknowledged (Financials_NotAcknowledged)
Loads Acknowledged (LoadsUnloads_Acknowledged)	Loads Not Acknowledged (LoadsUnloads_NotAcknowledged)	
Balance Adjustment Expiry Acknowledged (BalanceAdjustExpiry_Acknowledged)	First Transaction ID (FirstTxn_ID)	

1.9 EHI Configuration Options

This section provides information on the available EHI configuration options. Your implementation manager will set up EHI based on the options you selected in the product setup form.

Option	Description
Mode	Your EHI mode (setup option, such as Gateway, Cooperative or Full Service Processing). See EHI Operating Modes.
Include Declined Transactions	Whether to include declined authorisation transactions in EHI messages (used for information purposes only).
Stand In	In Cooperative Processing (mode 2): If this is enabled and there is no connection to Host then we operate as we would if there was no external host at all and authorise/decline based on balance and other information we have in our system.
Approve with Load	In Cooperative Processing (mode 2): The authorisation can be approved with simultaneous instructing to load certain amount to a card. If this is required and the product is enabled with the 'Approval with Load' feature, the authorisation response message of the approved transactions has to contain '0A' response code and amount to load. The Load will be done before the transaction amount is debited from the current balance. **Note**: Multi-Fx cards are not supported.
Delay Send	Applicable in Mode 3 (Full Service Processing) only: If enabled, EHI messages only sends messages after the defined time period. If not enabled. EHI attempts to send messages in real-time first, with subsequent attempts after the defined delay.
Transaction Types	The transaction types you want EHI to send: • Authorisation • Financial (mandatory for modes 1 and 2 - Gateway and Cooperative Processing) • Load/ Unload • Balance Adjustment / Expiry • Authorisation advice • TAR (transaction authorisation request for a token creation request)
External Host URL (Single EHI Endpoint)	The URL EHI uses to send messages to your external host if you have configured a single EHI endpoint to receive all messages from Thredd. Different endpoints (URLs) can be set up for each product.
Decisional URL (Multiple EHI endpoints)	The URL EHI uses to send all time-critical (real-time) messages such as Authorisations, Authorisation Reversals and Advices. Different endpoints can be set up for each product. **Note:** Discontinued.
Informational URL (Multiple EHI endpoints)	The URL EHI uses to send non-time-critical messages such as Chargebacks, Balance Adjustments, Loads/Unloads, Fees and Presentments. Different endpoints can be set up for each product. **Note:** Discontinued.
Clearing URL (Multiple EHI endpoints)	The URL EHI uses to send presentments. Only First Presentments and Second Presentments are sent to this endpoint. Different endpoints can be set up for each product. This optional field can be used to receive presentments in a separate EHI endpoint. If a Clearing URL is not provided, but an Informational URL is provided, then all presentments are sent to the Informational URL. **Note:** Discontinued.

Option	Description
Timeout after	Determines how long EHI waits for a response from the external host before timing out. The default timeout is 200 milliseconds. This can be changed to meet your system requirements. Please contact your account manager or implementations manager to discuss.
Repeat after	Indicates how long EHI waits to resend the message when it does receive any acknowledgement from the external host. The default is 2 minutes.
Times	Indicate how many times EHI needs to resend the message. Default value is 5.
Remove from buffer table after	Indicates the number of days your transaction data is stored in the Thredd buffer table. This can be useful in the scenario where your system is down and you need time to fix it. When the system is back up, Thredd can flush all data from the buffer. Default is 3 days. Maximum is 7 days.
Send Cut of Message	Whether to send a cut off message. See Cut Off Messages.
Cut off Interval	The cut-off period in hours (e.g. if it is set to 4 hours EHI sends a cut-off message every 4 hours). Default is 4 hours.
Cut off URL	The URL EHI uses to send Cut Off messages to your external host.
Version	The EHI version you are using.
Optional fields in Authorisation request message	Select the optional fields you would like sent in Authorisation messages: • Send CVV2 • Send PIN (If selected, please provide the PIN Key File) • Send Expiry Date • Send PAN Sequence Number
Notify	The email address to notify you If EHI cannot reach the external host.
DR EHI URL	The URL EHI uses to send messages to your external host if the primary URL is unavailable (i.e. Disaster Recovery).
DR Cut off URL	The URL EHI uses to send Cut Off messages to your external host if the primary URL is unavailable (i.e. Disaster Recovery).
SSL Key	SSL certification key to use, where SSL is enabled on your external host.
PIN Key File	PIN key file to be used where the *send PIN* field is enabled for inclusion in authorisation request messages. Triple DES keys are used to encrypt PINs in EHI messages. They can be generated either by Thredd or the Program Manager, and must be stored in a separate file. For details, see PIN Block Formats.
JSON format	EHI can be enabled to send and receive messages in JSON format. **Note**: You must be on EHI version 5.0 or above to receive this feature.

1.10 Integration Steps

This section describes the steps in integrating your external host system to the External Host Interface (EHI).

1.10.1 Setting up in the Test Environment

1. Complete your Thredd product setup form. See EHI Configuration Options.
2. Provide Thredd with a list of static IP addresses to your external host server for Thredd to allow access to.
3. Your implementation manager will set you up on the Thredd Test system and will:
    - Provide you with your user credentials to access the Thredd Test system.
    - Set up your External Host URL on EHI for sending GetTransaction messages.
    - Set up your External Host URL on EHI for sending CutOff messages.
    - Provide you with details of how to access Thredd Portal, where you can manage your cards and transactions.

    Note: The External Host URLs you provide need to resolve to the static IP addresses you provided to Thredd.
4. You will need to be set up with secure access to Thredd systems.
5. Integrate to Thredd using the Web Services API (SOAP) or Cards API (REST), in order to create cards and load them with funds. For details, see the *Web Services Guide* or the Cards API Website.
6. Set up your external host systems to be able to receive and process messages from EHI. Your systems should be able to:
    - Check for duplicate messages, respond to and acknowledge EHI messages. See Processing EHI Transactions.
    - Match and process transactions. See Transaction Matching.
    - Process GetMessage fields. See GetTransaction Messages.
    - Receive CutOf messages. See CutOff messages.
7. For EHI modes 1, 2 and 4 (Gateway and Cooperative Processing) where you provide the approve or decline decision for an authorisation transaction, make sure your systems can process the GetTransaction messages and block the available card balance accordingly.
8. For EHI modes 1, 2 and 4 (Gateway and Cooperative Processing) where you maintain the balance, make sure your systems can process the GetTransaction financial messages and update the card balance accordingly.
9. Submit test authorisation and financial transactions to the test environment:
    - You can requests test transactions from your implementation manager.
    - You can use the Card Transaction System (CTS) to create test transactions for different use case scenarios (e.g., POS, ATM, ecommerce and MOTO payments). See the *Card Transaction System (CTS) User Guide*.

1.10.2 Setting up in Production

When you have completed your integration and your card issuer has approved your Product Setup Form (PSF), we can set you up in the live environment.

1. A secure connection to Thredd is required to connect to the production system.
2. You will need to generate some live cards (i.e., internal pilot cards) from your card manufacturer in order to run live transactions. For more information on how to generate cards, see the *Web Services Guide* or contact your Implementation Manager.
3. Run card tests on live cards for different use case scenarios and check the end-to-end process. See Testing Use Case Scenarios below. Make sure your service works before rolling out!

Tip: Your first live cards should be for internal, pilot use only and Thredd recommend you complete your programme testing first before launching your service to cardholders and investors.

Testing Use Case Scenarios

Below are details of the type of test scenarios which Thredd recommends you complete:

- Do the cards support the functionality and behaviour you expect?
- Are the CHIP profiles on the cards correctly set up? (i.e., is the card working and card validation working as expected.)
- Is your mobile app behaving as expected? (e.g., displaying real-time details of card status, card transactions and account balances.)
- If you are using mobile tokenisation services such as VDEP and MDES have you tested different use case scenarios?
- Have you tested other components of your card service, such as:
    - Recurring payments
    - Fees
    - Cardholder authentication (3D Secure)
    - Exception flows, such as reversals, refunds and chargebacks.
- Have you checked the cardholder journey from an end-to-end perspective?

Thredd Card Tests

Thredd runs a set of generic pavement tests where we check a range of card functionality, such as:

- Keys are set up correctly
- Both contact and contactless card transactions are working
- The card usage groups set up for your programme are declining as expected
- General authorisations are being received, refunds are working correctly, authorisation requests are being declined and approved as expected.

Note: In order to check the Thredd platform is behaving according to how configured in your product setup form, we require a selection of cards per programme. Cards should be loaded with sufficient funds to enable testing.

1.10.3 Troubleshooting

Below are examples of some of the types of issues your systems need to be able to handle:

- System timeouts and connection issues
- Duplicate transactions and unmatchable transactions
- Reversals (0400 messages), where you need to approve and unblock funds
- Balance enquiries and issues relating to the card balance
- Cryptogram failures on the CHIP for a new chip profile being launched; this is normally resolved by the Card Manufacturer

For more information see the Troubleshooting FAQs.

SECTION 2: PROCESSING EHI TRANSACTIONS

You should read this section to understand how to integrate your external host system to EHI.

This section covers the following topics:

- Processing EHI Transactions
- Transaction Matching
- Data Types
- GetTransaction Message
- Cut_Off Messages

Tip: If you are new to EHI and want to understand how EHI works and the available configuration options, see the Getting Started section.

2.1 Processing EHI Transactions

This section describes how to process the real-time transactional data sent from EHI to your external host system. When your external host system receives a message from EHI, it must be able to implement the following:

- Return an acknowledgement to EHI - within the time limit set for a response
- Respond to requests - including updating the card balance (where required by your EHI mode).
- Respond to cut-off messages (optional)
- Check for duplicate requests - and respond to EHI accordingly
- Check fields used for 3D Secure Authentication (if applicable) - to verify that the merchant, currency and amount match the details in the authorisation
- Update the STIP balance if required - only relevant to EHI Mode 4 (Gateway Processing with STIP) where Thredd provides Stand-In Processing (STIP)
- Perform transaction matching and processing - this is internal to your systems and no response to EHI is required. For details, see Transaction Matching.

2.1.1 Returning an Acknowledgement to EHI

When you receive a GetTransaction message, your external host system must respond to EHI within the allowed time limit for a response (for the default timeout, see EHI Configuration Options), with the Acknowledgement field set to “1” to indicate that you have successfully processed the transaction.

EHI waits for a response with the Acknowledgement field set to “1” and if no response is received (or an acknowledgement = 0 is received), it continues to re-send the message until either:

- It receives a response with the Acknowledgement field set to “1”.

  Or

- The maximum number of permitted re-tries configured in Thredd has been reached for this message.

2.1.2 Responding to Requests

Responding to Authorisation Requests or Online Financial Requests

In an authorisation request message, the Message Type Identifier (MTID) = *0100* and the transaction type (Txn_Type) = *A*.

In all EHI modes, your systems should always acknowledge the request. In EHI modes 1, 2 and 4 (Gateway and Cooperative Processing) your systems should respond with a decision (*approve* or *decline*). See EHI Operating Modes.

- For a request where you approve, your response to EHI should look like this:

  "Responsestatus": "00" and *"Acknowledgement": "1"*

- For a request where you decline, your response to EHI should look something like this:

  *"Responsestatus": "05"*and *"Acknowledgement": "1"* *

* Responsestatus = 00 indicates the request is approved.

* Responsestatus = 05 indicates *Do not honour* (decline) – you can chose any suitable decline response code. See Response Status Values.

Acknowledgement = 1 informs Thredd that the message was received and Thredd does not need to resend.

For EHI mode 3 (Full Service Processing - advice only), your response should look like this:

"Acknowledgement": "1"

Response fields

For details of mandatory and optional fields that can be included in your response, see Response Message Fields.

IMPORTANT: Do not return the value "null" in any response fields which require numeric values, as this results in EHI declining the transaction. Exclude fields that are optional, if you do not want to return any values.

What happens if EHI does not receive a response?

If no response is received in the time limit for an authorisation or online financial request then the following happens in these EHI modes:

- Gateway Processing (mode 1): Thredd declines the transaction.
- Cooperative Processing (mode 2): If Stand-In processing is not enabled, Thredd declines the transaction. If Stand-In processing is enabled, Thredd makes the decision, which could be *Approve* or *Decline*.
- Gateway Processing with STIP (mode 4): Thredd makes a stand-in processing decision, which could be *Approve* or *Decline*.
- (Full Service Processing (mode 3) is advice only)

Thredd then resends the transaction to notify you of the decision made, with these changes:

- `SendingAttemptCount` field is:
  - EHI modes 1 and 2: “1” (1st repeat) or higher (“n” nth repeat)
  - EHI mode 4: “0” on first message, (and +1 for each time re-attempted)
- `Authorised_by_GPS` field is set to “Y”
- `Txn_Stat_Code` field is set to “A” (Approved) or “I” (Declined)
- `Resp_Code_DE39` field is set to the response code sent back to the network (normally “00” if approved, or “05” (declined) in most cases.)

Note: If you get an advice that has changed the decision you originally made, this may indicate that Thredd did not receive or could not process your original decision (example, due to a network timeout or invalid response format) and has therefore applied the default response for your mode. In this case you should acknowledge the advice and reverse the effect of the original approval (example, by unblocking any previously reserved amounts or reversing a previous debit).

How Thredd responds to the External Host

The table below shows a summary of the type of message content sent to the external host *after* the initial authorisation request.

Setup Option	Mode	Reponse Received from external host*	Thredd Response	Acknowledgement Message to External Host Includes	How you should Respond
Gateway Processing	1	No	Decline	Declined: 0100A - Authorised by Thredd "Y", Txn_Stat_Code "I" <DE39 Reason code>, Sending attempt count 1.	Acknowledge
Gateway Processing	1	Yes (approve or decline)	Pass on to scheme	No message sent to external host.	Not applicable
Cooperative Processing	2	N/a **	Thredd approved	Approved: 0100A - Authorised by Thredd "Y", Txn_Stat_Code "A" <DE39 Reason code 00>, Sending attempt count 0.	Approve or decline
Cooperative Processing	2	N/a **	Thredd declined	Declined: 0100A - Authorised by Thredd "Y", Txn_Stat_Code "I" <DE39 Reason code>, Sending attempt count 0.	Acknowledge or override[1]
Cooperative Processing	2	Yes	Pass on to scheme	No message sent to external host.	Not applicable
Full Service Processing	3	N/a **	Thredd approved	Approved: 0100A - Authorised by Thredd "Y", Txn_Stat_Code "A" <DE39 Reason code 00>, Sending attempt count 0.	Acknowledge

[1] In mode 2 - Approve with Load, you can override a Thredd decline decision if the reason for the decline is insufficient balance (e.g., where the card balance held on your systems indicates the card has sufficient funds). In this case you should use the load card web service to update the Thredd held balance.

Setup Option	Mode	Reponse Received from external host*	Thredd Response	Acknowledgement Message to External Host Includes	How you should Respond
Full Service Processing	3	N/a **	Thredd declined	Declined: 0100A - Authorised by Thredd "Y", Txn_Stat_Code "I" <DE39 Reason code>, Sending attempt count 0.	Acknowledge
Gateway Processing with STIP	4	No	STIP approved	Approved: 0100A - Authorised by Thredd "Y", Txn_Stat_Code "A" <DE39 Reason code 00>, Sending attempt count 0.	Acknowledge
Gateway Processing with STIP	4	No	STIP declined	Declined: 0100A - Authorised by Thredd "Y", Txn_Stat_Code "I" <DE39 Reason code>, Sending attempt count 0.	Acknowledge
Gateway Processing with STIP	4	Yes	Pass on to scheme	No message sent to external host.	Not applicable

Notes

* Your response must be received within the default time limit for a response (see EHI Configuration Options). **Note**: although you may have responded within the time limit, in some circumstances Thredd may not have received or processed your response due to a network timeout or invalid response format.

** An approve or decline response is not applicable to Cooperative Processing (mode 2) and Full Service Processing (mode 3) where Thredd makes the initial approval or decline decision. In EHI Mode 3 Thredd sends the response directly to the card scheme and sends the external host an acknowledgement. In Cooperative Processing (mode 2) Thredd first sends any approved decision to the external host, which can override the decision.

Responding to Authorisation Reversals or Online Financial Reversals

A reversal occurs when a merchant wants to reverse a previously submitted authorisation or inline financial request (for example, because the requested amount was entered incorrectly or the customer cancelled the order). The reversal normally occurs soon after the original authorisation or online financial message (or same day) and can be matched to the original authorisation or online financial message using the `traceid_lifecycle` field.

If you receive an authorisation reversal request (`MTID` = *0400* and `Txn_Type` = *D*), authorisation reversal advice (`MTID` = *0420* and `Txn_Type` = *D*) , your response to EHI should look like this:

"Responsestatus": "00" and *"Acknowledgement": "1"*.

Note that if your system was unable to process the request (For example, your database connection was down, so you could not update any outstanding blocks) you can request the message to be resent. In this case, your response to EHI should look like this:

"Responsestatus": "96" and *"Acknowledgement": "0"*. (You can use codes '91', '92' or '96'.)

Responding to Thredd Declines

In scenarios where Thredd initially declines an authorisation or online financial request, you can respond as follows:

- In Gateway Processing (mode 1), you are not able to overrule the decline, you should return a `Responsestatus` with the same `responsecodeDe39` value that Thredd sent.
- In Full Service Processing (mode 3), you can just acknowledge the message.
- In Cooperative Processing (mode 2), you can overrule the Thredd insufficient balance decline. If you send a `Responsestatus` of "*0A*", Thredd will load the amount you sent in `LoadAmount` field to the card, and recheck the balance is sufficient. Partial approval is also possible in this mode (see Responding to Partial Approvals.)
- In Gateway Processing with STIP (mode 4), you cannot overrule our decline (except for a partial approval).

2.1.3 Responding to Partial Approvals

A partial transaction approval occurs where the Program Manager approves part of the transaction amount only, for example, because the initial approval request was declined due to insufficient funds. For EHI modes where you can overrule the decline decision with a partial approval (Cooperative Processing - mode 2 , Gateway Processing with STIP - mode 4) the process is as follows:

1. Thredd receives an authorisation or online financial request from the card scheme.
2. Thredd initially declines the request due to insufficient funds.
3. The Program Manager overrides the decline, with a partial approval via EHI.
4. Thredd partially approves the request and returns the response to the card scheme.
5. Thredd sends an updated EHI message with the actual result (*Partially Approved*).
6. The Program Manager replies to the updated EHI message with an acknowledgement.

Example

The initial request is declined due to insufficient funds, for example: settlementBillingAmount= -60.00 and Responsestatus = 51.

For a partial approval, your response to EHI to override the decline should look like this:

"Responsestatus": "10" and *"Acknowledgement": "1"*

Thredd then sends the partial approval, for example: Bill_Amt = -50.00 and Resp_Code_DE39 = 10.

You will receive an authorisation or online financial advice and should respond as normal.

Partial Approvals - Mode 1 Clients

For Gateway Processing (mode 1) clients who make the authorisation decision, partial approval works as follows:

1. Thredd receives an authorisation or online financial request from the card scheme.
2. Thredd sends the authorisation or online financial request to the Program Manager, via EHI.
3. The Program Manager partially approves via EHI.
4. Thredd sends the response back to the card scheme.

2.1.4 Responding to Financial Notifications

Financial notifications include transactions such as first presentments (MTID/Txn_Type= 1240/P or 05/P, 06/P, 07/P), financial reversals (MTID/Txn_Type = 1240/ E or 25/E, 26/E, 27/E), chargebacks (MTID/Txn_Type = 1240/C or 1240/H).

Your response to EHI could look like this:

"Acknowledgement": "1".

2.1.5 Responding to Cut_Off Messages

When responding to Cut_Off messages, if you have successfully processed, Cut_OffResult should = “1”.

If a response with Cut_OffResult is received with “0” (or no valid response), EHI does not resend the message. (However, not that in a future version Thredd may re-send the Cut_Off message, as this indicates you have failed to process it and it requires re-sending.)

2.1.6 Checking for Duplicates

Note: In some cases it is possible that when your external host responds to EHI with a valid acknowledgement (Acknowledgement = 1), due to network issues, your acknowledgement may not be received by EHI. In this case EHI will re-send the message, resulting in a duplicate.

How to Identify a Duplicate Message

For GetTransaction messages, if either of the following conditions is true, then the message is a duplicate:

- If the SendingAttemptCount field is “1” or higher (i.e. non-zero)
- If you have already received a message with the same transaction ID (txn_id).

How to Process a Duplicate Message

1. First check to see if the SendingAttemptCount field is “1” or higher (i.e. non-zero).
2. If it is higher than 1, then check the transaction ID (TXn_ID) field. This is unique for every transaction (for the GetTransaction messages.)
3. If the transaction ID matches the transaction ID of an existing record in your database, this indicates a duplicate, which you should process as follows:

- If the original message was an advice, and your external host already has it then:
  - No need to re-process this
  - Respond with *"Acknowledgement": "1"*
- If the original message was an advice, and your external host does not have it then:
  - Process it
  - Respond with *"Acknowledgement": "1"*
- If the original message was an authorisation request (your external host is asked approve or decline), but the repeat is an advice, it will still have the same MTID. This table explains what to do:

External Host Originally:	Advice Indicates that Thredd:	Action required by the External Host
Approved transaction	Approved transaction	Nothing to do
Approved transaction	Declined transaction	Reverse effect of original approval
Declined transaction	Approved transaction	Action the approval
Declined transaction	Declined transaction	Nothing to do
Never received transaction	Approved transaction	Action the approval
Never received transaction	Declined transaction	Nothing to do (but it can be logged)

Cut_Off Duplicate Checking

For Cut_Off messages, since the CutoffID field is unique, you can use this field to detect if the message is a repeat.

Note: EHI currently does not re-send a Cut_Off message if it does not receive a valid response with Cut_OffResult of “1”. However, this may be added in a future version, so you should configure your systems to expect this.

2.1.7 Checking fields used for 3D Secure Authentication

The following fields in the authorisation message relate to the 3D Secure authentication data arriving in the authorisation message. You can use these fields to confirm whether the authorised transaction amount is equivalent to the 3D Secure authenticated amount. [2]

- AuthenticationCurrency
- AuthenticationAmountUpper
- AuthenticationMerchantHash

These fields can also be used to comply with the PSD2 Strong Customer Authentication (SCA) dynamic linking requirements (see Directive (EU) 2015/2366 Article 5 Dynamic Linking). See the figure below.

---

[2] This check ensures that important transaction details presented to the cardholder during a 3D Secure session (such as amount and currency) match the final details authorised by Thredd or the Program Manager. Significant discrepancies may indicate a potentially fraudulent transaction.

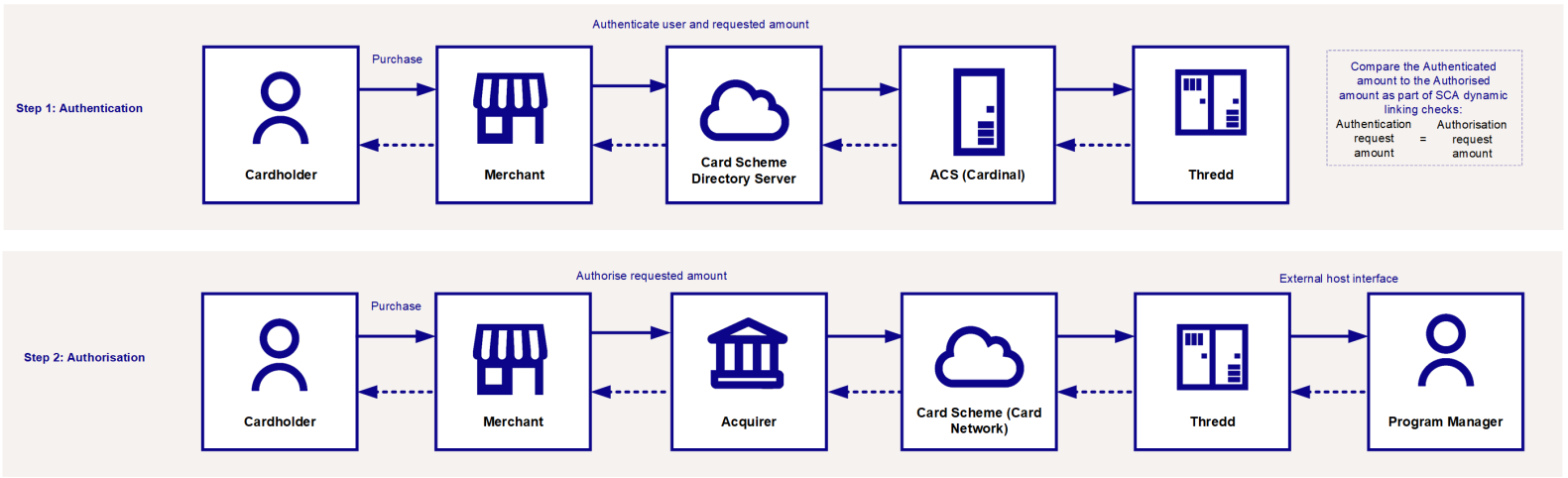


Figure 17: Matching the Authorisation amount to the authentication amount as part of SCA Dynamic Linking checks

Note: You can also use the indicators provided in the GPS_POS_DATA field positions 25 and 26 to check whether the transaction is exempt from SCA and to identify whether the authorisation and authentication amount and currency fields match.

Matching Authentications to Authorisations

The table below provides details of fields you can use to match the 3D Secure authentication details to the linked Authorisation or Online Financial transaction:

3D Secure Authentication Field	Authorisation / Online Financial Fields
AuthenticationCurrency	Txn_CCy
AuthenticationAmountUpper	Txn_Amt
AuthenticationMerchantHash	SHA 256 hash of Merch_Name **Note**: This only works if the identical name was provided at authentication. (e.g., Microsoft and MICROSOFT will be hashed differently)

Note: You can use the above fields to supplement or replace any authentication checks set up for your programme on Thredd systems. For more information, see the PSD2 and SCA Guide > PSD2 Product Settings.

2.1.8 Updating the STIP Balance

Note: Only relevant to EHI Modes where Thredd provides real-time Stand In Processing (STIP) if your systems are unavailable (Gateway Processing with STIP - mode 4).

Thredd approves or declines the transaction amount based on the available card balance in the Thredd database. The Thredd stand-in balances can be updated by any of the below options:

- EHI response messages (see Update_Balance field).
- Balance Update Web Service (see ws_BalanceUpdate in the *Web Services Guide*).
- STIP Balance Update endpoint (see the API Hub documentation).

Below is an example code snippet of a response returned by the Program Manager's systems, requesting a balance update:

```
<GetTransactionResult>
          <Responsestatus>00</Responsestatus>
          <CurBalance>0</CurBalance>
          <AvlBalance>100</AvlBalance>
          <Acknowledgement>1</Acknowledgement>
          <LoadAmount>50</LoadAmount>
          <Bill_Amt_Approved>0</Bill_Amt_Approved>
          <Update_Balance>1</Update_Balance>
          <New_Balance_Sequence_Exthost>200</New_Balance_Sequence_Exthost>
```

```
        <CVV2_Result>400</CVV2_Result>
        <CurBalance_GPS_STIP>0</CurBalance_GPS_STIP>
        <AvlBalance_GPS_STIP>100</AvlBalance_GPS_STIP>
</GetTransactionResult>
```

Note: You should only respond with `Update_Balance` = '1' (update balance) if you have received both `Balance_Sequence` and `Balance_Sequence_Exthost` in the EHI request message. These balance sequence fields are only relevant to real-time transactions where balance adjustments can be made in the response. If you receive a financial notification and need to adjust the Thredd-held balance, you must use the Balance Update Web Service or STIP Balance Update API.

2.2 Transaction Matching

A typical card payment transaction generates multiple messages during its life cycle. The GetTransaction message types you receive for a transaction must be linked to the previous messages for that transaction. This matching enables you to track the history of the transaction, compare the financial effect of a new messages with previous messages and re-calculate card balances.

Note: In Full Service Processing (mode 3) and Cooperative Processing (mode 2), Thredd manages transaction matching.

2.2.1 Matching Overview

Your systems should match new to previous transactions as follows:

New Message	..match to..	Previous Message
Authorization Request (A)	→	Authorization Request (A)
Authorization Reversal (D)	→	Authorization Request (A)
Authorization Advice (J)	→	Authorization Request (A)
Financial Notification (P)	→	Authorization Request (A) or Authorization Advice (J)
Financial Reversal (E)	→	Financial Notification (P, N)
Chargeback (C, H)	→	Financial Notification (P, N)
Chargeback Reversal (K)	→	Chargeback (C, H)
Financial Notification (N)	→	Chargeback (C, H)

Figure 18: Transaction Matching Criteria

For further details, see the Transaction Matching Criteria below.

Where 3D Secure authentication applies, additional transaction matching should be performed to match details in the authorisation to the 3D Secure authentication details. For detail see Transaction Matching - Authentications and Authorisations.

Matching Criteria and Accuracy

Note: Matching a transaction to its original (e.g., *Presentment* to matching *Authorisation*, or *Authorisation Reversal* to matching *Authorisation*) is based on the information received. In most cases transactions match. However, acquirers do not always send accurate information, so mistakes can occur.[1]

You can use the following options to find a match:

- The matching criteria recommended in the section Transaction Matching Criteria
- Your own matching criteria
- A combination of both the above.

As a general rule, the more matching fields that correctly match, the more reliable the match. If some fields match and some do not, this indicates an 'unreliable' match.

Transaction Matching Criteria

The table below provides best-practise guidelines on how to match transactions.

Match Criteria:

- If "*Match to*" is "-", this means there is nothing to match against.
- "THIS" = this transaction (i.e., the one with MTID + Txn_Type from the same row) is the transaction you have just received in the EHI message
- "OTHER" = the other transaction (in the "Match to" column) that is being found by matching (to match to THIS)
- Syntax: *OTHER.other_field_name = THIS.this_field_name* where the field names refer to the GetTransaction Message Fields.

MTID	Txn_Type	Description	Match to?	Match Criteria
0100	A	Authorisation Request	- (For an incremental authorisation, match to Authorisation Request.	OTHER.token=THIS.token AND OTHER.traceid_lifecycle = THIS.traceid_lifecycle **Tip:** For an incremental authorisation, check for a transaction of Txn_Type 'A' arriving with the same traceid_lifecycle as a previous authorisation request. For more information, see What is an incremental authorisation and how do I identify it?
-	D	Automatic Authorisation Reversal	Authorisation Request	OTHER.token=THIS.token AND OTHER.trans_link = THIS.trans_link
0101	A	Authorisation Repeat (Visa Only) **Note**: This transaction is uncommon as only a few acquirers use it. You should respond to a repeat request in the same way as you respond to an original authorisation request. If you decline the repeat authorisation, the terminal may send a new 0100 authorisation, however, you should not assume that this will always occur.	Authorisation Request	OTHER.mtid='0100' AND OTHER.traceid_lifecycle=THIS.traceid_lifecycle AND OTHER.trans_link=THIS.trans_link AND OTHER.Ret_Ref_No_DE37=THIS.Ret_Ref_No_DE37 AND OTHER.TXN_Time_DE07=THIS.TXN_Time_DE07 AND OTHER.POS_Termnl_DE41=THIS.POS_Termnl_DE41 AND OTHER.Token=THIS.Token
0120	J	Authorisation Advice	Authorisation Request (Auth request may not exist)	OTHER.token=THIS.token AND (if THIS.traceid_lifecycle exists) OTHER.traceid_lifecycle = THIS.traceid_lifecycle OR (if THIS.Auth_Code_DE38 exists) OTHER. Auth_Code_DE38 = THIS.Auth_Code_DE38 OR (if THIS.trans_link exists) OTHER.trans_link = THIS.trans_link **Note**: If neither THIS.traceid_lifecycle or THIS.trans_link is present, then there is no match. Normally traceid_lifecycle will always be present if an authorisation exists. For most authorisation advices, Auth_Code_DE38 and trans_link will probably be missing.
0120	D	Authorisation reversal due to a 0120 Automated Fuel	Authorisation Request	OTHER.token=THIS.token AND (if THIS.traceid_lifecycle exists)

MTID	Txn_Type	Description	Match to?	Match Criteria
		Dispenser Advice		OTHER.traceid_lifecycle = THIS.traceid_lifecycle AND (if THIS.Auth_Code_DE38 exists) OTHER. Auth_Code_DE38 = THIS.Auth_Code_DE38 AND (if THIS.trans_link exists) OTHER.trans_link = THIS.trans_link **Note**: If neither THIS.traceid_lifecycle or THIS.trans_link is present, then there is no match. Normally traceid_lifecycle will always be present if an authorisation exists.
0400	D	Authorisation Reversal Request	Authorisation Request	OTHER.token=THIS.token AND (if THIS.traceid_lifecycle exists) OTHER.traceid_lifecycle = THIS.traceid_lifecycle AND (if THIS.Auth_Code_DE38 exists) OTHER. Auth_Code_DE38 = THIS.Auth_Code_DE38 AND (if THIS.trans_link exists) OTHER.trans_link = THIS.trans_link **Note**: If neither THIS.traceid_lifecycle or THIS.trans_link is present, then there is no match. If the reversal is due to timeout at the acquirer, THIS.traceid_lifecycle may not exist. **Note**: The Auth_Code_DE38 is not mandatory for Visa authorisation reversal transactions and therefore acquirers can choose to send it or not.; In some cases, the auth code is sent in the original request but not in the authorisation reversal. In this case treat *Auth_Code_DE38 = '000000'* as you would do when it is blank.
0420	D	Authorisation Reversal Advice	Authorisation Request	OTHER.token=THIS.token AND (if THIS.traceid_lifecycle exists) OTHER.traceid_lifecycle = THIS.traceid_lifecycle AND (if THIS.Auth_Code_DE38 exists) OTHER. Auth_Code_DE38 = THIS.Auth_Code_DE38 AND (if THIS.trans_link exists) OTHER.trans_link = THIS.trans_link **Note**: If neither THIS.traceid_lifecycle or THIS.trans_link is present, then there is no match. If the reversal is due to a timeout at the acquirer, THIS.traceid_lifecycle may not exist.
1240 05pp	A	Authorisation Advice Notification	-	This message should be ignored. It indicates an offline transaction where Thredd has not received a previous authorisation request.

MTID	Txn_Type	Description	Match to?	Match Criteria
06pp 07pp (p=space)		(New dummy authorisation created if a financial notification has no matching authorisation.) 1240 for Mastercard 05pp, 06pp or 07pp for Visa where p=space		See First Presentment for an Offline Transaction. You will receive the financial notification corresponding to authorisation advice, which has all the information required.
1240	E	Financial Reversal **Note:** Some credit/refund transactions may be reported as MTID '1240', Txn_type 'P' (with processing code 20xxxx).	Financial Notification	OTHER.Acquirer_Reference_Data_031 = THIS.Acquirer_Reference_Data_031 AND OTHER.Txn_Amt=THIS.Txn_Amt AND OTHER.Txn_CCy=THIS.Txn_CCy AND OTHER. Auth_Code_DE38 = THIS.Auth_Code_DE38 AND OTHER.POS_Time_DE12=THIS.POS_Time_DE12 AND OTHER.Ret_Ref_No_DE37=THIS. Ret_Ref_No_DE37 **Note**: In some cases both OTHER.Auth_Code_DE38 and THIS.Auth_Code_DE38 are not present.
1240	C	Chargeback Notification	Financial Notification	OTHER.Acquirer_Reference_Data_031 = THIS.Acquirer_Reference_Data_031 AND OTHER.token=THIS.token AND OTHER. Auth_Code_DE38 = THIS.Auth_Code_DE38 AND OTHER.trans_link = THIS.trans_link **Note**: In some cases both OTHER.Auth_Code_DE38 and THIS.Auth_Code_DE38 are not present.
1240	H	Chargeback Notification (Non-Credit)	Financial Notification	As above (see MTID=1240, Txn_Type='C')
1240	K	Chargeback Reversal	Chargeback	As above (see MTID=1240, Txn_Type='C'), except that OTHER (the original to match) will have Txn_Type of 'C' or 'H')
1240	N	Financial Notification (Second Presentment)	Financial Notification and/or Chargeback Notification (Txn_Type H or N)	As above (see MTID=1240, Txn_Type='C')

MTID	Txn_Type	Description	Match to?	Match Criteria
1240	P	Financial Notification (First Presentment)	Authorisation (0100 or 0120)	Rule 1: (reliable match if found, Thredd and acquirer matching data) OTHER.token=THIS.token AND (if THIS.traceid_lifecycle exists) OTHER.traceid_lifecycle = THIS.traceid_lifecycle AND (if THIS.Auth_Code_DE38 exists) OTHER.Auth_Code_DE38 = THIS.Auth_Code_DE38 AND OTHER.trans_link = THIS.trans_link AND OTHER.TXn_ID = THIS.Matching_Txn_ID AND OTHER.Txn_CCy = THIS.Txn_CCy (see notes below) Rule 2: (run if no match on rule 1, AND THIS.traceid_lifecycle exists. Uses Acquirer matching data only) OTHER.token=THIS.token AND OTHER.traceid_lifecycle = THIS.traceid_lifecycle AND (if THIS.Auth_Code_DE38 exists) OTHER. Auth_Code_DE38 = THIS.Auth_Code_DE38 AND OTHER.Txn_CCy = THIS.Txn_CCy (see notes below too) Rule 3: (run if no match on rule 1. Uses Thredd matching data only) OTHER.token=THIS.token AND (if THIS.Auth_Code_DE38 exists) OTHER.Auth_Code_DE38 = THIS.Auth_Code_DE38 AND OTHER.trans_link = THIS.trans_link AND OTHER.TXn_ID = THIS.Matching_Txn_ID AND OTHER.Txn_CCy = THIS.Txn_CCy (see notes below) **NOTES** 1. The above rules are best advice, but there may be some instances where the authorisation and presentment do not match (due to acquirer inconsistencies). 2. OTHER.trans_link may not exist if matching to a MTID=0120. So rule 2 is useful here. 3. Other fields that should normally match include:

MTID	Txn_Type	Description	Match to?	Match Criteria
				• Txn_Amt (except for tips, partial approval, many-auths to 1 Presentment) • Proc_Code (but not a 1-to-1 match) • Merch_ID_DE42 • POS_Termnl_DE41 3. If rule 2 matches and rule 3 does not, (or vice-versa), this indicates an unreliable match. It is up to you if you use the found match or not. 4. Normally traceid_lifecycle will always be present if an authorisation exists. However, if this is a refund, then there will not be an authorisation with a matching traceid_lifecycle.
05pp (p = space)	N	Financial Notification of a Purchase (from Visa) (Second Presentment)	Prior Financial Notification or Chargeback	As above (see MTID=1240, Txn_Type='N')
06pp (p = space)	N	Financial Notification of a Refund or Credit-to-cardholder (from Visa) (Second Presentment) **Note:** Some credit/refund transactions may be reported as MTID '05pp', Txn_type 'P' (with processing code 20xxxx).	Prior Financial Notification or Chargeback	As above (see MTID=1240, Txn_Type='N')
07pp (p = space)	N	Financial Notification of a Cash Withdrawal or disbursement (from Visa) (Second Presentment)	Prior Financial Notification or Chargeback	As above (see MTID=1240, Txn_Type='N')
05pp (p = space)	P	Financial Notification of a Purchase (from Visa)	Authorisation	As above (see MTID=1240, Txn_Type='P')
06pp (p = space)	P	Financial Notification of a Refund or Credit-to-cardholder (from Visa) (First Presentment)	Authorisation	As above (see MTID=1240, Txn_Type='P')
07pp (p = space)	P	Financial Notification of a Cash Withdrawal or disbursement (from Visa) (First Presentment)	Authorisation	As above (see MTID=1240, Txn_Type='P')
25pp	E	Financial Reversal of a Purchase (from Visa)	Prior Financial notification	As 1240 Financial Reversal above (see MTID=1240 Txn_Type='E')

MTID	Txn_Type	Description	Match to?	Match Criteria
(p = space)		(First Presentment)	(MTID=05)	Note: If you cannot match on Acquirer_Reference_Data_031 then try matching on traceid_lifecycle and trans_link. If you cannot match on these, then try Auth_Code_DE38 and Merch_ID_DE42.
26pp (p = space)	E	Financial Reversal of a Refund/Credit-to-cardholder (from Visa)	Prior Financial notification (MTID=06)	As 1240 Financial Reversal above (see MTID=1240 Txn_Type='E') Note: If you cannot match on Acquirer_Reference_Data_031 then try matching on traceid_lifecycle and trans_link. If you cannot match on these, then try Auth_Code_DE38 and Merch_ID_DE42.
27pp (p = space)	E	Financial Reversal of a Cash Withdrawal/disbursement (from Visa)	Prior Financial notification (MTID=07)	As 1240 Financial Reversal above (see MTID=1240 Txn_Type='E') Note: If you cannot match on Acquirer_Reference_Data_031 then try matching on traceid_lifecycle and trans_link. If you cannot match on these, then try Auth_Code_DE38 and Merch_ID_DE42.
-	L	Load	-	-
-	U	Unload	-	-
-	G	Payment	-	-
-	B	Balance Adjustment	-	-
-	Y	Card Expiry	-	-
-	F	Fee	-	-

Resolving Transaction Matching Issues

For more information on resolving matching issues, see Troubleshooting FAQs: Transactions and Matching.

2.2.2 Blocking and Unblocking of Card Funds

When processing and matching transaction messages, you should appropriately apply or remove any card blocks. Below are some guidelines:

- If the authorisation request is for a debit, you should apply a card block to the full billing amount, plus any fees that you or Thredd has applied to the transaction.
- If the authorisation request is a reversal, you should remove the card block for the amount that has been reversed.
- If the authorisation request is for a credit, you can choose to not change any card blocks.

It is important to understand who sent the message before you update the block. Did these originate from the Acquirer, the Network or Thredd?

2.2.3 Transaction Processing Summary

The following table summarises how you should process the different types of transactions sent via EHI to the external host. For additional information, see Transaction Type Decoding.

MTID	Txn_Type	Description	Action
0100	A	Authorisation request.	Process normally. **Note**: if the traceid_lifecycle value matches the traceid_lifecycle value in a previous 0100 authorisation request, then this is an incremental authorisation. (Normally a single financial, with the same traceid_lifecycle, will arrive in this case.)
	D	Automatic authorisation reversal. Thredd automatically reverses a transaction if it does not receive a presentment transaction from the network within the hanging filter period. In the EHI message, all the transaction data fields normally sent by the acquirer (e.g., STAN, RRN, AID and FID) will be identical to the original authorisation request (MTID=0100, Txn_Type='A').	Match to the original authorisation request (MTID=0100, Txn_Type='A') and process accordingly.
0101	A	Authorisation repeat (Visa only)	Match to see if an 0100 original message existed (see above matching criteria table.) • If you find the 0100 original, this is the *same* authorisation. In this case, respond with the original 0100 response (and do not treat this as a new authorisation.) • If you cannot find the 0100 original, this indicates that you did not receive the original 0100 message. In this case, treat this as a new authorisation, and process as with a 0100 message with Txn_Type='A'.
0120	J	Authorisation advice Also provided in the following cases: • Stand-in processing (STIP) by the network. • Automated Fuel Dispenser (AFD) transactions if the final amount is higher than the amount originally authorised in the MTID=0100 Txn_Type="A" authorisation request.	Match to the original authorisation request (MTID=0100, Txn_Type='A') and process the advice normally. Before blocking any funds you should check the Resp_Code_DE39 field to determine whether the transaction was STIP approved or declined: • If approved, then replace the existing block for this transaction with a new block for the amount in this advice. • If declined, then remove the block for this transaction. • If the processing code indicates a credit, you can optionally choose to not change any blocks. For more information, see Transaction Matching Guidelines. **Note**: If a matching authorisation request exists (that needed to be cancelled), then you will separately receive a reversal (e.g. if the original response to the original authorisation request was not sent to the terminal). The following fields give more information on the advice: • Response_Source - indicates the system that sent the response to the authorisation message • Response_Source_Why - indicates the reason for the message response • Message_Source - indicates the system that sent the authorisation message • Message_Why - indicates the reason for the message response
0120	D	Authorisation reversal due to an	Match to the original authorisation request (MTID=0100,

MTID	Txn_Type	Description	Action
		Automated Fuel Dispenser (AFD) 0120 Advice message. (An AFD sends a 0120 advice to confirm how much fuel was actually dispensed. Thredd sends this to you as a reversal, to reverse the unspent part of the original authorisation from the AFD.)	Txn_Type='A') and process this reversal accordingly.
0400	D	Authorisation reversal request This is a reversal received from the network, to reverse a prior authorisation request (MTID=0100, Txn_Type='A').	Check you have not already received and processed this reversal. If so, ignore it. Match to the original authorisation request (MTID=0100, Txn_Type='A') and process accordingly (unblock the reversal amount) **Note**: if the Txn_Amt in the reversal matches the Txn_Amt in the original authorisation request, then this indicates a full reversal. Unblock whatever was originally blocked. (The Bill_Amt in the reversal may slightly differ to the Bill_Amt in the original due to exchange rate fluctuations.) **Note**: it is important to apply any blocks due to an 0120 Auth Advice before applying the 0400 reversal. Never unblock more than was currently blocked due to all the messages for the same transaction set. For more information, see Transaction Matching Guidelines.
0420	D	Authorisation reversal advice This is a reversal received from the network, to reverse a prior authorisation request (MTID=0100, Txn_Type='A'). This is effectively identical to to above (MTID=0400, Txn_Type='D'), only the MTID is different. The only reason for the difference is that we are sending the MTID as received from the network, and some network specifications for reversals use 0400, and others use 0420. But there is no effective difference - both should be treated as a reversal advice (as in you cannot decline.) (Note: Visa use 0400 and 0420. Mastercard use 0400 when originated by the acquirer, and 0420 when originated by the network.)	Check you have not already received and processed this reversal. If so, ignore it. Match to the original authorisation request (MTID=0100, Txn_Type='A') and process accordingly (unblock the reversal amount) **Note**: if the Txn_Amt in the reversal matches the Txn_Amt in the original authorisation request, then this indicates a full reversal. Unblock whatever was originally blocked. (The Bill_Amt in the reversal may slightly differ to the Bill_Amt in the original due to exchange rate fluctuations.)
1240 05pp 06pp 07pp (p = space)	A	Authorisation advice notification (Dummy authorisation created if a financial notification has no matching authorisation.) 1240 if from Mastercard 05pp, 06pp, or 07pp if from Visa. (p = space)	Discard - this is not needed. (The purpose of this message is to provide a dummy authorisation to match to a financial notification.)
1240	E	Financial reversal	Match to a financial notification (MTID=1240, Txn_Type='P' or Txn_Type='N') and process accordingly
1240	C	Chargeback notification	Process normally. (Optionally match to a financial notification (MTID=1240, Txn_Type='P') or (MTID=1240, Txn_Type='N'))

MTID	Txn_Type	Description	Action
1240	H	Chargeback notification (Non-Credit)	Process normally. (Optionally match to a financial notification (MTID=1240, Txn_Type='P') or (MTID=1240, Txn_Type='N'))
1240	K	Chargeback reversal	Process normally. This reverses the effect of a chargeback (e.g., if the chargeback changed the account balance, this reverses the effect on the account balance.) Optionally match to the chargeback (MTID=1240, (Txn_Type='C' or Txn_Type='H'))
1240	N	Financial notification (Second Presentment)	Process normally. (Optionally match to a financial notification (MTID=1240, Txn_Type='P') or Chargeback (MTID=1240, Txn_Type='H' / 'C')
1240	P	Financial notification (First Presentment)	Match to the original authorisation request (MTID=0100, Txn_Type='A') and process accordingly. Note that not all financial notifications will have a matching authorisation.
05pp (p = space)	N	Financial notification (Second Presentment)	Process normally. (Optionally match to a financial notification (MTID=05pp, Txn_Type='P') or Chargeback (MTID=1240, Txn_Type='H' / 'C')
06pp (p = space)	N	Financial notification (Second Presentment)	Process normally. (Optionally match to a financial notification (MTID=06pp, Txn_Type='P') or Chargeback (MTID=1240, Txn_Type='H' / 'C')
07pp (p = space)	N	Financial notification (Second Presentment)	Process normally. (Optionally match to a financial notification (MTID=07pp, Txn_Type='P') or Chargeback (MTID=1240, Txn_Type='H' / 'C')
05pp (p = space)	P	Financial notification of a purchase (from Visa)	Match to the original authorisation request (MTID=0100, Txn_Type='A') and process accordingly. Note that not all financial notifications will have a matching authorisation.
06pp (p = space)	P	Financial notification of a Refund/Credit-to-cardholder (from Visa)	Match to Auth request (MTID=0100, Txn_Type='A') and process accordingly. Note that not all Financial Notifications will have a matching Authorisation.
07pp (p = space)	P	Financial notification of a cash withdrawal/disbursement (from Visa)	Match to Auth request (MTID=0100, Txn_Type='A') and process accordingly. Note that not all Financial Notifications will have a matching Authorisation.
25pp (p = space)	E	Financial reversal of a purchase (from Visa)	Match to financial notification (MTID='05', Txn_Type='P' or Txn_Type='N') and process accordingly
26pp (p = space)	E	Financial reversal of a refund/credit-to-cardholder (from Visa)	Match to financial notification (MTID='06', Txn_Type='P' or Txn_Type='N') and process accordingly
27pp	E	Financial reversal of a cash	Match to financial notification (MTID='07', Txn_Type='P' or

MTID	Txn_Type	Description	Action
(p = space)		withdrawal/disbursement (from Visa)	Txn_Type='N') and process accordingly
-	L	Load	Process normally.
-	U	Unload	Process normally.
-	G	Payment	Process normally.
-	B	Balance Adjustment	Process normally.
-	Y	Card Expiry	Process normally.
-	P	Fee	Process normally Amounts are in the Fee fields (Bill_Amt will be zero)

2.2.4 Incremental Authorisations

Visa and Mastercard allow certain merchants – such as hotels, car rental companies and cruise liners – to obtain an estimated initial authorisation when the final amount of the purchase is unknown and to request incremental funds if needed.

You can match incremental authorisations using the traceid_lifecycle value; each incremental authorisation will have a different txn_ID.

Under normal circumstances Thredd expects, in the same life cycle:

Final presentment transaction amount = SUM(all approved transaction amounts) - SUM(all reversed transaction amounts)

Example 1

The following scenario illustrates how incremental authorisations work:

- Assume starting blocked amount is zero
  a. First Authorisation: £20 - blocked amount now £20
  b. Incremental Authorisation: £30 - blocked amount now £50
  c. Partial Reversal: £40 - blocked amount now £10
  d. Presentment would be for £10

Note that there is no guarantee the above sums will always add up:

- In all cases, on receipt of the presentment you should unblock the amount that was blocked
- the final presentment amount may be less than expected
- the final presentment amount may be more than expected

Incremental authorisations will have:

- Same Thredd token
- Same currency
- Different txn_ID
- Same traceid_lifecycle

You can decline any of the incremental authorisations (or all).

2.2.5 Exception Transactions

Some transactions may have slightly different rules than expected. This is normally due to waivers granted by the card scheme to permit this.

Below are some examples that Thredd are aware of. For more information on any of the below, or to see if there are any other situations, contact your Issuer.

Transport for London (United Kingdom of GB and NI) Merchant Transactions

Transport for London (TFL) (London's Public Transport network) have various waivers on authorisation requirements, in order to permit more offline transactions and for amounts larger than usually permitted, after a single approved authorisation request.

Example 2

The following example is from Mastercard:

(All of the below have the same traceid_lifecycle)

- MTID=0100 authorisation for GBP 6.60, which was approved
- MTID=1240 presentment for GBP 6.60
- MTID=1240 presentment for GBP 5.80
- MTID=1240 presentment for GBP 5.30

Note: Rules differ for UK and non-UK BIN ranges. Check with your Issuer for the latest network rules.

Other merchants

There may be other examples of merchants with waivers to the normal process.

Contact your Issuer or the network for more information.

[1] Visa/Mastercard do not verify whether acquirer information matches, so data from the acquirer may be inaccurate.

2.3 Data Types

This section describes the data types used in both GetTransaction Messages and Cut_Off WSDL messages.

For information on fields in the EHI JSON message and their data type, see JSON Data Types and EHI Fields.

Data Type	Minimum Length	Maximum Length	Description	Examples
N(min,max)	min	max	Numeric digits only (‘0’ to ‘9’.) Variable length of at least minimum digits up to a maximum of digits.	N(1,11) could contain any of: 1 0001 12345678901 N(3,3) could contain: 123 467 009 010
A(min,max)	min	max	Alpha characters: ‘a’-‘z’, ‘A’-Z’ only. Variable length of at least minimum characters up to a maximum of characters.	A(1,11) could contain any of: a azBC FFeRRtsD A(3,3) could contain: Abc GBX NzA zzA
HEX(min,max)	min	max	Hexadecimal digits only, where letters are in upper case only. i.e ‘0’ to ‘9’ and ‘A’-‘F’. Note that ‘A’-‘F’ will only be in upper case. Lower case ‘a’-‘f’ are not permitted. Variable length of at least minimum hexdigits up to a maximum of hexdigits	HEX(1,11) could contain any of: 1 ABF34AD2 0001 ABC45678901 HEX(3,3) could contain: 000 FFF 01A
AN(min,max)	min	max	Alphanumeric characters only (‘0’ to ‘9’, ‘a’-‘z’ and ‘A’-‘Z’) Variable length of at least minimum characters up to a maximum of characters	AN(1,11) could contain any of: 1 Abf34ZaD2 0001 ABC45678901 Decimal(3,3) could contain: 123 467 009 010
ANP(min,max)	min	max	Alpha-numeric and Pad (space) characters only. i.e.’ ‘ (Space), ‘a’-‘z’, ‘A’-‘Z’, ‘0’-‘9’.	ANS(1,11) could contain any of: A 0001 A B 00 5D

Data Type	Minimum Length	Maximum Length	Description	Examples
			Variable length of at least minimum characters up to a maximum of characters	
ANS(min,max)	min	max	Alphanumeric and Special Characters. Variable length of at least minimum characters up to a maximum of characters	ANS(1,11) could contain any of: A 0001 A B $ % & *
AmountUnsigned(a,f)	3	a+1+f	Numeric unsigned amount field, as a real number with '.' as decimal separator. It cannot be negative. (e.g., 123.4567) Where: a = maximum number of digits before decimal point f = maximum number of digits after decimal point **Note**: realtime authorisation message fields of type *AmountUnsigned* can contain numbers with up to four decimal places. Clearing message fields contain numbers with up to two decimal places; Thredd recommend supporting up to four decimal places to allow for future updates to the number of supported digits.	AmountUnsigned(19,4) field could contain: 12345.6780 99999.9999 1.001 1.0 6.72
AmountSigned(a,f)	3	1+a+1+f	Numeric signed amount field, as a real number with optional leading '-' (negative sign), with '.' as decimal separator. (e.g., -123.4567 or 0.09000) Where: '-' = optional leading negative sign (ASCII code 45) a = maximum number of digits before decimal point '.' = decimal point (ASCII code 46) f = maximum number of digits after decimal point **Note**: realtime authorisation message fields of type *AmountSigned* can contain numbers with up to four decimal places. Clearing message fields contain	AmountSigned(19,4) field could contain: 12345.6780 -99999.999 -1.001 1.0 -6.72

Data Type	Minimum Length	Maximum Length	Description	Examples
			numbers with up to two decimal places; Thredd recommend supporting up to four decimal places to allow for future updates to the number of supported digits.	
Datetime (Y_to_nnn)	23	23	Date time field, Year (y) to millisecond (nnn). Format “YYYY-MM-DD hh:mm:ss.nnn” Where: YYYY = 4 digit year 0001-9999 ‘-‘ = literal ‘-‘ character (ASCII 0x2D) MM = Month of year, 01 - 12 ‘-‘ = literal ‘-‘ character (ASCII 0x2D) DD = Day of month, 01-31 ‘ ‘ = literal space character (ASCII 0x20) hh = hour, 00 - 23 ‘:’ = literal colon character (ASCII 0x3A) mm = minute of hour, 00 - 59 ‘:’ = literal colon character (ASCII 0x3A) ss = second, 00-59 ‘.’ = literal decimal point (ASCII 0x2E) nnn = milliseconds, 000- 999	Examples: 2099-12-31 23:59:59.999 1872-01-01 00:00:00.000
Datetime(Y_to_ss)	19	19	Date time field, Year (Y) to second (ss). Format “YYYY-MM-DD hh:mm:ss” Where: YYYY = 4 digit year 0001-9999 ‘-‘ = literal ‘-‘ character (ASCII 0x2D) MM = Month of year, 01 - 12 ‘-‘ = literal ‘-‘ character (ASCII 0x2D) DD = Day of month, 01-31 ‘ ‘ = literal space character (ASCII 0x20) hh = hour, 00 - 23 ‘:’ = literal colon character (ASCII 0x3A) mm = minute of hour, 00 - 59 ‘:’ = literal colon character (ASCII 0x3A) ss = second, 00-59	2099-12-31 23:59:59 1872-01-01 00:00:00

Data Type	Minimum Length	Maximum Length	Description	Examples
Datetime(Y_to_D)	10	10	Date time field, Year (y) to day (d). Format “YYYY-MM-DD” Where: YYYY = 4 digit year 0001-9999 ‘-‘ = literal ‘-‘ character (ASCII 0x2D) MM = Month of year, 01 - 12 ‘-‘ = literal ‘-‘ character (ASCII 0x2D) DD = Day of month, 01-31	1999-12-31
DatetimeRaw (Y_to_D)	10	10	As Datetime (Y_to_D) but any of YYYY, MM or DD might contain invalid characters, such as space, letters or other. If YYYY is generated by Thredd, it will be set to ‘0000’ if the month/day information it is based on does not represent a valid date.	1999-12-31 0000-00-00 0000-x#-99 0000-pp-pp (where p indicates a space character)
Traceid	15	40	Thredd ‘traceid’ format: “nnnn-YYYYMMDD-i” Where: nnnn = 4 character network id, identifying the originating network: (‘BNET’ = Mastercard Banknet, ‘VIS1’ = Visa Base 1) ‘-‘ = literal minus sign YYYYMMDD = network trace date (YYYY=year), (MM=month of year, 01 to 12), (DD=day of month, 01 to 31) ‘-‘ = literal minus sign i = network reference (alphanumeric, 1 to 26)	BNET-19991231-MCC1234XY VIS1-19991231-489365567890123
TraceidRaw	15	40	As Traceid, except that the raw information received from the network will be passed as-is, without validation. As a result of passing the raw information: • the date YYYYMMDD inside it might contain invalid characters such as spaces, or might be an invalid date such as ‘00000000’. • the network reference ‘i’ inside it might be invalid in whole or in part, including containing spaces. If YYYY is generated by	BNET-20191231-MCC999999 BNET-0000pppp-000000000 (where p is the space character) VIS1-00000000-000000000000000

<table>
<tr><th>Data Type</th><th>Minimum Length</th><th>Maximum Length</th><th>Description</th><th>Examples</th></tr>
<tr><td></td><td></td><td></td><td>Thredd based on MMDD from the network, YYYY will be set to ‘0000’ if MMDD is not a valid date.)
If YYYYMMDD is generated by Thredd based on YDDD (last digit of year and day-of-year) from the network, YYYYMMDD will be set to ‘00000000’ if YDDD was not a valid date.</td><td></td></tr>
<tr><td>Rate</td><td>5</td><td>50</td><td>A conversion rate consisting of two parts separated by ‘:’ (colon.)
The RateDigits are provided separately so it is clear how many significant figures are in the rate value.
Format:
RateDigits:DecimalPointOffset
Format of each part:
RateDigits = N(1,10) format DecimalPointOffset = N(1,2) format (values from 0 to 12 only).

Meaning of each part:
The rate value = RateDigits / 10DecimalPointOffet
Examples:
<table><tr><th>Rate</th><th>Decimal value</th></tr><tr><td>1234567:03</td><td>1234.567</td></tr><tr><td>123456:0</td><td>123456</td></tr><tr><td>1234567:12</td><td>0.000001234567</td></tr></table></td><td>000001:12
1234567:0
1234567:1
1234567:2
1234567:03
1234567:6
1234567:7
1234567:8
123456:09
1234567:12
0:0
1:0
1000000:6</td></tr>
<tr><td>TLV10</td><td>14</td><td>999</td><td>A concatenation of many sets of the following:
<table><tr><th>Type</th><th>Format</th></tr><tr><td>Tag</td><td>AN(10,10)</td></tr><tr><td>Length</td><td>N(4,4)</td></tr><tr><td>Value</td><td>ANS (length,length)</td></tr></table></td><td>M1234567890001XM2222222220002YYTTTTTTTTTTT0003abc
(the above means there are three items as follows:
Tag: “M123456789”
Value “X”
Tag: “M222222222”
Value: “YY”
Tag: “TTTTTTTTTT”
Value: “abc”)</td></tr>
</table>

Data Type	Minimum Length	Maximum Length	Description	Examples
			Where: Tag = 10 character identifier. For tag meanings, see Misc_TLV_Data Field. Length = Length of the Value field (number of UTF-8 characters) as 4 decimal digits with leading zeros. Value = Value ('Length' characters long.) Usage of non ASCII-7-bit characters will be kept to a minimum. Notes: Tags are not in any particular order. Tags may repeat if stated in the field description. Tags might not all be defined in the specification – ignore any you do not recognise. Value will only contain printable characters (no binary data.)	
DECIMAL (p,s)	1	p + s + 1	Numeric data type with fixed precision and scale. • Precision (p) is the maximum total number of decimal digits that can be stored, both to the left and to the right of the decimal point. • Scale (s) is the maximum number of decimal digits that can be stored to the right of the decimal point. Scale must be a value from 0 through p. Scale can be specified only if precision is specified. The default scale is 0; therefore, 0 <= s <= p. Maximum storage sizes vary, based on the precision. Example: If p=5 and s=2, then "12345.00" is the maximum. if p=5 and s=5, then "0.12345" is the maximum.	1234567890123456789 1234567890.123456789

Note: An empty field is permitted when usage is 'Optional' even though the Data Type does not permit an empty value (min length = 0.)

2.4 JSON Data Types and EHI Fields

This section describes the data types of the fields in the JSON message. You should use these details together with the information on Data Types for EHI GetTransaction messages.

Note: The Request field values are case sensitive.

Note: The EHI feed does not send JSON fields to externally-hosted systems where the values for the field data are blank. This is different from EHI feeds with XML fields where the feed can send blank values.

Request Fields

Field	JSON Data Type	Null Allowed	Compatible with IEEE 754 binary-64 (double precision) ?
Acquirer_id_DE32	String		N/A
ActBal	Number	Y	Y
Additional_Amt_DE54	String		N/A
Amt_Tran_Fee_DE28	String		N/A
Auth_Code_DE38	String		N/A
Avl_Bal	Number	Y	Y
Bill_Amt	Number	Y	Y
Bill_Ccy	String		N/A
BlkAmt	Number	Y	Y
Cust_Ref	String		N/A
FX_Pad	Number	Y	Y
Fee_Fixed	Number	Y	Y
Fee_Rate	Number	Y	Y
LoadSRC	String		N/A
LoadType	String		N/A
MCC_Code	String		N/A
MCC_Desc	String		N/A
MCC_Pad	Number	Y	Y
Merch_ID_DE42	String		N/A
Merch_Name_DE43	String		N/A

Field	JSON Data Type	Null Allowed	Compatible with IEEE 754 binary-64 (double precision) ?
Note	String		N/A
POS_Data_DE22	String		N/A
POS_Data_DE61	String		N/A
POS_Termnl_DE41	String		N/A
POS_Time_DE12	String		N/A
Proc_Code	String		N/A
Resp_Code_DE39	String		N/A
Ret_Ref_No_DE37	String		N/A
Settle_Amt	Number	Y	Y
Settle_Ccy	String		N/A
Status_Code	String		N/A
Token	Number	Y	Y
Trans_link	String		N/A
Txn_Amt	Number	Y	Y
Txn_CCy	String		N/A
Txn_Ctry	String		N/A
Txn_Desc	String		N/A
Txn_GPS_Date	String		N/A
TXn_ID	Number	Y	Y
Txn_Stat_Code	String		N/A
TXN_Time_DE07	String		N/A
Txn_Type	String		N/A
Additional_Data_DE48	String		N/A
Authorised_by_GPS	String		N/A
AVS_Result	String		N/A
CU_Group	String		N/A
InstCode	String		N/A

Field	JSON Data Type	Null Allowed	Compatible with IEEE 754 binary-64 (double precision) ?
MTID	String		N/A
ProductID	Number	Y	Y
Record_Data_DE120	String		N/A
SubBIN	Number	Y	Y
TLogIDOrg	Number	Y	Y
VL_Group	String		N/A
Dom_Fee_Fixed	Number	Y	Y
Non_Dom_Fee_Fixed	Number	Y	Y
Fx_Fee_Fixed	Number	Y	Y
Other_Fee_Amt	Number	Y	Y
Fx_Fee_Rate	Number	Y	Y
Dom_Fee_Rate	Number	Y	Y
Non_Dom_Fee_Rate	Number	Y	Y
Additional_Data_DE124	String		N/A
CVV2	String		N/A
Expiry_Date	Number	Y	Y
PAN_Sequence_Number	Number	Y	Y
PIN	String		N/A
PIN_Enc_Algorithm	String		N/A
PIN_Format	String		N/A
PIN_Key_Index	String		N/A
SendingAttemptCount	Number	Y	Y
source_bank_ctry	String		N/A
source_bank_account_format	String		N/A
source_bank_account	String		N/A
dest_bank_ctry	String		N/A
dest_bank_account_format	String		N/A

Field	JSON Data Type	Null Allowed	Compatible with IEEE 754 binary-64 (double precision) ?
dest_bank_account	String		N/A
GPS_POS_Capability	String		N/A
GPS_POS_Data	String		N/A
Acquirer_Reference_Data_031	String		N/A
Response_Source	String		N/A
Response_Source_Why	Number	Y	Y
Message_Source	String		N/A
Message_Why	Number	Y	Y
traceid_lifecycle	String		N/A
Balance_Sequence	Number	Y	N
Balance_Sequence_Exthost	Number	Y	N
PaymentToken_id	Number	Y	Y
PaymentToken_creator	String		N/A
PaymentToken_expdate	String		N/A
PaymentToken_type	String		N/A
PaymentToken_status	String		N/A
PaymentToken_creatorStatus	String		N/A
PaymentToken_wallet	String		N/A
PaymentToken_deviceType	String		N/A
PaymentToken_lang	String		N/A
PaymentToken_deviceTelNum	String		N/A
PaymentToken_deviceIp	String		N/A
PaymentToken_deviceId	String		N/A
PaymentToken_deviceName	String		N/A
PaymentToken_activationCode	String		N/A
PaymentToken_activationExpiry	String		N/A
PaymentToken_ activationMethodData	String		N/A

Field	JSON Data Type	Null Allowed	Compatible with IEEE 754 binary-64 (double precision) ?
PaymentToken_activationMethod	Number	Y	Y
ICC_System_Related_Data_DE55 This field applies to both Visa and Mastercard.	String		N/A
Merch_Name	String		N/A
Merch_Street	String		N/A
Merch_City	String		N/A
Merch_Region	String		N/A
Merch_Postcode	String		N/A
Merch_Country	String		N/A
Merch_Tel	String		N/A
Merch_URL	String		N/A
Merch_Name_Other	String		N/A
Merch_Net_id	String		N/A
Merch_Tax_id	String		N/A
Merch_Contact	String		N/A
auth_type	String		N/A
auth_expdate_utc	String		N/A
Matching_Txn_ID	Number	Y	Y
Reason_ID	Number	Y	Y
Dispute_Condition	String		N/A
Network_Chargeback_Reference_Id	String		N/A
Acquirer_Forwarder_ID	String		N/A
Currency_Code_Fee	String		N/A
Currency_Code_Fee_Settlement	String		N/A
Interchange_Amount_Fee	Number	Y	Y
Interchange_Amount_Fee_ Settlement	Number	Y	Y

Field	JSON Data Type	Null Allowed	Compatible with IEEE 754 binary-64 (double precision) ?
Clearing_Process_Date	String		N/A
Settlement_Date	String		N/A
DCC_Indicator	Number	Y	Y
multi_part_txn	Number	Y	Y
multi_part_txn_final	Number	Y	Y
multi_part_number	Number	Y	Y
multi_part_count	Number	Y	Y
SettlementIndicator	String		N/A
Network_TxnAmt_To_BillAmt_Rate	String		N/A
Network_TxnAmt_To_BaseAmt_Rate	String		N/A
Network_BaseAmt_To_BillAmt_Rate	String		N/A
POS_Date_DE13	String		N/A
Traceid_Message	String		N/A
Traceid_Original	String		N/A
Network_Currency_Conversion_Date	String		N/A
Mastercard_AdviceReasonCode_ DE60	String		N/A
Network_Original_Data_Elements_ DE90	String		N/A
Visa_ResponseInfo_DE44	String		N/A
Visa_STIP_Reason_Code	String		N/A
Network_Issuer_Settle_ID	String		N/A
Network_Replacement_Amounts_ DE95	String		N/A
Visa_POS_Data_DE60	String		N/A
Network_Transaction_ID	String		N/A
Misc_TLV_Data	String		N/A
Acquirer_Country	String		N/A
PaymentToken_PanSource	String		N/A

Field	JSON Data Type	Null Allowed	Compatible with IEEE 754 binary-64 (double precision) ?
ClearingFileID	String		N/A
Network_Fraud_Data	String		N/A
SenderData	String		N/A
ReceiverData	String		N/A
AuthenticationAmountUpper	Number	Y	Y
AuthenticationCurrency	String		N/A
AuthenticationMerchantHash	String		N/A
FxProviderCardholderRate	Number		Y
FxProviderBookedRate	Number		Y

Note: For more information on JSON data types, see the RFC 8259 JSON specification.

Response Fields

Field	JSON Data Type	Null Allowed	Compatible with IEEE 754 binary-64 (double precision) ?
MerchantAdvice	String	Y	N/A
Responsestatus	String	Y	N/A
CurBalance	Number	Y	N/A
AvlBalance	Number	Y	N/A
Acknowledgement	String	Y	N/A
LoadAmount	Number	Y	N/A
Bill_Amt_Approved	Number	Y	N/A
Update_Balance	Number	Y	N/A
New_Balance_Sequence_Exthost	Number	Y	N/A
CVV2_Result	String	Y	N/A
CurBalance_GPS_STIP	Number	Y	N/A
AvlBalance_GPS_STIP	Number	Y	N/A

Number range and precision

For each field of JSON data type *Number*, refer to the field description in GetTransaction Message Fields. which describes the field length range and maximum value you need to support. This is important to ensure no loss of information, especially for the fields with potentially large values.

Tip: Some of the above fields of JSON data type *Number* have a bigger range than the RFC 8259 data type of IEEE 754 binary-64 (double precision) which is described for numbers. If using the JavaScript language to process JSON, then for whole numbers (of Thredd data type *N(min.max)*) the JavaScript data type *bigint* would be a suitable alternative to the IEEE 754 binary-64 number data type.

Example

The Matching_Txn_ID field is a number of type N(1,16), with a minimum length of 1 digits and maximum length of 16 digits. Your systems must be able to handle a value containing up to 16 digits.

2.5 GetTransaction Message Fields

This section describes the fields included in the GetTransaction message.

To view message examples for different types of transactions, see GetTransaction Example Messages.

2.5.1 Request Field Formats

Field	Description	Data Type [1]	Sample Data
Acquirer_id_DE32	Acquiring Bank ID as assigned by the network. Note that the format differs depending on whether this is an Authorisation or a Financial type message. For Authorisation messages: • 2 digits length of Acquirer ID (01 to 09) • Acquirer ID (possibly with leading zeros) For Financial messages: • 6 digit Acquirer ID (possibly with leading zeros) Examples: Authorisation examples: • “06123456” means: “06” = length of Acquirer ID. “123456” Acquirer ID. • “0501234” means: “05”=length of acquirer ID. “01234” = acquirer ID. Financial examples: • “123456” (acquirer id = 123456) • “00123” (acquirer id = 123)	N(3,15)	Mastercard Authorisation type: 06123456 Mastercard Financial type: 123456 VISA Authorisation type: 06454500 VISA Financial type: 10000398
ActBal	Actual balance on the card after the transaction, in the card account currency: • Positive indicates a credit balance. • Negative indicates a debit balance.	AmountSigned (19,4)	-250.0000
Additional_Amt_DE54	DE 54 (Additional Amounts) provides information on up to two amount types and related account data. See Additional Amount Field.	AN(20,120)	0040985D000000020000
Amt_Tran_Fee_DE28	DE 28 (Amount, Transaction Fee) is the fee charged (for example, by the acquirer) for transaction activity in the transaction currency code. The format differs between Authorisation and Financial messages, as follows: • Authorisation message	Authorisation: AN(9,9) Financial: AmountUnsigned(9,2)	For Authorisation: D00000500 For Financial: 0.00

Field	Description	Data Type (1)	Sample Data
	format: D= debit issuer or C = credit issuer; 8 digit fee amount in the minor units of currency held in the field Txn_CCy. • Financial message format: Number in the major units of currency held in the field Txn_CCy, with decimal places. For more information, see How are Acquirer fees applied and reported?		
Auth_Code_DE38	Authorisation code generated by Thredd for approved and declined authorisation requests.	ANP(1,6)	675093
Avl_Bal	Available balance on the card after the transaction, in the currency of Bill_Ccy field (card account currency). Negative indicates the account is in debit.	AmountSigned (19,4)	-60.7600
Bill_Amt	Settlement billing amount of the transaction in Bill_Ccy currency. Positive indicates the cardholder account is to be credited (e.g. used for Refunds). Negative means that cardholder account is to be debited (e.g. used for Purchase transactions). For usage in transactions, see Examples of Amount Signs. **Note**: This excludes the Thredd calculated fees (Fee_Fixed and Fee_Rate) and Padding (Fx_Pad and MCC_Pad). Financial Transactions do not have padding.	AmountSigned (19,4)	-189.2400
Bill_Ccy	ISO 3-digit numeric currency of the billing amount. See Currency Codes.	N(3,3)	978
BlkAmt	Total amount blocked on the card after this transaction, in the card's account currency (Bill_Ccy field). Normally zero (if no blocked amount on the card) or negative. For example: • If BlkAmt = 0.0000 the total amount blocked on this card for all outstanding transactions is 0.0000. • If BlkAmt = -24.0100 the total amount blocked on this card for all outstanding transactions is 24.0100 in the Bill_Ccy currency.	AmountSigned (19,4)	-134.6500

Field	Description	Data Type [1]	Sample Data
Cust_Ref	Customer account reference.	ANS(1,25)	4566DXF Imperial Majesty
FX_Pad	Foreign currency (FX) padding applied to the transaction in the card's account currency (Bill_Ccy field).	AmountUnsigned(19,4)	0.0000
Fee_Fixed	The total fixed fee amount which is the sum of all fixed fees calculated by Thredd (based on your Thredd Fee Group configuration). This is applied to the transaction in the card's account currency (Bill_Ccy field). Normally zero or positive.	AmountSigned(19,4)	0.0000
Fee_Rate	Fee amount due, including all percentage rate fees calculated by Thredd applied to the transaction. Normally zero or positive. Corresponds to your fee setup on the system.	AmountSigned(19,4)	0.0000
LoadSRC	The source of the load request. See Load Source. Present only for Txn_Type values of: L= Load; U = Unload; G = Payment	N(1,4)	14
LoadType	Payment method of funds for the load. See Load Types. Present only for Txn_Type values of: L= Load; U = Unload; G = Payment	N(1,1)	0
MCC_Code	The classification (card acceptor business code or merchant category code) of the merchant's type of business or service. See Merchant Category Codes.	N(1,4)	5411
MCC_Desc	The classification (card acceptor business code or merchant category code) of the merchant's type of business or service.	ANS(0,250)	Grocery Stores, Supermarkets
MCC_Pad	Merchant category code (MCC) padding applied for the transaction in the card's account currency (Bill_Ccy field).	AmountUnsigned(19,4)	0.0000
Merch_ID_DE42	Identifies the merchant or entity that accepted the card. This is always provided for a POS transaction and is optional for an ATM transaction. For a POS tansaction, the merchant name is defined by the acquirer (Acquirer_id_DE32). For	ANS(1,15)	Mastercard Authorisation: 51569373 Mastercard presentment: 82040424200019 VISA Authorisation: 372181910889 VISA Presentment: 005438482900826

Field	Description	Data Type (1)	Sample Data
	an ATM transaction, it typically identifies the entity that owns the ATM.		
Merch_Name_DE43	Identifies the merchant or entity that accepted the card and their location (excluding ATM and card-activated public phones). **Note**: For EHI Version 3.0 and beyond, Thredd recommend using the following fields: Merch_Name, Merch_Street, Merch_City, Merch_Region, Merch_Postcode, Merch_Country. The format differs depending on whether this is an Authorisation or a Financial message. For Visa and Mastercard authorisation message formats, see Merch_Name_DE43 Field in Authorisations. For Visa and Mastercard financial message formats, see Merch_Name_DE43 Field in Financials.	ANS(1,101)	Mastercard Authorisation: Golff Harmelen HARMELEN NLD FOR VISA: TONY ROMA'S CARACAS VE
Note	Note for the particular transaction. Notes are taken from transaction details appended during each type of transactions. For declined transactions, this might occasionally have text explaining why the transaction was declined.	ANS(0,500)	Declined due to incorrect PIN.
POS_Data_DE22	Point of Sale (POS) data field, indicating the PAN entry method and the capability of the terminal to accept a PIN. **Note**: For EHI Version 3.0 and beyond, Thredd recommend using the following fields: GPS_POS_Capability, GPS_POS_Data. Format and content differs per message type as follows: For Visa and Mastercard Authorisation messages: • This holds the PAN entry method and PIN capture capability. See POS_Data_DE22 in Authorisation Messages • For the extra POS methods and capabilities, see field POS_Data_DE61 instead For Mastercard Financial	Authorisation messages: N(3,4) Financial messages: AN(12,12)	Mastercard Authorisation messages: 071 Visa Authorisation messages: 0710 Mastercard Financial messages: C11101299001 Visa Financial messages: (empty)

Field	Description	Data Type (1)	Sample Data
	messages: this holds all the POS methods and capabilities. See POS_Data_DE22 in Mastercard Financial Messages. For Visa Financial messages: this is empty.		
POS_Data_DE61	**Note**: For EHI Version 3.0 and beyond, Thredd recommend using the following fields for accurate POS data: GPS_POS_Capability and GPS_POS_Data. The is because POS_Data_DE61 is only relevant to Mastercard authorisations and only the first 9 positions are guaranteed in Mastercard. For Mastercard authorisation-related messages: This holds additional POS condition codes. See POS_Data_DE61 Values For Visa Authorisation-related messages: this is empty. For Financial and all other messages: this is empty.	ANP(9,39)	For Mastercard Authorisation messages: 1025100006600442L2338 For VISA Authorisation messages: (empty) For All Financial messages: (empty)
POS_Termnl_DE41	Uniquely identifies the terminal which accepted the card. Always present if the card data was read by a terminal (i.e. field POS_Data_DE22 first two digits are any of: 02,03,04,05,06,07,08,80,90,91,92,95.) Otherwise may be omitted.	ANS(1,8)	1NDR01
POS_Time_DE12	This is the local time or date/time of the transaction in the time zone of the merchant or entity that accepted the card. The format varies depending on the message type as follows: For Authorisation messages (Transaction Type - Authorisation), the format is: “hhmmss” (hh=hour 00-23, mm=minute 00-59, ss=second 00-59.) **Note**: For Visa Authorisations, the time is optional, so this field may be blank. For Financial messages (Transaction Type - Financial, including dummy offline authorisations), the format is: “YYMMDDhhmmss” (YY=last 2	If Auth: N(6,6) or blank If Financial (inc. dummy auth): N(12,12)	If Auth: 141642 Empty-field If Financial: 991231141642 191129000000

Field	Description	Data Type (1)	Sample Data
	digits of year, MM=month 01-12, DD=day of month 01-31, hh=hour 00-23, mm=minute 00-59, ss=second 00-59.) **Note**: For Visa Financial format, the time is often "000000", so often only the YYMMDD will have a meaningful value.		
Proc_Code	Processing code for the transaction. See Processing Codes.	N(6,6)	090000
Resp_Code_DE39	This field is provided in 0120 (auth advice), 0400 (reversal request) and 0420 (reversal advice) messages to indicate the reason for the advice or reversal. You should check this field to determine whether the transaction was STIP approved or declined. For more information, see Resp_Code_DE39 Values. **Note**: For some Visa authorisation advices, this field is optional, so may be blank.	AN(2,2)	00
Ret_Ref_No_DE37	Document reference number supplied by the system. Retains the original source document of the transaction and assists in locating that source document.	ANP(1,12)	673001106898
Settle_Amt	Settlement amount in settlement currency, as received from the Network. Value varies per transaction types as follows: MTID/Txn_Type combinations listed in the section Transaction Type - Authorisation (auths, auth reversals): • the amount is always positive • The amount is the network converting the transaction amount into the settlement currency, and is not the net settlement amount MTID and Txn_Type combinations listed in the section Transaction Type - Financial (real financials and their reversals, dummy Auths): • The amount will have the same sign as the Bill_Amt	AmountSigned (19,4)	Authorisation: 67.0100 Financials: -189.2400 89.2400

Field	Description	Data Type [1]	Sample Data
	field: positive (e.g., 20.00) if the card is credited and negative (e.g., -20.00) if debited. • This amount will not include interchange or issuer fees – it is simply the transaction amount converted into the settlement currency by the network, then the sign adjusted to positive or negative. It is not the net settlement amount. For usage in transactions, see Examples of Amount Signs.		
Settle_Ccy	Settlement currency. ISO 3-digit numeric. See Currency Codes.	N(3,3)	978
Status_Code	Current status code of the card on the Thredd system. See Card Status Codes.	AN(2,2)	00
Token	Thredd public token of the card. The range includes values from 100000000 to 999999999 inclusive.	N(1,9)	231152625
Trans_link	An identifier used to link related transactions together. For details, see the Trans_Link Field Appendix.	N(1,19)	151231225367089085
Txn_Amt	Transaction amount, in the transaction currency (see Txn_CCy field). Always zero or positive. To identify whether this is a credit or debit, check the Proc_Code field. For usage in transactions, see Examples of Amount Signs.	AmountUnsigned(19,4)	189.2400
Txn_CCy	Currency in which transaction occurred. ISO 3-digit currency code. See Currency Codes.	N(3,3)	978
Txn_Ctry	Country code for the transaction. ISO 3-alpha country code. Upper case characters only.See Country Codes.	A(3,3)	NLD
Txn_Desc	Description of the transaction.	ANS(1,800)	Golff Harmelen HARMELEN NLD
Txn_GPS_Date	Date in which transaction occurred. It is 'GMT' in winter and 'GMT +1' in summer (BST stands for British Summer Time). Format: *YYYY-MM-DD hh:mm:ss.nnn* Where there is a space between the date and time fields, and nnn	Datetime (Y_to_nnn)	2015-11-05 13:11:30.910

Field	Description	Data Type[1]	Sample Data
	is the milliseconds. For TransactionType = A and MTID = 0100, this date is the time at the point just before Thredd sends the transaction to EHI.		
TXn_ID	Unique ID for the transaction, generated by Thredd. This should be used for duplicate checking. Maximum number will be 2^{53}-1. **Note**: Suitable for IEEE 754 binary-64 data type. See JSON Data Types and EHI Fields.	N(1,16)	51075303
Txn_Stat_Code	Transaction status code for the transaction. See Transaction Status Codes.	AN(1,1)	A
TXN_Time_DE07	Transmission Date and Time, in GMT (UTC) timezone. Date and time message was sent by the acquirer to MasterCard/Visa Network. Format: *MMDDhhmmss* Where: MM = Month of year 01-12 DD = Day of month 01-31 hh = hour of day 00-23 mm = minute of hour 00-59 ss = second 00-59	N(10,10)	0302131642
Txn_Type	Transaction type description for the transaction. See Transaction Types.	AN(1,1)	A
Additional_Data_DE48	Network Additional data DE48 field. Contact Thredd if there is any specific piece of information you need from here. Ignore unless mutually agreed with Thredd to extract certain data. **Note:** For certain sub-elements, Thredd may use a default value of "3" to replace the original content to keep the integrity of the data field. If your organisation is using a specific sub-element contained within a data field with a default value, please contact your Thredd account manager. **Note:** This field is passed through for scheme transaction risk scores, provided they are	ANS(1,5000)	For Mastercard Authorisation messages: 034T8202529203385420701032106105000000 For Mastercard Financial messages: 0002003MRG0003003MRG0023003NA 0146036002901840000000000023384 000000000023301480087842840 2 0158029MCC47840013412100304 NNNNN For VISA Authorisation message: 0B5CF0F0F1F9F7F2F1F4F2F0

Field	Description	Data Type (1)	Sample Data
	enabled by the Issuer as this is a chargeable service.		
Authorised_by_GPS	To identify whether authorised by Thredd or not for Stand-In enabled products: Y = Thredd can stand-in to authorise transaction in agreed circumstances. N = no stand-in authorisation	A(1,1)	Y
AVS_Result	The result of AVS checking. See AVS Results.	AN(1,1)	N
CU_Group	Group code assigned for usage checking.	ANS(1,10)	AER-CU-001
InstCode	Thredd Issuer (Program Manager) Code. Assigned by Thredd.	ANS(1,4)	TMS
MTID	The Message Type Identifier (MTID) describes the type of message being interpreted. 0100 = Authorisation Request 0400 = Reversal Request 0420 = Reversal Advice 1240 = Financial Notification (also used for Chargeback Notification for Mastercard and Visa; check TransactionType to tell the difference) '05 ' (05 with 2 spaces) = Financial Notification (Purchase from Visa) '06 ' (06 with 2 spaces) = Financial Notification (Credit from Visa) '07 ' (07 with 2 spaces) = Financial Notification (Cash from Visa) '25 ' (25 with 2 spaces) = Financial Reversal (of a Purchase from Visa) '26 ' (26 with 2 spaces) = Financial Reversal (of a Credit from Visa) '27 ' (27 with 2 spaces) = Financial Reversal (of Cash from Visa) For a full list, see Transaction Matching Criteria.	ANP(1,4)	For Mastercard Authorisation: 0100 For Mastercard presentment: 1240 For VISA Authorisation: 0100 For VISA presentment: ’05 ‘ ’06 ‘ ’07 ‘
ProductID	This value is the Product ID of the card. The Product ID is generated during product setup. For details, check with your Implementation	N(1,5)	1504

Field	Description	Data Type (1)	Sample Data
	Manager.		
Record_Data_DE120	This field is Mastercard-specific. DE 120 (Record Data) is a variable-length data element used for transmitting file record data or textual character string data in various message types.	ANS(1,1000)	For Mastercard: 018041414 For VISA: (empty)
SubBIN	The sub-BIN value assigned to the product. **Note:** Can only be used for 6-digit BINs. Displays the 6-digit BIN plus 2 additional sub-BIN digits. **Note:** For 8-digit BINs, displays the 8-digit BIN.	N(1,11)	6-digit BIN: 67592**12** (sub-BIN is last 2 digits) 8-digit BIN: 67592678 (no sub-BIN displayed)
TLogIDOrg	ID of original transaction for reversals. Maximum value will be 2^{53}-1. **Note**: Suitable for IEEE 754 binary-64 data type. See JSON Data Types and EHI Fields.	N(1,16)	0
VL_Group	Group code assigned for velocity checking.	ANS(1,10)	AVU-VL-005
Dom_Fee_Fixed	Domestic fixed fee amount applied to transaction by Thredd, in the card account currency. It is part of the Fixed_Fee. Domestic is defined as: Txn_CCy = Bill_Ccy Corresponds to your fee setup on the system.	AmountSigned (19,4)	0.0000
Non_Dom_Fee_Fixed	Non-domestic fixed fee amount applied t othe transaction by Thredd, in the card account currency. It is part of Fixed_Fee. Non-Domestic is defined as: Txn_CCy ≠ Bill_Ccy Corresponds to your fee setup on the system.	AmountSigned (19,4)	0.0000
Fx_Fee_Fixed	Fixed foreign exchange fee amount applied by Thredd to the transaction, in the card account currency. It is part of Fixed_Fee. Corresponds to your fee setup on the system. For example, if: • the "Fx Fixed" was "1.2000" (i.e., 1.20 in billing currency) in the fee configuration relevant for	AmountSigned (19,4)	0.0000

Field	Description	Data Type [1]	Sample Data
	this transaction • Bill_Amt=10.0000 • Txn_CCy = 840 • Bill_Ccy = 826 • Foreign exchange occurred (as Txn_Ccy ≠ Bill_Ccy) then Fx_Fee_Fixed Amount = 1.2000 (in account currency)		
Other_Fee_Amt	Other fees applied. It is part of Fixed_Fee.	AmountSigned (19,4)	0.0000
Fx_Fee_Rate	Fee Amount calculated by Thredd as part of the transaction, due to “Fx Rate” fee setting. It is part of Fixed_Fee. Corresponds to your fee setup on the system. For example, if: • the “Fx Rate” was “1.2000” (i.e., 1.20%) in the fee configuration relevant for this transaction • Bill_Amt=10.0000 • Txn_CCy = 985 • Bill_Ccy = 840 • Foreign exchange occurred (as Txn_CCy ≠ Bill_Ccy) then Fx_Fee_Rate Amount = 10.0000 * 0.0120 = 0.1200 (in account currency)	AmountSigned (19,4)	0.0000
Dom_Fee_Rate	Fee Amount calculated by Thredd as part of the transaction, due to “Dom Fee Rate” fee setting, in the card account currency. It is part of Fixed_Fee. Domestic is defined as: Txn_CCy = Bill_Ccy Corresponds to your fee setup on the system. For example, if: • The “Dom Fee Rate” fee setting was “1.7500” • Bill_Amt = 32.0000 • Txn_CCy = 978 • Bill_Ccy = 978 • Transaction is Domestic (as Txn_CCy = Bill_Ccy) Then Fee Amount due to “Dom Fee Rate” = 32.0000 * 0.0175 = 0.5600 (in account currency.)	AmountSigned (19,4)	0.0000

Field	Description	Data Type (1)	Sample Data
Non_Dom_Fee_Rate	Fee Amount calculated by Thredd, due to Non domestic rate fee setting, in the card account currency. It is part of Fee_Rate. Non-Domestic is defined as: Txn_CCy ≠ Bill_Ccy Corresponds to your fee setup on the system. For example, if: • The “Non Dom Fee Rate” fee setting was “2.00” (i.e. 2%) • Bill_Amt = 64.0000 • Txn_CCy = 840 • Bill_Ccy = 826 • Transaction is non-domestic (as Txn_CCy ≠ Bill_Ccy) Then Fee Amount due to “Non Dom Fee Rate” = 64.0000 * 0.0200 = 1.2800 (in account currency.)	AmountSigned (19,4)	0.0000
Additional_Data_DE124	This field is Mastercard specific. DE 124 is used only for MasterCard Money Send and transactions. In a Mastercard Networks Exchange SMS Network, acquirers can use DE 124 (Mastercard Networks Exchange Tags, Acquirer/Info, Text) to pass additional information to issuers on financial requests.	ANS(1,200)	For Mastercard: 19900064345324080218 01MC MONEY SEND ST SOVETSKAYA 58 For VISA: (empty)
CVV2	Cardholder Verification Value 2. This will only be present if configured for the customer. Format of this if present will be: • If 3 characters long: 3 digit CVV2 value • If 6 characters long: Position 1 (CVV2 presence indicator) Position 2 (CVV2 Response Type indicator)Position 3 (Space) Positions 4-6 (CVV2 Value) (Thredd always sends the 3-digit CVV2 values for Mastercard. For Visa Threddsends the 6-character version)	N(3,6)	Mastercard: 123 Visa: 11 123
Expiry_Date	Card or Token expiry date as received in transaction. Format: *YYMM* This will only be present if configured for by the Program Manager.	N(4,4)	2912

Field	Description	Data Type (1)	Sample Data
PAN_Sequence_ Number	PAN sequence number. Only present if sent by the acquirer.	N(1,2)	8
PIN	PIN block of format PIN_Format (see PIN Block Formats) encrypted under the EHI PIN Key of index = PIN_Key_Index using algorithm PIN_Enc_Algorithm. Present only if Online PIN message and customer is configured to receive it. If this field is present, then these fields will also be present: • PIN_Key_Index • PIN_Format • PIN_Enc_Algorithm	HEX(32,32)	B7A85096C4C5EE23
PIN_Enc_Algorithm	PIN block encryption algorithm. Describes the encryption algorithm used to encrypt the PIN in the PIN field. Values: • 3DES = Triple DES using ECB, using a triple length DES key. **Note**: Other values may be added in future versions. (This field is always present if PIN field is present)	AN(1,16)	3DES
PIN_Format	The format of the PIN block used as clear text before encryption to create the PIN field. PIN Block formats: 0 = ISO9564-1 Format 0 1 = ISO9564-1 Format 1 2 = ISO9564-1 Format 2 3 = ISO9564-1 Format 3 Currently only value '1' (implying ISO9564-1 Format 1) is supported. This is because it is the only PIN block format that varies for the same PIN and does not require a PAN. (This field is always present if the PIN field is present)	N(1,4)	1
PIN_Key_Index	Index of the PIN Key used to encrypt the PIN field. (This field is always present if the PIN field is present)	N(1,4)	2
SendingAttemptCount	Indicates the number of times Thredd has repeated this message: 0 = not repeated (1st transmit) 1 = repeated once (2nd transmit) 2 = repeated twice (3rd transmit) … n = repeated n times ((n+1)	N(1,4)	2

Field	Description	Data Type (1)	Sample Data
	transmit)		
source_bank_ctry	**Note**: This is Mastercard-specific. Source Bank Country code as ISO 3-alpha uppercase. See Country Codes.	A(3,3)	For Mastercard: GBR For VISA: (empty)
source_bank_account_format	Format of the bank account number in the source_bank_account field. See Bank Account Format.	AN(1,8)	For Mastercard: GBR For VISA: (empty)
source_bank_account	Source bank account number. In format specified by source_bank_account_format	ANP(1,34)	For Mastercard: 601608 39857710 For VISA: (empty)
dest_bank_ctry	Destination Bank Country code as ISO 3-alpha uppercase. See Country Codes.	A(3,3)	For Mastercard: GBR For VISA: (empty)
dest_bank_account_format	Format of the bank account number in the dest_bank_account field. See Bank Account Format.	AN(1,8)	For Mastercard: IBAN For VISA: (empty)
dest_bank_account	Destination bank account number. In format specified by dest_bank_account_format. See Bank Account Format.	ANP(1,34)	For Mastercard: GB29NWBK60161331926819 For VISA: (empty)
GPS_POS_Capability	Thredd defined POS Capability codes. Defines what the POS terminal capabilities are for this transaction. See GPS_POS_Capability.	AN(2,255)	1100100100010000000000010010010100000000019234CR
GPS_POS_Data	Thredd defined POS Data codes. Defines what happened at the POS terminal (e.g. card data input method). See GPS_POS_Data field.	AN(1,255)	0171000300002Nx000
Acquirer_Reference_Data_031	Acquirer Reference Number (ARN). This field is a 23 digit number for Mastercard and Visa transactions and an 8-digit alphanumerical value for Discover Global Network transactions. The acquirer reference number exists for clearing messages only (Financial advices/notifications, and Chargeback advices/notifications (and reversals of)). If MTID=1240 and Txn_Type='A'	N(23)	For Mastercard and VISA: 74456126366123456789014 For Discover: 000Or6P3

Field	Description	Data Type (1)	Sample Data
	(dummy auth created if no matching auth to the financial) – in this case there may or may not be Acquirer_Reference_Data_031 present. It is created by the acquirer in the first financial presentment, according to the scheme rules. It will be the same value for all clearing messages in the entire lifecycle. **Note**: Values should be unique per card scheme within a 10-year time period.		
Response_Source	Indicates which system sent the 0110 or 0210 response to the terminal. Normally present only for some Authorisation advices and Authorisation reversals. See Response_Source and Message_Source values. The field is ANS, but the special character is restricted to '_' (underscore) and '-' (minus sign), and special character will not begin the string.	ANS*(1,10) Special characters only '-' or '_'	VISA-STIP
Response_Source_Why	Indicates the reason why the Response_Source sent a response to the terminal. Normally present only for some Authorisation advices and Authorisation reversals. See Response_Source_Why and Message_Why values.	N(1,4)	1
Message_Source	Indicates which system sent this message. Normally present only for some Authorisation advices and Authorisation reversals. See Response_Source and Message_Source values. The field is ANS, but the special character is restricted to '_' (underscore) and '-' (minus sign), and special character will not begin the string.	ANS*(1,10) Special characters only '-' or '_'	MC-STIP
Message_Why	Indicates the reason why Response_Source sent a response to the terminal. Normally present only for some Authorisation advices and Authorisation reversals. See Response_Source_Why and Message_Why values.	N(1,4)	18
traceid_lifecycle	Lifecycle Trace ID. This consists of alphanumeric and '-' characters only. This is a value	ANS*(1,40) * * the only	VIS1-20160608-086160508692217 BNET-20151231-MRG9001AB

Field	Description	Data Type (1)	Sample Data
	assigned to the lifecycle of the transaction, which is identical for all messages relating to the same transaction. For example, the following messages relating to the same transaction will all have the same Lifecycle Trace ID value: *Authorisation*, *Second incremental authorisation*, *authorisation reversal*, *Financial Presentment*, *Chargeback*, *Second Presentment* and *Second chargeback*. If there is more than one authorisation for the same transaction, both authorisations will have the same value. This is a reliable matching field and should be used for matching in the first instance if present. **Construction of this field's value** The traceid_lifecycle is a concatenation of: *network_id + "-" + date_yyyymmdd + "-" + a unique identifier* For more information, see the FAQs: What is the traceid_ lifecycle field and how is it constructed? **Note**: We strongly advise you not to use hard-coded logic on your side based on the current format of this field, as Thredd may change the format of this field in the future. **Note**: Will be present in most messages, but may not be included in some Authorisation Reversals (e.g. timeout reversals) and some Financial messages which were not authorised online (e.g. refunds, offline approved transactions).	special character is "-" (hyphen)	
Balance_Sequence	Thredd balance sequence number. Incremented by 1 each time the actual_balance or blocked_amount of the card account changes on the Thredd system. Maximum value =2^{63}-1. This gives the external host an idea of how out-of-sync the Thredd actual_balance and blocked_amount fields are compared to the external host. This will always be present in any	N(1,19) Max value is 2^{63}-1.	568474

Field	Description	Data Type (1)	Sample Data
	transaction where external host can respond with a Balance Update (Update_Balance=1 in response.) This happens only in online transactions sent to EHI as soon as Thredd receives them (not for after-the-event transactions sent later to EHI via a queue mechanism at Thredd, e.g., presentments.)		
Balance_Sequence_Exthost	The external host balance sequence number received from the EHI response. See field 'New_Balance_Sequence_Exthost' in the section Response Field Formats. Maximum value = 2^{63}-1. Maintained by the External host. This tells the external host how recent Thredd's external balance is. A higher number indicates a more recent balance. This field will always be present in any transaction where external host can respond with a Balance Update (Update_Balance=1 in response.) This happens only in online transactions sent to EHI as soon as Thredd receives them (not for after-the-event transactions sent later to EHI via a queue mechanism at Thredd, e.g., presentments.)	N(1,19) Max value is 2^{63}-1.	450
PaymentToken_id	Unique Thredd ID of the payment token. Only present if transaction relates to a payment token (for example, Apple Pay).	N(1,10)	12345
PaymentToken_creator	Identifies which system created the payment token.Only present if the transaction relates to a payment token (for example, Apple Pay). See Response_Source and Message_Source.	AN(1,10)	For Mastercard: MC-MDES For VISA: VISA-T
PaymentToken_expdate	Expiry date of the payment token. Only present if the transaction relates to a payment token (for example, Apple Pay). Format *YYYY-MM-DD* **Note**: In the case of a Token Replacement message (MTID='0100', Txn_Type='A', Proc_Code='360000', Message_Why=52) then this contains the *new* payment token expiry date. (The previous payment-	Datetime(Y_to_D)	2099-12-31

Field	Description	Data Type (1)	Sample Data
	token expiry date is currently not included.)		
PaymentToken_type	The type of system the payment token is encoded onto (defines how the payment token PAN is held). Only present if the transaction relates to a payment token (for example, Apple Pay). See PaymentToken_type. **Note**: not to be confused with the device type (PaymentToken_deviceType).	AN(1,10)	SE
PaymentToken_status	Current status of the payment token as set by Thredd. Only present if the transaction relates to a payment token (for example, Apple Pay). See Card Status Codes.	AN(1,2)	00
PaymentToken_creatorStatus	Current status of the payment token as set by the creator of the payment token. Only present if the transaction relates to a payment token (for example, Apple Pay). See PaymentToken_creatorStatus.	AN(1,1)	A
PaymentToken_wallet	Wallet that the payment token belongs to. Only present if the transaction relates to a payment token (for example, Apple Pay). See PaymentToken_wallet.	AN(1,10)	APPLE
PaymentToken_deviceType	Indicates the type of the device in which the payment token is held. Only present if the transaction relates to a payment token (for example, Apple Pay). See PaymentToken_deviceType.	AN(1,10)	X
PaymentToken_lang	The ISO 639-1 2 character alpha language code reported by the payment token device at digitisation time. Only present if the transaction relates to a payment token (for example, Apple Pay). For a list of ISO 639-1 language codes, see http://www.iso.org **Note**: this may not be known, in which case the field will be empty.	A(0,2)	en
PaymentToken_deviceTelNum	The telephone number of the device on which the payment token is present, as reported by the creator at digitisation time. Only present if the transaction	ANS(0,15)	1 (656) 1234-3244

Field	Description	Data Type (1)	Sample Data
	relates to a payment token (for example, Apple Pay). **Note**: this may be empty, a full or partial number, and may be masked in various ways as the creator and/or wallet provider determines.		
PaymentToken_deviceIp	IPv4 address of the device on which the payment token is present, as reported by the creator at digitisation time. Only present if the transaction relates to a payment token (for example, Apple Pay). May arrive in either of 2 formats: Hex format: PPQQRRSS Where: • PP = 1st IP byte, as 2 hex digits (00 to FF) • QQ=2nd IP byte, as 2 hex digits (00 to FF) • RR=3rd IP byte, as 2 hex digits (00 to FF) • SS=4th IP byte, as 2 hex digits (00 to FF) Or decimal format: p.q.r.s Where: • p = 1st IP byte, in decimal (0 to 255) • q = 2nd IP byte, in decimal (0 to 255) • r = 3rd IP byte, in decimal (0 to 255) • s = 4th IP byte, in decimal (0 to 255) **Note**: each decimal number may be prefixed with 0, 1 or 2 leading zeros, up to a maximum of 3 decimal digits (eg byte “4” could be encoded as “4”, “04” or “004”.	ANS(1,15)	255.255.255.255 FFFFFFFF 081.5.006.255 A17F001E
PaymentToken_deviceId	Payment token device ID as reported by the Wallet service provider. Only present if the transaction relates to a payment token (for example, Apple Pay).	ANS(0,48)	ABCD 043B28DB7E478
PaymentToken_ deviceName	Payment token device name as given by the device owner (i.e., cardholder). Only present if the transaction relates to a payment token (for example, Apple Pay).	ANS(0,20)	Cookie Monster Phone
PaymentToken_ activationCode	Activation code that the	AN(1,8)	

Field	Description	Data Type (1)	Sample Data
	cardholder must enter into the payment token holding device to complete Tokenisation. Only present if the first two characters of Proc_Code="34" (payment token activation notification)		987654
PaymentToken_ activationExpiry	The Date and Time in UTC (GMT) that the activation code in the field PaymentToken_activationCode expires. Only present if the first two characters of Proc_Code="34" (payment token activation notification). **Note**: milliseconds are present, but will always be zero. For Mastercard, seconds will always be zero.	Datetime(Y_to_ nnn)	For Mastercard: 2019-12-31 23:59:00.000 For VISA: 2019-12-31 23:59:59.000
PaymentToken_ activationMethodData	Data to indicate the value corresponding the selected PaymentToken_activationMethod. Only present if the first two characters of Proc_Code="34" (payment token activation notification). See PaymentToken_ activationMethod.	ANS(1,255)	Siobhan@bananarama.co.uk
PaymentToken_ activationMethod	The method by which the cardholder should obtain the Activation Code (in the field PaymentToken_activationCode) which they must enter into the device holding the payment token in order to activate it. Only present if first two characters of Proc_Code="34" (payment token activation notification). See PaymentToken_ activationMethod.	N(1,4)	3
ICC_System_Related_ Data_DE55	EMV Chip data in TLV hex format: • Hexadecimal digits (0-9 and A-F) where 2 hexadecimal digits represent 1 byte, where the encoded bytes mean: ◦ EMV TLV data as Tag, Length, Value bytes encoded as Basic Encoding Rules (BER) as described in EMV Book 3 Annex B, Rules for BER-TLV data objects. • Note that all tags sent from the acquirer will be present (even if not defined by EMV)	HEX(0,512)	9F35012282021980

Field	Description	Data Type (1)	Sample Data
	Example (if sending tags 9F35 and 82) 9F35012282021980 For format of Tag, Length and Value: See EMV Book 4.3 (www.emvco.com) Annex B – "Rules for BER-TLV Data Objects" For definitions of Tags, see the following: • *EMV Book 3 Annex A – Data Elements Dictionary* • *EMV Book 3 Annex C – Coding of Data Elements Used in Transaction Processing* • *EMV Book 3 Annex A – Coding of Terminal Data Elements* For the definition of tag 9F10, and any tag in the range 9F50 – 9F7F inclusive, see the specification of the EMV chip card application that are used by the card. **Note:** This field applies to both Visa and Mastercard.		
Merch_Name	Merchant (or ATM owner) name. Many sources limit the Merchant/ATM-owner name to between 22 to 25 characters.	ANS(0,40)	Bananarama Fan Club
Merch_Street	Merchant/ATM street address. Not always provided.	ANS(0,80)	Flat 2, 3-19 St. Pancras Road
Merch_City	Merchant/ATM city. Many sources limit the city name at 13 characters	ANS(0,40)	Newcastle Upo
Merch_Region	Merchant/ATM region code. Defines a sub-region of a country. Usage varies per country. Not always provided. If Merch_Country=USA, this will be a 2-alpha US state code (e.g. "AK" for Alaska). If Merch_Country=CAN (i.e. Canada) this will be a 2-alpha Canadian province code (e.g. "QC" for Quebec). Other countries may put a region code in here.	ANS(0,3)	AK
Merch_Postcode	Merchant or ATM postal code. Postal code existence and format varies country to country. Not always provided.	ANS(0,20)	A6-12 34
Merch_Country	Merchant or ATM country code.	A(3)	USA

Field	Description	Data Type (1)	Sample Data
	ISO 3-alpha country code. See Country Codes. **Note:** Inclusion of this field is typically *optional*, but may be *mandatory*, depending on the program or service being processed. For more information, refer to the Card Scheme documentation.		
Merch_Tel	Merchant (or ATM operator) telephone number. Provided occasionally by some merchants	ANS(25)	+1 (636) - 0363
Merch_URL	Merchant website URL. Provided by some merchants.	ANS(255)	http://petshopboys.co.uk/
Merch_Name_Other	Alternative merchant name. This could be the Sole Trader or Legal name if provided.	ANS(40)	Governor and Company of the Bank of Engl
Merch_Net_id	Merchant ID assigned by Visa or Mastercard. The card networks assign unique merchant IDs to some merchants (generally larger ones).	ANS(30)	F9800D0001
Merch_Tax_id	Merchant's Tax ID (reference), if provided.	ANS(30)	ABCDE12345FGHIJ67890
Merch_Contact	Merchant alternative contact details. Provided occasionally. (For example, may contain an email address, secondary phone numbers, customer service operation hours and contact name.)	ANS(30)	Mark-F_Knopfler@markknopfler.c
auth_type	Type of authorisation request, as indicated by the acquirer. 0 = normal/undefined P = Preauth (amount will be an estimate) F = Final auth (amount is correct and for the full amount. No incremental auths will be received after this.) V = Account Verification Blank/empty = not applicable (e.g. for non-authorisation message types). **Note**: See `auth_expdate_utc` below for how long the authorisation block should survive.)	AN(1,1)	P

Field	Description	Data Type (1)	Sample Data
auth_expdate_utc	Expiry date and time of this authorisation in UTC/GMT, as set by the acquirer or estimated by Thredd. This field only applies to Authorisations and Authorisation Advices (MTID/Txn_Type combinations: '0100'/'A' or '0120'/'J'.) For both, this is when the authorisation expires, but note the following: • If the auth_type field indicates a pre-auth (value 'P') then this will be the UTC/GMT time when the pre-auth expires. It is calculated from the time Thredd receives the pre-auth, then adding the number of days the acquirer indicates it should survive for. • If the auth_type field is not pre-auth (not 'P') then this is Thredd's estimate of how long the authorisation should survive. It may not be 100% accurate (as Thredd may be unaware of all timeliness criteria, which can be changed at any time by Visa/Mastercard.)	Datetime(Y_to_nnn)	2019-12-31 23:59:59.000
Matching_Txn_ID	For Authorisation Reversals, Incremental Authorisations, Incremental Authorisation Reversals and first presentments this is set to the TXn_ID field of the original authorisation that this transaction Thredd matched it to. For all other transactions, it will be blank. Maximum value is 2^{53}-1. **Note:** For offline authorisations or where Thredd does not receive an original authorisation due to any reason, Thredd will not populate the Matching_Txn_ID field. **Note**: Suitable for IEEE 754 binary-64 data type. See JSON Data Types and EHI Fields.	N(1,16)	6634938
Reason_ID	For various messages, this contains a value explaining the reason for the message. • For chargebacks, it contains the chargeback reason.	N(1,4)	For Mastercard chargeback: 4808 For Visa chargeback: 11

Field	Description	Data Type (1)	Sample Data
	• For Visa authorisation-related messages, it contains the Visa Message Reason Code (from Visa Base 1 field 63.3) • For other messages, it may describe the reasons for these. See Reason ID. Maximum value: 9999		For Visa Auths/Reversals: 3900
Dispute_Condition	Additional information, in addition to Reason_ID field. For Visa chargebacks, it contains the Visa Dispute Condition. For other messages, it is currently not used. See Dispute Condition.	ANS(1,3)	For Visa chargeback: 6.1
Network_Chargeback_Reference_Id	The reference numbers assigned by VISA or MasterCard during VROL or Mastercom initiated chargebacks.	N(1,19)	Visa: 0000001000 Mastercard: 0000000300002329285
Acquirer_Forwarder_ID	Identifies the acquiring institution forwarding a Request or Advice message.	N(1,11)	000405700
Currency_Code_Fee	Currency code of the interchange fee. ISO 3-digit currency code. See Currency Codes.	N(3,3)	876
Currency_Code_Fee_Settlement	Currency code that the interchange fee will be settled in. ISO 3-digit currency code. See Currency Codes.	N(3,3)	876
Interchange_Amount_Fee	Interchange fee amount in the currency defined in Currency_Code_Fee. The interchange fee is an additional amount charged by the Card Scheme, Issuer or Acquirer. For example: • POS transactions – positive interchange fee is paid to the issuer • ATM transactions – negative interchange fee is paid to the operator of the ATM • ATM card capture – fee is paid to the operator of the ATM • Stolen card fee – interchange fee is paid to the issuer These fees are only finalised at the presentment stage when settlement and transfer of funds	AmountSigned (15,6)	01.020000

Field	Description	Data Type (1)	Sample Data
	occurs. You should factor your fee structure in line with potential network fees.		
Interchange_Amount_Fee_Settlement	Interchange fee amount in the currency defined in Currency_Code_Fee_Settlement.	AmountSigned (15,6)	01.020000
Clearing_Process_Date	Indicates the clearing system's processing date expressed in the local time zone of the clearing system's processing centre. This is referred to as the Reconcilliation Date in the Thredd Transaction XML (for details, see the *Transaction XML Guide*).	Datetime(Y_to_D)	2099-12-31
Settlement_Date	Identifies the date when the schemes settlement services initiate the movement of funds for settlement. **Note**: This date may be different from Clearing_Process_Date if files are processed on days which settlement banks are closed.	Datetime(Y_to_D)	For Mastercard: 2099-12-31 For Visa: 2099-12-31
DCC_Indicator	Indicates whether Dynamic Currency Conversion (DCC) has taken place. 0 = DCC has not been performed 1 = DCC has been performed	N(1,1)	1
multi_part_txn	Indicates whether the message is any part of a multi-auth/clearing sequence. 0 = Message is not part of a multi-auth/clearing sequence or no information was received from the acquirer 1= Message is any part of a multi-auth/clearing sequence **Note**: This field is as received by Thredd; if the value received from the acquirer is blank, then the field is populated with *0*.	N(1,1)	1
multi_part_txn_final	Indicates whether the message is the final part of a multi-auth/clearing sequence. 0 = Message is not the final part of a multi-auth/clearing sequence or no information was received from the acquirer 1 = Message is the final part of a multi-auth/clearing sequence	N(1,1)	1

Field	Description	Data Type (1)	Sample Data
	Note: This field is as received by Thredd; if the value received from the acquirer is blank, then the field is populated with *0*.		
multi_part_number	Only available for Visa transactions. Indicates what part of a multi-auth/clearing sequence the message is. This value will not be higher than the total parts in multi_part_count field. 0 = N/A or unknown part number.	N(2,2)	For Mastercard: Blank For Visa: 05
multi_part_count	Only available for Visa transactions. Indicates how many parts there are in the multi-auth/clearing sequence. 0 = N/A or unknown.	N(2,2)	For Mastercard: Blank For Visa: 09
SettlementIndicator	Defines what settlement service the network will use to settle transactions: 0 = International Settlement Services 3 = Clearing Only 4 = Bilateral Settlement 8 = National Net Settlement Services	N(1,1)	0
Network_TxnAmt_To_BillAmt_Rate	The card network's currency conversion rate that they used to convert Txn_Amt into Bill_Amt. The rate used will be associated with the Network_Currency_Conversion_Date field. There will normally be seven significant figures in the rate, as that is what Visa and Mastercard currently send.	Rate	0000001:6 0000000:0
Network_TxnAmt_To_BaseAmt_Rate	The card network's currency conversion rate used to convert Txn_Amt into the network's base amount (often in US Dollars). This can be used in conjunction with Network_BaseAmt_To_BillAmt_Rate to understand how the Network converted Txn_Amt into Bill_Amt. For Visa Base2, this is what arrives in Draft Data TCR5's *Source Amount to Base Amount conversion rate* field; there will always be six significant figures. **Note**: The network Base Amount is not provided, as Thredd do not receive this.	Rate	Visa Financials: 987654:12
Network_BaseAmt_To_BillAmt_Rate	The card network's currency	Rate	Visa Financials:

Field	Description	Data Type (1)	Sample Data
	conversion rate used to convert from the network's base amount (often in US Dollars) to the Bill_Amt. This can be used in conjunction with Network_TxnAmt_To_BaseAmt_Rate to understand how the Network converted Txn_Amt into Bill_Amt. For Visa Base2, this is what arrives in Draft Data TCR5's *Base Amount to Destination Amount conversion rate* field; there will always be six significant figures. **Note**: The network Base Amount is not provided, as Thredd do not receive this.		987654:3
POS_Date_DE13	Terminal local date of transaction. The network normally provides the date as MMDD, and Thredd will add YYYY which most likely corresponds to it. MMDD will be transmitted exactly as received, even if invalid. Thredd will set the YYYY to '0000' if MMDD received is not a valid date.	DatetimeRaw (Y_to_D)	20240617
Traceid_Message	The card network's reference. Data reflects exactly what was received. • Mastercard: date is from DE15, reference is from DE63 (exactly as provided.) • Visa: date is from Transaction ID DE62.2, reference is Transaction ID DE62.2 (exactly as provided) This should always be valid, except for a Visa message if the acquirer provided an invalid value.	TraceidRaw	Mastercard: BNET-19991231-MCC1234XY Visa: VIS1-19991231-489365789012345
Traceid_Original	The card network's original reference. Data reflects exactly what was received, and may or may not be valid. • Mastercard: date MMDD is from DE48.63 positions 10-13, with YYYY completed by Thredd (or '0000' if MMDD is not a valid date. Reference is from DE48.63 positions 1-9.	TraceidRaw	Mastercard Authorisations: BNET-0000pppp-000000000 (where 'p' is a space) BNET-20201231-SUR9876UX Visa Authorisations: VIS1-00000000-000000000000000 VIS1-20201231-660366000004444

<table>
<tr><th>Field</th><th>Description</th><th>Data Type (1)</th><th>Sample Data</th></tr>
<tr><td></td><td>Visa: date is from Original Transaction ID DE125, dataset 3 Tag 3, reference is Original Transaction ID DE125, dataset 3 Tag 3 (exactly as provided)</td><td></td><td></td></tr>
<tr><td>Network_Currency_ Conversion_Date</td><td>The card network’s currency conversion date. Reflects the date of Visa/Mastercard currency conversion rate used in the transaction came from. MMDD is supplied by the network, Thredd add the corresponding year YYYY. If the MMDD received from the network is not a valid date, Thredd will set YYYY to ‘0000’.</td><td>DatetimeRaw (Y_to_D)</td><td>2020-12-31</td></tr>
<tr><td>Mastercard_ AdviceReasonCode_ DE60</td><td>Mastercard Authorisation Advice Reason Code (field 60).
Explains why Mastercard Stand-In processing (STIP) occurred or why an advice was created.
This field has a length of 999, but currently Mastercard send a maximum of 60. Format:
First 3 digits = Advice Reason Code – this indicates the main reason for the advice
Next 4 digits: Advice Detail Code – generally ‘0000’ indicates ‘Accept’ (e.g. by STIP or X-Code), and all other values indicate a decline/error detail
Everything else: Advice Detail text – human readable text message
See Mastercard_ AdviceReasonCode_DE60.</td><td>ANS(1,999)</td><td>400

4002000

1010000</td></tr>
<tr><td>Network_Original_Data_ Elements_DE90</td><td>The raw network data present in online reversals to explain which original (MTID=0100) the reversal is referring to. Format:<table><tr><th>Positions</th><th>Length</th><th>Content</th></tr><tr><td>1-4</td><td>4</td><td>Original MTID</td></tr><tr><td>5-10</td><td>6</td><td>Original STAN</td></tr><tr><td>11-20</td><td>10</td><td>Original transmission datetime MMDDhhmmss</td></tr></table></td><td>N(42,42)</td><td>0100481019042200131600000476666000000000

0100000000000000000000000000000000000000

0100988836050600052400000459535000004564
56

0100231528050523501600000013445000002003
53</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th><th>Data Type (1)</th><th>Sample Data</th></tr>
<tr><td></td><td>
<table>
<tr><th>Positions</th><th>Length</th><th>Content</th></tr>
<tr><td>21-31</td><td>11</td><td>Original Acquirer ID</td></tr>
<tr><td>32-42</td><td>11</td><td>Original Forwarder ID</td></tr>
</table>
This is provided to aid diagnostics in exception cases.
Note: This field is as received by Thredd; data accuracy depends on the acquirer.
</td><td></td><td></td></tr>
<tr><td>Visa_ResponseInfo_DE44</td><td>Visa Base1 field 44 - Visa's Additional Response Data, exactly as provided from Visa to Thredd. This will only be present for transactions received by Thredd from Visa Base1, if DE44 was present.
It provides information on Visa's validation checks of data in the message. This will only be set for Visa online authorisation transactions.</td><td>ANS(25)</td><td>pppppppppMppp2
pppp2ppp2
(where p is a space)</td></tr>
<tr><td>Visa_STIP_Reason_Code</td><td>Visa Base 1 field 63.4 STIP/Switch Reason Code. This maybe present for Visa online authorisation advices and reversals, to explain why Visa STIP responded instead of Thredd. This will only be set for Visa online authorisation-related transactions (MTID=0120 and MTID=0420).</td><td>N(4,4)</td><td>9045</td></tr>
<tr><td>Network_Issuer_Settle_ID</td><td>A multi-purpose field providing additional settlement data:
For Mastercard: this field provides the member ID (ICA) of the Issuer responsible for the transaction (IPM DE93).
For Visa: Not supported</td><td>N(6,11)</td><td>019111</td></tr>
<tr><td>Network_Replacement_Amounts_DE95</td><td>DE95 replacement amounts from the card network. Used in reversals and completion advices to advise of the new amounts.
It is received only if the reversal is partial. Otherwise, it is blank.
Note: Currently applicable to Visa network transactions only. For Mastercard the reversal</td><td>AN(42,42)</td><td>000000000778000000000000000000007780000000
000000000147000000000000000000001470000000</td></tr>
</table>

Field	Description	Data Type (1)	Sample Data
	amount is stated in the Bill_Amt field. Format for Mastercard: • Positions 1-12: Actual transaction amount in minor units. • Positions 13-24: Actual settlement amount in minor units • Positions 25-36: Actual cardholder billing amount in minor units • Positions 37-42 fixed '000000'. Format for Visa: • Positions 1-12: Actual transaction amount in minor units. • Positions 13-42: Not used (zero filled)		
Visa_POS_Data_DE60	Visa Base 1 field 60 – Additional POS Data. Thredd already map the Visa POS data into the GPS_POS_Data and GPS_POS_Capability fields, which Thredd recommend to use in preference. This will only be set for Visa online authorisation transactions. **Note**: the raw Visa POS Data is also provided for extra information.	N(2,12)	00 0109 0100000007 750000400023
Network_Transaction_ID	The raw transaction ID, exactly as received from the card network without any alteration. Present only if received. Thredd load this as follows: • Visa Online: 16 hexdigits of the DE62.2 Visa Transaction ID. The leading hexdigit should be a '0' padding character. (Format HEX(16,16).) • Visa Clearing: 15 characters, which should all be digits. (15 '0' characters indicates unknown.) (Format N (15,15).) • Mastercard Online: DE63 concatenated with DE15 (Format ANS(1,13)) • Mastercard Clearing: DE63 (Format ANS(1,16)) **Note**: Thredd provide this to aid resolving exception messages. Thredd recommend you use	ANS(1,16)	Mastercard Authorisations: SUR9876UX1231 Mastercard Financials: pSUR9876UX1231 (where 'p' is a space) Visa Authorisations: 0489365789012345 Visa Financials: 489365789012345

Field	Description	Data Type [1]	Sample Data
	traceid_lifecycle instead.		
Misc_TLV_Data	Miscellaneous data. See section Misc_TLV_Data field. **Note**: Thredd expect you to normally ignore this field. It is used to contain rarely used pieces of data that are not normally required for transaction processing. The field maximum is 8000, however in EHI 4.1, we never expect this to be more than 200.	TLV10(0,8000)	V12503000300160489365863994444
Acquirer_Country	If present, contains the ISO 3-alpha uppercase country code of the acquirer. **Note**: This field is available on EHI version 5.0 and beyond.	A(3,3)	GBR
PaymentToken_ PanSource	Describes the originator of a Tokenisation Authorisation Request. For possible values, see PaymentToken_PanSource. **Note**: This field is available on EHI version 5.0 and beyond.	AN (1,1)	4
ClearingFileID	Populated for Clearing records. Shows the File ID of the file that contains the presentment record. **Note**: This field is available on EHI version 5.0 and beyond.	ANS (1, 50)	Visa: 444444020191220C0409OCE Mastercard: T112.00201010100000999674011O1
Network_Fraud_Data	Contains Fraud or Risk Indicators received from the card network. See Network_Fraud_Data Format. **Note**: This field is available on EHI version 5.0 and beyond.	AN (1, 32)	Visa: “011099 1122 013099 33 “ Mastercard: “00599903 0079990507 “
SenderData	Contains the sender details in a money transfer message (Visa OCT or Mastercard Money Send) This field is represented as a Tag-Length-Value (TLV) record with the following order and lengths: • Tag - two characters • Length - two decimal digits • Data - the number of characters	ANS (1, 512)	0106Mickey0305Mouse0411Main Street0508Annaheim0703USA

Field	Description	Data Type (1)	Sample Data
	as given by the length See SenderData and ReceiverData Fields. **Note**: This field is available on EHI version 5.0 and beyond.		
ReceiverData	Contains the receiver details in a money transfer message (Visa OCT or Mastercard Money Send). This field is represented as a Tag-Length-Value (TLV) record, with the following order and lengths: • Tag - two characters • Length - two decimal digits • Data - the number of characters as given by the length See SenderData and ReceiverData Fields. **Note**: This field is available on EHI version 5.0.	ANS (1, 512)	0106Mickey0305Mouse0411Main Street0508Annaheim0703USA
AuthenticationAmountUpper	The maximum authentication amount in the currency specified in the AuthenticationCurrency, as provided during a 3D Secure authentication session. This field can be used to confirm whether the amount that was submitted for authentication is the same as the amount that was submitted for authorisation. For details, see Checking fields used for 3D Secure Authentication. **Note**: For Visa, the authentication amount is the exact amount authenticated. For Mastercard, if AuthenticationAmountUpper is a value of 14000 or below in the minor units of currency, then it is exact. If AuthenticationAmountUpper is a value of more than 14000 in the minor units of currency, then it is the maximum possible Authentication Amount from the approximate value that Thredd received from Mastercard.	AmountUnsigned(14,4)	562.342
AuthenticationCurrency	The 3-digit authentication currency code, used for AuthenticationAmountUpper.	N(3,3)	036

Field	Description	Data Type (1)	Sample Data
AuthenticationMerchantHash	A hash of the merchant name as received at the authentication stage, in decimal digits or hex digits. For Visa, this is the *Information Data* provided by the Access Control Server (ACS), which may contain the merchant name hash, '00000000' or an IP address[1]. For Mastercard, this field contains the hash (using SHA 256) of the merchant name.	AN (8,8)	Mastercard: D36A8275 Visa: 01765342
FxProviderCardholderRate	Provides the Currency Cloud Foreign Exchange (FX Rate) sent in the authorisation message.	DECIMAL (19,9)	1234.000000000
SchemeTransactionIdentifier	Business Application ID (Visa) or Transaction Type Identifier (Mastercard) received in an authorisation message for an Original Credit Transaction (OCT) or Account Funding Transaction (AFT). • For Visa – this is a concatenation of VIS1 + a 2 digit transaction identifier • For Mastercard – this is a concatenation of BNET+ a 3 digit transaction identifier For details, see Scheme Transaction Identifier Values. **Note:** Available on GetTransaction version 5.1 onwards	AN (0,7)	Visa: VIS1BB Mastercard: BNETC01
TokenUniqueReference	The unique token reference as supplied by the token creator in a tokenisation message (MDES or VDEP transaction). **Note:** Available on GetTransaction version 5.1 onwards	AN (0,48)	VDEP: DNITHE582599999942043245 MDES: DM4MMC1PT0000000be3ec16ef999999ab7d4b47da4456277
PaymentTokenPan	The DPAN (Device Primary Account Number), which is a tokenised version of the card number used in digital transactions. This field is only populated if the transaction uses a payment token.	AN(0,16)	5372XXXXX6767765

[1]For Visa, this is the hashed value of Merchant Name as provided in the Authentication Request (data element ‘merchantName’ in AReq) or Payer Authentication Request (DTD element ‘Merchant.name’ in PAReq) message. SHA-256 to be used, first 8 numerical digits (digits 0 through 9) from the result of hashing to be used. If 8 numerical digits are not found, subtract 10 from all character digits (digits A through F) and use the first result(s) for as many digits missing of the 8 digit value.

Field	Description	Data Type (1)	Sample Data
	Note: This field is available from EHI version 5.1 onwards.		

(1) Data Types - lists the data type; depending on the datatype, numbers in parentheses represent either (*minimum,maximum*) or (*precision,scale*); for details, see Data Types.

2.5.2 Rounding off of currencies with exponents greater than 2

Thredd can store received currency amounts with a value of up to four decimal places. For currencies with exponents greater than 2, we round this to 2 decimal places and add zero padding for the remaining decimal places. For example:

- Value received: 12.3456.
- Rounded off to: 12.3500

This applies to the following fields of data type AmountSigned and AmountUnsigned, received in *authorisation messages only*:

ActBal, Avl_Bal,Bill_AmtBlkAmt, FX_Pad, Fee_Fixed, Fee_Rate, MCC_Pad, Settle_Amt, Dom_Fee_Fixed, Non_Dom_Fee_Fixed, Fx_Fee_Fixed, Other_Fee_Amt, Fx_Fee_Rate, Dom_Fee_Rate, Non_Dom_Fee_Rate.

2.5.3 Response Field Formats

Definition of response message field formats:

Field	Description	Data type	Sample Data
Responsestatus	Response Code for the authorisation request. See Responsestatus Values. **Note**:If sending value “10” (partial approval), then response field Bill_Amt_Approved must be provided too.	AN(2,2)	00
CurBalance	Actual balance on card after the transaction. Positive means the card is in credit. Negative means the card is in debit.	AmountSigned(9,2)	189.24
AvlBalance	Available balance on card after the transaction. Positive means the card is in credit. Negative means the card is in debit.	AmountSigned(9,2)	89.24
Acknowledgement	Notification message for the transaction is acknowledged or not. Valid values are: 0 = Not Acknowledged (i.e. Thredd should re-transmit this); 1 = Acknowledged	N(1,1)	1
LoadAmount	This column must contain the amount that needs to be loaded to the card if approval is with an '0A' (Approve with Load) response code. Applicable only to Cooperative Processing (mode 2) with ‘Approve with Load’ feature set on.	AmountUnsigned (9,2)	100.45
Bill_Amt_Approved	Contains the amount approved in the billing currency code (Bill_Ccy.) This is mandatory for all partial approval messages, to inform the acquirer how much of the transaction amount is approved. Note that partial approval (Resp_Code_DE39="10") is only permitted if GPS_POS_Capability position 1 (partial approval support indicator) is 1 (partial approval supported by POS)	AmountSigned(9,2)	-52.64

<table>
<tr><th>Field</th><th>Description</th><th>Data type</th><th>Sample Data</th></tr>
<tr><td></td><td>It should have the same sign as Bill_Amt in the request message. However, Thredd will take the absolute value of this (for example, sending -52.64 is the same as sending 52.64).
<table>
<tr><th>Transaction is approved (Resp_Code_DE39="00")</th><th>Transaction is partially approved (Resp_Code_DE39="10")</th><th>Transaction is declined</th></tr>
<tr><td>Bill_Amt_Approved is included and contains the same value as Bill_Amt in the request message
-Or -
Bill_Amt_Approved is not present</td><td>Bill_Amt_Approved must be present and contain a value between 0 and Bill_Amt (but non-zero, and not Bill_Amt)</td><td>Bill_Amt_Approved must be zero or not present</td></tr>
</table></td><td></td><td></td></tr>
<tr><td>Update_Balance</td><td>Indicates whether Thredd should update stand-in balances.
0=do not update balance (default); 1=update balance (using CurBalance_GPS_STIP and AvlBalance_GPS_STIP as provided in this response)
Note: You should only respond with ‘1’ (update balance) if you have received both Balance_Sequence and Balance_Sequence_Exthost in the request message.
Note: the Thredd stand-in balances can also be updated via the WS_BalanceUpdate web service or the API Hub STIP Balance Update endpoint.</td><td>N(1,1)</td><td>0</td></tr>
<tr><td>New_Balance_Sequence_Exthost</td><td>New external host balance sequence number for this card account.
New balance (and this New_Balance_Sequence_Exthost number) to be installed if both Update_Balance=1, AND this balance sequence number is strictly higher than the existing external host balance sequence number (CARDS.bal_seqno_exthost). Use of this will prevent Thredd from installing an out-of-date balance.
External host usage:
Each time the external host returns a balance, it should include this number.
The external host should increment this number each time it changes the card balance.
Numbers do not need to be sequential.
Thredd interprets a higher number as indicating a more recent balance
Example:
External host sends Thredd two response messages:
Message A: CurBalance=11.11; AvlBalance=22.22; Update_Balance=1
New_Balance_Sequence_Exthost = 18
Message B: CurBalance=77.77 ; AvlBalance=88.88; Update_Balance=1
New_Balance_Sequence_Exthost=20

Since the New_Balance_Sequence_Exthost in message B is higher than message A, Thredd will always apply the</td><td>N(1,19)

Max possible value is $2^{63}-1$</td><td>95736</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th><th>Data type</th><th>Sample Data</th></tr>
<tr><td></td><td>balances from Message B, irrespective of which message is received first.</td><td></td><td></td></tr>
<tr><td>CVV2_Result</td><td>Used only if CVV2 is present in request. M=Match; N=No-match.
Any other values other than M and N will cause a format error rejection.
Note: If the CVV2_Result field is blank, then the merchant did not provide this information. In this case, Thredd will not complete the CVV2 pre-check and will authorise or decline the transaction based on the card usage group settings for your programme.</td><td>A(1,1)</td><td>M</td></tr>
<tr><td>AvlBalance_GPS_STIP</td><td>Similar to AvlBalance, this field is used in Gateway Processing with STIP (mode 4 only) to update the available Thredd stand-in balance. It will only be used to approve or decline EHI messages where a response from the External Host is not received and it will be decremented with every approval.
It is never sent back to the card network for any response message where the acquirer is expecting the card's available balance, such as Balance Inquiry transactions. Instead, the AvlBalance field, if sent by the External Host, is used for this purpose.</td><td>AmountSigned (9,2)</td><td>120.32</td></tr>
<tr><td>CurBalance_GPS_STIP</td><td>Similar to CurBalance, this field is used in Gateway Processing with STIP (mode 4) to update the current Thredd stand-in balance.</td><td>AmountSigned (9,2)</td><td>129.32</td></tr>
<tr><td>MerchantAdvice</td><td>If this field is included, then it contains a Merchant Advice Code, to tell the merchant whether to re-try the transaction on a decline. See below for possible values.
<table><tr><th>Value</th><th>Description</th><th>Examples</th></tr><tr><td>01</td><td>Merchant needs updated or additional information.</td><td>Expired card - merchant needs to retry after obtaining the new card expiry date. Incorrect CVV1/CVV2 or AVS - merchant needs corrected data to retry.</td></tr><tr><td>02</td><td>Merchant should re-try the transaction later.</td><td>Insufficient funds (more funds may be available later). Short-term temporary card block (card will be re-enabled soon).</td></tr><tr><td>03</td><td>Merchant should not retry again.</td><td>Only used for a stolen, destroyed card or closed account. Future transactions will never be approved.
Warning: If you return an "03" value in your response to a Mastercard network authorisation request (applicable to Program Managers using EHI Gateway or Cooperative</td></tr></table></td><td>N(2,2)</td><td>01</td></tr>
</table>

Field	Description	Data type	Sample Data
	processing) you must not approve any future transactions on this card or Mastercard may impose fines. For details, see the FAQs: What is the MerchantAdvice field and how is it used? If not included, then for declines on Mastercard cards, Thredd will set the Merchant Advice automatically based on the Responsestatus provided. **Note**: This field is available from EHI version 5.0 onwards.		

2.5.4 Transaction Type Decoding

When a GetTransaction message is received, the receiver should use the MTID and Txn_Type fields as follows to determine which of the below sections is appropriate to decode it.

MTID	Txn_Type	Description	Transaction Type decoding
0100	A	Authorisation Request	Transaction Type - Authorisation
	D	Automatic Authorisation Reversal	Transaction Type - Authorisation
0101	A	Authorisation Repeat (Visa Only)	Transaction Type - Authorisation
0120	J	Authorisation Advice	Transaction Type - Authorisation
0120	D	Authorisation Reversal Advice (due to AFD 0120 auth advice)	Transaction Type - Authorisation
0400	D	Authorisation Reversal Request	Transaction Type - Authorisation
0420	D	Authorisation Reversal Advice	Transaction Type - Authorisation
1240 05pp 06pp 07pp (p = space)	A	Authorisation Advice Notification (Dummy authorisation created if a Financial notification has no matching authorisation.)	Transaction Type - Financial
1240 25pp	E	Financial Reversal	Transaction Type - Financial

MTID	Txn_Type	Description	Transaction Type decoding
26pp 27pp (p = space)			
1240	C	Chargeback Notification	Transaction Type - Financial
1240	H	Chargeback Notification (Non-Credit)	Transaction Type - Financial
1240	K	Chargeback Reversal	Transaction Type - Financial
1240 05pp 06pp 07pp (p = space)	N	Financial Notification (Second Presentment)	Transaction Type - Financial
1240 05pp 06pp 07pp (p = space)	P	Financial Notification (First Presentment)	Transaction Type - Financial
	L	Load	Transaction Types - Non-Card-Network Transactions
	U	Unload	Transaction Types - Non-Card-Network Transactions
	G	Payment	Transaction Types - Non-Card-Network Transactions
	B	Balance Adjustment	Transaction Types - Non-Card-Network Transactions
	Y	Card Expiry	Transaction Types - Non-Card-Network Transactions
	F	Fee	Transaction Types - Non-Card-Network Transactions

2.5.5 Transaction Type - Authorisation

Authorisation message types are used for the following Message Type Identifier MTID types:

MTID	Txn_Type	Description
0100	A	Authorisation Request. If this arrives with: Txn_Stat_Code = “I” (declined) Authorised_By_GPS = “Y” (Thredd authorised the transaction) Then this means that the authorisation is being re-sent as an advice, to inform you that Thredd authorised this transaction, and the response code used was Resp_Code_DE39. This should be accepted as an advice.
	D	Automatic Authorisation reversal. This is created by Thredd system to unblock the authorised amount when all the following have happened: • an 0100 approved authorisation request was received by Thredd • No matching reversal or matching financial for this authorisation has been received • A configurable amount of time has elapsed. This will ensure that outstanding authorisations which never have a financial do not permanently block the account.
0101	A	Authorisation Repeat (Visa Only).
0120	J	Authorisation Advice This is an advice received from the network, normally to advise of a MTID=0110 response generated by the network sent to the acquirer. (In case where for some reason or other, the Thredd 0110 response does not exist or could not be used.)
0400	D	Reversal Request Note: although this is an 0400 message, it cannot be declined, as it is telling you a reversal has already happened. There is no difference in practice between 0400 and 0420 - treat both as reversal advices.
0420	D	Reversal Advice

Request Message Fields (Authorisation Messages)

The following fields are included in an authorisation request message:

Field	Usage		Field	Usage		Field	Usage
Acquirer_id_DE32	Optional		VL_Group	Optional		Merch_Street	Optional
ActBal	Mandatory		Dom_Fee_Fixed	Mandatory		Merch_City	Mandatory
Additional_Amt_DE54	Optional		Non_Dom_Fee_Fixed	Mandatory		Merch_Region	Optional
Amt_Tran_Fee_DE28	Optional		Fx_Fee_Fixed	Mandatory		Merch_Postcode	Optional
Auth_Code_DE38	Optional		Other_Fee_Amt	Mandatory		Merch_Country	Optional*
Avl_Bal	Mandatory		Fx_Fee_Rate	Mandatory		Merch_URL	Optional
Bill_Amt	Mandatory		Dom_Fee_Rate	Mandatory		Merch_Name_Other	Optional
Bill_Ccy	Mandatory		Non_Dom_Fee_Rate	Mandatory		Merch_Net_id	Optional

Field	Usage		Field	Usage		Field	Usage
BlkAmt	Mandatory		Additional_Data_DE124	Optional		Merch_Tax_id	Optional
Cust_Ref	Optional		CVV2	Optional		Merch_Contact	Optional
FX_Pad	Mandatory		Expiry_Date	Optional		auth_type	Optional
Fee_Fixed	Mandatory		PAN_Sequence_Number	Optional		auth_expdate_utc	Optional
Fee_Rate	Mandatory		PIN	Optional		Matching_Txn_ID	Optional
LoadSRC	Optional		PIN_Enc_Algorithm	Optional		Reason_ID	Optional
LoadType	Optional		PIN_Format	Optional		Dispute_Condition	Optional
MCC_Code	Optional		PIN_Key_Index	Optional		Network_Chargeback_Reference_Id	Optional
MCC_Desc	Optional		SendingAttemptCount	Mandatory		Acquirer_Forwarder_ID	Optional
MCC_Pad	Mandatory		source_bank_ctry	Omitted		DCC_Indicator	Optional
Merch_ID_DE42	Optional		source_bank_account_format	Omitted		multi_part_txn	Optional
Merch_Name_DE43	Mandatory		source_bank_account	Omitted		multi_part_txn_final	Optional
Note	Optional		dest_bank_ctry	Omitted		multi_part_number	Optional
POS_Data_DE22	Optional		dest_bank_account_format	Omitted		multi_part_count	Optional
POS_Data_DE61	Optional		GPS_POS_Capability	Mandatory		SettlementIndicator	Optional
POS_Termnl_DE41	Optional		GPS_POS_Data	Optional		Clearing_Process_Date	Optional
POS_Time_DE12	Optional		Acquirer_Reference_Data_031	Omitted		Settlement_Date	Optional
Proc_Code	Mandatory		Response_Source	Optional		Currency_Code_Fee	Optional
Resp_Code_DE39	Depends on EHI mode: Mode 1: Optional Mode 2: Optional Mode 3: Mandatory Mode 4 : Optional		Response_Source_Why	Optional		Currency_Code_Fee_Settlement	Optional
Ret_Ref_	Optional		Message_Source	Optional		Interchange_Amount_Fee	Optional

Field	Usage		Field	Usage		Field	Usage
No_DE37							
Settle_Amt	Optional		Message_Why	Optional		Interchange_Amount_Fee_Settlement	Optional
Settle_Ccy	Optional		traceid_lifecycle	Optional		Traceid_Message	Optional
Status_Code	Mandatory		Balance_Sequence	Optional		Traceid_Original	Optional
Token	Mandatory		Balance_Sequence_Exthost	Optional		Network_Transaction_ID	Optional
Trans_link	Mandatory		PaymentToken_id	Optional		POS_Date_DE13	Optional
Txn_Amt	Mandatory		PaymentToken_creator	Optional		Network_Currency_Conversion_Date	Optional
Txn_CCy	Mandatory		PaymentToken_expdate	Optional		Network_TxnAmt_To_BillAmt_Rate	Optional
Txn_Ctry	Optional		PaymentToken_type	Optional		Network_TxnAmt_To_BaseAmt_Rate	Omitted
Txn_Desc	Optional		PaymentToken_status	Optional		Network_BaseAmt_To_BillAmt_Rate	Omitted
Txn_GPS_Date	Mandatory		PaymentToken_creatorStatus	Optional		Network_Original_Data_Elements_DE90	Optional
TXn_ID	Mandatory		PaymentToken_wallet	Optional		Network_Replacement_Amounts_DE95	Optional
Txn_Stat_Code	Mandatory		PaymentToken_deviceType	Optional		Network_Issuer_Settle_ID	Omitted
TXN_Time_DE07	Mandatory		PaymentToken_lang	Optional		Visa_ResponseInfo_DE44 Optional	(Visa only)
Txn_Type	Mandatory		PaymentToken_deviceTelNum	Optional		Visa_POS_Data_DE60 Optional	(Visa only)
Additional_Data_DE48	Optional		PaymentToken_deviceIp	Optional		Visa_STIP_Reason_Code Optional	(Visa only)
Authorised_by_GPS	Optional		PaymentToken_deviceId	Optional		Mastercard_AdviceReasonCode_DE60 Optional	(Mastercard only)
AVS_Result	Optional		PaymentToken_deviceName	Optional		Misc_TLV_Data	Optional
CU_Group	Optional		PaymentToken_activationCode	Optional		Network_Fraud_Data	Mandatory
InstCode	Mandatory		PaymentToken_activationExpiry	Optional		SenderData	Optional
MTID	Mandatory		PaymentToken_	Optional		ReceiverData	Optional

Field	Usage		Field	Usage		Field	Usage
			activationMethod				
ProductID	Mandatory		PaymentToken_ PanSource	Optional		AuthenticationCurrency	Optional
Record_ Data_DE120	Optional		PaymentToken_ activationMethodData	Optional		AuthenticationAmountUppe r	Optional
Acquirer_ Country	Optional		ICC_System_ Related_Data_DE55	Optional		AuthenticationMerchantHas h	Optional
SubBIN	Mandatory		VL_Group	Optional		FxProviderCardholderRate	Optional
TLogIDOrg	Optional		Merch_Name	Mandatory		SchemeTransactionIdentifi er	Optional (v5.1 onwards)
			PaymentTokenPan	Optional (v5.1 onwards)		TokenUniqueReference	Optional (v5.1 onwards)

* The `MerchCountry` field is typically optional, but note that in certain cases the Card Schemes may consider this field as mandatory. For details, please check the Card Scheme documentation.

Usage Notes

- **Omitted** - can be omitted (fields not included) or included with an empty value (e.g.`"Bill_Ccy": ""`)
- **Optional** - can be omitted (fields not included) or included with an empty value. Can be present (e.g., `"Bill_Ccy": "0"`)
- **Mandatory** - field must be present. For example: `"Bill_Ccy": "978"`

Response Message Fields

The following fields must be present in an authorisation response message:

IMPORTANT: Response field values are case sensitive.

IMPORTANT: Do not return the value "null" in any response fields which require numeric values, as this will result in EHI declining the transaction. Exclude fields that are optional, if you do not want to return any values.

Field	Usage
Responsestatus	Mandatory
CurBalance	Conditional: If Proc_Code begins “30” (Balance enquiry) AND transaction is being approved THEN: Gateway Processing (modes 1 and 4): Must be provided Cooperative Processing (mode 2): Should be provided if Thredd balance does not reflect actual account balance Full Service Processing (mode 3): not required Otherwise: optional
AvlBalance	Conditional: IF Proc_Code begins “30” (Balance enquiry) AND transaction is being approved THEN: Gateway Processing (modes 1 and 4): Must be provided

Field	Usage
	Cooperative Processing (mode 2): Should be provided if Thredd balance does not reflect actual account balance Full Service Processing (mode 3): not required Otherwise: optional
Acknowledgement	Mandatory
LoadAmount	Optional
Bill_Amt_Approved	Optional
Update_Balance	Optional
New_Balance_Sequence_ Exthost	Optional
CVV2_Result	Optional
AvlBalance_GPS_STIP	Conditional: Required if Update_Balance=1 Otherwise optional.
CurBalance_GPS_STIP	Conditional: Required if Update_Balance=1 Otherwise optional.
MerchantAdvice	Optional

2.5.6 Transaction Type – Financial

Financial message types are used for the following message types:

MTID	Txn_Type	Description
1240 05pp 06pp 07pp (p = space)	A	Authorisation Advice notification (Dummy authorisation created if a Financial notification has no matching authorisation.)
1240	C	Chargeback notification
1240	H	Chargeback (non-credit) notification
1240	K	Chargeback reversal
1240 05pp 06pp 07pp (p = space)	P	Financial notification (first presentment)
1240 25pp	E	Financial Reversal notification

MTID	Txn_Type	Description
26pp 27pp (p = space)		
1240 05pp 06pp 07pp (p = space)	N	Financial notification (second presentment)

Request Message Fields (Financial Messages)

The following fields must be present in a Financial request message:

Field	Usage		Field	Usage
Acquirer_id_DE32	Optional		dest_bank_account_format	Omitted
ActBal	Mandatory		dest_bank_account	Omitted
Additional_Amt_DE54	Optional		GPS_POS_Capability	Mandatory
Amt_Tran_Fee_DE28	Optional		GPS_POS_Data	Optional
Auth_Code_DE38	Optional		Acquirer_Reference_Data_031	Mandatory
Avl_Bal	Mandatory		Response_Source	Omitted
Bill_Amt	Mandatory		Response_Source_Why	Omitted
Bill_Ccy	Mandatory		Message_Source	Omitted
BlkAmt	Mandatory		Message_Why	Omitted
Cust_Ref	Optional		traceid_lifecycle	Optional
FX_Pad	Mandatory		Balance_Sequence	Optional
Fee_Fixed	Mandatory		Balance_Sequence_Exthost	Optional
Fee_Rate	Mandatory		PaymentToken_id	Optional
LoadSRC	Optional		PaymentToken_creator	Optional
LoadType	Optional		PaymentToken_expdate	Optional
MCC_Code	Optional		PaymentToken_type	Optional
MCC_Desc	Optional		PaymentToken_status	Optional
MCC_Pad	Mandatory		PaymentToken_creatorStatus	Optional
Merch_ID_DE42	Optional		PaymentToken_wallet	Optional

Field	Usage		Field	Usage
Merch_Name_DE43	Mandatory		PaymentToken_deviceType	Optional
Note	Optional		PaymentToken_lang	Optional
POS_Data_DE22	Optional		PaymentToken_deviceTelNum	Optional
POS_Data_DE61	Optional		PaymentToken_deviceIp	Optional
POS_Termnl_DE41	Optional		PaymentToken_deviceId	Optional
POS_Time_DE12	Optional		PaymentToken_deviceName	Optional
Proc_Code	Mandatory		PaymentToken_activationCode	Omitted
Resp_Code_DE39	Optional		PaymentToken_activationExpiry	Omitted
Ret_Ref_No_DE37	Optional		PaymentToken_activationMethod	Omitted
Settle_Amt	Optional		PaymentToken_activationMethodData	Omitted
Settle_Ccy	Optional		ICC_System_Related_Data_DE55	Optional
Status_Code	Mandatory		Merch_Name	Mandatory
Token	Mandatory		Merch_Street	Optional
Trans_link	Mandatory		Merch_City	Mandatory
Txn_Amt	Mandatory		Merch_Region	Optional
Txn_CCy	Mandatory		Merch_Postcode	Optional
Txn_Ctry	Optional		Merch_Country	Optional*
Txn_Desc	Optional		Merch_Tel	Optional
Txn_GPS_date	Mandatory		Merch_URL	Optional
TXn_ID	Mandatory		Merch_Name_Other	Optional
Txn_Stat_Code	Mandatory		Merch_Net_id	Optional
TXN_Time_DE07	Optional		Merch_Tax_id	Optional
Txn_Type	Mandatory		Merch_Contact	Optional
Additional_Data_DE48	Optional		Auth_Type	Optional
Authorised_by_GPS	Optional		auth_expdate_utc	Optional
AVS_Result	Optional		Matching_Txn_ID	Optional
CU_Group	Optional		Reason_ID	Optional
InstCode	Mandatory		Dispute_Condition	Optional

Field	Usage		Field	Usage
MTID	Mandatory		Network_Chargeback_Reference_Id	Optional
ProductID	Mandatory		Acquirer_Forwarder_ID	Optional
Record_Data_DE120	Omitted		DCC_Indicator	Optional
SubBIN	Mandatory		multi_part_txn	Optional
TLogIDOrg	Optional		multi_part_txn_final	Optional
VL_Group	Optional		multi_part_number	Optional
Dom_Fee_Fixed	Mandatory		multi_part_count	Optional
Non_Dom_Fee_Fixed	Mandatory		SettlementIndicator	Optional
Fx_Fee_Fixed	Mandatory		Clearing_Process_Date	Optional
Other_Fee_Amt	Mandatory		Settlement_Date	Optional
Fx_Fee_Rate	Mandatory		Currency_Code_Fee	Optional
Dom_Fee_Rate	Mandatory		Currency_Code_Fee_Settlement	Optional
Non_Dom_Fee_Rate	Mandatory		Interchange_Amount_Fee	Optional
Additional_Data_DE124	Optional		Interchange_Amount_Fee_Settlement	Optional
CVV2	Omitted		Traceid_Message	Optional
Expiry_Date	Optional		Traceid_Original	Optional
PAN_Sequence_Number	Optional		Network_Transaction_ID	Optional
PIN	Omitted		POS_Date_DE13	Optional
PIN_Enc_Algorithm	Omitted		Network_Currency_Conversion_Date	Omitted
PIN_Format	Omitted		Network_TxnAmt_To_BillAmt_Rate	Optional
PIN_Key_Index	Omitted		Network_TxnAmt_To_BaseAmt_Rate	Optional (Visa only)
SendingAttemptCount	Mandatory		Network_BaseAmt_To_BillAmt_Rate	Optional (Visa only)
source_bank_ctry	Omitted		Network_Original_Data_Elements_DE90	Omitted
source_bank_account_format	Omitted		Network_Replacement_Amounts_DE95	Omitted
source_bank_account	Omitted		ReceiverData	Optional
ClearingFileId	Optional		FxProviderCardholderRate	Optional
dest_bank_ctry	Omitted			

Response Message Fields (Financial Messages)

The following fields must be present in the Financial response message:

Field	Usage
Responsestatus	Optional
CurBalance	Optional
AvlBalance	Optional
Acknowledgement	Mandatory
LoadAmount	Optional
Bill_Amt_Approved	Optional
Update_Balance	Optional
New_Balance_Sequence_Exthost	Optional
CVV2_Result	Optional
AvlBalance_GPS_STIP	Conditional: Required if Update_Balance=1 Otherwise optional.
CurBalance_GPS_STIP	Conditional: Required if Update_Balance=1 Otherwise optional.

2.5.7 Transaction Types – Non-Card-Network Transactions

This section is for non-card-network originated transactions (i.e., where the cardholder has not used their card to perform this transaction, the transaction is not received from Visa or Mastercard, but another source, such as Web Services/Cards API or BACS). As a result, the card network specific fields are not present (e.g., MTID and Acquirer ID (Acquirer_id_DE32) are not present.)

The following message types are non-card-network transactions:

MTID	Txn_Type	Description
n/a (not present)	L	Load
n/a (not present)	U	Unload
n/a (not present)	G	Payment
n/a (not present)	B	Balance Adjustment
n/a (not present)	Y	Card Expiry
n/a (not present)	P	Fee

Request Message Fields (Non-Card Network Messages)

The following fields must be present in non-card-network transaction request message:

Field	Usage		Field	Usage
Acquirer_id_DE32	Omitted		dest_bank_account	Optional
ActBal	Mandatory		GPS_POS_Capability	Omitted
Additional_Amt_DE54	Omitted		GPS_POS_Data	Omitted
Amt_Tran_Fee_DE28	Omitted		Acquirer_Reference_Data_031	Omitted
Auth_Code_DE38	Omitted		Response_Source	Omitted
Avl_Bal	Mandatory		Response_Source_Why	Omitted
Bill_Amt	Mandatory		Message_Source	Omitted
Bill_Ccy	Mandatory		Message_Why	Omitted
BlkAmt	Mandatory		traceid_lifecycle	Omitted
Cust_Ref	Optional		Balance_Sequence	Omitted
FX_Pad	Mandatory		Balance_Sequence_Exthost	Omitted
Fee_Fixed	Mandatory		PaymentToken_id	Omitted
Fee_Rate	Mandatory		PaymentToken_creator	Omitted
LoadSRC	Optional		PaymentToken_expdate	Omitted
LoadType	Optional		PaymentToken_type	Omitted
MCC_Code	Omitted		PaymentToken_status	Omitted
MCC_Desc	Omitted		PaymentToken_creatorStatus	Omitted
MCC_Pad	Omitted		PaymentToken_wallet	Omitted
Merch_ID_DE42	Omitted		PaymentToken_deviceType	Omitted
Merch_Name_DE43	Omitted		PaymentToken_lang	Omitted
Note	Optional		PaymentToken_deviceTelNum	Omitted
POS_Data_DE22	Omitted		PaymentToken_deviceIp	Omitted
POS_Data_DE61	Omitted		PaymentToken_deviceId	Omitted
POS_Termnl_DE41	Omitted		PaymentToken_deviceName	Omitted
POS_Time_DE12	Omitted		PaymentToken_activationCode	Omitted

Field	Usage		Field	Usage
Proc_Code	Mandatory		PaymentToken_activationExpiry	Omitted
Resp_Code_DE39	Omitted		PaymentToken_activationMethod	Omitted
Ret_Ref_No_DE37	Omitted		PaymentToken_activationMethodData	Omitted
Settle_Amt	Optional		ICC_System_Related_Data_DE55	Optional
Settle_Ccy	Optional		Merch_Name	Omitted
Status_Code	Mandatory		Merch_Street	Omitted
Token	Mandatory		Merch_City	Omitted
Trans_link	Mandatory		Merch_Region	Omitted
Txn_Amt	Mandatory		Merch_Postcode	Omitted
Txn_CCy	Mandatory		Merch_Country	Optional*
Txn_Ctry	Optional		Merch_Tel	Omitted
Txn_Desc	Optional		Merch_URL	Omitted
Txn_GPS_Date	Mandatory		Merch_Name_Other	Omitted
TXn_ID	Mandatory		Merch_Net_id	Omitted
Txn_Stat_Code	Mandatory		Merch_Tax_id	Omitted
TXN_Time_DE07	Omitted		Merch_Contact	Omitted
Txn_Type	Mandatory		auth_type	Omitted
Additional_Data_DE48	Omitted		auth_expdate_utc	Omitted
Authorised_by_GPS	Omitted		Matching_Txn_ID	Omitted
AVS_Result	Omitted		Reason_ID	Omitted
CU_Group	Optional		Dispute_Condition	Omitted
InstCode	Mandatory		Network_Chargeback_Reference_Id	Omitted
MTID	Omitted		Acquirer_Forwarder_ID	Omitted
ProductID	Mandatory		DCC_Indicator	Omitted
Record_Data_DE120	Omitted		multi_part_txn	Omitted
SubBIN	Mandatory		multi_part_txn_final	Omitted
TLogIDOrg	Omitted		multi_part_number	Omitted
VL_Group	Optional		multi_part_count	Omitted

Field	Usage		Field	Usage
Dom_Fee_Fixed	Mandatory		SettlementIndicator	Omitted
Non_Dom_Fee_Fixed	Mandatory		Clearing_Process_Date	Omitted
Fx_Fee_Fixed	Mandatory		Settlement_Date	Omitted
Other_Fee_Amt	Mandatory		Currency_Code_Fee	Omitted
Fx_Fee_Rate	Mandatory		Currency_Code_Fee_Settlement	Omitted
Dom_Fee_Rate	Mandatory		Interchange_Amount_Fee	Omitted
Non_Dom_Fee_Rate	Mandatory		Interchange_Amount_Fee_Settlement	Omitted
Additional_Data_DE124	Omitted		Traceid_Message	Omitted
CVV2	Omitted		Traceid_Original	Omitted
Expiry_Date	Omitted		Network_Transaction_ID	Omitted
PAN_Sequence_Number	Omitted		POS_Date_DE13	Omitted
PIN	Omitted		Network_Currency_Conversion_Date	Omitted
PIN_Enc_Algorithm	Omitted		Network_TxnAmt_To_BillAmt_Rate	Omitted
PIN_Format	Omitted		Network_TxnAmt_To_BaseAmt_Rate	Omitted
PIN_Key_Index	Omitted		Network_BaseAmt_To_BillAmt_Rate	Omitted
SendingAttemptCount	Mandatory		Network_Original_Data_Elements_DE90	Omitted
source_bank_ctry	Optional		Network_Replacement_Amounts_DE95	Omitted
source_bank_account_format	Optional		Network_Issuer_Settle_ID	Omitted
source_bank_account	Optional		Visa_ResponseInfo_DE44	Omitted
dest_bank_ctry	Optional		Visa_POS_Data_DE60	Omitted
dest_bank_account_format	Optional		Visa_STIP_Reason_Code	Omitted

Response Message Fields

The following fields must be present in a non-card-network response message:

Field	Usage
Responsestatus	Optional
CurBalance	Optional
AvlBalance	Optional

Field	Usage
Acknowledgement	Mandatory
LoadAmount	Optional
Bill_Amt_Approved	Optional
Update_Balance	Omitted
New_Balance_Sequence_Exthost	Omitted
CVV2_Result	Optional
AvlBalance_GPS_STIP	Optional
CurBalance_GPS_STIP	Optional

2.6 Cut_Off Messages

You can optionally enable receiving batch cut-off messages which provide summary information of the data sent via EHI. The frequency of cut-off messages is configurable.

Tip: The recommended frequency is 2-3 times per day.

2.6.1 Message Fields

The following fields are included in the *Cut_Off* message:

Field	Description	Data type (min, max)	Sample Data	Usage
CutoffID	A unique identifier of the cut_off message.	N(1,9)	12	Mandatory
ProductID	The Product ID of the card.	N(1,9)	1504	Mandatory
CutoffDate	Date and time of this cut_off message.	Datetime (Y_to_nnn)	2021-03-02 13:16:42.999	Mandatory
FirstTxn_ID	First Txn_ID in this cut_off period. Maximum is 2^63-1.	N(1,19)	1234564	Mandatory
LastTxn_ID	Last Txn_ID in this cut_off period. Maximum is 2^63-1.	N(1,19)	4523587	Mandatory
Auths_Acknowledged	Number of acknowledged Authorisations during this cut_off	N(1,9)	5000	Mandatory
Auths_NotAcknowledged	Number of un-acknowledged Authorisations during this cut_off	N(1,9)	100	Mandatory
Financials_Acknowledged	Number of acknowledged Financials during this cut_off	N(1,9)	5000	Mandatory
Financials_ NotAcknowledged	Number of un-acknowledged Financials during this cut_off	N(1,9)	100	Mandatory
LoadsUnloads_ Acknowledged	Number of acknowledged Loads/Unloads during this cut_off	N(1,9)	5000	Mandatory
LoadsUnloads_ NotAcknowledged	Number of un-acknowledged Loads/Unloads during this cut_off	N(1,9)	100	Mandatory
BalanceAdjustExpiry_ Acknowledged	Number of acknowledged Balance Adjustment and Expiry during this cut_off	N(1,9)	5000	Mandatory
BalanceAdjustExpiry_ NotAcknowledged	Number of un-acknowledged Balance Adjustment and Expiry during this cut_off	N(1,9)	100	Mandatory

2.6.2 Response Message Fields

The following fields must be present in the Cut_off response message:

Field	Description	Data type (min,max)	Sample Data	Usage
Cut_ OffResult	Valid values: 0 = Not Acknowledged (in a future release, Thredd may re-transmit the cut off message.) 1 = Acknowledged	N(1,1)	1	Mandatory

2.7 HTTP Message Format

EHI messages are HTTP 1.1 formatted, according to RFC 2616 and any superseding RFCs such as RFCs 7230 and RFC 7231.

2.7.1 Request Message

The outgoing request message is a HTTP/1.1 POST request. The header fields are specified below. The body data is the JSON fields of the GetTransaction message or Cut-Off message. For details, see GetTransaction Message Fields and Cut_Off Messages.

2.7.2 Request Header Fields

Header	Content example	Status	Comment
host	192.168.51.16	Mandatory	IP of the sending host, set by the sending host (Thredd).
traceparent	00-c24a548a2883cf4aac38eb40410a5e5d-593f9603da624910-00	Optional	Identifies the incoming request in a tracing system. For details see the W3.org description of Traceparent Header.
content-type	application/json	Mandatory	Indicates JSON formatted content.
content-length	778	Mandatory	Length of the body in bytes.

Request Body Fields

For details, see GetTransaction Message Fields and Cut_Off Messages.

2.7.3 Response Message

The incoming response message is a valid HTTP/1.1 response. The header fields are specified below, and the body data is the XML data of either the GetTransaction response or the Cut_Off response. For details, see GetTransaction Message Fields and Cut_Off Messages.

2.7.4 Response Header Fields

Header	Content example	Status	Comment
host	192.168.51.16	Mandatory	IP of the sending host, set by the sending host (Program Manager systems).
traceparent	00-c24a548a2883cf4aac38eb40410a5e5d-593f9603da624910-00	Optional	Identifies the incoming request in a tracing system. For details see the W3.org description of Traceparent Header.
content-type	application/json	Mandatory	Indicates JSON formatted content.
content-length	778	Mandatory	Length of the body in bytes.
other items	Various	Optional	Other standard headers permitted in the

Header	Content example	Status	Comment
			HTTP/1.1 as valid for the response may be included.

Response Body Fields

For details, see For details, see GetTransaction Message Fields and Cut_Off Messages.

SECTION 3: JSON EXAMPLES

This section provides examples of common transaction messages and responses.

3.1 GetTransaction Example Messages

This section provides examples of common transaction messages and responses. This section includes these topics:

- Example Authorisation
- Example Authorisation Reversal
- Example Financial Presentment (Mastercard)
- Example Financial Reversal (Visa)
- Example Financial Reversal (Mastercard)
- Example Visa Authorisation Advice
- Example Mastercard Authorisation Advice
- Example Balance Enquiry Message
- Example ATM Cash Withdrawal Messages (Mastercard)
- Example Tokenisation Messages
- Example Incremental Authorisation Messages
- Examples of Amount Sign

Note: EHI_JSON_Guide_5.1 The EHI feed does not send JSON fields to externally-hosted systems where the values for the field data are blank. This is different from EHI feeds with XML fields where the feed can send blank values.

3.1.1 Example Authorisations

Authorisation Request

Below is an example of the HTTP POST body data for an authorisation request.


```
{
  "Acquirer_Country": "GBR",
  "FxProviderCardholderRate": 0.0,
  "POS_Date_DE13": "00000000",
  "Traceid_Message": "VIS1-20221219-002353117950020",
  "Visa_POS_Data_DE60": "020000000000",
  "Network_Transaction_ID": "0002353117950020",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2022-12-27 07:28:36.045",
  "Merch_Name": "Travel Like A Pro",
  "Merch_Country": "HRV",
  "GPS_POS_Capability": "000010010000000000000001000100100010000000001130C0",
  "GPS_POS_Data": "9968000800000Nx000NNNNNU0NUUXXU",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "VIS1-20221219-002353117950020",
  "Balance_Sequence": 114,
  "Balance_Sequence_Exthost": 0,
  "Acquirer_id_DE32": "0844622180",
  "ActBal": 10001.0000,
  "Auth_Code_DE38": "143088",
  "Avl_Bal": 10001.0000,
  "Bill_Amt": 1.0000,
  "Bill_Ccy": "826",
  "BlkAmt": 0.0000,
  "FX_Pad": 0.0000,
  "Fee_Fixed": 0.0000,
  "Fee_Rate": 0.0000,
  "MCC_Code": "4111",
  "MCC_Desc": "Commuter Transport, Ferries",
  "MCC_Pad": 0.0000,
```

```
  "Merch_ID_DE42": "4111",
  "Merch_Name_DE43": "Travel Like A Pro HR",
  "POS_Data_DE22": "0110",
  "Proc_Code": "200000",
  "Resp_Code_DE39": "00",
  "Ret_Ref_No_DE37": "235303502517",
  "Settle_Amt": 1.0000,
  "Settle_Ccy": "826",
  "Status_Code": "00",
  "Token": 107419774,
  "Trans_link": "221219002517622180",
  "Txn_Amt": 1.0000,
  "Txn_CCy": "826",
  "Txn_Ctry": "HRV",
  "Txn_Desc": "Travel Like A Pro HR",
  "Txn_GPS_Date": "2022-12-19 07:28:37.526",
  "TXn_ID": 6155805913,
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "1219072835",
  "Txn_Type": "A",
  "Authorised_by_GPS": "N",
  "CU_Group": "DEF_PV",
  "InstCode": "TEST",
  "MTID": "0100",
  "ProductID": 99883,
  "SubBIN": 44622180,
  "TLogIDOrg": 0,
  "VL_Group": "MLMS_PV_GB",
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "PIN": "0",
  "SendingAttemptCount": 0
}
```


Note: The above example does not include all available fields as not all fields are required for a message. For example, in the above message, the Network_Replacement_Amounts_DE95 field is not required as part of the message.

Authorisation Response

Below is an example of HTTP response to the above Authorisation request message.


```
{
    "MerchantAdvice":"",
    "Responsestatus":"00",
    "CurBalance":0,
    "AvlBalance":100,
    "Acknowledgement":"1",
    "LoadAmount":50,
    "Bill_Amt_Approved":0,
    "Update_Balance":1,
    "New_Balance_Sequence_Exthost":200,
    "CVV2_Result":"M",
    "CurBalance_GPS_STIP":0,
    "AvlBalance_GPS_STIP":100
}
```

3.1.2 Example Authorisation Reversal

Authorisation Reversal Request

Below is an example of the HTTP POST body data for an Authorisation Reversal message.


```
{
  "AuthenticationAmountUpper": 0.0000,
  "FxProviderCardholderRate": 0.0,
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2022-12-26 07:27:14.180",
  "Matching_Txn_ID": 0,
  "Reason_ID": 0,
  "Merch_Name": "Travel Like A Pro",
  "Merch_Country": "HRV",
  "Merch_Tax_id": "0",
  "GPS_POS_Capability": "00110000100000000000000000000000100000000001016",
  "GPS_POS_Data": "0168000800000Nx000",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20221219-MC 004279",
  "PaymentToken_id": 0,
  "PaymentToken_creatorStatus": " ",
  "PaymentToken_lang": "  ",
  "PaymentToken_activationMethod": 0,
  "Acquirer_id_DE32": "0852729540",
  "ActBal": 3535.47,
  "Amt_Tran_Fee_DE28": "D00000010",
  "Auth_Code_DE38": "183715",
  "Avl_Bal": 3401.72,
  "Bill_Amt": 10.00,
  "Bill_Ccy": "826",
  "BlkAmt": -133.75,
  "FX_Pad": 0.00,
  "Fee_Fixed": 0.50,
  "Fee_Rate": 0.00,
  "MCC_Code": "4111",
  "MCC_Desc": "Commuter Transport, Ferries",
  "MCC_Pad": 0.00,
  "Merch_ID_DE42": "4111           ",
  "Merch_Name_DE43": "Travel Like A Pro HRV",
  "Note": "Testing  User - Dhanya.B Date - 19/12/2022 16:18:08 BillAmt - 10.00 Location - Travel Like A Pro    ",
  "POS_Data_DE22": "010",
  "POS_Data_DE61": "2000000006000191",
  "POS_Termnl_DE41": "        ",
  "POS_Time_DE12": "072714",
  "Proc_Code": "000000",
  "Resp_Code_DE39": "00",
  "Ret_Ref_No_DE37": "235303504279",
  "Settle_Amt": 10.00,
  "Settle_Ccy": "826",
  "Status_Code": "00",
  "Token": 107612119,
  "Trans_link": "221219004279729540",
  "Txn_Amt": 10.0000,
  "Txn_CCy": "826",
  "Txn_Ctry": "HRV",
  "Txn_Desc": "Travel Like A Pro HRV",
  "Txn_GPS_Date": "2022-12-19 10:48:03.580",
  "TXn_ID": 6155806244,
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "1219072714",
  "Txn_Type": "D",
  "Authorised_by_GPS": "N",
```

```
  "CU_Group": "CRN-CU-001",
  "InstCode": "TEST",
  "ProductID": 99884,
  "SubBIN": 52729540,
  "TLogIDOrg": 0,
  "VL_Group": "CRN-VL-100",
  "Dom_Fee_Fixed": 0.50,
  "Non_Dom_Fee_Fixed": 0.00,
  "Fx_Fee_Fixed": 0.00,
  "Other_Fee_Amt": 0.00,
  "Fx_Fee_Rate": 0.00,
  "Dom_Fee_Rate": 0.00,
  "Non_Dom_Fee_Rate": 0.00,
  "SendingAttemptCount": 0
}
```


Note: The above example does not include all available fields as not all fields are required for a message. For example, in the above message, the Network_Original_Data_Elements_DE90 field is not required as part of the message.

Authorisation Reversal Response

Below is an example of HTTP response to the above Authorisation Reversal message.


```
{
    "MerchantAdvice":"",
    "Responsestatus":"00",
    "CurBalance":0,
    "AvlBalance":100,
    "Acknowledgement":"1",
    "LoadAmount":50,
    "Bill_Amt_Approved":0,
    "Update_Balance":1,
    "New_Balance_Sequence_Exthost":200,
    "CVV2_Result":"M",
    "CurBalance_GPS_STIP":0,
    "AvlBalance_GPS_STIP":100
}
```


3.1.3 Example Financial Presentment (Mastercard)

The following is an example presentment from Mastercard (MTID = 1240 and Txn_Type = P).

Financial Request

Below is an example of the HTTP POST body data for a financial request.


```
{
  "ClearingFileID": "T112.00122091200052069000000025     ",
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "1000000:6",
  "POS_Date_DE13": "20220912",
  "Traceid_Message": "BNET-20220912-MC 694327",
  "Network_Issuer_Settle_ID": "52069000",
  "Network_Transaction_ID": " MC 6943270912  ",
  "Acquirer_Forwarder_ID": "500000",
  "Clearing_Process_Date": "2022-09-12",
  "Settlement_Date": "2022-09-12",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "multi_part_number": 0,
  "multi_part_count": 0,
  "SettlementIndicator": "0",
  "auth_type": "0",
```

```
  "Matching_Txn_ID": 6153911205,
  "Reason_ID": 0,
  "Merch_Name": "E-Comm Merchant",
  "Merch_City": "CITY",
  "Merch_Country": "GBR",
  "Merch_Tel": "5032277600      ",
  "Merch_Tax_id": "0",
  "GPS_POS_Capability": "00100000000000000000000000000000100000000990016",
  "GPS_POS_Data": "51V8000800000Nx000",
  "Acquirer_Reference_Data_031": "15000005123000006943271",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20220912-MC 694327",
  "PaymentToken_id": 0,
  "PaymentToken_activationMethod": 0,
  "Acquirer_id_DE32": "500000",
  "ActBal": 0.00,
  "Auth_Code_DE38": "187239",
  "Avl_Bal": 0.00,
  "Bill_Amt": 50.00,
  "Bill_Ccy": "124",
  "BlkAmt": 0.00,
  "FX_Pad": 0.00,
  "Fee_Fixed": 0.00,
  "Fee_Rate": 0.00,
  "MCC_Code": "5734",
  "MCC_Desc": "Computer Software Stores",
  "MCC_Pad": 0.00,
  "Merch_ID_DE42": "ECOMM          ",
  "Merch_Name_DE43": "E-Comm Merchant  \\\\CITY \\ GBR",
  "Note": " Refund matching credit auth",
  "POS_Data_DE22": "090951S99001",
  "POS_Termnl_DE41": "11223344",
  "POS_Time_DE12": "220912184813",
  "Proc_Code": "200000",
  "Ret_Ref_No_DE37": "225504594327",
  "Settle_Amt": 50.00,
  "Settle_Ccy": "124",
  "Status_Code": "00",
  "Token": 107916050,
  "Trans_link": "220912694327500000",
  "Txn_Amt": 50.0000,
  "Txn_CCy": "124",
  "Txn_Ctry": "GBR",
  "Txn_Desc": "E-Comm Merchant \\\\CITY \\ GBR",
  "Txn_GPS_Date": "2022-09-12 19:49:25.513",
  "TXn_ID": 6153911206,
  "Txn_Stat_Code": "S",
  "Txn_Type": "P",
  "Additional_Data_DE48":
"0002003MRG0003003MRG0023003CT60052003   014800412420158030MCC10106017322091201  NNNNNN0159067  1521544702350  1US00000001N2209120-
1220912010165001M01700165032277600",
  "Authorised_by_GPS": "N",
  "CU_Group": "PMT-CU-001",
  "InstCode": "PMT",
  "MTID": "1240",
  "ProductID": 1234,
  "SubBIN": 52111111,
  "TLogIDOrg": 0,
  "VL_Group": "PMT-VL-001",
  "Dom_Fee_Fixed": 0.00,
  "Non_Dom_Fee_Fixed": 0.00,
  "Fx_Fee_Fixed": 0.00,
  "Other_Fee_Amt": 0.00,
  "Fx_Fee_Rate": 0.00,
  "Dom_Fee_Rate": 0.00,
  "Non_Dom_Fee_Rate": 0.00,
  "SendingAttemptCount": 0
}
```

Financial Response

Below is an example of HTTP response to the above Financial Request message.


```
{
    "Acknowledgement": "1",
    "Responsestatus": "00"
}
```


3.1.4 Financial Reversal (Mastercard)

Below is an example of the HTTP POST body data for a financial reversal (MTID = 1240 and Txn_Type = E).

A financial reversal occurs when the acquirer cancels all or part of a prior transaction (which may be a purchase, refund, cashback, cash, PIN change, or any other transaction type).


```
{
  "ClearingFileID": "T112.00124020200000020326011010     ",
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "1000000:6",
  "POS_Date_DE13": "20240131",
  "Traceid_Message": "BNET-20240131-MDW2YHECL",
  "Network_Issuer_Settle_ID": "021075",
  "Network_Transaction_ID": " MDW2YHECL0131  ",
  "Acquirer_Forwarder_ID": "032208",
  "Currency_Code_Fee": "978",
  "Currency_Code_Fee_Settlement": "978",
  "Interchange_Amount_Fee": 0.009200,
  "Interchange_Amount_Fee_Settlement": 0.009200,
  "Clearing_Process_Date": "2024-02-02",
  "Settlement_Date": "2024-02-02",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "multi_part_number": 0,
  "multi_part_count": 0,
  "SettlementIndicator": "0",
  "auth_type": "0",
  "Matching_Txn_ID": 0,
  "Reason_ID": 0,
  "Merch_Name": "COFFEE ISLAND",
  "Merch_Street": "ALKINOOU 2",
  "Merch_City": "DAFNI",
  "Merch_Region": "GRC",
  "Merch_Postcode": "17235",
  "Merch_Country": "GRC",
  "Merch_Tel": "2109766611      ",
  "Merch_Tax_id": "0",
  "GPS_POS_Capability": "000000000000000000000010001000000000000000911341R",
  "GPS_POS_Data": "0175000400000Nx000",
  "Acquirer_Reference_Data_031": "77673704031974724943402",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20240131-MDW2YHECL",
  "PaymentToken_id": 61531240,
  "PaymentToken_activationMethod": 0,
  "ActBal": 0.0000,
  "Auth_Code_DE38": "150683",
  "Avl_Bal": 0.0000,
  "Bill_Amt": 4.6000,
  "Bill_Ccy": "978",
  "BlkAmt": 0.0000,
  "FX_Pad": 0.0000,
  "Fee_Fixed": 0.0000,
  "Fee_Rate": 0.0000,
  "MCC_Code": "5812",
  "MCC_Desc": "Eating Places, Restaurants",
  "MCC_Pad": 0.0000,
```

```
  "Merch_ID_DE42": "5053986        ",
  "Merch_Name_DE43": "COFFEE ISLAND\\ALKINOOU 2\\DAFNI\\17235     GRCGRC",
  "POS_Data_DE22": "M19101M54341",
  "POS_Termnl_DE41": "67500288",
  "POS_Time_DE12": "240131103058",
  "Proc_Code": "000000",
  "Ret_Ref_No_DE37": "403102239336",
  "Settle_Amt": 4.6000,
  "Settle_Ccy": "978",
  "Status_Code": "00",
  "Token": 256713034,
  "Trans_link": "1240131943402767370",
  "Txn_Amt": 4.6000,
  "Txn_CCy": "978",
  "Txn_Ctry": "GRC",
  "Txn_Desc": "COFFEE ISLAND\\ALKINOOU 2\\DAFNI\\17235     GRCGRC",
  "Txn_GPS_Date": "2024-02-02 01:36:04.133",
  "TXn_ID": 13917006447,
  "Txn_Stat_Code": "S",
  "Txn_Type": "E",
  "Additional_Data_DE48": "0001018O 5372143399965026000 2003MDW0003003MDW0015007240130100230 03POI0025007R2402010044002
I00580020000590115018303832501460360029019780000000000009780000000000000147048002901978000000000000009200978000000000000009200014 8-
00497820149006978000015 8031DMC4300001L424020201    NNNNNNN015906721075      14097113                    1EUD2000008N24020201240202-
010165030M                          01700162109766611      0177002N 019100120207003337",
  "Authorised_by_GPS": "N",
  "CU_Group": "PMT-CU-002",
  "InstCode": "PMT",
  "MTID": "1240",
  "ProductID": 6496,
  "SubBIN": 12345678,
  "TLogIDOrg": 0,
  "VL_Group": "PMT-VL-004",
  "Dom_Fee_Fixed": 0.00,
  "Non_Dom_Fee_Fixed": 0.00,
  "Fx_Fee_Fixed": 0.00,
  "Other_Fee_Amt": 0.00,
  "Fx_Fee_Rate": 0.00,
  "Dom_Fee_Rate": 0.00,
  "Non_Dom_Fee_Rate": 0.00,
  "SendingAttemptCount": 0
}
```


Financial Reversal Response

Below is an example of HTTP response to the above Financial Notification message.


```
{"Acknowledgement":"1"}
```


3.1.5 Financial Reversal (Visa)

Below is an example of the HTTP POST body data for a financial reversal (from Visa, `MTID`= 27 and `Txn_Type` = E) used for a Cash Withdrawal/disbursement reversal.


```
{
  "Network_TxnAmt_To_BillAmt_Rate": "1000000:6",
  "POS_Date_DE13": "20220830",
  "Traceid_Message": "VIS1-20220830-002242207570295",
  "Network_Issuer_Settle_ID": "099999",
  "Network_Transaction_ID": "002242207570295",
  "Clearing_Process_Date": "2022-08-30",
  "Settlement_Date": "2022-08-30",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "multi_part_number": 1,
```

```
  "multi_part_count": 1,
  "SettlementIndicator": "0",
  "auth_type": "0",
  "Matching_Txn_ID": 0,
  "Reason_ID": 0,
  "Merch_Name": "BNP ATM",
  "Merch_Postcode": "00000",
  "Merch_Country": "CYP",
  "Merch_Tel": "               ",
  "Merch_Net_id": "          ",
  "Merch_Tax_id": "0",
  "GPS_POS_Capability": "00000001000000000000000010000000000000000000029301A",
  "GPS_POS_Data": "0151800380000 x000",
  "Acquirer_Reference_Data_031": "77882202242000000000011",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "VIS1-20220830-002242207570295",
  "PaymentToken_id": 0,
  "PaymentToken_activationMethod": 0,
  "Acquirer_id_DE32": "00000001",
  "ActBal": 848.99,
  "Additional_Amt_DE54": "0040826D000000000000",
  "Auth_Code_DE38": "146367",
  "Avl_Bal": 792.79,
  "Bill_Amt": 1.00,
  "Bill_Ccy": "826",
  "BlkAmt": -56.20,
  "FX_Pad": 0.00,
  "Fee_Fixed": 1.00,
  "Fee_Rate": 0.00,
  "MCC_Code": "6011",
  "MCC_Desc": "Automated Cash Disburse",
  "MCC_Pad": 0.00,
  "Merch_ID_DE42": "6011           ",
  "Merch_Name_DE43": "BNP ATM\\\\\\00000        CYP",
  "POS_Data_DE22": "05          ",
  "POS_Termnl_DE41": "        ",
  "POS_Time_DE12": "220830000000",
  "Proc_Code": "010000",
  "Settle_Amt": 1.00,
  "Settle_Ccy": "826",
  "Status_Code": "00",
  "Token": 100029683,
  "Trans_link": "220830001921788220",
  "Txn_Amt": 1.0000,
  "Txn_CCy": "826",
  "Txn_Ctry": "CYP",
  "Txn_Desc": "BNP ATM\\\\\\00000        CYP",
  "Txn_GPS_Date": "2022-08-30 15:12:04.157",
  "TXn_ID": 6153544584,
  "Txn_Stat_Code": "S",
  "Txn_Type": "E",
  "Authorised_by_GPS": "N",
  "CU_Group": "PMTPAYROLL",
  "InstCode": "PMT",
  "MTID": "27  ",
  "ProductID": 1234,
  "SubBIN": 43111111,
  "TLogIDOrg": 0,
  "VL_Group": "PMT CO1",
  "Dom_Fee_Fixed": 1.00,
  "Non_Dom_Fee_Fixed": 0.00,
  "Fx_Fee_Fixed": 0.00,
  "Other_Fee_Amt": 0.00,
  "Fx_Fee_Rate": 0.00,
  "Dom_Fee_Rate": 0.00,
  "Non_Dom_Fee_Rate": 0.00,
  "SendingAttemptCount": 0
}
```

Financial Reversal Response

Below is an example of HTTP response to the above Financial Reversal message.


```
{
  "FxProviderCardholderRate": 0.0,
  "POS_Date_DE13": "00000000",
  "Visa_ResponseInfo_DE44": "020000000000",
  "Visa_STIP_Reason_Code": "9020",
  "Network_Transaction_ID": "0002353127640022",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2022-12-27 07:44:44.137",
  "Matching_Txn_ID": 0,
  "Reason_ID": 0,
  "Merch_Name": "Passenger Railway - SCAEx",
  "Merch_Country": "CYP",
  "Merch_Tax_id": "0",
  "GPS_POS_Capability": "00001001000000000000000100010010001000000001130C0",
  "GPS_POS_Data": "9968000800000Nx000",
  "Response_Source": "VISA-STIP",
  "Response_Source_Why": 5,
  "Message_Source": "VISA-STIP",
  "Message_Why": 5,
  "traceid_lifecycle": "VIS1-20221219-002353127640022",
  "PaymentToken_id": 0,
  "PaymentToken_creatorStatus": " ",
  "PaymentToken_lang": "  ",
  "PaymentToken_activationMethod": 0,
  "Acquirer_id_DE32": "0844622180",
  "ActBal": 10001.00,
  "Avl_Bal": 10001.00,
  "Bill_Amt": 1.00,
  "Bill_Ccy": "826",
  "BlkAmt": 0.00,
  "FX_Pad": 0.00,
  "Fee_Fixed": 0.00,
  "Fee_Rate": 0.00,
  "MCC_Code": "4112",
  "MCC_Pad": 0.00,
  "Merch_ID_DE42": "4112           ",
  "Merch_Name_DE43": "Passenger Railway - SCAEx CY",
  "POS_Data_DE22": "0110",
  "Proc_Code": "000000",
  "Resp_Code_DE39": "00",
  "Ret_Ref_No_DE37": "235303502519",
  "Settle_Amt": 0.00,
  "Status_Code": "00",
  "Token": 107419774,
  "Trans_link": "221219002519622180",
  "Txn_Amt": 1.0000,
  "Txn_CCy": "826",
  "Txn_Ctry": "CYP",
  "Txn_Desc": "Passenger Railway - SCAEx CY",
  "Txn_GPS_Date": "2022-12-19 07:44:44.203",
  "TXn_ID": 6155805963,
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "1219074444",
  "Txn_Type": "J",
  "Authorised_by_GPS": "N",
  "InstCode": "TEST",
  "MTID": "0120",
  "ProductID": 99883,
  "SubBIN": 44622180,
  "TLogIDOrg": 0,
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
```

```
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "SendingAttemptCount": 0
}
```


3.1.6 Example Visa Authorisation Advice

Below is an example of the HTTP POST body data for a Visa authorisation advice.


```
{
  "FxProviderCardholderRate": 0.0,
  "POS_Date_DE13": "00000000",
  "Visa_ResponseInfo_DE44": "020000000000",
  "Visa_STIP_Reason_Code": "9020",
  "Network_Transaction_ID": "0002353127640022",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2022-12-27 07:44:44.137",
  "Matching_Txn_ID": 0,
  "Reason_ID": 0,
  "Merch_Name": "Passenger Railway - SCAEx",
  "Merch_Country": "CYP",
  "Merch_Tax_id": "0",
  "GPS_POS_Capability": "00001001000000000000000010001001000100000000001130C0",
  "GPS_POS_Data": "9968000800000Nx000",
  "Response_Source": "VISA-STIP",
  "Response_Source_Why": 5,
  "Message_Source": "VISA-STIP",
  "Message_Why": 5,
  "traceid_lifecycle": "VIS1-20221219-002353127640022",
  "PaymentToken_id": 0,
  "PaymentToken_creatorStatus": " ",
  "PaymentToken_lang": "  ",
  "PaymentToken_activationMethod": 0,
  "Acquirer_id_DE32": "0844622180",
  "ActBal": 10001.00,
  "Avl_Bal": 10001.00,
  "Bill_Amt": 1.00,
  "Bill_Ccy": "826",
  "BlkAmt": 0.00,
  "FX_Pad": 0.00,
  "Fee_Fixed": 0.00,
  "Fee_Rate": 0.00,
  "MCC_Code": "4112",
  "MCC_Pad": 0.00,
  "Merch_ID_DE42": "4112           ",
  "Merch_Name_DE43": "Passenger Railway - SCAEx CY",
  "POS_Data_DE22": "0110",
  "Proc_Code": "000000",
  "Resp_Code_DE39": "00",
  "Ret_Ref_No_DE37": "235303502519",
  "Settle_Amt": 0.00,
  "Status_Code": "00",
  "Token": 107419774,
  "Trans_link": "221219002519622180",
  "Txn_Amt": 1.0000,
  "Txn_CCy": "826",
  "Txn_Ctry": "CYP",
  "Txn_Desc": "Passenger Railway - SCAEx CY",
  "Txn_GPS_Date": "2022-12-19 07:44:44.203",
  "TXn_ID": 6155805963,
```

```
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "1219074444",
  "Txn_Type": "J",
  "Authorised_by_GPS": "N",
  "InstCode": "TEST",
  "MTID": "0120",
  "ProductID": 99883,
  "SubBIN": 44622180,
  "TLogIDOrg": 0,
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "SendingAttemptCount": 0
}
```


Response

Below is an example of HTTP response to the above Visa authorisation advice message.


```
{
    "MerchantAdvice":"",
    "Responsestatus":"00",
    "CurBalance":0,
    "AvlBalance":100,
    "Acknowledgement":"1",
    "LoadAmount":50,
    "Bill_Amt_Approved":0,
    "Update_Balance":1,
    "New_Balance_Sequence_Exthost":200,
    "CVV2_Result":"M",
    "CurBalance_GPS_STIP":0,
    "AvlBalance_GPS_STIP":100
}
```


3.1.7 Example Mastercard Authorisation Advice

Below is an example of the HTTP POST body data for a Mastercard authorisation advice.


```
{
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "1000000:6",
  "POS_Date_DE13": "20221219",
  "Traceid_Message": "BNET-20221219-MC 004280",
  "Network_Currency_Conversion_Date": "2022-12-19",
  "Mastercard_AdviceReasonCode_DE60": "4020000",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2022-12-26 07:39:24.520",
  "Matching_Txn_ID": 0,
  "Reason_ID": 0,
  "Merch_Name": "Travel Like A Pro",
  "Merch_Country": "HRV",
  "Merch_Tax_id": "0",
  "GPS_POS_Capability": "00110000100000000000000000000000100000000001016",
  "GPS_POS_Data": "0168000800000Nx000",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20221219-MC 004280",
  "PaymentToken_id": 0,
  "PaymentToken_creatorStatus": " ",
  "PaymentToken_lang": "  ",
  "PaymentToken_activationMethod": 0,
```

```
  "Acquirer_id_DE32": "0852729540",
  "ActBal": 3535.47,
  "Amt_Tran_Fee_DE28": "D00000010",
  "Auth_Code_DE38": "183716",
  "Avl_Bal": 3392.72,
  "Bill_Amt": 10.00,
  "Bill_Ccy": "826",
  "BlkAmt": -142.75,
  "FX_Pad": 0.00,
  "Fee_Fixed": 0.00,
  "Fee_Rate": 0.00,
  "MCC_Code": "4111",
  "MCC_Pad": 0.00,
  "Merch_ID_DE42": "4111",
  "Merch_Name_DE43": "Travel Like A Pro HRV",
  "POS_Data_DE22": "010",
  "POS_Data_DE61": "0162000000006000191",
  "POS_Time_DE12": "072725",
  "Proc_Code": "000000",
  "Resp_Code_DE39": "00",
  "Ret_Ref_No_DE37": "235303504280",
  "Settle_Amt": 0.00,
  "Status_Code": "00",
  "Token": 107612119,
  "Trans_link": "221219004280729540",
  "Txn_Amt": 10.0000,
  "Txn_CCy": "826",
  "Txn_Ctry": "HRV",
  "Txn_Desc": "Travel Like A Pro HRV",
  "Txn_GPS_Date": "2022-12-19 07:39:24.607",
  "TXn_ID": 6155805959,
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "1219072725",
  "Txn_Type": "J",
  "Additional_Data_DE48": "001R",
  "Authorised_by_GPS": "N",
  "InstCode": "TEST",
  "MTID": "0120",
  "ProductID": 99884,
  "SubBIN": 52729540,
  "TLogIDOrg": 0,
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "SendingAttemptCount": 0
}
```


Response

Below is an example of HTTP response to the above Mastercard authorisation advice message.


```
{
    "MerchantAdvice":"",
    "Responsestatus":"00",
    "CurBalance":0,
    "AvlBalance":100,
    "Acknowledgement":"1",
    "LoadAmount":50,
    "Bill_Amt_Approved":0,
    "Update_Balance":1,
    "New_Balance_Sequence_Exthost":200,
    "CVV2_Result":"M",
    "CurBalance_GPS_STIP":0,
    "AvlBalance_GPS_STIP":100
}
```

3.1.8 Example Balance Enquiry Message

Below is an example of the HTTP POST body data for a balance enquiry request. A balance enquiry provides details of changes to a card's account balance. Card balance adjustments are made using Thredd's API (web services or Cards API) and are relevant to program managers on EHI Operating modes where Thredd maintains a record of the card balance.


```
{
  "Acquirer_Country": "GBR",
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "1000000:6",
  "POS_Date_DE13": "20240925",
  "Traceid_Message": "BNET-20240924-MPB4IFV1M",
  "Network_Currency_Conversion_Date": "2024-09-24",
  "Network_Transaction_ID": "MPB4IFV1M0924",
  "Acquirer_Forwarder_ID": "200148",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2024-10-01 23:27:09.712",
  "Merch_Name": "HFX  ECCLES CHURCH ST",
  "Merch_City": "MANCHESTER",
  "Merch_Postcode": "M30 0DA",
  "Merch_Country": "GBR",
  "GPS_POS_Capability": "000010010000000000000001000000100000000000012230CA",
  "GPS_POS_Data": "0151000300000Nx0002110NU0NCUXXU",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20240924-MPB4IFV1M",
  "Balance_Sequence": 0,
  "Balance_Sequence_Exthost": 0,
  "ICC_System_Related_Data_DE55":
"9F2608FF63FD5AD4CEDDF89F2701809F10120110A00003220000000000000000000000FF9F3704E4F0B2D09F3602009B95058000048000 9A032409259C01309F0-
2060000000000005F2A020826820218009F1A0208269F34034203009F33036040208407A0000000041010",
  "Acquirer_id_DE32": "06002309",
  "ActBal": 0.0000,
  "Auth_Code_DE38": "161883",
  "Avl_Bal": 0.0000,
  "Bill_Amt": 0.0000,
  "Bill_Ccy": "826",
  "BlkAmt": 0.0000,
  "Cust_Ref": "A2",
  "FX_Pad": 0.0000,
  "Fee_Fixed": 0.0000,
  "Fee_Rate": 0.0000,
  "MCC_Code": "6011",
  "MCC_Desc": "Automated Cash Disburse",
  "MCC_Pad": 0.0000,
  "Merch_ID_DE42": "LTS1",
  "Merch_Name_DE43": "HFX  ECCLES CHURCH ST    MANCHESTER  GBR",
  "Note": "PSD2 Counter Reset",
  "POS_Data_DE22": "051",
  "POS_Data_DE61": "1010010000500826M30 0DA",
  "POS_Termnl_DE41": "HA88EC11",
  "POS_Time_DE12": "002709",
  "Proc_Code": "300000",
  "Resp_Code_DE39": "00",
  "Ret_Ref_No_DE37": "20882       ",
  "Settle_Amt": 0.0000,
  "Settle_Ccy": "826",
  "Status_Code": "00",
  "Token": 358713475,
  "Trans_link": "240925925631002309",
  "Txn_Amt": 0.0000,
  "Txn_CCy": "826",
  "Txn_Ctry": "GBR",
  "Txn_Desc": "HFX  ECCLES CHURCH ST    MANCHESTER  GBR",
  "Txn_GPS_Date": "2024-09-25 00:27:09.911",
  "TXn_ID": 14890418727,
```

```
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "0924232709",
  "Txn_Type": "A",
  "Additional_Data_DE48": "007Z8002TV",
  "Authorised_by_GPS": "N",
  "CU_Group": "PMT-CU-004",
  "InstCode": "PMT",
  "MTID": "0100",
  "ProductID": 15455,
  "SubBIN": 53908886,
  "TLogIDOrg": 0,
  "VL_Group": "PMT-VL-008",
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "SendingAttemptCount": 0
}
```


Message Response

Below is an example of HTTP response to the above balance enquiry message.


```
{
"Acknowledgement":"1",
"Responsestatus":"00",
"CurBalance":2425.6300,
"AvlBalance":2125.6300
}
```


3.1.9 Example ATM Cash Withdrawal Messages (Mastercard)

Example Authorisation Message

The example below shows a typical authorisation message of an ATM cash withdrawal for Mastercard.

Note: Note that there is a value for Amt_Tran_Fee_DE28. This indicates that there is a transaction fee for the cash withdrawal as there is a value (D00000590),


```
{
  "Acquirer_Country": "DEU",
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "1121282:5",
  "POS_Date_DE13": "2025-08-21",
  "Traceid_Message": "BNET-20250821-*********",
  "Network_Currency_Conversion_Date": "2025-08-20",
  "Network_Transaction_ID": "MDW2*****0821",
  "Acquirer_Forwarder_ID": "200123",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "F",
  "auth_expdate_utc": "2025-08-22 05:34:17.926",
  "Merch_Name": "M-Hbf. III",
  "Merch_City": "Hauptbahnhof",
  "Merch_Postcode": "60489",
  "Merch_Country": "DEU",
  "GPS_POS_Capability": "000010010000000000000010000001000000000012130C1",
  "GPS_POS_Data": "*****************************",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20250821-*********",
  "Balance_Sequence": 0,
```

```
  "Balance_Sequence_Exthost": 0,
  "ICC_System_Related_Data_DE55":
"*****************************************************************************************************************_
*****************************************************************************************************************_
***************",
  "Acquirer_id_DE32": "06010480",
  "ActBal": 0.0000,
  "Amt_Tran_Fee_DE28": "D00000590",
  "Auth_Code_DE38": "60**05",
  "Avl_Bal": 0.0000,
  "Bill_Amt": -2308.7200,
  "Bill_Ccy": "752",
  "BlkAmt": 0.0000,
  "FX_Pad": 0.0000,
  "Fee_Fixed": 0.0000,
  "Fee_Rate": 0.0000,
  "MCC_Code": "6011",
  "MCC_Desc": "Automated Cash Disburse",
  "MCC_Pad": 0.0000,
  "Merch_ID_DE42": "52410300",
  "Merch_Name_DE43": "M-Hbf. III             Hauptbahnhof  DEU",
  "Note": "PSD2 Counter Reset",
  "POS_Data_DE22": "051",
  "POS_Data_DE61": "100010000150128060489",
  "POS_Termnl_DE41": "00002468",
  "POS_Time_DE12": "073337",
  "Proc_Code": "010000",
  "Resp_Code_DE39": "00",
  "Ret_Ref_No_DE37": "08******8158",
  "Settle_Amt": 2308.7200,
  "Settle_Ccy": "752",
  "Status_Code": "00",
  "Token": 14******4,
  "Trans_link": "25082******010480",
  "Txn_Amt": 205.9000,
  "Txn_CCy": "978",
  "Txn_Ctry": "DEU",
  "Txn_Desc": "M-Hbf. III             Hauptbahnhof  DEU",
  "Txn_GPS_Date": "2025-08-21 06:34:18.011",
  "TXn_ID": *****475865,
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "0821053417",
  "Txn_Type": "A",
  "Additional_Data_DE48": "******************",
  "Authorised_by_GPS": "N",
  "CU_Group": "***-**-***",
  "InstCode": "***",
  "MTID": "0100",
  "ProductID": 1234,
  "SubBIN": ********,
  "TLogIDOrg": 0,
  "VL_Group": "***-VL-***",
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "SendingAttemptCount": 0
}
```


Response

Example response from the external host system:


```
{
"Responsestatus":"00",
"Acknowledgement":"1"
```

```
}
```


Example Presentment Message

The example below shows a presentment message for an ATM cash withdrawal for Mastercard.


```
{
  "ClearingFileID": "T112.00125082200000002032602201     ",
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "1121282:5",
  "POS_Date_DE13": "20250821",
  "Traceid_Message": "BNET-20250821-MDW2IPTG0",
  "Network_Issuer_Settle_ID": "021075",
  "Network_Transaction_ID": " MDW2IPTG00821  ",
  "Acquirer_Forwarder_ID": "010480",
  "Currency_Code_Fee": "978",
  "Currency_Code_Fee_Settlement": "978",
  "Interchange_Amount_Fee": 0.000000,
  "Interchange_Amount_Fee_Settlement": 0.000000,
  "Clearing_Process_Date": "2025-08-22",
  "Settlement_Date": "2025-08-22",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "multi_part_number": 0,
  "multi_part_count": 0,
  "SettlementIndicator": "0",
  "auth_type": "0",
  "Matching_Txn_ID": 16386475865,
  "Reason_ID": 0,
  "Merch_Name": "REISEBANK FRANKFURT AT",
  "Merch_City": "MUENCHEN",
  "Merch_Region": "DEU",
  "Merch_Postcode": "60528",
  "Merch_Country": "DEU",
  "Merch_Tax_id": "0",
  "GPS_POS_Capability": "00000001000000000000000100000100000000000000121346A",
  "GPS_POS_Data": "0151000100000Nx000",
  "Acquirer_Reference_Data_031": "75506185234281662061591",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20250821-MDW2IPTG0",
  "PaymentToken_id": 0,
  "PaymentToken_activationMethod": 0,
  "ActBal": 0.0000,
  "Additional_Amt_DE54": "0042978D000000000590",
  "Auth_Code_DE38": "606805",
  "Avl_Bal": 0.0000,
  "Bill_Amt": -2308.7200,
  "Bill_Ccy": "752",
  "BlkAmt": 0.0000,
  "FX_Pad": 0.0000,
  "Fee_Fixed": 0.0000,
  "Fee_Rate": 0.0000,
  "MCC_Code": "6011",
  "MCC_Desc": "Automated Cash Disburse",
  "MCC_Pad": 0.0000,
  "Merch_ID_DE42": "4052245/4052245",
  "Merch_Name_DE43": "REISEBANK FRANKFURT AT\\\\MUENCHEN     \\60528     DEUDEU",
  "POS_Data_DE22": "511201C11346",
  "POS_Termnl_DE41": "00002468",
  "POS_Time_DE12": "250821073337",
  "Proc_Code": "010000",
  "Ret_Ref_No_DE37": "082107058158",
  "Settle_Amt": -205.9000,
  "Settle_Ccy": "978",
  "Status_Code": "00",
  "Token": 143654784,
```

```
  "Trans_link": "250821882458010480",
  "Txn_Amt": 205.9000,
  "Txn_CCy": "978",
  "Txn_Ctry": "DEU",
  "Txn_Desc": "REISEBANK FRANKFURT AT\\\\MUENCHEN     \\60528     DEUDEU",
  "Txn_GPS_Date": "2025-08-22 04:15:05.103",
  "TXn_ID": 16390740846,
  "Txn_Stat_Code": "S",
  "Txn_Type": "P",
  "Additional_Data_DE48":
"0002003MDW0003003MDW001500725082010023003ATM01460360019019780000000000009780000000000000147048001901978000000000000000000097800000-
00000000000000148008978275220158031DMC30500125625082202    N2NNNNN015906721075      14097113                    1EUD2000008N250822-
02250822010165001M0177002N 01910012",
  "Authorised_by_GPS": "N",
  "CU_Group": "CRV-CU-002",
  "InstCode": "CRV",
  "MTID": "1240",
  "ProductID": 6540,
  "SubBIN": 55744496,
  "TLogIDOrg": 0,
  "VL_Group": "CRV-VL-182",
  "Dom_Fee_Fixed": 0.00,
  "Non_Dom_Fee_Fixed": 0.00,
  "Fx_Fee_Fixed": 0.00,
  "Other_Fee_Amt": 0.00,
  "Fx_Fee_Rate": 0.00,
  "Dom_Fee_Rate": 0.00,
  "Non_Dom_Fee_Rate": 0.00,
  "SendingAttemptCount": 0
}
```


Response

Example response from the external host system:


```
{"Acknowledgement":"1"}
```


3.1.10 Example Tokenisation Messages

Example EHI TAR (330000) Message

The example below shows a typical EHI 0100 authorisation message for a Token Authorisation Request (TAR) in a JSON format.


```
{
  "SchemeTransactionIdentifier": "BNETF64",
  "TokenUniqueReference": "DM4MMC1PT0000000be3ec16ef999999ab7d4b47da4456277",
  "PaymentTokenPan": "5372403458767765",
  "PaymentToken_PanSource": "F",
  "Network_Fraud_Data": "00199991",
  "FxProviderCardholderRate": 0.000000000,
  "Network_TxnAmt_To_BillAmt_Rate": "7849290:7",
  "POS_Date_DE13": "00000000",
  "Traceid_Message": "BNET-20240604-MDWWKZ1AT",
  "Network_Currency_Conversion_Date": "2024-06-04",
  "Network_Transaction_ID": "MDWWKZ1AT0604",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2024-06-12 01:00:01.307",
  "Matching_Txn_ID": 0,
  "Reason_ID": 0,
  "Merch_Name": "Klarna-EU",
  "Merch_City": "St. Louis",
  "Merch_Postcode": "63368",
  "Merch_Country": "USA",
  "Merch_Tax_id": "0",
```

```
  "GPS_POS_Capability": "00110000100000000000000000000000001000000000230010",
  "GPS_POS_Data": "5018000800000Nx000",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20240604-MDWWKZ1AT",
  "PaymentToken_id": 0,
  "PaymentToken_creatorStatus": "N",
  "PaymentToken_wallet": "MRCHTOKEN",
  "PaymentToken_lang": "  ",
  "PaymentToken_activationMethod": 0,
  "Acquirer_id_DE32": "06015611",
  "ActBal": 0.00,
  "Auth_Code_DE38": "117574",
  "Avl_Bal": 0.00,
  "Bill_Amt": 0.00,
  "Bill_Ccy": "826",
  "BlkAmt": 0.00,
  "Cust_Ref": "49538776",
  "FX_Pad": 0.00,
  "Fee_Fixed": 0.00,
  "Fee_Rate": 0.00,
  "MCC_Code": "5969",
  "MCC_Desc": "Direct Marketing - Other",
  "MCC_Pad": 0.00,
  "Merch_ID_DE42": "CARD ACCPT IDC",
  "Merch_Name_DE43": "Klarna-EU St. Louis USA",
  "Note": "DR: Declined due to Card Status: Card Destroyed (Original status 83, changed to 05) ",
  "POS_Data_DE22": "010",
  "POS_Data_DE61": "102510900000084063368",
  "Proc_Code": "330000",
  "Resp_Code_DE39": "57",
  "Settle_Amt": 0.00,
  "Settle_Ccy": "826",
  "Status_Code": "83",
  "Token": 138602839,
  "Trans_link": "240605048358015611",
  "Txn_Amt": 0.0000,
  "Txn_CCy": "840",
  "Txn_Ctry": "USA",
  "Txn_Desc": "Klarna-EU              St. Louis     USA",
  "Txn_GPS_Date": "2024-06-05 02:00:01.410",
  "TXn_ID": 14419002829,
  "Txn_Stat_Code": "I",
  "TXN_Time_DE07": "0605010001",
  "Txn_Type": "A",
  "Additional_Data_DE48": "063T260332733260101H0611501929199980802037513010300102029171041 8C ",
  "Authorised_by_GPS": "Y",
  "CU_Group": "PMT-CU-002",
  "InstCode": "PMT",
  "MTID": "0100",
  "ProductID": 3004,
  "SubBIN": 53759000,
  "TLogIDOrg": 0,
  "VL_Group": "PMT-VL-020",
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "Additional_Data_DE124":
"195TAD00162036556451
                                        1                       C",
  "SendingAttemptCount": 0
}
```


Response

Example response from the external host system:

```
{"Acknowledgement":"1"}
```


ACN (340000) Message


```
{
  "SchemeTransactionIdentifier": "BNETF64",
  "TokenUniqueReference": "DM4MMC1DE0000000cac6e366341d49819f38090c57f15677",
  "PaymentTokenPan": "5372403458767765",
  "Network_Fraud_Data": "00199991                          ",
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "7878970:7",
  "POS_Date_DE13": "00000000",
  "Traceid_Message": "BNET-20240603-BPD83TR98",
  "Network_Currency_Conversion_Date": "2024-06-03",
  "Network_Transaction_ID": "BPD83TR980603",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2024-06-11 02:37:56.380",
  "Merch_Name": "APPLE PAY",
  "Merch_City": "St. Louis",
  "Merch_Postcode": "63368",
  "Merch_Country": "USA",
  "GPS_POS_Capability": "00110000100000000000000000000000000100000000230010",
  "GPS_POS_Data": "5018000800000Nx000NNNNNM0NUUXXU",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20240603-BPD83TR98",
  "Balance_Sequence": 0,
  "Balance_Sequence_Exthost": 0,
  "PaymentToken_id": 72322899,
  "PaymentToken_creator": "MC-MDES",
  "PaymentToken_type": "SE",
  "PaymentToken_status": "00",
  "PaymentToken_creatorStatus": "N",
  "PaymentToken_wallet": "APPLE",
  "PaymentToken_deviceType": "M",
  "PaymentToken_lang": "  ",
  "PaymentToken_deviceIp": "4E916C0C",
  "PaymentToken_deviceId": "012345678917900221990361503163 80EEB395872B0AC6ED",
  "PaymentToken_activationCode": "169961",
  "PaymentToken_activationExpiry": "2024-06-04 05:37:00.000",
  "PaymentToken_activationMethodData": "+447880646031",
  "PaymentToken_activationMethod": 1,
  "Acquirer_id_DE32": "06015611",
  "ActBal": 0.0000,
  "Auth_Code_DE38": "152085",
  "Avl_Bal": 0.0000,
  "Bill_Amt": 0.0000,
  "Bill_Ccy": "826",
  "BlkAmt": 0.0000,
  "FX_Pad": 0.0000,
  "Fee_Fixed": 0.0000,
  "Fee_Rate": 0.0000,
  "MCC_Code": "5969",
  "MCC_Desc": "Direct Marketing - Other",
  "MCC_Pad": 0.0000,
  "Merch_ID_DE42": "CARD ACCPT IDC",
  "Merch_Name_DE43": "APPLE PAY St. Louis     USA",
  "POS_Data_DE22": "010",
  "POS_Data_DE61": "102510900000084063368",
  "Proc_Code": "340000",
  "Resp_Code_DE39": "00",
  "Settle_Amt": 0.0000,
  "Settle_Ccy": "826",
  "Status_Code": "00",
  "Token": 335635281,
  "Trans_link": "240604612291015611",
```

```
  "Txn_Amt": 0.0000,
  "Txn_CCy": "840",
  "Txn_Ctry": "USA",
  "Txn_Desc": "APPLE PAY St. Louis     USA",
  "Txn_GPS_Date": "2024-06-04 03:37:56.518",
  "TXn_ID": 14414319424,
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "0604023756",
  "Txn_Type": "J",
  "Additional_Data_DE48": "063T230221260310333200101C06115011003027375130103001020291710418C ",
  "Authorised_by_GPS": "N",
  "CU_Group": "PMT-CU-001",
  "InstCode": "PMT",
  "MTID": "0120",
  "ProductID": 4252,
  "SubBIN": 51694000,
  "TLogIDOrg": 0,
  "VL_Group": "PMT-VL-001",
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "Additional_Data_DE124": "048ACD00151510492061699610  24060405371#########6031",
  "SendingAttemptCount": 0
}
```


Response

Example response from the external host system:


```
{
  "Responsestatus":"00",
  "CurBalance":0.0,
  "AvlBalance":0.0,
  "Acknowledgement":1,
  "LoadAmount":0.0,
  "Bill_Amt_Approved":0.0,
  "Update_Balance":0,
  "New_Balance_Sequence_Exthost":0,
  "CVV2_Result":"",
  "AvlBalance_GPS_STIP":0.0,
  "CurBalance_GPS_STIP":0.0
}
```


TCN (350000) Message


```
{
  "SchemeTransactionIdentifier": "BNETF64",
  "TokenUniqueReference": "DM4MMC1DE0000000cac6e366341d49819f38090c57f15677",
  "PaymentTokenPan": "5372403458767765",
  "Network_Fraud_Data": "00199991                          ",
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "7878970:7",
  "POS_Date_DE13": "00000000",
  "Traceid_Message": "BNET-20240603-BPDR46YHK",
  "Network_Currency_Conversion_Date": "2024-06-03",
  "Network_Transaction_ID": "BPDR46YHK0603",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2024-06-11 01:01:20.030",
  "Merch_Name": "APPLE PAY",
  "Merch_City": "St. Louis",
  "Merch_Postcode": "63368",
  "Merch_Country": "USA",
```

```
  "GPS_POS_Capability": "00110000100000000000000000000000010000000230010",
  "GPS_POS_Data": "5018000800000Nx000NNNNNM0NUUXXU",
  "Response_Source_Why": 0,
  "Message_Why": 0,
  "traceid_lifecycle": "BNET-20240603-BPDR46YHK",
  "Balance_Sequence": 0,
  "Balance_Sequence_Exthost": 0,
  "PaymentToken_id": 72322246,
  "PaymentToken_creator": "MC-MDES",
  "PaymentToken_expdate": "2027-07-31",
  "PaymentToken_type": "SE",
  "PaymentToken_status": "00",
  "PaymentToken_creatorStatus": "A",
  "PaymentToken_wallet": "APPLE",
  "PaymentToken_deviceType": "M",
  "PaymentToken_lang": "  ",
  "PaymentToken_deviceTelNum": "7181",
  "PaymentToken_deviceIp": "97E3830C",
  "PaymentToken_deviceId": "0123456789E5C800201030806453051O2E616B5CB01EB3DD6",
  "PaymentToken_deviceName": "Stephanie's phone (3",
  "Acquirer_id_DE32": "06015611",
  "ActBal": 0.0000,
  "Auth_Code_DE38": "166647",
  "Avl_Bal": 0.0000,
  "Bill_Amt": 0.0000,
  "Bill_Ccy": "826",
  "BlkAmt": 0.0000,
  "FX_Pad": 0.0000,
  "Fee_Fixed": 0.0000,
  "Fee_Rate": 0.0000,
  "MCC_Code": "5969",
  "MCC_Desc": "Direct Marketing - Other",
  "MCC_Pad": 0.0000,
  "Merch_ID_DE42": "CARD ACCPT IDC",
  "Merch_Name_DE43": "APPLE PAY St. Louis USA",
  "POS_Data_DE22": "010",
  "POS_Data_DE61": "102510900000084063368",
  "Proc_Code": "350000",
  "Resp_Code_DE39": "00",
  "Settle_Amt": 0.0000,
  "Settle_Ccy": "826",
  "Status_Code": "00",
  "Token": 374414990,
  "Trans_link": "240604229542015611",
  "Txn_Amt": 0.0000,
  "Txn_CCy": "840",
  "Txn_Ctry": "USA",
  "Txn_Desc": "APPLE PAY St. Louis USA",
  "Txn_GPS_Date": "2024-06-04 02:01:20.142",
  "TXn_ID": 14414251623,
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "0604010119",
  "Txn_Type": "J",
  "Additional_Data_DE48": "097T230221260310333540101C021653724083642754730304270706115011003027308020575130103001020291710418C ",
  "Authorised_by_GPS": "N",
  "CU_Group": "PMT-CU-001",
  "InstCode": "PMT",
  "MTID": "0620",
  "ProductID": 4252,
  "SubBIN": 51694000,
  "TLogIDOrg": 0,
  "VL_Group": "PMT-VL-001",
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "Additional_Data_DE124": "192TCD001514838250601ZILCHCONS enStephanie's phone (31269d868a6a0394114a347cfe-
f4ee0901e24060401010DAPLMC000026259835f4ba50cdd94aea8725b3beedde4545FAPLMC00002625988947bff5eb134ffcae9822bf49031d09S",
```

```
  "SendingAttemptCount": 0
}
```

Response

Example response from the external host system:


```
{
  "Responsestatus":"00",
  "CurBalance":0.0,
  "AvlBalance":0.0,
  "Acknowledgement":1,
  "LoadAmount":0.0,
  "Bill_Amt_Approved":0.0,
  "Update_Balance":0,
  "New_Balance_Sequence_Exthost":0,
  "CVV2_Result":"",
  "AvlBalance_GPS_STIP":0.0,
  "CurBalance_GPS_STIP":0.0
}
```


TEN (360000) Message


```
{
  "SchemeTransactionIdentifier": "BNETF64",
  "TokenUniqueReference": "DM4MMC1PT0000000be3ec16ef999999ab7d4b47da4456277",
  "PaymentTokenPan": "5372403458767765",
  "Network_Fraud_Data": "00199991                          ",
  "FxProviderCardholderRate": 0.0,
  "Network_TxnAmt_To_BillAmt_Rate": "7878970:7",
  "POS_Date_DE13": "00000000",
  "Traceid_Message": "BNET-20240603-BPDH0UE75",
  "Network_Currency_Conversion_Date": "2024-06-03",
  "Network_Transaction_ID": "BPDH0UE750603",
  "DCC_Indicator": 0,
  "multi_part_txn": 0,
  "multi_part_txn_final": 0,
  "auth_type": "0",
  "auth_expdate_utc": "2024-06-11 01:00:16.001",
  "Merch_Name": "Visa Provisioning Service",
  "Merch_City": "St. Louis",
  "Merch_Postcode": "63368",
  "Merch_Country": "USA",
  "GPS_POS_Capability": "00110000100000000000000000000000000100000000230010",
  "GPS_POS_Data": "5018000800000Nx000NNNNNM0NUUXXU",
  "Response_Source_Why": 0,
  "Message_Source": "CRDHLR",
  "Message_Why": 51,
  "traceid_lifecycle": "VIS1-20240604-304156486459325",
  "Balance_Sequence": 0,
  "Balance_Sequence_Exthost": 0,
  "PaymentToken_id": 58098832,
  "PaymentToken_creator": "Visa-T",
  "PaymentToken_expdate": "2026-03-31",
  "PaymentToken_type": "SE",
  "PaymentToken_status": "00",
  "PaymentToken_creatorStatus": "D",
  "PaymentToken_wallet": "APPLE",
  "PaymentToken_deviceType": "M",
  "PaymentToken_lang": "  ",
  "PaymentToken_deviceTelNum": "1504",
  "PaymentToken_deviceIp": "94FC8598",
  "PaymentToken_deviceId": "01234567896A800211990999163114401 0A4926E8D6D1C36",
  "PaymentToken_deviceName": "iPhone",
  "Acquirer_id_DE32": "06015611",
  "ActBal": 0.0000,
  "Auth_Code_DE38": "161404",
  "Avl_Bal": 0.0000,
  "Bill_Amt": 0.0000,
```

```
  "Bill_Ccy": "826",
  "BlkAmt": 0.0000,
  "FX_Pad": 0.0000,
  "Fee_Fixed": 0.0000,
  "Fee_Rate": 0.0000,
  "MCC_Code": "5969",
  "MCC_Desc": "Direct Marketing - Other",
  "MCC_Pad": 0.0000,
  "Merch_ID_DE42": "CARD ACCPT IDC",
  "Merch_Name_DE43": "Visa Provisioning Service FR",
  "POS_Data_DE22": "010",
  "POS_Data_DE61": "102510900000084063368",
  "Proc_Code": "360000",
  "Resp_Code_DE39": "00",
  "Settle_Amt": 0.0000,
  "Settle_Ccy": "826",
  "Status_Code": "00",
  "Token": 155027420,
  "Trans_link": "240604919020015611",
  "Txn_Amt": 0.0000,
  "Txn_CCy": "840",
  "Txn_Ctry": "USA",
  "Txn_Desc": "Visa Provisioning Service FR",
  "Txn_GPS_Date": "2024-06-04 02:00:16.121",
  "TXn_ID": 14414250789,
  "Txn_Stat_Code": "A",
  "TXN_Time_DE07": "0604010015",
  "Txn_Type": "J",
  "Additional_Data_DE48": "091T230221260310333480101C021653724083932605950304260306115011003027375130103001020291710418C ",
  "Authorised_by_GPS": "N",
  "CU_Group": "PMT-CU-001",
  "InstCode": "PMT",
  "MTID": "0620",
  "ProductID": 4252,
  "SubBIN": 51694000,
  "TLogIDOrg": 0,
  "VL_Group": "PMT-VL-001",
  "Dom_Fee_Fixed": 0.0000,
  "Non_Dom_Fee_Fixed": 0.0000,
  "Fx_Fee_Fixed": 0.0000,
  "Other_Fee_Amt": 0.0000,
  "Fx_Fee_Rate": 0.0000,
  "Dom_Fee_Rate": 0.0000,
  "Non_Dom_Fee_Rate": 0.0000,
  "Additional_Data_DE124": "068TVD00067408479624  2DAPLMC000026259862dc013463464968ac77488b5bd11e9d",
  "SendingAttemptCount": 0
}
```


Response

Example response from the external host system:


```
{
  "Responsestatus":"00",
  "CurBalance":0.0,
  "AvlBalance":0.0,
  "Acknowledgement":1,
  "LoadAmount":0.0,
  "Bill_Amt_Approved":0.0,
  "Update_Balance":0,
  "New_Balance_Sequence_Exthost":0,
  "CVV2_Result":"",
  "AvlBalance_GPS_STIP":0.0,
  "CurBalance_GPS_STIP":0.0
}
```

3.1.11 Example Incremental Authorisation Messages

Incremental Authorisation Request

Below is an example of the HTTP POST body data for an incremental authorisation request.


```
{
  "FxProviderCardholderRate":0.000000000,
  "Network_TxnAmt_To_BillAmt_Rate":"1000000:6",
  "POS_Date_DE13":"20241127",
  "Traceid_Message":"BNET-20241127-MCC680561",
  "Traceid_Original":"BNET-20241127-MCC686194",
  "Network_Currency_Conversion_Date":"2024-11-27",
  "Network_Transaction_ID":"MCC6805611127",
  "DCC_Indicator":0,
  "multi_part_txn":0,
  "multi_part_txn_final":0,
  "auth_type":"P",
  "auth_expdate_utc":"2024-12-27 13:26:26.363",
  "Matching_Txn_ID":0,
  "Reason_ID":0,
  "Merch_Name":"ASDA GROCERIES",
  "Merch_City":"LONDON",
  "Merch_Postcode":"SW1 3AN",
  "Merch_Country":"GBR",
  "Merch_Tax_id":"0",
  "GPS_POS_Capability":"00010000000001000000000000000000001000000000100M",
  "GPS_POS_Data":"10V8000800000Nx006",
  "Response_Source_Why":0,
  "Message_Why":0,
  "traceid_lifecycle":"BNET-20241127-MCC686194",
  "PaymentToken_id":0,
  "PaymentToken_creatorStatus":" ",
  "PaymentToken_lang":"  ",
  "PaymentToken_activationMethod":0,
  "Acquirer_id_DE32":"06555555",
  "ActBal":100723.40,
  "Auth_Code_DE38":"166297",
  "Avl_Bal":100009.40,
  "Bill_Amt":-20.00,
  "Bill_Ccy":"826",
  "BlkAmt":-714.00,
  "FX_Pad":0.00,
  "Fee_Fixed":2.00,
  "Fee_Rate":0.00,
  "MCC_Code":"5734",
  "MCC_Desc":"Computer Software Stores",
  "MCC_Pad":0.00,
  "Merch_ID_DE42":"MERCHANT 000001",
  "Merch_Name_DE43":"ASDA GROCERIES         LONDON        GBR",
  "Note":"  Gen: Pre-Authorization Request",
  "POS_Data_DE22":"812",
  "POS_Data_DE61":"2031104000100826SW1 3AN",
  "POS_Termnl_DE41":"ECOMM001",
  "POS_Time_DE12":"012626",
  "Proc_Code":"000000",
  "Resp_Code_DE39":"00",
  "Ret_Ref_No_DE37":"433210456861",
  "Settle_Amt":20.00,
  "Settle_Ccy":"826",
  "Status_Code":"00",
  "Token":108336227,
  "Trans_link":"241127683518555555",
  "Txn_Amt":20.0000,
  "Txn_CCy":"826",
  "Txn_Ctry":"GBR",
  "Txn_Desc":"ASDA GROCERIES         LONDON        GBR",
```

```
  "Txn_GPS_Date":"2024-11-27 13:26:26.783",
  "TXn_ID":6162588064,
  "Txn_Stat_Code":"A",
  "TXN_Time_DE07":"1127132626",
  "Txn_Type":"A",
  "Additional_Data_DE48":"038T4207010381063l5MCC6861941127  9203***",
  "Authorised_by_GPS":"N",
  "CU_Group":"PMT-CU-001",
  "InstCode":"TEST",
  "MTID":"0100",
  "ProductID":99884,
  "SubBIN":52729540,
  "TLogIDOrg":0,
  "VL_Group":"QE-LIMIT",
  "Dom_Fee_Fixed":2.0000,
  "Non_Dom_Fee_Fixed":0.0000,
  "Fx_Fee_Fixed":0.0000,
  "Other_Fee_Amt":0.0000,
  "Fx_Fee_Rate":0.0000,
  "Dom_Fee_Rate":0.0000,
  "Non_Dom_Fee_Rate":0.0000,
  "SendingAttemptCount":0
  }
```


Incremental Authorisation Response

Below is an example response.


```
{
  "MerchantAdvice":null,
  "Responsestatus":"00",
  "CurBalance":0,
  "AvlBalance":100,
  "Acknowledgement":"1",
  "LoadAmount":50,
  "Bill_Amt_Approved":0,
  "Update_Balance":1,
  "New_Balance_Sequence_Exthost":200,
  "CVV2_Result":"M",
  "CurBalance_GPS_STIP":0,
  "AvlBalance_GPS_STIP":100
}
```


3.1.12 Examples of Amount Signs

The table below provides an overview of the signs on important amount fields used in many transactions and illustrates using examples.

Note: The TXn_ID field is provided for internal Thredd usage and can be ignored.

MTID	Txn_ Type	cr/db	Proc_ Code	Source	settl e_ccy	settle_ amt	txn_ ccy	txn_amt	bill_ ccy	bill_amt	TXn_ID
0100	A	Debit	00000 0	Banknet	978	7.1900	826	6.3000	978	-7.1900	3178117382
0100	A	Debit	00000 0	Visa B1	978	22.2500	826	19.4800	978	-22.2500	3178117377
0100	A	Credit	28000 0	Banknet	826	47.7500	826	47.7500	826	47.7500	3178096311

MTID	Txn_ Type	cr/db	Proc_ Code	Source	settl e_ccy	settle_ amt	txn_ ccy	txn_amt	bill_ ccy	bill_amt	TXn_ID
0100	A	Credit	260000	Visa B1	978	77.7100	826	70.0000	978	77.7100	3076890895
	D	Credit	000000	Banknet	978	1.0000	978	1.0000	978	1.0000	3177930769
	D	Credit	003000	Visa B1	978	29.9400	554	50.0000	978	29.9400	3177930766
	D	Debit	280000	Banknet	826	10.0000	826	10.0000	826	-10.0000	3179976368
	D	Debit	200000	Visa B1	840	10.0000	826	8.0200	124	-14.0400	(not real)
0120	J	Credit	000000	Banknet		0.0000	784	21.0300	826	4.4400	3178071058
0120	J	Credit	003000	Visa B1		0.0000	458	2.4800	978	0.5400	3178059229
0120	J	Credit	200000	Banknet		0.0000	826	25.0000	978	30.0000	(not real)
0120	J	Credit	260000	Visa B1		0.0000	826	70.0000	978	77.7100	3076890919
1240	P	Debit	000000	GCMS	978	-129.0000	978	129.0000	978	-129.0000	3185427850
1240	P	Credit	200000	GCMS	978	39.2300	978	39.2300	978	39.2300	3185427844
05pp	P	Debit	000000	Visa B2	826	-30.5800	710	550.0000	826	-30.5800	3184113150
06pp	P	Credit	200000	Visa B2	978	7.1300	036	11.3600	978	7.1300	3183968531
07pp	P	Debit	010000	Visa B2	978	-901.7500	978	901.7500	978	-901.7500	3183970358
1240	A	Debit (dummy auth)	010000	GCMS	840	-64.9300	704	1500000.0000	978	-57.6000	3189756992
1240	A	Credit (dummy auth)	200000	GCMS	978	39.2300	978	39.2300	978	39.2300	(not real)
05pp	A	Debit (dummy auth)	000000	Visa B2	840	-18.9300	756	19.0000	840	-18.9300	3189248664
06pp	A	Credit (dummy auth)	200000	Visa B2	978	7.1300	036	11.3600	978	7.1300	(not real)

MTID	Txn_ Type	cr/db	Proc_ Code	Source	settl e_ccy	settle_ amt	txn_ ccy	txn_amt	bill_ ccy	bill_amt	TXn_ID
07pp	A	Debit (dummy auth)	01000 0	Visa B2	826	- 207.710 0	484	5100.0000	826	- 207.710 0	31892469 92
1240	C	Chargeba ck	18000 0	Other	978	200.000 0	978	200.0000	978	200.000 0	31860937 86
1240	C	Chargeba ck	00000 0	Other	826	98.0000	826	98.0000	826	98.0000	31896946 82
1240	C	Chargeba ck	01000 0	Other	978	80.0000	978	80.0000	978	80.0000	31893235 24
	L	Load	22000 0	Other	978	90.0000	978	90.0000	978	90.0000	31897591 69
	U	Unload	23000 0	Other	826	8.8400	826	8.8400	826	-8.8400	29935098 94
	B	Bal Adj	19000 0	Other	978	0.1900	978	0.1900	978	-0.1900	31880586 06
	B	Bal Adj	02100 0	Other	826	4.9900	826	4.9900	826	4.9900	31880579 35
	P	Fee	08399 9	Thredd (Fee fields have amount s)	826	0.0000	826	0.0000	826	0.0000	50717732 34

Notes

In the above table, a ‘p’ indicates the space character, and the ‘Source’ column indicates the origin of the message as follows:

- “Visa B1” if from Visa Base 1 (i.e., Visa online authorisation system)
- “Visa B2” if from Visa Base 2 (i.e., Visa offline clearing system)
- “Banknet” if from Mastercard Banknet (i.e., Mastercard online authorisation system)
- “GCMS” if from Mastercard Global Clearing system (i.e., Mastercard offline clearing system)
- “Other” means not Visa or Mastercard. For example, internal (via Thredd Portal, Smart Client) or a web service call / Cards API call.

3.2 Cut-Off Message Example

This section provides an example of a cut off message and response.

Note: If you are set up to receive EHI in JSON format, you will also receive cut-off messages in JSON format.

Note: EHI_JSON_Guide_5.1 The EHI feed does not send JSON fields to externally-hosted systems where the values for the field data are blank. This is different from EHI feeds with XML fields where the feed can send blank values.

3.2.1 Example Cut-Off Request Message


```
{
 "CutOffId":38077,
 "ProductId":99883,
 "CutOffDate":"2022-11-29 13:00:01.837",
 "FirstTransactionId":6154805771,
 "LastTransactionId":6154805771,
 "AuthsAcknowledged":1,
 "AuthsNotAcknowledged":0,
 "FinancialsAcknowledged":0,
 "FinancialsNotAcknowledged":0,
 "LoadsUnloadsAcknowledged":0,
 "LoadsUnloadsNotAcknowledged":0,
 "BalanceAdjustExpiryAcknowledged":0,
 "BalanceAdjustExpiryNotAcknowledged":0
 }
```


3.2.2 Example Cut-Off Response Message

This is an example response to the above example request message, showing the HTTP Response body data:


```
{"Acknowledgement":"1"}
```

SECTION 4: APPENDICES

This section provides appendices with additional reference information.

4.1 Appendices

Refer to the table below for a list of the available appendices, organised alphabetically.

#	Appendix	Description
4.1	Appendices	Provides a list of the available appendices.
4.2	Additional Amounts Field	Additional amount field contains additional amount information for a transaction.
4.3	AVS Results	Provides details of AVS Result values.
4.4	Bank Account Format	Describes the valid values for the source_bank_account_format and dest_bank_account_format fields.
4.5	Calculating the Total	Explains how the total cost of the transaction can be calculated.
4.6	Card Status Codes	Describes the possible card status codes.
4.7	Country Codes	Lists alpha and numeric country codes.
4.8	Currency Codes	Provides a list of currency codes, based on the ISO 4217 specification.
4.9	CVV2 Indicators	Provides details of the CVV2 Presence Type and Response Type indicators.
4.10	Dispute Condition	Describes the Visa dispute reason codes returned in the Dispute_Condition field.
4.11	Dynamic CVV2	Describes the dynamic Card Verification Value 2 (CVV2) functionality, and how to implement.
4.12	GPS_POS_Capability field	Describes the GPS_POS_Capability subfields.
4.13	GPS_POS_Data field	Thredd defined field that records POS Data codes, which are specific to this transaction.
4.14	Load Source	Lists values for the LoadSRC field, identifying the source of a Load.
4.15	Load Type	Lists the load types that describe how the card was loaded.
4.16	Mastercard_AdviceReason	Describes the Mastercard_AdviceReasonCode_DE60 field.
4.17	Merch_Name_DE43 Field in Authorisations	Describes the format of the Merchant Name/Location (DE43) authorisation field Merch_Name_DE43.
4.18	Merch_Name_DE43 in Financials	Describes the subfields in the Merch_Name_DE43 field for a financial message.
4.19	Merchant Category Codes	Provides details of the merchant category codes (MCC).
4.20	Misc_TLV_Data Field	Describes the Misc_TLV_Data field, which is used for sending rarely used fields that can normally be ignored.
4.21	Network_Fraud_Data Format	Provides details of the Fraud and Risk indicators received from the network, which are populated in the Network_Fraud_Data field.
4.22	Payment Token Fields	Describes the fields used for mobile device payment tokens: PaymentToken_activationMethod

#	Appendix	Description
		PaymentToken_creatorStatus PaymentToken_deviceType PaymentToken_type PaymentToken_wallet PaymentToken_PanSource
4.23	PIN Fields	Describes the format of PIN blocks.
4.24	POS_Data_DE61 field	Describes the format and layout of the POS_Data_DE61 field.
4.25	POS_Data_DE22 in Authorisation	Describes the format and layout of the POS_Data_DE22 field.
4.26	POS_Data_DE22 in Mastercard	Describes the subfields in the POS_Data_DE22 field.
4.27	Processing Codes	Describes the subfields in the processing code (Proc_Code) field.
4.28	Reason_ID	Provides details of the Reason_ID field, which indicates the reason for a message.
4.29	Response_Code_DE39 Response Codes	Provides details of the reason for the advice or reversal for Mastercard 0120, 0400 and 0420 messages.
4.30	Responsestatus Values	Lists the response codes that you can returned to Thredd in response to a payment authorisation request.
4.31	Response_Source and Message_Source	Lists codes and possible values for the Response_Source and Message_Source fields.
4.32	Response_Source_Why and Message_Source_Why	Lists the possible values for the reason why the Response_Source and Message_Source sent the message.
4.33	Scheme Transaction Identifier Values	List the different identifier values for transactions from Mastercard and Visa.
4.34	SenderData and ReceiverData Fields	The SenderData and ReceiverData fields provide details of the sender and receiver in a money transfer message. This appendix lists the possible subfield values.
4.35	Special Characters	Describes Special Characters that may be used in fields of Data Type ANS.
4.36	Transaction Matching - Authentications and Authorisations	Provides guidelines and examples of common transaction matching and processing scenarios for different types of messages and fields.
4.37	Transaction Status Codes	Provides details of the available Transaction Status Code (Txn_Stat_Code) values.
4.38	Transaction Types	Provides details of available Transaction Type (Txn_Type) values.
4.39	Trans_Link Field	Provides details of available Trans_Link field values.
4.40	Visa_POS_Data_DE60	Provides details of the layout and format of the Visa_POS_Data_DE60 field.
4.41	Visa_ResponseInfo_DE44	Provides details of the layout and format of the Visa_ResponseInfo_DE44 field.
4.42	Visa_STIP_Reason_Code	Provides details of the Visa_STIP_Reason_Code field.

4.2 Additional Amount Field

The additional amount field (Additional_Amt_DE54) contains additional amount information for the transaction, if relevant. For example, for purchase with cashback transactions, the additional amounts field is present with the cashback amount. In practice, in request messages, you probably only want to read this field for cashback transactions to extract the cashback amount should you need it. (See also Get Transaction Message fields: Additional_Amt_DE54)

Note: Mastercard and Visa may add new Account Type and Amount Type codes at any time. Ignore any amounts where you do not understand the amount type or account type. These are not errors.

4.2.1 Additional Amount Subfields

The Additional amounts field (Additional_Amt_DE54) can contain between 1 and 6 different amounts. Each individual amount is a 20 character block. There can be between 1 and 6 blocks. Each block is formatted as follows:

Subfield	Name	Format	Description / Valid Values
1	Account Type	2 digits 00-99	Describes which account this amount refers to. See Account Type Codes for valid values.
2	Amount Type	2 digits 00-99	Describes what this amount means. See Amount Type Codes for valid values.
3	Currency Code	3 digits 000-999	ISO 3-digit numeric currency code. See Currency Code for valid values.
4	Amount sign	'D' or 'C'	C = Positive (credit) amount D = Debit (negative) amount
5	Amount value	12 decimal digits	The amount in minor units of the currency in subfield 3 (currency code.)

4.2.2 Amount Type Codes

Amount Type provides a description of this amount.

Amount Type	Description
01	Debit accounts: Ledger Balance Credit card accounts: credit amount remaining for customer (the open to buy amount)
02	Debit accounts: Available Balance Credit Card accounts: customer's credit limit
03	Amount Owing
04	Amount Due
10	Healthcare eligibility amount. Allows the acquirer to indicate the portion of the amount spent on eligible healthcare products/services (USA only).
11	Prescription eligibility amount. Allows the acquirer to indicate the portion of the amount spent on eligible prescriptions (USA only).
12	Vision Rx eligibility amount. Allows the acquirer to indicate the portion of the amount spent on eligible vision Rx or vision products/services (USA only).

Amount Type	Description
17	Mastercard prepaid online bill pay transaction fee amount
40	Cashback amount
42	Surcharge amount
44	Gratuity amount
56	Member provided fee
57	Original amount
58	Point of Interaction amount (e.g. before Dynamic Currency Conversion at the terminal)
59	Limit/Balance available amount from Mastercard In-Control

4.3 AVS Results

The table below provides details of available AVS Results (AVS_Result) values. (See also Get Transaction Message fields: AVS_Result) .

Value	Description
A	Address matches, postal code does not
N	Both Postal Code and address not matching
R	Retry, system unable to process. If the AVS response does not contain data to enable you to match, respond with a retry.
U	No data received
W	Postal code matches, address does not. This is used for both US and non-US addresses.
X	Postal code matches (address not supplied or not checked). This is used for both US and non-US addresses.
Y	Both Postal Code and address matching
Z	Postal or ZIP codes match, street addresses do not match or street address not included in request.

4.4 Bank Account Formats

This section describes the valid values for the source_bank_account_format and dest_bank_account_format fields. (See also Get Transaction Message fields: source_bank_account_format and dest_bank_account_format)

Value	Description	Examples
IBAN	International Bank Account Number. **Note**: must not contain spaces.	GR1601101250000000012300695 GB29NWBK60161331926819
GBR	6 digit sort code 1 space character 8 digit account number	601613 31926819

Note: Thredd plan to use the ISO 3-alpha country code in uppercase for the 'value' to identify bank account number formats which are specific to that country.

4.5 Calculating the Total Transaction Cost

When the External Host decides whether to approve or decline the transaction, it takes into account the total cost of the transaction, which is the sum of:

- Billing amount (`Bill_Amt` field)
- Fixed Fees (`Fee_Fixed` field)
- Rate variable Fees (`Fee_Rate` field)
- Foreign Exchange Padding (`Fx_Pad` field)
- MCC Padding (`MCC_Pad` field)

Example:

Bill_Amt	Fee_Fixed	Fee_Rate	Fx_Pad	MCC_Pad	Total amount blocked
109.45	1.41	0.92	2.04	5.08	118.90

For use of this calculation in payment authorisation, see EHI Operating Modes.

4.6 Card Status Codes

This section lists the possible card status codes. These are status codes that you can set for card via Thredd API, Thredd Portal or Smart Client. They are also used to indicate the status of a payment token. For details of transaction response codes, see Response Codes.

Status Code	Description
00	All Good. Indicates that the card is good for use, but does not indicate whether it is active.
01	Refer to card issuer
02	Card not yet activated
04	Capture Card
05	Do not honour
14	Invalid card (if you receive this status, it indicates that this card does not exist on the Thredd system and was used for a fraudulent transaction)
41	Lost card
43	Stolen card
46	Closed Account
54	Expired card
59	Suspected Fraud
62	Restricted card
63	Security violation
70	Cardholder to contact issuer
75	Allowable number of PIN tries exceeded
83	Card destroyed
98	Refund given to customer
99	Card voided
G1	A short-term block which temporarily blocks card usage for all card transactions (excluding Credits and Refunds) for a short period.
G2	Short-term full block (all transactions are blocked).
G3	Long-term block (excluding Credits and Refunds).
G4	Long-term full block (all transactions are blocked).
G5	Fraud Transaction Monitoring/Thredd Protect: A short-term block that temporarily blocks card usage for all card transactions (excluding Credits and Refunds) for a short period.
G6	Fraud Transaction Monitoring/Thredd Protect: Short-term full block (all transactions are blocked).

Status Code	Description
G7	Thredd Protect: Long-term block (excluding Credits and Refunds).
G8	Thredd Protect: Long-term full block (all transactions are blocked).
G9	IVR Lost/Stolen block. Non-reversable status, equivalent to status code 41.

4.6.1 Notes on Card Blocks (G1 - G9)

- Short-term blocks result in merchants receiving a message to try again; Visa guidelines instruct merchants to attempt up to 15 retries over 30 days.
- Long-term blocks result in merchants receiving a message not to try again. These are considered as permanent blocks. Visa expect that the card should not return to the '00 Approve' state at all, or at least not within 30 days.

4.7 Country Codes

Country codes are based on the Visa and Mastercard country codes, which are generally based on ISO 3166 country codes, but with some exceptions (as described below). You should use the correct alpha-3, alpha-2 or numeric-3 code correctly as described below.

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Afghanistan	AFG	AF	004
Åland Islands	ALA	AX	248
Albania	ALB	AL	008
Algeria	DZA	DZ	012
American Samoa	ASM	AS	016
Andorra	AND	AD	020
Angola	AGO	AO	024
Anguilla	AIA	AI	660
Antarctica	ATA	AQ	010
Antigua and Barbuda	ATG	AG	028
Argentina	ARG	AR	032
Armenia	ARM	AM	051
Aruba	ABW	AW	533
Australia	AUS	AU	036
Austria	AUT	AT	040
Azerbaijan	AZE	AZ	031
Bahamas	BHS	BS	044
Bahrain	BHR	BH	048
Bangladesh	BGD	BD	050
Barbados	BRB	BB	052
Belarus	BLR	BY	112
Belgium	BEL	BE	056
Belize	BLZ	BZ	084
Benin	BEN	BJ	204
Bermuda	BMU	BM	060

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Bhutan	BTN	BT	064
Bolivia, Plurinational State of	BOL	BO	068
Bonaire, Sint Eustatius and Saba	BES	BQ	535
Bosnia and Herzegovina	BIH	BA	070
Botswana	BWA	BW	072
Bouvet Island	BVT	BV	074
Brazil	BRA	BR	076
British Indian Ocean Territory	IOT	IO	086
Brunei Darussalam	BRN	BN	096
Bulgaria	BGR	BG	100
Burkina Faso	BFA	BF	854
Burundi	BDI	BI	108
Cambodia	KHM	KH	116
Cameroon	CMR	CM	120
Canada	CAN	CA	124
Cape Verde	CPV	CV	132
Cayman Islands	CYM	KY	136
Central African Republic	CAF	CF	140
Chad	TCD	TD	148
Chile	CHL	CL	152
China	CHN	CN	156
Christmas Island	CXR	CX	162
Cocos (Keeling) Islands	CCK	CC	166
Colombia	COL	CO	170
Comoros	COM	KM	174
Congo	COG	CG	178
Congo, the Democratic Republic of the	ZAR	CD	180
Cook Islands	COK	CK	184

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Costa Rica	CRI	CR	188
Côte d'Ivoire	CIV	CI	384
Croatia	HRV	HR	191
Cuba	CUB	CU	192
Curaçao	CUW	CW	531
Cyprus	CYP	CY	196
Czech Republic	CZE	CZ	203
Denmark	DNK	DK	208
Djibouti	DJI	DJ	262
Dominica	DMA	DM	212
Dominican Republic	DOM	DO	214
Ecuador	ECU	EC	218
Egypt	EGY	EG	818
El Salvador	SLV	SV	222
Equatorial Guinea	GNQ	GQ	226
Eritrea	ERI	ER	232
Estonia	EST	EE	233
Ethiopia	ETH	ET	230
Falkland Islands (Malvinas)	FLK	FK	238
Faroe Islands	FRO	FO	234
Federal Republic of Germany	DDR	DD	280
Fiji	FJI	FJ	242
Finland	FIN	FI	246
France	FRA	FR	250
French Guiana	GUF	GF	254
French Polynesia	PYF	PF	258
French Southern Territories	ATF	TF	260
Gabon	GAB	GA	266

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Gambia	GMB	GM	270
Georgia	GEO	GE	268
Germany	DEU	DE	276
Ghana	GHA	GH	288
Gibraltar	GIB	GI	292
Greece	GRC	GR	300
Greenland	GRL	GL	304
Grenada	GRD	GD	308
Guadeloupe	GLP	GP	312
Guam	GUM	GU	316
Guatemala	GTM	GT	320
Guernsey	GGY	GG	831
Guinea	GIN	GN	324
Guinea-Bissau	GNB	GW	624
Guyana	GUY	GY	328
Haiti	HTI	HT	332
Heard Island and McDonald Islands	HMD	HM	334
Holy See (Vatican City State)	VAT	VA	336
Honduras	HND	HN	340
Hong Kong	HKG	HK	344
Hungary	HUN	HU	348
Iceland	ISL	IS	352
India	IND	IN	356
Indonesia	IDN	ID	360
Iran, Islamic Republic of	IRN	IR	364
Iraq	IRQ	IQ	368
Ireland	IRL	IE	372
Isle of Man	IMN	IM	833

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Israel	ISR	IL	376
Italy	ITA	IT	380
Jamaica	JAM	JM	388
Japan	JPN	JP	392
Jersey	JEY	JE	832
Jordan	JOR	JO	400
Kazakhstan	KAZ	KZ	398
Kenya	KEN	KE	404
Kiribati	KIR	KI	296
Korea, Democratic People's Republic of	PRK	KP	408
Korea, Republic of	KOR	KR	410
Kosovo - see “UNMI Kosovo” below	See below	See below	See below
Kuwait	KWT	KW	414
Kyrgyzstan	KGZ	KG	417
Lao People's Democratic Republic	LAO	LA	418
Latvia	LVA	LV	428
Lebanon	LBN	LB	422
Lesotho	LSO	LS	426
Liberia	LBR	LR	430
Libyan Arab Jamahiriya	LBY	LY	434
Liechtenstein	LIE	LI	438
Lithuania	LTU	LT	440
Luxembourg	LUX	LU	442
Macao	MAC	MO	446
Macedonia, the former Yugoslav Republic of	MKD	MK	807
Madagascar	MDG	MG	450
Malawi	MWI	MW	454
Malaysia	MYS	MY	458

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Maldives	MDV	MV	462
Mali	MLI	ML	466
Malta	MLT	MT	470
Marshall Islands	MHL	MH	584
Martinique	MTQ	MQ	474
Mauritania	MRT	MR	478
Mauritius	MUS	MU	480
Mayotte	MYT	YT	175
Mexico	MEX	MX	484
Micronesia, Federated States of	FSM	FM	583
Moldova, Republic of	MDA	MD	498
Monaco	MCO	MC	492
Mongolia	MNG	MN	496
Montenegro	MNE	ME	499
Montserrat	MSR	MS	500
Morocco	MAR	MA	504
Mozambique	MOZ	MZ	508
Myanmar	MMR	MM	104
Namibia	NAM	NA	516
Nauru	NRU	NR	520
Nepal	NPL	NP	524
Netherlands	NLD	NL	528
Netherlands Antilles	ANT	AN	530
New Caledonia	NCL	NC	540
New Zealand	NZL	NZ	554
Nicaragua	NIC	NI	558
Niger	NER	NE	562
Nigeria	NGA	NG	566

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Niue	NIU	NU	570
Norfolk Island	NFK	NF	574
Northern Mariana Islands	MNP	MP	580
Norway	NOR	NO	578
Oman	OMN	OM	512
Pakistan	PAK	PK	586
Palau	PLW	PW	585
Palestinian Territory, Occupied	PSE	PS	275
Panama	PAN	PA	591
Papua New Guinea	PNG	PG	598
Paraguay	PRY	PY	600
Peru	PER	PE	604
Philippines	PHL	PH	608
Pitcairn	PCN	PN	612
Poland	POL	PL	616
Portugal	PRT	PT	620
Puerto Rico	PRI	PR	630
Qatar	QAT	QA	634
Réunion	REU	RE	638
Romania	ROM[1]	RO	642
Russian Federation	RUS	RU	643
Rwanda	RWA	RW	646
Saint Barthélemy	BLM	BL	652
Saint Helena, Ascension and Tristan da Cunha	SHN	SH	654
Saint Kitts and Nevis	KNA	KN	659
Saint Lucia	LCA	LC	662
Saint Martin (French part)	MAF	MF	663

[1] Note that this differrs from the ISO 3-digit country code for Romania of ROU.

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Saint Pierre and Miquelon	SPM	PM	666
Saint Vincent and the Grenadines	VCT	VC	670
Samoa	WSM	WS	882
San Marino	SMR	SM	674
Sao Tome and Principe	STP	ST	678
Saudi Arabia	SAU	SA	682
Senegal	SEN	SN	686
Serbia	SRB	RS	688
Seychelles	SYC	SC	690
Sierra Leone	SLE	SL	694
Singapore	SGP	SG	702
Sint Maarten(D)	SXM	SX	534
Slovakia	SVK	SK	703
Slovenia	SVN	SI	705
Solomon Islands	SLB	SB	090
Somalia	SOM	SO	706
South Africa	ZAF	ZA	710
South Georgia and the South Sandwich Islands	SGS	GS	239
South Sudan	SSD	SS	728
Spain	ESP	ES	724
Sri Lanka	LKA	LK	144
Sudan	SDN	SD	729
Suriname	SUR	SR	740
Svalbard and Jan Mayen	SJM	SJ	744
Swaziland	SWZ	SZ	748
Sweden	SWE	SE	752
Switzerland	CHE	CH	756
Syrian Arab Republic	SYR	SY	760

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Taiwan, Province of China	TWN	TW	158
Tajikistan	TJK	TJ	762
Tanzania, United Republic of	TZA	TZ	834
Thailand	THA	TH	764
Timor-Leste	TMP	TL	626
Togo	TGO	TG	768
Tokelau	TKL	TK	772
Tonga	TON	TO	776
Trinidad and Tobago	TTO	TT	780
Tunisia	TUN	TN	788
Turkey	TUR	TR	792
Turkmenistan	TKM	TM	795
Turks and Caicos Islands	TCA	TC	796
Tuvalu	TUV	TV	798
Uganda	UGA	UG	800
Ukraine	UKR	UA	804
United Arab Emirates	ARE	AE	784
United Kingdom	GBR	GB	826
United States	USA	US	840
United States Minor Outlying Islands	UMI	UM	581
UNMI Kosovo	QZZ	QZ	900
Uruguay	URY	UY	858
Uzbekistan	UZB	UZ	860
Vanuatu	VUT	VU	548
Venezuela, Bolivarian Republic of	VEN	VE	862
Viet Nam	VNM	VN	704
Virgin Islands, British	VGB	VG	092
Virgin Islands, U.S.	VIR	VI	850

Country Name	Country 3-alpha code	Country 2-alpha code	Country 3-numeric code
Wallis and Futuna	WLF	WF	876
Western Sahara	ESH	EH	732
Yemen	YEM	YE	887
Zambia	ZMB	ZM	894
Zimbabwe	ZWE	ZW	716

4.8 Currency Codes

Currency codes are based on the ISO 4217 specification.

Code	Number	Exponent	Currency
AED	784	2	United Arab Emirates dirham
AFN	971	2	Afghan afghani
ALL	008	2	Albanian lek
AMD	051	2	Armenian dram
ANG	532	2	Netherlands Antillean guilder
AOA	973	2	Angolan kwanza
ARS	032	2	Argentine peso
AUD	036	2	Australian dollar
AWG	533	2	Aruban florin
AZN	944	2	Azerbaijani manat
BAM	977	2	Bosnia and Herzegovina convertible mark
BBD	052	2	Barbados dollar
BDT	050	2	Bangladeshi taka
BGN	975	2	Bulgarian lev
BHD	048	3	Bahraini dinar
BIF	108	0	Burundian franc
BMD	060	2	Bermudian dollar
BND	096	2	Brunei dollar
BOB	068	2	Boliviano
BOV	984	2	Bolivian Mvdol
BRL	986	2	Brazilian real
BSD	044	2	Bahamian dollar
BTN	064	2	Bhutanese ngultrum
BWP	072	2	Botswana pula
BYN	933	2	Belarusian ruble (new)
BYR	974	2	Belarusian Ruble (old)

Code	Number	Exponent	Currency
BZD	084	2	Belize dollar
CAD	124	2	Canadian dollar
CDF	976	2	Congolese franc
CHE	947	2	Swiss WIR Euro
CHF	756	2	Swiss franc
CHW	948	2	Swiss WIR Franc
CLF	990	4	Chile Unidad de Fomento
CLP	152	0	Chilean peso
CNH	157	2	Chinese Offshore Renminbi/Yuan
CNY	156	2	Chinese Renminbi/Yuan
COP	170	2	Colombian peso
COU	970	2	Unidad de Valor Real (UVR)
CRC	188	2	Costa Rican colon
CUC	931	2	Cuban convertible peso
CUP	192	2	Cuban peso
CVE	132	0	Cape Verde escudo
CZK	203	2	Czech koruna
DJF	262	0	Djiboutian franc
DKK	208	2	Danish krone
DOP	214	2	Dominican peso
DZD	012	2	Algerian dinar
EGP	818	2	Egyptian pound
ERN	232	2	Eritrean nakfa
ETB	230	2	Ethiopian birr
EUR	978	2	Euro
FJD	242	2	Fiji dollar
FKP	238	2	Falkland Islands pound
GBP	826	2	Great Britain (UK) Pound Sterling

Code	Number	Exponent	Currency
GEL	981	2	Georgian lari
GHS	936	2	Ghanaian cedi
GIP	292	2	Gibraltar pound
GMD	270	2	Gambian dalasi
GNF	324	0	Guinean franc
GTQ	320	2	Guatemalan quetzal
GYD	328	2	Guyanese dollar
HKD	344	2	Hong Kong dollar
HNL	340	2	Honduran lempira
HRK	191	2	Croatian kuna
HTG	332	2	Haitian gourde
HUF	348	2	Hungarian forint
IDR	360	2	Indonesian rupiah
ILS	376	2	Israeli new shekel
INR	356	2	Indian rupee
IQD	368	3	Iraqi dinar
IRR	364	2	Iranian rial
ISK	352	0	Icelandic króna
JMD	388	2	Jamaican dollar
JOD	400	3	Jordanian dinar
JPY	392	0	Japanese yen
KES	404	2	Kenyan shilling
KGS	417	2	Kyrgyzstani som
KHR	116	2	Cambodian riel
KMF	174	0	Comoro franc
KPW	408	2	North Korean won
KRW	410	0	South Korean won
KWD	414	3	Kuwaiti dinar

Code	Number	Exponent	Currency
KYD	136	2	Cayman Islands dollar
KZT	398	2	Kazakhstani tenge
LAK	418	2	Lao kip
LBP	422	2	Lebanese pound
LKR	144	2	Sri Lankan rupee
LRD	430	2	Liberian dollar
LSL	426	2	Lesotho loti
LYD	434	3	Libyan dinar
MAD	504	2	Moroccan dirham
MDL	498	2	Moldovan leu
MGA	969	2	Malagasy ariary
MKD	807	2	Macedonian denar
MMK	104	2	Myanmar kyat
MNT	496	2	Mongolian tögrög
MOP	446	2	Macanese pataca
MRO	478	2	Mauritanian ouguiya (old)
MRU	929	2	Mauritanian ouguiya (new)
MUR	480	2	Mauritian rupee
MVR	462	2	Maldivian rufiyaa
MWK	454	2	Malawian kwacha
MXN	484	2	Mexican peso
MXV	979	2	Mexican Unidad de Inversion (UDI)
MYR	458	2	Malaysian ringgit
MZN	943	2	Mozambican metical
NAD	516	2	Namibian dollar
NGN	566	2	Nigerian naira
NIO	558	2	Nicaraguan córdoba
NOK	578	2	Norwegian krone

Code	Number	Exponent	Currency
NPR	524	2	Nepalese rupee
NZD	554	2	New Zealand dollar
OMR	512	3	Omani rial
PAB	590	2	Panamanian balboa
PEN	604	2	Peruvian sol
PGK	598	2	Papua New Guinean kina
PHP	608	2	Philippine peso
PKR	586	2	Pakistani rupee
PLN	985	2	Polish zloty (new)
PYG	600	0	Paraguayan guaraní
QAR	634	2	Qatari riyal
RON	946	2	Romanian leu
RSD	941	2	Serbian dinar
RUB	643	2	Russian ruble (old)
RUR	810	2	Russian ruble
RWF	646	0	Rwandan franc
SAR	682	2	Saudi riyal
SBD	090	2	Solomon Islands dollar
SCR	690	2	Seychelles rupee
SDG	938	2	Sudanese pound
SEK	752	2	Swedish krona/kronor
SGD	702	2	Singapore dollar
SHP	654	2	Saint Helena pound
SLE	925	2	Sierra Leonean leone (new)
SLL	694	2	Sierra Leonean leone (old)
SOS	706	2	Somali shilling
SRD	968	2	Surinamese dollar
SSP	728	2	South Sudanese pound

Code	Number	Exponent	Currency
STD	678	2	São Tomé and Príncipe dobra (old)
STN	930	2	São Tomé and Príncipe dobra (new)
SVC	222	2	Salvadoran colón
SYP	760	2	Syrian pound
SZL	748	2	Swazi lilangeni
THB	764	2	Thai baht
TJS	972	2	Tajikistani somoni
TMM	795	0	Turkmenistan manat (old)
TMT	934	2	Turkmenistan manat (new)
TND	788	3	Tunisian dinar
TOP	776	2	Tongan pa-anga
TRL	792	2	Turkish lira
TRY	949	2	Turkish lira
TTD	780	2	Trinidad and Tobago dollar
TWD	901	2	New Taiwan dollar
TZS	834	2	Tanzanian shilling
UAH	980	2	Ukrainian hryvnia
UGX	800	0	Ugandan shilling
USD	840	2	United States dollar
USN	997	2	US Dollar (next day)
USS	998	2	US Dollar (same day)
UYI	940	0	Uruguay Peso en Unidades Indexadas
UYU	858	2	Uruguayan peso
UYW	927	4	Unidad previsional
UZS	860	2	Uzbekistan som
VEF	937	2	Venezuelan Bolivar Fuerte (old)
VES	928	2	Venezuelan bolívar soberano (new)
VND	704	0	Vietnamese dong

Code	Number	Exponent	Currency
VUV	548	0	Vanuatu vatu
WST	882	2	Samoan tala
XAF	950	0	CFA franc BEAC
XAG	961	2	Silver (one troy ounce)
XAU	959	2	Gold (one troy ounce)
XBA	955	2	European Composite Unit (EURCO) (bond market unit)
XBB	956	2	European Monetary Unit (E.M.U.-6) (bond market unit)
XBC	957	2	European Unit of Account 9 (E.U.A.-9) (bond market unit)
XBD	958	2	European Unit of Account 17 (E.U.A.-17) (bond market unit)
XCD	951	2	East Caribbean dollar
XDR	960	2	Special drawing rights
XOF	952	0	CFA franc BCEAO
XPD	964	2	Palladium (one troy ounce)
XPF	953	0	CFP franc (franc Pacifique)
XPT	962	2	Platinum (one troy ounce)
XSU	994	2	SUCRE
XTS	963	2	Code reserved for testing purposes
XUA	965	2	ADB Unit of Account
XXX	999	2	No currency
YER	886	2	Yemeni rial
ZAR	710	2	South African rand
ZMK	894	2	Zambian kwacha (old)
ZMW	967	2	Zambian kwacha (new)
ZWD	716	2	Zimbabwean dollar
ZWL	932	2	Zimbabwean dollar A/10

4.9 CVV2 Indicators

4.9.1 CVV2 Presence Type Indicator

If the CVV2 field has 6 characters, then the first character is the CVV2 Presence Type indicator.

This has the following values:

CVV2 Presence Type indicator	Description	Comment
0	CVV2 value not provided	Nothing to validate.
1	CVV2 present	CVV2 will be present in positions 4 to 6 inclusive in the 'CVV2' field. If you have chosen to validate CVV2 yourself, then check the CVV2.
2	CVV2 value on card but not legible	Nothing to validate. You may want to consider declining the transaction if you expect CVV2 to be present on the card.
3	Dynamic CVV2 present	You should never receive this (only for issuers that subscribe to CVV2 fallback service from Visa)
9	No CVV2 value on card	Nothing to validate. You may want to consider declining the transaction if you expect CVV2 to be present on the card.

4.9.2 CVV2 Response Type Indicator

If the CVV2 field has 6 characters, then the second character is the CVV2 Response Type indicator.

This has the following values:

CVV2 Response Type indicator	Description	Comment
0	Visa do not expect field 44.9 result of CVV2 validation	Ignore - Thredd will handle this
1	Visa expect field 44.9 result of CVV2 validation	Ignore - Thredd will handle this

4.10 Dispute Condition

The Dispute_Condition field contains a code to indicate additional information to the Reason_ID field.

Note: Describes the Dispute Condition for a Visa chargeback; may be used as additional information to describe chargebacks and/or representments.

The usage varies per type of message, as follows:

MTID	Txn_Type	Description	Details
1240	C	Chargeback Notification	For Visa cards: Dispute Reason for the chargeback (in addition to Reason_ID field.) See below. For Other cards: not defined. Will be blank.
1240	H	Chargeback Notification (Non-Credit)	For Visa cards: Dispute Reason for the chargeback (in addition to Reason_ID field.) See below. For Other cards: not defined. Will be blank.
(all other combinations)		(all other transactions)	Not defined. Will be blank.

4.10.1 Visa Dispute_Condition for Chargeback (Txn_Type C and H)

In Visa network chargeback message types, the Dispute_Condition field provides additional information on the reason for the chargeback (in addition to details in the Reason_ID field). For more information, refer to the *Visa chargeback documentation*.

Visa codes are defined in the BASE2 file TC33 "*Base2 Dispute Financial Status Advice*" TCR1 record position 9-11 "*Dispute Condition*". This is specific to Visa chargebacks initiated on the VROL system. The meaning varies depending on the value of the Reason_ID field.

Note: Visa do not explicitly define the codes in the BASE2 document; the table below provides the Thredd interpretaion for guidance only.

Table of Thredd Interpretation of the VISA Codes

Visa Reason_ID	Visa Dispute_ Condition	Thredd's interpretation as to the Visa meaning
10 (Fraud)	1	EMV liability shift Counterfeit fraud
10 (Fraud)	2	EMV liability shift non-counterfeit fraud
10 (Fraud)	3	Other Fraud (Card Present Environment)
10 (Fraud)	4	Other Fraud (Card Absent Environment)
10 (Fraud)	5	Visa Fraud Monitoring Program
10 (Fraud)	(other)	Refer to Visa
11 (Authorisation)	1	Card Recovery Bulletin
11 (Authorisation)	2	Declined Authorisation
11 (Authorisation)	3	No Authorisation
11 (Authorisation)	(other)	Refer to Visa

Visa Reason_ID	Visa Dispute_ Condition	Thredd's interpretation as to the Visa meaning
12 (Processing Error)	1	Late Presentment
12 (Processing Error)	2	Incorrect Transaction Code
12 (Processing Error)	3	Incorrect Currency
12 (Processing Error)	4	Incorrect Account Number
12 (Processing Error)	5	Incorrect Amount
12 (Processing Error)	6	Duplicate Processing / Paid by Other Means
12 (Processing Error)	6.1	Not sure. Probably one of 'Duplicate Processing', or 'Paid by Other Means'
12 (Processing Error)	6.2	Not sure. Probably one of 'Duplicate Processing', or 'Paid by Other Means'
12 (Processing Error)	7	Invalid Data
12 (Processing Error)	(other)	Refer to Visa
13 (Consumer Dispute)	1	Merchandise/Services not as received
13 (Consumer Dispute)	2	Cancelled Recurring
13 (Consumer Dispute)	3	Not as Described or Defective Merchandise/services
13 (Consumer Dispute)	4	Counterfeit Merchandise
13 (Consumer Dispute)	5	Misrepresentation
13 (Consumer Dispute)	6	Credit not processed
13 (Consumer Dispute)	7	Cancelled Merchandise/services
13 (Consumer Dispute)	8	Original Credit Transaction Not Accepted
13 (Consumer Dispute)	9	Non-receipt of Cash or Load Transaction Value
13 (Consumer	(other)	Refer to Visa

Visa Reason_ID	Visa Dispute_ Condition	Thredd's interpretation as to the Visa meaning
Dispute)		

4.11 Dynamic CVV2

The Card Verification Value 2 (referred to by Visa as CVV2 and Mastercard as CVC 2) is a 3 digit code displayed on the back or front of the card. The cardholder must enter or provide the CVV2 during a card-not-present transaction, as a way of verifying that they have the card in their possession. Since the CVV2 is a static number, this makes it more susceptible to fraud.

With dynamic CVV2[1], the default CVV2 value linked to the card record is ignored; the CVV2 value is verified during transaction authorisation against another value which your systems dynamically supply to the cardholder (e.g., via their card app or SMS). This can improve the security of card-not-present transactions.

4.11.1 How it works

Thredd assigns a static CVV2 to the card record when it is generated. If Dynamic CVV2 is enabled, then we by-pass our CVV2 value checks during the authorisation stage and send the transaction to your systems through EHI to authorise or decline. You should then ignore the card's default CVV2 value, and check the CVV2 value in the EHI transaction record against the dynamic value you provided to your cardholder.

Note: Dynamic CVV2 is only available on Gateway Processing (mode 1) or Gateway Processing with STP (mode 4), where you approve the transaction.

4.11.2 How to Configure

In the **Card Usage Rules** tab on your Product Setup Form (PSF), in the **Verification Checks (V)** box, set the **Bypass CVV2/CVC2 Check** field to **Yes**.

Thredd will not verify the CVV2 and instead this will be sent over EHI for you to verify and approve.

Allow? Y/N	Verification Checks (V)
No	Bypass Online PIN Check
No	Bypass Expiry Date Check
Yes	Bypass CVV2/CVC2 Check
No	Blank CVV2 in Card not Present E-commerce
No	Blank CVV2 in Card not Present Phone/Mail Order
No	Blank CVV2 in Card not Present Recurring
No	Blank CVV2 in Card not Present Manual Key Entry
No	Allow Blank DE014
No	Expiry date optional for Recurring Payments
No	Bypass Card Status Check for Refund Authorisations

Figure 19: Card Usage Groups: Verification Checks

If you want Thredd to ignore the default value for Dynamic CVV2 with printed cards and print the card without a CVV2 field, you must discuss this with your Card Manufacturer. For more information on configuration options and card designs for physical cards, see the Physical Cards Guide.

If using Dynamic CVV2 with virtual cards, then you can configure your Virtual Image to not display the CVV2 field. For details, see the Virtual Cards Guide > Virtual Card Image Design.

Dynamic CVV2 can be set at card level by assigning the Card Usage group to the card, and therefore can be applied to cards already issued (the cards must be on a product where you are on Gateway Processing - modes 1 and 4).

To be able to check that the VV2 value is included in the EHI Authorisation message, confirm with your Implementation Manager that you require the **send CVV2** option to be enabled on your EHI Configuration. See EHI Configuration Options.

---

[1] Visa refer to this service as dynamic CVV2 (dCVV2) and Mastercard refer to it as dynamic Card Validation Code 2 (dynamic CVC 2). **Important**: You should not confuse this with dynamic CVV1 /CVC 1 or dynamic CVV3 /CVC 3, which are different services.

Note: Large merchants such as Paypal and Amazon may not send CVV2. If you specify that a CVV2 response is mandatory, then this may cause declines. We therefore recommend that in your **Card Usage Rules** you set the **Allow Blank CVV2 in Card not Present E-commerce** to **Yes**. See The Physical Cards Guide > Cards Usage Options.
During the transaction authorisation stage, we recommend that your systems do not decline a blank CVV2 value where the transaction originated from a large merchant such as Payal or Amazon[2].

4.11.3 Checking the CVV2 at the Authorisation Stage

During transaction authorisation (using Dynamic CVV2):

1. The cardholder enters the CVV2 value provided to them by your systems (e.g., via phone app, SMS, web portal or smart card).
2. The Merchant includes the CVV2 value in the authorisation request.
3. When Thredd receives the request from the card scheme, we bypass the CVV2 value checks (as **Bypass CVV2** is enabled in the card Usage Group). Thredd then takes the clear CVV2 value and encrypts it.
4. The Authorisation request is sent to your systems to validate the CVV2 value, along with any other checks; your systems must return an approve or decline decision.
5. Thredd returns your response to the card scheme.

Note: The CVV2 validation result is provided in the 0110 authorisation response message, in the **F44.10** field for Visa and in the **DE048.87** field for Mastercard.

4.11.4 CVV2 Processing at the Card Scheme

Check with your Implementation Manager for relevant CVV2 processing options that should be configured at scheme level.

---

2 You can use Merch_ID_DE42 or Merch_Name_DE43 to identify the merchant.

4.12 GPS_POS_Capability field

This is a Thredd defined field that records POS terminal capabilities for this transaction. It is made up of various subfields.

4.12.1 GPS_POS_Capability Fields

Refer to the table below for details

Note: All subfields are concatenated together in order. Subfields begin at position 1. You may only receive the leading subfields (i.e. 1 or more). Additional subfields may be added.

Position	Name	Format	Description / Valid Values
1	Partial Approval Support	N(1,1)	Indicates if POS terminal supports partial approval or not: 0 = not supported (default assumption) 1 = supported
2	Purchase Amount only approval support	N(1,1)	Indicates if POS terminal supports approval of the purchase amount only, in a purchase with cashback transaction. 0 = not supported (default assumption) 1 = supported
3 to 22	Card Data Input Capability	AN(20,20)	Card Data Input methods supported by the terminal. 1 position for each possible method. Each position is set to: 1=Supported, 0=Not supported See Card Data Input Capability subfield
23 to 42	Cardholder authentication capability	AN(20,20)	Cardholder authentication methods supported by the terminal. 1 position for each possible method. Each position is set to: 1=Supported, 0=Not supported See Cardholder Authentication Capability subfield
43	Card capture capability	AN(1,1)	0 = Card capture not supported 1 = Card capture supported 9 = Unknown
44	Terminal Attended indicator	AN(1,1)	Indicates if the terminal is attended by the merchant 0 = No terminal used 1 = Attended 2 = Unattended 9 = Unknown **Note**: On Visa card transactions, the information in GPS_POS_Capability position 44 should not be relied on, as merchants/Acquirers do not always submit the correct information.
45	Terminal Environment	AN(1,1)	Indicates the Terminal Environment or Location-type 0 = No terminal used 1 = On premises of card acceptor 2 = Off premises of card acceptor 3 = On premises of cardholder 9 = Unknown
46	Terminal Card Data Output	AN(1,1)	Indicates the ability of the terminal to write to the card

Position	Name	Format	Description / Valid Values
	Capability		0 = Unknown 1 = None (eg if no terminal used) 2 = Magnetic Stripe Write 3 = ICC S = Other
47	Terminal output capability	AN(1,1)	Indicates the output capabilities of the terminal 0 = Unknown 1 = None 2 = Print only 3 = Display only 4 = Print and Display
48	Terminal PIN capture capability	AN(1,1)	Terminal PIN Capture Capability. Says if the terminal can capture PINs, and if so, the maximum length of PIN supported: 0 = None 1 = Unknown 4 = Yes, max length 4 digits 5 = Yes, max length 5 digits 6 = Yes, max length 6 digits 7 = Yes, max length 7 digits 8 = Yes, max length 8 digits 9 = Yes, max length 9 digits A = Yes, max length 10 digits B = Yes, max length 11 digits C = Yes, max length 12 digits
49	Terminal Type	AN(1,1)	Defines what sort of terminal this is. (here 'CAT' means Cardholder Activated Terminal.) 0 = Unknown/Unspecified 1 = CAT level 1 - Automated Dispensing Machine 2 = CAT level 2 - self-service terminal 3 = CAT level 3 - Limited Amount Terminal 4 = CAT level 4 - In-flight commerce terminal 5 = CAT level 5 6 = CAT level 6 - e-commerce terminal 7 = CAT level 7 - Transponder 8 = Remote Terminal (eg Mastercard Tap to More transaction) 9 = Mobile POS acceptance device M = Manual (no terminal used) A = ATM R = Electronic Cash Register or normal attended POS device

4.12.2 Card Data Input Capability subfield

This describes the "Card Data Input Capability"subfield of GPS_POS_Capability. See above.

Card Data Input Capability is a 20 character field. Each position represents a different capability, with a value set to either: 1=Supported or 0=Not supported.

See the table below.

GPS_POS_Capability position	Card Data Input Capability position	Name
3	1	Unknown
4	2	Manual (eg zip-zap); no terminal or server
5	3	Magnetic Stripe
6	4	Barcode
7	5	OCR
8	6	EMV contact
9	7	PAN Key Entry
10	8	Contactless Magnetic Stripe
11	9	EMV contactless or qVSDC contactless
12	10	Account Data on File
13	11	QR code
14	12	E-Commerce
15	13	E-Commerce with EMV cryptogram
16	14	MICR reader
17	15	Reserved
18	16	Reserved
19	17	Reserved
20	18	Reserved
21	19	Reserved
22	20	Reserved

Example 1

If GPS_POS_Capability *= "11001001000100000000000100100101000000000019234CR"* then this indicates that the following card data input capabilities are supported: Magnetic Stripe, EMV contact, Account Data on File.

4.12.3 Cardholder Authentication Capability subfield

Positions 23 to 42 inside the GPS_POS_Capability field represent the Cardholder Authentication Capabilities.

The table defines which Cardholder Authentication Capability is defined by each position. Each position's value is set to either: 1=Supported, or 0=Not supported / unknown.

GPS_POS_Capability position	Cardholder authentication Capability position	Name
23	1	None

GPS_POS_Capability position	Cardholder authentication Capability position	Name
24	2	PIN (online or offline)
25	3	Electronic signature analysis
26	4	biometrics
27	5	biographic
28	6	Manual signature verification
29	7	Manual other (eg drivers licence / ID card)
30	8	Offline PIN
31	9	Online PIN
32	10	3D-Secure
33	11	Account based digital signature
34	12	Public key based digital signature
35	13	Unknown
36	14	Reserved
37	15	Reserved
38	16	Reserved
39	17	Reserved
40	18	Reserved
41	19	Reserved
42	20	Reserved

Example 2

If GPS_POS_Capability = “1100100100010000000000010010010100000000019234CR” this indicates that the following Cardholder authentication methods are supported: PIN, biographic, Offline PIN, 3D-secure.

4.12.4 Full GPS_POS_Capability example

If GPS_POS_Capability = “11001001000100000000000100100101000000000019234CR”

Then this indicates:

Position	Value	Meaning
1	1	Partial approval supported
2	1	Purchase amount only approval supported

Position	Value	Meaning
3	0	Card data input capability not unknown
4	0	Card data input by manual not supported
5	1	Card data input by magnetic stripe supported
6	0	Card data input by barcode not supported
7	0	Card data input by OCR not supported
8	1	Card data input by EMV contact supported
9	0	Card data input by PAN key entry not supported
10	0	Card data input by Contactless Magnetic stripe not supported
11	0	Card data input by EMV contactless not supported
12	1	Card data input by Account Data on file supported
13	0	Card data input by QR code not supported
14	0	Card data input by E-commerce not supported
15	0	Card data input by E-commerce with EMV not supported
16	0	Card data input by MICR reader not supported
17	0	Reserved for future use.
18	0	Reserved for future use.
19	0	Reserved for future use.
20	0	Reserved for future use.
21	0	Reserved for future use.
22	0	Reserved for future use.
23	0	No Cardholder authentication at all is not supported
24	1	Cardholder authentication by PIN supported
25	0	Cardholder authentication by Electronic signature analysis not supported
26	0	Cardholder authentication by biometrics not supported
27	1	Cardholder authentication by biographic supported
28	0	Cardholder authentication by manual signature not supported
29	0	Cardholder authentication by manual (other) not supported
30	1	Cardholder authentication by offline PIN supported

Position	Value	Meaning
31	0	Cardholder authentication by online PIN not supported
32	1	Cardholder authentication by 3D-secure supported
33	0	Cardholder authentication by Account based digital signature not supported
34	0	Cardholder authentication by Public key based digital signature not supported
35	0	Cardholder authentication by unknown means not indicated
36	0	Reserved for future use.
37	0	Reserved for future use.
38	0	Reserved for future use.
39	0	Reserved for future use.
40	0	Reserved for future use.
41	0	Reserved for future use.
42	0	Reserved for future use.
43	1	Card capture supported
44	9	Unknown if terminal is attended
45	2	Terminal is off premises of card acceptor
46	3	Terminal supports card output by ICC writing
47	4	Terminal has Print and Display capability
48	C	Terminal can capture up to 12 digit PINs
49	R	Terminal is a normal POS or cash register

4.13 GPS_POS_Data field

This is a Thredd field that records POS Data codes, which are specific to this transaction. Each position records a different piece of information. Positions 33 onwards are reserved for future use.

Note: All subfields are concatenated together in order. Subfields begin at 1. You may only receive the leading subfields (i.e. 1 or more.)

4.13.1 GPS_POS_Data Positions

Position	Name	Format	Values defined in section
1	Cardholder Present	AN(1,1)	Cardholder Present Indicator
2	Card Present	AN(1,1)	Card Present Indicator
3	Card Data Input Method	AN(1,1)	Card Data Input Method
4	Cardholder authentication method 1	AN(1,1)	Cardholder authentication Method
5	Cardholder authentication method 2	AN(1,1)	Cardholder authentication Method
6	Cardholder authentication method 3	AN(1,1)	Cardholder authentication Method
7	Cardholder authentication method 4	AN(1,1)	Cardholder authentication Method
8	Cardholder authentication entity 1	AN(1,1)	Cardholder authentication Entity
9	Cardholder authentication entity 2	AN(1,1)	Cardholder authentication Entity
10	Cardholder authentication entity 3	AN(1,1)	Cardholder authentication Entity
11	Cardholder authentication entity 4	AN(1,1)	Cardholder authentication Entity
12	Chip fallback indicator	AN(1,1)	Chip Fallback Indicator
13	Fraud indicator	AN(1,1)	POS Fraud Indicator
14	Security protocol in the cardholder->merchant interaction	AN(1,1)	Security Protocol (between cardholder device and merchant)
15	3D secure authentication method	AN(1,1)	3D-secure Authentication Method
16	InstantFunding_Network	N(1,1)	InstantFunding_Network
17	InstantFunding_GPS	N(1,1)	InstantFunding_GPS
18	ExemptFromSCA	AN(1,1)	ExemptFromSCA
19	SCA assessment result	AN(1,1)	SCA assessment result
20	SCA test: Knowledge	AN(1,1)	SCA test: Knowledge
21	SCA test: Possession	AN(1,1)	SCA test: Possession
22	SCA test: Biometric (inherence)	AN(1,1)	SCA test: Biometric (inherence)

Position	Name	Format	Values defined in section
23	Thredd Exempt from SCA Indicator	AN(1,1)	Thredd Exempt from SCA Indcator
24	Card/device type (form factor)	AN(1,1)	Card/Device Type (Form Factor)
25	Acquirer Exempt from SCA Indicator (specifies if the acquirer sent an exemption indicator in the incoming message)	AN(1,1)	Acquirer Exempt from SCA Indicator
26	Result of the Authentication Amount and Currency comparison (applicable for 3D Secure transactions only).	AN(1,1)	Authentication Amount and Currency Comparison
27	Merchant or cardholder initiated indicator	AN(1,1)	Merchant or Cardholder Initiated Indicator
28	Merchant Initiated transaction type (or setup of) indicator	AN(1,1)	Merchant Initiated Transaction Type Indicator
29	Original transaction SCA exempt indicator	AN(1,1)	Original Transaction SCA Exempt Indicator
30	Original transaction SCA assessment result	AN(1,1)	Original Transaction SCA Assessment Result
31	Original transaction status value	AN(1,1)	Original Transaction Status Value
32	Extended Authorization indicator	AN(1,1)	Extended Authorization Indicator
33	Reserved for future use	AN	Ignore this, if arrives.

Note: Any positions not received should be treated as 'Unknown'.

4.13.2 Cardholder Present Indicator

This field describes if the cardholder was present at the point of sale, or if not, why not. Values are as follows:

Cardholder Present value	Meaning
0	Cardholder present
1	Cardholder not present, unspecified
2	Cardholder not present, mail order
3	Cardholder not present, telephone order
4	Cardholder not present, standing auth/recurring transaction (could recur forever)
5	Cardholder not present, e-commerce
6	Cardholder not present, installment transaction (like recurring but fixed number of installments)
9	Unknown

4.13.3 Card Present Indicator

This field describes if the card was present at the point of sale, or if not, why not. Values are as follows:

Cardholder Present value	Meaning
0	Card not present
1	Card present
9	Unknown

4.13.4 Card Data Input Method

This field describes how the card data (eg PAN) was provided to the terminal. Values are as follows:

Card Data Input Method value	Meaning
0	Information not provided
1	Manual, no terminal
2	Magnetic stripe read
3	Bar code
4	Optical Character Recognition
5	Chip dip (i.e. EMV contact)
6	Key entered / added manually
7	EMV contactless or VSDC contactless
V	E-Commerce
C	E-Commerce with EMV cryptogram
E	Contactless magnetic stripe
F	Account Data on File
G	Key entered by Acquirer (merchant phoned acquirer with card data)
M	MICR reader
Q	QR code

4.13.5 Cardholder Authentication Method

There are four cardholder authentication methods recorded in `GPS_POS_Data`. The table below describes the possible cardholder authentication method values.

Value	Meaning
0	Not authenticated.
1	PIN.
2	Electronic signature analysis.
3	Biometrics (eg fingerprint, vein scan).
4	Biographic (eg date-of-birth, other data).
5	Manual signature verification.
6	Other manual verification (e.g. drivers licence).
7	Other.
8	Unknown.
9	Passcode/Password (e.g. to unlock a smartphone).
A	Pattern (e.g. to unlock a smartphone).
B	Possession of Hardware device (e.g. number generating key fob).
C	Possession of Hardware device with user verification (as 'B', but additionally the cardholder was verified too).
D	Possession of software application (e.g. passcode generating program).
E	Possession of software application with user verification (as 'D', but additionally the cardholder was verified too).
S	3D-Secure.
T	Tokenization Authentication Framework.

Note: It is possible for a merchant to specify two cardholder authentication methods. For example, a merchant could apply both PIN verification and Signature verification to an authorisation. Where a method is more secure (such as PIN vs signature), Thredd will put the more secure method in GPS_POS_Data position 4 and the less secure in GPS_POS_Data position 5. Note that GPS_POS_Data positions 6 and 7 are reserved for future use.

Note: Values 7,9,A,B,C,D,E as of 06/01/2021 Thredd expect to see from Visa only, and initially only for transactions on a payment-token (e.g. a smartphone).

4.13.6 Cardholder Authentication Entity

There are four cardholder authentication methods recorded in GPS_POS_Data.

For each authentication method, the entity performing that authentication method is recorded in the four cardholder authentication entity values.

For example: “Cardholder authentication entity 2” describes which entity performed the “Cardholder authentication method 2” test.

The table below describes the possible values for cardholder authentication entities.

Value	Meaning
0	Not authenticated

Value	Meaning
1	Chip Card
2	Card Acceptance Device / Terminal
3	Authorising Agent
4	Merchant
5	Other
6	Cardholder device (e.g. mobile phone)
7	Wallet Provider and/or Token Requestor. (E.g. Apple Pay)
8	Unknown

4.13.7 Chip Fallback Indicator

This is used by Visa to indicate the likely cause of the fallback (e.g., a terminal or card problem).

This is done by noting if the previous chip transaction at the same terminal (which would 99% be on a completely different card) was also a fallback.

The table below describes the possible values for the Chips Fallback Indicator:

Value	Meaning
0	n/a (This transaction is not a chip fallback transaction, or unknown).
1	Previous transaction at same terminal was not fallback from chip.
2	Previous transaction at same terminal was fallback from chip.

4.13.8 POS Fraud Indicator

This is used by the merchant to indicate if the merchant thought the transaction was suspicious. Not all networks, acquirers or terminals may support this.

Values are as follows:

Fraud Indicator	Meaning
0	No problem
1	Merchant suspicious (in UK, this is a code 10 call)
2	Merchant verified the cardholder ID

4.13.9 Security Protocol (between cardholder device and merchant)

This describes, for an e-commerce or equivalent card data input method, what security was in place between the cardholder device and merchant system.

Values are as follows:

Security Protocol value	Meaning
0	None
1	Channel encryption (https)
N	Not applicable

4.13.10 3D Secure Authentication Method

If 3D Secure was used to authenticate the cardholder, then this indicates what type of authentication was used.

This is the authentication method as reported by the network.

Note: This field is only populated with an accurate value if Thredd receive this information from the network. The table below summarises this situation.

Network	3D-secure version	Content of this 3D Secure field on 3D Secure transactions
Visa	1 (all variants)	Limited, only values ‘x’ or ‘0’
Visa	2.0 and up	Provided, any value may be set. (From Base1 field 126.20)
Mastercard	SPA v1	Provided: only values 0,1,2,3 are possible
Mastercard	SPA v2	Provided: only values D, E, F, L, v, x, y, z are possible

Values are as follows:

3D-secure auth method	Visa Meaning	Mastercard Meaning
x	Unknown / not applicable	Unknown / not applicable
0	3DS 1.0.2 or prior (all authentication methods), or 3DS 1.0.2 frictionless flow.	No cardholder authentication performed (for SPA v1 only)
1	Challenge flow using static Passcode	Password (for SPA v1 only)
2	Challenge flow using OTP (One-Time Password) via SMS method	Secret Key (For example, a chip card) (for SPA v1 only)
3	Challenge flow using OTP via key fob or card reader method	PKI (for SPA v1 only)
4	3DS 2.0 Challenge flow using OTP via app method	3DS 2.0 Challenge flow using OTP via app method
5	3DS 2.0 Challenge flow using OTP via any other method	3DS 2.0 Challenge flow using OTP via any other method
6	3DS 2.0 Challenge flow using KBA (Knowledge-Based Authentication) method	3DS 2.0 Challenge flow using KBA (Knowledge-Based Authentication) method
7	3DS 2.0 Challenge flow using OOB (Out of Band) with biometric method	3DS 2.0 Challenge flow using OOB (Out of Band) with biometric method
8	3DS 2.0 Challenge flow using OOB with app	3DS 2.0 Challenge flow using OOB with app login method

3D-secure auth method	Visa Meaning	Mastercard Meaning
	login method	
9	3DS 2.0 Challenge flow using OOB with any other method	3DS 2.0 Challenge flow using OOB with any other method
A	3DS 2.0 Challenge flow using any other authentication method	3DS 2.0 Challenge flow using any other authentication method
B	3DS unrecognized authentication method	3DS unrecognised authentication method
C	3DS 2.0 Push Confirmation	3DS 2.0 Push Confirmation
D	3DS 2.0 Frictionless flow, RBA (Risk-based authentication) review	3DS 2.0 Frictionless flow, RBA (Risk-based authentication) review
E	3DS 2.0 Attempts server responding	3DS 2.0 Attempts server responding
F	3DS 2.0 Frictionless flow	3DS 2.0 Frictionless flow
L	Delegated authentication	Delegated authentication
S	Frictionless flow, Smart attempts	Not applicable - only available on Visa networks
y	3DS 2.0 Challenge with Unknown authentication method	3DS 2.0 Challenge with Unknown authentication method
v	Authenticated by Mastercard IDCX ('Identity Check Express') service (or a Visa similar equivalent)	Authenticated by Mastercard IDCX ('Identity Check Express') service
z	AAV refresh transaction successfully authenticated by the ACS (Access Control Server)	AAV refresh transaction successfully authenticated by the ACS (Access Control Server)

4.13.11 InstantFunding_Network

Network flag to indicate the transaction uses instant funding (MoneySend or Visa Direct). Values are as follows:

InstantFunding_ Network value	Meaning
0	Normal transaction
1	Instant Funding Transaction

4.13.12 InstantFunding_GPS

Thredd flag to indicate the transaction uses instant funding (MoneySend or Visa Direct). Values are as follows:

InstantFunding_GPS value	Meaning
0	Normal transaction

InstantFunding_GPS value	Meaning
1	Instant Funding Transaction

4.13.13 ExemptFromSCA

Indicates if the transaction is exempt from Strong Customer Authentication (SCA) as per the Payments Service Directive Two (PSD2). Values are as follows:

ExemptfromSCA value	Description
0	Transaction not exempt from SCA or unknown.
1	Transaction is exempt from SCA due to being on an exempt Merchant Category Code (MCC). (Acquirer did not provide an SCA exemption indicator.) (As of 11/02/2020, exempt MCCs are: 4111, 4112, 4131, 4784, 7523)
2	Contactless transaction under low-value limits (identified by Thredd).
3	E-commerce transaction under low-value limits (identified by Thredd).
4	Recurring/installment transaction (identified by Thredd).
5	Credit (identified by Thredd). Visa expects credit transactions to be out-of-scope.
6	Mail Order, Telephone Order or other cardholder-not-present transaction (except recurring which is above) which is excluded from SCA requirements (identified by Thredd). This means GPS_POS_Data position 1 (cardholder present indicator) will have any value except for 0 (present), 4 (recurring) or 5 (e-commerce).
7	Acquirer is exempt (located in a country outside of the EEA or UK, so do not fall under the PSD2 jurisdiction).
8	Not a transaction under PSD2 rules
9	Reserved for a possible future Thredd detected exemption
A	Acquirer transaction risk analysis.
C	Secure corporate payment.
D	SCA delegation.
M	Merchant initiated transaction.
O	Authentication outage exemption.
R	Recurring payment.
T	Trusted merchant.
V	Low value payment.

4.13.14 SCA Assessment Result

Indicates if Thredd tested whether the transaction met the criteria for Strong Customer Authentication (SCA), and if so, what was the basis for the assessment decision.

Note: Thredd only does SCA assessments for authorisation requests; for all other transaction types (authorisation advices, clearing, reversals) this will always be 'N'. For a clearing transaction, always check the matching authorisation request(s) to determine if SCA was done.

SCA assessment result values are as follows:

Value	Description
0	Thredd tested for SCA and the transaction did not meet the criteria for SCA.
1	Thredd tested for SCA and the transaction met the criteria for SCA.The card/payment token performed SCA.
2	Thredd tested for SCA and the transaction met the criteria for SCA. At least two of the three SCA tests were performed (Knowledge, Possession and Biometric tests passed).
3	Thredd tested for SCA and the transaction met the criteria for SCA. Passed the SCA tests in both '1' (payment token performed SCA) and '2' (two of the three biometric, knowledge, possession tests).
D	Thredd did not test for SCA. When Thredd assessed the transaction, it was detected that PSD2 checks were delegated to the card/payment token. No further PSD2 assessment was required of Thredd.
N	Thredd did not test for SCA. SCA not performed or not applicable (and value 'D' not appropriate). For example, the transaction was declined or PSD2 checks were not turned on for the product.

4.13.15 SCA Test: Knowledge

Indicates whether Thredd detected that the SCA Knowledge test was performed, and if so, what was the result.

The Knowledge test checks if the cardholder knew some information known only to them (e.g. provided a PIN or Passcode.)

Note: Thredd only does SCA assessment for authorisation requests; for all other transactions (authorisation advices, clearing, reversals) this will always be 'N'.

Values are as follows:

Value	Description
N	Not performed or not applicable
0	Failed test
1	Passed test

4.13.16 SCA Test: Possession

Indicates whether Thredd detected that the SCA Possession test was performed, and if so, what was the result.

The Possession test checks that the cardholder has something that only they should possess (e.g. a physical chip card.)

Note: Thredd only does SCA assessment for authorisation requests; for all other transactions (authorisation advices, clearing, reversals) this will always be 'N'.

Values are as follows:

Value	Description
N	Not performed or not applicable
0	Failed test
1	Passed test

4.13.17 SCA Test: Biometric (inherence)

Indicates whether Thredd detected that the SCA Biometric (inherence) test was performed, and if so, what was the result.

Biometric testing includes authentication via methods such as fingerprint, iris and facical scans.

Note: Thredd only does SCA assessment for authorisation requests; for all other transactions (authorisation advices, clearing, reversals) this will always be 'N'.

Values are as follows:

Value	Description
N	Not performed or not applicable
0	Failed test
1	Passed test

4.13.18 Thredd Exempt from SCA Indicator

Indicates whether Thredd detected an SCA exemption. (**Note**: Thredd exemption is only loaded in position 18 if no Acquirer exemption exists)

This position has the same values as position 18, but, no Acquirer values will be present. See ExemptFromSCA.

4.13.19 Card/Device Type (Form Factor)

Indicates the type (form factor) of the card or payment token used to perform the transaction. Only available if present on the chip and sent by the acquirer. See PaymentToken_deviceType.

You can use this field to identify the type of payment device and capabilities it supports (e.g., to determine if EMV contact is possible).

4.13.20 Acquirer Exempt from SCA Indicator

Indicates whether the transaction is exempt from the EU's'Payment Services Directive 2 (PSD2) Strong Cardholder Authentication (SCA) requirement. This position contains:

- The acquirer's exemption, if it exists
- '0' (not exempt)

Note: Only online authorisation transactions set these exemption flags. Values are as listed below.

Value	Description
0	Transaction not exempt from SCA or unknown.
A	Acquirer Transaction Risk Analysis (identified by Acquirer).

Value	Description
C	Secure Corporate Payment (identified by Acquirer).
D	SCA Delegation (identified by Acquirer).
M	Merchant Initiated Transaction (identified by Acquirer).
O	(15th letter of the alphabet) ; Authentication Outage Exemption (identified by Acquirer).
R	Recurring Payment (identified by Acquirer).
T	Trusted Merchant (identified by Acquirer).
V	Low Value Payment (identified by Acquirer).

4.13.21 Authentication Amount and Currency Comparison

This position indicates the results of the *amount* and *currency* comparison between a 3D Secure authentication transaction and the linked authorisation transaction. You can use this result to determine whether the amount authenticated during a 3D Secure session matches the final authorised amount. (Applicable for EMV 3D Secure transactions only).

Values are as listed below.

Value	Description
N	Test not performed (e.g., not a 3D Secure transaction, or not performed since the transaction was already declined for another reason).
U	Unknown; 3D Secure transaction, but currencies not available.
C	Transaction currency different to Authentication currency.
0	Currencies match: amounts not compared.
1	Currencies match: Authorisation amount is less than or equal to the Authentication amount.
2	Currencies match: Authorisation amount is higher than the Authentication amount; difference is less than or equal to 20%.
3	Currencies match: Authorisation amount is higher than the Authentication amount; difference is greater than 20%.

4.13.22 Merchant or Cardholder Initiated Indicator

Indicates who initiated the transaction.

Value	Meaning
C	Cardholder initiated.
M	Merchant Initiated.
U	Unknown (other information in the transaction may imply one of the above two, but nothing directly indicated either).

4.13.23 Merchant Initiated Transaction Type (or setup of) Indicator

From Banknet DE48.22.05 (introduced in Mastercard announcement AN 5524, live on 07-06-2022) the 4th character (1 to 8) or U=Unknown, so:

Value	Meaning
1	Credential on file.
2	Standing Order (variable amount, fixed frequency).
3	Subscription (fixed amount, fixed frequency).
4	Instalment (known amount over a specified duration based on a single purchase).
5	Partial Shipment (for when e-commerce ordered goods are not all available at the time of shipment. Each shipment is a separate transaction).
6	Related / Delayed Charge (An additional charge after initial services have been paid for. (For example: mini-bar charge in hotel.)
7	No Show Charge (a penalty charge permitted by the merchant's cancellation policy).
8	Resubmission (previous authorisation was declined, but merchant can try again. (For example: transit debt recovery.)
U	Unknown or not applicable.

4.13.24 Original Transaction SCA Exempt Indicator

Either the `GPS_POS_Data` position 18 value from the original transaction or:

Value	Meaning
L	Lookup of original transaction attempted, but original not found.
X	Not applicable (original transaction not applicable or lookup was not attempted).

4.13.25 Original Transaction SCA Assessment Result

Either the `GPS_POS_Data` position 19 value from the original transaction or:

Value	Meaning
L	Lookup of original transaction attempted, but original not found.
X	Not applicable (original transaction not applicable or lookup was not attempted).

4.13.26 Original Transaction Status Value

Either the Transaction Status `Txn_Stat_Code` from the original transaction (for values, see Transaction Status Codes) or:

Value	Meaning
U	Original transaction status not known or not applicable

4.13.27 Extended Authorisation Indicator

For cardholder-initiated card-not-present transactions, indicates whether the acquirer has requested a 30-day clearing extension. If requested, then the acquirer will have up to 30 days to submit the linked presentment transaction.

Note: Applicable to Visa network transactions only.

Value	Description
0	No clearing extension requested.
1	Acquirer requested a 30-day clearing extension. If you receive this value, then note that this will extend the number of days the transaction funds remain blocked on the card, up to 30 days. If you manage the balance ledger, then you should keep the transaction amount block in place for the 30-day period or until you receive the linked presentment.

4.13.28 GPS_POS_Data Example

Below is an example of GPS_POS_Data.

Example 1 - Length of 18 characters

If GPS_POS_Data = “0151500340002Nx000”

Then this indicates:

Position	Value	Meaning
1	0	Cardholder is present
2	1	Card is present
3	5	EMV contact
4	1	1st cardholder authentication method was PIN
5	5	2nd cardholder authentication method was signature
6	0	No 3rd cardholder authentication method was used
7	0	No 4th cardholder authentication method was used
8	3	PIN (1st cardholder authentication method) was checked by the authorising Agent (i.e. Network, Thredd or EHI)
9	4	Signature (2nd cardholder authentication method) was checked by the Merchant
10	0	n/a (as no 3rd cardholder authentication method)
11	0	n/a (as no 4th cardholder authentication method)
12	0	Not a chip fallback transaction
13	2	Merchant verified the cardholder ID
14	N	Security protocol (cardholder to merchant) not applicable

Position	Value	Meaning
15	x	3D-secure not applicable
16	0	Instant Funding (Thredd indicator) not applicable
17	0	Instant Funding (Network indicator) not applicable
18	9	ExemptFromSCA not applicable or unknown

Note: Positions 19 onwards are not present and can be treated as 'Unknown'.

Example 2 - Length of 32 characters

If GPS_POS_Data = "0151500340002Nx00031109C01MU93U1"

Then this indicates:

Position	Value	Meaning
1	0	Cardholder is present
2	1	Card is present
3	5	EMV contact
4	1	1st cardholder authentication method was PIN
5	5	2nd cardholder authentication method was signature
6	0	No 3rd cardholder authentication method was used
7	0	No 4th cardholder authentication method was used
8	3	PIN (1st cardholder authentication method) was checked by the authorising Agent (i.e. Network, Thredd or EHI)
9	4	Signature (2nd cardholder authentication method) was checked by the Merchant
10	0	n/a (as no 3rd cardholder authentication method)
11	0	n/a (as no 4th cardholder authentication method)
12	0	Not a chip fallback transaction
13	2	Merchant verified the cardholder ID
14	N	Security protocol (cardholder to merchant) not applicable
15	x	3D-secure not applicable
16	0	Instant Funding (Thredd indicator) not applicable.
17	0	Instant Funding (Network indicator) not applicable.
18	9	ExemptFromSCA not applicable or unknown.

Position	Value	Meaning
19	3	Transaction is SCA, as passed 2+ of the knowledge, possession & biometric tests.
20	1	SCA Knowledge test passed.
21	1	SCA Possession test passed.
22	0	SCA Biometric (inherence) test failed.
23	9	Thredd Exempt from SCA Indicator not applicable or unknown.
24	C	Card or device type is card.
25	0	Acquirer Exempt from SCA Indicator: Transaction not exempt from SCA or unknown.
26	1	Currencies match, Authorisation amount is less than or equal to Authentication amount.
27	M	Merchant initiated.
28	U	Unknown or not applicable.
29	9	GPS_POS_Data Position 18 value from the original transaction.
30	3	GPS_POS_Data Position 19 value from the original transaction.
31	U	Original Transaction status not known or not applicable.
32	1	Acquirer requested a 30-day clearing extension.

4.14 Load Source

The table below lists the valid values for the `LoadSRC` field, identifying the source of a Load. (See also Get Transaction Message fields: LoadSRC)

ID	Source	Notes
1	POS standard	
2	Thredd Kiosk	
3	Thredd Website	
4	Card Processor	
5	Standard Web Service or Cards API	
6	Agent	
7	Head Office	
8	Call Centre	
9	Customer Web site	
10	Wirecard	
11	Customer kiosk	
12	Customer mobile app	
13	Thredd IVR	
14	Unknown	
16	Load From Card Request File	
17	Corporate	
18	epay	
19	HOCA Verifiable	
20	Post Office	
21	HOCA Non Verifiable	
22	Paypoint	
23	DXB POS Reload	
24	TCC Web Report	
25	TCC Online	
26	VIRGIN POS Reload	

ID	Source	Notes
27	TCC POS Reload	
28	TCC Promotion	
29	DXB Zero Load	
30	AlFardan Reload	
31	UAEx Reload	
32	AlAnsari Reload	
33	14 day Cool Off	
34	Unload to Repatriate	
35	Loan Repayment	
36	DXB Online	
37	Payzone	
38	VIRGIN Zero Load	
39	VIRGIN POS standard	
40	JADE Web Report	
41	JADE POS standard	
42	JADE POS Reload	
43	JADE Zero Load	
44	Wirecard-Cadooz	
45	Crunch POS Standard	
46	CRUNCH POS Reload	
47	Unload Fee Test	
48	Balance Transfer Fee Test	
49	Sofort Banking	
50	Wirecard e-commerce	
51	UAExAirport POS Standard	
52	UAExAirport Reload	
53	Cadooz Load	
54	Cadooz Reload	

ID	Source	Notes
55	Cadooz web unload	
56	Sofort Bank Transfer Load	
57	Billpay Payment	
60	Post Office and Paypoint	
61	Credit Limit	
62	Credit Card Payment	
63	Ukash Payment	
64	Bank Transfer	For Bank transfers, the following fields will be present in the request message: source_bank_ctry source_bank_account_format source_bank_account dest_bank_ctry dest_bank_account_format dest_bank_account
65	Giropay	
66	Sofortüberweisung	
67	Debit Card	
68	Primary Card	
74	Master Virtual Card	
75	Micropayment	
76	MVC Load	
77	iMVC Load	

4.15 Load Type

The table below lists the valid values for the `LoadType` field, identifying the type of Load. (See also Get Transaction Message fields: LoadType)

ID	Source
0	Unknown
1	Cash
2	Debit card
3	Credit card
4	e-Wallet
5	Bank account
6	Import
7	Savings Stamps
8	Cheque
9	Export
10	Transfer
11	From/To Offline Balance

4.16 Mastercard_AdviceReasonCode_DE60

The Mastercard_AdviceReasonCode_DE60 field is present for MTID='0120' (Authorisation Advice) and MTID='0420' (Reversal Advice) transactions on Mastercard. In both cases it provides information on why the advice was generated.

Note: Mastercard may add, remove or change any of the values at any time.

The field is divided into three parts:

Position	Length	Format	Description
1 to 3	3	N(3,3)	Advice Reason Code - reason why this advice was created See Positions 1-3 Advice Reason Code
4 to 7	4	N(4,4)	Advice Detail Code - May be present (depending on the Advice Reason Code) providing additional information. See Positions 4-7 Advice Detail Code
8 to the end	1 to 53	ANS(1,53)	Advice Detail Text - May be present (depending on the Advice Reason Code) providing additional information as human readable format.

4.16.1 Positions 1-3 Advice Reason Code

Provides three digits to describe why the MTID=0120 or MTID=0420 advice was created. See the table below.

Note: Not all the codes below are applicable, for example: some may only apply to Acquirers, and some only apply to services you may not be using.

- *Alternate Issuer Route* refers to the Mastercard STIP system.
- *MIP* is part of the Mastercard system. The Acquirer is connected to one MIP, Issuer (Thredd) is connected to another MIP.

Advice Reason Code	Meaning
100	Alternate Issuer Route: Issuer selected option
101	Alternate Issuer Route: IPS signed out
102	Alternate Issuer Route: IPS timed out
103	Alternate Issuer Route: IPS unavailable
105	Transaction processed via X-Code (i.e., Mastercard processed this at their Acquiring MIP).
107	PIN processing error
108	Alternate Issuer Route: MIP Error
109	Alternate Issuer Route: Issuer Edit Response Error
111	Alternate Issuer Route: Issuer Host System Error
112	Alternate Route: Network Not Dispatched Error
113	Alternate Route: Issuer Undelivered
114	Alternate Route: Direct Down Option
115	Transaction Processed via On-behalf Service Decision

Advice Reason Code	Meaning
116	Invalid Merchant
120	Transaction Blocking (blocked by a Mastercard Fraud System; this normally configured with your issuer; Thredd is not involved .)
121	Account Lookup Service
126	Pay with Rewards Processing Advice to Issuer
140	Unable to convert contactless or virtual account number
141	Mastercard Digital Enablement Service Advice to Issuer
150	Mastercard Transaction blocking for Mastercard Send or other transaction blocking service.
151	In Control Processing Advice to Issuer (Mastercard Merchant Presented QR)
160	Authentication Advice to Issuer
180	CAT Risk Level 3
190	Acquirer Processing System (APS) Approved
191	Acquirer Processing System (APS) Completed Authorization Transaction
192	M/Chip Offline Advice to Issuer
200	In Control Processing Advice to Issuer
400	Unable to deliver response from Mastercard to Acquirer
401	No acknowledgement from Acquirer to Mastercard
402	Issuer Time-out
403	Issuer Signed out
409	Issuer Response Error
410	Reversal message provided by a system other than Mastercard’s online authorisation system (Banknet)
413	Issuer Undelivered
other	Mastercard may add other values when they please

4.16.2 Positions 4-7 Advice Detail Code

This is a 4 digit number which may be present, providing additional information, as follows:

Advice Detail Code	Meaning
0000	Accepted/Approved
Any other code	Reason why transaction was declined. There are too many codes to practically put them in this specification, if you want to know a particular value, if you have access to the Mastercard Customer Interface Specification you can look in there, otherwise you can ask Thredd.

4.17 Merch_Name_DE43 Field in Authorisations

This section describes the format of the Merchant Name/Location Field (DE43) procided in authorisation messages Merch_Name_DE43. (See also Get Transaction Message fields: Merch_Name_DE43)

4.17.1 Mastercard Authorisation

The merchant name/location field for Mastercard is made up of various subfields.

Positions	Length	Field Name	Description / Valid Values
1-22	22	Card Acceptor Name	Name of Card Acceptor or ATM service provider. (Space padded on the right to make up to 22 characters.)
23-23	1	Separator	Space character ‘ ‘
24-36	13	Card Acceptor City	City of the merchant/ATM (Space padded on the right to make up to 13 characters.)
37-37	1	Separator	Space character ‘ ‘
38-40	3	State or Country Code	If Card Acceptor is in the USA or Canada, this contains a 2 character US state or Canadian Province code then a space. Otherwise, this contains a ISO 3-alpha upper case country code.

Examples

Below are examples of the type of data that can arrive in Merch_Name_DE43 in authorisation messages:

Authorisation Message Merch_Name_DE43 value	Things to note
PAYPAL *YIWUYUYICHE 35314369001 GBR	Normal country code
ROBLOX CORPORATION 888-858-2569 CA	Last 3 characters are a 2-letter US state code, followed by a space e.g. TX = Texas, NY = New York etc.
3600 LAS VEGAS BLVD SO LAS VEGAS NV	Last 3 characters are a space, followed by a 2-letter US state code e.g. TX = Texas, NY = New York etc.
NOOR DUBAI MALL BRANCH BAI AE ARE	Emirate within UAE e.g. Dubai/DXB, Abu Dhabi/AUH, Ras Al Khaimah/RAK etc.
GOOGLE *FiLMiC Inc g.co/payhelp# GBR	URL in city field
MICROSOFT *XBOX BILL.XBOX.COM IRL	Website hostname in city field

4.17.2 VISA Authorisation

The merchant name/location field for Visa is made up of various subfields.

Positions	Length	Field Name	Description / Valid Values
1-25	25	Card Acceptor Name	Name of Card Acceptor or ATM service provider. (Space padded on the right to make up to 25 characters.)
26-38	23	City Name	POS: City where the customer transaction occurs.

Positions	Length	Field Name	Description / Valid Values
			Card-Not-Present Transactions: Instead of the city name, these positions must contain the merchant's customer service telephone number. ATM: City where the ATM is located. The institution name is in field 42.
39-40	2	Country Code	The 2-character alpha code in uppercase format for the country where the cardholder transaction occurs or the ATM is located.

4.18 Merch_Name_DE43 in Financial Messages

The Merch_Name_DE43 field is made up the subfields described below. (See also Get Transaction Message fields: Merch_Name_DE43)

4.18.1 Mastercard Merch_Name_DE43 (Financial) Format

Most fields are variable in length, separated by a backslash '\' character.

Length	Field Name	Description / Valid Values
0-100	Card Acceptor Name	Name of Card Acceptor or ATM service provider. May contain special characters.
1	Separator	Backslash '\' character
0-100	Card Acceptor Street Address	Card Acceptor/ATM street address. May contain special characters.
1	Separator	Backslash '\' character
0-100	Card Acceptor City	Card Acceptor or ATM city. For cardholder not present transactions, this may contain a URL or phone number of customer support. May contain special characters.
1	Separator	Backslash '\' character
10	Postal Code	May contain nothing or special characters (e.g. Polish postcodes contain '-')
3	Region Code	If the country is USA, this is the US state code. If the country is CAN, this is the Canadian province code. If the country has regions or provinces, it may contain the region or province code. If not applicable, may be blank or contain the 3-alpha country code of the merchant.
3	Country Code	ISO 3-alpha country code of the merchant or ATM.

4.18.2 VISA Merch_Name_DE43 (Financial) Format

Positions	Length	Field Name	Description / Valid Values
1-25	25	Card Acceptor Name	Name of Card Acceptor or ATM service provider. (Space padded on the right to make up to 25 characters.)
26-38	23	City Name	POS: City where the customer transaction occurs. Card-Not-Present Transactions: Instead of the city name, these positions must contain the merchant's customer service telephone number. ATM: City where the ATM is located. The institution name is in field Merch_ID_DE42.
39-40	2	Country Code	The 2-character alpha code in uppercase format for the country where the cardholder transaction occurs or the ATM is located.

4.18.3 Merch_Name_DE43 (Financial) Examples

Examples of Merch_Name_DE43 in financial type messages:

Financial Message Merch_Name_DE43 value	Notes
MARTIN MCCOLL\152 HUNTSPOND ROAD\FAREHAM\PO14 4PL GBRGBR	Normal. Country in region field.
IMPERIAL CHINA \25A LISLE STREET \LONDON WC2H \WC2H 7BA GBR	Blank region field
MECK \Stora Varvsgatan 6A \Malmo \21119 SWESWE	Numbers-only postcode
VUE BSL LTD\3 CRANBOURN STREET\WEST END\WC2H 7AL GBRGBR	
THE CHIC PEA\4545 BLACKCOMB WAY\WHISTLER\V0N1B4 BC CAN	'BC ' 6th to 4th last characters are the Canadian province code
USCUSTOMS ESTA APPL PM\6650 TELECOM DR STE 100\317-617-4458\46278 IN USA	'IN ' 6th to 4th last characters are the US state code
CCSF MTA IPS PRKNG MET\1 S VAN NESS AVE FL 8 \SAN FRANCISCO\94103 CA USA	'CA ' 6th to 4th last characters are the US state code
LINODE.COM\329 E. Jimmie Leeds Road\855-4546633\08205 NJ USA	Notice phone number in the City field
BADAVI SL 60508603\CL CARACAS 50 A\BARCELONA\08030 080ESP	Notice '080' in region field
LA BANQUE POSTAL\\VAL D ISERE\7315000000FR FRA	Notice no street address. 73150 is the postcode.
STARBUCKS CC 4461 \\DUBAI \ ARE	Notice no street address or postcode
Eymundsson Leifsstod \Grensásvegi 11 \REYKJAVÍK \108 ISLISL	Notice accented characters present in both street address and city
Uber BV\Hamminkweg 5\help.uber.com\7251B NLDNLD	Notice URL in city field
*BNP\14 RUE AUBER\PARIS 15\75000 FRAFRA	Notice asterik as first character in name field.
CHEFETTE RESTAURANT-BL\CHEFETTE RESTAURANT-BLACST MICHAEL BB\ST. MICHAEL\BB23027 BRB	
KEYCDN CREDITS \Room 424, 7 Gra\41445853152 \3011 CHECHE	Notice street address.
APOTEKET SERGEL \SERGELGÅNGEN 14 \STOCKHOLM \111 57 SWESWE	Special character in street address.
Vikurskali/Strondin\Sigtuni 5\Vik\870 ISLISL	Notice '/' in name field
mytaxi.com\C/ Diputacio 39, Local B1\taxi tour\8015 ESP	Notice '/' in street address field (Abbreviation of 'Calle' which means Street in Spanish
Amazon UK Marketplace\5 rue plaetis\800-279-6620\L2338 LUXLUX	Notice telephone number and '-' in city field

Financial Message Merch_Name_DE43 value	Notes
MICROSOFT *XBOX \-- \01157761000 \89119 NV USA	Notice '-' signs in street address and '*' in name field
BANQUE RHONES AL\\BARALP L' ALP\3875000000FR FRA	Notice apostrophe in city name
ROAD TRANSPORT AUTH\RTA-DUBAI METRO-TVM DUBAI AE\DUBAI\0000000784UAEARE	Notice all postcode characters used
WWW.REMIXSHOP.COM \ST.L.KOSTOV3\SOFIA \1407 BGRBGR	
CONVERSE # 39\8166 VINELAND AVE #1725\ORLANDO\32821 FL USA	
ANUDAN HOLDINGS (PVT)\ANUDAN HOLDINGS (PVT) LTD\HIKKADUWA\UNKNOWN LKA	
CT TNHH IHOME TEAM\31 E2 BIET THU TAN LAP NT KH\KHANH HOA\650000 VNM	
L'ESCORCHEVEL \LE PRAZ \SAINT BON TAR\73120 FRAFRA	
HUMBLEBUNDLE.COM HUMBL\201 POST ST FL 11 \8778877815 \94108 CA USA	
ADO TERMINAL TULUM\AV TULUM NO 9 ENTRE\SOLIDARIDAD Q\77780 QR MEX	Notice region code present for non-US and non-Canada country
"TAVRIA-V"\"TAVRIA-V"\NIKOLAEV\54056 UKR	Notice double quote characters in name and street
"BGEU" BR.519 ATM \PR.PARTIZANSKIY,26A\MINSK \220070 BLRBLR	Notice double quote characters in name
(BK-R1) BK- T1 #021-53\101 THOMSON RD\SINGAPORE\307591 SGPSGP	Notice '(', ')', '-', '#' characters in name.
#5 LUCILLE'S SMOKE\6257 E. 2ND ST\LONG BEACH\90803 CA USA	Notice apostrophe and '#' characters in name.
*BARCLAYS/GWERU*BARCLAYS/GWERU\GWERU\UNKNOWN ZWEZWE	Notice '*' '/' in both name and street
*DEUTSCHE BANK AG \\F-FLUGHAF. \60486 DEUDEU	
00/HBCG-AERO-PODGORICA\00/HBCG-AERO-PODGORICA\PODGORICA\81000 499MNE	
+CHURCHGATE RAI\+CHURCHGATE RAILWAY ST\M M\400020 INDIND	
000000003006002\LAOS DEVELOPMENT BANK\03006002\UNKNOWN LAOLAO	
000000017200001\000000017200001 TSCN,\Bac Kan\UNKNOWN VNMVNM	
000000074200002\000000074200002 Toa an\Chau Doc\UNKNOWN VNMVNM	
000000099999999\91Tran H Dao Tx Hoi An\Da Nang\UNKNOWN VNMVNM	
013109669990000\Line2,kejiguan\Shanghai\UNKNOWN CHNCHN	
018 STARBUCKS PTY\219/3Y YAMAMOTO 13/1 SOI.BEACH\CHONBURI\20150 THATHA	
02010002\(02010002),Yuri Meiko\inYangon\UNKNOWN MMRMMR	

Financial Message Merch_Name_DE43 value	Notes
2BuySafe.com/ MCCOYS\Kirchstrasse 6\.\9494 LIELIE	Notice '.' Is the city
589359000000000\AV0POTOSI0SN0000000000\00POTOSI0000\UNKNOWN BOLBOL	
99BILL*JUNEYAOAIR.\SHANGHAI PU DONG PU DIAN LU 360 HAO 12 L\SHANGHAI\200122 SHACHN	
WOOLWORTHS V A WRON\\CAPE TOWN\8000 ZA ZAF	No street
TRAVELEX LHR T5 BA (1)\\London\AB21 0DU GBRGBR	Postcode is not valid and does not correspond to city
Piraeus Bank,S/M MASOU\\Thessaloniki\ GRCGRC	
HSBC CASH MACHINE\\TILEHURST\ GBRGBR	No street, description in name
HOUSE BOUTIQUE \\PHNOM PENH \ KHM	No street
Goldman Sachs\\London\EC4A 2BB GBRGBR	No street
BOI ATM\\TRINITY \00000 IRLIRL	Dummy postcode (probably)
Twoj Market\ul.Pelplinska 41\Bydgoszcz\85-794 POLPOL	'-' in postcode field.
ASDA GEORGE COM LEEDS\LEEDS\GB	
WWW.ALZA.CZ\PRAHA 7\CZ SYMBAL.BY\PAVEL.BELAVUS\BY	
WWW.ALZA.SK\PRAHA 7\CZ	
mall.hu\Budapest\HU	
RYANAIR 22400000MUYY2\LONDON\GB	
WWW.ALZA.CZ\PRAHA 7\CZ	

4.19 Merchant Category Codes

The table below lists the valid values for the MCC_Code field, identifying the merchant category code. (See also Get Transaction Message fields:MCC_Code)

MCC Lower	MCC Upper	MCC Category Description
742	742	Veterinary Services
763	763	AGRICULTURAL COOPERATIVES
780	780	LANDSCAPE AND HORTICULTURAL SERVICES
1520	1520	General Contractors
1711	1711	Heating, Plumbing, A/C
1731	1731	Electrical Contractors
1740	1740	Masonry, Stonework, and Plaster
1750	1750	Carpentry Contractors
1761	1761	Roofing/Siding, Sheet Metal
1771	1771	Concrete Work Contractors
1799	1799	Special Trade Contractors
2741	2741	Miscellaneous Publishing and Printing
2791	2791	Typesetting, Plate Making, and Related Services
2842	2842	Specialty Cleaning
3000	3299	Airlines
3001	3001	AMERICAN AIRLINES
3004	3004	DRAGONAIR
3005	3005	BRITISH AIRWAYS
3006	3006	JAPAN AIRLINES
3007	3007	AIR FRANCE
3008	3008	LUFTHANSA
3009	3009	AIR CANADA
3010	3010	KLM (ROYAL DUTCH AIRLINES)
3011	3011	AEROFLOT
3012	3012	QANTAS

MCC Lower	MCC Upper	MCC Category Description
3013	3013	ALITALIA
3014	3014	SAUDI ARABIAN AIRLINES
3015	3015	SWISS INTERNATIONAL AIRLINES - SWISS AIR
3016	3016	SAS
3017	3017	SOUTH AFRICAN AIRWAYS
3018	3018	VARIG AIR (BRAZIL)
3019	3019	Eastern Airline
3020	3020	AIR INDIA
3021	3021	AIR ALGERIE
3022	3022	PAL AIR
3024	3024	PAKISTAN INTERNATIONAL
3025	3025	AIR NEW ZEALAND
3026	3026	EMIRATES AIRLINES
3027	3027	UTA/INTERAIR
3028	3028	AIR MALTA
3029	3029	SN BRUSSELS AIRLINES - SNBRU AIR
3030	3030	AEROLINEAS ARGENTINAS
3031	3031	OLYMPIC AIRWAYS
3032	3032	EL AL
3033	3033	ANSETT AIRLINES
3034	3034	TRANS AUSTRAILIAN AIRWAYS (TAA)
3035	3035	TAP (PORTUGAL)
3037	3037	EGYPTAIR
3038	3038	KUWAIT AIRWAYS
3039	3039	AVIANCA
3040	3040	GULF AIR (BAHRAIN)
3042	3042	FINNAIR
3043	3043	AER LINGUS

MCC Lower	MCC Upper	MCC Category Description
3044	3044	AIR LANKA
3047	3047	THY (TURKEY)
3048	3048	AIRMARO
3049	3049	TUNIS AIR
3050	3050	ICELANDAIR
3051	3051	AUSTRIAN AIRLINES
3052	3052	LAN AIRLINES-LANAIR
3056	3056	QUEBECAIRE
3057	3057	EAST/WEST AIRLINES (AUSTRALIA)
3058	3058	DELTA
3063	3063	U.S. AIR
3064	3064	ADRIA AIRWAYS
3065	3065	AIRINTER
3066	3066	SOUTHWEST
3068	3068	AIR ASTANA
3069	3069	Sun Country Airlines
3070	3070	Fly Dubai
3072	3072	CEBU PAC
3075	3075	SINGAPORE AIRLINES
3076	3076	AEROMEXICO
3077	3077	THAI AIRWAYS
3078	3078	CHINA AIRLINES
3079	3079	JETSTAR AIRLINES
3080	3080	Airline Swoop Inc
3081	3081	Xiamen Airlines
3082	3082	KOREAN AIRLINES
3084	3084	EVA AIRWAYS
3088	3088	CROATIA AIRLINES

MCC Lower	MCC Upper	MCC Category Description
3089	3089	TRANSAERO
3096	3096	AIR ZIMBABWE
3098	3098	ASIANNA AIRLINES - ASIANNA
3099	3099	CATHAY PACIFIC
3100	3100	MALAYSIAN AIRLINE SYSTEM
3102	3102	IBERIA
3103	3103	GARUDA (INDONESIA)
3111	3111	BRITISH MIDLAND
3112	3112	WINDWARD ISLAND
3125	3125	TAN
3127	3127	TACA INTERNATIONAL
3129	3129	SURINAM AIRWAYS
3132	3132	FRONTIER AIRLINES
3136	3136	QATAR AIRWAYS
3144	3144	VIRGIN ATLANTIC
3146	3146	LUXAIR
3161	3161	ALL NIPON AIRWAYS
3168	3168	Hainan Airlines
3169	3169	RIYADH AIR
3174	3174	JETBLUE AIRLINES
3175	3175	MIDDLE EAST AIR
3177	3177	AIRTRAN AIRWAYS
3178	3178	MESA AIR
3180	3180	WESTJETAIR
3182	3182	LOT (POLAND)
3183	3183	OMANAIR
3184	3184	LIAT

MCC Lower	MCC Upper	MCC Category Description
3190	3190	JUGOSLAV AIR
3191	3191	ISLAND AIRLINES
3196	3196	HAWAIIAN AIR
3206	3206	CHINA EASTERN AIRLINES
3211	3211	NORWEGIAN AIR SHUTTLE
3217	3217	CSA
3219	3219	COPA
3223	3223	COMAIR
3228	3228	CAYMAN AIRWAYS
3234	3234	CARIBBEAN AIRLINES
3236	3236	AIR ARABIA
3240	3240	BAHAMASAIR
3245	3245	EASYJET AIR
3246	3246	RYANAIR
3247	3835	3247-3835
3248	3248	TAM AIR
3256	3256	ALASKA AIRLINES
3260	3260	SPIRIT AIRLINES
3261	3261	AIR CHINA
3267	3267	AIR PANAMA
3292	3292	CYPRUS AIRWAYS
3294	3294	ETHIOPIAN AIRLINES
3295	3295	KENYA AIRWAYS
3296	3296	AIR BERLIN
3297	3297	TAROM
3298	3298	AIR MAURITIUS
3299	3299	WIDEROE'S FLYVESELSKAP
3303	3303	Tigerair

MCC Lower	MCC Upper	MCC Category Description
3304	3304	Air Baltic
3305	3305	Air Transat
3308	3308	China Southern
3351	3441	Car Rental
3351	3441	Car Rental Agencies 2
3355	3355	SIXT CAR RENTAL
3357	3357	HERTZ RENT-A-CAR
3359	3359	PAYLESS CAR RENTAL
3364	3364	AGENCY RENT-A-CAR
3366	3366	BUDGET RENT-A-CAR
3368	3368	HOLIDAY RENT-A-CAR
3381	3381	EUROP CAR
3387	3387	ALAMO RENT-A-CAR
3389	3389	AVIS RENT-A-CAR
3390	3390	DOLLAR RENT-A-CAR
3393	3393	NATIONAL CAR RENTAL
3395	3395	THRIFTY RENT-A-CAR
3400	3400	AUTO HOST CAR RENTALS
3405	3405	ENTERPRISE RENT-A-CAR
3409	3409	GENERAL RENT-A-CAR
3412	3412	A-1 RENT-A-CAR
3420	3420	ANSA INTL RENT-A-CAR
3427	3427	AVON RENT-A-CAR
3437	3437	CITE RENT-A-CAR
3438	3438	INTERENT RENT-A-CAR
3441	3441	ADVANTAGE RENT-A-CAR
3501	3790	Hotels/Motels/Inns/Resorts

MCC Lower	MCC Upper	MCC Category Description
3501	3835	3501-3835
3502	3502	BEST WESTERN HOTELS
3503	3503	SHERATON HOTELS
3504	3504	HILTON HOTELS
3505	3505	FORTE HOTELS
3506	3506	GOLDEN TULIP HOTELS
3507	3507	FRIENDSHIP INNS
3508	3508	QUALITY INNS & QUALITY SUITES
3509	3509	MARRIOTT HOTELS
3510	3510	DAYS INNS OR DAYSTOP
3511	3511	ARABELLA HOTELS
3512	3512	INTER-CONTINENTAL HOTELS
3513	3513	WESTIN HOTELS
3514	3514	AMERISUITES
3515	3515	RODEWAY INNS
3516	3516	LA QUINTA MOTOR INNS
3519	3519	PULLMAN INTERNATIONAL HOTELS
3520	3520	MERIDIEN HOTELS
3521	3521	ROYAL LAHAINA RESORTS
3523	3523	PENINSULA HOTEL
3526	3526	PRINCE HOTELS
3528	3528	RED LION HOTELS OR RED LION INNS
3530	3530	RENAISSANCE HOTELS
3533	3533	HOTEL IBIS
3535	3535	HILTON INTERNATIONAL
3536	3536	AMFAC HOTELS
3537	3537	ANA HOTEL
3538	3538	CONCORDE HOTELS

MCC Lower	MCC Upper	MCC Category Description
3539	3539	SUMMERFIELD SUITES HOTEL
3540	3540	IBEROTEL HOTELS
3541	3541	HOTEL OKURA
3542	3542	ROYAL HOTELS
3543	3543	FOUR SEASONS HOTELS
3545	3545	SHANGRI-LA INTERNATIONAL
3548	3548	HOTELS MELIA
3549	3549	AUBERGE DES GOVERNEURS
3551	3551	MIRAGE HOTEL AND CASINO
3552	3552	COAST HOTELS
3553	3553	PARK INNS INTERNATIONAL
3555	3555	TREASURE ISLAND HOTEL AND CASINO
3558	3558	JOLLY HOTELS
3559	3559	CANDLEWOOD SUITES - THISTLE HOTELS
3560	3560	DISALLOWED - Aladdin Resort and Casino
3561	3561	GOLDEN NUGGET
3562	3562	COMFORT INNS
3567	3567	SOHO GRAND HOTEL
3570	3570	FORUM HOTELS
3572	3572	MIYAKO HOTELS
3573	3573	SANDMAN HOTELS
3575	3575	VAGABOND HOTELS
3577	3577	MANDARIN ORIENTAL HOTEL
3579	3579	HOTEL MERCURE
3581	3581	DELTA HOTEL
3583	3583	SAS HOTELS
3586	3586	SOKOS HOTELS
3590	3590	FAIRMONT HOTELS

MCC Lower	MCC Upper	MCC Category Description
3591	3591	SONESTA HOTELS
3592	3592	OMNI HOTELS
3595	3595	HOSPITALITY INNS
3596	3596	WYNN LAS VEGAS
3597	3597	DISALLOWED - Riverside Resort and Casino
3598	3598	REGENT INTERNATIONAL HOTELS
3602	3602	HUDSON HOTEL
3604	3604	HILTON GARDEN RESORT/INN
3607	3607	FONTAINEBLEAU RESORTS
3608	3608	GAYLORD OPRYLAND
3612	3612	MOVENPICK HOTELS
3613	3613	MICROTEL INN AND SUITES
3615	3615	TRAVELODGE
3617	3617	AMERICAS BEST VALUE INN
3618	3618	GREAT WOLF
3619	3619	ALOFT
3621	3621	EXTENDED STAY
3623	3623	DORINT HOTELS
3625	3625	HOTEL UNIVERSALE
3628	3628	EXCALIBUR HOTEL AND CASINO
3629	3629	DAN HOTELS
3630	3630	Tokyu Hotels
3631	3631	SLEEP INNS
3632	3632	PHOENICIAN
3634	3634	SWISSOTEL
3635	3635	RESO HOTELS
3636	3636	SAROVA HOTELS
3637	3637	RAMADA INNS & RAMADA LIMITED

MCC Lower	MCC Upper	MCC Category Description
3638	3638	HOWARD JOHNSON
3639	3639	MOUNT CHARLOTTE THISTLE
3640	3640	HYATT HOTELS
3641	3641	SOFITEL HOTELS
3642	3642	NOVOTEL HOTELS
3643	3643	STEIGENBERGER HOTELS
3644	3644	ECONO LODGES
3645	3645	QUEENS MOAT HOUSES
3647	3647	HUSA HOTELS
3648	3648	DE VERE HOTELS
3649	3649	RADISSON HOTELS
3650	3650	RED ROOF INNS
3651	3651	IMPERIAL LONDON HOTEL
3652	3652	EMBASSY HOTELS
3653	3653	PENTA HOTELS
3654	3654	LOEWS HOTELS
3655	3655	SCANDIC HOTELS
3657	3657	OBEROI HOTELS
3659	3659	TAJ HOTELS INTERNATIONAL
3660	3660	KNIGHTS INNS
3661	3661	METROPOLE HOTELS
3662	3662	CIRCUS CIRCUS HOTEL AND CASINO
3663	3663	HOTELES EL PRESIDENTE
3665	3665	HAMPTON INNS
3667	3667	LUXHOR HOTEL AND CASINO
3668	3668	MARITIM HOTELS
3670	3670	ARCADE HOTELS
3672	3672	CAMPANILE HOTELS

MCC Lower	MCC Upper	MCC Category Description
3674	3674	RANTASIPI HOTELS
3676	3676	MONTE CARLO HOTEL AND CASINO
3677	3677	CLIMAT DE FRANCE HOTELS
3678	3678	CUMULUS HOTELS
3680	3680	HOTEIS OTHAN
3681	3681	ADAMS MARK HOTELS
3684	3684	BUDGET HOST INNS
3687	3687	CLARION HOTELS
3689	3689	CONSORT HOTELS
3690	3690	COURTYARD BY MARRIOTT
3692	3692	DOUBLTREE HOTELS
3693	3693	DRURY INNS
3694	3694	ECONOMY INNS OF AMERICA
3695	3695	EMBASSY SUITES
3698	3698	HARLEY HOTELS
3699	3699	MIDWAY MOTOR LODGE
3700	3700	MOTEL 6
3703	3703	RESIDENCE INNS
3706	3706	SHILO INNS
3709	3709	SUPER 8 MOTELS
3710	3710	THE RITZ CARLTON HOTELS
3715	3715	FAIRFIELD INN
3716	3716	CARLTON HOTELS
3717	3717	CITY LODGE HOTELS
3719	3719	PROTEA HOTELS
3721	3721	HILTON CONRAD
3722	3722	WYNDHAM HOTEL & RESORTS
3723	3723	RICA HOTELS

MCC Lower	MCC Upper	MCC Category Description
3728	3728	BALLY'S HOTEL AND CASINO
3730	3730	MGM GRAND HOTEL
3731	3731	HARRAH'S HOTELS AND CASINOS
3732	3732	OPRYLAND HOTEL
3733	3733	Boca Raton Resort
3736	3736	Colorado Belle Edgewater Resort
3737	3737	Riviera Hotel and Casino
3738	3738	Tropicana Resort and Casino
3739	3739	Woodside Hotels and Resorts
3740	3740	MARRIOTT/TOWNPLACE SUITES
3741	3741	MILLENNIUM HOTELS
3745	3745	ST. REGIS HOTEL
3750	3750	CROWNE PLAZA HOTEL
3751	3751	HOMEWOOD SUITES
3752	3752	PEABODY HOTELS
3754	3754	AMELIA ISLAND PLANTATION
3756	3756	Tokyo Inn
3765	3765	BELLAGIO
3769	3769	DISALLOWED - Stratosphere Hotel and Casino
3770	3770	SPRINGHILL SUITES
3771	3771	DISALLOWED - Ceasers Hotel and Casino
3772	3772	NEMACOLIN WOODLANDS
3773	3773	DISALLOWED - Venetian Resort, Hotel and Casino
3774	3774	DISALLOWED - New York - New York Hotel and Casino
3775	3775	SANDS RESORT
3777	3777	MANDALAY BAY RESORT
3778	3778	FOUR POINTS HOTELS
3779	3779	W HOTELS

MCC Lower	MCC Upper	MCC Category Description
3780	3780	DISNEY RESORTS
3782	3782	ROSEN HOTELS & RESORTS
3783	3783	TOWN AND COUNTRY RESORT
3784	3784	FIRST HOSPITALITY HOTELS
3785	3785	OUTRIGGER HOTELS AND RESORTS
3786	3786	OHANA HOTELS OF HAWAII
3790	3790	RAFFLES HOTEL
3791	3791	Staybridge Suites
3792	3792	Claridge Casino Hotel
3793	3793	Flamingo Hotels
3794	3794	Grand Casino Hotels
3795	3795	Paris Las Vegas Hotel
3796	3796	Peppermill Hotel Casino
3797	3797	Atlantic City Hilton Resorts
3798	3798	Embassy Vacation Resort
3799	3799	Hale Koa Hotel
3801	3801	WILDERNESS HOTEL AND RESORT
3802	3802	THE PALACE HOTEL
3808	3808	LXR (LUXURY RESORTS)
3811	3811	PREMIER TRAVEL INN
3812	3812	HYATT PLACE
3813	3813	HOTEL INDIGO
3814	3814	THE ROOSEVELT HOTEL NY
3819	3819	OXFORD SUITES
3822	3822	CROSSLAND
3839	3839	Kyoritsu Hotels
3840	3840	Rio hotels
3841	3841	Tribute Portfolio

MCC Lower	MCC Upper	MCC Category Description
3842	3842	Marriott Executive Apartments
3843	3843	Moxy
3844	3844	AC Hotels
3845	3845	Bulgari
3846	3846	The Luxury Collection
3847	3847	JW Marriott
3848	3848	Edition
3849	3849	Minacia
3850	3850	Breezbay Group
3851	3851	Candeo Hotels
3852	3852	Core Global Management Hotels and Resorts
3853	3853	Granbell Hotels and Resorts
3854	3854	JHAT
3855	3855	C'est la vie Resort Izumigo
3856	3856	Banyan Tree Hotels and Resorts
3857	3857	Hotel Sunroute
3858	3858	Sotetsu Fresa-Inn
3859	3859	La Vista
3860	3860	JR-East Hotel Mets
3861	3861	AB Hotel
3862	3862	Chisun Hotels
3863	3863	Super Hotel
3864	3864	Itoen Hotel
3865	3865	Quintessa Hotel
3866	3866	Smile Hotel
3867	3867	Hotel Alpha-1
3868	3868	Relo Vacations

MCC Lower	MCC Upper	MCC Category Description
3869	3869	Yutorelo
3870	3870	Keio Presso inn
3871	3871	Villa-Fontaine
3872	3872	Meitetsu Inn
3873	3873	Tokyo Harvestclub
3874	3874	Hotel Livemax
3875	3875	Fufu Japan
3876	3876	HMI Hotel Group
3877	3877	Orix Hotels and Resorts
3878	3878	Washington Hotel
3979	3979	Sanco Inn
3880	3880	Hotel Unizo
3881	3881	Hotel Metropolitan
3882	3882	Centurion Hotels
3883	3883	Nest Hotel
4011	4011	Railroads
4111	4111	Commuter Transport, Ferries
4112	4112	Passenger Railways
4119	4119	Ambulance Services
4121	4121	Taxicabs/Limousines
4131	4131	Bus Lines
4214	4214	Motor Freight Carriers and Trucking - Local and Long Distance, Moving and Storage Companies, and Local Delivery Services
4215	4215	Courier Services
4225	4225	Public Warehousing and Storage - Farm Products, Refrigerated Goods, Household Goods, and Storage
4411	4411	Cruise Lines
4457	4457	Boat Rentals and Leases
4468	4468	Marinas, Service and Supplies

MCC Lower	MCC Upper	MCC Category Description
4511	4511	Airlines, Air Carriers
4582	4582	Airports, Flying Fields
4722	4722	Travel Agencies, Tour Operators
4723	4723	TUI Travel - Germany
4761	4761	TRANSPORTATION/TRAVEL-RELATED ARRANGEMENT
4784	4784	Tolls/Bridge Fees
4789	4789	Transportation Services (Not Elsewhere Classified)
4812	4812	Telecommunication Equipment and Telephone Sales
4813	4813	Special Telecom Merchants
4814	4814	Telecommunication Services
4816	4816	Computer Network Services
4821	4821	Telegraph Services
4829	4829	Money Transfer, Money Orders - Merchant
4899	4899	Cable, Satellite, and Other Pay Television and Radio
4900	4900	Utilities
5013	5013	Motor Vehicle Supplies and New Parts
5021	5021	Office and Commercial Furniture
5039	5039	Construction Materials (Not Elsewhere Classified)
5044	5044	Photographic, Photocopy, Microfilm Equipment, and Supplies
5045	5045	Computers, Peripherals, and Software
5046	5046	Commercial Equipment (Not Elsewhere Classified)
5047	5047	Medical, Dental, Ophthalmic, and Hospital Equipment and Supplies
5051	5051	Metal Service Centers
5065	5065	Electrical Parts and Equipment
5072	5072	Hardware, Equipment, and Supplies
5074	5074	Plumbing, Heating Equipment, and Supplies
5085	5085	Industrial Supplies (Not Elsewhere Classified)
5094	5094	Precious Stones and Metals, Watches and Jewelry

MCC Lower	MCC Upper	MCC Category Description
5099	5099	Durable Goods (Not Elsewhere Classified)
5111	5111	Stationary, Office Supplies, Printing and Writing Paper
5122	5122	Drugs, Drug Proprietaries, and Druggist Sundries
5131	5131	Piece Goods, Notions, and Other Dry Goods
5137	5137	Uniforms, Commercial Clothing
5139	5139	Commercial Footwear
5169	5169	Chemicals and Allied Products (Not Elsewhere Classified)
5172	5172	Petroleum and Petroleum Products
5192	5192	Books, Periodicals, and Newspapers
5193	5193	Florists Supplies, Nursery Stock, and Flowers
5198	5198	Paints, Varnishes, and Supplies
5199	5199	Nondurable Goods (Not Elsewhere Classified)
5200	5200	Home Supply Warehouse Stores
5211	5211	Lumber, Building Materials Stores
5231	5231	Glass, Paint, and Wallpaper Stores
5251	5251	Hardware Stores
5261	5261	Nurseries, Lawn and Garden Supply Stores
5262	5262	Marketplaces
5271	5271	Mobile Home Dealers
5300	5300	Wholesale Clubs
5309	5309	Duty Free Stores
5310	5310	Discount Stores
5311	5311	Department Stores
5331	5331	Variety Stores
5382	5382	Antique Shops - Sales, Repairs, and Restoration Services
5399	5399	Miscellaneous General Merchandise
5411	5411	Grocery Stores, Supermarkets
5422	5422	Freezer and Locker Meat Provisioners

MCC Lower	MCC Upper	MCC Category Description
5441	5441	Candy, Nut, and Confectionery Stores
5451	5451	Dairy Products Stores
5462	5462	Bakeries
5499	5499	Miscellaneous Food Stores - Convenience Stores and Specialty Markets
5511	5511	Car and Truck Dealers (New & Used) Sales, Service, Repairs Parts and Leasing
5521	5521	Car and Truck Dealers (Used Only) Sales, Service, Repairs Parts and Leasing
5531	5531	Auto and Home Supply Stores
5532	5532	Automotive Tire Stores
5533	5533	Automotive Parts and Accessories Stores
5541	5541	Service Stations
5542	5542	Automated Fuel Dispensers
5551	5551	Boat Dealers
5561	5561	Motorcycle Shops, Dealers
5571	5571	Motorcycle Shops and Dealers
5592	5592	Motor Homes Dealers
5598	5598	Snowmobile Dealers
5599	5599	Miscellaneous Auto Dealers
5611	5611	Men’s and Boy’s Clothing and Accessories Stores
5621	5621	Women’s Ready-To-Wear Stores
5631	5631	Women’s Accessory and Specialty Shops
5641	5641	Children’s and Infant’s Wear Stores
5651	5651	Family Clothing Stores
5655	5655	Sports and Riding Apparel Stores
5661	5661	Shoe Stores
5681	5681	Furriers and Fur Shops
5691	5691	Men’s, Women’s Clothing Stores
5697	5697	Tailors, Alterations
5698	5698	Wig and Toupee Stores

MCC Lower	MCC Upper	MCC Category Description
5699	5699	Miscellaneous Apparel and Accessory Shops
5712	5712	Furniture, Home Furnishings, and Equipment Stores, Except Appliances
5713	5713	Floor Covering Stores
5714	5714	Drapery, Window Covering, and Upholstery Stores
5718	5718	Fireplace, Fireplace Screens, and Accessories Stores
5719	5719	Miscellaneous Home Furnishing Specialty Stores
5722	5722	Household Appliance Stores
5723	5723	Gun and Ammunition Store
5732	5732	Electronics Stores
5733	5733	Music Stores-Musical Instruments, Pianos, and Sheet Music
5734	5734	Computer Software Stores
5735	5735	Record Stores
5811	5811	Caterers
5812	5812	Eating Places, Restaurants
5813	5813	Drinking Places
5814	5814	Fast Food Restaurants
5815	5815	Digital Goods - Audiovisual Medai
5816	5816	Digital Goods - Games
5817	5817	Digital Goods - Software
5818	5818	Digital Goods - Multi Categorry
5912	5912	Drug Stores and Pharmacies
5921	5921	Package Stores-Beer, Wine, and Liquor
5931	5931	Used Merchandise and Secondhand Stores
5932	5932	Antique Shops
5933	5933	Pawn Shops
5935	5935	Wrecking and Salvage Yards
5937	5937	Antique Reproductions
5940	5940	Bicycle Shops

MCC Lower	MCC Upper	MCC Category Description
5941	5941	Sporting Goods Stores
5942	5942	Book Stores
5943	5943	Stationery Stores, Office, and School Supply Stores
5943	5968	5943-5968
5944	5944	Jewelry Stores, Watches, Clocks, and Silverware Stores
5945	5945	Hobby, Toy, and Game Shops
5946	5946	Camera and Photographic Supply Stores
5947	5947	Gift, Card, Novelty, and Souvenir Shops
5948	5948	Luggage and Leather Goods Stores
5949	5949	Sewing, Needlework, Fabric, and Piece Goods Stores
5950	5950	Glassware, Crystal Stores
5960	5960	Direct Marketing - Insurance Services
5961	5961	MAIL ORDER HOUSES INCL CATALOG ORDER STORES BOOK/RECORD CLUB
5962	5962	Direct Marketing - Travel
5963	5963	Door-To-Door Sales
5964	5964	Direct Marketing - Catalog Merchant
5965	5965	Direct Marketing - Combination Catalog and Retail Merchant
5966	5966	Direct Marketing - Outbound Tele
5967	5967	Direct Marketing - Inbound Tele
5968	5968	Direct Marketing - Subscription
5969	5969	Direct Marketing - Other
5970	5970	Artist’s Supply and Craft Shops
5971	5971	Art Dealers and Galleries
5972	5972	Stamp and Coin Stores
5973	5973	Religious Goods Stores
5975	5975	Hearing Aids Sales and Supplies
5976	5976	Orthopedic Goods - Prosthetic Devices
5977	5977	Cosmetic Stores

MCC Lower	MCC Upper	MCC Category Description
5978	5978	Typewriter Stores
5983	5983	Fuel Dealers (Non Automotive)
5992	5992	Florists
5993	5993	Cigar Stores and Stands
5994	5994	News Dealers and Newsstands
5995	5995	Pet Shops, Pet Food, and Supplies
5996	5996	Swimming Pools Sales
5997	5997	Electric Razor Stores
5998	5998	Tent and Awning Shops
5999	5999	Miscellaneous Specialty Retail
6010	6010	Financial Institutions - Manual Cash Disbursements
6011	6011	Automated Cash Disburse
6012	6012	Financial Institutions - Merchandise and Services
6050	6050	Quasi Cash, Money Orders - Member Financial Institution
6051	6051	Quasi Cash, Money Orders - Non-Financial institution
6211	6211	Security Brokers/Dealers
6300	6300	Insurance Underwriting, Premiums
6381	6381	Insurance Premiums
6399	6399	Insurance - Default
6513	6513	Real Estate Agents and Managers - Rentals
6529	6529	Remote Stored Value Load--MemberFinancial Inst
6530	6530	Remote Stored Value Load--Merchant
6531	6531	Payment Service Provider - MoneyTransfer For A Purchase
6532	6532	Payment Service Provider - MemberFinancial Inst. - Pymt Trans.
6533	6533	Payment Service Provider - Merchant - Payment Transaction
6534	6534	Money Transfer - Member FinancialInstitution
6535	6535	Value Purchase-Member Financial Institution
6538	6538	MASTERCARD MONEYSEND FUNDING TRANSACTION

MCC Lower	MCC Upper	MCC Category Description
6540	6540	POI Funding Transactions (Excluding Mastercard MoneySend)
6760	6760	Savings Bonds
7011	7011	Hotels, Motels, and Resorts
7012	7012	Timeshares
7032	7032	Sporting/Recreation Camps
7033	7033	Trailer Parks, Campgrounds
7210	7210	Laundry, Cleaning Services
7211	7211	Laundries
7216	7216	Dry Cleaners
7217	7217	Carpet/Upholstery Cleaning
7221	7221	Photographic Studios
7230	7230	Barber and Beauty Shops
7251	7251	Shoe Repair/Hat Cleaning
7261	7261	Funeral Services, Crematories
7273	7273	Dating/Escort Services
7276	7276	Tax Preparation Services
7277	7277	Counseling Services
7278	7278	Buying/Shopping Services
7296	7296	Clothing Rental
7297	7297	Massage Parlors
7298	7298	Health and Beauty Spas
7299	7299	Miscellaneous General Services
7311	7311	Advertising Services
7321	7321	Credit Reporting Agencies
7322	7322	Debt Collection Agency
7333	7333	Commercial Photography, Art and Graphics
7338	7338	Quick Copy, Repro, and Blueprint
7339	7339	Secretarial Support Services

MCC Lower	MCC Upper	MCC Category Description
7342	7342	Exterminating Services
7349	7349	Cleaning and Maintenance
7361	7361	Employment/Temp Agencies
7372	7372	Computer Programming
7375	7375	Information Retrieval Services
7379	7379	Computer Repair
7392	7392	Consulting, Public Relations
7393	7393	Detective Agencies
7394	7394	Equipment Rental
7395	7395	Photo Developing
7399	7399	Miscellaneous Business Services
7511	7511	Truck Stop
7512	7512	CAR RENTAL AGENCIES -- NOT LISTED BELOW
7513	7513	Truck/Utility Trailer Rentals
7519	7519	Recreational Vehicle Rentals
7521	7521	Car Rental Agencies
7523	7523	Parking Lots, Garages
7531	7531	Auto Body Repair Shops
7534	7534	Tire Retreading and Repair
7535	7535	Auto Paint Shops
7535	7535	Paint Shop Automotives
7538	7538	Auto Service Shops
7542	7542	Car Washes
7549	7549	Towing Services
7622	7622	Electronics Repair Shops
7623	7623	A/C, Refrigeration Repair
7629	7629	Small Appliance Repair
7631	7631	Watch/Jewelry Repair

MCC Lower	MCC Upper	MCC Category Description
7641	7641	Furniture Repair, Refinishing
7692	7692	Welding Repair
7699	7699	Miscellaneous Repair Shops
7800	7800	Government Owned Lottery
7801	7801	Internet Gambling
7802	7802	Government Licensed Horse/Dog Racing
7829	7829	Picture/Video Production
7832	7832	Motion Picture Theaters
7841	7841	Video Tape Rental Stores
7911	7911	Dance Hall, Studios, Schools
7922	7922	Theatrical Ticket Agencies
7929	7929	Bands, Orchestras
7932	7932	Billiard/Pool Establishments
7933	7933	Bowling Alleys
7941	7941	Sports Clubs/Fields
7991	7991	Tourist Attractions and Exhibits
7992	7992	Golf Courses - Public
7993	7993	Video Amusement Game Supplies
7994	7994	Video Game Arcades
7995	7995	Betting/Casino Gambling
7995	7995	DISALLOWED - Gambling Transactions
7996	7996	Amusement Parks/Carnivals
7997	7997	Country Clubs
7998	7998	Aquariums
7999	7999	Miscellaneous Recreation Services
8011	8011	Doctors
8021	8021	Dentists, Orthodontists
8031	8031	Osteopaths

MCC Lower	MCC Upper	MCC Category Description
8041	8041	Chiropractors
8042	8042	Optometrists, Ophthalmologist
8043	8043	Opticians, Eyeglasses
8049	8049	Chiropodists, Podiatrists
8050	8050	Nursing/Personal Care
8062	8062	Hospitals
8071	8071	Medical and Dental Labs
8082	8082	Health Care
8099	8099	Medical Services
8111	8111	Legal Services, Attorneys
8211	8211	Elementary, Secondary Schools
8220	8220	Colleges, Universities
8241	8241	Correspondence Schools
8244	8244	Business/Secretarial Schools
8249	8249	Vocational/Trade Schools
8299	8299	Educational Services
8351	8351	Child Care Services
8398	8398	Charitable and Social Service Organizations - Fundraising
8641	8641	Civic, Social, Fraternal Associations
8651	8651	Political Organizations
8661	8661	Religious Organizations
8675	8675	Automobile Associations
8699	8699	Membership Organizations
8734	8734	Testing Laboratories
8911	8911	Architectural/Surveying Services
8931	8931	Accounting/Bookkeeping Services
8999	8999	Professional Services
9211	9211	Court Costs, Including Alimony and Child Support - Courts of Law

MCC Lower	MCC Upper	MCC Category Description
9222	9222	Fines - Government Administrative Entities
9223	9223	Bail and Bond Payments (payment to the surety for the bond, not the actual bond paid to the government agency)
9311	9311	Tax Payments - Government Agencies
9399	9399	Government Services (Not Elsewhere Classified)
9402	9402	Postal Services - Government Only
9405	9405	U.S. Federal Government Agencies or Departments
9700	9700	Automated Referral Service
9701	9701	Visa Credential Service
9702	9702	Emergency Services
9751	9751	U.K. Supermarkets - Electronic HotFile
9752	9752	U.K. Petrol Stations - ElectronicHot File
9754	9754	GAMBLING-HORSE, DOG RACING-ST LOTTERY
9950	9950	Intra-Company Purchases
9999	9999	CLIENT DEFINED MCC

4.20 Misc_TLV_Data Field

The Misc_TLV_Data field is used for sending rarely used fields that can normally be ignored.

For the format of this field, see section Data Types: *TLV10*.

The table below lists the tag values and their meaning.

Note: Thredd may add tags at any time (without a specification update). To avoid errors, your systems should ignore any unknown tags.

Tag	Value Format	Description
V125030003	N(16,16)	Visa Original Trace ID, exactly as received from Visa. For information only - Traceid_Original is the recommended field to use instead, this can be used if you suspect Traceid_Original is not as expected.
V1045D0082	AN(10)	35AN Plan Registration System Identifier. Contains the plan registration system identifier value to identify the transaction as a Visa Installment Solutions transaction. This identifier is a10-character alphanumeric unique value. (Note: ISO definition allows up to 35 characters, but Visa will send 10 characters).
CGBRDEBT01	ANS(1,35)	UK Debt repayment - Recipient Last Name (Specific to UK country)
CGBRDEBT02	ANS(1,10)	UK Debt repayment - Recipient Postal Code (Specific to UK country)
CGBRDEBT03	N(8,8)	UK Debt repayment - Recipient Date of Birth YYYYMMDD (Specific to UK country)
CGBRDEBT04	ANS(1,20)	UK Debt repayment - Recipient Account Number (Specific to UK country)
G00001S0*nn*	ANS(1,99)	Sender data obtained from Mastercard authorisation message field 108 and Visa fields 56 and 104. For details, see Sender and Receiver Tags.
G00001R0*nn*	ANS(1,99)	Receiver data obtained from Mastercard authorisation message field 108 and Visa fields 56 and 104. For details, see Sender and Receiver Tags.
V034xxxxxx	HEX(2,4000)	This field is used by acquirers to indicate if they have appplied any Strong Customer Authentication (SCA) acquirer exemption to the transaction; see the PSD2 SCA Guide > PSD2 Acquirer Exemptions. **Note**: You should not normally need to extract the data in this field, as Thredd already provides this information in the GPS_POS_DATA field, position 25, Acquirer Exempt from SCA Indicator. Visa Base1 field 34 e-commerce data (complete) is provided as hexadecimals. Each two hexadecimal digits represents one binary byte of data as Thredd received it from Visa. The first two hexadecimals will be the first dataset identifier. Example: *0100078605F14BA74BA7* For more information on the Visa field 34, refer to the following Visa documents: *VisaNet Authorization-Only Online Messages - Technical Specification* and Visa PSD2 SCA for Remote Electronic Transactions Implementation Guide. **Note**: If character data is present, the hexadecimal values will be represented as an IBM EBCDIC code page 1148 character (e.g., if Visa provided the letter “x” in 1 byte, then this is represented here as the hexadecimal value “A7”.). For more information on IBM character sets defined in the EBCDIC code page 1148, see ibm.com: docs > Character sets.

Tag	Value Format	Description
Any other value	Anything	Unknown

Where *nn* represents additional digits.

The following formats are intended for future Mastercard and Visa raw data, if they are required:

Data Source	Tag Construction plan
Banknet (Mastercard online authorisations)	'M' + 3 digit DE + 3 digit subelement + 3 digit subfield
Visa Base1 (visa online authorisations)	'V' + 3 digit DE + 2 hexdigit dataset ID + 4 hexdigit Tag (if sending all datasets, 'xx' will be used as the dataset ID) (if sending all tags, 'xxxx' will be used as the Tag)
GCMS (Mastercard clearing)	'm' + 3 digit DE + 4 digit PDS + 2 digit subfield
Visa Base 2 (Visa clearing)	'v' + 2 digit TC + 1 digit TCR + 3 digit start offset + 3 digit end offset
Specific to a particular country	'C' + 3-alpha-country-code + 6 char identifier
Other	Initial character will not be any of 'M','V','m','v','C'

4.20.1 Sender and Receiver Tags

The table below provides details of Sender and Receiver data obtained from the Mastercard authorisation message field 108 and Visa fields 56 and 104.

The length of the value precedes the actual value, for example: *G00001S0030007Johnson*, where *G00001S003* is the tag for last name, *0007* is the tag value length, and *Johnson* is the tag value.

Misc_TLV_Data Tag Name	Description
G00001S001	Sender first name
G00001S002	Sender middle name
G00001S003	Sender last name
G00001S004	Sender street address
G00001S005	Sender city
G00001S006	Sender province
G00001S007	Sender country (three character alpha ISO code)
G00001S008	Sender postcode
G00001S009	Sender phone number

Misc_TLV_Data Tag Name	Description
G00001S010	Sender date of birth (MMDDYYYY). For example 25011996.
G00001S011	Sender account number (rightmost 4 digits)
G00001S012	Sender identity document (ID) type (00 = passport; 01 = National Identification Card; 02 = Driver's License; 03 = Government Issued; 04 = Other; 05-10 reserved for future use)
G00001S013	Sender ID number
G00001S014	Sender ID country; three character alpha ISO code (e.g., CYP = Cypress)
G00001S015	Sender ID expiry Date (MMDDYYYY)
G00001S016	Sender nationality (three character alpha ISO code)
G00001S017	Sender birth country (three character alpha ISO code)
G00001S018	Sender account number type. See Account Number Type.
G00001S0V1	Sender funds source. See Source of Funds.
G00001S0V2	Sender claim code
G00001R001	Receiver first name
G00001R002	Receiver middle name
G00001R003	Receiverlast name
G00001R004	Receiver street address
G00001R005	Receiver city
G00001R006	Receiver province
G00001R007	Receiver country (3 letter country code, e.g., CYP = Cypress)
G00001R008	Receiver postcode
G00001R009	Receiver phone number
G00001R010	Receiver date of birth (MMDDYYYY). For example 12311996.
G00001R011	Receiver account number (rightmost 4 digits)
G00001R012	Receiver identity type (00 = passport; 01 = National Identification Card; 02 = Driver's License; 03 = Government Issued; 04 = Other; 05-10 reserved for future use)
G00001R013	Receiver ID number
G00001R014	Receiver ID country code (three character alpha ISO code)
G00001R015	Receiver ID expiry date (MMDDYYYY)
G00001R016	Receiver nationality (three character alpha ISO code)

Misc_TLV_Data Tag Name	Description
G00001R017	Receiver birth country (three character alpha ISO code)
G00001R018	Receiver account number type. See Account Number Type.

Account Number Type

Value	Description
0	Other
1	RTN + Bank account
2	IBAN
3	Card account
4	Email
5	Phone number
6	Bank account number (BAN) + Bank Identification Code (BIC)
7	Wallet ID
8	Social Network ID

Source of Funds

Value	Description
1	Visa credit
2	Visa debit
3	Visa prepaid
4	Cash
5	Debit/deposit access accounts other than those linked to a Visacard (includes checking/savings accounts and proprietary debit/ATM cards)
6	Credit accounts other than those linked to a Visa card (includes credit cards and proprietary credit lines)

Example

Sender Data = *0104Adam0703ROM080511A56V10205*

Receiver Data = *0310John Smith*

MiscTLVData = *G00001S0010004AdamG00001S0070003ROMG00001S008000511A56G00001S0V1000205G00001R0030010John Smith*

4.21 Network_Fraud_Data Format

The Network_Fraud_Data field contains Fraud and Risk indicators from the network. This field is a fixed format field. There is no identifier of subfields; each position refers to a specific field from Visa or Mastercard. See the table below.

Positions	Subfield Name (Not part of message)	Visa Usage	Mastercard Usage
1-3	Fraud Score 1	VAA Score	Mastercard Fraud Score
4-6	Fraud Score 1 Maximum Value	Fixed “099”	Fixed “999“
7-8	Fraud Score Reason 1.1	Spaces	Fraud Score Reason Code 1
9-10	Fraud Score Reason 1.2	Spaces	Spaces
11-12	Fraud Score Condition 1.1	VAA Condition Code 1	Spaces
13-14	Fraud Score Condition 1.2	VAA Condition Code 2	Spaces
15-16	Fraud Score Condition 1.3	Spaces (RFU)	Spaces
17-19	Fraud Score 2	VISA Risk Assessment Score	MastercardFraud Rule Manager Score
20-22	Fraud Score 2 Maximum Value	Fixed “099“	Fixed “999“
23-24	Fraud Score Reason 2.1	Spaces	Fraud Rule Manager Reason Code 1
25-26	Fraud Score Reason 2.2	Spaces	Fraud Rule Manager Reason Code 2
27-28	Fraud Score Condition 2.1	VISA Risk Assessment Condition Code 1	Spaces
29-30	Fraud Score Condition 2.2	Spaces (RFU)	Spaces
31-32	Fraud Score Condition 2.3	Spaces (RFU)	Spaces

4.22 Payment Token Fields

This section provides details of the fields which hold payment token information.

4.22.1 PaymentToken_activationMethod

Describes the method used to activate the payment token. The table below describes the valid options and the content for each method.

PaymentToken_activationMethod	Description	Content included
0	None	Empty
1	SMS to mobile	Mobile phone number held on Thredd for the cardholder
2	Email	Email address held on Thredd for the cardholder
3	Cardholder to call automated call centre	Call centre number
4	Cardholder to call normal call centre	Call centre number
5	Website	Website URL
6	Mobile application	Mobile application reference
7	Cardholder will receive voice call	Mobile phone number held on Thredd for the cardholder

4.22.2 PaymentToken_deviceType

Describes the type of device the payment token is installed on. Below is a list of possible values.

PaymentToken_deviceType	Description
A	Clothing / apparel
B	Media/gaming device, eg XBox, TV, set-top box
C	Card
E	Mini-card. A physical card of reduced dimensions (height and width) which is smaller than the standard ID-1 card size (See ISO 7810 for the ID-1 standard.)
D	Domestic application (e.g., fridge, washing machine)
F	Fob or key fob
G	Mobile tag, case or sleeve
H	Fashion accessory (e.g., handbag, glasses)
J	Jewelry (e.g., necklace, rings, bracelets). For Visa Contactless devices, this implies any wrist-worn device (including watches and wristbands.)
M	Mobile phone
N	Non-Card. This originates from Visa Contactless devices, where it indicates anything except: Card (C), Mini-Card (E), Mobile Phone (M) or Wrist-worn device (J).

PaymentToken_deviceType	Description
P	Personal computer or laptop
R	Wristband
S	Sticker
T	Tablet
U	Unknown
V	Vehicle
W	Watch
X	Mobile phone or tablet
other	Ask Thredd for any additional values

4.22.3 PaymentToken_type

Describes the type of payment token. Below is a list of possible values.

PaymentToken_type	Description
BW	Browser accessible Wallet
C	Contactless device PAN
CF	Card on File PAN
CL	Cloud-base payments PAN
P	Real PAN
SE	Secure Element PAN
U	Unknown - other PAN mapping not otherwise defined
V	Virtual PAN

4.22.4 PaymentToken_creatorStatus

Describes the status of the payment token on the token creator's system. Below is a list of possible values.

Note: Thredd receive this value from the token creator's system.

Note: This field can contain " " or be empty when no value has been provided.

.

PaymentToken_creatorStatus	Description	Is this status reversible?
A	Active	Yes

PaymentToken_creatorStatus	Description	Is this status reversible?
D	Deleted on cardholder device	No
I	Inactive	Yes
N	Not tokenised	Yes
S	Suspended	Yes
X	Deactivated	No

4.22.5 PaymentToken_wallet

Describes the type of eWallet the payment token belongs to. Below is a list of possible values.

PaymentToken_wallet	Description
ADYEN	Adyen (Gateway TSP)
AMAZON	Amazon
ANDROID	Google Pay Wallet (known before 20/2/2018 as “Android Pay Wallet”)
APPLE	Apple Pay Wallet
ASIA	Asia Pay
CHUNGHWA	Chungwa
FITBIT	Fitbit Pay Wallet
GARMIN	Garmin Pay
LGPAY	LG Electronics
MASTERPASS	MasterPass from Mastercard
MICROSOFT	Microsoft
MRCHTOKEN	Merchant Tokenisation Program
MTBLANC	Montblanc Pay
PAYNETPHYR	Phyre
RELIANCE	Reliance
SAMA	Saudi Arabia Monetary Authority
SAMSUNG	Samsung Pay Wallet
SECURECO	SecureCo
STOCARD	Stocard Pay Wallet

PaymentToken_wallet	Description
VISA_DCA	Visa Digital Commerce App
VISACKOUT	Visa Checkout
WORLDPAY	WorldPay
other	Ask Thredd for any additional wallets

4.22.6 PaymentToken_PanSource

Describes the originator of a Tokenisation Authorisation Request.

Value	Description
0	Information not provided
5	Chip dip (i.e. EMV contact)
6	Key entered / added manually
7	EMV contactless or VSDC contactless
F	Account Data on File
P	Card added via application / Mobile banking app
W	DPAN input from Wallet Provider (Token to Token)

4.23 PIN Fields

The card's Primary Identification Number (PIN) is encapsulated in a PIN block and then encrypted using the Triple-DES algorithm.

The Data Encryption Standard (DES), including Triple-DES, is described by the United States National Institution of Standards and Technology (NIST) in document NIST 800-67 which is available here: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf

4.23.1 PIN Block Formats

The authorisation request message field PIN_Format describes the PIN block format as follows:

Note: This version of the specification only sends PIN blocks in format 1 (ISO9564-1 Format 1.) This ensures that PINs are properly protected and the receiver can decrypt them without needing to know the PAN. ISO9564-1 is available from https://www.iso.org/home.html

PIN_Format	Format	Example
0	ISO 9564-1 Format 0	PAN = 5299887766554439 PIN = 223344 Plaintext PIN field = '0'+ PIN length (4-C) + PIN + 'F's padding to 16 hex digits = 06223344FFFFFFFF Account number field = '0000' + rightmost 12 digits of the PAN excluding the check digit = 0000988776655443 Now XOR the 2 results to get the PIN block: 06223344FFFFFFFF xor 0000988776655443 => PIN BLOCK = 0622ABC3899AABBC
1	ISO 9564-1 Format 1	PIN BLOCK = '1' + PIN length (4-C) + PIN + random padding to 16 hex digits e.g. PIN = 223344 => 8 random padding bytes needed, e.g. 358C44BF => PIN BLOCK = 16223344358C44BF
2	ISO 9564-1 Format 2 (also see EMV 4.3 book 3 VERIFY command)	PIN BLOCK = '2' + PIN length (4-C) + PIN + 'F' pad nibbles up to 16 hex e.g. PIN = 223344 => PIN BLOCK = '2' + '6' + '223344' + 'FFFFFFFF' => PIN BLOCK = 26223344FFFFFFFF
3	ISO 9564-1 Format 3	PAN = 5299887766554439 PIN = 223344 Plaintext PIN field = '3'+ PIN length (4-C) + 'A-F' random padding to 16 hex digits = 36223344CBADFEEA Account number field = '0000' + rightmost 12 digits of the PAN excluding the check digit = 0000988776655443 36223344CBADFEEA xor 0000988776655443 => PIN BLOCK = 3622ABC3BDC8AAA9

4.23.2 PIN Encryption Example

In this example:

- PIN_Format =1 (ISO 9564-1 Format 1)
- PIN = 223344
- Random padding nibbles for PIN block = 358C44BF

- EHI PIN Key established between Thredd and 3rd party is Triple length 3DES key = 0123456789abcdeffedcba9876543210B5BC921385681AB9

=> PIN BLOCK = 16223344358C44BF

=> PIN field (PIN block 3DES encrypted with EHI PIN Key 0123456789abcdeffedcba9876543210B5BC921385681AB9)

=> PIN field = 479ECEE7AEA0EBAE

4.23.3 Establishment of EHI PIN Keys

Before you can transfer PIN data over EHI, the following needs to have occurred first:

- Establishment of a triple length DES key, which is used to transfer PIN encryption keys for the EHI Zone. (Zone Master Key.)
- Transmission of a PIN key encrypted under the EHI Zone key in ECB mode using 3DES.
- All PINs will be encrypted under the PIN key.

This process is expected to be done manually, as it will be done rarely.

For example:

1. New random 3DES triple length EHI Zone key of clear value '022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02' is generated by Thredd.
2. This is split into 3 clear XOR components of:
    1. D7E307AEDA98D35498E986145A735D367FBA8D6BF0C3ED30
    2. 92464A17A5C6CC2CEC25CC381617A282A6F0E69ABE692E02
    3. 47803B6687EDCC7062EF65AA7BCFF2CBB188215FE6018C30
3. These 3 XOR components are delivered to the 3rd party, to separate people independently.
4. Each 3rd party who has received an XOR component enters them into their Hardware Security Module (HSM).
5. The 3rd party HSM now has the clear Zone Master key of 022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02 installed.
6. Thredd then generate a random triple length EHI PIN Key of clear value '20438354E545C7CD2FB5B9F84CE385C10431A91CF9B98FA5'.
7. Thredd then transmit the EHI PIN key encrypted using Triple-DES in ECB mode under the EHI Zone Key. EHI PIN Key under Zone key is '898AEA86B81C1CA61E575F208E0535A25A1E84D4E88B9097'.
8. The 3rd party then sends this EHI PIN Key under Zone key value to their HSM.
9. 3rd party HSM now has the clear EHI PIN Key of '20438354E545C7CD2FB5B9F84CE385C10431A91CF9B98FA5'.
10. 3rd party can now use this to decrypt the PIN field.

4.23.4 Worked example of 3DES ECB encrypting the PIN key under the Master Key

Using the above example, this is how you encrypt:

- the PIN key (20438354E545C7CD2FB5B9F84CE385C10431A91CF9B98FA5)
- under the Master key (022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02).

Encryption mode is ECB (Electronic Code Book.) This means each 8-byte input block is separately encrypted under the encryption key.

Starting point:

- Clear Zone Master key = 022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02 (Triple length DES key)
- Clear Zone PIN key = 20438354E545C7CD2FB5B9F84CE385C10431A91CF9B98FA5 (Triple length DES key)

Steps:

1. First 8 bytes of PIN key = 20438354E545C7CD
   Triple DES encrypt 20438354E545C7CD under 022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02
   = 898AEA86B81C1CA6
2. Second 8 bytes of PIN key = 2FB5B9F84CE385C1
   Triple DES encrypt 2FB5B9F84CE385C1 under 022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02
   = 1E575F208E0535A2

3. Third 8 bytes of PIN key = 0431A91CF9B98FA5
   Triple DES encrypt 0431A91CF9B98FA5 under 022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02
   = 5A1E84D4E88B9097
4. Now concatenate the 3 encrypted results = 898AEA86B81C1CA6 1E575F208E0535A2 5A1E84D4E88B9097
5. PIN key under Master Key = 898AEA86B81C1CA61E575F208E0535A25A1E84D4E88B9097

4.23.5 Example Triple DES operations with a triple length key

Various examples above involve a triple length DES key encrypting or decrypting an 8-byte block.

Basic Algorithm:

- A Triple length key is 3 DES (8-byte) keys concatenated: K1, K2, K3
- Encryption of Data D = $ENCRYPT_{K3}(DECRYPT_{K2}(ENCRYPT_{K1}(D)))$
- Decryption of Data D = $DECRYPT_{K1}(ENCRYPT_{K2}(DECRYPT_{K3}(D)))$

This is an example of how that works.

Suppose the Triple Length key = 022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02 (e.g. same as clear Zone Master Key above)

Suppose 8-byte block = 20438354E545C7CD (e.g. same as first 8 bytes of the clear PIN key).

Triple DES Encryption

To encrypt this block with the triple length key:

1. DES Encrypt 20438354E545C7CD with 1st part of Triple length key (022576DFF8B3D308)
   = 23085EE9F52CE247
2. DES Decrypt the result of above (23085EE9F52CE247) with 2nd part of Triple length key (16232F8637AB0D7F)
   = 2A5D03C4B8A9F91D
3. DES Encrypt the result of above (2A5D03C4B8A9F91D) with 3rd part of Triple length key (68C24AAEA8AB4F02)
   = 898AEA86B81C1CA6

So the 3DES encryption of 20438354E545C7CD, with key 022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02,
is 898AEA86B81C1CA6

Triple DES Decryption

As an example, we can decrypt the result of above (898AEA86B81C1CA6) with the same triple length key
(022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02)

To decrypt this block with the triple length key:

1. DES Decrypt 898AEA86B81C1CA6 with 3rd part of Triple length key (68C24AAEA8AB4F02)
   = 2A5D03C4B8A9F91D
2. DES Encrypt the result of above (2A5D03C4B8A9F91D) with 2nd part of Triple length key (16232F8637AB0D7F)
   = 23085EE9F52CE247
3. DES Decrypt the result of above (23085EE9F52CE247) with 1st part of Triple length key (022576DFF8B3D308)
   = 20438354E545C7CD

So the 3DES decryption of 898AEA86B81C1CA6, with key 022576DFF8B3D30816232F8637AB0D7F68C24AAEA8AB4F02,
is 20438354E545C7CD.

4.24 POS_Data_DE61 field

The table below describes the POS_Data_DE61 field, used for Mastercard Authorisation related message. (See also Get Transaction Message fields: POS_Data_DE61)

All subfields are concatenated together in order. Subfields begin at 1. Only the first 9 subfields (i.e. subfields 1 to 9, the first 9 characters) in the field are mandatory. For example, you might have just the first 9 subfields, or first 10, or first 11, or first 12, or first 13 or all 14.

Note: This field is deprecated in EHI version 3.0.

subfield	Name	Format	Description / Valid Values
1	POS Terminal Attendance	N(1,1)	POS Terminal Attendance - indicates if the card acceptor is: 0 = Attended terminal 1 = Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA) 2 = No terminal used (voice/audio response unit [ARU] authorisation)
2	RFU	N(1,1)	0 = Reserved for future use.
3	POS Terminal Location	N(1,1)	POS Terminal Location - indicates the terminal location: 0 = On premises of card acceptor facility 1 = Off premises of card acceptor facility (merchant terminal–remote location) 2 = Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA) 3 = No terminal used (voice/ARU authorisation) 4 = On premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)
4	POS Cardholder Presence	AN(1,1)	POS Cardholder Presence - indicates whether the cardholder is present at the point of service and explains the condition if the cardholder is not present. 0 = Cardholder present 1 = Cardholder not present, unspecified 2 = Mail/facsimile order 3 = Phone/ARU order 4 = Standing order/recurring transactions 5 = Electronic order (home PC, Internet, mobile phone, PDA)
5	POS Card Presence	N(1,1)	POS Card Presence - indicates if the card is present at the point of service. 0 = Card present 1 = Card not present
6	POS Card Capture Capabilities	N(1,1)	POS Card Capture Capabilities - indicates whether the terminal has card capture capabilities. 0 = Terminal/operator has no card capture capability 1 = Terminal/operator has card capture capability
7	POS Transaction Status	N(1,1)	POS Transaction Status - indicates the purpose or status of the request. 0 = Normal request (original presentment) 2 = SecureCode phone order 3 = ATM installment inquiry 4 = Preauthorised request 6 = ATC update

subfield	Name	Format	Description / Valid Values
			8 = Account Status Inquiry (ASI) service 9 = Tokenization request/notification
8	POS Transaction Security	N(1,1)	POS Transaction Security indicates the card acceptor's security level. 0 = No security concern 1 = Suspected fraud (merchant suspicious–code 10) 2 = ID verified
9	RFU	N(1,1)	0 = Reserved for future use.
10	Cardholder-Activated Terminal Level	N(1,1)	Indicates whether the cardholder activated the terminal with the use of the card and the CAT security level. 0 = Not a CAT transaction 1 = Authorized Level 1 CAT: Automated dispensing machine with PIN 2 = Authorized Level 2 CAT: Self-service terminal 3 = Authorized Level 3 CAT: Limited-amount terminal 4 = Authorized Level 4 CAT: In-flight commerce 5 = Reserved 6 = Authorized Level 6 CAT: Electronic commerce 7 = Authorized Level 7 CAT: Transponder transaction 8 = Remote Terminal (eg Mastercard Tap to More transaction) 9 = MPOS Acceptance Device
11	POS Card Data Input Capabilities	N(1,1)	Terminal capabilities for transferring the data on the card into the terminal. 0 = Unknown or unspecified 1 = No terminal used (voice/ARU authorization); server 2 = Magnetic stripe reader only 3 = Contactless M/Chip (Proximity Chip) Terminal supports PayPass M/Chip and PayPass magstripe transactions. The terminal also may support other card input types, including contact transactions 4 = Contactless Magnetic Stripe (Proximity Chip) only The terminal supports PayPass magstripe transactions. The terminal also may support other card input types, including contact transactions 5 = EMV specification (compatible chip reader) and magnetic stripe reader. The terminal also may support contactless transactions; however contactless transactions should always be submitted with value 3 or 4. 6 = Key entry only 7 = Magnetic stripe reader and key entry 8 = EMV specification (compatible chip reader), magnetic stripe reader and key entry. The terminal also may support contactless transactions; however contactless transactions should always be submitted with value 3 or 4. 9 = EMV specification (compatible chip reader) only - The terminal also may support contactless transactions; however contactless transactions should always be submitted with value 3 or 4. DE 61, subfield 11 values 3, 4, 5, 8, and 9 can only be used if the terminal is chip certified by Mastercard.

subfield	Name	Format	Description / Valid Values
12	POS Authorization Life Cycle	N(2,2)	Indicates the number of days pre-authorization will stay in effect. Used mainly for car rentals and hotel reservations. Zeros indicate it does not apply. Zero fill or number of days.
13	POS Country Code	N(3,3)	ISO 3-digit numeric country code of the terminal location. See Country Codes.
14	POS Postal Code	ANS(0,10)	Merchant postal code.

4.25 POS_Data_DE22 in Authorisation Messages

The POS Entry Mode and POS PIN Capture capability field (POS_Data_DE22) is made up of various subfields. (See also Get Transaction Message fields: POS_Data_DE22)

Note: Similar values are used by Visa and Mastercard, but there are some subtle differences. The differences for each are described in the tables below.

4.25.1 POS_Data_DE22 Layout Format

The field for Mastercard Authorisation Messages consists of 3 decimal digits as follows:

Position	Length	Description
1-2	2	PAN Entry Method See POS_Data_DE22 positions 1-2: PAN Entry Method
3	1	PIN Entry Capability See POS_Data_DE22 positions 3: Terminal PIN Entry Capability

The field for Visa Authorisation Messages consists of 4 decimal digits as follows:

Position	Length	Description
1-2	2	PAN Entry Method See POS_Data_DE22 positions 1-2: PAN Entry Method
3	1	PIN Entry Capability See POS_Data_DE22 positions 3: Terminal PIN Entry Capability
4	1	Filler - value ‘0’

4.25.2 POS_Data_DE22 positions 1-2: PAN Entry Method

Note: A normalised value to identify the Card Data Input Method can be found in GPS_POS_Data field, in position 3. See "GPS_POS_Data field" on page 190 for more information.

This field is formatted as follows:

Value	Mastercard Description	Visa Description
00	Unknown or no terminal	Unknown or terminal not used
01	Manual Key Entry	(manual key entry) for application-based e-commerce transactions, and card-not-present transactions initiated with a token
02	Partial Magnetic Stripe Read	Magnetic stripe read; CVV checking may not be possible Plus transactions: Exact Track 2 contents read, but transaction is not eligible for CVV checking
03	Barcode	Optical code
04	OCR	Not valid
05	Contact EMV ICC	Integrated circuit card read; CVV or iCVV checking is possible

Value	Mastercard Description	Visa Description
07	Contactless EMV ICC	(contactless chip using VSDC rules) for transactions at contactless-enabled devices with a mobile-issued token payment
10	Credential-on-file Indicates a Merchant is initiating a transaction on behalf of the Cardholder using credentials stored on file.	Credential-on-file Indicates a Merchant is initiating a transaction on behalf of the Cardholder using credentials stored on file.
79	PAN+expdate key entered by Acquirer (PAN+expdate read from Magnetic Stripe and communicated verbally to acquirer who keyed in the transaction. Neither Track1 or Track2 will be present.)	Not valid
80	Magnetic Stripe (fallback from EMV ICC)	Not valid
81	e-commerce	Not valid
82	PAN data on file	Not valid
90	Magnetic Stripe Read	(magnetic stripe read; CVV check is possible; exact content of Track 1 or Track 2 included)
91	Contactless Magnetic Stripe	(contactless chip using magnetic stripe data rules) for transactions at contactless-enabled devices with a mobile-issued token payment
95	Contact EMV ICC (something unreliable)	Integrated circuit card read; CVV or iCVV checking may not be possible
96	Stored Value from pre-registered checkout service	Not valid

4.25.3 POS_Data_DE22 positions 3: Terminal PIN Entry Capability

Note: A normalised value to identify if the terminal supports PIN entry can be found in GPS_POS_Capability field, specifically in positions 24, 30, 31 and 48. See "GPS_POS_Capability field" on page 184 for more information.

This describes the capability of the Terminal to accept a PIN. The field is formatted as follows:

Value	Mastercard Description	Visa Description
0	Unknown	Unknown
1	Terminal supports PIN.	Indicates that the point-of-transaction terminal can accept and forward an online PIN.
2	Terminal does not support PIN.	Indicates that the point-of-transaction terminal cannot accept and forward an online PIN.
8	Terminal supports PIN, but PIN pad is not working.	Terminal PIN pad is down

4.26 POS_Data_DE22 in Mastercard Financial Messages

Note: The POS_Data_DE22 field applies to Mastercard Financial Clearing messages only (i.e., MTID=1240, MTID=1442). For Visa, use GPS_POS_Data. (See also Get Transaction Message fields: POS_Data_DE22 and GPS_POS_Data)

The POS Data codes (POS_Data_DE22) field is made up of various subfields. Its format is based on ISO8583:1993 DE 22 specification, and consists of both:

- Terminal capabilities (what the terminal can do)
- Terminal methods (what the terminal did do, or what actually happened)

Positions	Length	Field Name	Description / Valid Values
1	1	Card Data Input Capability	0 = Unknown 1 = Manual, no terminal; server 2 = Magnetic stripe reader (MSR) 3 = Barcode 4 = OCR 5 = ICC 6 = PAN Key entry (PKE) only A = Contactless MSR (possibility also optionally including ICC, MSR or PKE) B = MSR + PKE C = MSR, ICC, PKE D = MSR + ICC E = ICC + PKE M = Contactless ICC + Contactless MSR (possibly also optionally including ICC, MSR or PKE) V = Other
2	1	Cardholder Authentication Capability	0 = No electronic authentication capability 1 = PIN 2 = Electronic signature analysis capability 3 = Biometrics 4 = Biographic 5 = Electronic authentication capability is inoperative 9 = Unknown
3	1	Card Capture Capability	0 = No capture capability 1 = Card Capture capability 9 = Unknown
4	1	Terminal Operating Environment	0 = No Terminal used 1 = On card acceptor premises, attended 2 = On card acceptor premises, unattended 3 = Off card acceptor premises, attended 4 = Off card acceptor premises, unattended 5 = On cardholder premises, unattended 6 = Off cardholder premises, unattended 9 = Unknown
5	1	Cardholder present data	0 = Cardholder present 1 = Cardholder not present (unspecified) 2 = Cardholder not present (mail order) 3 = Cardholder not present (telephone order) 4 = Cardholder not present (standing order or recurring transaction) 5 = Cardholder not present (e-commerce)

Positions	Length	Field Name	Description / Valid Values
6	1	Card Present Data	0 = Card not present 1 = Card Present
7	1	Card Data Input Method	0 = Unknown or no terminal 1 = Manual Input (no terminal used) 2 = Partial Magnetic Stripe Read 3 = Barcode 4 = OCR 5 = Contact EMV ICC 6 = PAN Key Entry A = Contactless Magnetic Stripe B = Magnetic Stripe Read C = Contact EMV ICC, Online Transaction F = Contact EMV ICC, Offline Transaction M = Contactless EMV ICC N = Contactless EMV ICC or Contactless Magnetic Stripe (PAN mapping service applied by Network) O = e-commerce with EMV ICC. Mastercard Digital Enablement Service Applied. R = e-commerce with EMV ICC S = e-commerce T = Pan auto-entry via server (issuer, acquirer or third party vendor system) V = e-commerce or PAN auto-entry by server. Card on File service applied by Network.
8	1	Cardholder authentication Method	0 = Not authenticated 1 = PIN 2 = Electronic Signature Analysis 3 = Biometrics 4 = Biographic 5 = Manual signature verification 6 = Other Manual verification (e.g. drivers licence) 9 = Unknown S = Other systematic verification (including biometrics + biographic)
9	1	Cardholder authentication entity	Identifies who verified the cardholder (using the method described in the *Cardholder authentication method* field above). 0 = Not authenticated 1 = ICC 2 = Terminal 3 = Authorising Agent 4 = Merchant 5 = Other 9 = Unknown
10	1	Card Data Output Capability	This is rarely used. 10 = Unknown 1 = None 2 = Magnetic Stripe writer 3 = ICC S = Other
11	1	Terminal Data Output Capability	This is rarely used. 0 = Unknown 1 = None

Positions	Length	Field Name	Description / Valid Values
			2 = Printing only 3 = Display only 4 = Printing and Display
12	1	PIN Capture Capability	0 = No PIN capture capability 1 = Unknown 4 = PIN capture up to 4 digits max 5 = PIN capture up to 5 digits max 6 = PIN capture up to 6 digits max 7 = PIN capture up to 7 digits max 8 = PIN capture up to 8 digits max 9 = PIN capture up to 9 digits max A = PIN capture up to 10 digits max B = PIN capture up to 11 digits max C = PIN capture up to 12 digits max

4.27 Processing Codes

The Processing code (`Proc_Code`) is a 6 digit field made up of:

- 2 characters transaction code. See Transaction Codes.
- 2 characters source account type code. See Account Type Codes.
- 2 characters destination account type code. See Account Type Codes.

For transactions initiated via web services or the Cards API, the processing code is formed of:

- 3 digits load source supplied in the request
- 3 digits “999”

4.27.1 Transaction Codes

The first two characters of the processing code is the transaction code, as follows:

Value	Description	Impacts Balance
00	Debits (goods and services)	Yes
01	Debits for ATM cash withdrawals (on Visa and Mastercard networks) May also be used for manual cash disbursements as follows: • Mastercard *Authorisation* transactions on Maestro cards only • Visa *Authorisation* and *Clearing* transactions on Visa cards	Yes
02	Adjustment Credits Indicates a Credit adjustment.	Yes
09	Debits (goods with cash back)	Yes
10	Account Funding	Yes
11	Quasi-Cash Visa-specific quasi-cash transaction. This is used for specific merchants where the purchased items could be converted to cash (e.g., gaming chips, money orders, wire-transfer).	Yes
12	Debits (for manual cash disbursements). Type of transaction where cash is given to the cardholder, for example, from a bank branch by a member of staff using a Point of Sale (POS) terminal. **Note**: Used for *Clearing* transactions on Mastercard Credit, Cirrus, Maestro and Mastercard Debit.	Yes
17	Debits (for manual cash disbursements). Type of transaction where cash is given to the cardholder, for example, from a bank branch by a member of staff using a Point of Sale (POS) terminal. **Note**: Used for *Authorisation* transactions on Mastercard Credit, Cirrus and Mastercard Debit.	Yes
18	Unique Transaction (requires unique MCC) Mastercard-specific transaction category. Similar to Visa's quasi-cash, this is used for specific merchants where the purchased items could be converted to cash (e.g., gaming chips, money orders).	Yes
19	Debit Adjustments May be received for non-card money transfers (out), manual or one-off balance adjustments or additional	Yes

Value	Description	Impacts Balance
	fees.	
20	Credits (for refund) / Credit voucher or merchandise return authorisation	Yes
21	Credits (for deposit)	Yes
22	Credits - Card Load	Yes
23	Debits - Card Unload	Yes
26	Original Credits Visa-specific Money Send transaction. Also called an Original Credit Transaction (OCT).	Yes
28	Credits (for Payment Transaction) Mastercard-specific Money Send transaction.	Yes
30	Balance inquiry service (supported by both Visa and Mastercard)	No
32	Visa Tokenisation - Tokenisation Eligibility. Only used by Visa.	No
33	MDES / Visa Tokenisation – Tokenisation Authorisation	No
34	MDES/ Visa Tokenisation – Activation Code Notification	No
35	MDES / Visa Tokenisation – Tokenisation Complete Notification	No
36	MDES / Visa Tokenisation – Token Event Notification. See the 'Message_Source' field for which system originated the Token Event. See the 'Message_Why' field for what sort of Token Event occurred.	No
37	Visa Tokenisation - Get Supported Cardholder Authentication Methods (for Approve with Authentication). Only used by Visa.	No
38	Visa Tokenisation - Device Binding. Only used by Visa.	No
39	Indicates an Account Verification transaction (eligibility inquiry) for a Debit Account Status Inquiry (ASI). A Debit ASI is a Visa service that checks if an amount can be debited from an account, Thredd uses this code for mapping from a debit transaction (authorisation code 00).	No
70	PIN change (Visa only)	No
71	Card Data File Action (e.g., new PAN or expdate)	No
72	PIN unblock (Visa only)	No
89	A Credit ASI that checks if an account is open and able to receive funds for a credit transaction.	No
91	PIN unblock (Mastercard only)	No
92	PIN change (Mastercard only)	No

4.27.2 Account Type Codes

The 3rd & 4th digits in Processing code is the Source account type code.

The 5th and 6th digits in Processing code is the Destination account type code.

Both codes are from the following list of account type codes (based on ISO 8583:2003 Account Type Codes).

Value	Description
00	Default Account (not specified or not applicable)
10	Savings Account
20	Cheque Account
30	Credit Card Account
35	Deferred debit account
36	Charge account
38	Credit Line Account
39	Corporate Account
40	Universal Account
50	Money Market Investment Account
58	IRA Investment Account
60	Prepaid or Stored Value Account
90	Revolving Loan Account
91	Instalment Loan Account
92	Real Estate Loan Account

4.28 Reason_ID

The Reason_ID field contains a code to indicate the reason behind this message.

This field is used to describe the reason for a chargeback, but may be used to explain the reason behind other messages. See also the Message_Why field.

4.28.1 Reason_ID Usage

The usage varies per type of message, as follows:

MTID	Txn_Type	Description	Reason_ID meaning
0100 0120 0400 0420	A, D, J D, J D D	If message comes from Visa then: Visa's Message Reason Code (otherwise blank)	Visa's Reason for the message. See below.
1240	C	Chargeback Notification	Reason for the chargeback. See below.
1240	H	Chargeback Notification (Non-Credit)	Reason for the chargeback. See below.
(all other combinations)		(all other transactions)	Not defined. Will be blank.

4.28.2 Reason_ID for a Chargeback (Txn_Type C and H)

In Chargeback message types, the Reason_ID field is the reason for the chargeback.

The code is specific to the payment network the chargeback relates to, as networks define the valid chargeback reasons, and may change them. The table below list the reason_ID codes. For more information on the code, refer to the following Visa/Mastercard chargeback documentation:

Mastercard codes are defined in the *Mastercard GCMS IPM clearing formats manual*, Field 25 (Message Reason Code), as applicable for chargeback messages.

Visa codes are defined in the BASE2 file TC33 "Base2 Dispute Financial Status Advice" TCR1 record position 74-75 "Dispute Financial Reason Code". Since Thredd expects all customers to initiate Visa Chargebacks on the VROL system, only VROL-related chargeback reasons are listed below. See also the Dispute_Condition code.

Reason_ID	Mastercard network meaning (Chargeback Message Reason Code)	Visa network meaning (Dispute Financial Reason Code)
10	-	Fraud
11	-	Authorisation
12	-	Processing Error
13	-	Consumer Dispute
4515	Cardholder Denies Transaction Finalised	
4804	Multiple Processing, Duplicate	
4807	Warning Bulletin	
4808	Requested/Required Authorisation not obtained	

Reason_ID	Mastercard network meaning (Chargeback Message Reason Code)	Visa network meaning (Dispute Financial Reason Code)
4809	Transaction not reconcilied	
4811	Stale Transaction	
4812	Account Number not on file	
4831	Transaction Amount Differs	
4834	Duplicate Processing	
4837	Fraudulent Transaction, no cardholder authorisation	
4840	Fraudulent Processing of Transaction	
4841	Cancelled Recurring Transaction	
4842	Late Presentment	
4846	Correct Transaction Currency Not Provided	
4849	Questionable Card Acceptor Activity	
4850	Installment Transaction Dispute	
4853	Cardholder Dispute Defective/Not as described	
4854	Cardholder Dispute (not elsewhere classified) - USA only	
4855	Non-receipt of merchandise	
4859	Services not rendered	
4860	Credit not processed	
4863	Cardholder does not recognize - Potential Fraud	
4870	Chip Liability Shift	
4871	Chip/PIN Liability Shift	
4880	Maestro Late Presentment	
4890	Syntax Error Return	
4900	Invalid Second Presentment (Generic)	
4901	Required documentation not received to support second presentment	
4902	Documentation received was illegible	
4903	Scanning error - unrelated documents or partial scan	
4905	Invalid Acquirer Reference Number in Second Presentment, no documentation required or provided	

Reason_ID	Mastercard network meaning (Chargeback Message Reason Code)	Visa network meaning (Dispute Financial Reason Code)
4908	Invalid Acquirer Reference Number in Second Presentment, documentation received	
4999	Domestic Chargeback Dispute	

4.28.3 Reason_ID for an Authorisation (Txn_Type A, D, J)

In authorisation-related messages (Txn_Types: A, D or J) if Thredd receives the transaction from Visa, then the Visa Message Reason code is included, if available.

Note: Thredd maps important Visa Message Reasons to the Thredd field Message_Why. This field is provided for additional information. Thredd does not recommend you process this, but you can store for information if desired.

Reason Code	Used for	Description
2104	Acquirer generated 0120 (USA only)	Acquirer Advice. No 0100 was sent
2501	Reversal messages	Transaction voided by customer
2502	Reversal messages	Transaction not completed
2503	Reversal messages	No confirmation from Point of Sale (POS) terminal
2504	Reversal messages	Partial dispense by ATM or POS partial reversal
3700	Payment token related messages	Token create
3701	Payment token related messages	Token deactivate
3702	Payment token related messages	Token suspend
3703	Payment token related messages	Token resume
3711	Payment token related messages	Device provisioning result
3712	Payment token related messages	One Time Password (OTP) verification result
3713	Payment token related messages	Call Centre activation
3714	Payment token related messages	Mobile Banking App activation
3715	Payment token related messages	Replenishment confirmation of limited-use keys
3716	Payment token related messages	Token expiry update
3717	Payment token related messages	3DS browser activation
3720	Payment token related messages	PAN expiry update
3721	Payment token related messages	PAN update
3730	Payment token related messages	Device provisioning update results

Reason Code	Used for	Description
3740	Payment token related messages	Device binding
3741	Payment token related messages	Device binding results
3742	Payment token related messages	One Time Password (OTP) verification results - device binding
3743	Payment token related messages	Call centre step up - device binding
3744	Payment token related messages	Mobile banking app step up - device binding
3745	Payment token related messages	Device binding removed
3748	Payment token related messages	3DS browser setup - device binding
3749	Payment token related messages	Device binding with FIDO intent.
3751	Payment token related messages	Cardholder verification results
3752	Payment token related messages	OTP verification result - cardholder verification
3753	Payment token related messages	Call center step up - cardholder verification
3754	Payment token related messages	Mobile banking app step up - cardholder verification
3755	Payment token related messages	3DS browser setup - cardholder verification
3760	Payment token related messages	Device binding Green Flow
3900	Merchant initiated transactions	Incremental authorization
3901	Merchant initiated transactions	Resubmission
3902	Merchant initiated transactions	Delayed charges
3903	Merchant initiated transactions	Reauthorization
3904	Merchant initiated transactions	No show
5206	Deferred authorisation	Deferred Authorisation
5400	Fee collection/funds disbursement transactions	Preauthorisation
5401	Fee collection/funds disbursement transactions	Purchase
5402	Fee collection/funds disbursement transactions	Original Credit Transaction (OCT)
5403	Fee collection/funds disbursement transactions	Account Funding Transaction (AFT)
5404	Fee collection/funds disbursement transactions	Bill Pay
5405	Fee collection/funds disbursement transactions	Preauthorisation Completion
5406	Fee collection/funds disbursement transactions	Reversal
5407	Fee collection/funds disbursement transactions	Chargeback

Reason Code	Used for	Description
5408	Fee collection/funds disbursement transactions	Representment
5409	Fee collection/funds disbursement transactions	Adjustment
Any other value	Unknown	Unknown. Visa may add extra codes at any time.

4.29 Response Status Values

The table below lists the response status codes that you can return in a response to a payment authorisation request through EHI. See Get Transaction Message field: Responsestatus.

Note: For details of `<Resp_Code_DE39>` response codes that the Card Scheme (Network) sends to Thredd, see Response_Code_DE39 Values. For card status codes, see Card Status Codes.

Response Code	Description	Action
00	All good.	Approve
01	Refer to card issuer. **Note**: Not permitted for Visa transactions.	Refer
03	Invalid merchant.	Decline
05	Do not honour.	Decline
0A	Approval with Load.	Approve
5C	Transaction not supported or blocked by issuer. **Note**: For Visa transactions only.	Decline
9G	Blocked by cardholder, contact cardholder. **Note**: For Visa transactions only.	Decline
10	Partial approval. **Note:** This is permitted only if GPS_POS_Capability position 1 (partial approval supported) is '1' (POS supports partial approval)	Approve
12	Invalid transaction. May also be used when Integrated Circuit Card (ICC) Card Verification Value (iCVV) or Card Authentication Method (CAM) authorization request cryptogram (ARQC) validation was not successful. **Note**: For Visa transactions only.	Decline
13	Invalid amount	Decline
14	Invalid card number (no such number)	Decline
15	No such issuer. **Note**: For Visa transactions only.	Decline
33	Expired card (Capture).	Decline and *Pickup* card
41	Lost card (Capture).	Decline and *Pickup* card
43	Stolen card (Capture).	Decline and *Pickup* card
46	Account closed and no further authorisation requests will be approved.	Decline

Response Code	Description	Action
51	Insufficient funds.	Decline
54	Expired card.	Decline
55	Incorrect PIN.	Decline
57	Transaction not permitted to cardholder. **Note: M**ay be used if the decline condition applies to all primary account numbers (PANs) for the same product. It cannot be used for individual PANs to generically decline a transaction. **Note**: For Visa transactions only.	Decline
58	Transaction not permitted to terminal.	Decline
59	Suspected fraud.	Decline
61	Exceeds withdrawal amount limit.	Decline
62	Restricted card (e.g. card invalid in region or country).	Decline
63	Security violation.	Decline
65	Exceeds withdrawal frequency limit.	Decline
6P	Verification Data Failed. Applies to cardholder, card, and other verification data. Includes both: • Provided verification data is invalid • Required verification data is missing **Note**: if a more specific code exists (e.g. '55' if PIN incorrect), then use that.	Decline
70	Cardholder to contact issuer. **Note**: only for Mastercard transactions.	Decline
72	Account not yet activated.	Decline
75	Allowable number of PIN tries exceeded.	Decline
78	Card is not active (including created but not yet activated).	Decline
91	Issuer or switch is inoperative. • Gateway and Cooperative Processing (modes 1 or 2) – Thredd will decline • Gateway Processing with STIP (mode 4) – Thredd to stand-in If your systems are unavailable, then use '05' decline if you do not want to invoke STIP. **Note**: Gateway and Cooperative Processing (modes 1 or 2), for Mastercard: using this code will invoke STIP at the Mastercard, which may approve the transaction (depending on your STIP setup at Mastercard.)	Decline or Invoke STIP (at Thredd or Network)
92	Unable to Route Transaction (to Issuer or EHI). • Gateway Processing (modes 1 or 2) – Thredd will decline	Decline or Invoke STIP (at Thredd or Network)

Response Code	Description	Action
	• Gateway Processing with STIP (mode 4) - Thredd to stand-in If your systems have a fatal error, then use '05' decline if you to not want to invoke STIP. **Note:** If this received in advices, it can indicate that Thredd failed to connect to EHI. **Note:** Gateway and Cooperative Processing (modes 1 or 2), for Mastercard: using this code will invoke STIP at Mastercard, which may approve the transaction (depending on your STIP setup at Mastercard.)	
93	Violation of law. (Transaction is illegal or against regulations in this jurisdiction.) **Note**: Visa use only. For Mastercard Thredd suggest using value 57 instead.	Decline
96	System malfunction. • Gateway or Cooperative Processing (modes 1 or 2) - Thredd will decline • Gateway Processing with STIP (mode 4) - Thredd to stand-in If your systems have a fatal error, then use '05' decline if you to not want to invoke STIP. **Note**: Gateway or Cooperative Processing (modes 1 or 2): using this code will invoke Card Scheme STIP at Mastercard or Visa, which may approve the transaction (depending on your STIP setup).	Decline or Invoke STIP (at Thredd or Network)
C0	Strong Customer Authentication (SCA) required, card form factor.	Decline (reattempt with SCA)
C1	SCA required, non-card form factor.	Decline (reattempt with SCA)
N7	Decline for CVV2 failure.	Decline
R0	Merchant level one-time stop payment to be used for VSPS-eligible (Visa Stop Payment Service) transactions (recurring, instalment, and credential-on-file).	Stop this payment.
R1	Used when a cardholder requests to stop all VSPS-eligible (Visa Stop Payment Service) transactions (recurring, instalment, and credential-on-file) payments against a single merchant. **Note:** This is a Category 1 response code, meaning the issuer will never approve the transaction and further attempts are not permitted.	Stop all future payments for a single merchant.
R3	Used when a cardholder requests to stop all VSPS-eligible (Visa Stop Payment Service) payments (recurring, instalment, and credential-on-file) against all merchants. **Note:** This is a Category 1 response code, meaning the issuer will never approve the transaction and further attempts are not permitted.	Stop all future payments for all merchants.
(any code not in the above list)	Invalid response.	If 0110 response, then Thredd will invoke STIP in EHI mode 4, otherwise will decline (05).

Notes:

- Response code "01" is not permitted for Visa Transactions. If "01" is sent, then Visa will discard the authorisation response and instead invoke STIP.
- Response codes 12 and 15 are Visa-only codes effective from 12 April 2025.

- Response Code 57 (Transaction not permitted to cardholder) cannot be used for individual PANs to generically decline a transaction. It can still be used if the decline condition applies to all PANs for the same product. This change is effective from 18 October 2025.
- Response codes 04, 07, 14, 41, 43, and 46 are only used for listing permanently closed or invalid accounts.
- If an Issuer uses the 12, 15 or 57 response codes incorrectly, then Visa will convert the response and send it to the Acquirer as a generic response code decline.

4.30 Resp_Code_DE39 Values

This field is provided in Mastercard 0120 (authorisation advice), 0400 (reversal request) and 0420 (reversal advice) messages to indicate the reason for the advice or reversal, which is sent to Thredd by the Card Scheme (Network). For more details, see Get Transaction Message fields: Resp_Code_DE39.

Note: For details of authorisation response status codes that is sent to Thredd through EHI, see ResponseStatus Values. For card status codes, see Card Status Codes.

Code	Reason for Advice or Reversal
06	Error.
17	Customer cancellation. This code is also used for reversals where other reasons in this section do not apply. For example, if doing an EMV contact transaction and the card returns an AAC (decline) after receiving an approve response from the Issuer, this code is used. This code is also normally used if the terminal decides to reverse a transaction from the Issuer, where the Issuer approved it (but additionally stated that some authentication data such as Address or CVV2 was incorrect.)
32	Partial reversal.
34	Suspected fraud.
68	Response received too late.
82	Timeout from network to issuer. Visa/Mastercard was unable to send the original 0100 message to Thredd.

4.30.1 Code values that explain the reason for the advice

Below is a list of other codes values in the `Resp_Code_DE39` field which can be used to explain the reason for the advice:

- For an 0120 advice, this indicates the response that was originally sent to the terminal.
- For an 0400 advice or 0420 reversal, this code is what was used in the original 0110 acquirer response, and does not provide information on why the reversal was created.

Code	Description	Action
00	All good	Approve
01	Refer to card issuer	Refer
03	Invalid merchant	Decline
04	Capture card	Decline and *Pickup* card
05	Do not honour	Decline
06	Unspecified error	Decline
08	Honor with identification	Approve
10	Partial approval	Approve

Code	Description	Action
12	Invalid transaction	Decline
13	Invalid amount	Decline
14	Invalid card number (no such number)	Decline
15	Unable to route at IEM (Issuer's Europay Module). Card Scheme network cannot connect to Thredd.	Decline
30	Format error	Decline
41	Lost card (Capture)	Decline and *Pickup* card
43	Stolen card (Capture)	Decline and *Pickup* card
46	Account closed	Decline
51	Insufficient funds	Decline
54	Expired card	Decline
55	Incorrect PIN	Decline
57	Transaction not permitted to cardholder	Decline
58	Transaction not permitted to terminal	Decline
59	Suspected fraud	Decline
61	Exceeds withdrawal amount limit.	Decline
62	Restricted card (e.g. card invalid in region or country)	Decline
63	Security violation	Decline
65	Exceeds withdrawal frequency limit	Decline
70	Cardholder to contact issuer	Decline
71	PIN not changed	Decline
72	Account not yet activated	Decline
75	Allowable number of PIN tries exceeded	Decline
76	Wrong PIN, allowable number of PIN tries exceeded	Decline
77	Issuer does not participate in the service	Decline
78	Card is not active (including created but not yet activated)	Decline
79	Unacceptable PIN - Transaction declined. Retry.	Decline

Code	Description	Action
81	Domestic debit transaction not allowed	Decline
85	Approved (used for some non-financial transactions such as a PIN Unblock request)	Approve
86	PIN validation not possible	Decline
87	Purchase amount only. No Cashback allowed.	Approve
88	Cryptographic failure	Decline
89	Authentication failure	Decline
91	Issuer or switch is inoperative	Decline
92	Unable to Route Transaction (to Issuer or EHI)	Decline
94	Duplicate transmission	Decline
96	System malfunction	Decline

4.30.2 Using the Resp_Code_DE39 value in your response to Thredd

When declining a transaction, you must respond with a valid decline reason; we recommend that you use the same response code as received in the `Resp_Code_DE39` field. You should avoid declining with the generic response code *05 - Do not honour*.

The decline reason should be provided in the `ResponseStatus` field of your EHI message response. See GetTransaction Message Fields.

4.31 Response_Source and Message_Source

This field is used to identify the source (originator) of the message. It indicates:

- Who sent the 0110 response message to the terminal (Response_Source)
- Who sent this (usually advice/reversal) message in the first place (Message_Source)
- Who created the payment token (PaymentToken_creator)

Response_Source and Message_Source may be present in the Authorisation Advice and/or Authorisation Reversal messages.

4.31.1 Possible Values

Source	Description
UNKNOWN	Unknown or not applicable
ISSUER	Thredd Issuer Auth System (primary site)
ISSUER-ALT	Alternate Issuer System (Secondary site)
ACQUIRER	Acquirer
TERMINAL	Terminal
CARD	Chip Card
EHI	Issuer PM Host via EHI connection
ACQ-MC-X	Acquirer X-Code (Mastercard)
MC-X	Mastercard X-Code at acquirer MIP
MC-STIP	Mastercard Stand-In processing
VISA-STIP	Visa Stand-In processing
VISA-IARS	Visa International Automated Referral Service
MC-ICPS	Mastercard in-control processing service
MC-PREVAL	Mastercard pre-validation services
MC-BLOCK	Mastercard transaction blocking service
MC-RPCS	Mastercard Recurring Payment cancellation service
MC-MDES	Mastercard tokenisation system (MDES)
CARD-APP	Application running on cardholder’s card device (e.g. phone application)
VISA-T	Visa Tokenisation system (Visa Europe/International Token Service)
CARD-WAL	Wallet application running on cardholder’s card device (e.g. phone)
WALLET	Wallet Service Provider (generic) systems - not on cardholder device (e.g. WAL-AP or WAL-AN or WAL-SA)

Source	Description
WAL-AP	Apple Wallet Systems (Apple servers - not on cardholder device)
WAL-AN	Android Wallet Systems (Google servers - not on cardholder device)
WAL-SA	Samsung Wallet Systems (Samsung servers - not on cardholder device)
CRDHLR	Cardholder
MC	Mastercard
VISA	Visa

4.32 Response_Source_Why and Message_Why

This field describes the reason why the response and message source sent the message. It indicates:

- Why the Response_Source sent the 0110 response message to the terminal.
- Why the Message_Source created this (usually advice/reversal) message in the first place.

It may be present in Authorisation Advice and/or Authorisation Reversal messages.

4.32.1 Possible Values

Why	Description
0	Unknown / not-applicable / not-a-fault
1	Issuer signed off
2	Issuer signed off by switch
3	Issuer communications line down or unavailable
4	Issuer sent DE39 instruction to force network Stand In Processing (STIP)
5	Issuer timed out
6	PCAS/Limit-1 diverted (transactions under the limit sent to network STIP)
7	Issuer is in *Suppress Inquiry* mode
8	Issuer selected option
9	MIP/VAP error
10	Issuer Edit Response Error (if Mastercard, DE60.3 may contain DE in error)
11	Issuer system error
12	Network not dispatched error
13	Issuer undelivered
14	Direct down option
15	Network unable to map virtual PAN
16	Automated Fuel Dispenser (AFD) transaction acquired in USA met Visa Transaction Advisor Service criteria
17	Visa Payment Controls (VPC) rule
18	Selective acceptance service
19	Automated Referral Service
20	Original processed in STIP
21	Network Account Management system

Why	Description
22	PIN verification error
23	Unable to translate PIN
24	CVV error
25	Source or destination does not support service
26	ARQC verification error
27	Network error
28	Network unable to deliver response to acquirer
29	Duplicate detected by network
30	Invalid merchant
31	Network transaction blocking service
32	Acquirer acknowledgement of 0110 not received
33	Foreign system sent message
34	AFD confirmation advice
35	Exception file maintenance
36	Reversal matched original authorisation request
37	No matching original authorisation request found
38	Issuer notification of token vault provisioned or status change
39	Issuer notification of card-on-file token issuance
40	Pay with rewards processing advice to issuer
41	Network MDES advice to issuer
42	Authentication advice to issuer
43	CAT Risk Level 3
44	EMV Offline advice to issuer
45	In-Control processing advice to issuer
46	Adminstrative text message
47	Transaction voided by customer
48	Transaction not completed
49	No confirmation from terminal

Why	Description
50	Partial Reversal
51	Payment Token Status Change In this case (MTID='0100', Txn_Type='A', Proc_Code='360000' Token Event Notification) it indicates that the PaymentToken_creatorStatus has been changed by the payment token creator. The Thredd status may also have changed too. • PaymentToken_id - indicates which payment token the status change is for • PaymentToken_creatorStatus - indicates the new status as set by the creator • PaymentToken_status - indicates the current Thredd status as set on Thredd Portal or Smart Client
52	Payment Token Replaced In this case (MTID='0100', Txn_Type='A', Proc_Code='360000' Token Event Notification) it indicates that a new payment token has been digitised (i.e. personalised) with the following properties: • There was already a previously digitised payment token on the same device • The properties of the new digitised token as the same as the previous one, except that the expiry date has been updated. • PaymentToken_id is the same (as same underlying payment token entry on the Thredd system) • PaymentToken_expdate has the new payment token expiry date • The previous expiry date is not included (if this is required, you should request it)
53	Activation code expired (e.g. for a payment token activation)
54	Activation code wrong (e.g. for a payment token activation)
55	Activation code maximum attempts exceeded (e.g. for a payment token activation)
56	Incremental authorisation
57	Resubmission
58	Delayed charges
59	Re-authorisation
60	No show
61	Account top up
62	Consumer Transaction Controls service
63	Dispute financial
64	Recurring payment Blocking Service
65	Merchant country on Issuers exclusion list
66	Office of Foreign Assets Control (OFAC) embargo
67	Cashback processing error
68	Invalid CAVV
69	Luhn check digit failure

Why	Description
70	Issuer does not support gambling transactions
71	Payment token created
72	Payment token provisioning result
73	Payment token activation code verification result
74	Payment token call centre activation result
75	Payment token mobile banking activation result
76	Payment token EMV session keys replenishment confirmation
77	Payment token provisioning-update results
78	PAN expiry date changed
79	PAN replaced
80	Payment token activated
81	Payment token suspended
82	Payment token deactivated
83	Network Payment Fraud Disruption service
84	Payment-Token Device binding
85	Payment-Token Device binding removed
86	Payment-Token Device binding complete without authentication
87	Payment-Token Device binding activation code verification result
88	Payment-Token Device binding call centre activation result
89	Payment-Token Device binding mobile banking verification result
90	Cardholder verification complete without authentication
91	Cardholder verification activation code verification result
92	Cardholder verification call centre activation result
93	Cardholder verification mobile banking activation results
94	Payment-Token re-personalised after personalisation data update
95	Payment-Token expiry date updated
96	Deferred Authorisation. (i.e. authorisation is received a long time after the cardholder interacted with the terminal. Could easily be many hours later. Common for mass-transit transactions, such as commuter railways and buses.)

Why	Description
97	Acquirer authorisation advice (Merchant/Acquirer approved authorisation offline)
100	Device binding with FIDO intent.
101	Device binding - implicit green flow.
other	Ask Thredd for updated information codes

4.33 Scheme Transaction Identifier Values

The following are Scheme Transaction Identifier values for Visa and Mastercard.

4.33.1 Visa

Value	Description
AA	Account to account
AL	AFT (Account Funding Transactions) or OCT (Original Credit Transactions) eligibility
BB	Business to business
BI	Bank initiated money transfers
BP	Non-card bill payment
CB	Consumer bill payment
CD	Cash deposit
CI	Cash in
CO	Cash out
CP	Card bill payment
FD	Funds disbursement (general)
GD	Government disbursement
GP	Gambling payout (other than online gambling)
LA	Liquid assets
LO	Loyalty and offers
MD	Merchant disbursement
MI	Merchant initiated OCT for faster refund
MP	Merchant payment
OG	Online gambling payout
PD	Payroll/pension disbursement
PG	Payment to government
PP	Person to person
PS	Payment for goods and services (general)
RP	Request to pay

Value	Description
TU	Top-up for enhanced prepaid loads
VA	Visa Accept
WT	Wallet Transfer

4.33.2 Mastercard

Value	Description
CO4	Gaming replay
C07	General person-to-person transfer
C51	Mastercard send indicator (reserved for future use)
C52	General transfer to own account
C53	Agent cash out
C54	Payment of own credit card bill
C55	Business disbursement
C56	Government/non-profit disbursement
C57	Rapid merchant settlement
C58	Cash in at ATM
C59	Cash in at point-of-sale
C60	Fast refund to original card
C61	Mastercard send indicator (reserved for future use)
C62	Mastercard send indicator (reserved for future use)
C63	Mastercard send indicator (reserved for future use)
C64	Mastercard send indicator (reserved for future use)
C65	General business-to-business transfer
C66	Mastercard send indicator (reserved for future use)
F07	General person-to-person transfer
F08	Person-to-person transfer to card account
F52	General transfer to own account

Value	Description
F53	Agent cash out
F54	Payment of own credit card bill
F55	Business disbursement
F61	Transfer to own staged digital wallet account
F64	Transfer to own staged debit or prepaid account
F65	General business-to-business transfer
P10	Purchase repayment
P11	Business-to-business payment
P70	Direct purchase of floating cryptocurrencies and other crypto tokens (for example, Bitcoin or Ethereum)
P71	High-risk securities
P76	Direct purchase of fully fiat-backed stablecoins and Central Bank Digital Currencies (CBDCs) (for example, USDC, PYUSD, eNaira)

4.34 SenderData and ReceiverData Fields

The SenderData and ReceiverData fields provide details of the sender and receiver in a money transfer message. Both fields are represented as a TLV with following order and lengths:

- Tag - two characters
- Length - two decimal digits
- Value - the number of characters as given by the length

The table below describes the subfields (tags).

Tag	Field Name	Description
1	FirstName	First name
2	MiddleName	Middle name
3	LastName	Last name
4	StreetAddress	Street address
5	City	City
6	Province	Province
7	Country	Three letter ISO country code (e.g., CYP = Cypress)
8	PostCode	Postcode
9	PhoneNumber	Phone number
10	DateOfBirth	Date of birth (MMDDYYYY). For example 12311996.
11	AccountNumber	Account number
12	IdType	Type of Identity Document (ID). (00 = passport; 01 = National Identification Card; 02 = Driver's License; 03 = Government Issued; 04 = Other; 05-10 reserved for future use)
13	IdNbr	ID number
14	IdCtryCode	ID three-letter country code (e.g., MLT = Malta)
15	IdExpDate	ID expiry date (MMDDYYYY)
16	Nationality	Nationality (three character alpha ISO code)
17	BirthCtry	Country of birth (three character alpha ISO code)
18	AcctNbrType	Type of account number. See Account Number Type.
V1	FundsSource	Source of funds. See Source of Funds.
V2	ClaimCode	Claim code

Example

0106Mickey0305Mouse0411Main Street0508Annaheim0703USA

4.35 Special Characters

Special characters include any printable characters not counted as alphanumeric. Special characters may be used in fields of Data Type ANS (Alphanumeric and Special). Special characters received from the card schemes are based on the following standards:

- For Mastercard Banknet - any printable ISO8859-1 character (excluding alphanumeric)
- For Visa Base1 - any printable IBM EBCDIC code page 1148 character (excluding alphanumeric). See the figure below.

HEX DIGITS 1ST → 2ND ↓	4-	5-	6-	7-	8-	9-	A-	B-	C-	D-	E-	F-
-0	(SP) SP010000	& SM030000	- SP100000	ø LO610000	Ø LO620000	° SM190000	µ SM170000	¢ SC040000	{ SM110000	} SM140000	\ SM070000	0 ND100000
-1	(RSP) SP300000	é LE110000	/ SP120000	É LE120000	a LA010000	j LJ010000	~ SD190000	£ SC020000	A LA020000	J LJ020000	÷ SA060000	1 ND010000
-2	â LA150000	ê LE150000	Â LA160000	Ê LE160000	b LB010000	k LK010000	s LS010000	¥ SC050000	B LB020000	K LK020000	S LS020000	2 ND020000
-3	ä LA170000	ë LE170000	Ä LA180000	Ë LE180000	c LC010000	l LL010000	t LT010000	· SD630000	C LC020000	L LL020000	T LT020000	3 ND030000
-4	à LA130000	è LE130000	À LA140000	È LE140000	d LD010000	m LM010000	u LU010000	© SM520000	D LD020000	M LM020000	U LU020000	4 ND040000
-5	á LA110000	í LI110000	Á LA120000	Í LI120000	e LE010000	n LN010000	v LV010000	§ SM240000	E LE020000	N LN020000	V LV020000	5 ND050000
-6	ã LA190000	î LI150000	Ã LA200000	Î LI160000	f LF010000	o LO010000	w LW010000	¶ SM250000	F LF020000	O LO020000	W LW020000	6 ND060000
-7	å LA270000	ï LI170000	Å LA280000	Ï LI180000	g LG010000	p LP010000	x LX010000	¼ NF040000	G LG020000	P LP020000	X LX020000	7 ND070000
-8	ç LC410000	ì LI130000	Ç LC420000	Ì LI140000	h LH010000	q LQ010000	y LY010000	½ NF010000	H LH020000	Q LQ020000	Y LY020000	8 ND080000
-9	ñ LN190000	ß LS610000	Ñ LN200000	` SD130000	i LI010000	r LR010000	z LZ010000	¾ NF050000	I LI020000	R LR020000	Z LZ020000	9 ND090000
-A	[SM060000	] SM080000	¦ SM650000	: SP130000	« SP170000	ª SM210000	¡ SP030000	¬ SM660000	(SHY) SP320000	1 ND011000	2 ND021000	3 ND031000
-B	. SP110000	$ SC030000	, SP080000	# SM010000	» SP180000	º SM200000	¿ SP160000	| SM130000	ô LO150000	û LU150000	Ô LO160000	Û LU160000
-C	< SA030000	* SM040000	% SM020000	@ SM050000	ð LD630000	æ LA510000	Ð LD620000	¯ SM150000	ö LO170000	ü LU170000	Ö LO180000	Ü LU180000
-D	(SP060000	) SP070000	_ SP090000	' SP050000	ý LY110000	¸ SD410000	Ý LY120000	¨ SD170000	ò LO130000	ù LU130000	Ò LO140000	Ù LU140000
-E	+ SA010000	; SP140000	> SA050000	= SA040000	þ LT630000	Æ LA520000	Þ LT640000	´ SD110000	ó LO110000	ú LU110000	Ó LO120000	Ú LU120000
-F	! SP020000	^ SD150000	? SP150000	" SP040000	± SA020000	€ SC200000	® SM530000	× SA070000	õ LO190000	ÿ LY170000	Õ LO200000	(EO)

Figure 20: IBM Special Characters - EBCDIC code page 1148

Note: Ignore the EBCDIC encoding value for the characters, as Thredd sends you the values encoded in UTF-8 format.

For more information on ISO-8859-1 character sets, see: charset.org: Character sets > ISO-8859-1 (Western Europe)

For more information on IBM character sets defined in EBCDIC code page 1148, see ibm.com: docs > Character sets

4.36 Transaction Matching - Authentications and Authorisations

There are a number of the checks you can perform as part of PSD2 Dynamic SCA Linking to verify whether the details provided in the original 3D Secure authentication matches the details that were provided during the transaction authorisation. For example, matching of the authorised amount to the authenticated amount, and matching of the merchant name.

4.36.1 Matching the Authorised Amount

From EHI version 5.0 we provide an AuthenticationAmountUpper field, which can be used to determine whether the amount authorised in a 3D Secure authentication session matches the amount that was authorised in the authorisation message.

Note: In addition to doing your own checks, you can use the value returned in the GPS_POS_Data field position 26 to identify if the authentication amount does not match the authorisation amount.

For Visa, the amount will always be the exact amount, but for Mastercard, if the amount is above 14000 in minor units, the amount may be an estimate, due to their rounding algorithm. See the examples below.

Currency	Amount	Value in Minor Units	Rounding?
Japanese Yen (0dp currency	14000	<=14000 Yen	No, exact amount
Japanese Yen (0dp currency)	14011	> 14000 Yen	Yes, Upper bound
GBP (2dp currency)	140	<= 140.00 Pounds	No, exact amount
GBP (2dp currency)	140.11	> 140.00 Pounds	Yes, Upper bound
Jordanian Dinar (3dp currency)	14.000	<= 14.000 Dinar	No, exact amount
Jordanian Dinar (3dp currency)	14.010	> 14.000 Dinar	Yes, Upper bound

4.36.2 Matching Merchant Name

The merchant name hash is returned in the response to a 3D Secure authentication session. Below are guidelines for how to match the merchant name in the Merch_Name_DE43 field of the Authorisation message to the merchant name hash returned in the AuthenticationMerchantHash field for a 3D Secure authentication.

Guidelines

Since the merchant name is provided as a hashed value, you will need to hash the Merch_Name_DE43 field using the SHA-256 algorithm and then compare it to the hashed value in the AuthenticationMerchantHash field.

- The merchant name field may contain '00000000' or an IP address, depending on your setup at the card scheme. In this case it will not be possible to match.
- For Mastercard, the merchant name that was hashed at authentication time might not match the name provided in the authorisation if the 3D Secure provider and the acquirer were using different naming conventions.
- The merchant name must have the same letters and Case in order for the hash to match. For example, "Microsoft*Store" and "MICROSOFT*STORE" will return different hashed values:
  • "Microsoft*Store" is hashed as 3a884dcdb1bcea65c907e61d90c1c6cd4b3acf4a1b5696406cfb453743c82ccb.
  • "MICROSOFT*STORE" is hashed as 7b7a55d1690a2f6061550fb824322b9d71f7ae0b3e9a7584fad54a970011c544.

See the examples below of common merchant name hashes:

Mastercard Examples

Merchant name	Hex of ASCII chars	SHA256 hash
Microsoft	4D6963726F736F6674	C7BAC46904BE785CD0C965BF5659610044F0CDB4CBB02D2EC398DC56648988FD
Microsoft*Store	4D6963726F736F66742A53746F7265	3A884DCDB1BCEA65C907E61D90C1C6CD4B3ACF4A1B5696406CFB453743C82CCB
Microsoft*Xbox	4D6963726F736F66742A58626F78	F32B0B5416D7C9C15A653AF18EDD52ABBF88CA2178EA0686C42F98D7F7284159
MICROSOFT*XBOX	4D4943524F534F46542A58424F58	EC4CFC1BBB33769BDD299E0443A652341B84144AE846C566920EED69680524DB
PLAYSTATIONNETWORK	504C415953544154494F4E4E4554574F524B	B50D55B889F8B068EB8144145E2BD007C0C332BEC5284F06C8DC45C6D1AC6FC3
CRV	435256	0107A39935A165F3AB2A3DD226802294E2BD417A0DB8EB6B71A16420DB3FB070
CRV*	4352562A	1B49BAF46A3B718691623FF9E3BC9A70DF0816AB30B9305FE2A95E5EA100C48C
Just Eat	4A75737420456174	7FBFB81FC52DFEFEF50ACA038126ABCD46505B3FB5672DAA3E473558E507EB48
PADDLE.NET* RENDRFORST	504144444C452E4E45542A2052454E4452464F525354	B18D1EF6F5A03AD39FBC4E8DBB94BE7A1CD5E098C3120C7CAA926A16589509B0
Nintendo of Europe Gmb	4E696E74656E646F206F66204575726F706520476D62	152FFDEBDC5E99FB2B44E40E02F7B2010E13D43641F7A2706CEB012FD1EA022C
Mango.com	4D616E676F2E636F6D	937ED44169DB30AAFB3F423FD24954F38BD7B2E69A397F604611240BE2565710

Visa Examples

Note: For Visa, most merchants are using the Merchant_Name field in UPPERCASE, after removing non-alphanumeric characters. Some merchants may use a different name to that provided in the Merchant_Name field (see the example of PlaystationNetwork/SONY)

DE43 merchant name (as provided in Merchant_Name)	AuthenticationMerchantHash	Actual merchant name used to generate the DE126.9 Merchant name hash (found by Thredd by Trial and Error)
Play Online Solutions	17722204	PLAYONLINESOLUTIONS
PlaystationNetwork	24837652	SONY
MICROSOFT*STORE	36838472	MICROSOFT

DE43 merchant name (as provided in Merchant_Name)	AuthenticationMerchantHash	Actual merchant name used to generate the DE126.9 Merchant name hash (found by Thredd by Trial and Error)
CK Stores B.V.	31186286	CKSTORESBV
PayU*Allegro	93816075	PAYUALLEGRO

4.37 Transaction Status Codes

The table below provides details of available Transaction Status Code (`Txn_Stat_Code`) values. (See also Get Transaction Message fields: Txn_Stat_Code)

Value	Description	Impacts Balance?
A	Accepted	Yes. Authorised amount is blocked.
C	Cleared	No
I	Declined	No
S	Settled	Yes. The actual balance is adjusted by the settled amount.
V	Reversed	Yes. Reversed amount is unblocked (if matching authorisation found)

Note: When Thredd receives a presentment which matches an existing authorisation message, the Authorisation message status is updated to *Cleared (C)* and the Presentment message status is updated at the same time to *Settled (S)*. If Thredd controls the balance, we will adjust the balance by the settlement amount. If your systems control the balance, you can adjust the balance by the settled amount.

4.38 Transaction Types

The table below provides details of available Transaction Type (`Txn_Type`) values. (See also Get Transaction Message fields: Txn_Type)

Value	Description	Mapping	Impacts Balance
A	Authorisation	Authorisation (if MTID=0100) Financial (if MTID=1240)	Yes (If approved)
B	Balance Adjustment	Bal Adjustment/Expiry	Yes
C	Chargeback	Financial	Yes
D	Auth Reversal	Authorisation	Yes (If matching auth exists)
E	Financial Reversal	Financial	Yes
G	Payment	Load/Unload	Yes
H	Chargeback - Non Credit	Financial	No
J	Authorisation Advice	Authorisation	Yes (if approved)
K	Chargeback Reversal	Financial	Yes
L	Load	Load/Unload	Yes
N	Sec Presentment	Financial	Yes
P	Presentment	Financial	Yes
U	Unload	Load/Unload	Yes
Y	Card Expiry	Bal Adjustment/Expiry	Yes

4.39 Trans_Link Field

The Trans_Link field is a string between 0-19 digits, the length and value of which depends on the type of transaction as described in the table below.

Transaction Description	Type	Other Criteria	Trans_Link Content	Trans_link Examples
Dummy authorisation (Created from unmatched First Presentment)	A	Description begins '*OFFLINE*', MTID 1240 (Mastercard) or 5, 6 or 7 (Visa)	19 digits: '1' + *date* + *digit locator* + *Acquirer BIN* Where: • '1' – is the offline transaction indicator • *date (yymmdd)* – is the 6 digit acquirer process date from the Acquirer Reference Number (ARN) • *Digit locator*– is the last 6 digits of ARN • *Acquirer BIN*– is the 6 digit acquiring BIN/ID from ARN **Note**: Ensure it does not match other normal values.	1230310339532446366 1230310321639446366 1230311008318483857
Most normal authorisation requests and advices	A, J	MTID 0100, 0101, 0120	18 digits: *date* (*yymmdd*) + *6 digit STAN* + *6 digit Acquirer ID* **Note**: the 0120 advice and 0100 request should have the same trans_Link values.	230311604412007460
Most normal authorisation reversals	D	MTID 0400, 0420	18 digits: *date (YYMMDD*) + *6 digit OrigSTAN* + *6 digit Acquirer ID* Where: *OrigSTAN* comes from DE90.2 and contains the same STAN (DE11) as the original being reversed. **Note**: 0400 and 0420 reversals should have same trans_Link values as the original authorisation request or advice.	
Some declined authorisations	A	Some declined MTID 01xx with Acquirer ID present	16 digits: *date (YYMM) + 6 digit STAN + 6 digit Acquirer ID*	2302994754416361 2302134370016901
Visa 0620 TCN or TEN	J	MTID 0620 with no Acquirer ID present (These are always ProcessingCode 35xxxx or 36xxxx, from Visa)	12 digits: *date (YYMMDD) + 6 digit STAN*	230225030928 230225005491
Recurring Fees, Activation Fees	P	Meets both of these criteria: ProcessingCode ends with '999' ProcessingCode indicates Recurring or	Fixed value of '0'	0 0 0

Transaction Description	Type	Other Criteria	Trans_Link Content	Trans_link Examples
		Activation Fees		
Fees related to Balance Transfers or Loads	P	Meets both of these criteria: ProcessingCode ends with '999' (A Fee) ProcessingCode indicates Balance Transfer Fees or Load Fees	Transaction ID of the related Balance Transfer or Load	12659871933 12659347510
First Presentments that matches a prior authorisation	P	Meets both of these criteria: ProcessingCode does not end with '999' (not a Fee) Matched to an authorisation	Set to the trans_Link value of the original authorisation	230310784631401134 230309725008494605 230308638653443973
First presentment with no matching auth (and not a refund)	P	Meets both of these criteria: ProcessingCode does not begin with '20' and does not end with '999' (Not a Refund, not a Fee) No matching authorisation	19 digits: '1' + *date* + *digit locator* + *Acquirer BIN* Where: • '1' – is the offline transaction indicator • *date (yymmdd)* – is the 6 digit acquirer process date from the Acquirer Reference Number (ARN) • *Digit locator* – is the last 6 digits of ARN • *Acquirer BIN* – is the 6 digit acquiring BIN/ID from ARN **Note**: ARN is the unique Acquirer Reference Number received in the clearing message.	1230310339532446366 1230310321639446366
First Presentment of a refund, with no matching auth, but a matching non-refund first presentment	P	Meets both of these criteria: ProcessingCode begins with '20' (Refund) No matching authorisation, but a matching non-refund first presentment	Set to the trans_link of the matching first presentment.	
First Presentment of a refund, with no matching authorisation, and no matching non-refund first presentment	P	Meets both of these criteria: ProcessingCode begins with '20' (Refund) No matching authorisation, and no matching non-refund first presentment	18 digits: *transaction date ("YYMMDDmssxxx") + last 6 digits of DE031 ARN*	230218621277522576 230218621287522584 230218621297522592
Chargeback	H, C		Set to the trans_Link value of the matching Presentment.	221023402304009260 1230108385918520914
Financial Reversal (received in	E	Matching financial found	Set to the trans_Link value of the matching Presentment.	1230310299729410157

Transaction Description	Type	Other Criteria	Trans_Link Content	Trans_link Examples
clearing file), and matches a previous financial				
Financial Reversal (received in clearing file), but no matching financial found	E	No matching financial found	18 digits: *YYMMDDmssxxx + last 6 digits of ARN*.	230311243300809653
Second Presentment, matching a chargeback	N	Matching chargeback found	Set to the trans_Link value of the matching chargeback.	221023402304009260 1230108385918520914
Second Presentment, but related chargeback not found	N	No matching chargeback found	18 digits: *YYMMDDmssxxx + last 6 digits of ARN*.	230307223653154848 230303431430593766
Balance Adjustment (debit)	B	ProcessingCode='190000'	Transaction ID value of this transaction.	12613916745
Balance Update from EHI response, net debit	B	ProcessingCode begins with '60'	Transaction ID value of the related transaction that caused this Balance Adjustment. (Due to new Balance Update information being sent back in an EHI response message to an online authorisation.)	12613979001
Balance Update from Web Service call, net debit	B	ProcessingCode begins with '61'	Set to empty string.	*Empty string*
Balance Update from EHI response, net credit	B	ProcessingCode begins with '65'	Transaction ID value of the related transaction that caused this Balance Adjustment. (Due to new Balance Update information being sent back in an EHI response message to an online authorisation.)	12613917117
Balance Update from Web Service call, net credit	B	ProcessingCode begins with '66'	Set to empty string.	*Empty string*
Payment Transaction	G		Transaction ID value of this transaction.	12613921478 12668419405
Load, relating to a prior Unload	L	Relates to a prior Unload	Transaction ID value of the related unload.	12639991950 12668158805
Load (not related to an Unload)	L	Unrelated to a prior Unload	Transaction ID value of this transaction.	12613916737
Unload, relating to a prior Load	U	Relates to a prior Load	Transaction ID of the related load.	12672545523

Transaction Description	Type	Other Criteria	Trans_Link Content	Trans_link Examples
Unload (not related to an Load)	U	Unrelated to a prior Load	Transaction ID value of this transaction.	12613916878

Matching the Trans_Link to a Previous Transaction

Refer to the table below for a summary of how to match the Trans_Link value in the current transaction to the value in a previous transaction.

Current Transaction Type	How it matches to a previous transaction
Authorisation Advices (TxnType ‘J') and Authorisation Reversals (TxnType 'D’	Has the same value as the original Authorisation Request it relates to (if any).
Presentments (TxnType 'P')	Has the same value as the original Authorisation Request or Advice it relates to.
Chargebacks (TxnType ‘C' or ‘H’)	Has the same value as original Presentment (TxnType ‘P’ or 'N’).
Balance Adjustments (TxnType 'B')	Has the same value as the related transaction.
For Loads (TxnType 'L')	Has the same value as the prior related Unload.
Unloads (TxnType 'U')	Has the same value as the prior related Load.

4.40 Visa_POS_Data_DE60

The Visa_POS_Data_DE60 field contains the raw Visa POS data Thredd received in Visa online authorisation related messages. It can be useful for diagnosis in exception cases. Thredd processes this field to set the GPS_POS_Data and GPS_POS_Capability fields.

Note: The values supplied in this field are subject to change by Visa. We advise you not to configure your systems to make decisions based on this field.

4.40.1 Visa_POS_Data_DE60 Positions

Each different position holds a different piece of POS information. Note that not all positions may arrive.

For more information on this field, refer to Visa. Only a summary of the relevant values are given below.

The position is the character offset in the field; the first character is “position 1”.

Position	Description	More Information
1	Terminal Type	See Position 1 - Terminal Type
2	Terminal Entry Capability	See Position 2 - Terminal Entry Capability
3	Chip Condition Code	See Position 3 - Chip Condition Code
4	Special Condition indicator - existing debt	See Position 4 - Special condition (existing debt)
5 - 6	RFU	
7	Chip Transaction Indicator	See Position 7 - Chip Transaction indicator
8	Chip Card Authentication reliability indicator	See Position 8 - Chip card authentication reliability indicator
9 - 10	Mail/Phone/E-Commerce/Payment indicator	See Position 9-10 - Mail/Phone/E-Commerce/Payment indicator
11	Cardholder ID method indicator	See Position 11 - Cardholder ID Method Indicator
12	Additional authorisation indicators	See Position 12 - Additional Authorisation Indicators
13 and up	Unknown	Reserved for future use

4.40.2 Position 1 - Terminal Type

Value	Description
0	Unspecified
1	Unattended cardholder-activated, no authorization, below-floor-limit transaction (not allowed in zero floor markets)
2	ATM
3	Unattended cardholder-activated, authorized transaction
4	Electronic cash register
5	Home terminals, which include personal computers, personal digital assistants, interactive televisions, and telephones

Value	Description
7	Telephone device (including Visa dial terminals)
8	Reserved for future use
9	Mobile acceptance solution (mPOS)
Any other value	Unknown

4.40.3 Position 2 – Terminal Entry Capability

Value	Description
0	Unknown
1	Terminal not used
2	Magnetic Stripe read capability
3	Barcode read capability
4	OCR-read capability
5	Chip-capable terminal
8	Proximity-read-capable terminal
9	Terminal does not have the capability to read card data
Any other value	Unknown

4.40.4 Position 3 – Chip Condition Code

Value	Description
0	Not applicable
1	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	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.
Any other value	Unknown

4.40.5 Position 4 – Special Condition (existing debt)

Value	Description
0	Default value
1	Purchase of Central Bank Digital Currency (CBDC) or tokenized depositsCentral Bank Digital Currency (CBDC) or tokenized deposits
2	Purchase of Stablecoin (Fiat-backed)
3	Purchase of Blockchain Native Token/Coin
4	Purchase of Non-Fungible Token (NFT)
7	Purchase of Cryptocurrency
8	Quasi-Cash
9	Existing debt indicator
Any other value	Unknown

4.40.6 Position 7 – Chip Transaction Indicator

Value	Description
0	Not applicable
1	Standard third bitmap or field 55 used to submit chip data
2	Expanded third bitmap used to submit chip data
3	Visa dropped chip data due to invalid format for chip card type
4	Token-based transaction
Any other value	Unknown

4.40.7 Position 8 – Chip Card Authentication Reliability Indicator

Value	Description
0	No information / not applicable
1	Acquirer indicates that Card Authentication may not be reliable
2	Visa indicates acquirer inactive for Card Authentication
3	Visa indicates issuer inactive for Card Authentication
Any other value	Unknown

4.40.8 Position 9-10 – Mail/Phone/E-Commerce/Payment Indicator

Value	Description
00	Not applicable
01	Mail/Phone Order (MOTO). Indicates that the transaction is a mail/phone order purchase, not a recurring transaction or installment payment.
02	Recurring transaction from acquirer in Visa US region
03	Installment payment. Indicates a purchase of goods or services that is billed to the account in multiple charges over a period of time agreed upon by the cardholder and merchant.
04	Unknown classification/other mail order. Indicates that the type of mail/telephone order is unknown.
05	Secure electronic commerce transaction. Indicates that the electronic commerce transaction has been authenticated using a Visa-approved protocol, such as 3D Secure.
06	Non-authenticated security transaction at a 3D Secure-capable merchant, and merchant attempted to authenticate the cardholder using 3D Secure Identifies an electronic commerce transaction where the merchant attempted to authenticate the cardholder using 3D Secure, but was unable to complete the authentication because the issuer or cardholder does not participate in the 3D Secure program.
07	Non-authenticated Security Transaction Identifies an electronic commerce transaction that uses data encryption for security; however, cardholder authentication is not performed using a Visa-approved protocol, such as 3D Secure.
08	Non-secure transaction Identifies an electronic commerce transaction that has no data protection. (This value is not allowed in Europe)
09	Reserved for future use
Any other value	Unknown

4.40.9 Position 11 – Cardholder ID Method Indicator

Value	Description
0	Unspecified
1	Signature
2	Online PIN
3	Unattended terminal, no PIN pad
4	Mail/Telephone/Electronic Commerce
Any other value	Unknown

4.40.10 Position 12 – Additional Authorisation Indicators

Value	Description
0	Not applicable
1	Terminal accepts partial authorization responses, amount is not an estimate.
2	Estimated amount, terminal does not support partial authorization responses.
3	Estimated amount and terminal accepts partial authorization responses
Any other value	Unknown

4.41 Visa_ResponseInfo_DE44

The Visa_ResponseInfo_DE44 field contains a summary of verifications performed by the Visa system on the transaction, before it reached Thredd. It is a useful source of additional information for Visa authorisation-related transactions.

Note: The values supplied in this field are subject to change by Visa. We advise you not to configure your systems to make decisions based on this field.

Note: Only some of the values below apply to the Thredd to Visa connection.

4.41.1 Visa_ResponseInfo_DE44 Positions

Each position holds the result of a verification check at Visa. The Visa system may vary on which checks it performs on which transactions.

The position is the character offset in the field; the first character is *position 1*. A space character in any position indicates the information is not provided.

In the table below, *Issuer* indicates Thredd, *STIP* indicates the Visa Stand-In Processing system and *Switch* refers to the Visa Network.

Note: Only a summary of the relevant values are given below. For more information, refer to the Visa documentation.

Position	Description	More Information
1	Response Source/Reason	See Position 1 - Response Source/Reason Code.
2	AVS result	See AVS_Results.
3	Reserved for future use	See Visa documentation
4	Reserved for future use	See Visa documentation
5	CVV/iCVV/dCVV result	Values: Space = CVV, iCVV or dCVV was not verified 0 = CVV, iCVV or dCVV could not be verified 1 = CVV, iCVV, dCVV, or Online CAM failed verification, or Offline PIN authentication was interrupted 2 = CVV, iCVV, dCVV, or Online CAM passed verification. 3 = Transaction passed CVV, Emergency Replacement Card (ERC) service value only, which is used exclusively by the Global Customer Assistance Service (GCAS).
6 - 7	PACM diversion level	See Visa documentation
8	PACM diversion reason	See Visa documentation
9	Card Authentication Results	Values: Space = no information 1 = EMV ARQC checked and failed verification 2 = EMV ARQC checked and passed verification
10	Reserved for future use	See Visa documentation
11	CVV2 Result	See Position 11 - CVV2 Result Code
12-13	Original Response code	See Visa documentation
14	Cheque settlement code (USA only)	See Visa documentation

Position	Description	More Information
15	CAVV result	See Position 15 – CAVV Result Code
16 - 19	Response Reason Code	See Visa documentation. (Not applicable to Thredd)
20 - 23	Last 4 digits of PAN for receipt	Holds the last four digits of the cardholder PAN, for some payment-token transactions.
24	CVM requirement for PIN-less	Values: Space = no information 0 = No CVM required 1 = Signature prompt required
25 and up	Unknown	See Visa documentation

4.41.2 Position 1 – Response Source/Reason Code

This position explains who responded to the acquirer and why. Thredd already map this into the Response_Source and Response_Source_Why fields.

In the table below, Issuer indicates Thredd, and STIP indicates the Visa Stand-In Processing sytem.

Value	Description
space	No information
0	Advice of Exception file change initiated by Global Customer Assistance Service (GCAS) or Automatic Cardholder Database Update (Auto-CDB) Service
1	Response provided by STIP because the request was timed out by Switch (ATR) or the response contained invalid data
2	Response provided by STIP because the transaction amount was below issuer limit (PCAS processing), or transaction amount is below sliding dollar limit (PACM processing), or in response to a verification request
4	Response provided by STIP because issuer was not available for processing
5	Response provided by issuer
7	Reversal message matched to the original authorization request message
8	No matching original authorization request message found. V.I.P. attempts to match reversals with originals when possible; however, 8 does not guarantee that an original was not received
A	Automated Fuel Dispenser Advice
B	Response provided by STIP: Transaction met Visa Transaction Advisor Service criteria
C	Response provided by STIP for conditions not listed. See the Thredd fields Response_Source_Why and Visa_STIP_Reason_Code for why (see section Visa_STIP_Reason_Code field)
Any other value	Unknown

4.41.3 Position 11 - CVV2 Result Code

Result of Visa's CVV2 verification.

Value	Summary
space	No information
M	CVV2/dCVV2 match verified by issuer or Visa
N	CVV2/dCVV2 verified but did not match
P	CVV2/dCVV2 not performed due to system settings or STIP
S	System error (e.g., missing expiry date or CVV2)
U	Issuer [actual issuer, not Thredd] does not participate or lacks encryption keys
Any other value	Unknown

4.41.4 Position 15 - CAVV Result Code

Result of Visa's CAVV (3D-secure) verification.

Value	CAVV result
space	No information
0	CAVV could not be verified or CAVV data was not provided when expected
1	CAVV failed verification–authentication.
2	CAVV passed verification–authentication.
3	CAVV passed verification–attempted authentication. A 3D Secure (3DS) authentication value of 07 from the Issuer Attempts Server indicates that authentication was attempted. Issuer attempts CAVV key was used to generate the CAVV.
4	CAVV failed verification–attempted authentication. A 3D Secure (3DS) authentication value of 07 from the Issuer Attempts Server indicates that authentication was attempted. Issuer attempts CAVV key was used to generate the CAVV.
5	RFU
6	CAVV not verified, issuer not participating in CAVV verification (except as noted, only Visa generates this code, issuers do not).
7	CAVV failed verification–attempted authentication. A 3D Secure (3DS) Authentication Results Code value of 07 from Visa Attempts Service indicates that an authentication attempt was performed. (Visa CAVV attempts key was used to generate the CAVV)
8	CAVV passed verification–attempted authentication A 3D Secure (3DS) Authentication Results Code value of 07 from Visa Attempts Service indicates that an authentication attempt was performed.

Value	CAVV result
	(Visa CAVV attempts key was used to generate the CAVV)
9	CAVV failed verification–attempted authentication A 3D Secure (3DS) Authentication Results Code value of 08 from Visa Attempts Service indicates that an authentication attempt was performed when the Issuer Access Control Server (ACS) was not available. (Visa CAVV attempts key was used to generate the CAVV)
A	CAVV passed verification–attempted authentication A 3D Secure (3DS) Authentication Results Code value of 08 from Visa Attempts Service indicates that an authentication attempt was performed when the Issuer ACS was not available. Visa CAVV attempts key was used to generate the CAVV.
B	CAVV passed verification–attempted authentication, no liability shift. Only Visa generates this code, issuers do not.
C	CAVV was not verified–attempted authentication. If 3D Secure (3DS) Authentication Results Code value is 07 in the CAVV and the issuer did not return a CAVV results code in the authentication response, or, if, Field 44.13 = 0 in the response message and the CAVV encryption keys do not exist in V.I.P., V.I.P.. sets the value to C in Field 44.13. Only Visa generates this code, issuers do not.
D	CAVV was not verified–cardholder authentication. If 3D Secure (3DS) Authentication Results code value is 00 in the CAVV and the issuer did not return a CAVV results code in the authorization response, or, if, Field 44.13 = 0 in the response message and the CAVV encryption keys do not exist in V.I.P., V.I.P. sets the value to D in Field 44.13. Only Visa generates this code, issuers do not.
Any other value	Unknown

4.42 Visa_STIP_Reason_Code

The Visa_STIP_Reason_Code field provides Visa's reason codes for why an advice was generated. This information can be used to supplement the details returned in the Message_Why and Response_Source_Why fields of an advice message that originated from Visa.

Note: The values supplied in this field are subject to change by Visa. We advise you not to configure your systems to make decisions based on this field.

Note: Only some of the values below apply to the Thredd to Visa connection.

Definitions used below:

- Issuer - means Thredd in this scenario
- STIP – Visa's STand-In Processing system
- Switch – the Visa Network

Value	Action taken by Visa	Detailed reason (why action was taken)
9001	STIP processed transaction	Issuer is signed off [to Visa]
9002	STIP processed transaction	Issuer was signed off by Visa
9011	STIP processed transaction	Line [from] Visa to Issuer is down
9012	STIP processed transaction	Forced STIP because of N0 (Force STIP) original response from issuer
9020	STIP processed transaction	Response from Issuer timed out
9022	STIP processed transaction	PACM (Positive Authorisation Capacity Management) - diverted
9023	STIP processed transaction	PCAS (Positive Cardholder Authorisation Service) -diverted
9024	STIP processed transaction	Transaction declined due to Visa Payment Controls (VPC) rule
9025	STIP processed transaction	Declined by Selective Acceptance Service
9026	STIP processed transaction	Transaction reviewed by the Visa Transaction Advisor Service: additional authentication required.
9027	STIP processed transaction	Declined by token provisioning service
9030	STIP processed transaction	Based on the Issuer response, the account was either listed in the ASAF via the Auto-CDB Service or updated by the ASAF Downgrade feature.
9031	STIP processed transaction	Original processed in stand-in
9033	STIP processed transaction	Declined due to active account management threshold exceeded
9034	STIP processed transaction	Unable to deliver response to Acquirer
9035	STIP processed transaction	Process recurring payment in STIP
9037	STIP processed transaction	Declined by Visa CTC (Consumer Transaction Controls) service
9038	STIP processed transaction	Merchandise return authorization processed in STIP

Value	Action taken by Visa	Detailed reason (why action was taken)
9041	STIP processed transaction	There was a PIN verification error
9042	STIP processed transaction	Offline PIN authentication was interrupted
9045	STIP processed transaction	Switch was unable to translate the PIN
9047	STIP processed transaction	Declined by Real-Time Decisioning (RTD) processing
9048	STIP processed transaction	There is an invalid CVV with the All Respond Option
9054	STIP processed transaction	There is an invalid CAM [EMV ARQC invalid normally]
9063	STIP processed transaction	Transaction declined, processing requirements not met. This value is set by Visa when the value in field 39 is 96 and: • Transaction required to process in-country, but the in-country Visa system is unavailable, or, • Transaction not eligible to be processed by the in-country Visa System
9091	STIP processed transaction	Dispute financial
9095	STIP processed transaction	Issuer notification of token vault provisioned or status change
9050	STIP generated advice	Source or destination does not participate in this service
9061	Switch-Detected Error	There is an internal system error or other switch-detected error condition
9102	Switch-Generated Reversal Advice	Switch generated this 0420 reversal advice because an approval response could not be delivered to the acquirer. Visa Europe only
9103	Switch-Generated Reversal Advice	An approval response could not be delivered to the acquirer because the issuer timed out
9201	STIP Decline Advice	Decline due to PPCS (Stop recurring payment service)
9202	STIP Decline Advice	Decline due to issuer country exclusion list
9203	STIP Decline Advice	Decline due to Office of Foreign Assets Control (OFAC) embargo
9204	STIP Decline Advice	Cashback processing error
9205	STIP Decline Advice	Invalid CAVV with Visa Verify and decline options (V and W)
9206	STIP Decline Advice	Mod-10 check failure
9207	STIP Decline Advice	Issuer does not support gambling transactions
9208	STIP Decline Advice	Declined because issuing identifier and/or routing identifier is blocked
9209	STIP Decline Advice	Declined because issuer does not support transaction type
9210	STIP Decline Advice	Declined because of issuer participation options

Value	Action taken by Visa	Detailed reason (why action was taken)
9211	STIP Decline Advice	Declined because acquirer does not support the service requested
9212	STIP Decline Advice	Declined due to fraud condition
9213	STIP Decline Advice	Declined because call-out to an external service timed out
9214	STIP Decline Advice	Declined because of error return from call-out to external service
9215	STIP Decline Advice	Declined because issuer blocked specific POS entry mode
9218	STIP Decline Advice	Product subtype is MB (Interoperable mobile branchless) and business application identifier is not MP or business application identifier is MP and product subtype is not MB.
9219	STIP Decline Advice	Merchant Blocking Service Decline Reason Code
9302	STIP Decline Advice	Exceeds Settlement Risk Exposure Cap. This code appears in 0120 messages
Any other value	Unknown	Ignore this. **Note**: Visa may add other values at any time without prior warning, so you must ignore any values that you are not expecting.

SECTION 5: FAQS

This section provides answers to Frequently Asked Questions:

- General FAQs
- Troubleshooting FAQs

General FAQs

This section provides answers to frequently asked questions. It is divided into the following sections:

- EHI Setup
- EHI Modes
- Duplicate Checking and Transaction Matching
- EHI Cut Off Messages
- Transaction Processing
- Transaction Lifecycle

EHI Setup

Q. How do I change my EHI configuration?

Please discuss changes with your implementation manager or account manager.

Q. Can I use a private IP in the Test Environment?

A private IP is used internally within your own network and will require a secure connection for EHI to access. In the test environment Thredd recommends the EHI connection resolves to a public IP.

In the test environment Thredd recommends the EHI connection resolves to a public IP using Thredd's Secure Connectivity framework. However, you can use a private IP internally within your own network, which also uses the Thredd's Secure Connectivity framework. For more information, see the Connecting to Thredd Guide.

EHI Setup and Modes

Q. Which EHI mode should I choose?

Thredd offers four EHI setup options (modes), which are configured when your account is set up on the Thredd platform.

You should select your EHI mode based on how you want the balance on the cards in your programme to be held and how you want to handle payment authorisation transactions:

- Gateway Processing (mode 1) is used where you want full to control the card balance and authorisation process
- Cooperative Processing (mode 2) offers flexible scenarios where Thredd maintains the balance and performs authorisation, but you can override an approval decision.
- Full Service Processing (mode 3) is used where you want Thredd to control the card balance and authorisation process
- Gateway Processing with STIP (mode 4) is similar to Gateway Processing (mode 1), but offers Thredd Stand-in processing if your systems are unavailable.

For more information, see EHI Operating Modes.

Q. Can I be on more than one EHI mode?

You can only choose one EHI mode per product.

Q. Can I change my EHI mode?

Yes. The following are typical reasons why you may decide to change your EHI mode at a later stage:

- You started using Full Service Processing (mode 3) for convenience and to launch your service quickly, but later decide to maintain your own card balance ledger and payment authorisation process. In this case, you could switch to Gateway Processing (mode 1) or Gateway Processing with STIP (mode 4).
- You started using Gateway Processing (mode 1), but have been experiencing persistent processing issues and timeouts on your end, so decide to switch to one of the EHI options that provide Thredd stand-in processing (STIP) when your systems are unavailable. For example: Gateway Processing with STIP (mode 4).

For more information, see EHI Operating Modes.

Q. How do I change my EHI mode?

To change your EHI mode, please contact your Account Manager.

Note: Your Account Manager will need to fully assess and cost any changes to your EHI mode.

Changing your EHI mode may require changes to the way in which Thredd and your external host systems maintain the card balance and respond to authorisation requests. It may also require other EHI configuration changes and testing.

Duplicate Checking and Transaction Matching

Q. What is duplicate checking and how can I ensure a message is unique?

EHI is designed to resend messages if a successful acknowledgement is not received by Thredd. Even if you respond with a valid acknowledgement, due to network issues, this may not be received by Thredd, in which case Thredd resends the message. This ultimately means that any message can be received through EHI more than once. You must ensure that accounts are not debited or credited multiple times due to duplicate messages.

Duplicate checking must be performed for any new message received through EHI. You can use the transaction ID (`Txn_ID`) field to check the uniqueness of a transaction in EHI.

Q. What is transaction matching and how should I perform this?

You are likely to receive multiple linked messages for a card payment transaction throughout its lifecycle (for example, from authorisation, through to presentment and so on). Incoming messages must be linked with each other. The main reason for linkage is to compare financial effect of new messages with previous messages and re-calculate card balances.

Matching of a received message to an earlier message is done by comparison of some key data fields. For details see Transaction Matching.

Q. What fields should I use for transaction matching?

You can use the following fields to match your transactions:

1. `traceID_lifecyle` - this is the primary identifier to match a message to a previous transaction.
2. `authcode` and `date`- can be used to match where you cannot find a match using `traceID_lifecyle`

EHI Cut Off Messages

Q. What are Cut Off messages and what are they used for?

The EHI cut off message is an optional service, which provides a summary of messages sent to the External host in the last X hours (where X is configurable). This is set at product level and sent every X hours to the specified URL you provided.

The cut off message enables you to check all the messages that Thredd has sent to and received from the external host and to identify where any messages were not received/acknowledged (e.g., because of a network connection issue or timeout). It is an important aid to transaction reconciliation and troubleshooting.

The cut off message structure is different to the normal EHI transaction message structure, so Thredd recommends you use a different URL for your cut off messages.

Q. How do the timings on EHI Cut off messages work?

EHI starts sending the cut off message at the end of the cut-off period that was applied to a product.

For example if you select a cut off period of every 6 hours, if added to a product at 1 am, EHI will start sending at 7 am.

Cut of times often vary per product as they can be added to different products at different times.

Q. What happens if there is no data within the cut off period?

If there is no data, then zero is sent as a count at the end of the cut-off period.

Transaction Processing

Q: What are processing codes and how can I identity them?

The processing code (`Proc_Code`) is a 6 digit field made up of a 2 character transaction code identifying the type of payment, a 2 character source account type code and a 2 character destination account type code. The (`Proc_Code`) is based on information obtained from the card scheme networks as well as Thredd's own systems. You can use the processing code to apply processing rules to the transaction (for example, to restrict card usage or charge fees based on the type of transaction. For details, see Processing Codes.

Q: What is the difference between Card Scheme Stand In Processing (STIP) and Thredd STIP?

Scheme STIP is configured on the Card Scheme network:

- The Scheme makes the authorisation decision when the Issuer Processor (Thredd) is unavailable or does not respond in time.
- STIP is enabled only up to a maximum predefined Stand-in authorisation amount
- Configured on the Scheme's systems at BIN level

Thredd STIP is configured on Thredd systems:

- Thredd make the authorisation decision when the Program Manager's external host system is unavailable or does not respond in time.
- Allows flexible STIP authorisation amounts, within the limit set for the product
- Configured on Thredd systems at Product level

Q: How does Mastercard STIP work?

A Mastercard STIP allows Mastercard to complete a transaction when the systems for the Issuer or Thredd are unavailable. Each transaction where Mastercard has processed on Thredd or the Issuer's behalf is followed by an Authorisation Advice message (MTID: 0120), indicating the outcome of the transaction, for example, Accepted or Declined.

Q. How are fees applied and reported for declined transactions?

When a transaction is declined, the system applies a pre-configured decline fee. This fee is processed and reported in EHI messages as follows:

- The *Fixed Fee* and *Rate Fee* are set to 0.
- The *Note* field is updated to include details of both the *Fixed Fee* and *Rate Fee*.
- If a *Decline Fee* is defined for the specific card product:
    - This fee is deducted from the card balance.
    - The deducted amount is populated in the *Fixed fee* field in the EHI message.

  This will be the only fee that is applied to the card for a declined transaction.

Note: Applicable if you are using the Thredd Fees module to apply fees to transactions. See Fees Guide > Completing your PSF: Decline Fees.

Transaction Lifecycle

Authorisations

Q. What are Authorisations and how do they work?

Authorisation is the stage in a transaction life-cycle where a merchant requests approval for a card payment amount. If the authorisation is approved, the amount is ring-fenced on the card. Ring-fencing means that the amount is blocked and the available balance on the card is reduced by this amount.

There are different types of authorisations:

- **Pre-auth** - the merchant requests authorisation for an initial amount. This may be followed by authorisation requests for additional amounts.
- **Auth** - the merchant requests authorisation for a purchase amount. This could either be the full amount of the purchase or a partial amount.
- **Auth and Capture** - the merchant requests the authorisation and taking of the amount at the same time.

When Thredd receives the authorisation request, this is processed according to your EHI mode. In Full Service Processing (mode 3), Thredd approves or declines. In Gateway Processing (mode 1), the Program Manager approves or declines. Other modes use a combination of Thredd and Program Manager approval. Where the Program Manager maintains the card balance, they need to block the approved amount on the card and reduce the available balance. See EHI Operating Modes.

For an approved transaction, typically the merchant then has up to 7-10 days to request settlement of the authorised amount. The time-period when a merchant needs to request settlement of the authorised amount may vary, depending on their Merchant Category Code (MCC) and can be up to 28 days. They can respond by:

- Sending an **authorisation reversal request** - for example, if the transaction is a duplicate or was submitted in error. When the Program Manager receives the authorisation reversal message and they hold the card balance, they should unblock the amount reserved on the card.
- Sending a **presentment request** - to take part or all of the authorised amount. When the Program Manager receives the presentment request, they should match it to the original authorisation; where they hold the card balance, they should deduct the amount from the balance on the card.

  This captured amount is transferred from the card issuer to the merchant's acquirer during the settlement process. (Thredd is not involved in settlement, although we do receive copies of settlement reports.)

If no response is received from the card scheme network within the Thredd configured hanging filter time period, Thredd automatically issues an authorisation reversal message. When the Program Manager receives the authorisation reversal message and they hold the card balance, they should unblock the amount reserved on the card.

For more information, see Transaction Flow Scenarios.

Q. What is an incremental authorisation and how do I identify it?

An incremental authorisation is an additional authorisation, following a previous transaction authorisation, which is used to request an additional amount for the same product or service purchased by the cardholder. It is commonly used by merchants in the hospitality and tourism industry, for items such as hotel bills and car rentals, where the final amount is not known at the time the original authorisation is requested.

Multiple incremental authorisations are usually linked to a single presentment.

Note: The incremental authorisation is for an additional payment and doesn't affect any previous authorisations made on the card.

You can identify an incremental authorisation as follows:

- `txn_type` = A (authorisation)
- In `Message_Why`, the `Response_Source_Why` value = 56 (for Visa) and will be blank for Mastercard. See Response_Source_Why and Message_Why.
- `auth_type` = 0 or P (used for both preauths and incremental auths)
- The following fields are the same as in the original authorisation: `Token`, `Txn_CCy` and `traceid_lifecycle`
- The `Network_Transaction_ID` field will be unique.

Other ways you can use to identify incremental authorisations:

- For Mastercard, you can use the Traceid_Original field. Positions 1-9 will have the same value as the original authorisation.

  Note: The same Traceid_Original value can also appear in subscription payments and recurring payment scenarios. You should exclude these non-incremental cases, which can be identified where position 1 of GPS_POS_Data is equal to 4.

- For Visa, Reason_ID = 3900 (incremental auth for Visa).

  Note: In some instances, this field may be blank, so you should not rely on it.

Q. What is an ASI transaction and how do I identify it?

Account Status Inquiry (ASI) is a type of authorisation transaction, supported by Mastercard, which allows a merchant to check the Card Validation Code (CVC) and, if address details are provided, to optionally use the Address Verification Service (AVS). If these checks are successful, Thredd responds to the merchant with 00 (approve). The merchant typically then submits a second authorisation transaction, with an actual transaction amount included.

(Note: for a decline, the typical response is *62 - Restricted card*)

You can identify the Authorisation Request/0100 message for an ASI transaction as follows:

- Proc_Code has a value of *39*.
- Bill_Amt has a value of zero.
- auth_type field has a value of V to identify account verifications
- POS_Data_DE61 subfield 7 (POS Transaction Status), has a value of 8 (Account Status Inquiry Service (ASI))
- Additional_Data_DE48 subelement 82 (Address Verification Service Request), has a value of 52 (AVS and Authorization Request/0100) for AVS requests (optional)
- Additional_Data_DE48 subelement 92 (CVC 2 Value), has a CVC 2 value (optional)

Q. What is the MerchantAdvice field and how is it used?

The MerchantAdvice field contains a Merchant Advice Code (MAC), which provides the merchant with some further information about the decline, which they can use to decide what to do next: whether to obtain updated details from the cardholder, re-try the transaction later or not attempt any further transactions on the card.

- Where Thredd manages the authorisation response on your behalf (Full Service Processing), the system returns an appropriate advice to the merchant in the authorisation response. This advice code is based on the card status and available funds.
- Where your systems manage the authorisation response (Gateway or Cooperative Processing), you can optionally return one of the advice codes listed in the description of the MerchantAdvice field. See GetTransaction Message Fields: MerchantAdvice.

When declining a transaction and returning a Merchant Advice Code value of “03” (Merchant should not retry again), you must not approve any future transactions on this card. This advice code is reserved for lost, stolen or destroyed cards that are permanently blocked.

Note: Be aware that Mastercard could impose issuer fines for transactions that are authorised on a PAN where previously a Merchant Advice Code value of “03” (Merchant should not retry again) was returned to the merchant.

Q. What is an offline transaction and how do I handle it?

In an offline transaction, Thredd has not received a previous authorisation transaction from the card network. In this case you will not receive any authorisation request message. See the Presentments section below for details of how to handle a presentment message for an offline transaction.

Q. What is the traceid_lifecycle field and how is it constructed?

This is a unique transaction lifecycle identifier which can be used to track a transaction across its lifecycle, enabling linking of authorisations and financial messages relating to the same transaction.

The traceid_lifecycle is a concatenation of: *network_id + "-" + date_yyyymmdd + "-" + a unique identifier*

For details of how this is constructed for different networks, see the following table:

Card Scheme (Network)	network_id	date_yyyymmdd	Unique identifier	Example
Mastercard Banknet	BNET	Banknet trace date from DE15 that corresponds to the Banknet serial number (from DE63).	The traceid from field 63 (or equivalent from field 48.63, e.g., for incremental authorisations)	"BNET-20181231-MCC1234XY"

Card Scheme (Network)	network_id	date_yyyymmdd	Unique identifier	Example
Visa Base I	VIS1	Date from inside the Visa Transaction ID	The Base field 62.2 Visa Transaction Id. For details, see Visa's Base II documentation.	"VIS1-20180331-918090604354364"
VDEP/Visa-Tokenisation-System API call	VDEP	No date. The traceid_lifecycle format is: "*VDEP" + 1 space + X-REQUEST-ID"*	The 36-character X-REQUEST-ID from VDEP API incoming HTTP header field.	"VDEP 90bc1da9-4f7e-491d-ba3b-1e0d70c1b601"

Presentments

Q. What are presentments and how do they work?

A presentment (settlement or clearing request) is a financial transaction where Thredd receives a request to settle an amount that was previously authorised on a card. A presentment is typically linked to a previous authorisation transaction. Thredd receives several daily batch clearing files from the card schemes, containing, amongst other records, presentments.

The majority of presentment transactions are requests for settlement of transactions authorised the previous day. However, for a normal authorisation, under current card scheme rules, merchants have up to 7-10 days to request settlement of an authorisation. For some merchant category codes (e.g., card rentals and hotels), settlement can be up to 28 days after the authorisation.

Thredd processes the presentments in the batch file, records details in the Thredd database, and sends a presentment message for each presentment, via EHI to the external host (Program Manager's system).

When you receive a presentment, you should try and match to an existing preauthorisation. Where your systems hold the card balance, you should reduce the balance by the amount of the presentment.

Q. Are there any cases where Thredd receives a presentment which does not have a linked previous authorisation?

Yes. In the case of offline transactions, the authorisation approval is made without Thredd and we will have no record of the transaction in the system. In this case, Thredd creates a new authorisation transaction and sends this to the Program Manager, followed by the linked presentment message. For more information, see First Presenment for an Offline Transaction.

Q. What are incremental presentments and how do I handle them?

An incremental presentment may occur when a merchant requests an authorisation for a specific amount, but then submits multiple presentments for different partial amounts. So, an incremental presentment has one authorisation and multiple presentment files. The final presentment total usually equals the total of the original authorised amount.

An incremental presentment can be identified in a GetTransaction financial message if the multi_part_txn field = 1. Additional fields provide information on the sequence and number of expected partial presentments: multi_part_txn, multi_part_txn_final, multi_part_number and multi_part_count (Visa only). See GetTransaction Message Fields.

When you receive an incremental presentment, you should only unblock the amount stated and not the full amount previously authorised. When you have received the final presentment, you can calculate the total and unblock any amount left on the original authorisation.

Note: A presentment must be correctly flagged by the acquirer in order for Thredd to identify it as an incremental presentment. This option is specific to Visa and some acquirers may not report this information.

Q. How is a partial presentment processed?

For a partial presentment (i.e., for part of the authorised amount), the authorised fees are partially cleared as well, with the remaining amount blocked on the card.

Q. What happens if a presentment is more than the amount available on the card?

The presentment always debits or credits the card balance, regardless of the existing amount. If the presentment is more than the amount held on the card, the card account would go into a negative balance.

Note: whether negative balances are permitted on your programme will depend on the nature of the program type and the agreements with the issuer.

Q: How do I identify a negative card balance?

In processing modes where Thredd manages the balance (Full Service Processing - mode 3 and Cooperative Processing - mode 2) a negative balance is indicated in the balance and available_balance fields.

Clearing Files

Q. How often do Thredd receive clearing files from the schemes?

Mastercard send 8 clearing files per day, seven days a week. Visa send 2 clearing files per day.

How often does Thredd process clearing files?

It is possible for Thredd to process clearing files 7 days a week. Please note, this does not change the date of settlement. If you are interested in enabling 7 day clearing file processing, please contact your account manager for more details.

How long does it take Thredd to process the clearing files?

It takes Thredd a few hours to process the clearing files and send notifications via EHI.

Q. What happens if Thredd does not receive a presentment for a previously authorised card amount?

If no presentment is received within a defined hanging filter period, Thredd sends a financial authorisation reversal message, via EHI, to the external host. The Program Manager should unblock any amount ring-fenced on the card, so that it is available to the cardholder.

Credit Transactions

Q. Can a refund be online?

Yes. Visa and Mastercard allow acquirers to send refunds with or without authorisation. If an online refund (authorisation) is received, it will be normally followed by a presentment (financial) similar to purchase authorisation flow. Thredd recommend that you do not make the funds available to the cardholder before the financial is received.

Q. What is the difference between refund authorisation and reversal authorisation?

Authorisation reversals occur against authorisations that have not yet become financial (no presentment is created). Reversals are typically received on the same day. If a reversal authorisation is received for a purchase which is already cleared (i.e. the presentment is received before the authorisation reversal), it indicates a transaction processing error on the acquirer's side.

Refunds are standalone transactions that have their own lifecycle (financial message and possibly an authorisation message). Refunds might be linked with a previous purchase or they may not. Unlike reversals, there is no strict linking requirement for refunds against previous purchases (due to the independent flow, there is no need to backward balance update).

Q. What is the difference between Refunds and Fund Transfers (Original Credits)?

Refunds are common way of returning funds to customers relating to a previous card transaction. Thredd recommends that you only transfer the refund to the cardholder after you have received the financial message confirming the refund.

Original credits are fund transfer transactions from one entity to another and are not linked to a previous transaction. Visa Fast Funds and Mastercard Money Send are examples. Unlike refunds, most of the Fund Transfer transactions should be funded to the target card within 30 minutes of authorisation. This needs a careful approach to detect the appropriate fund transfers and credit the cards in 30 minutes and not credit the cards again when financials are received. (Please check with your Visa / Mastercard representative to confirm the funding requirements for your region/country).

Network Fees

Q. How are Acquirer fees applied and reported?

Acquirer fees do not affect the cardholder balance at Thredd and are passed as data only, requiring program managers to handle fees separately. This fee data is provided in the EHI field Amt_Tran_Fee_DE28.

Q. How are Acquirer ATM fees applied and reported?

Acquirer fees for ATM balance inquiries, PIN changes and cash withdrawals are sent in the EHI field `Amt_Tran_Fee_DE28` and are not included in the `Bill_Amt` used for card limit checks. See the example below, showing a cash withdrawal of 100 GBP and an Acquirer ATM fee of 1.5 GBP.

```
<GetTransaction
            xmlns="http://tempuri.org/">
            <Acquirer_id_DE32>0852729540</Acquirer_id_DE32>
            <ActBal>884.9800</ActBal>
            <Additional_Amt_DE54 />
            <Amt_Tran_Fee_DE28>D00015000</Amt_Tran_Fee_DE28>
            <Auth_Code_DE38>129833</Auth_Code_DE38>
            <Avl_Bal>660.7800</Avl_Bal>
            <Bill_Amt>-100.0000</Bill_Amt>
            <Bill_Ccy>826</Bill_Ccy>
            <BlkAmt>-100.0000</BlkAmt>
```

During transaction authorisation for an ATM withdrawal, for EHI modes (e.g., Full Service Processing) where Thredd controls the card balance, the authorisation approval is made only for the amount in the `Bill_Amt` field. If there is a sufficient balance held on the card, the request will be approved.

Q. Does Thredd provide an option to deduct Issuer transaction-related fees from a card?

This applies to EHI modes (e.g., Cooperative Processing and Full Service Processing) where Thredd controls the card balance.

You can use the Thredd Fees module to deduct Issuer fees (e.g., ATM withdrawals and balance inquiries) from the card at the time of the transaction authorisation.

If there is sufficient balance on the card, the fee will be deducted from the card's available balance.

If there is insufficient balance on the card and you have enabled *Partial Fees*, then Thredd will deduct a part of the fee amount and create a Pending Fee Record. If you have not enabled Partial Fees, the transaction will be declined.

For other EHI modes (e.g. Gateway Processing) where Thredd does not control the card balance, the Issuer fees must be calculated and sent in the relevant EHI fields to the External Host.

For more information, see the Fees Guide.

Troubleshooting FAQs

This section provides answers to common integration queries.

System timeouts and connection issues

Q.How can I identify if a transaction has been timed out and view details of the response time?

You can view details in Thredd Portal or in Smart Client: In the **View Transactions** screen, double-click the declined transaction.

The **Response Status (DE039)** field indicates "*92 - Unable to route*". The **difference (in Milliseconds)** field shows the response time.

Q. Why is the Thredd default timeout set to its current level and should I request a change for my program?

The default Thredd limit for a timeout is set to its current level to avoid potential network timeouts by the card scheme (Visa/Mastercard/Discover) as well as to reduce delays for the cardholder which may result in them abandoning their purchase. Each card scheme has different timeout rules. For details, check with your Implementation Manager. The Thredd timeout limit takes into account the full, end-to-end transaction round trip, which involves several parties and systems, each of which take a portion of the available time. See the figure below.

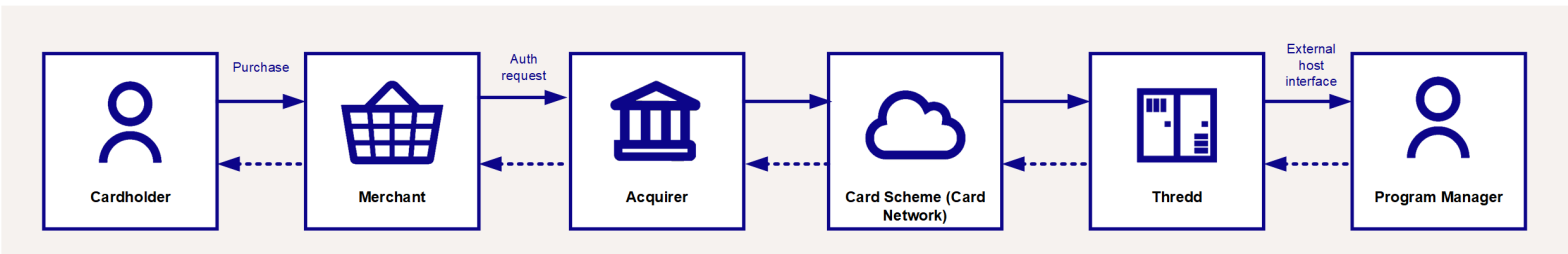


Figure 21: Parties involved in transaction authorisation

For suggestions as to how you can reduce response timeouts, see below.

Q. How can I reduce the number of response timeouts (where my external host does not respond within the allowed time period)?

The default permitted response time (see EHI Configuration Options) is the full round-trip time, including your processing and routing, between Thredd and your external host.

Factors that could impact on your response time include your system processing time and the network transport time. Below are some suggestions as to how you can improve your external host response times and avoid response timeouts during real-time authorisation requests:

- Make sure you have an appropriate level of monitoring and logging on your systems so that you can quickly identify potential issues affecting your service.
- Where response delays are due to slow processing on your systems, consider upgrading your hardware, software or processing logic. As a general rule, you should be processing a message and returning a decision as quickly as possible, in order to enable sufficient time for the message to pass over the network. Your system design should also take into account future traffic loads as your service grows.
- Implement a separate endpoint for your Cut-off messages (to reduce traffic going into your main data feed).
- We recommend you provide Thredd with IP addresses for your external host endpoints and do not use a DNS as this can create potential additional lookup traffic overhead prior to the authorisation being sent.
- It may be possible to request a higher limit for much longer geographical (e.g.,intercontinental) distances from the Thredd data centres. (**Note**: any permanent higher timeouts may be chargeable.)
- If you are experiencing occasional timeouts, consider moving to Gateway Processing with STIP (mode 4), where Thredd can provide the approve or decline decision for an authorisation request in the event that your external host system does not respond with the timeout limit. See EHI Operating Modes.
- If you are experiencing consistent timeouts, try confirm the days and times when this occurs. This may help identify a possible cause.
- Consider the time it takes to connect to any external third party services you are using for your authorisation decisions, such as fraud screening and foreign exchange (FX) conversion services.

- If you are using an older version of EHI, you can reduce the number of connection timeouts by upgrading to a later version. See Upgrading your EHI Version.
- If you have high traffic volumes, you should consider requesting a dedicated session for your authorisation traffic (set up between the card scheme and Thredd). Thredd will need to negotiate this with the card scheme (Visa/Mastercard). For details, check with your Implementation Manager.

Transactions and Matching

Q. I am receiving an unexpectedly high volume of repeat messages per day via EHI

This could be due to a number of reasons:

- Check that the message format of your external response matches the EHI specifications. An invalidly formatted response may result in the response message being rejected and the original advice or authorisation request message being resent to your external host.
- Make sure you remove the namespace from the response as this causes EHI to resend the messages.
- Ensure you are acknowledging all Thredd messages with a value of `acknowledge` = 1. See Processing EHI Transactions.
- If you do not acknowledge messages within the permitted period, this will result in EHI resending messages. This may be due to your systems processing and responded to messages slowly. See How can I reduce the number of response timeouts?
- At times of peak traffic load, consider prioritising messages that require real-time decision-making, such as authorisations.

Q. How can I ensure the card balance is always correctly updated?

For Gateway and Cooperative Processing (modes 1, 2 and 4) where you maintain the balance, Thredd does not match advices received from the card networks; we will pass the advice through to your external host system. When you receive an advice for an approved authorisation, you should block the funds and match the subsequent presentment using appropriate matching criteria; see Transaction Matching.

For Full Service Processing (mode 3), since Thredd maintains the balance, Thredd matches transactions and updates the balance on your behalf.

Note: In some circumstances, the card schemes may perform Stand-In processing on our behalf and approve an authorisation request (e.g.,where the Thredd system is unavailable and or does not respond in time). In these circumstances Thredd does not block the approved amount on the card. Once we receive the presentment, we will create an authorisation advice and send this to you, along with the presentment advice.

Q. How can I prevent a card balance going into negative on a card?

In certain circumstances, such as for offline transactions or where Thredd or the card scheme performs Stand-In processing this may potentially result in the card not having sufficient funds available to cover the presentment, and therefore going into a negative balance. Other examples include late presentments or where merchants send in a presentment for a declined transaction.

When Thredd receive a presentment from the merchant, we will always take the money from the card (Full Service Processing - mode 3). If you receive a presentment, you must update the balance (Gateway and Cooperative Processing - modes 1, 2 and 4). You cannot decline a presentment. If the original transaction was declined and you subsequently receive a presentment, you may have the right to a chargeback. If a late presentment is received after the original authorisation block has expired, this could result in the card going into a negative balance. In this case you *may* have the right to a chargeback.

You cannot fully prevent a card going into a negative balance. To mitigate the risks, Thredd recommends you consider the following options:

- Prevent offline transactions. This option is recommended for prepaid cards. However, note that this will also reduce the available merchant locations where the card can be used.
- Reduce the need for stand-in authorisation processing by ensuring your external host system is able to respond to authorisation requests in a timely manner.
- Consider implementing an automated reminder notification to cardholders to top up when their card balance is running low. The terms and conditions of your service may allow you to implement a service charge or a standing order instruction that debits the cardholder's linked account to cover any negative card balances.

Q. I cannot match the Acquirer reference in linked messages

The `Trans_link` field provides a reference which can be used to match different types of linked authorisation and financial messages; this reference contains acquirer reference data, such as the *Acquirer Reference Number (ARN)* and *Acquirer Bank Identification Number (BIN)*.

For Mastercard transactions the acquirer reference data is unique and should always match across transactions. For Visa transactions, this data may not be unique and traceid_lifecycle can be used as an alternative for transaction matching. In general, the traceid_lifecycle field is a good field to use for matching transactions across the transaction lifecyle, as the value of this field should be identical for all messages relating to the same transaction.

Other EHI fields which contain acquirer reference data that can be used for matching include:

- Acquirer_Reference_Data_031 – contains the Acquirer Reference Number (ARN) used for clearing messages only.
- Acquirer_id_DE32 – the Acquiring Bank Identification Number as assigned by the network.
- Acquirer_Forwarder_ID – the ID of the Acquiring institution forwarding a Request or Advice message.

For more information on transaction matching criteria, see Transaction Matching.

Note: In most cases, the Acquirer reference data for Authorisation and Financial messages and any linked transactions (e.g., reversals) should be the same. However, some acquirers may not follow the standard processing rules, which could result in Acquirer reference data values that are not the same in linked messages. In this case, you should contact the acquirer for clarification.

Q. What's the difference between the processing codes 01, 12 and 17?

The Proc_Code for 01, 12 and 17 are based on information received from the card scheme networks. See below for details.

On Mastercard networks:

Processing Code	Type of Transaction	Mastercard Product	MCC
01	ATM cash withdrawals	All Mastercard cards	6011
01	Manual cash disbursements - Authorisation transactions Example of a manual cash disbursement: A POS device in a bank branch operated by bank staff is used, and if approved, the bank employee hands cash over the counter to the cardholder.	Maestro cards only	6010
12	Manual cash disbursements - Clearing transactions	All Mastercard cards	6010
17	Manual cash disbursements - Authorisation transactions	Mastercard Credit, Cirrus and Mastercard Debit.	6010

On Visa networks:

Processing Code	Type of Transaction	Visa Product	MCC
01	ATM cash withdrawals	All Visa cards	6011
01	Manual cash disbursements - Authorisation and Clearing transactions	All Visa cards	6010
12	Not used		
17	Not used		

Q. How to handle processing errors due to invalid characters?

Thredd receives data in the authorisation messages from the Card Scheme/Acquirer, which occasionally contains fields that have been populated with unrecognised hexadecimal characters. The inclusion of such characters is typically within String fields of type AN or ANS, such as <Merch_Name_DE43>, <Txn_Desc>, <MCC_Desc>, <Merch_ID_DE42>, <Network_Transaction_ID>,<Merch_City>, <GPS_POS_Capability> and <GPS_POS_Data>.

The Thredd Platform is able to successfully process data in these fields, irrespective of special character formats.

During conversion in EHI to the JSON format, data is encoded according to the JSON specification.

Where the converter does not recognise a character, this results in character substitution in the field, based on the conversion standard. You can find several examples below.

Substitution Examples

Hexa-decimal character	Descrip-tion	Con-verted to in JSON	Exampl-e: Ori-ginal 0100 Mes-sage	Example: Conversion to JSON Format
20	space	\u0000	<GPS_POS_ Data> </GPS_POS_Data>	"GPS_POS_Data": "\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000000", "GPS_POS_Capability": "\u0000\u0000 \u0000\u0000\u0000\u0000\u0000\u0000\u0000",

Your systems should be able to handle such invalid characters (for example, by using regular expressions to blank out or convert the invalid characters).

Known Issues

For a list of known issues, please contact your Implementation Manager.

EHI Versions

This section provides details of the differences in fields between EHI versions 3.0 and 5.1.

Fields included in the EHI Request

EHI Version 3.0	EHI Version 4.0	EHI Version 4.1	EHI Version 5.0	EHI Version 5.1
Account_Type_From				
Account_Type_To				
	Acquirer_Forwarder_ID	Acquirer_Forwarder_ID	Acquirer_Forwarder_ID	Acquirer_Forwarder_ID
			Acquirer_Country	Acquirer_Country
Acquirer_id_DE32	Acquirer_id_DE32	Acquirer_id_DE32	Acquirer_id_DE32	Acquirer_id_DE32
Acquirer_Reference_Data_031	Acquirer_Reference_Data_031	Acquirer_Reference_Data_031	Acquirer_Reference_Data_031	Acquirer_Reference_Data_031
ActBal	ActBal	ActBal	ActBal	ActBal
Additional_Amt_DE54	Additional_Amt_DE54	Additional_Amt_DE54	Additional_Amt_DE54	Additional_Amt_DE54
Additional_Data_DE124	Additional_Data_DE124	Additional_Data_DE124	Additional_Data_DE124	Additional_Data_DE124
Additional_Data_DE48	Additional_Data_DE48	Additional_Data_DE48	Additional_Data_DE48	Additional_Data_DE48
Amt_Tran_Fee_DE28	Amt_Tran_Fee_DE28	Amt_Tran_Fee_DE28	Amt_Tran_Fee_DE28	Amt_Tran_Fee_DE28
Auth_Code_DE38	Auth_Code_DE38	Auth_Code_DE38	Auth_Code_DE38	Auth_Code_DE38
	auth_expdate_utc	auth_expdate_utc	auth_expdate_utc	auth_expdate_utc
	auth_type	auth_type	auth_type	auth_type
Authorised_by_GPS	Authorised_by_GPS	Authorised_by_GPS	Authorised_by_GPS	Authorised_by_GPS
Avl_Bal	Avl_Bal	Avl_Bal	Avl_Bal	Avl_Bal
AVS_Result	AVS_Result	AVS_Result	AVS_Result	AVS_Result
Balance_Sequence	Balance_Sequence	Balance_Sequence	Balance_Sequence	Balance_Sequence
Balance_Sequence_Exthost	Balance_Sequence_Exthost	Balance_Sequence_Exthost	Balance_Sequence_Exthost	Balance_Sequence_Exthost
Bill_Amt	Bill_Amt	Bill_Amt	Bill_Amt	Bill_Amt
Bill_Ccy	Bill_Ccy	Bill_Ccy	Bill_Ccy	Bill_Ccy

EHI Version 3.0	EHI Version 4.0	EHI Version 4.1	EHI Version 5.0	EHI Version 5.1
BlkAmt	BlkAmt	BlkAmt	BlkAmt	BlkAmt
			ClearingFileId	ClearingFileId
	Clearing_Process_ Date	Clearing_Process_ Date	Clearing_Process_Date	Clearing_Process_Date
CU_Group	CU_Group	CU_Group	CU_Group	CU_Group
	Currency_Code_Fee	Currency_Code_Fee	Currency_Code_Fee	Currency_Code_Fee
	Currency_Code_ Fee_Settlement	Currency_Code_ Fee_Settlement	Currency_Code_Fee_ Settlement	Currency_Code_Fee_ Settlement
Cust_Ref	Cust_Ref	Cust_Ref	Cust_Ref	Cust_Ref
CVV2	CVV2	CVV2	CVV2	CVV2
	DCC_Indicator	DCC_Indicator	DCC_Indicator	DCC_Indicator
dest_bank_account	dest_bank_account	dest_bank_account	dest_bank_account	dest_bank_account
dest_bank_account_ format	dest_bank_account_ format	dest_bank_account_ format	dest_bank_account_format	dest_bank_account_format
dest_bank_ctry	dest_bank_ctry	dest_bank_ctry	dest_bank_ctry	dest_bank_ctry
	Dispute_Condition	Dispute_Condition	Dispute_Condition	Dispute_Condition
Dom_Fee_Fixed	Dom_Fee_Fixed	Dom_Fee_Fixed	Dom_Fee_Fixed	Dom_Fee_Fixed
Dom_Fee_Rate	Dom_Fee_Rate	Dom_Fee_Rate	Dom_Fee_Rate	Dom_Fee_Rate
Expiry_Date	Expiry_Date	Expiry_Date	Expiry_Date	Expiry_Date
Fee_Fixed	Fee_Fixed	Fee_Fixed	Fee_Fixed	Fee_Fixed
Fee_Rate	Fee_Rate	Fee_Rate	Fee_Rate	Fee_Rate
Fx_Fee_Fixed	Fx_Fee_Fixed	Fx_Fee_Fixed	Fx_Fee_Fixed	Fx_Fee_Fixed
Fx_Fee_Rate	Fx_Fee_Rate	Fx_Fee_Rate	Fx_Fee_Rate	Fx_Fee_Rate
FX_Pad	FX_Pad	FX_Pad	FX_Pad	FX_Pad
GPS_POS_ Capability	GPS_POS_ Capability	GPS_POS_ Capability	GPS_POS_Capability	GPS_POS_Capability
GPS_POS_Data	GPS_POS_Data	GPS_POS_Data	GPS_POS_Data	GPS_POS_Data
ICC_System_ Related_Data_DE55	ICC_System_ Related_Data_DE55	ICC_System_ Related_Data_DE55	ICC_System_Related_ Data_DE55	ICC_System_Related_ Data_DE55
InstCode	InstCode	InstCode	InstCode	InstCode
	Interchange_	Interchange_	Interchange_Amount_Fee	Interchange_Amount_Fee

EHI Version 3.0	EHI Version 4.0	EHI Version 4.1	EHI Version 5.0	EHI Version 5.1
	Amount_Fee	Amount_Fee		
	Interchange_ Amount_Fee_ Settlement	Interchange_ Amount_Fee_ Settlement	Interchange_Amount_Fee_ Settlement	Interchange_Amount_Fee_ Settlement
LoadSRC	LoadSRC	LoadSRC	LoadSRC	LoadSRC
LoadType	LoadType	LoadType	LoadType	LoadType
	Matching_Txn_ID	Matching_Txn_ID	Matching_Txn_ID	Matching_Txn_ID
MCC_Code	MCC_Code	MCC_Code	MCC_Code	MCC_Code
MCC_Desc	MCC_Desc	MCC_Desc	MCC_Desc	MCC_Desc
MCC_Pad	MCC_Pad	MCC_Pad	MCC_Pad	MCC_Pad
Merch_City	Merch_City	Merch_City	Merch_City	Merch_City
Merch_Contact	Merch_Contact	Merch_Contact	Merch_Contact	Merch_Contact
Merch_Country	Merch_Country	Merch_Country	Merch_Country	Merch_Country
Merch_ID_DE42	Merch_ID_DE42	Merch_ID_DE42	Merch_ID_DE42	Merch_ID_DE42
Merch_Name	Merch_Name	Merch_Name	Merch_Name	Merch_Name
Merch_Name_DE43	Merch_Name_DE43	Merch_Name_DE43	Merch_Name_DE43	Merch_Name_DE43
Merch_Name_Other	Merch_Name_Other	Merch_Name_Other	Merch_Name_Other	Merch_Name_Other
Merch_Net_id	Merch_Net_id	Merch_Net_id	Merch_Net_id	Merch_Net_id
Merch_Postcode	Merch_Postcode	Merch_Postcode	Merch_Postcode	Merch_Postcode
Merch_Region	Merch_Region	Merch_Region	Merch_Region	Merch_Region
Merch_Street	Merch_Street	Merch_Street	Merch_Street	Merch_Street
Merch_Tax_id	Merch_Tax_id	Merch_Tax_id	Merch_Tax_id	Merch_Tax_id
Merch_Tel	Merch_Tel	Merch_Tel	Merch_Tel	Merch_Tel
Merch_URL	Merch_URL	Merch_URL	Merch_URL	Merch_URL
Message_Source	Message_Source	Message_Source	Message_Source	Message_Source
Message_Why	Message_Why	Message_Why	Message_Why	Message_Why
MTID	MTID	MTID	MTID	MTID
	multi_part_count	multi_part_count	multi_part_count	multi_part_count
	multi_part_number	multi_part_number	multi_part_number	multi_part_number

EHI Version 3.0	EHI Version 4.0	EHI Version 4.1	EHI Version 5.0	EHI Version 5.1
	multi_part_txn	multi_part_txn	multi_part_txn	multi_part_txn
	multi_part_txn_final	multi_part_txn_final	multi_part_txn_final	multi_part_txn_final
			Network_Fraud_Data Format	Network_Fraud_Data Format
	Network_ Chargeback_ Reference_Id	Network_ Chargeback_ Reference_Id	Network_Chargeback_ Reference_Id	Network_Chargeback_ Reference_Id
Non_Dom_Fee_ Fixed	Non_Dom_Fee_ Fixed	Non_Dom_Fee_ Fixed	Non_Dom_Fee_Fixed	Non_Dom_Fee_Fixed
Non_Dom_Fee_Rate	Non_Dom_Fee_Rate	Non_Dom_Fee_Rate	Non_Dom_Fee_Rate	Non_Dom_Fee_Rate
Note	Note	Note	Note	Note
Other_Fee_Amt	Other_Fee_Amt	Other_Fee_Amt	Other_Fee_Amt	Other_Fee_Amt
PAN_Sequence_ Number	PAN_Sequence_ Number	PAN_Sequence_ Number	PAN_Sequence_Number	PAN_Sequence_Number
PaymentToken_ activationCode	PaymentToken_ activationCode	PaymentToken_ activationCode	PaymentToken_ activationCode	PaymentToken_ activationCode
PaymentToken_ activationExpiry	PaymentToken_ activationExpiry	PaymentToken_ activationExpiry	PaymentToken_ activationExpiry	PaymentToken_ activationExpiry
PaymentToken_ activationMethod	PaymentToken_ activationMethod	PaymentToken_ activationMethod	PaymentToken_ activationMethod	PaymentToken_ activationMethod
PaymentToken_ activationMethodDat a	PaymentToken_ activationMethodDat a	PaymentToken_ activationMethodDat a	PaymentToken_ activationMethodData	PaymentToken_ activationMethodData
PaymentToken_ creator	PaymentToken_ creator	PaymentToken_ creator	PaymentToken_creator	PaymentToken_creator
PaymentToken_ creatorStatus	PaymentToken_ creatorStatus	PaymentToken_ creatorStatus	PaymentToken_ creatorStatus	PaymentToken_ creatorStatus
PaymentToken_ deviceId	PaymentToken_ deviceId	PaymentToken_ deviceId	PaymentToken_deviceId	PaymentToken_deviceId
PaymentToken_ deviceIp	PaymentToken_ deviceIp	PaymentToken_ deviceIp	PaymentToken_deviceIp	PaymentToken_deviceIp
PaymentToken_ deviceName	PaymentToken_ deviceName	PaymentToken_ deviceName	PaymentToken_ deviceName	PaymentToken_ deviceName
PaymentToken_ deviceTelNum	PaymentToken_ deviceTelNum	PaymentToken_ deviceTelNum	PaymentToken_ deviceTelNum	PaymentToken_ deviceTelNum
PaymentToken_ deviceType	PaymentToken_ deviceType	PaymentToken_ deviceType	PaymentToken_ deviceType	PaymentToken_ deviceType
PaymentToken_	PaymentToken_	PaymentToken_	PaymentToken_expdate	PaymentToken_expdate

EHI Version 3.0	EHI Version 4.0	EHI Version 4.1	EHI Version 5.0	EHI Version 5.1
expdate	expdate	expdate		
PaymentToken_id	PaymentToken_id	PaymentToken_id	PaymentToken_id	PaymentToken_id
PaymentToken_lang	PaymentToken_lang	PaymentToken_lang	PaymentToken_lang	PaymentToken_lang
			PaymentToken_PanSource	PaymentToken_PanSource
PaymentToken_ status	PaymentToken_ status	PaymentToken_ status	PaymentToken_status	PaymentToken_status
PaymentToken_type	PaymentToken_type	PaymentToken_type	PaymentToken_type	PaymentToken_type
PaymentToken_ wallet	PaymentToken_ wallet	PaymentToken_ wallet	PaymentToken_wallet	PaymentToken_wallet
PIN	PIN	PIN	PIN	PIN
PIN_Enc_Algorithm	PIN_Enc_Algorithm	PIN_Enc_Algorithm	PIN_Enc_Algorithm	PIN_Enc_Algorithm
PIN_Format	PIN_Format	PIN_Format	PIN_Format	PIN_Format
PIN_Key_Index	PIN_Key_Index	PIN_Key_Index	PIN_Key_Index	PIN_Key_Index
POS_Data_DE22	POS_Data_DE22	POS_Data_DE22	POS_Data_DE22	POS_Data_DE22
POS_Data_DE61	POS_Data_DE61	POS_Data_DE61	POS_Data_DE61	POS_Data_DE61
POS_Termnl_DE41	POS_Termnl_DE41	POS_Termnl_DE41	POS_Termnl_DE41	POS_Termnl_DE41
POS_Time_DE12	POS_Time_DE12	POS_Time_DE12	POS_Time_DE12	POS_Time_DE12
Proc_Code	Proc_Code	Proc_Code	Proc_Code	Proc_Code
ProductID	ProductID	ProductID	ProductID	ProductID
	Reason_ID	Reason_ID	Reason_ID	Reason_ID
			ReceiverData	ReceiverData
Record_Data_DE120	Record_Data_DE120	Record_Data_DE120	Record_Data_DE120	Record_Data_DE120
Resp_Code_DE39	Resp_Code_DE39	Resp_Code_DE39	Resp_Code_DE39	Resp_Code_DE39
Response_Source	Response_Source	Response_Source	Response_Source	Response_Source
Response_Source_ Why	Response_Source_ Why	Response_Source_ Why	Response_Source_Why	Response_Source_Why
Ret_Ref_No_DE37	Ret_Ref_No_DE37	Ret_Ref_No_DE37	Ret_Ref_No_DE37	Ret_Ref_No_DE37
			SenderData	SenderData
SendingAttemptCoun t	SendingAttemptCoun t	SendingAttemptCoun t	SendingAttemptCount	SendingAttemptCount

EHI Version 3.0	EHI Version 4.0	EHI Version 4.1	EHI Version 5.0	EHI Version 5.1
Settle_Amt	Settle_Amt	Settle_Amt	Settle_Amt	Settle_Amt
Settle_Ccy	Settle_Ccy	Settle_Ccy	Settle_Ccy	Settle_Ccy
	Settlement_Date	Settlement_Date	Settlement_Date	Settlement_Date
	SettlementIndicator	SettlementIndicator	SettlementIndicator	SettlementIndicator
source_bank_ account	source_bank_ account	source_bank_ account	source_bank_account	source_bank_account
source_bank_ account_format	source_bank_ account_format	source_bank_ account_format	source_bank_account_ format	source_bank_account_ format
source_bank_ctry	source_bank_ctry	source_bank_ctry	source_bank_ctry	source_bank_ctry
Status_Code	Status_Code	Status_Code	Status_Code	Status_Code
SubBIN	SubBIN	SubBIN	SubBIN	SubBIN
TLogIDOrg	TLogIDOrg	TLogIDOrg	TLogIDOrg	TLogIDOrg
Token	Token	Token	Token	Token
traceid_lifecycle	traceid_lifecycle	traceid_lifecycle	traceid_lifecycle	traceid_lifecycle
Trans_link	Trans_link	Trans_link	Trans_link	Trans_link
Txn_Amt	Txn_Amt	Txn_Amt	Txn_Amt	Txn_Amt
Txn_CCy	Txn_CCy	Txn_CCy	Txn_CCy	Txn_CCy
Txn_Code				
Txn_Ctry	Txn_Ctry	Txn_Ctry	Txn_Ctry	Txn_Ctry
Txn_Desc	Txn_Desc	Txn_Desc	Txn_Desc	Txn_Desc
Txn_GPS_Date	Txn_GPS_Date	Txn_GPS_Date	Txn_GPS_Date	Txn_GPS_Date
TXn_ID	TXn_ID	TXn_ID	TXn_ID	TXn_ID
Txn_Stat_Code	Txn_Stat_Code	Txn_Stat_Code	Txn_Stat_Code	Txn_Stat_Code
TXN_Time_DE07	TXN_Time_DE07	TXN_Time_DE07	TXN_Time_DE07	TXN_Time_DE07
Txn_Type	Txn_Type	Txn_Type	Txn_Type	Txn_Type
VL_Group	VL_Group	VL_Group	VL_Group	VL_Group
		Traceid_Message	Traceid_Message	Traceid_Message
		Traceid_Original	Traceid_Original	Traceid_Original
		Network_ Transaction_ID	Network_Transaction_ID	Network_Transaction_ID

EHI Version 3.0	EHI Version 4.0	EHI Version 4.1	EHI Version 5.0	EHI Version 5.1
		POS_Date_DE13	POS_Date_DE13	POS_Date_DE13
		Network_Currency_Conversion_Date	Network_Currency_Conversion_Date	Network_Currency_Conversion_Date
		Network_TxnAmt_To_BillAmt_Rate	Network_TxnAmt_To_BillAmt_Rate	Network_TxnAmt_To_BillAmt_Rate
		Network_TxnAmt_To_BaseAmt_Rate	Network_TxnAmt_To_BaseAmt_Rate	Network_TxnAmt_To_BaseAmt_Rate
		Network_BaseAmt_To_BillAmt_Rate	Network_BaseAmt_To_BillAmt_Rate	Network_BaseAmt_To_BillAmt_Rate
		Network_Original_Data_Elements_DE90	Network_Original_Data_Elements_DE90	Network_Original_Data_Elements_DE90
		Network_Replacement_Amounts_DE95	Network_Replacement_Amounts_DE95	Network_Replacement_Amounts_DE95
		Network_Issuer_Settle_ID	Network_Issuer_Settle_ID	Network_Issuer_Settle_ID
		Visa_ResponseInfo_DE44	Visa_ResponseInfo_DE44	Visa_ResponseInfo_DE44
		Visa_POS_Data_DE60	Visa_POS_Data_DE60	Visa_POS_Data_DE60
		Visa_STIP_Reason_Code	Visa_STIP_Reason_Code	Visa_STIP_Reason_Code
		Mastercard_AdviceReasonCode_DE60	Mastercard_AdviceReasonCode_DE60	Mastercard_AdviceReasonCode_DE60
		Misc_TLV_Data	Misc_TLV_Data	Misc_TLV_Data
			AuthenticationCurrency	AuthenticationCurrency
			AuthenticationAmountUpper	AuthenticationAmountUpper
			AuthenticationMerchantHash	AuthenticationMerchantHash
			FxProviderCardholderRate	FxProviderCardholderRate
				SchemeTransactionIdentifier
				TokenUniqueReference
				PaymentTokenPan

Fields included in the External Host Response

EHI Version 3.0	EHI Version 4.0	EHI Version 4.1	EHI Version 5.0	EHI Version 5.1
			MerchantAdvice	MerchantAdvice
Responsestatus	Responsestatus	Responsestatus	Responsestatus	Responsestatus
CurBalance	CurBalance	CurBalance	CurBalance	CurBalance
AvlBalance	AvlBalance	AvlBalance	AvlBalance	AvlBalance
Acknowledgement	Acknowledgement	Acknowledgement	Acknowledgement	Acknowledgement
LoadAmount	LoadAmount	LoadAmount	LoadAmount	LoadAmount
Bill_Amt_Approved	Bill_Amt_Approved	Bill_Amt_Approved	Bill_Amt_Approved	Bill_Amt_Approved
Update_Balance	Update_Balance	Update_Balance	Update_Balance	Update_Balance
New_Balance_ Sequence_Exthost	New_Balance_ Sequence_Exthost	New_Balance_ Sequence_Exthost	New_Balance_ Sequence_Exthost	New_Balance_ Sequence_Exthost
CVV2_Result	CVV2_Result	CVV2_Result	CVV2_Result	CVV2_Result
AvlBalance_GPS_STIP	AvlBalance_GPS_STIP	AvlBalance_GPS_STIP	AvlBalance_GPS_STIP	AvlBalance_GPS_STIP
CurBalance_GPS_STIP	CurBalance_GPS_STIP	CurBalance_GPS_STIP	CurBalance_GPS_STIP	CurBalance_GPS_STIP

Glossary

This page provides a list of glossary terms used in this guide.

#

3D Secure

3D Secure (3-domain structure), also known as a payer authentication, is a security protocol that helps to prevent fraud in online credit and debit card transactions. This security feature is supported by Visa and Mastercard and is branded as ‘Verified by Visa/Visa Secure’ and ‘Mastercard SecureCode/Mastercard Identity Check’ respectively.

A

Account Funding Transaction (AFT)

Card Scheme transaction to debit funds from a card account. It is used to "pull" funds from a card account in order to fund a real-time "push" OCT to a different account, which can be either the cardholder's or another person's account.

Account Status Inquiry (ASI)

A standard message type which allows the merchant to check the Card Validation Code (CVC) and, if address details are provided, to optionally use the Address Verification Service (AVS). If these checks are successful Thredd responds with an 00 approval to the merchant. They normally then submit a second transaction, but with an actual transaction amount included.

Account Verification

A type of authorisation transaction which is intended to confirm that the account is genuine and active. Account Verifications are always for a zero amount, so only appear in Authorisation messages and never in clearing messages.

Acquirer

The merchant acquirer or bank that offers the merchant a trading account, to enable the merchant to take payments in store or online from cardholders.

Adjustment Credits

Indicates a Credit adjustment.

Authentication

This includes checks to confirm the cardholder identity, such as PIN, CVV2 and CAVV.

Authorisation

Stage where a merchant requests approval for a card payment by sending a request to the card issuer to check that the card is valid, and that the requested authorisation amount is available on the card. At this stage the funds are not deducted from the card.

Authorisation Reversal

An authorisation reversal occurs when a merchant wants to reverse a previously submitted authorisation request (e.g., because the authorised amount was entered incorrectly or the customer cancelled the order). The authorisation reversal normally occurs very soon after the original authorisation and can be matched to the original authorisation using the traceid_lifecycle.

Automated Fuel Dispenser (AFD)

Automatic fuel dispensers (AFDs) are used at petrol or gas stations for customer self-service fuel payments. Typically the customer inserts their card and enters a PIN number and the AFD authorises a fixed amount (e.g. £99). Once the final payment amount is known, the AFD may reverse the authorisation and/or request a second authorisation.

C

Card Scheme

Card network, such as MasterCard or Visa, responsible for managing transactions over the network and for arbitration of any disputes.

Cards API

The Thredd Cards API is a new REST-based API which can be used to connect to the Thredd system in place of using the traditional Thredd SOAP-based Web Services. The REST API provides messages in JSON format. If you are interested in the Cards API, please contact your Account Manager.

Cash Disbursement

Type of transaction where cash is given to the cardholder, for example, from a bank branch by a member of staff using a Point of Sale (POS) terminal.

Chargeback

Where a cardholder disputes a transaction on their account and is unable to resolve directly with the merchant, they can raise a chargeback with their card issuer. The chargeback must be for a legitimate reason, such as goods and services not received, faulty goods, or a fraudulent transaction.

Clearing File/Clearing Transaction

Thredd receive batch clearing files from the card networks, containing clearing transactions, such as presentments and network fees. The card issuer transfers the requested settlement amount to the acquirer and 'clears' the amount on the card, reducing the available card balance accordingly.

Credits (for deposit)

Credit transaction for deposit. Not supported in Dual Message System networks.

Credits (for Payment Transaction)

Mastercard-specific Money Send transaction.

D

Debit Adjustments

May be received for non-card money transfers (out), manual/one-off balance adjustments or additional fees.

E

EMV

EMV originally stood for "Europay, Mastercard, and Visa", the three companies which created the standard. EMV cards are smart cards, also called chip cards, integrated circuit cards, or IC cards which store their data on integrated circuit chips, in addition to magnetic stripes for backward compatibility.

EMV 3D Secure

EMV 3-D Secure (3DS) is a new 3D Secure specification that supports app-based authentication and integration with digital wallets, as well as traditional browser-based e-commerce transactions. See: https://www.emvco.com/emv-technologies/3d-secure/

External Host

The external system to which Thredd sends real-time transaction-related data. The URL to this system is configured within Thredd per programme or product. The Program Manager uses their external host system to hold details of the balance on the cards in their programme and perform transaction-related services, such as payment authorisation, transaction matching and reconciliation.

F

Fee Groups

Groups which control the card transaction authorisation fees, and other fees, such as recurring fees and Thredd web service API fees.

Financial Reversal

A financial reversal occurs when the acquirer cancels all or part of a prior transaction (which may be a purchase, refund, cashback, cash, PIN change, or any other transaction type). For example, if the acquirer has already taken the funds and are aware of a processing error (e.g., double charging), they can submit an 1240 Financial Reversal.

Form Factor

A payment device's physical design features which define the size, shape and other physical specifications of the device.

H

Hanging Filter

The period of time during which Thredd waits for an approved authorisation amount to be settled. This is defined at a Thredd product level. A typical default is 7 days for an auth and 10 days for a pre-auth.

I

Incremental Authorisation

A request for an additional amount on a prior authorisation. An incremental authorisation is used when the final amount for a transaction is greater than the amount of the original authorisation. For example, a hotel guest might register for one night, but then decide to extend the reservation for additional night. In that case, an incremental authorisation might be performed in order to get approval for additional charges pertaining to the second night.

Issuer

The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme.

J

JSON

JSON is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute-value pairs and arrays.

M

Mastercard Debit Switch (MDS)

This is a Single Message System at Mastercard for sending online financial messages (e.g., 0200). It includes transactions from Mastercard, Cirrus and Maestro cards. Thredd supports processing messages from this system.

Mastercard Network Exchange

Enables smaller networks to use Mastercard as a routing platform for payments. Can also be referred to as MNEX or MNGS.

Merchant

The shop or store providing a product or service that the cardholder is purchasing. A merchant must have a merchant account, provided by their acquirer, in order to trade. Physical stores use a terminal or card reader to request authorisation for transactions. Online sites provide an online shopping basket and use a payment service provider to process their payments.

Merchant Category Code (MCC)

A unique identifier of the merchant, to identity the type of account provided to them by their acquirer.

MIP

Mastercard Interface Processor (MIP) The processing hardware and software system that interfaces with Mastercard's Global Payment System communications network.

O

Offline Transaction

This is often used in scenarios where the merchant terminal is not required to request authorisation from the card issuer (for example for certain low risk, small value transactions used by airlines and transport networks). The card CHIP EMV determines if the offline transaction is permitted; if not supported, the terminal declines the transaction. Note: Since the balance on the card is not checked in realtime, there is a risk that the card may not have the amount required to cover the transaction.

Online Financial Message

In Single Message Systems operated in some regions (such as the US and some Asia Pacific countries), the card scheme sends real-time financial messages for payment authorisations. Examples of online financial messages include: Online Financial Request, Online Financial Advice and Online Financial Reversal.

Original Credit Transaction (OCT)

Card Scheme transaction to credit funds to a card account. It can be used to send or "push" funds to an eligible card account, resulting in a real-time credit of funds to the cardholder's account.

Original Credits

Visa-specific Money Send transaction. Also called an Original Credit Transaction (OCT).

P

Partial Amount Approval

Some acquirers support a partial amount approval for Debit or Prepaid payment authorisation requests. The issuer can respond with an approval amount less than the requested amount. The cardholder then needs to pay the remainder using another form of tender.

Payments Service Directive Two (PSD2)

PSD2 is a European regulation for payment services that has the purpose of making payments more secure in Europe. It introduces legislation to improve the payment service authentication process.

Presentment

Stage in a transaction where the funds authorised on a card are captured (deducted from the cardholder's account). See also Clearing. Also referred to as the First presentment.

Program Manager

A Thredd customer who manages a card program. The program manager can create branded cards, load funds and provide other card or banking services to their end customers.

Q

Quasi-Cash

Visa-specific quasi-cash transaction. This is used for specific merchants where the purchased items could be converted to cash (e.g., gaming chips, money orders). Identified by the (11xxxx) processing code.

R

Refund

A refund transaction occurs when a merchant refunds a customer part or all of a previously purchased item. Refunds are standalone transactions that have their own lifecycle (financial message and possibly authorisation message). The refunds may be linked with a previous purchase or not, as there is no strict linking requirement for refunds against previous purchases.

S

sFTP

Secure File Transfer Protocol. File Transfer Protocol FTP) is a popular unencrypted method of transferring files between two remote systems. SFTP (SSH File Transfer Protocol, or Secure File Transfer Protocol) is a separate protocol packaged with SSH that works in a similar way but over a secure connection.

Smart Client

Smart Client is Thredd's legacy desktop application for managing your cards and transactions on the Thredd Platform.

SOAP

SOAP (Simple Object Access Protocol) SOAP is a messaging protocol for exchanging structured information. It uses Extensible Markup Language (XML) for its message format and relies on application layer protocols such as HTTP for message negotiation and transmission. SOAP allows developers to invoke processes running on disparate operating systems (such as Windows, macOS, and Linux) to authenticate, authorise and communicate using XML.

SSL Certification

An SSL certificate displays important information for verifying the owner of a website and encrypting web traffic with SSL/TLS, including the public key, the issuer of the certificate, and the associated subdomains.

Stand In Processing (STIP)

The card network (Visa and Mastercard) may perform approve or decline a transaction authorisation request on behalf of the card issuer. Depending on your Thredd mode, Thredd may also provide STIP on your behalf, where your systems are unavailable.

Strong Customer Authentication (SCA)

When the cardholder is authenticated during a payment transaction using a combination of at least two of the following authentication methods: Knowledge (Something the cardholder knows, such as a password), Possession (Something the cardholder has access to, such as a phone number or email account) and Biometrics (such as a fingerprint, face or voice) Under the Payment Service Directive 2 (PSD2), strong customer authentication is required on all cardholder-initiated transactions when both the card issuer and acquirer are within the European Economic Area (EEA).

T

Tag-Length-Value (TLV)

TLV is an encoding scheme. A TLV-encoded record contains the record type (tag), followed by record Length, and finally the Value itself. Example: 0104John where: tag type = 01 (first name) tag length = 4 digits tag value = John

Thredd Portal

Thredd Portal is Thredd's new web application for managing your cards and transactions on the Thredd Platform.

Triple DES

Triple DES (3DES or TDES), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block to produce a more secure encryption.

U

Unique Transaction (requires unique MCC)

Mastercard-specific transaction category. Similar to Visa's quasi-cash, this is used for specific merchants where the purchased items could be converted to cash (e.g., gaming chips, money orders). Identified by the (18xxxx) processing code.

V

Validation

Checks to confirm the card is valid, such as CHIP cryptograms, mag-stripe data (if available) and expiry date

Visa DPS

This is a processing network for US issuers, where messages are processing based on Single Message System flow. Thredd supports messages from this system.

VROL System

Visa Dispute Resolution Online system, provided by Visa for managing transaction disputes.

Document History

This section contains details of all changes to this guide.

Note: In version 4.1.08 and 5.0 we changed the section numbering. We've added links in the comments section below which take you to the relevant section or topic.

Version	Date	Comments	Revised by
5.1	31/03/2026	Updated the description of the P70 Mastercard Scheme Transaction Identifier value, and added the P76 Mastercard Scheme Transaction Identifier value. See Scheme Transaction Identifier Values.	JB
	18/03/2026	Added R0, R1 and R3 response codes to support VISA subscription management. See Response Status Values.	JB
	13/03/2026	Removed support for CVV2 result codes *C*, *D*, *K*, and *L* to align with Visa's updated Field 44.10 CVV2 response code mandate. See Visa_ResponseInfo_DE44.	GF
5.1	19/02/2026	Added links to the STIP Balance Update endpoint in the API Hub. See EHI Operating Modes.	JB
5.1	18/02/2026	Amended amount sign examples to ensure correct credit and debit information appears in the table. See Examples of Amount Signs.	KD
5.1	10/02/2026	Corrected the match criteria for an Authorisation Advice. See Transaction Matching Criteria.	KD
	27/01/2026	Added support for Tokenization Authentication Framework (TAF) as an entry for the Cardholder Authentication Method. See GPS_POS_Data field.	JB
	06/01/2026	Amended an incorrect link to the *Response Source Why and Message Why* page in the Incremental Authorisation FAQ item. See Q. What is an Incremental Authorisation and how do I identify it?	KD
	11/12/2025	Added new Mastercard Advice Reason code for Mastercard Send or other transaction blocking service. See Positions 1-3 Advice Reason Code.	KD
	19/11/2025	Updated the description and examples of Financial Notification messages to indicate that the Acknowledgement in the response is mandatory and that the response status is optional. See EHI Connections and Messages and Processing EHI Transactions.	KD
	14/10/2025	Added a new page in the appendix for Scheme Transaction Identifier values for Visa and Mastercard.	KD
	15/10/2025	Provided further details of transaction flows for Automated Fuel Dispenser (AFD) transactions. See Transaction Flow Scenarios: AFD Authorisations.	WS
	22/09/2025	Added the *Remote Terminal Value* to subfield 10 in GPS_POS_Capability and subfield 49 in POS_Data_DE61. See GPS_POS_Capability Fields and POS_Data_DE61 field.	KD
	12/09/2025	Added clarification related to how the Additional_Data_DE48 field is passed through for scheme transaction risk scores. See GetTransaction Message Fields.	JB
	03/09/2025	Included an example ATM cash withdrawal authorisation request and presentment. Added a note to indicate that the Amt_Tran_Fee_DE28 field is populated with a value when there is a transaction fee for withdrawal. See Example ATM Cash Withdrawal Messages (Mastercard).	KD

Version	Date	Comments	Revised by
	09/09/2025	Added a new value of *S*, *Frictionless flow, Smart attempts*, to the GPS_POS_Data field, position 15, 3D secure authentication method. See GPS_POS_Data field.	WS
	03/09/2025	Added Network Fee section to the FAQs to explain acquirer and issuer transaction-related network fees.	KD
	03/09/2025	Added a note in the field description for ICC_System_Related_Data_DE55 that the field applies to both Visa and Mastercard (see JSON Data Types and EHI Fields).	KD
	23/07/2025	EHI version 5.1 now released for general availability. See EHI Versions.	WS
	24/07/2025	Added details to clarify how Acquirer fees are reported and how this affects card authorisation and balance updates. See How are Acquirer fees applied and reported?	WS
	06/08/2025	Updated the list of Merchant Category Codes (MCCs) to include MCCs 3304 and 3841-3853. See Merchant Category Codes.	WS
	24/07/2025	Added a note to clarify support for Master Virtual Cards (MVCs) on EHI Cooperative Processing (mode 2) with *approve with load*. See EHI Operating Modes: Approve with Load.	WS
	15/07/2025	Updates to the descriptions of the Processing Codes for PIN Change and PIN Unblock to clarify use of these codes.	WS
	10/07/2025	Removed references to EHI mode 5, which has been decommissioned.	WS
	03/07/2025	Added additional information to the Transaction Matching section on matching for incremental authorisations and revised the FAQ on incremental authorisations and how to identify them.	WS
5.0.17	03/07/2025	Added a note to the description of Additional_data_de48 to clarify the usage of this field. See GetTransaction Message Fields.	WS
	03/07/2025	Added further details on the use of the MerchantAdvice field and use of Merchant Advice Code 03. See GetTransaction Message Fields: MerchantAdvice. See also the FAQs: What is the MerchantAdvice field and how is it used?	WS
	03/07/2025	Updated the example for POS_Date_DE13. Provided more details of how traceid_lifecycle is constructed. See GetTransaction Message Fields.	WS
	27/06/2025	Updated the card status codes page to indicate that Card Status Codes G5 and G6 (temporary blocks) can also be set by Fraud Transaction Monitoring (FTM) service. See Card Status Codes.	WS
	20/06/2025	Clarified the description of multi_part_txn_final. See GetTransaction Message Fields.	SH
	16/05/2025	Added notes to clarify the use of the SubBIN field for 6-digit and 8-digit BINs. See GetTransaction Message Fields.	WS
	15/05/2025	Updated the FAQs with additional information on incremental authorisations and how to identify them.	WS
	08/05/2025	Added EHI response codes 12 and 15 to the Response Status Values page. Revised the description of response code 57. Removed card status code 57 from the Card Status Codes page. See PRN-220.	WS

Version	Date	Comments	Revised by
	08/05/2025	The Matching_Txn_ID field in EHI is now populated with data for the following types of transactions: Presentments, Authorisation Reversals, Incremental Authorisations and Incremental Authorisation Reversals. See GetTransaction Message Fields. See also PRN-224.	WS
	08/05/2025	Removed references to the 0120 A message type, as this is not supported. The appropriate message type to process is the 1240 A (for Mastercard) or 05 A, 06 A and 07 A (For Visa).	WS
	30/04/2025	Updated the description of the Settlement_Date field. See GetTransaction Message Fields.	WS
	16/04/2025	Added digital asset categories, for example Central Bank Digital Currency (CBDC) or tokenised deposits, to the list of POS codes. See Position 4 - Special Condition (existing debt) in Visa_POS_Data_DE60.	KD
	16/04/2025	Added the following codes for device binding that supports FIDO: 3749 and 3760. See Reason ID for an Authorisation.	KD
5.0.17	09/04/2025	Added Response Code 72 and 46 to the Response Status Values and the Resp_Code_DE39 pages.	KD
	09/04/2025	Added two new Visa response codes: 5C - Transaction not supported or blocked by issuer and 9G - Blocked by cardholder, contact cardholder. See Response Status Values.	WS
5.0.16	27/03/2025	Added references to the Thredd Secure Connectivity Framework.	KD
	17/02/2025	Multiple EHI endpoints functionality has been deprecated. See EHI Configuration Options.	WS
	07/03/2025	Updated descriptions and examples for how to handle processing errors due to invalid characters. See Troubleshooting FAQs.	JB
	07/03/2025	Added extra values 100 and 100 for 'Message_Why' field in Appendix A.26 (Response_Source_Why + Message_Why).	JB
	17/02/2025	Added details of how to set up multiple EHI endpoints (URLs). See EHI Configuration Options.	WS
	13/02/2025	Added new processing codes for Credit Account Status Inquiry (ASI) and Debit ASI to Transaction Codes.	KD
	13/02/2025	Updated the description of the 9030 reason code in the Visa_STIP_Reason_Code field.	WS
	12/02/2025	Added references to Thredd Portal, our new web application for managing your cards and transactions.	WS
	20/01/2025	Added 3169 RIYADH AIR to Merchant Category Codes.	WS
	16/01/2025	Added the *V1045D0082* tag, 35AN Plan Registration System Identifier, to the Misc_TLV_Data Field.	WS
5.0.16	16/01/2025	Corrections to JSON tokenisation examples: ACN, TCN and TEN messages should have Txn_Type = J. ACN messages should have an MTID = 0120, while TCN and	WS

Version	Date	Comments	Revised by
		TEN messages have an MTID = 0620. See GetTransaction Example Messages.	
5.0.16	19/12/2024	Added incremental authorisation message examples to the section GetTransaction Example Messages.	KD
5.0.16	06/12/2024	Updated the format of the Acquirer_Reference_Data_031 field to AN(8,23). See GetTransaction Message Fields. See PRN-200.	WS
5.0.16	29/11/2024	Added a note to indicate that the functionality to update the balance in Mode 4 (Gateway Processing with STIP) is currently only available via SOAP Web Services. See EHI Operating Modes.	WS
5.0.16	08/11/2024	Added examples of tokenisation messages to the section GetTransaction Example Messages.	WS
5.0.16	06/11/2024	Added the following codes for Reason ID: 3717, 3748, 3755. See Reason ID	KD
5.0.16	06/11/2024	Updated AVS Results page. Removed unused codes, and clarified address and postcode/zip code results for US and non-US addresses.	KD
	07/11/2024	Updated the description of response code 61 to remove the previous restriction on Visa usage, as this code is now supported by Visa. See Response Status Values.	WS
	31/10/2024	Added FAQ item for Mastercard STIP. See General FAQs.	KD
	01/10/2024	Added an example of a balance enquiry message. See GetTransaction Example Messages.	WS
5.0.16	12/09/2024	Removed references to VPN.	WS
	02/09/2024	The inclusion of the Merch_Country field is typically *Optional*, but may be mandatory in certain cases, depending on the program or service being processed. See GetTransaction Message Fields.	WS
	15/08/2024	Added 3437 CITE RENT-A-CAR to Merchant Category Codes.	JB
	13/08/2024	Added notes to clarify that some credit/refund transactions may be reported as follows: • Visa: MTID '05pp', Txn_type 'P' (with processing code 20xxxx). • Mastercard: MTID '1240', Txn_type 'P' (with processing code 20xxxx). See Transaction Matching.	WS
	06/08/2024	New FAQ added, explaining how fees are applied and reported for declined transactions. See the FAQs.	WS
	06/08/2024	Clarification that response code 96 may trigger card Scheme Stand-In Processing (STIP) for both Visa and Mastercard, depending on your STIP setup. See Response Codes.	WS
	01/08/2024	Added sort functionality to the tables in the online guide version.	WS
	25/07/2024	Added "U - No data received" to the list of possible AVS Results.	WS
	17/07/2024	Updated the description of Txn_GPS_Date. See GetTransaction Message Fields.	WS
	02/07/2024	Updated the company address.	PC

Version	Date	Comments	Revised by
5.015	22/04/2024	Updates to field descriptions in JSON Data Types and EHI Fields.	WS
5.015	27/06/2024	Removed the MTID value of 0100 from the Automatic Authorisation Reversal message on the Transaction Matching and GetTransaction Message Fields pages.	JB
	31/05/2024	Clarification on use of the 3-digit country code for Romania. See Country Codes.	WS
	28/05/2024	Added a new value to the GPS_POS_DATA field position 32, to indicate, whether the acquirer requested a 30-day clearing extension (Visa Only). See GPS_POS_Data Field.	WS
	22/04/2024	Revised description of the usage of the 0101 A Authorisation Repeat message (Visa Only). See Transaction Matching.	WS
	28/03/2024	Added descriptions of usage of positions 27-31 in the GPS_POS_Data field. See GPS_POS_Data Field.	WS
5.0.14	14/03/2024	Added note to state that EHI feeds in JSON cannot send fields to externally hosted systems where its data values are blank. This differs from EHI data feeds for XML that allow the sending of fields with blank values. See JSON Data Types and EHI Fields.	KD
5.0.14	14/03/2024	New terminology introduced around EHI modes: *Gateway Processing* (mode 1), *Cooperative Processing* (mode 2), *Full Service Processing* (mode 3) and *Gateway Processing with STIP* (mode 4). See EHI Modes.	WS
	12/03/2024	New Merchant Category Code (MCC) added: 3168 Hainan Airlines (as part of Visa mandate 2024 Q2 VISA Article 2.5 Changes to Merchant Category Codes and Response Code). See Merchant Category Codes.	WS
	12/03/2024	Added additional processing codes and account types now supported by Visa (as part of Article 2.1 Changes to Support Global Processing Alignment for Issuer). See Processing Codes. For more information, see PRN-179.	WS
	07/03/2024	Clarified how the transaction status of *Cleared (C)* and *Settled (S)* impacts the card balance. See Transaction Status Codes.	WS
	07/03/2024	Correction to description of the processing code for ASI transactions listed in the FAQs section. Should be 39.	WS
	14/02/2024	Added examples of Financial Reversals (1240 type E messages). See GetTransaction Example Messages.	WS
	14/02/2024	Updated the list of values that can be returned in the Visa_ResponseInfo_DE44 field position 5 (CVV/iCVV/dCVV result). See Visa_ResponseInfo_DE44.	WS
	10/01/2024	Added details to clarify the usage of the Resp_Code_DE39 field. See GetTransaction Message Fields.	WS
	02/01/2024	Clarified usage of the Auth_Code_DE38 field: an authorisation code is generated for both approved and declined authorisations. See GetTransaction Message Fields.	WS
	02/01/2024	Added a new page to describe the HTTP header fields in EHI request and response messages. See HTTP Message Format.	WS
	02/01/2024	Added a note to clarify that the EHI message response should not contain the value "null" in any response fields where EHI is expecting a numeric value, as this may result in EHI declining the transaction. See Response Message Fields.	WS

Version	Date	Comments	Revised by
5.0.13	13/12/2023	Added MCC code 5262 to the Merchant Category Codes page. See Merchant Category Codes.	KD
	13/12/2023	Added details of how to use the Resp_Code_DE39 field when returning a decline response to Thredd. See the appendix Resp_Code_DE39 Values.	WS
	06/11/2023	Correction to matching logic table for transactions of type 1240 N. See Transaction Matching.	WS
	02/11/2023	Updates to the WSDL for the EHI XML version. See GetTransaction WSDL.	JB
	24/10/2023	EHI can now support up to two External Host URLs per card product. See EHI Configuration Options.	WS
	21/09/2023	Added details to clarify that the field PaymentToken_creatorStatus can contain " " or be empty when no value has been provided. See Payment Token Fields.	WS
	14/09/2023	In the section Checking fields used for 3D Secure Authentication, added a note and reference to the PSD2 and SCA Guide.	WS
	22/08/2023	In the GetTransaction Message Fields section, added information on the interchange fee received in the Interchange_Amount_Fee and Interchange_Amount_Fee_Settlement fields.	WS
5.0.12	31/07/2023	In the GetTransaction Message Fields section, updated the Request Message Fields headings to clarify whether this applies to authorisation, financial or non-card network messages. On the GPS_POS_Data field page, fixed the link to the Card Present Indicator section. Added further information describing the use of transaction processing codes 01,02,11, 12, 21, 26, 28 and 39. See Processing Codes.	WS
	23/06/2023	Added a new section describing implementation of Dynamic CVV2 functionality. This section is also available as a stand-alone document.	WS
	31/05/2023	Updated Operations email address to be occ@thredd.com	MW
5.0.12	16/05/2023	Updated the Trans_link field data type from *Number* (Long) to *String*, to align with the RFC 8259 Standard for JSON fields. See JSON Data Types and EHI Fields. See PRN-154.	WS
5.0.12	27/04/2023	Guide rebrand to new company name and brand identity.	WS
5.0.11	06/04/2023	Added a new appendix which provides details of the contents of the Trans_Link Field.	WS
	07/03/2023	Added a note to explain that in EHI Mode 2, you can override the Thredd decline code of 51 (Insufficient Funds) with another decline code, if you would like to use a more specific decline reason to be passed to cardholder. See EHI Operating Modes.	WS
5.0.11	02/03/2023	Added further details and clarification on the use of JSON data types and the compatibility of EHI fields with the IEEE 754 binary-64 (double precision) format. See JSON Data Types and EHI Fields.	WS
5.0.11	02/03/2023	Correction to description of the *token* field and its possible values. See GetTransaction Message Fields.	WS

Version	Date	Comments	Revised by
	02/03/2023	In the GetTransaction Message Fields section, updated the maximum length and maximum values for the following fields: *Token*, *TXn_ID*, *TLogIDOrg*, *Trans_link* and *Matching_Txn_ID*.	WS
	28/02/2023	Added Chinese Offshore Renminbi (currency code CNH) to the list of supported currencies. See Currency Codes.	WS
	20/02/2023	Added two new Visa Merchant Category Codes (MCC): 3839 and 5723. See PRN-147. Added a note to clarify the use of *GPS_POS_Capability* position 44. See GPS_POS_Capability field.	WS
5.0.10	15/02/2023	Added a note to *GPS_POS_DATA* Cardholder Authentication Methods, to indicate that it is possible for merchants to send two authentication values, which are recording in positions 4 and 5. Added details to clarify how the transaction processing codes 01, 12 and 17 are used. See Processing Codes and the Troubleshooting FAQs. Fixed version numbering issue.	WS
	25/01/2023	Updated the FAQs with additional information around clearing files. Updated the description of the following fields to clarify their usage: *POS_Data_DE61*, *POS_Data_DE22* and *Merch_Name_DE43*. See GetTransaction Message Fields.	WS
5.0.10	20/01/2023	Updated the GetTransaction Example Messages.	JB
5.0.10	05/01/2023	Added a note to indicate that if the *CVV2_Result* field is blank, then the merchant did not provide this information. In this case, Thredd will not complete the CVV2 pre-check and will authorise or decline the transaction based on the card usage group settings for your programme. See GetTransaction Message Fields. Amended the description of *Auth_Code_DE38*. Thredd will generate this code for an approved authorisation request.	WS
	01/12/2022	Updated the Copyright Statement Updated the headings for the GPS_POS_Capability field, GPS_POS_Data field and the POS_Data_DE61 field.	MW
5.0.10	01/12/2022	New cut-off messages in JSON format now available. See Cut-Off Message Example.	WS
5.0.9	22/11/2022	Added further matching criteria for the MTIDs TC25, TC26 and TC27 in transaction matching.	JB
	11/11/2022	Added a note to the transaction matching section for 0400 authorisation reversals about Visa transactions potentially missing an Auth_Code_DE38 value and how to treat this.	WS
	10/11/2022	Added Glossary definitions for OCT and AFT transactions.	WS
5.0.8	26/10/2022	Added a note and examples of cut-off message, which are currently only available in XML format.	WS
	13/10/2022	Added a new value of '*L*' (delegated authentication) to the *GPS_POS_Data* field, position 15 (3D secure authentication method). See GPS_POS_Data field.	WS
	03/10/2022	Added status code 59 to the table of status values appearing in the Resp_Code_DE39 field.	WS
	03/10/2022	Added new sections on Refunds and Financial Reversals to the Transaction Flow	WS

Version	Date	Comments	Revised by
		Scenarios section.	
5.0.8	14/09/2022	Updated the examples on the GetTransaction Example Messages page.	JB
5.0.8	08/09/2022	Added new column to 3D Secure Authentication Method section of GPS_POS_Data field to differentiate between the differences between Mastercard and Visa. Also clarified content for Mastercard SPA v2.	JB
	05/09/2022	Added a new Currency Code, SLE, for the new Sierra Leonean leone.	WS
	01/09/2022	Added a note to the description of data types*AmountUnsigned* and *AmountSigned* to clarify that values can contain up to four decimal places. For customers processing currencies that have more than 2 decimal places, we now round this off to 2 decimal places and add zero padding for the remaining decimal places; see GetTransaction Message Fields > Rounding off of currencies with exponents greater than 2. See PRN-116.	WS
5.0.7	18/08/2022	New Merchant Category Codes added.	WS
	04/07/2022	For fields of data type *AmountSigned*, the number of supported decimal places has been updated from 9.2 to 19.4. For example: *72.1230*. See GetTransaction Message Fields. Examples in the GetTransaction Example Messages also updated for this change. See PRN-114. Corrections made to POS_DATA_DE22 Authorisation and POS_DATA_DE22 Mastercard appendices. Corrections made to MTID references on Processing EHI Transactions.	WS
5.0.6	10/03/2022	Added a new appendix to describe Special Characters that may be used in fields of Data Type ANS.	WS
	31/03/2022	Removed the field *FxProviderBookedRate*.	
	07/04/2022	Processing Code (*Proc_Code*) = 39 is now used to identify an Account Verification transaction. See Processing Codes. See PRN-102.	
	19/04/2022	Updates to the description of the *Acquirer Exempt from SCA Indicator* in GPS_POS_Data field position 25. Added a new tag for Visa Base 1 e-commerce data to the Misc_TLV_Data Field. Standardised the field values used in the EHI field PaymentToken_PanSource so that they align with existing values already used in the EHI field GPS_POS_Data field position 3 (Card Data Input Method). See PRN-104. Updated examples in the guide to reflect that fields with no data are sent in a closed tag format and not as an open and close tag (e.g., as <Note /> and not as <Note></Note>).	
5.0.5	02/02/2022	New section added to explain Updating the STIP Balance (EHI Modes 4 and 5 only)	WS
	26/01/2022	GPS_POS_Data field position 18, *ExemptFromSCA* value 8 changed to "*Not a transaction under PSD2 rules*".	
5.0.4	22/12/2021	Updates to Misc_TLV_Data Field description to include new Sender and Receiver data tags. Updates to descriptions in SenderData and ReceiverData Fields. **Note**: Changed guide version number from 5.1 to 5.0.4 to reflect actual current version of EHI (5.0).	WS

Version	Date	Comments	Revised by
	14/12/2021	Additional information provided on Responding to Authorisation Declines and Responding to Partial Approvals. Changes to the description of the DECIMAL data type. See Data Types.	WS
	08/12/2021	Minor change to description in MTID field 1240. New fields added for Currency Cloud FX service: FxProviderCardholderRate and *FxProviderBookedRate*.	AL
	18/11/2021	New Visa examples provided for *AuthenticationMerchantHash*. See Matching Merchant Name. New data type of DECIMAL added to Data Types page.	WS
5.0.3	21/10/2021	New values in *GPS_POS_DATA* for 3D Secure Authentication: v = Authenticated by Mastercard IDCX ('Identity Check Express') service; z = AAV refresh transaction successfully authenticated by ACS. See 3D Secure Authentication Method. New guide using the EHI REST version is now available. Both versions of the guide have been updated to clarify differences between REST and XML message formats.	WS
	04/11/2021	For a Visa purchase with Cashback, Thredd now sends the value of *Proc_Code* as 09 (instead of 00) and includes the cashback amount in the *Additional_Amt_DE54* field. Thredd has standardised the format of the *Additional_Amt_DE54* field in the GetTransaction Message to use the format provided by GCMS IPM / Visa Base 2, which contains only the data (a multiple of 20 characters). See PRN-72. In ResponseStatus and Response_Code_DE39 the description of response code *78* has been updated to *Card is not active (including created but not yet activated)*	
	11/11/2021	Document updates: Corrected the spelling of *Responsestatus* in Transaction Flow Scenarios and Processing EHI Transactions. Additional details provided on transaction matching of Financial Reversals for Visa transactions. See Transaction Matching. New information provided to support matching transactions where the Acquirer data does not match; see Troubleshooting FAQs: Transactions and Matching. Information provided on Account Status Inquiry (ASI) transactions and how to identify them. Corrected the field name of AuthenticationMerchantHash. (This was previously incorrectly communicated as AuthenticationMerchantNameHash)	
5.0.2	27/09/2021	New value V = Account Verification added to the Auth_Type field in the GetTransaction message. See PRN-69. New description of how to respond to Authorisation Reversals. See Processing EHI Transactions. Updates to Card Status Codes to reflect new card block status codes. See PRN-48. Note: For additional information about Thredd updates to status and response codes, see the guide Changes to Thredd Card Status and Response Codes.	WS
5.0.1	10/08/2021	Added new EHI fields to authorisation messages for EHI version 5.0, which can be used to compare the 3D Secure authentication amount and currency to the authorised amount and currency: AuthenticationCurrency AuthenticationAmountUpper AuthenticationMerchantHash These fields can be used to comply with the PSD2 Strong Customer Authentication (SCA) Dynamic Linking requirements (see PRN-56). See Checking fields used for 3D Secure Authentication. Positions 25 and 26 have been added to GPS_POS_Data field, which you can use to identify if the authentication amount does not match the authorisation amount.	WS

Version	Date	Comments	Revised by
		Updates to recommendations for matching and handling authorisation advises and authorisation reversal requests. New appendix with Transaction Matching - Authentications and Authorisations. New optional MerchantAdvice response field added, for use when returning decline responses. In the ResponseStatus Values section, clarified when to use response codes 70 and 93.	
5.0	16/07/2021	Updates to reflect new fields added for EHI version 5.0. For details, see EHI Versions. New fields: Acquirer_Country ClearingFileId Network_Fraud_Data PaymentToken_PanSource ReceiverData SenderData Addition of new appendices: Network_Fraud_Data Format and SenderData and ReceiverData Fields. Changes to numbering in Appendices. Document corrections: Updated the GPS_POS_Data field, position 16 and 17 descriptions. Updated the incorrect spelling of the *Proc_Code* field in some descriptions which refered to this field. Updated the *PaymentToken_status* field description to point to the correct appendix to use for possible values: Card Status Codes. Changed the following field names to lower-case, to be consistent with how these are used in the GetTransaction message: auth_type, auth_expdate_utc, multi_part_txn, multi_part_txn_final, multi_part_number, multi_part_count. Updated the description for Incremental presentments	WS
4.1.13	06/07/2021	Updates to Amount Type Codes for the Additional Amounts field: added values 12, 42, 57 and 58.	WS
4.1.12	01/06/2021	Updates to response code appendices: new appendices for ResponseStatus Response Codes and Response_Code_DE39 Response Codes. New value of *N* for *Non-Card* and updates to description of *J* value in PaymentToken_deviceType.	WS
4.1.11	20/05/2021	In GPS_POS_Data field, changed the descriptions for SCA Assessment Result. Updates to Card Status Codes and Response Codes. New EHI E value for a mini-card in appendix PaymentToken_deviceType. New GPS_POS_Data field position 24: Card/Device Type (Form Factor).	WS
4.1.10	23/04/2021	In GPS_POS_Data field, added a new value of '3' for position 19, and news values of 8 and 9 for position 18; rewrote the SCA section to improve usability. Added new section for position 23.	WS
4.1.09	26/03/2021	Added new tokenisation transaction codes 32, 37 and 28 to Processing Codes. New tokenisation examples added New page with details of fields per EHI Versions	WS
4.1.08	25/02/2021	Major revamp to guide. New format and content rewrite. New Getting Started section and FAQs. Topics and appendices have been reorganised.	WS
4.1.07	16/03/2021	Added new values to ExemptFrom SCA field.	Mark
4.1.06	19/02/2021	Corrected 'CutoffDate' field in Cut-Off message as follows: Section 10.1 (Cut-off message request fields) – both Description and Data Type corrected. GPS_POS_Data field changes (Appendix A.24)	Mark

Version	Date	Comments	Revised by
		‘ExemptFromSCA’ position (Appendix A.24.13) Corrected ‘Low Value’ character from ‘L’ to ‘V’ Corrected ‘SCA Delegation character from ‘S’ to ‘D’ Added new value ‘O’ (15th letter of alphabet in capitals) for ‘Authentication Outage Exemption’ New positions added after ‘ExemptFromSCA’ Updated position list in A.24.1, and added comments after the table Extra example (with 22 positions) in Appendix A.24.18 added Correct field name typo from “Txn_Stat_Cde” to “Txn_Stat_Code” (see GetTransaction Message) New EHI response codes: 46, 78, 6P, 59, 93 (Appendix A.4) New Response_Source_Why and Message_Why values 83 to 97 (Appendix A.26) Appendix A.37 – Noted that for sending Visa Base1 raw values, ‘xx’ will be used for ‘all datasets’, and ‘xxxx’ will be used for ‘all tags’.	
4.1.05	10/02/2021	Corrected section 7.1.1 (WSDL response requirements). Updated contact details on first page.	Mark
4.1.04	27/01/2021	Added new Appendix A.41 to describe Additional_Data_DE48 format for Mastercard Authorisations & Clearing messages.	Mark
4.1.03	06/01/2021	Added new Cardholder Authentication Method values 7,9,A,B,C,D,E in GPS_POS_Data field (Appendix A.24.5) Added new Cardholder Authentication Entity value 7 in GPS_POS_Data field (Appendix A.24.6) Added info in A.24.10 (GPS_POS_Data 3d-secure method) to clarify that for Mastercard SPA v2, this information is not received by Thredd. Added explanation of DES in PIN fields (previously A.14)	Mark
4.1.02	20/10/2020	Added in A.37 the plans for Misc_TLV_Data tags	Mark
4.1.01	15/07/2020	Appendix A.37 (Misc_TLV_Data): - added ‘Value Format’ column - added tags: ‘CGBRDEBT01’, ‘CGBRDEBT02’, ‘CGBRDEBT03’, ‘CGBRDEBT04’ for UK debt repayment transaction information. Appendix A.7 - Standardised the headings - Renumbered Appendix A.7.8 (Examples of Amount Signs) from A.7.8 to A.7.9. - Inserted number Appendix A.7.8 with a Card Expiry example request and response	Mark
4.1.00	03/06/2020	Noted that Bill_Amt_Approved response field in section 9.1.2 GetTransaction Message Fields can be positive or negative (Thredd takes absolute value.) Section 9.1.1 fields ‘interchange_amount_fee’ and ‘interchange_amount_fee_settlement’ – corrected the case of their names. Added new field formats into section 8: - DatetimeRaw(Y_to_D) - Traceid - TraceidRaw - Rate Added 14 new fields, to provide additional diagnostic information for transactions: - Traceid_Message / - Traceid_Original - Network_Transaction_ID / - POS_Date_DE13 - Network_Currency_Conversion_Date / - Network_TxnAmt_To_BillAmt_Rate	Mark

<table>
<tr><th>Version</th><th>Date</th><th>Comments</th><th>Revised by</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>- Network_TxnAmt_To_BaseAmt_Rate</td><td>- Network_BaseAmt_To_BillAmt_Rate</td></tr>
<tr><td>- Network_Original_Data_Elements_DE90</td><td>- Network_Replacement_Amounts_DE95</td></tr>
<tr><td>- Network_Issuer_Settle_ID</td><td>- Visa_ResponseInfo_DE44</td></tr>
<tr><td>- Visa_POS_Data_DE60</td><td>- Visa_STIP_Reason_Code</td></tr>
<tr><td>- Mastercard_AdviceReasonCode_DE60</td><td>- Misc_TLV_Data</td></tr>
</table>
Existing fields can take new values:
- Reason_ID – Visa Base 1 reason code loaded here now
- ProcCode – new Transaction code “10” Account Funding
Existing field size extended: Additional_data_de48 now up to 5000 long
Split Appendix A.7.2 into A.7.2M (for Mastercard examples) and A.7.2V (for Visa Examples)
Added new appendices:
<table>
<tr><td>A.32.4 for new Reason_ID values from Visa</td><td>A.36 for Mastercard_AdviceReasonCode_DE60</td></tr>
<tr><td>A.37 for Misc_TLV_Data</td><td>A.38 for Visa_STIP_Reason_Code</td></tr>
<tr><td>A.39 for Visa_ResponseInfo_DE44</td><td>A.40 for Visa_POS_Data_DE60</td></tr>
</table>
Altered some Appendices:
<table>
<tr><td>A.10 Currency Code: table now takes less space</td><td>A.13 Merchant Category Codes: corrected table headings, table now takes less space</td></tr>
<tr><td>A.17 POS_Data_DE22: corrected to take into account different format for Visa Authorisation messages.</td><td>A.19 Country Codes: table now takes less space</td></tr>
</table>
Corrected order of fields in WSDL
<table>
<tr><td>From this:
- DCC_Indicator
- multi_part_txn
- multi_part_txn_final
- multi_part_number
- multi_part_count
- SettlementIndicator
- Clearing_Process_Date
- Settlement_Date
- Currency_Code_Fee
- Currency_Code_Fee_Settlement
- Interchange_Amount_Fee
- Interchange_Amount_Fee_Settlement</td><td>To this:
- Currency_Code_Fee
- Currency_Code_Fee_Settlement
- Interchange_Amount_Fee
- Interchange_Amount_Fee_Settlement
- Clearing_Process_Date
- Settlement_Date
- DCC_Indicator
- multi_part_txn
- multi_part_txn_final
- multi_part_number
- multi_part_count
- SettlementIndicator</td></tr>
</table>
Corrected order of fields in all examples to match the WSDL order.
Clarified section 9.1.1 descriptions of both “POS_Data_DE22” and “POS_Data_DE61” to make clearer differences between Visa/Mastercard and authorisation/clearing. (see GetTransaction Message Fields)
Appendix A.24.10 – 3D secure auth method: Added new value ‘C’
Section 7.4 -> added entry for MTID=0120 TxnType=’A’ (see GetTransaction WSDL and Examples)
Section 7.4 -> corrected entry for MTID=0120 TxnType=’J’
</td><td></td></tr>
<tr><td>4.0.03</td><td>14/02/2020</td><td>Corrected links in A.24 GPS_POS_Data field to these:
- InstantFunding_GPS</td><td>Mark</td></tr>
</table>

<table>
<tr><th>Version</th><th>Date</th><th>Comments</th><th>Revised by</th></tr>
<tr><td></td><td></td><td>- InstantFunding_Network
- ExemptFromSCA
Added Txn_Type value ‘K’ (Chargeback Reversal) to sections: A.2, 9.4, 5, 7.4, 7.3, 9.2
In A.17POS_Data_DE22 in Authorisation message – ‘10’ is valid for Mastercard (same meaning as Visa ‘10’)
In 7.3, noted that matching is not 100% accurate, and expanded rule on matching presentment (1240/05/06/07,P) to Auth (0100/0120,A/J)
In 7.4, note on 0400/D and 0420/D reversals to state that if the Txn_Amt matches, it is a full reversal.
In A.1 (processing codes), added ‘11’ (Quasi cash).
Corrected subsection 7.6.1 and 7.6.2 that were labelled 7.1.1 & 7.1.2
In A.24.13 (GPS_POS_Data field ExemptFromSCA position) added new value ‘1’
In 9.1.1 SettlementIndicator added values ‘3’ and ‘4’ (see GetTransaction Message Fields)
Renumbered Appendix A.7.7 (GetTransaction WSDL and Examples) to A.7.8 (to allow below insert)
Added Fee transaction (MTID=empty, Txn_Type=’P’) to sections 5, 7.3 and 7.4, 9.2, 9.5, and an example in inserted Appendix A.7.7</td><td></td></tr>
<tr><td>4.0.02</td><td>05/11/2019</td><td>Added new positions to GPS_POS_Data field: ExemptFromSCA
Throughout:
- Added in details for MTID 0101 Authorisation Duplicate (Visa only)
- Added in clarification for Visa second presentment MTIDs (05/06/07 N)
- Corrected the CVV2 field description and examples
- Added appendix A.24.11 for ExemptFromSCA field
- Added appendix A.34 for CVV2 field char 1 (if 6 chars)
- Added appendix A.35 for CVV2 field char 2 (if 6 chars)</td><td>Sarah + Mark</td></tr>
<tr><td>4.0.00</td><td>14/06/2019</td><td>Changed order of the following fields to match WSDL:
- Matching_Txn_ID (was underneath TLogIDOrg, now under auth_expdate_utc)
- Auth_Type (was underneath GPS_POS_Data now under Merch_Contact)
- Auth_Expdate_UTC (still underneath Auth_Type but auth_type moved)
- Reason_ID (was underneath Message_Why but now under Matching_Txn_ID)
- Dispute_Condition (still underneath Reason_ID but Reason_ID has moved)
Added new fields:
<table>
<tr><td>- Settlement_Service</td><td>- Central_Process_Date</td></tr>
<tr><td>- Settlement_Date</td><td>- Acquirer_Forwarding_ID</td></tr>
<tr><td>- multi_part_txn</td><td>- multi_part_txn_final</td></tr>
<tr><td>- multi_part_number</td><td>- multi_part_count</td></tr>
<tr><td>- currency_code_fee</td><td>- currency_code_fee_settlement</td></tr>
<tr><td>- interchange_amount_fee</td><td>- interchange_amount_fee_settlement</td></tr>
<tr><td>- DCC_Indicator</td><td>- Network_Chargeback_Reference_Id</td></tr>
<tr><td>Added new positions to GPS_POS_Data</td><td>- InstantFunding_GPS</td></tr>
<tr><td>- InstantFunding_Network</td><td></td></tr>
</table>
9.1 Field formats - clarified CVV2 formatting with position details (see GetTransaction Message Fields)
A.4. Response Codes - Added new response codes C0 and C1 for PSD2 compliance and response code 86
A.6 AVS results – added code Z</td><td>Sarah</td></tr>
</table>

Version	Date	Comments	Revised by
		A.29 PaymentToken_Wallet Added a number of new wallet providers supported by Visa	
3.1.0	12/03/2019	New request fields - Matching_Txn_ID to indicate the TXn_ID of the matching Authorisation for Financial transactions. - Auth_Type (to indicate if preauth, final-auth, or unknown) - Auth_Expdate_UTC (when Thredd/acquirer think authorisation will expire) - Reason_ID (eg reason code for a chargeback) - Dispute_Condition (Visa chargeback Dispute Condition) - Updated section 9 and examples in appendex A.7 for this. Removed spurious 'dd' from end of section A.7.2.1 (Auth example) and A.7.2.3 (Financial example). Added new section "3.3 EHI Interface Design considerations for Customers" Added notes to A.4 "Response Code Values" to state that for EHI modes 1,2, for Mastercards, response codes 91,92,96 will invoke STIP. Section 9.2 removed spurious sentence about "Authorisation Message Types" above the table. (see GetTransaction Message Fields) Removed these fields that are not provided (Thredd internal refs: DEV_MT_CORE-1429 and DEV_MT_CORE-1606) - Account_Type_From - Account_Type_To - Txn_Code Sections 9.1.1, 9.3.1, 9.4.1, 9.5.1 – re-ordered fields to match WSDL order of arrival. Now all field tables are in exactly the same order. (see GetTransaction Message Fields)	Mark
3.0.9	26/04/2018	Added value 26 (Original Credits) to Appendix 1.1, Transaction Code Values. Added additional response fields, AvlBalance_GPS_STIP and CurBalance_GPS_STIP in EHI response message components for Mode 4 enhanced functionality, in the following sections: 9.1.2 Response Field Formats (see GetTransaction Message Fields) 9.3.2 Response Message Fields A.7.1 GetTransaction WSDL A.7.2.2 Example Authorisation Response Message	Chip
3.0.8	24/04/2018	Appendix A.4 Response Code Values changes: - Removed spurious "Note – not all codes are" sentence - Added code 92 (Mark) - Added code 32 (Harry C)	Mark (92) Harry C (32)
3.0.7	05/04/2018	Added the value 12 to Transaction Code values in Appendix A.1.1 (part of ProcCode field). (see Processing Codes)	Harry C
3.0.6	07/03/2018	Section 9.1.1 correct format of "PaymentToken_activationExpiry" from Datetime(Y_to_ss) to Datetime(Y_to_nnn) to reflect what is actually sent. (DEV_MT_CORE-2613) Corrected date of 3.0.5 spec from 29/01/2018 to 06/03/2018 (in change logs at top and bottom.) Added Payment Token Activation Request (appendix A.7.2.5)	Mark
3.0.5	06/03/2018	Appendix A.29 PaymentToken_wallet values – 'ANDROID' wallet name changed from 'Android Pay' to 'Google Pay'. No field changes. Removed (MTID=0120, Txn_Type=A) and (MTID=0100, Txn_Type=D) from sections 9.2 and 9.3, as these combinations do not exist. Added MTIDs 25,26,27 (Visa Financial Reversals) into sections: 7.3, 7.4. Added MTIDs 05,06,07,25,26,27 into MTID field in section 9.1.1 (request message	Mark

<table>
<tr><th>Version</th><th>Date</th><th>Comments</th><th>Revised by</th></tr>
<tr><td></td><td></td><td>fields.) (see GetTransaction Message Fields)</td><td></td></tr>
<tr><td>3.0.4</td><td>09/01/2018</td><td>Added additional description in Appendix A.1.1 (Transaction Code values) for ‘36’ Transaction code.
Added extra values 51 to 55 for ‘Message_Why’ field in Appendix A.26 (Response_Source_Why + Message_Why)
Added new PaymentToken_creatorStatus value ‘D’ in Appendix A.28
Corrected email address on first page.</td><td>Mark</td></tr>
<tr><td>3.0.3</td><td>22/12/2017</td><td>Added values 47 to 50 for Response_source_why + message_why in section A.26
Added new wallet values FITBIT + PAYNETPHYR in section A.29 PaymentToken_wallet.
Added table borders in appendices A.25 to A.31.
Removed MTID=0120 Txn_Type=A from section ‘7’ as this combination does not exist.
Removed MTID=0100 Txn_Type=D from section ‘7’, as this combination does not exist (hanging auth removals are always created with MTID=’’ (blank).
Added enhanced description of reversals in section 7.4.</td><td>Mark</td></tr>
<tr><td>3.0.2</td><td>15/11/2017</td><td>Added 2 missing fields in GetTransaction to sections: A.7.1 (WSDL), Field info sections: 9.1.1, 9.3.1, 9.4.1, 9.5.1: (see GetTransaction Message Fields)
PaymentToken_deviceId
PaymentToken_deviceName
Added GPS_POS_Capability and GPS_POS_Data values and made POS/Merchant fields more consistent in examples in sections:
- A.7.2.1 (Auth request example)
- A.7.2.3 (Auth Advice example)
- A.7.3.1 (Financial request example)
Added fields after Message_Why to Auth Advice example in section A.7.3.</td><td>Mark</td></tr>
<tr><td>3.0.19</td><td>19/02/2019</td><td><table>
<tr><td>7.1.1 WSDL GetTransaction response</td><td>Txn_Stat_Cde and Resp_Code_DE39 could indicate approval for EHI mode 4
SendingAttemptCount is value-1 for EHI mode 4</td></tr>
<tr><td>7.3 Transaction Matching</td><td>1240 dummy auth - added 05pp 06pp 07pp
corrected 05,06,07,25,26,27 -> add 2 spaces on the end</td></tr>
<tr><td>7.4 Transaction processing by receiver</td><td>0120 J -> add note in Description to say can arrive for network STIP and AFD
0420 D -> fix note as visa use both 0400 and 0420.
1240 A dummy -> add 05pp 06pp 07pp
05,06,07,25,26,27 -> add 2 spaces on end</td></tr>
<tr><td>7.5 Incremental auths</td><td>Added expected final transaction amount
added notes on if final tranasaction amount too high or too low
clarified some language</td></tr>
<tr><td>7.6 Added section on Exception transactions</td><td></td></tr>
<tr><td>9.1.1 Request fields: (see GetTransaction Message Fields)</td><td>Settle_Amt: description corrected
LoadType: corrected link to valid values
POS_Time_DE12: clarified description
Status_Code: clarified description
payment-token fields corrected examples for visa/mc:
- PaymentToken_id
- PaymentToken_expdate</td></tr>
</table></td><td>Mark + Glenn</td></tr>
</table>

Version	Date	Comments	Revised by
		<table><tr><td></td><td>- PaymentToken_type - PaymentToken_status - PaymentToken_creatorStatus - PaymentToken_wallet - PaymentToken_deviceType - PaymentToken_lang - PaymentToken_deviceTelNum - PaymentToken_deviceIp - PaymentToken_activationCode - PaymentToken_activationMethod - PaymentToken_activationMethodData</td></tr><tr><td>9.1.2 Response fields:</td><td>- Update_Balance - added note that WS_BalanceUpdate can also be used to update the balance.</td></tr><tr><td>9.2 = added visa clearing mtids</td><td>05pp,06pp,07pp (fin) 25pp,26pp,27pp (fin rev)</td></tr><tr><td>9.3.1 - request fields:</td><td>- Resp_Code - notes for modes 4 added</td></tr><tr><td>9.3.2 - response fields</td><td>- CurBalance + AvlBalance conditional based on EHI mode, proccode and if approved - AvlBalance_GPS_STIP + CurBalance_GPS_STIP - now made conditional with explanation.</td></tr><tr><td>9.4 - added the visa MTIDs</td><td>05pp,06pp,07pp (txntype A and P) 25pp,26pp,27pp (txntype='E' financial reversal)</td></tr><tr><td>9.4.2 - Response message fields:</td><td>AvlBalance_GPS_STIP + CurBalance_GPS_STIP - now made conditional with explanation.</td></tr><tr><td>A.1.1 added 70, 71, 72 proccodes</td><td></td></tr><tr><td>A.3 clarified Txn_Stat_ Cde 'C' (Cleared)</td><td></td></tr><tr><td>A.7.7 – new section added to aid understanding of amount signs</td><td></td></tr><tr><td>A.13 MCC ranges:</td><td>- removed all non-descript ranges of 2+ MCCs - removed entries which were duplicated (kept correct description) - removed “DISALLOWED” if not appropriate (Various entries) added 3733 "Boca Raton Resort" added 3736 "Colorado Belle Edgewater Resort" added 3739 "Woodside hotels and resorts"</td></tr><tr><td>A.19 Country codes</td><td>- Added Kosovo, to see UNMI Kosovo</td></tr><tr><td>A.22 Bank Account Format</td><td>- Added table borders</td></tr><tr><td>A.26 added why values 71 to 82 inclusive</td><td></td></tr><tr><td>A.27 paymenttoken_ type</td><td>added BW - Browser Accessible Wallet</td></tr><tr><td>A.28 Paymenttoken_ creatorStatus</td><td>added I - Inactive</td></tr></table>	

Version	Date	Comments	Revised by
		A.29 PaymentToken_wallet: - Added STOCARD	
3.0.18	04/01/2019	Field POS_Termnl_DE41 is only mandatory for electronically-card-read transactions, so changed: Section 9.1.1 - POS_Termnl_DE41 description to add note (see GetTransaction Message Fields) Section 9.3.1 - Authorisation request fields: POS_Termnl_DE41 changed from “Mandatory” to “Optional” Section 9.4.1 - Financial request fields: POS_Termnl_DE41 changed from “Mandatory” to “Optional” Repeated the headers in country code table in A.19	Mark
3.0.17	17/10/2018	Existing section A.10 (currency codes) enhanced to provide the names of all the currency codes. Added a full table of country codes, providing the following details: - Country name / - Country 3-alpha code - Country 2-alpha code / - Country 3-numeric code	Ajeesh
3.0.16	16/10/2018	Addition of Garmin Pay and Mont Blanc pay Noted in section 1.2 that real time data feed permits sending real-time alerts to cardholders Numerous linguistic changes	Matt Clare
3.0.15	17/09/2018	Corrected MTID data type from N(1,4) to ANP(1,4) in section 9.1.1 (see GetTransaction Message Fields)	Harry C
3.0.14	14/08/2018	Corrected the following WSDL types in section A.7.1 from “s:int” (-2^31 to 2^31-1) to “s:long” (-2^63 to 2^63-1), so that data types are appropriate as per https://www.w3.org/2001/XMLSchema.xsd for the data content as described in chapter 9 (see GetTransaction Message Fields). These GetTransaction WSDL elements were corrected: “SubBin” from “s:int” to “s:long” “Balance_Sequence” from “s:int” to “s:long” “Balance_Sequence_Exthost” from “s:int” to “s:long” These GetTransactionResponse WSDL elements were corrected: “New_Balance_Sequence_Exthost” from “s:int” to “s:long” Added note at top section A.7 (WSDL) that the datatype definitions are found as per https://www.w3.org/2001/XMLSchema.xsd	Mark
3.0.13	07/08/2018	Corrected the Datatype (min,max) for: - Balance_Sequence (in section 9.1.1) (see GetTransaction Message Fields) - Balance_Sequence_Exthost (in section 9.1.1) - New_Balance_Sequence_Exthost (in section 9.1.2) Included that for all, the maximum value is 2^63-1 which has 19 digits.	Mark
3.0.12	31/07/2018	Section A.7.1 GetTransaction Message Fields, corrected request message: - Balance_Sequence changed minOccurs from “1” to “0” - Balance_Sequence_Exthost changed minOccurs from “1” to “0” Because these fields only exist properly for transactions sent at the time they occur (not for transactions sent after the event on the queue mechanism.) Expanded description in section 9.1.1 for fields “Balance_Sequence” and “Balance_Sequence_Exthost”. (see GetTransaction Message Fields)	Mark
3.0.11	20/06/2018	Removed spurious ‘7’ at start of section 9.1.2 (see GetTransaction Message Fields)	Mark

<table>
<tr><th>Version</th><th>Date</th><th>Comments</th><th>Revised by</th></tr>
<tr><td></td><td></td><td>Reinserted 3.0.8 comment above
Added 3.0.9 + 3.0.10 comment above
Appendix A.26 (‘why’ codes) – added value 56 to 70, and enhanced description of codes 51 (token status change), and 52 (token replacement)
Ensured this table is not too wide for the page.
Fixed some spacing in the changelog at top and bottom.
Improved spacing and commas (grammar) in section 5 (Transaction Types.)</td><td></td></tr>
<tr><td>3.0.10</td><td>07/06/2018</td><td>Minor corrections for editing errors in previous version.</td><td>Chip</td></tr>
<tr><td>3.0.1</td><td>15/11/2017</td><td>Added new fields in WSDL section Appendix A.7
Added new fields to examples in section A.7.1 and A.7.2.3.
Removed fields Txn_Code, Account_Type_From, Account_Type_To (from WSDL GetTransaction in Appendix A.7) as these are not sent.
Added these fields to the GetTransaction request example in section A.7.2.1 and A.7.2.3
<table>
<tr><td>source_bank_ctry</td><td>source_bank_account_format</td></tr>
<tr><td>source_bank_account</td><td>dest_bank_ctry</td></tr>
<tr><td>dest_bank_account_ format</td><td></td></tr>
<tr><td>dest_bank_account</td><td></td></tr>
<tr><td>GPS_POS_Capability</td><td></td></tr>
<tr><td>GPS_POS_Data</td><td></td></tr>
</table>
Aligned fields in the examples in sections A.7.2.1 and A.7.2.3 so fields are in WSDL order (and same order as we send)
Added MTID=0120 Txn_Type=J (Auth Advice) to section 9.2 – Transaction Type Decoding, and top of section 9.3 – “Transaction Type – Authorisation” to include it in the Authorisation message types. (see GetTransaction Message Fields)
Renamed Appendix A.18 from “POS_Data_DE22 in Financial Messages” to “POS_ Data_DE22 in Mastercard Financial Messages” to stress that this does not apply for Visa messages at all.
Added notes to existing fields as follows:
<table>
<tr><td>Merch_Name_DE43</td><td>now depreciated in favour of new Merch_... fields (for card txns)</td></tr>
<tr><td>POS_Data_DE61</td><td>now depreciated in favour of new GPS_POS_Capability and GPS_POS_Data</td></tr>
<tr><td>POS_Data_DE22</td><td>now depreciated in favour of new GPS_POS_Capability and GPS_POS_Data</td></tr>
<tr><td>Txn_Desc</td><td>see new Merch_... fields that may be more useful</td></tr>
</table></td><td></td></tr>
<tr><td>3.0.0</td><td>15/11/2017</td><td>Added new normalized POS and Merchant data fields as follows:
Added new fields to GetTransaction messages:
<table>
<tr><td><Merch_Name></td><td><Merch_Street></td><td><Merch_City></td></tr>
<tr><td><Merch_Region></td><td><Merch_Postcode></td><td><Merch_Country></td></tr>
<tr><td><Merch_Tel></td><td><Merch_URL></td><td><Merch_Name_Other></td></tr>
<tr><td><Merch_Net_id></td><td><Merch_Tax_id></td><td><Merch_Contact></td></tr>
</table>
(Updated sections 9.1.1, 9.3.1, 9.4.1, A.7.1 as a result)
GPS_POS_Capability (Appendix A.23) Added definitions of new positions 3-49 inclusive.</td><td>Mark</td></tr>
</table>

Version	Date	Comments	Revised by
		GPS_POS_Data (Appendiox A.24) Added definitions of new positions 1-22 inclusive.	
2.0.6	08/11/2017	Added Txn_Type=J (Auth Advice) to: - section 7.3 Transaction matching - section 7.4 Transaction processing - Appendix A.2 Txn_Type values Improved matching rules in section 7.3 for the following (MTID, Txn_Type) combinations: (0100, 'A'): added THIS.token=OTHER.token (0120, 'A'): added traceid_lifecycle and Auth_Code_DE38 (0120, 'D'): added traceid_lifecycle and Auth_Code_DE38 (0120, 'J'): added new rule (0400, all): added traceid_lifecycle, but noted it and auth_code_DE38 may be missing for timeout reversals (0420, all): added traceid_lifecycle, but noted it and auth_code_DE38 may be missing for timeout reversals (1240, 'P'): Changed to 2 rules, first with trans_link, then without trans_link. Added notes to section 7.4 that for 0400, 0420 reversals, first check the reversal is not a duplicate before doing any unblocking if needed. Added rules in 7.4 for Txn_Type='J' MTID=0120	Mark
2.0.5	18/10/2017	Section 7.3 Matching criteria corrected the following: - Removed Acquirer_Reference_Data_031 from all MTID=1240 TxnType='P' matching to Auths (as no DE31 in auth.) - Added traceid_lifecycle as a matching criteria (if it exists in financial) for MTID=1240 TxnType='P' matching to auths - Changed the MTID=05, 06, 07 (i.e. Visa presentments) matching to Auths to say do as MTID=1240 TxnType='P' Updated company info on front page	Mark
2.0.4	29/08/2017	Edited section 9.1 to specify MC/VISA fields. (see GetTransaction Message Fields) Edited section 9.4.1 to make the Resp_Code_DE39, TXN_Time_DE07 optional for financial messages. Included details for VISA in sections A.17, A.18, A.20	Sudheesh
2.0.4	07/09/2017	Added section 7.5 for incremental authorisations	Sudheesh
2.0.3	29/06/2017	Changed Txn_Time_DE07 to TXN_Time_DE07 in WSDL	Sudheesh
2.0.2	26/06/2017	Changed field ICC_System_Related_Data_DE55 internal format: From: (if Mastercard) - display binary (ASCII '0' and '1' chars – 8 chars for 1 byte) where the encoded bytes represent: - first 3 bytes: length of following data in binary bytes (1 binary byte is 8 ASCII '0'/'1' chars in the string), encoded as 3 ASCII digits '0' to '9'. - following bytes: EMV TLV data as Tag, Length, Value bytes encoded as Basic Encoding Rules (BER) as described in EMV Book 4.3 Annex B "Rules for BER-TLV data objects" - note that alls tags sent from the acquirer will be present (even if not defined by EMV) (if Visa) - Hexadecimal digits ('0'-'9' and 'A'-'F') where 2 hexadecimal digits represent 1 byte, where the encoded bytes represent: - First byte is full length of data - Next byte is value 1 (hex '01')	Mark

<table>
<tr><th>Version</th><th>Date</th><th>Comments</th><th>Revised by</th></tr>
<tr><td></td><td></td><td>- Next 2 bytes (4 hex digits) is the length of the following TLV data in binary bytes (eg ‘000F’ if 15 bytes (30 hex digits) follows
- Following bytes: EMV TLV data as Tag, Length, Value bytes encoded as Basic Encoding Rules (BER) as described in EMV Book 4.3 Annex B “Rules for BER-TLV data objects”
- note that alls tags sent from the acquirer will be present (even if not defined by EMV)
From examples (eg if sending tags 9F35 and 82)
Mastercard: 0011000000110000001110001001111100110101000000001
0010001010000010000000100001100110000000
Visa: 0B0100089F35012282021980
To:
- Hexadecimal digits (0-9 and A-F) where 2 hexadecimal digits represent 1 byte, where the encoded bytes mean:
- EMV TLV data as Tag, Length, Value bytes encoded as Basic Encoding Rules (BER) as described in EMV Book 4.3 Annex B “Rules for BER-TLV data objects”
- Note that alls tags sent from the acquirer will be present (even if not defined by EMV)
To example (eg if sending tags 9F35 and 82)
(for Visa and Mastercard): 9F35012282021980
Shrank text in section 9.1.2 (response fields) for field “New_Balance_Sequence_Exthost” to ensure it can all be read. (see GetTransaction Message Fields)
Added new note in section 7.3 (Transaction Matching) and section 7.4 (Transaction Processing) so that customer can match a 0100 incremental authorisation to a previous 0100 authorisation.</td><td></td></tr>
<tr><td>2.0.1</td><td>20/06/2017</td><td>1.Corrected casing for:
Acquirer_ID_DE32 -> Acquirer_id_DE32
Txn_ID -> TXn_ID
Txn_Time_DE07
Traceid_Lifecycle -> traceid_lifecycle
2.New response field CVV2_Result (sections 9.1.2, 9.3.2, 9.4.2, 9.5.2)</td><td>Sudheesh</td></tr>
<tr><td>2.0.0</td><td>02/06/2017</td><td>DEV_MDES-19 changes:
Added the following new optional PaymentToken_... fields for MDES:
<table>
<tr><td>- PaymentToken_id</td><td>- PaymentToken_creator</td></tr>
<tr><td>- PaymentToken_expdate</td><td>- PaymentToken_type</td></tr>
<tr><td>- PaymentToken_status</td><td>- PaymentToken_creatorStatus</td></tr>
<tr><td>- PaymentToken_wallet</td><td>- PaymentToken_deviceType</td></tr>
<tr><td>- PaymentToken_lang</td><td>- PaymentToken_deviceTelNum</td></tr>
<tr><td>- PaymentToken_deviceIp</td><td>- PaymentToken_activationCode</td></tr>
<tr><td>- PaymentToken_activationExpiry</td><td>- PaymentToken_activationMethod</td></tr>
<tr><td>- PaymentToken_activationMethodData</td><td></td></tr>
</table>
So therefore updated the following places:
- Section 9.1.1 field definitions (see GetTransaction Message Fields)
- Section 9.3.1 Authorisation request fields
- Section 9.4.1 Financial request fields
- Section 9.5.1 Non-Card-Network-Transaction request fields
- Appendix A.7.1 WSDL for GetTransaction
Added extra SOURCE codes to section A.25 (Response_Source and Message_Source values) as MDES PaymentToken_creator field uses some of the new values.</td><td>Mark</td></tr>
</table>

<table>
<tr><th>Version</th><th>Date</th><th>Comments</th><th>Revised by</th></tr>
<tr><td></td><td></td><td>Added new formats “Datetime(Y_to_D)” and “Datetime(Y_to_ss)” in section 8.1 Data Types
Added the following new Appendices, for new values related to PaymentToken_... fields:
Appendix A.27: PaymentToken_type
Appendix A.28: PaymentToken_creatorStatus
Appendix A.29: PaymentToken_wallet
Appendix A.30: PaymentToken_deviceType
Appendix A.31: PaymentToken_activationMethod and PaymentToken_ activationMethodData</td><td></td></tr>
<tr><td>1.5.9</td><td>28/04/2017</td><td>Changed WSDL for FirstTxn_ID and
LastTxn_ID to Long from Int, A.8 Cut-Off Message WSDL and Examples.</td><td>Arjun C V</td></tr>
<tr><td>1.5.8</td><td>27/03/2017</td><td>Made the following changes, in order to merge this version of the spec (hosted on confluence) with the changes I made to the incorrect version of the spec (hosted on JIRA DEV_EHI15-19)
Updated format of CutOffDate in CutOff message specification to YYYY/MM/DD hh:mm:ss - CS_PAGOBOX-16, 10.1 Request Message.
Replaced GetTransaction message WSDL with correct version - DEV_EHI15-26, A.7.1 GetTransaction WSDL. Changes from the original include:<table><tr><td>- <s:all>, replaced by <s:sequence></td><td></td></tr><tr><td>- GPS_POS_Capability</td><td>- GPS_POS_Data</td></tr><tr><td>- Acquirer_Reference_Data_031</td><td>- Response_Source</td></tr><tr><td>- Response_Source_Why</td><td>- Message_Source</td></tr><tr><td>- Message_Why</td><td>- traceid_lifecycle</td></tr><tr><td>- Balance_Sequence</td><td>- Balance_Sequence_Exthost</td></tr><tr><td>- Txn_Code</td><td>- Account_Type_From</td></tr><tr><td>- Account_Type_To (these are in request)</td><td>- Bill_Amt_Approved</td></tr><tr><td>- Update_Balance" type="s:int</td><td></td></tr></table>New_Balance_Sequence_Exthost (these are in response)
Added note on processing code values - CS_OX2B-30, A.1 ProcCode (Processing Code) values.
Removed section on Keepalive Timeout, as this functionality is not currently scheduled for release - DEV_MT_EHI-81, 3.2 Protocol Layer connection.
Added to description of Txn_GPS_Date, clarifying when this is set - CS_HOLVI-95, 9.1.1 Request Field Formats</td><td>Jake</td></tr>
<tr><td>1.5.7</td><td>27/03/2017</td><td>Added 3 new fields as different parts of existing Proc_Code field:<table><tr><td>Account_Type_From</td><td>Account_Type_To</td></tr><tr><td>Txn_Code</td><td></td></tr></table>For DEV_MT_CORE-1429.
Changed as a result:<table><tr><td>Fields in sections 9.x</td><td>WSDL for GetTransaction</td></tr></table>Examples
Added these fields (introduced in 1.5.3 above) into sections 9.3, 9.4, 9.5 (where it was missing):<table><tr><td>Balance_Sequence (request field)</td><td>- Balance_Sequence_Exthost (request</td></tr></table></td><td>Mark</td></tr>
</table>

Version	Date	Comments	Revised by
		<table><tr><td></td><td>field)</td></tr></table> Added these to Authorisation example in section A.7.2. Corrected typo ‘Responsestaus’ in section 9.5.2 (Non-Card Network Transaction response message.)	
1.5.6	17/02/2017	Added missing response fields: - Bill_Amt_Approved - Update_Balance - New_Balance_Sequence_Exthost to tables in sections: 9.3 (Transaction Type – Authorisation) 9.4 (Transaction Type – Financial) 9.5 (Transaction Type – Non-Card Network) And added these to the authorisation example in section A.7	Mark
1.5.5	14/02/2017	Section A.8 – Cut-Off Message WSDL Corrected Cut-Off Response Message element name from ‘th’ to ‘Cut_OffResult’ for Response element. (Example is correct.)	Mark
1.5.4	02/02/2017	Added new EHI mode 4 for DEV_EHI15-2 (balance stand-in.) Added new response fields: - Balance_Update - New_Balance_Sequence_Exthost For DEV_EHI15-2 balance stand-in. Clarified in MTID in section 9.1.1 that value ‘1240’ is used for both Financial Notification and Chargeback Notification (user must check TransactionType to tell the difference.) Section 9.1.1 value MTID ‘1442’ removed as we currently do not use this for chargebacks. (We may add 1442 in the future.)	Mark
1.5.3	21/10/2016	Added fields: <table><tr><td>- GPS_POS_Capability (in card related requests)</td><td>- GPS_POS_Data (in card related requests)</td></tr><tr><td>- Bill_Amt_Approved (in responses)</td><td></td></tr></table> Added new Appendices: <table><tr><td>- A.23 GPS_POS_Capability</td><td>- A.24 GPS_POS_Data</td></tr></table> Initially done to support partial approvals. Added these new fields to example Auth request message and Financial request message. Added field traceid_lifecycle for GetTransaction request messages (DEV_EHI15-5) Added in changes from EHI spec version 1.4.6 (adding MTID=”0120”, Txn_ Type=”D” (Auth reversal due to AFD 0120 advice):- Added the Automated Fuel Dispenser (AFD) Auth Reversal (due to AFD auth advice) which is: <table><tr><td>- MTID=”0120” (auth advice)</td><td>- Txn_Type=”D” (auth reversal)</td></tr></table> into the MTID + Transaction type tables in sections 7.3 (Transaction Matching), 7.4 (Transaction Processing) and 9.2 (Transaction Type Decoding. Added fields: <table><tr><td>- Acquirer_Reference_Data_031</td><td>Added Acquirer_Reference_Data_031 into the Financial matching logic.</td></tr></table>	Mark, Jake

<table>
<tr><th>Version</th><th>Date</th><th>Comments</th><th>Revised by</th></tr>
<tr><td></td><td></td><td>Corrected POS_Data_DE22 for authorisation messages (appendix A.17) – position 3 was slightly inaccurate regarding online vs offline PIN support (DEV_MT_EHI-88)
Added these fields for DEV_EHI15-2 for balance updating:<table><tr><td>- Balance_Sequence (request field)</td><td>- Balance_Sequence_Exthost (request field)</td></tr><tr><td>- Update_Balance (response field)</td><td>- New_Balance_Sequence_Exthost (response field)</td></tr></table>Added information on field usage.
Added these fields for DEV_EHI15-17<table><tr><td>- Response_Source</td><td>- Response_Source_Why</td></tr><tr><td>- Message_Source</td><td>- Message_Why</td></tr></table>The values are as described in DEV_TRXSCR-3 and fields map to columns of the same name on AUTHORISATION and 0120_STORE database tables.
Added Appendix A.25 to describe Response_Source and Message_Source values.
Added Appendix A.26 to describe Response_Source_Why and Message_Why values.
Added new Transaction type decoding combination of:
MTID=0120
Txn_Type='A'
to all the message decoding tables.
Added missing value “82” (PAN data on file) to POS_Data_DE22 in Authorisation message section (appendix A.17)
Added paragraph on keepalive timeout setting, configurable for every product, in 3.2 Protocol Layer connection.</td><td></td></tr>
<tr><td>1.5.12</td><td>30/05/2017</td><td>Corrected definition of POS_Time_DE12 field in section 9.1.1 Request Field Formats</td><td>Mark</td></tr>
<tr><td>1.5.11</td><td>16/05/2017</td><td>Removed spurious first sentence of section 7.1.1</td><td>Mark</td></tr>
<tr><td>1.5.10</td><td>02/05/2017</td><td>Corrected capitalisation of Agency Banking fields in GetTransaction to lower case to match WSDL and code:<table><tr><td>source_bank_ctry</td><td>source_bank_account_format</td></tr><tr><td>source_bank_account</td><td>dest_bank_account_format</td></tr><tr><td>dest_bank_account</td><td>dest_bank_ctry</td></tr></table>Fixed typo in section A.22 ‘r’ missing from ‘Source_Bank_Account_Format’
Added 2 new responsestatus code values in section A.4:<table><tr><td>30 – Format Error (to be used if customer thinks our request is invalid)</td><td>96 – System Malfunction (to be used if customer system has fatal error)</td></tr></table>Commented on these existing codes:<table><tr><td>17 – customer cancellation</td><td>68 – Response received too late</td></tr><tr><td>82 – Timeout at IEM</td><td>91 – Issuer unavailable</td></tr></table>To clarify usage in each case
Note: DEV_EHI16-7 will handle this on Thredd side.
For DEV_MT_CORE-1804 - Section 9.1.1 Request Field Formats new future trans_link format for offline cleared transactions (implementation date TBC). Also clarified existing formats.</td><td>Mark</td></tr>
<tr><td>1.4.5</td><td>18/07/2016</td><td>Moved this full change log down to this appendix.</td><td>Mark</td></tr>
</table>

Version	Date	Comments	Revised by
		GetTransaction Request field 'POS_Data_DE61' no longer has leading subfield 0 (3 digit length) – presence of this leading subfield was fixed in DEV_MT_EHI-26.) Fixed example Authorisation messages in section A.7 to remove leading '026' in field POS_Data_DE61	
1.4.4	12/04/2016	Corrected Fx_Pad in Authorisation and Financial to state that this amount is in the Billing Currency (Bill_Ccy.) Previously incorrectly stated as in the Transaction Currency (Txn_CCy.) Clarified that the Bill_Amt in Authorisation message does not include Fx_Pad amount field or MCC_Pad amount field. Inserted new section 8 – Data Types, which describes the common data types used for both GetTransaction and Cut_Off WSDL messages. Therefore, most of original section 8 (message formats) is now section 9. Created new table under new section 9.1 (Field Definitions for GetTransaction), which describes in a single place all of the field formats. This has been done so it is clear for the reader the overall format of each field, instead of describing it per message (Authorisation/Financial/Non-Card-Network.)	Mark
		Altered the Authorisation, Financial and Non-Card-Network tables to remove the field definitions, as these are now described in a single place in new section 9.1. Now you only need to record for Authorisation/Financial/Non-Card-Network which fields are mandatory / optional / omitted. Added section A.21 (Calculating the Total Transaction impact to the balance), and referenced it in section 6, so external hosts authorising the transaction are clear on the total transaction impact. (Note that partial auth approving by External Host (as per calculation in DEV_MT_CORE-587) would require the original fee rate percentages to be sent to External Host. Therefore, External hosts should not partial approve unless they are clear on the total balance impact with the partial approved amount.)	
		Noted in section A.4 (Response Codes) that Refer-to-issuer codes (i.e. "01") is not permitted from 16 April 2016 for Visa Transactions. Corrected POS_Data_DE61 field as Thredd send it including the 3 Banknet length digits at the front (although length may no longer match this due to trailing space removal on EHI transmission.) Renamed section 7 from "Request Response" to "Transaction Processing Requirements", and included new sections on: - How receiver should duplicate check - How receiver should match transactions Added 6 new fields to bottom of all GetTransaction Request messages for Agency Banking (Source_Bank_Ctry, Source_Bank_Account_Format, Source_Bank_Account, Dest_Bank_Ctry, Dest_Bank_Account_Format, Dest_Bank_Account.) Added new section A.22 for the values for Source_Bank_Account_Format and Dest_Bank_Account_Format. Added new fields for Agency Banking to the GetTransaction WSDL message (only present for Non-Card-Network transactions, of type Payment with LoadSRC=64 (bank transfer)).	
		Adjusted the payment transaction examples for new Agency Banking fields. Adjusted Appendix A.16 (Authorisation field Merch_Name_DE43) to state that if card acceptor is in Canada, then the 2-character Canadian province codes are present (instead of country code.) Corrected Cut_Off response message (section 10.2 Response Message) as the response field was incorrectly named. Removed initial text from section 7.1 Response requirements as other parts of the specification state the same thing clearer. Corrected "Acknowledgment" to "Acknowledgement" as that is what the field (defined in section 9.1.2 Response Field Formats). Renumbered section 8.1.1 to 8.1, and 8.1.2 to 8.2 (as there was no original section 8.1)	

Version	Date	Comments	Revised by
		Removed extraneous text from A.5 POS_Data_DE61 Values Added ‘Payment’ to section 5 (Transaction Types.) Added ‘Omitted’ as a Data Usage Type in section 8.2.	
1.4.3	09/03/2016	Adding message repeat counter field “SendingAttemptCount” for project DEV_ EHI14-7. This indicate will tell the receiver how many times we have repeated a message. (0=not repeated, 1=first repeat, 2=second repeat …) This field is applied to all non-CutOff messages. Clarified that currently, Thredd defines “Thredd Calculated Non-Domestic Fees” as Fees that apply when Txn_CCy ≠ Bill_Ccy. Clarified that currently, Thredd defines “Thredd Calculated Domestic Fees” as Fees that apply when Txn_CCy = Bill_Ccy. Updated all applicable fee descriptions as a result. Clarified in section 7 (Request and response), that Thredd will continue to re-send an EHI message until either <Acknowledgement> is set to “1” in response or Thredd reach maximum permitted re-tries.	Mark
		Added Txn_Type=’N’ (Second Presentment) into the Txn_Type values for MTID=1240. This is processed in the Financial Request message format. Renamed section 10.2 (TxnType), to use actual field name of Txn_Type (instead of TxnType.) Corrected setion 10.2 (Txn_Type) to specify that Txn_Type=’A’ (Authorisation) transactions can be either “Authorisation” or “Financial” formatted messages, as determined by the MTID field. Added Txn_Type new value of ‘G’ (Payment Transaction) for DEV_EHI14-4 project. Added to section 8.2 (Txn_Type / MTID) Txn_Type ‘G’. In the section 8 the “Balance Adjustment / Expiry” transaction types and “Load Unload” transaction types have been merged into a single section “Non-Card-Network Transactions”. This is clearer and simpler.	
		Renamed appendix “TxnStatCde” to “Txn_Stat_Cde” to precisely match the name of the field. Renamed appendix “AVS Result values” to “AVS_Result values” to precisely match the name of the field. Renamed appendix “POS Data DE61 …” to “POS_Data_DE61 …” to precisely match the name of the field. Renamed appendix “POS Data DE 22 …” to “POS_Data_DE22 …” to precisely match the name of the field. Added information from project DEV_MT_EHI-44. Added to section 7 and section 8 (Authorisation subsection) to indicate how customer detects a 0100 auth request being sent as an advice (due to original auth request was not correctly responded to in time.)	
1.4.2	07/03/2016	Inserted new section at 8.2 “Transaction Type Table” to indicate which Transaction type section is applicable for every message. Added Transaction type ‘C’ (Chargeback) to section 8 – Financial request message section, as chargeback comes under here. Clarified what combinations of MTID + Txn_Type mean in new section 8.2, and start of other sections in section 8. Added expanded descriptions of all the fee fields in section 8. Clarified that Bill_Amt does not include Thredd Calculated fees (Fee_Fixed and Fee_Rate). Changed examples in section 10.7 to have non-zero fee amounts. Clarified that Settle_Amt is what is received from the Network.	Mark
1.4.1	03/03/2016	Corrected field names in section 8 and WSDL section to ensure case correct to match actual fields sent in live. Corrected:	Mark

Version	Date	Comments	Revised by
		<table><tr><td>- Txn_Ccy -> Txn_CCy</td><td>- TXN_Time_DE07 -> TXN_Time_DE07</td></tr></table> Updated description for Additional_Data_DE48 to clarify customers should ignore this unless mutually agreed with Thredd (in which case Thredd would instruct you how to extract the required data from this field.) Added Authorised_by_Thredd field to Financial Request Message to align with existing functionality. Changed Authorised_by_Thredd field in Authorisation request message from Mandatory to Optional, as it might not be present (to align with existing functionality.) Added AVS_Result field to Financial Request message (to align with existing functionality.) Renamed new field PAN_sequence_number to PAN_Sequence_Number to align with standard field formatting for names and cases (first letter in each word in field is normally upper case.) Indented section A.8 Cut-Off Message WSDL to make easier to read. Corrected the Response field names to align with WSDL response in section 8. Renamed section 8 from “Data Dictionary” to “EHI GetTransaction Message Fields” to better reflect the fact that it corresponds to the GetTransaction in WSDL. In the WSDL Appendix, I’ve added an example request and response for each different message type.	
1.4.0.c	26/02/2016	Fixed typo in changelog for v.1.3.4 release (year 2014 -> 2015) Added section 10.20 for financial type message Merch_Name_DE43 field. Added response code 58 – Transaction not permitted to Terminal. (E.g. this might be used by client if card is not allowed in ATMs, but cardholder attempted to use at ATM.) Added response code 43 – Stolen Card (Pickup). Clarified in the Status Code section that not all codes are appropriate for card status values. Corrected response code “85” to action Approve instead of Decline. Section 6.3 – corrected wording of “Mode 3”, to clarify that Thredd will ignore any authorisation response messages received from customer in this mode. Removed Hyperlinks in the section 8 name fields – as links are all clearly mentioned in the description field. So now max of 1 link per field.	Mark
1.4.0.b	25/02/2016	Changed PIN encryption from using double length DES keys to Triple length DES keys. Triple DES with a triple length key is NIST approved up to 2030, and HSMs are known to support this. (See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf section 4.2.2.2). It provides a key space of 2^168 (about 3.7*10^50) possibilities. Currently Thredddoes not supporting AES PIN encryption as HSM support for this is unknown. But Pin fields support a possible future seamless migration. Inserted new section 8.1.2 Usage, to clarify that if a field is optional, it can be present with an empty value, even if Data Type does not permit an empty value. Clarified that POS_Data_DE61 might have anywhere between first 9 and all 14 subfields.	Mark
1.4.0.a	25/02/2016	Added: <table><tr><td>- CVV2</td><td>- Expiry_Date</td></tr><tr><td>- PAN_sequence_number</td><td>- PIN</td></tr><tr><td>- PIN_Key_Index</td><td>- PIN_Format</td></tr><tr><td>- PIN_Enc_Algorithm</td><td></td></tr></table> All these fields will only be present if both:	Mark

Version	Date	Comments	Revised by
		<table><tr><td></td><td>- Customer is configured to receive them</td></tr><tr><td></td><td>- And relevant data is received in the transaction</td></tr></table> Corrected Appendix 10.1 Processing code to correctly describe the 6 digit field (previously only the first two digits – the Transaction Code, were described.) Fixed Hyperlinks and Cross References. Cross reference example: A.1 ProcCode (Processing Code) values Hyperlink example: 10.1 ProcCode (Processing Code) values Re-wrote Appendix 10.5 (DE 61 POS Data) to add missing field values and clarify that not all fields may be present, and that subfields are concatenated. Added the following Appendices: Added PIN Block Formats appendix (10.14.1) Added PIN Encryption example appendix (10.14.2) Added Additional Amounts formatting appendix (10.15) Added Merchant name/location formatting appendix (10.16) Added POS Data DE22 Authorisation field formatting appendix (10.17) Added POS Data DE22 Financial field formatting (10.18) Added Country Codes (10.19) Removed Response code “32 – Completed partially” as not applicable. (For partial approval, use code 10.) Added Action column to Response code values appendix. Made Merch_ID_DE42 Optional in Authorisation and Financial, as this is not guaranteed to arrive for ATM transactions. New section 8.1 “Data Types” explains precisely what the formats mean in the rest of section 8 Data Dictionary. Changed all the data-types in section 8 to better describe the field content, in line with the new Data-Types. Corrected ActBal (actual balance amount in billing currency) from Numeric (5,2) to Amount (9,2) Reformatted document to remove the super-tables that 99% of the entire document was sitting inside. This cause lots of formatting problems. Now the ‘Navigation’ of heading works (MS Word -> View -> Navigation Pane.) Deleted all existing tables in the appendix, and re-created with the same data, as they had broken formatting.	
1.3.6	02/11/2015	Added Approval with Load functionality	Ajeesh
1.3.6	17/12/2015	Added details on fees Dom_Fee_Fixed, Non_Dom_Fee_Fixed, Fx_Fee_Fixed, Other_Fee_Amt, Fx_Fee_Rate, Dom_Fee_Rate and Non_Dom_Fee_Rate. Added DE124	Ajeesh
1.3.6	14/01/2016	Added comment on Approval with Load	Sudheesh
1.3.6	17/11/2015	Removed ‘06’ from Response code values	Ajeesh
1.3.5	16/10/2015	Data type length amended from Char(2) to Char(3) for field LoadSRC. Added appendix for field LoadType	Ajeesh
1.3.4	23/09/2015	Added valid values for AVS result field	Ajeesh
1.3.3	22/09/2015	Modified the data type for field Authorised_by_Thredd	Ajeesh
1.3	16/09/2015	Stand In for Mode 2, Cut off message, Added new fields to EHI - Additional_Data_DE48, Authorised_by_Thredd, AVS_Result, CU_Group, InstCode, MTID, ProductID, Record_Data_DE120, SubBIN, TLogIDOrg, VL_Group	Ajeesh

Version	Date	Comments	Revised by
1.2	25/08/2015	Applied consistencies in naming fields	Ajeesh
1.1	22/07/2015	Corrected Txn_Type and Txn_Stat_Code sample data values.	Ajeesh
1.1	13/08/2015	Correction in Web Services Security at Transport Level and Message Level	Ajeesh
1.1	23/06/2015	Added DE022	Ajeesh
1.1	25/06/2015	Added EHI WSDL, DE28 and DE54	Ajeesh
1.1	09/07/2015	Removed HTTP GET and POST from WSDL, Amount data type to double	Ajeesh
1.1	24/06/2015	Added mapping column in Transaction type table	Ajeesh
1.0	28/04/2015	Corrections	Ajeesh
1.0	06/05/2015	Corrections	Ajeesh
1.0	26/04/2015	Comments	Vlad Yanpolsky

Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Thredd UK Ltd.

Company registration number 09926803

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House

229-231 High Holborn

London

WC1V 7DA

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@thredd.com.