

EHl Guide

(JSON Version)

Version: 5.0.5

17/02/2022

Global Processing Services

6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA

Support Email: ops24@globalprocessing.com

Support Phone: +442037409682

For the latest technical documentation, see the [Developer Portal](#).

(c) 2021. Global Processing Services Ltd. 6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA
Publication number: JSON EHI-5.0.5-2/17/2022

Copyright

(c)2021. Global Processing Services All Rights Reserved.

The material contained in this guide is copyrighted and owned by Global Processing Services 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 Global Processing Services Ltd., and, then, only in such a way that the source and intellectual property rights are acknowledged.

To the maximum extent permitted by law, Global Processing Services 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 Global Processing Services Ltd. assumes no responsibility for any errors.

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 About this Guide

This guide describes the GPS 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 GPS, 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](#).

1.1.1 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 a copy of the GetMessages WSDL and message examples for different types of transactions, see [GetTransaction WSDL and Example Messages](#).

1.1.2 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., <code>"Bill_Ccy": ""</code>) • Optional - can be omitted (fields not included) or included with an empty value. Can be present (e.g., <code>"Bill_Ccy": "0"</code>) • Mandatory - field must be present. For example: <code>"Bill_Ccy": "978"</code>
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: <code>Bill_Ccy</code> or <code>Bill_Ccy</code> (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 .

1.1.3 Other Documentation

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 GPS Web Services API.
Cards API Documentation	For customers using the GPS REST-based Cards API, see the Cards API Docs Website .
Smart Client Guide	Describes how to use the GPS Smart Client to manage your account.
Chargeback Guide	Describes the chargeback process and options for managing chargebacks.

Document	Description
Transaction XML Reporting Guide	Describes the transaction XML report sent to Program Managers.
3D Secure Guide	Describes the GPS 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 Developer Portal .	

1.2 Overview

The External Host Interface (EHI) offers a way to exchange transactional data between the GPS processing system and the Program Manager's externally hosted systems. All transaction data processed by GPS 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

1.2.1 Real-time Transactional Data Feed

GPS receives global real-time card and payment-related notifications from the card schemes (Visa and Mastercard networks). These notifications are merged into a single GPS message format which your systems can process. The real-time notifications are sent via a secure VPN connection to the external host URL endpoint you have requested for your programme. These include notifications for: *Authorisations*, *Pre-sentments*, *Financial* messages, <

1.3 EHI Version Control

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

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

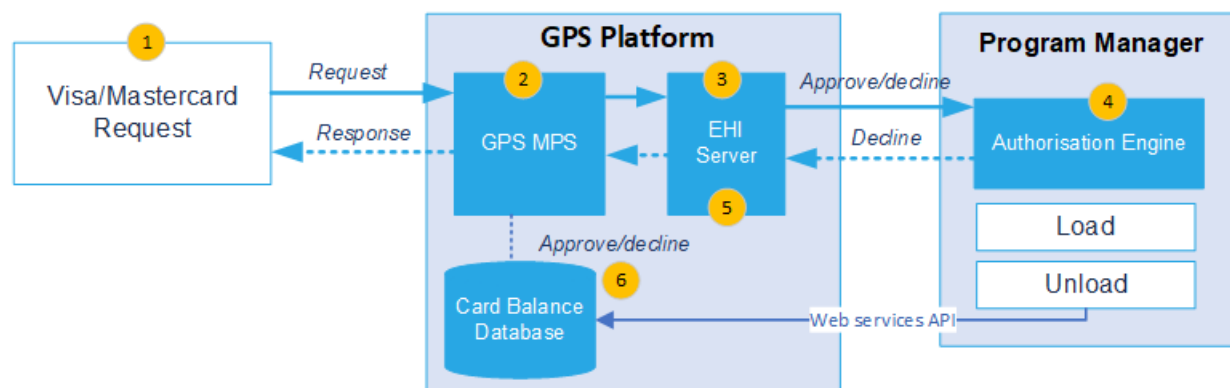
We distinguish between the following versions:

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

1.4 EHI Operating Modes

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

Mode	Who Author-ises?	Who Maintains the Balance?	GPS Stand-In	Details
1	External Host	External Host	No	Your systems maintain the balance and perform authorisation.
2	GPS	GPS / External Host	Yes	GPS maintains the balance and performs authorisation. You can override an approval decision. In Approval with Load your systems maintain the balance and can update the GPS-main-tained balance.
3	GPS	GPS	No	GPS maintains the balance and performs authorisation. You receive a read-only response.
4	External Host	External Host		



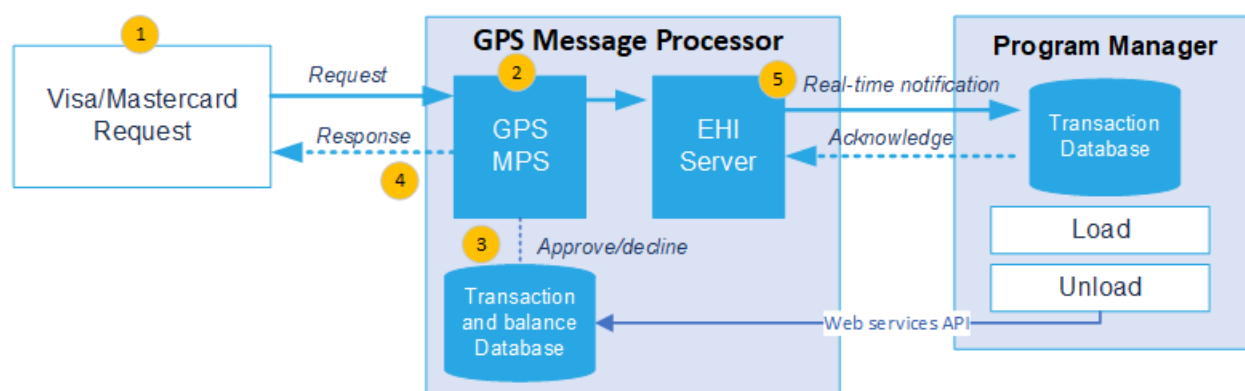


Figure 4: EHI Mode 3 - GPS approves and external host receives data subscription service only

1. The card scheme (Visa or Mastercard) sends an authorisation request.
2. The GPS Message Processing System (MPS) performs checks such as authentication, validation and fraud protection, as well as checks based on your product configuration.
3. GPS decides whether to approve or decline the transaction

1.4.5 EHI Mode 5 - External Host Maintains Balance (with GPS Stand-in)

As with EHI Mode 4, except that clearing transactions do not update the GPS stand-in balance (i.e. so only authorisation-related messages will change the stand-in balance).

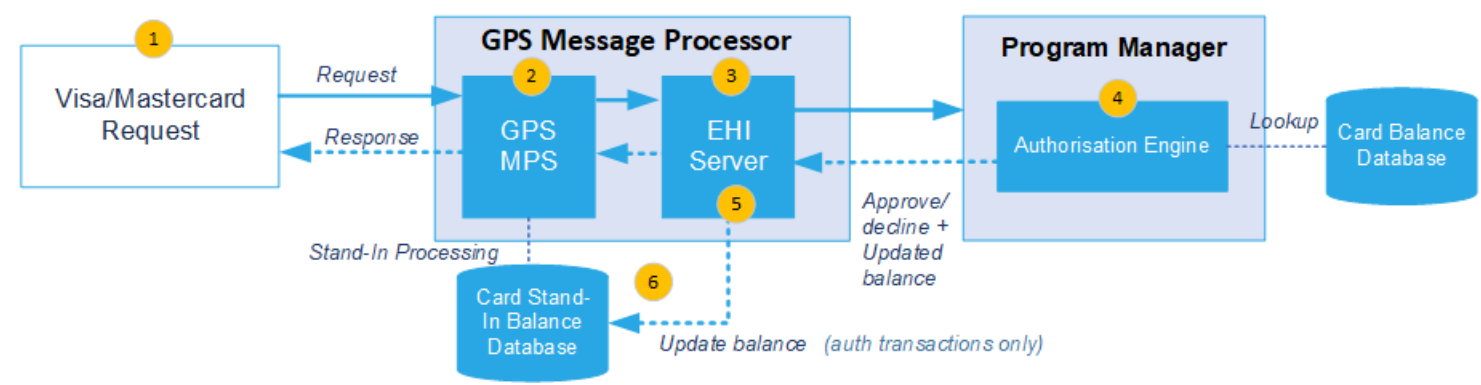
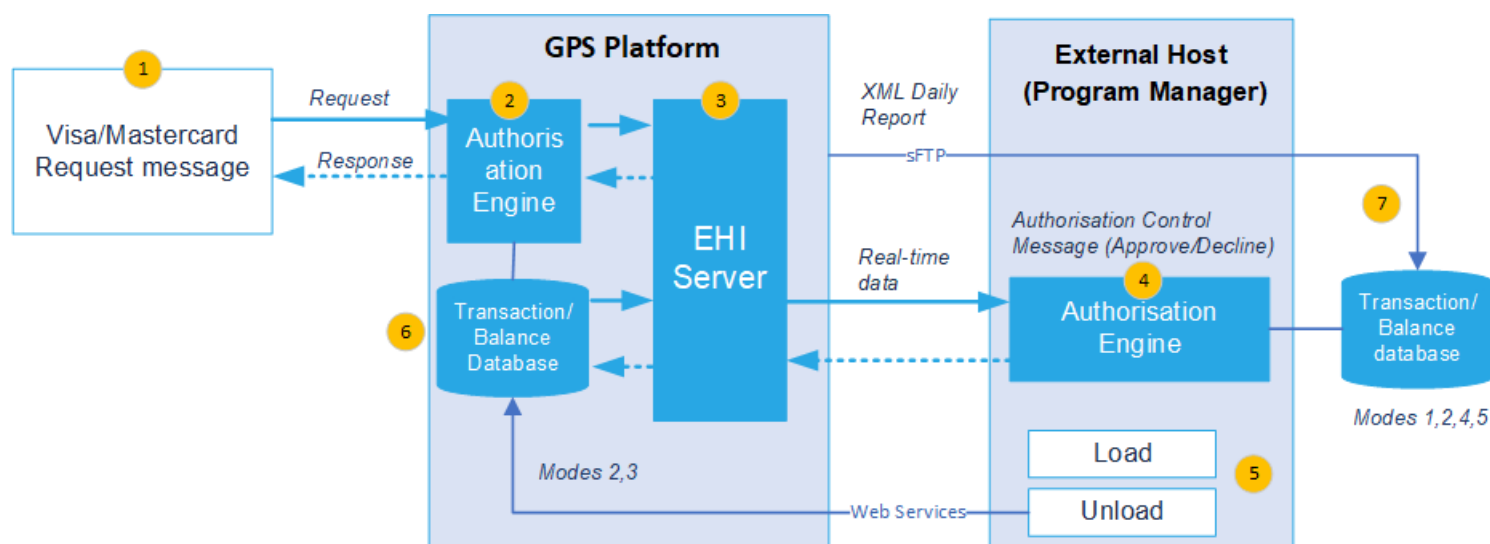


Figure 6: EHI Mode 5 - External host authorises, but GPS can approve if external host is not available

1.5 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 GPS system components and typical message flow.



GetTransaction WSDL

The GPS GetTransaction WSDL defines the structure of the GPS SOAP message sent to the external host and the structure of the response expected to be returned by the external host. The message format is based largely on the [ISO 8583 standard](#), with some differences which are unique to GPS.

For details and examples of GetMessages for different types of transactions, see [GetTransaction WSDL and Example Messages](#).

1.5.1 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. GPS 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 messages are sent over a VPN tunnel.

1.5.2 EHI Security

The EHI web services can use the TLS security protocol, which implements SSL Certification to provide a private and secure connection . You will need to provide the SSL certificate.

Note: In the production environment, we use a VPN for security reasons. We recommend not using TLS for performance reasons.

1.6 Card Payment Networks

GPS currently supports cards enabled for use by the Mastercard and Visa card schemes. These card schemes provide global card payment networks open to financial institutions and processors, which allows cardholders to pay with Mastercard and Visa enabled cards and merchants to accept card payments in their businesses worldwide. GPS operates on the card Issuing side, acting as the gateway between the Card Schemes (Visa and Mastercard) and the card issuers/Program Managers.

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

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

1.6.1 Card Payment (Network) Transactions

1.6.2 Non-Card-Network Transactions

These are transactions that are not originated via the Visa or Mastercard networks, 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.

1.7 Transaction Flow Scenarios

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

1.7.1 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 up 28 days to request the transfer of the authorised funds. 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 1,2,4 and 5.

1. The scheme sends an 0100 authorisation request to GPS.
2. GPS 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. GPS 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](#).

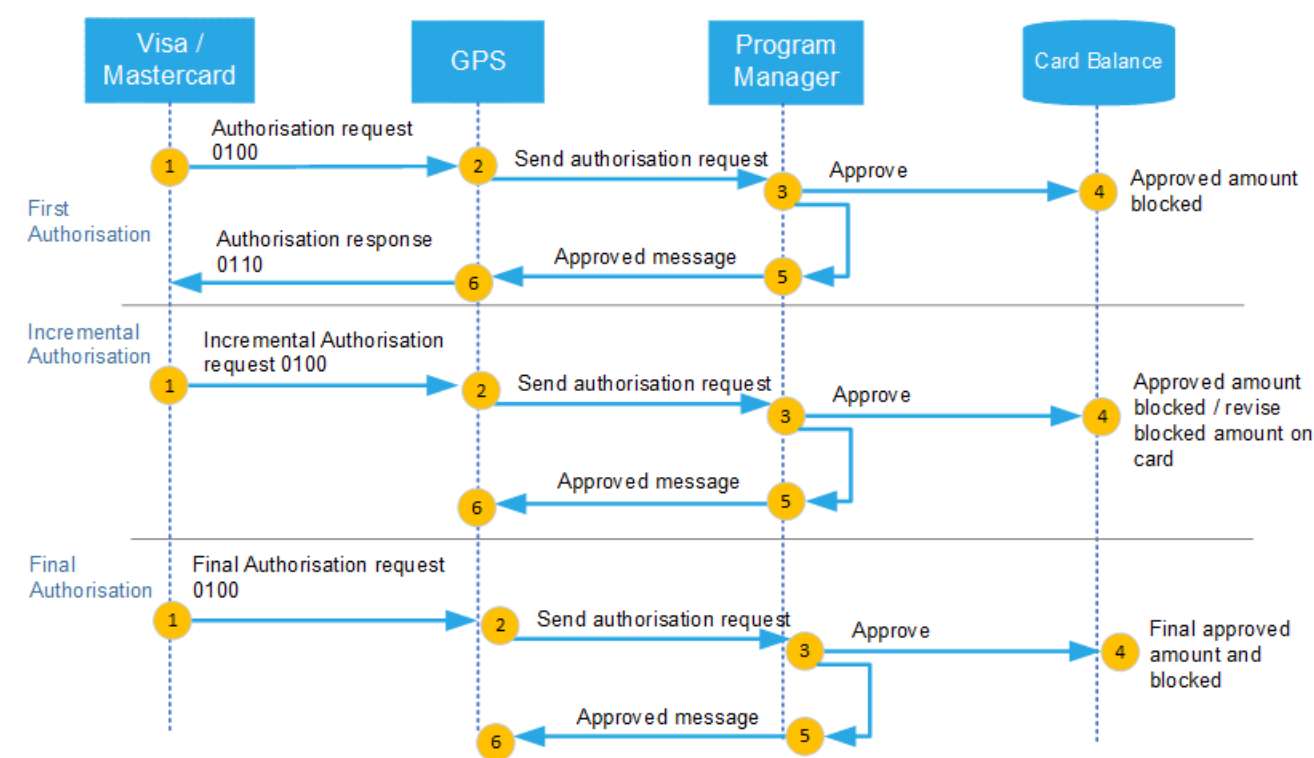
Acknowledgement = 1 informs GPS that the message was received and GPS does not need to resend.

Authorisation Reversal (network)

This type

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?](#)



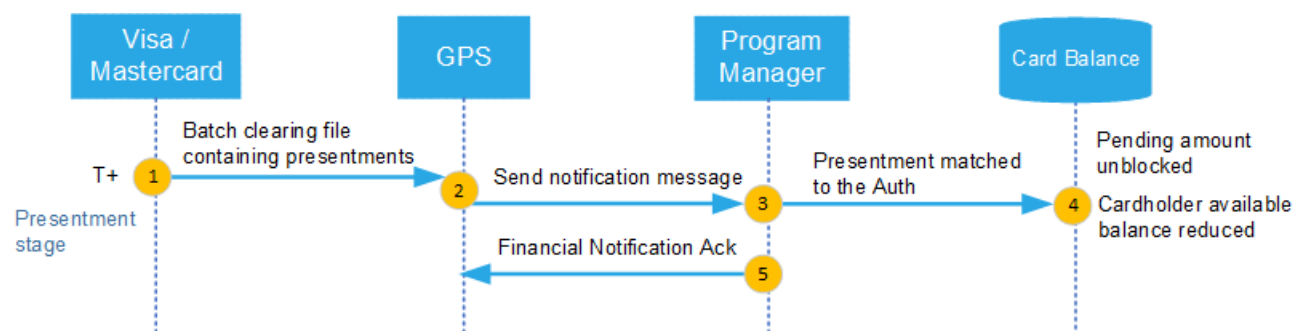


Figure 14: Presentment Flow

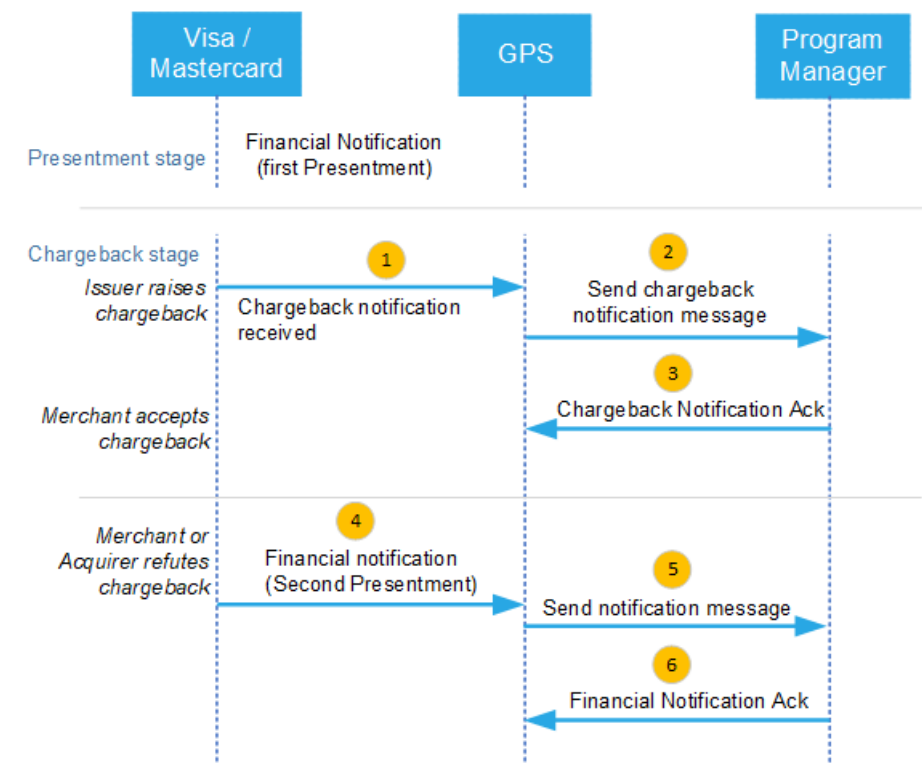
1. The scheme sends a batch clearing file to GPS.
2. GPS processes the file and sends a notification message per

1.7.3 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 GPS Smart Client. For more information, refer to the *GPS 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.



1.8 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.	EHI modes 1,2,4,5: Approve or decline. If approved and you maintain the balance, block the approved amount on the customer's card.	EHI modes 1,2,4,5: Return a decision (approve or decline) and an acknowledgement. EHI modes 3: Return an acknowledgement.
Financial	A notification message which GPS 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 author	

1.9 EHI Data Feeds

The EHI can be used as a source of read-only transactional data. For each transaction that GPS 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](#).

GetTransaction message: Real-time transactional data feed fields

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

1.10 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 your product setup form.

Option	Description
Mode	Your EHI mode. See EHI Operating Modes .
Include Declined Transactions	Whether to include declined authorisation transactions in EHI messages (used for information purposes only).
Stand In	In 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 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 '

Option	Description
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.

- Do the cards support the functionality and behavior 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?

GPS Card Tests

GPS 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

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.

- **SendingAttemptCount** field will be:
 - EHI modes 1 and 2: “1” (1st repeat) or higher (“n” nth repeat)
 - EHI modes 4 and 5: “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 GPS did not receive or could not process your original decision (e.g., 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 (e.g., by unblocking any previously reserved

- 3. The Program Manager partially approves via EHI.
- 4. GPS 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 should look like this:

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

2.1.5 Responding to Cut_Off Messages

External Host Originally:	Advice Indicates that GPS:	Action required by the External Host
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.


```
<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 realtime/online transactions where balance adjustments can be made in the response. If you receive a financial notification and need to adjust the GPS-held balance, you must use the [Balance Update Web Service](#) or Adjust Balance Cards API.

MTID	Txn_Type	Description	Match to?	Match Criteria
				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

MTID	Txn_Type	Description	Match to?	Match Criteria
				3. Other fields that should normally match include: 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)	Authorisation	As above (see

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 GPS 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 GPS?

- 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 GPS token
- Same currency
- Different `txn_ID`
- Same `traceid_lifecycle`

You can decline any of the incremental authorisations (or all

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

Data Type	Minimum Length	Maximum Length	Description	Examples
			(e.g., -123.45 or 0.090) 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	1.0 -6.72
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 (	

Data Type	Minimum Length	Maximum Length	Description	Examples
Traceid	15	40	GPS '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 (alpha- numeric, 1 to 26)	BNET-19991231-MCC1234XY VIS1-19991231-489365567890123
TraceidRaw	15	40	As Traceid, except that the raw information received	

Data Type	Minimum Length	Maximum Length	Description	Examples							
			<table><tr><td>12</td><td>567</td></tr></table>	12	567						
12	567										
TLV10	14	999	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> 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	Type	Format	Tag	AN(10,10)	Length	N(4,4)	Value	ANS (length,length)
Type	Format										
Tag	AN(10,10)										
Length	N(4,4)										
Value	ANS (length,length)										

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.

Field	Type	Null Allowed
Acquirer_id_DE32	String	
ActBal	Decimal	Y
Additional_Amt_DE54	String	
Amt_Tran_Fee_DE28	String	
Auth_Code_DE38	String	
Avl_Bal	Decimal	Y
Bill_Amt	Decimal	Y
Bill_Ccy	String	

Field	Type	Null Allowed
Txn_Ctry	String	
Txn_Desc	String	
Txn_GPS_Date	String	
TXn_ID	Long	Y
Txn_Stat_Code	String	
TXN_Time_DE07	String	
Txn_Type	String	
Additional_Data_DE48	String	
Authorised_by_GPS	String	
AVS_Result	String	
CU_Group	String	
InstCode	String	
MTID	String	
ProductID	Int	

Field	Type	Null Allowed
dest_bank_account	String	
GPS_POS_Capability	String	
GPS_POS_Data	String	
Acquirer_Reference_Data_031	String	
Response_Source	String	
Response_Source_Why	Int	Y
Message_Source	String	
Message_Why	Int	Y
traceid_lifecycle	String	
Balance_Sequence	Long	Y
Balance_Sequence_ExtHost	Long	Y
PaymentToken_id	Int	Y

Field	Type	Null Allowed
Merch_Tax_id	String	
Merch_Contact	String	
auth_type	String	
auth_expdate_utc	String	
Matching_Txn_ID	Long	Y
Reason_ID	Long	Y
Dispute_Condition	String	
Network_Chargeback_Reference_Id	String	
Acquirer_Forwarder_ID	String	
Currency_Code_Fee	String	
Currency_Code_Fee_Settlement	String	
Interchange_Amount_Fee	Decimal	Y

Field	Type	Null Allowed
ClearingFileID	String	
Network_Fraud_Data	String	
SenderData	String	
ReceiverData	String	
AuthenticationAmountUpper	Decimal	Y
AuthenticationCurrency	String	
AuthenticationMerchantHash	String	
FxProviderCardholderRate	Decimal	
FxProviderBookedRate	Decimal	

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](#).

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)		

Field	Description	Data Type ⁽¹⁾	Sample Data
	client for approved authorisation requests.		
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 (9,2)	-60.76
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 GPS calculated fees (Fee_Fixed and Fee_Rate) and Padding (Fx_Pad and MCC_Pad). Financial Transactions do not have padding.	AmountSigned (9,2)	-189.24

