ethoca™

Making ecommerce simply about commerce.

INTEGRATION GUIDE FOR

Consumer Clarity MERCHANT API

SUPPORTING Consumer Clarity

IN THE Digital and Call Center Applications

Version 4.0.0

© 2022 Ethoca. All Rights Reserved.

Contents

1. Introduction 3
2. Technical Onboarding Process 3
2.1 Discovery Phase 3
2.2 Integration Phase 4
2.3 Testing and Verification Phase 4
2.4 Deployment Phase 4
3. Integration Details 5
3.1 API Request Information 6
3.2 API Response Information 10
3.3 API Health Check Information 12
4. Security 13
4.1 Encryption 13
4.2 Authorization 13
4.3 Information Security 15
4.4 Replay Mitigation 15
5. Product Requirements 15
6. Test Cases 15
Appendix 1: API Specification Fields for Digital Receipts 17
responseStatus 17
merchantProfile 17
merchantCustomerServiceContact 18
Order 18
OrderItem 19
Payment 19
Refund 19
Copyright 20

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

1. Introduction

Ethoca's Consumer Clarity (Clarity) brokers order information between an organization and an issuer or an organization and their customer. As a result, issuers are connected to merchant order and account history details in real time, which helps reduce disputes and friendly fraud.

This document provides your technical team with the information you need to implement Ethoca's Merchant API – the API that makes the data you provide accessible to the issuer or customer. Issuers – or partners on behalf of issuers – use this data to avoid chargebacks or represent against them through Consumer Clarity for the Call Center.

Customers can view transaction information and merchant contact information in their online portal or mobile banking app when an organization has elected to participate in Consumer Clarity Digital Receipts. For Merchants, one integration into Consumer Clarity provides access to both the Call Center and Digital channels.

2. Technical Onboarding Process

Full integration with Ethoca's Merchant API (referred to as API going forward) proceeds in four phases: Discovery, Integration, Testing/Verification, and Deployment.

Note that your Ethoca representative and the Ethoca technical team contacts are available to assist at any point in the process.

Note: Ethoca's Development team releases updates to the API on a frequent basis. If you receive documentation but are unable to complete development in a timely manner, check back with your Ethoca contact to make sure a newer version of the documentation has not been made available. Your Ethoca representative will make every attempt to provide the updated documentation once it becomes available.

2.1 Discovery Phase

Review all documentation prior to the kickoff meeting. For your integration, Ethoca will supply the following files:

- Ethoca Merchant API v4.0.0, Integration Guide (this document)
- Ethoca Merchant Data Provision API v 4.0.0, JSON Schema in YAML (merchant_spec_4_0_0.yml)
- Consumer Clarity – Merchant Onboarding and Integration Questionnaire

Discuss any needs or uncertainties you have with your Ethoca contact or bring those questions to the kickoff meeting.

Complete the Merchant Questionnaire.

Complete the Merchant Questionnaire and submit it to your Ethoca contact.

Kick Off Meeting

Your Ethoca contact will schedule a technical kickoff meeting with your technical team, the business owners, as well as technical resources from Ethoca.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

2.2 Integration Phase

Environment set-up

Merchant provides sample API search values, which will be used to retrieve sample order payloads in the sandbox environment.

SSL connectivity testing against Sandbox and Production environments to ensure SSL certificates are matching correctly and both sides can connect at a basic level. Number of connections tested is determined by how many different servers are used in the deployment stages.

Development

Merchant technical team implements a web server that serves the required API methods as described in Section 3. Integration Details below.

Merchant notifies their Ethoca technical team when the API is operational in the sandbox environment to initiate integration testing.

2.3 Testing and Verification Phase

Testing

You must conduct thorough testing of the integration to ensure the foundational functionality is in place before moving to production. Your Ethoca technical team contact is available during this stage to support the testing process. See Test cases for more information.

Verification

Once basic testing is complete, Ethoca will perform final validation tests to ensure the Merchant Data Provision API is fully approved for production.

2.4 Deployment Phase

Pre go-live

API Secret Key Generation

A Production grade Secret key needs to be generated so that there can be a transition from Sandbox to Production.

Verification

The same testing performed in the Testing and Verification Phase must also be repeated during the smoke testing stage of Production/Go-Live to ensure issues were not missed during integration testing.

Post go-live

Live environment verification

Merchant and Ethoca technical team contact perform final verifications against live Production environment to ensure that the HMAC signature and API key are both working in production and that everything tested in sandbox is functioning the same way in production.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

Monitoring and reporting

Ethoca will coordinate with you on communicating metrics associated with your implementation's request processing and results.

3. Integration Details

This section details technical requirements for implementing Ethoca's Merchant API.

To facilitate order inquiry collaboration, members of the program will need to expose a webservice capable of responding to POST method requests over HTTPS with JSON responses.

The POST request body will be sent to you by Ethoca and will contain metadata properties as well as the order search criteria, formatted as follows:

```
{
    "requestReference": {
        "originatorChannel": "DIGITAL",
        "originatorId": "420f0845bd9b808abd7acc053b0b372ceb461edd584e9b9db02b35304255715f",
        "sourceId": "66666688ggg0845bd9b808abd7acc053b0b372ceb461edd584e9b9db02b324gf",
        "originatorDescription": "Test Issuer",
        "correlationId": "zebj8evpeo",
        "locale": "en-US"
    },
    "searchCriteria": {
        "paymentType": "MC",
        "transactionIdentifierType": "BANKNET_REF_NUM",
        "transactionIdentifierValue": "90989JJJNM7767",
        "acquirerReferenceNumber": "12345678901234567890123",
        "transactionDateTime": "2020-06-18T17:11:05-05:00",
        "cardFirstSix": "123456",
        "cardLastFour": "1234",
        "issuerAuthorizationCode": "123456",
        "transactionAmount": "250.35",
        "transactionCurrencyCode": "USD",
        "merchantId": "GHF5F67DFSD468GJJXH78",
        "cardAcceptorName": "MicrosoftXBox",
        "cardAcceptorLocation": "Austin",
        "cardAcceptorRegionCode": "TX",
        "cardAcceptorCountryCode": "US"
    }
}
```

Note: the POST request body will be in UTF-8 format and will be sent as content type: application/json.

The Data Provision API implementation must support shared secret key authorization via an HMAC Authorization header. See Section: 4. Security for details.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

3.1 API Request Information

3.1.1. Resource URI and Method

The webservice endpoint must respond only to POST method requests and the URI must end with the following path:

```
/api/orders
```

Note: the path can be prefixed as required to specialize the URI and avoid collisions. For example:

```
/<custom context>/api/orders
```

3.1.2. Order Search Criteria

The search criteria are used to locate a particular transaction within your database or systems. You'll receive transaction-specific information as input, contained in the POST request body. You then use the fields sent in the request to search and locate order data that matches the input you received. The goal of this process is to match the data received to a unique transaction.

The fields listed below as **Expected Search Fields** will be sent on most requests. However, these fields alone might not be enough for you to return a single, unique transaction with a high rate of success. In these instances, you must identify which of the **Additional Search Fields** will help you achieve the desired match rate. See Product Requirements for more information on the desired match rate.

The search criteria supported by the POST request body are listed in the following tables:

Expected Search Fields

Field	Description	Example
transactionDateTime	Date, time, and time zone of the transaction, or date and time of the transaction in Coordinated Universal Time (UTC), or if time or time zone is unknown, then date of the transaction. ISO 8601 format. This is the date of authorization, not the date of settlement.	2020-06-18T17:11:05-05:00
transactionAmount	Total amount value associated with the transaction. Decimal point period is expected to denote separation of the fractional suffix from the rest of the amount, if applicable for the currency. Decimal point period must not be the first character.	250.35
cardFirstSix	The first six digits of the card number associated with the transaction. Exactly six numeric characters.	524167

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

Field	Description	Example
cardLastFour	Last four characters of the card used in the transaction.	1234

Additional Search Fields

Field	Description	Example
transactionIdentifierValue	The Transaction ID for this order; for Mastercard purchases, this is field DE63, and for Visa this is Tran ID or Tran ID1. The transactionIdentifierValue field is highly effective in locating American Express transactions.	T123456
acquirerReferenceNumber	The Acquirer Reference Number of the transaction. The acquirerReferenceNumber field is unique to MasterCard and Visa transactions, and is only available for settled transactions.	12345678901234567890123
issuerAuthorizationCode	Issuer authorization code for the transaction.	123456
merchantId	The alphanumeric ID of the sub-merchant associated with the purchase details. Only required for channel partners.	GHF5F67DFSD468GJJXH78
paymentType	The card brand or network as provided by the issuer. Allowed values: • AMEX (for American Express) • DISCOVER (for Discover) • MC (for Mastercard) • VISA (for Visa)	MC
transactionCurrencyCode	Alphabetic currency code associated with the value in ISO 4217 format.	USD
transactionIdentifierType	Payment type-specific transaction identifier type associated with the value specified in transactionIdentifierValue. Current values: • BANKNET_REF_NUM • INVOICE_REF_NUM Definition of current values: • Mastercard: DE 63, Subfield 2: Banknet Reference Number	BANKNET_REF_NUM

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

Field	Description	Example
	• American Express: TAB Field 26: Invoice/Reference Number	
cardAcceptorName	Merchant 'doing business as' name, or website name • Mastercard: DE 43, Subfield 1; Card Acceptor Name • Visa: TC 05, positions 92-116; Merchant Name	MicrosoftXBox
cardAcceptorLocation	Merchant city, telephone number, email address, or URL • Mastercard: DE 43, Subfield 3: Card Acceptor City • Visa: TC 05, positions 117-129: Merchant City	Austin
cardAcceptorRegionCode	Merchant U.S. state code or Canada province code • Mastercard Clearing: DE 43, Subfield 5: Card Acceptor State, Province, or Region Code (2-character alpha state or province code defined by ISO 3166-2:US or ISO 3166-2:CA, respectively) • Mastercard Debit: DE 43, Subfield 5: Card Acceptor State or Province (2-character alpha state or province code defined by ISO 3166-2:US or ISO 3166-2:CA, respectively) • Visa Authorization: Field 59, Positions 1-2: Card Acceptor State or Province Code (2-character numeric state or province code defined by ANSI X3.38) • Visa Clearing: TC 05, positions 142-144: Merchant State/Province Code (2-character alpha state or province code defined by ISO 3166-2:US or ISO 3166-2:CA, respectively)	TX
cardAcceptorCountryCode	Merchant country code • Mastercard Clearing: DE 43, Subfield 6: Card Acceptor Country Code (3-character alpha country code defined by ISO 3166-1 alpha-3) • Mastercard Debit: DE 43, Subfield 5: Card Acceptor Country Code (3-	US

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

Field	Description	Example
	character alpha country code defined by ISO 3166-1 alpha-3) • Visa Authorization: Field 43, Positions 39-40: Card Acceptor Country Code (2-character alpha country code defined by ISO 3166-1 alpha-2) • Visa Clearing: TC 05, positions 130-132: Merchant Country Code (2-character alpha country code defined by ISO 3166-1 alpha-2)	

See the Merchant Data Provision API v 4.0.0, JSON Schema in YAML (merchant_spec_4_0_0.yml) for detailed descriptions and examples for each parameter.

3.1.3. Order Search Semantics and Responses

It is important to note that at times, you might receive search fields other than your pre-defined search criteria. In these situations, use only the fields that you need. Don't return an error if additional fields are sent with the request. The expectation is that you'll use the fields necessary to return a unique transaction and ignore any others.

Follow these recommended best practices to ensure a high rate of success in identifying unique transactions:

- We recommend using acquirerReferenceNumber (ARN) to achieve a high rate of success in locating settled Mastercard & Visa transactions (for MC & Visa)

- We recommend using transactionIdentifierValue, along with issuerAuthorizationCode to achieve a high rate of success in locating American Express transactions

3.1.4. Request Message Components

```
POST https://<host>:<port>/api/orders HTTP/1.1
Accept: application/json
Accept-Encoding: gzip, deflate
X-ETH-CHANNEL: DIGITAL or CALL CENTER
X-ETH-ORIGINATOR-ID: <Member ID of Issuer making request>
Content-Type: application/json
Host: <host>
User-Agent: Ethoca-purchase-inquirer (version 3.0)
Authorization: ETHOCA-SHA1 KeyRef=<API Key ID>,Signature=<base64UrlSafe_hmac_signature>
Post request body:
{
    "requestReference": {
        "originatorChannel": "DIGITAL",
        "originatorId": "420f0845bd9b808abd7acc053b0b372ceb461edd584e9b9db02b35304255715f",
        "sourceId": "66666688ggg0845bd9b808abd7acc053b0b372ceb461edd584e9b9db02b324gf",
        "originatorDescription": "Test Issuer",
        "correlationId": "zebj8evpeo",
        "locale": "en-US"
```


ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

```
    },
    "searchCriteria": {
        "paymentType": "MC",
        "transactionIdentifierType": "BANKNET_REF_NUM",
        "transactionIdentifierValue": "90989JJJNM7767",
        "acquirerReferenceNumber": "12345678901234567890123",
        "transactionDateTime": "2020-06-18T17:11:05-05:00",
        "cardFirstSix": "123456",
        "cardLastFour": "1234",
        "issuerAuthorizationCode": "123456",
        "transactionAmount": "250.35",
        "transactionCurrencyCode": "USD",
        "merchantId": "GHF5F67DFSD468GJJXH78",
        "cardAcceptorName": "MicrosoftXBox",
        "cardAcceptorLocation": "Austin",
        "cardAcceptorRegionCode": "TX",
        "cardAcceptorCountryCode": "US"
    }
}
```


3.1.5. Identifying request origination

The request header includes the fields X-ETH-CHANNEL and X-ETH-ORIGINATOR-ID, which identify whether the request originated from a Call Center application or from the Digital channel. This table shows the values for X-ETH-CHANNEL and X-ETH-ORIGINATOR-ID and how they identify from where the transaction originated:

Origination	X-ETH-CHANNEL	X-ETH-ORIGINATOR-ID
Call Center	CALL CENTER	An encrypted value that represents the Issuer making the request. For example: f3a2520e31202df12b1cd9ed38af4e
Digital channel	DIGITAL	An encrypted value that represents the Issuer making the request. For example: f3a2520e31202df12b1cd9ed38af4e
Ethoca test	CALL CENTER or DIGITAL	“null”

3.2 API Response Information

3.2.1. Resource Information

Response Format	JSON
Required Authorization	Yes

3.2.2. Response Compression

To reduce response bandwidth, gzip compression should be enabled.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

The request will include a header indicating the acceptable content encodings, for example:

```
Accept-Encoding: gzip, deflate
```

Use the appropriate response header to indicate the payload compression used, for example:

```
Content-Encoding: gzip
```

Note: Content-type should be application/json for both requests and responses.

3.2.3. Response Field Requirements

Ethoca recommends providing all available fields related to your specific vertical domain (Online Services, Downloaded Products, Physical Goods, etc.). Although the JSON message will not fail if some fields are missing, the efficacy of the Product will vary if fewer fields are provided.

For comprehensive information including types, lengths, enumeration values, and other details on required, suggested, and optional response fields, see the JSON validation schema in YAML, ("merchant_spec_4_0_0.yml").

3.2.4. Example Response

Payload schema and samples will be provided by the Ethoca technical team during the integration phase as described in Section 2.3. Deployment Phase.

3.2.5. Response Status Codes

The client invoking the API expects response status codes consistent with the HTTP1.1 standard as described in RFC 7231 at https://tools.ietf.org/html/rfc7231. The following responses have particular relevance or common application to Ethoca's API:

HTTP Code	Description	Relevance
200	Ok	Standard response for successful HTTP requests: Indicates that the merchant has successfully received the request. More information can be found in the **ResponseStatus** object.
400	Bad Request	Returned for any case where the request cannot be understood by the merchant system due to a malformed URL syntax or URL parameters.
401	Unauthorized	The server understood the request but is refusing to fulfill it. Return this code if the HMAC signature does not match.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

HTTP Code	Description	Relevance
403	Forbidden	The request is valid, but the caller does not have the necessary permissions, typically because the Authorization header is invalid.
405	Method Not Allowed	The server does not implement the request's specified HTTP method, in this case, anything other than POST.
500	Internal Error	Unexpected error.
503	Service Unavailable	The server received the request but is not able to fulfill it.

For 200 responses, use the **ResponseStatus** object to provide additional response information as described in this table:

Scenario	Accepted ResponseStatus Values	Sample ResponseStatus Message
Transaction was identified and some response data provided.	TRANSACTION_FOUND	OK.
Transaction was not identified so no response data provided.	TRANSACTION_NOT_FOUND	The transaction could not be found.
Multiple transactions were identified from the request data.	MULTIPLE_TRANSACTIONS_FOUND	Multiple transactions were found for this request.

3.3 API Health Check Information

3.3.1. Resource URI and Method

A Health or Echo or Heartbeat endpoint ensures that your API is running. To facilitate health check inquiry, you need to expose a webservice capable of responding to GET method requests over HTTPS with JSON responses. The webservice endpoint must respond only to GET method requests and the URI must end with the following path:

```
/api/orders/healthchecks
```

The path can be prefixed as required to specialize the URI and avoid collisions. For example:

```
/<custom context>/api/orders/healthchecks
```

IMPORTANT: If you specify a `<custom context>`, it must be the same for both `/api/orders` and `/api/orders/healthchecks`.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

Ethoca will send a GET request two times each day to monitor the health of your endpoint.

3.3.2. Response Information

The webservice should return an **HTTP 200 OK** success status response code indicating that the API is up and running.

4. Security

4.1 Encryption

The transport of data is to be secured by encryption with the use HTTPS. **The use of HTTP without SSL/TLS is not supported.**

4.2 Authorization

Every request sent to the Merchant API must be authorized. To facilitate authorization, every request **must** contain a time stamped, symmetric-key based HMAC signature header.

The HMAC signature ensures that the API secret key and key ID are exchanged securely between Ethoca and the merchant out-of-band. The entropy of the issued API key must be no less than 128 bits.

The API Key ID must be provided with every request along with an HMAC signature header in the following format:

```
Authorization: ETHOCA-SHA1 KeyRef=<API Key_ID>,Signature=<base64UrlSafe_hmac_signature>
```

The HMAC signature is based on the following API request data elements, concatenated using a new line character. Note that the elements **must** be in this order:

- Host
- Canonicalized Resource
- Request Body string (without spaces)
- HTTP Verb
- Content-Type (POST request content type: “application/json”)
- Request Timestamp in UTC

Base64 URL-Safe Encoding:

The computed HMAC hash string must be encoded using Base64 URL-safe encoding. The url-safe variation uses ‘-‘ and ‘_’ instead of ‘+’ and ‘/’ characters, respectively, and strips out ‘=’ characters.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

4.2.1 Signature Verification Example

```
POST https://merchant.com:443/api/orders HTTP/1.1
Accept: application/json
Accept-Encoding: gzip, deflate
Content-Type: application/json
Host: merchant.com
User-Agent: Ethoca-purchase-inquirer (version 3.0)
X-Eth-Date: 2017-06-19T13:18:18Z
Authorization: ETHOCA-SHA1 KeyRef=<API Key_ID>,Signature=<base64UrlSafe_hmac_signature>
Post request body:
{
    "requestReference": {
        "originatorChannel": "DIGITAL",
        "originatorId": "420f0845bd9b808abd7acc053b0b372ceb461edd584e9b9db02b35304255715f",
        "sourceId": "66666688ggg0845bd9b808abd7acc053b0b372ceb461edd584e9b9db02b324gf",
        "originatorDescription": "Test Issuer",
        "correlationId": "zebj8evpeo",
        "locale": "en-US"
    },
    "searchCriteria": {
        "paymentType": "MC",
        "transactionIdentifierType": "BANKNET_REF_NUM",
        "transactionIdentifierValue": "90989JJJNM7767",
        "acquirerReferenceNumber": "12345678901234567890123",
        "transactionDateTime": "2020-06-18T17:11:05-05:00",
        "cardFirstSix": "123456",
        "cardLastFour": "1234",
        "issuerAuthorizationCode": "123456",
        "transactionAmount": "250.35",
        "transactionCurrencyCode": "USD",
        "merchantId": "GHF5F67DFSD468GJJXH78",
        "cardAcceptorName": "MicrosoftXBox",
        "cardAcceptorLocation": "Austin",
        "cardAcceptorRegionCode": "TX",
        "cardAcceptorCountryCode": "US"
    }
}
```

4.2.2 Create your HMAC Signature

For step-by-step instructions about how to create a HMAC signature, including examples and sample values, see the provided text file **Create your HMAC Signature**.

If you need further assistance in creating your HMAC signature, you can reach out to your Ethoca technical team contact.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

4.3 Information Security

Responses to API requests may include personally identifiable information (PII). Ethoca classifies this data as "Regulated-Classified". Consistent with Ethoca's policy on Applications and Systems Development and Maintenance, Ethoca requires that **members/customers not deliver production data to the Sandbox environment at any time.**

4.4 Replay Mitigation

To reduce the risk of a replay attack, Ethoca strongly recommends validating the request timestamp to ensure it is within an acceptable timeframe – e.g. not older than 1 minute.

5. Product Requirements

Ethoca's Merchant Data Provision API is a component of a real-time, mission-critical system. As such it is required that this service is highly available and performant. Incoming webservice requests should be fulfilled in real time, and peaks of up to several hundred requests per second should be handled without performance degradation.

Key product requirements:

Metric	Requirement
Response time	900 milliseconds
Average Load	100 queries per second (qps)
Peak Load	200 qps
Data availability	13 months of transactional data must always be available. Transaction data must be made available within 24 hours of authorization.

6. Test Cases

Thorough testing must be conducted by merchants during the development phase of the integration to ensure the foundational functionality is in place during the final validation stage before going to Production. This testing must also be repeated during the smoke testing stage of Production/Go-Live to ensure issues were not missed during Integration testing.

Your test environment must remain available to Ethoca after you go to Production. Notify your Ethoca representative or your Ethoca technical team contacts if your test environment ever becomes unavailable. Your test environment should be able to support stress testing, and should have at minimum 200 test transactions to use for testing purposes. The test transactions should not contain Production data, but are representative of what would be returned in a Production environment.

Retrieving order details from the API
Using an API client, Ethoca will invoke the API using the agreed upon sample search values. The following outcomes will be confirmed:

1. **Merchant can receive requests and validate the Authorization header**

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

a. Validate Authorization header as per the rules described in the Merchant Data Provision API specification.
b. Confirm that requests are rejected with an HTTP status code of 403 when the Authorization header is invalid.
c. Confirm that any requests that specifies an HTTP method other than POST is rejected with an HTTP status code of 405.

Note: response error codes are outlined in Section 3.2.5 Response Status Codes.

2. **Merchant returns valid API payload for valid sample requests**
   a. Once the valid payload is received Ethoca will perform the following validations:
      i. Validate that payload contains all required fields as outlined in the Merchant Data Provision API specification.
      ii. Validate that all the fields containing data conform to the specified data type.
      iii. Validate that fields with specified character limits have not been exceeded.
      iv. Validate that fields requiring a specific enumerated value conform to those values.

3. **Merchant passes all requirements for pre-defined SLAs**
   a. Merchant can sustain the required number of QPS (200) during stress testing.
   b. Merchant returns a match rate of greater than 90%.
   c. Merchant's response call latency averages less than 2 seconds.

Once all of these outcomes have been confirmed in the lower environment, the Merchant will be promoted to our Production environment so that these tests can be repeated in Production. When the Merchant has passed all of the same testing in Production, then they will be enabled for all Issuer clients, and considered live and available.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

Appendix 1: API Specification Fields for Digital Receipts

This section shows the specific objects and associated field IDs that are used by the Digital Receipts service to generate a digital receipt. Fields are required unless otherwise indicated.

responseStatus

Shows whether the response received is successful.

Field ID	Type	Description
code	Alpha Numeric	States the result of the request.
message	Alpha Numeric	Provides more detail about the result of the request.
trackingId	Alpha Numeric	Any internal reference ID linked to this search.

merchantProfile

Details that identify your company, including name and description about your products or services. You can also provide an absolute URL that allows issuers to access your company logo image.

Field ID	Type	Description	Example
name	Alpha Numeric	Name of the merchant from which the item was purchased.	SHOE STORE 1234
description	Alpha Numeric	Description of the primary merchant tied to the transaction and responsible for providing the products or services (description of the business, what they do, markets, etc.). Used to help cardholder understand the business responsible for the charge.	Austin's largest shoe store
logoUrl optional	Instance	A URL pointing to your company logo.	https://content.ethoca.com/merchant/1a34567891012b123d123.png

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

merchantCustomerServiceContact

Details about your company's customer service.

Field ID	Type	Description	Example
address	Instance	Merchant's customer service contact address.	1234 Main St, Austin, TX, 78701
phoneNumber	Alpha Numeric	Merchant's customer service phone number. Include the country code and any applicable separators.	+1-234-567-8901
email optional	Alpha Numeric	Merchant's customer service email address.	support@shoestore1234.com
website optional	Alpha Numeric	URL for merchant's customer service focused information.	www.shoestore1234.com

Order

Specific information about the order being analyzed, including the item purchased and the total amount of the order.

Field ID	Type	Description	Example
merchantOrderId	Alpha Numeric	Merchant internal order tracking number. Usually assigned by eCommerce/ Store system.	123456789
subtotal	Amount Type	Order subtotal before tax. Summary amount of all products purchased in this order. Tax and shipping are not included in this amount.	42
shippingHandling	Amount Type	Total cost of shipping/ handling for the order. If several different shipping and handling fees, summarize into one field.	6.5
tax	Amount Type	Total amount of tax.	4
total	Amount Type	Total amount of order.	52.5
currencyCode	Alpha Numeric	Currency applied to order. This currency will apply to all amount/price fields throughout entire payload and must be three-character ISO currency code. https://en.wikipedia.org/wiki/ISO_4217#Active_codes	CAD

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

OrderItem

List of items (products) included in the order.

Field ID	Type	Description	Example
id	Alpha Numeric	Order Item unique identifier (merchant generated sequence-based ID for each order item).	12345
productName	Alpha Numeric	Name of the product.	Boy's running shoe
productDescription	Alpha Numeric	Description of item which can contain extended details of the product.	size: 6, color: blue
quantity	Integer	Number of items purchased.	2
productPrice	Amount Type	Price per unit.	21

Payment

Payment object unique identifier (merchant generated sequence-based ID for each payment).

Field ID	Type	Description	Example
id	Alpha Numeric	Payment object unique identifier (merchant generated sequence-based ID for each payment).	23456
paymentType	Alpha Numeric	Visa/ MC/ Amex/ Store Card	MC
cardLastFour	Alpha Numeric	Last 4 of the bank card payment method.	1234

Refund

List of refunds made for the order.

Field ID	Type	Description	Example
id	Alpha Numeric	Refund object unique identifier (merchant generated sequence-based ID for each refund).	34567
total	Amount Type	Total amount that was refunded on the transaction.	23

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.

Copyright

Information in this document is subject to change without notice. While care has been taken to ensure accuracy, Ethoca assumes no responsibility for errors or omissions; any patent liability for the use of the information contained within; or for any damages resulting from its use.

All companies and products mentioned in this document currently retaining registered trademarks, have patents pending, or protected by common copyright are respectfully noted by Ethoca. Users are advised to respect and adhere to the legal protection of all trademarks, patents and copyrights.

No part of this manual may be reproduced or transmitted in any form or by any means whatsoever, electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's use, without the express written permission of Ethoca. Any reproduction or disassembly of all embodied computer programs or databases without the express written consent of the rights-holder is prohibited.

Copyright ©2022, Ethoca Limited

All Rights Reserved.

ETHOCA CONFIDENTIAL ©2022 Ethoca. All Rights Reserved.