Api authentication:

1. Introduction:

The Payzone payment platform validates API requests with a HMAC signature. Only requests with the correct signature are allowed to access the system resources.
The signature together with other important security information is expected to be sent in the request headers. You will receive an error message with HTTP status 401 if the signature is missing or invalid.
The document is to explain how to generate the signature.

2. API Caller Credentials:

You will receive these credentials when your merchant account is created. If you don't have these credentials, please contact your account manager.

Name	Description
Merchant Account Name	Assigned by Payzone. The unique merchant account name
Caller Name	Assigned by Payzone. The api caller ID
Caller Password	Assigned by Payzone. The api caller password, it is also the encrypted secret for HMAC signature.

3. Request Security Headers:

These HTTP request header values are required for each API call to the Payzone platform. Without any of these headers, the request is treated as an unauthorised request.

Header Name	Description
X-MerchantAccount	The Merchant Account name assigned to you.
X-CallerName	The name of the API Caller making the request
X-HMAC-Timestamp	Unix timestamp (seconds from epoch). Signatures generated with timestamps more than 30 minutes older than the request (as well as future timestamps) are rejected. e.g
X-HMAC-Signature	The generated signature

4. Generate the Signature:

Parameter definitions:

- **X-CallerName** - the name of the caller
- **X-MerchantAccount** - the name of the merchant account
- **X-HMAC-Timestamp** - current Unix time in seconds. This MUST be in UTC
- **request_path** - relative path of API, include query params if present
- **request_content** - The HTTP method body if present. Put it as an empty string ("") if it is not present.

The signature can be generated as follows (pseudo-code):

```
var timestamp = seconds_from_epoch_utc
var message = string_concat(callerName, merchantAccountName, timestamp, request_path, request_body)
var signature = hmac_sha256_as_hexadecimal(api_secret, message)
```

As a concrete example, suppose we have a caller calling the healthcheck endpoint:

- **X-CallerName** = "$caller"
- **X-MerchantAccount** = "MYNAME"
- **X-HMAC-Timestamp** = "1633767872"
- **Caller's password** = "123456"
- **Request url** = "https://payment-sandbox.payzone.ma/api/v3/healthcheck"

It goes:
message = "$callerMYNAME1633767872/api/v3/healthcheck"
signature =
"B6693ABCCB887DD65B8DD05FAC5AC19653154C63006896ED4912EAAEBF10FEB1"
Finally, the request goes as below (in CURL):

```
curl --location --request GET 'https:// payment-sandbox.payzone.ma/api/v3/healthcheck' \
--header 'X-MerchantAccount: MYNAME' \
--header 'X-CallerName: $caller' \
--header 'X-HMAC-Timestamp: 1633767872' \
--header 'X-HMAC-Signature: B6693ABCCB887DD65B8DD05FAC5AC19653154C63006896ED4912EAAEBF10FEB1' \
--header 'Content-Type: application/json'
```

You will receive a HTTP 200 status with an empty response if your signature is correct.
You will see this error message when the signature is wrong:

```
{"requestId":"44d123b4-5cdc-4522-908b-3d5765addbf3","errorCode":"authentication_error","message":"HMAC Authentication failed. Invalid name or password"}
```

Get Transaction

The get transaction API helps to retrieve a charge or credit transaction detail. The API requires HMAC signature, please refer to *API Authentication* for more information about the signature.

API Endpoint	https://{{server}} /api/v3/charges/
Method	GET
Content Type	Application-json

1. Accepted parameters

Field	Required	Description
id	No	String (The id of a specific charge / credit.) <= 255 characters
customerId	No	String (The merchant provided ID of the customer this charge / credit belong to.) <= 255 characters
customerEmail	No	String (The Customer Email of charge / credit.) <= 255 characters
orderStates	No	String (Return only with one of the specified order states.) optional but if specified must be a list of one or more separated by commas
createdAfter	No	String <date-time> (Return only created after this date. ISO-8601 format YYYY-MM-DDThh:mm:ssZ Example 2016-11-24T12:34:56Z
createdBefore	No	String <date-time> (Return only created before this date. ISO-8601 format YYYY-MM-DDThh:mm:ssZ Example 2016-11-24T12:34:56Z
modifiedAfter	No	String <date-time> (Return only modified after this date. ISO-8601 format YYYY-MM-DDThh:mm:ssZ Example 2016-11-24T12:34:56Z
modifiedBefore	No	String <date-time> (Return only modified before this date. ISO-8601 format YYYY-MM-DDThh:mm:ssZ Example 2016-11-24T12:34:56Z
paymentMethod	No	String (Return only for the specified payment method) Enum: "VISA" "MASTERCARD"

paymentType	No	String (Return only for the specified payment type) Enum: "CREDIT_CARD" "DEBIT_CARD"
gatewayProvidedId	No	String (Search by gateway provided ID.)
page	No	Integer (Starting index of results to fetch) >= 0 Default: 0
size	No	Integer (Size of the block to fetch) Default: 10