



GestoPago PortalVentas.net HTTPS Service Datasheet Security v2.00



Reviews Log

Date	Version	Description	Author
01 Sep 2019	1.0	Document Creation	Alberto García/Ezequiel García
01 Dec 2019	1.01	Method revision	Alberto García
06 Dec 2019	1.02	Revision of AES256 enc	Alberto García/Ezequiel García
15 Dec 2019	1.03	Diagram update	Alberto García
20 Dec 2019	1.04	Endpoints parameter updates	Alberto García/Ezequiel García
22 Dec 2019	1.05	accessToken expiration details	Alberto García/Ezequiel García
17 Jun 2020	1.08	Added details for requests	Ezequiel García
29 Jun 2020	2.00	Added response codes	Ezequiel García

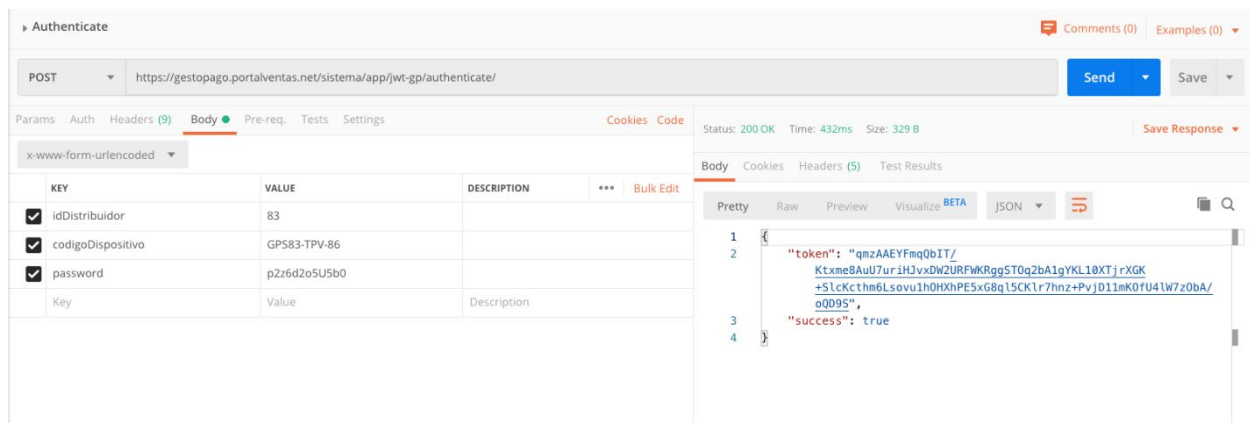
Authorization

All the requests to the Gestopago API are protected with JWT which defines a compact and autonomous way to securely transmit the information.

The client will send their credentials to an authentication server in **form-url-encoded** format via POST. Which are made up of the following 3 values that will be delivered to the implementer:

- idDistribuidor
- codigoDispositivo
- password

To which Gestopago will verify that they are correct and in case of success an accessToken will be provided which has an expiration of 24 hrs. It is the responsibility of the implementer to obtain a new token in case the expiration is not valid (http status code: 403).



Authenticate

POST <https://gestopago.portalventas.net/sistema/app/jwt-gp/authenticate/> Send Save

Params Auth Headers (9) Body Pre-req. Tests Settings Cookies Code Status: 200 OK Time: 432ms Size: 329 B Save Response

x-www-form-urlencoded

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> idDistribuidor	83	
<input checked="" type="checkbox"/> codigoDispositivo	GPS83-TPV-86	
<input checked="" type="checkbox"/> password	p2z6d2o5U5b0	
Key	Value	Description

Body Cookies Headers (5) Test Results

Pretty Raw Preview Visualize BETA JSON

```
1 {
2   "token": "qmzAAEYFmq0bIT/
3     Ktxme8AuU7ur1H3vxDWZURFWKrgg5TOq2bA1gYKL10XTjrXGK
4     +5LcKcthm6Lsovu1h0HXhPE5xG8q15CK1r7hnz+PvjD11mK0fU41W7z0bA/
      oQ095",
  "success": true
}
```

This token must be used to authenticate all subsequent calls to the Gestopago's WebService, where it must be added in the Authorization header in the form of a Bearer Token

Note: It's not allowed to get a new token for each request that the implementer makes to Gestopago API

Example of a petition with accessToken:



GET http://<servidor>:8080/sistema/service/<metodo>.do

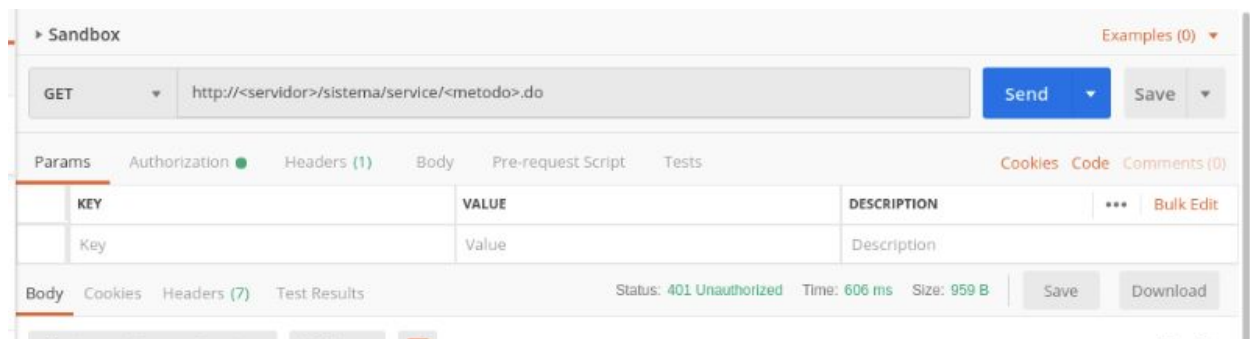
Params Authorization Headers (1) Body Pre-request Script Tests

Headers (1)

KEY	VALUE	DESCRIPTION
Authorization	Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJpbmtpbmUgSldUIE1aW...	
Key	Value	Description

Response

In case of not providing the accessToken or if it is incorrect, Gestopago will not allow the request to be processed. **Therefore it will send a 401 Unauthorized error.**



Sandbox

GET http://<servidor>/sistema/service/<metodo>.do

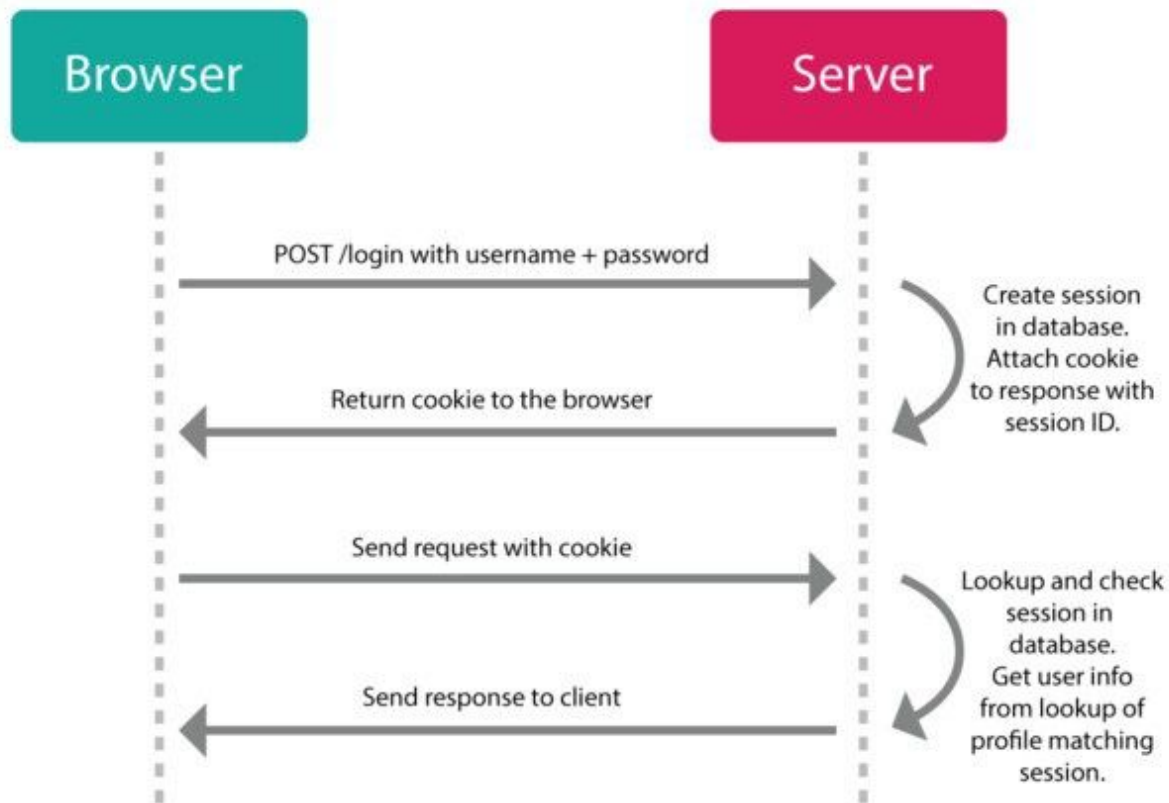
Params Authorization Headers (1) Body Pre-request Script Tests

Body Cookies Headers (7) Test Results

Status: 401 Unauthorized Time: 606 ms Size: 959 B

It is the client's responsibility to handle the 401 Unauthorized responses and request a new accessToken from Gestopago and continue with its normal flow.

In case of not providing the valid accessToken, Gestopago will not allow the request to be processed. **Therefore it will send a 403 Forbidden error.**



Information Exchange

The parameters to be sent (Payload) must be encrypted using the AES-256 Paddingmode PKCS7 algorithm, Gestopago will provide the implementer with the key and the initialization vector with which the encryption should be implemented.

The implementer must construct an object in JSON format with the parameters required in each method to later encrypt it with the algorithm previously mentioned. The result of this process must be sent in the payload of the endpoint as form-data (key: value) where the key must be called signed.



POST example

signed = key name in the payload parameter, with the encrypted data value

POST http://<servidor>/sistema/service/<metodo>.do

Send Save

Params Authorization Headers (2) **Body** Pre-request Script Tests Cookies Code Comments (0)

none form-data x-www-form-urlencoded raw binary GraphQL BETA

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> signed	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJpbmtpbmUgSldU...	
Key	Value	Description

Response

GET example

signed = key name in the payload parameter, with the encrypted data value

GET http://<servidor>/sistema/service/<metodo>.do

Send Save

Params Authorization Headers (2) **Body** Pre-request Script Tests Cookies Code Comments (0)

none form-data x-www-form-urlencoded raw binary GraphQL BETA

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> signed	1aWxkZXIiLCJpYXQiOiE1NjkwMTUwODcsmV4cCI6MTYwMDU1MTA4...	
Key	Value	Description

Response

To see the detail of each api method, review the document GPS_API_V####.pdf