



Integration Guide Application Model

Revision History

DATE	DESCRIPTION
03/May/2014	Overview

Copyright

Todos os direitos reservados. O UOL é uma marca comercial do UNIVERSO ONLINE S / A. O logotipo do UOL é uma marca comercial do UNIVERSO ONLINE S / A. Outras marcas, nomes, logotipos e marcas são de propriedade de seus respectivos proprietários.

As informações contidas neste documento pertencem ao UNIVERSO ONLINE S/A. Todos os direitos reservados. UNIVERSO ONLINE S/A. - Av. Faria Lima, 1384, 6º andar, São Paulo / SP, CEP 01452-002, Brasil.

O serviço PagSeguro não é, nem pretende ser comparável a serviços financeiros oferecidos por instituições financeiras ou administradoras de cartões de crédito, consistindo apenas de uma forma de facilitar e monitorar a execução das transações de comércio eletrônico através da gestão de pagamentos. Qualquer transação efetuada através do PagSeguro está sujeita e deve estar em conformidade com as leis da República Federativa do Brasil.

Aconselhamos que você leia os termos e condições cuidadosamente.

Disclaimer

UOL offers no guarantees of any kind [implicit, implied or statutory] with respect to the information contained therein. UOL does not undertake any liability for loss or damage (direct or indirect), caused by error or omission, or resulting from the use of this document or the information contained herein or resulting from the App or use of a product or service described in this document. UOL is entitled to make any changes to any information herein without prior notice.

Contents

Revision History	2
Copyright	2
Disclaimer	2
Contents.....	3
Overview.....	4
Integration Stages.....	4
Apps	4
Authorization	7
Informing the request data.....	8
Response of Authorization API	17
Directing the buyer to the authorization flow	18
Authorization Flow.....	18
Notifications.....	20
Configuring the receipt of notifications.....	21
Receiving a transaction notice	21
Searches.....	23
See below how to perform a search:.....	23
Searching an authorization by notification code	23
Searching an authorization by its code.....	24
Searching all the app authorization	27
Using APIs of PagSeguro	30
Payment API.....	30
Notification API.....	31
Search API	31
Creation of Subscription	32
Revocation of authorization	33
Table of Errors	33

Overview

The Apps model of PagSeguro allows your App to create checkouts, receive payment notifications among other features in the name of the client without the need to configure tokens, return URLs and other information in your PagSeguro account.

As such, your client can register in your platform, authorize it and start to sell without the need to include information or enter the PagSeguro account for create the settings.

The Apps model of PagSeguro is available for accounts of the Seller and Enterprise type.

Integration Stages

The integration of the Apps Model includes some basic stages:

1. Apps

Create and manage an App.

2. Authorization

Obtain permission from your client to create checkouts, perform searches among other actions.

3. Payments

Create checkouts and direct the buyer to the website of PagSeguro, where he/she can safely and conveniently make the payment.

4. Notifications

Receive notifications informing the status of the authorization and the billing.

5. Search

Perform searches in PagSeguro to check up on your transactions at any time.

It is important to follow the steps above in order to fully understand the tool.

Apps

In order to use PagSeguro's App model you need to create an App. This App will be responsible for centralizing the authorizations granted by your clients.



Warning: Since the Apps model is a tool allowed only for some partners, it is accessed through a few direct URLs that you will see throughout the documentation.

In order to create a new App, access the link <https://pagseguro.uol.com.br/aplicacao/listagem.html> and click on “create you Apps” as shown in Image 1:

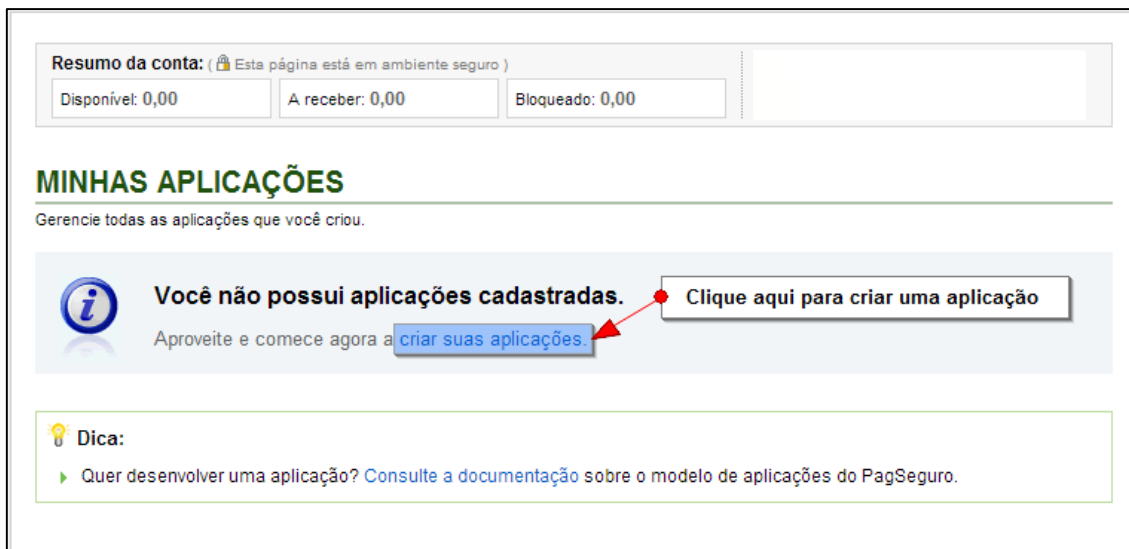


Image 1

You can also directly access the registration page through the link <https://pagseguro.uol.com.br/aplicacao/cadastro.html>

On the creation page, you must fill out the data requested:

FIELD	DESCRIPTION
Name of App	This name will appear for you and for other clients that will use your App.
ID of App	The ID of the App will be the code that identifies this App in PagSeguro. Note: PagSeguro will suggest an ID based on the name that you chose in the preceding field.
Description of App	Write the description that will appear to the users in your App. Be objective and briefly explain its purpose.
URL of App	Type in the URL where your App will be available for access on the internet.
Logo	Inform the address (URL) of your logo or upload the image file. Note: No more than 500kbytes, accepted formats: JPG, GIF, PNG, BMP. Your logo may be reduced to the maximum size of 150 x 55 pixels.
Notification URL	Type in the URL where you will receive the notifications performed in your App.
Redirect URL	Type in the URL where the user will be taken after the payment has been completed.

You can also enable the redirect with the transaction code. With the enabled option, PagSeguro will send as a parameter, via GET, the authorization code that was generated. Your App may use this code to display the authorization information to the client.

If this option is enabled, you can choose the name of the GET parameter that will be used according to Image 2.

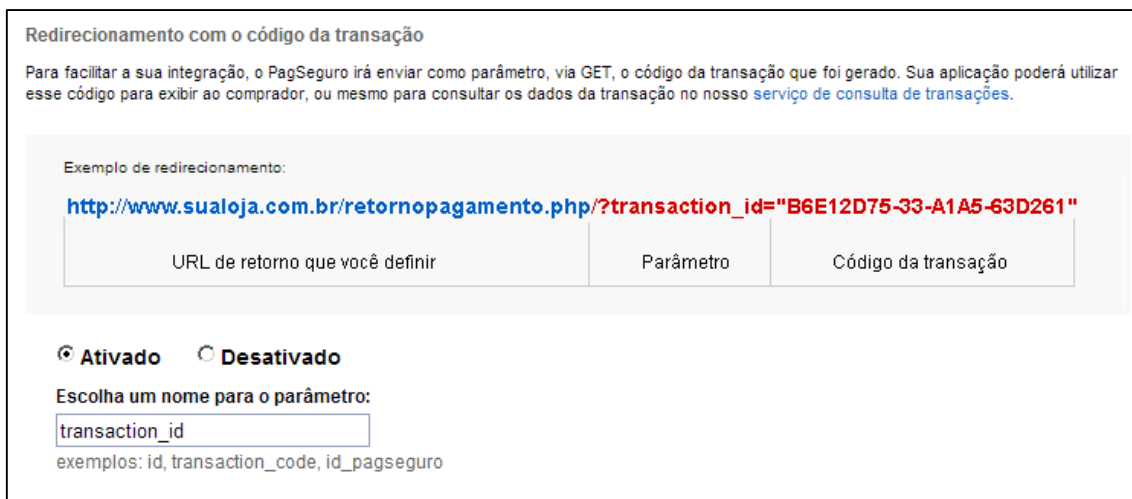


Image 2

After creating your App, a summary with the App data, including the appKey will be displayed as shown in Image 3.

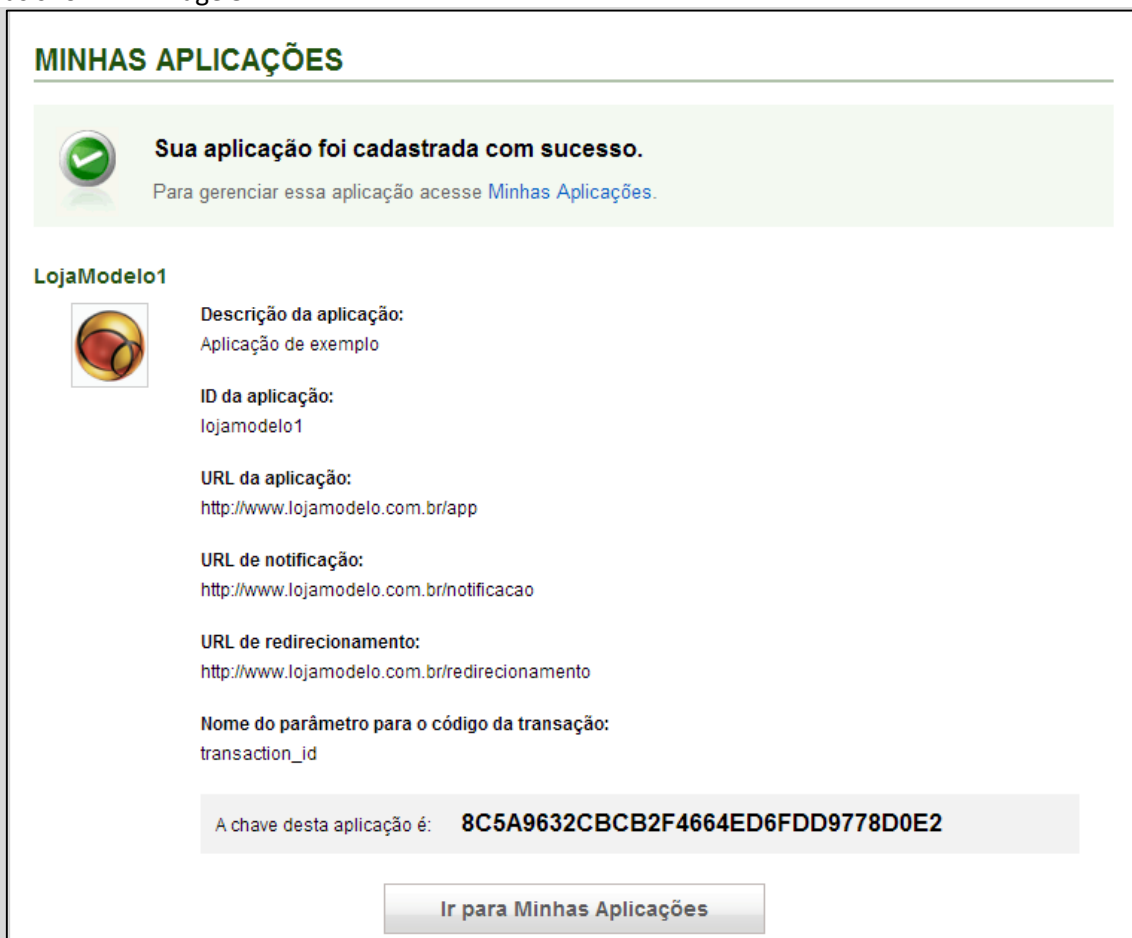
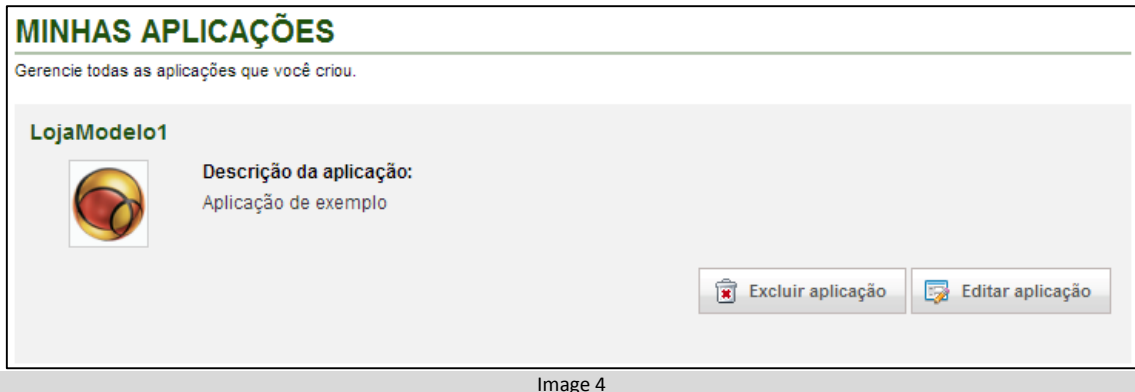


Image 3



Warning: Keep your app key in a safe place because it is essential for you to make the iterations with the Payment and Signature APIs.

After storing your app key, click on “Go to My Apps” to see a list of apps. The list is shown as in Image 4.



You can edit the information of your app, including generate a new appKey at any time by clicking on Edit app > Generate new key. With the exception of the app ID, all the app fields are editable.

It is also possible to exclude an app. By excluding an app, all permissions granted to it will be lost, that is:

- It will no longer be able to create checkouts
- It will no longer be able to receive payments based on the checkouts created prior to the removal
- It will continue to receive notifications
- It will no longer be displayed on the list of apps of the integrator
- It will no longer be displayed on the list of granted authorizations

Authorization

After creating an app, you can ask for your client’s authorization to create checkout, signatures, perform searches among other actions.

The authorization flow is shown in Image 5:

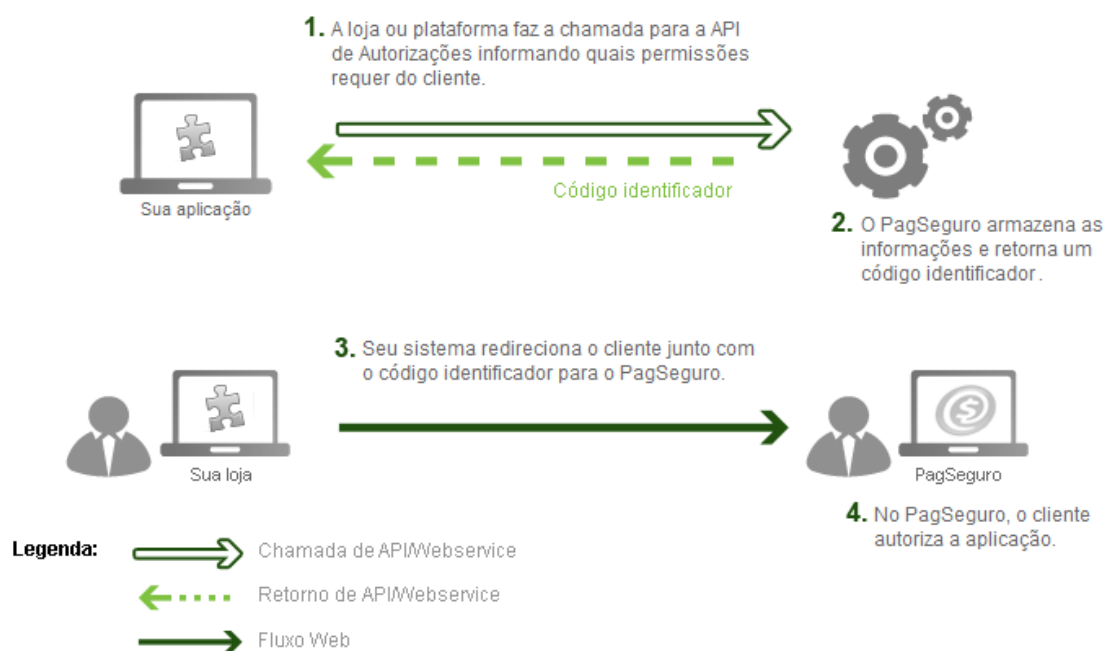


Image 5

Informing the request data

The request to the Authorization API is done by informing the authorization data via XML in combination with the parameters of authentication of your app (appId and appKey) using the POST method.

URL of PagSeguro’s Authorization API

<https://ws.pagseguro.uol.com.br/v2/authorizations/request?appId={appId}&appKey={appKey}>

Authentication parameters

PARAMETER	DESCRIPTION
appId	ID of App Presence: Required Type: Text Format: A string of no more than 60 characters.
appkey	Specifies the token that corresponds to the PagSeguro App that is making the request. Presence: Required Type: Text Format: A string of 32 characters.

See below the HTTP header needed to make the request to the authorization API of PagSeguro informing the data in XML format.

The header **Content-Type** must be informed as in the example below:

```
Content-Type: application/xml; charset=ISO-8859-1
```

Note: if your app or store does **not** use the set of characters **ISO-8859-1**, ex., (**UTF-8**), you will need to replace the charset parameter of the example above.

The response of the transaction search by code is given in XML format, as shown below.

```
1. <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2. <authorizationRequest>
3.   <reference>REF1234</reference>
4.   <permissions>
5.     <code>CREATE_CHECKOUTS</code>
6.     <code>RECEIVE_TRANSACTION_NOTIFICATIONS</code>
7.     <code>SEARCH_TRANSACTIONS</code>
8.     <code>MANAGE_PAYMENT_PRE_APPROVALS</code>
9.   </permissions>
10.  <redirectURL>http://seusite.com.br/redirect</redirectURL>
11.  <notificationURL>http://seusite.com.br/notification</notificationURL>
12. </authorizationRequest>
```

Request parameters

The parameters expected by the Request API are case sensitive and are described in the table below:

XML PARAMETER	DESCRIPTION
<reference>	<p>ID used to refer to the authorization of your request.</p> <p>Presence: Optional. Type: Text. Format: Free, restricted to a total of 20 characters.</p>

XML PARAMETER	DESCRIPTION												
<permissions>	<p>Permission to be authorized Presence: Required. Type: Text. Accepted values:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CREATE_CHECKOUTS</td> <td>The app may direct buyers to PagSeguro and may mediate payments</td> </tr> <tr> <td>RECEIVE_TRANSACTION_NOTIFICATIONS</td> <td>The app may receive transaction notification searches that it mediated</td> </tr> <tr> <td>SEARCH_TRANSACTIONS</td> <td>The app may search the transactions that it mediated</td> </tr> <tr> <td>MANAGE_PAYMENT_PRE_APPROVALS</td> <td>The app may manage and use payment pre-approvals</td> </tr> <tr> <td>DIRECT_PAYMENT</td> <td>The app may manage payments via transparent checkout. Warning: It is necessary to clear such through PagSeguro's commercial area</td> </tr> </tbody> </table>	Value	Description	CREATE_CHECKOUTS	The app may direct buyers to PagSeguro and may mediate payments	RECEIVE_TRANSACTION_NOTIFICATIONS	The app may receive transaction notification searches that it mediated	SEARCH_TRANSACTIONS	The app may search the transactions that it mediated	MANAGE_PAYMENT_PRE_APPROVALS	The app may manage and use payment pre-approvals	DIRECT_PAYMENT	The app may manage payments via transparent checkout. Warning: It is necessary to clear such through PagSeguro's commercial area
Value	Description												
CREATE_CHECKOUTS	The app may direct buyers to PagSeguro and may mediate payments												
RECEIVE_TRANSACTION_NOTIFICATIONS	The app may receive transaction notification searches that it mediated												
SEARCH_TRANSACTIONS	The app may search the transactions that it mediated												
MANAGE_PAYMENT_PRE_APPROVALS	The app may manage and use payment pre-approvals												
DIRECT_PAYMENT	The app may manage payments via transparent checkout. Warning: It is necessary to clear such through PagSeguro's commercial area												
<redirectURL>	<p>URL to where the buyer will be redirected after the completion of the authorization flow. If it is informed in the call, it will be used instead of the URL informed in the registration of the app. Presence: Required. Type: Text. Format: A valid URL, restricted to 255 characters.</p>												
<notificationURL>	<p>URL to where the notification will be directed after the completion of the authorization flow. If it is informed in the call, it will be used instead of the URL informed in the registration of the app Presence: Required. Type: Text. Format: A valid URL, restricted to 255 characters.</p>												

Client data and suggestion for registration

While creating an authorization you can also forward the client data. As such, if the Seller's e-mail sent via the API is already registered in the base, a login with this e-mail will be suggested. If the client does not have an account, the data will be used as a suggestion for a registration and this will make it easier for the client's registration.



Warning: The more correct data is informed, the greater are the chances of converting the Seller that has not been registered in this flow.

It is possible to forward the data of a Seller client (using the CPF number) as well as a Enterprise client (using the CNPJ number).

See below an example of the structured XML to represent the data of an authorization with a suggestion of a **Seller** account:

```

1. <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2. <authorizationRequest>
3.   <reference>123</reference>
4.   <permissions>
5.     <code>CREATE_CHECKOUTS</code>
6.     <code>SEARCH_TRANSACTIONS</code>
7.     <code>RECEIVE_TRANSACTION_NOTIFICATIONS</code>
8.   </permissions>
9.   <redirectURL>http://seusite.com.br/redirect</redirectURL>
10.  <notificationURL>http://seusite.com.br/notification</notificationURL>
11.  <account>
12.    <email>usuario@seusite.com.br</email>
13.    <type>SELLER</type>
14.    <person>
15.      <name>Antonio Carlos</name>
16.      <documents>
17.        <document>
18.          <type>CPF</type>
19.          <value>23606838450</value>
20.        </document>
21.      </documents>
22.      <birthDate>1982-02-05</birthDate>
23.      <phones>
24.        <phone>
25.          <type>HOME</type>
26.          <areaCode>11</areaCode>
27.          <number>30302323</number>
28.        </phone>
29.        <phone>
30.          <type>MOBILE</type>
31.          <areaCode>11</areaCode>
32.          <number>976302323</number>
33.        </phone>
34.      </phones>
35.      <address>
36.        <postalCode>01452002</postalCode>
37.        <street>Av. Brig. Faria Lima</street>
38.        <number>1384</number>
39.        <complement>5o andar</complement>
40.        <district>Jardim Paulistano</district>
41.        <city>Sao Paulo</city>
42.        <state>SP</state>
43.        <country>BRA</country>
44.      </address>
45.    </person>
46.  </account>
47. </authorizationRequest>

```

See below an example of a structured XML to represent the data of an authorization with the suggestion of a Enterprise account:

```
1. <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2. <authorizationRequest>
3.   <reference>123</reference>
4.   <permissions>
5.     <code>CREATE_CHECKOUTS</code>
6.   </permissions>
7.   <redirectURL>http://seusite.com.br/redirect</redirectURL>
8.   <notificationURL>http://seusite.com.br/notification</notificationURL>
9.   <account>
10.    <email>usuario@seusite.com.br</email>
11.    <type>COMPANY</type>
12.    <company>
13.      <name>Seu Site</name>
14.      <documents>
15.        <document>
16.          <type>CNPJ</type>
17.          <value>17302417000101</value>
18.        </document>
19.      </documents>
20.      <displayName>Seu Site</displayName>
21.      <websiteURL>http://www.seusite.com.br</websiteURL>
22.      <partner>
23.        <name>Antonio Carlos</name>
24.        <documents>
25.          <document>
26.            <type>CPF</type>
27.            <value>34163749160</value>
28.          </document>
29.        </documents>
30.        <birthDate>1982-02-05</birthDate>
31.      </partner>
32.      <phones>
33.        <phone>
34.          <type>BUSINESS</type>
35.          <areaCode>11</areaCode>
36.          <number>30302323</number>
37.        </phone>
38.        <phone>
39.          <type>BUSINESS</type>
40.          <areaCode>11</areaCode>
41.          <number>976302323</number>
42.        </phone>
43.      </phones>
44.      <address>
45.        <postalCode>01452002</postalCode>
46.        <street>Av. Brig. Faria Lima</street>
47.        <number>1384</number>
48.        <complement>5o andar</complement>
49.        <district>Jardim Paulistano</district>
50.        <city>Sao Paulo</city>
51.        <state>SP</state>
52.        <country>BRA</country>
53.      </address>
54.    </company>
55.  </account>
56. </authorizationRequest>
```

Request parameters

The parameters below are aligned with the tag <authorizationRequest>.

XML PARAMETER	DESCRIPTION
<account>	This field is the root of the XML and includes the registration data. Presence: Optional.
<account> <email>	Account to be registered Presence: Optional. Type: Text. Format: A valid email (ex., user@site.com.br), restricted to 60 characters.
<account> <type>	Account type. Presence: Optional. Type: Text. Format: The account types are: PERSONAL, SELLER or COMPANY
<account> <person>	Groups seller data.
<account> <seller> <name>	Full name of seller Presence: Optional. Type: Text. Format: Free, restricted to 50 characters.
<account> <seller> <documents>	Groups the information of seller's document.
<account> <seller> <documents> <document>	Groups the information of seller's document. Presence: Optional (CPF number).
<account> <seller> <documents> <document> <type>	Document type Presence: Required, if the tag document is informed. Type: Text. Format: The document type allowed for the seller is only CPF.
<account> <seller> <documents> <document> <type> <value>	CPF number of seller Presence: Required, if the tag document is informed. Type: Number. Format: Will accept only valid and unrestricted CPF numbers (in PagSeguro/UOL).

XML PARAMETER	DESCRIPTION
<account> <seller> <birthDate>	Date of birth of Seller Presence: Optional. Type: Text. Format: DD/MM/AAAA.
<account> <seller> <phones>	Groups the telephone information of seller.
<account> <seller> <phones> <phone>	Groups the telephone information of seller. Presence: Optional.
<account> <seller> <phones> <phone> <type>	Telephone type Presence: Required, if tag phone is informed. Type: Text. Format: The types of phone numbers are HOME, MOBILE and BUSINESS.
<account> <seller> <phones> <phone> <areaCode>	Area code of phone. Presence: Required, if tag phone is informed. Type: Number. Format: A 2-digit number that represents a valid area code (DDD).
<account> <seller> <phones> <phone> <number>	Telephone number. Presence: Required, if tag phone is informed. Type: Number. Format: Accepts only numbers with 8 to 9 digits.
<account> <company>	Groups the company data
<account> <company> <displayName>	Full name of company Presence: Optional. Type: Text. Format: Free, restricted to 50 characters.
<account> <company> <documents>	Groups the information of the documents of the legal representative of the company and the company.

XML PARAMETER	DESCRIPTION
<account> <company> <documents> <document>	Groups the information of the documents of the legal representative of the company and the company. Presence: Optional (CPF and CNPJ)
<account> <company> <documents> <document> <type>	CNPJ of company Presence: Required, if tag document is informed. Type: Number. Format: Accepts only valid and unrestricted CNPJ numbers (in PagSeguro/UOL).
<account> <company> <websiteURL>	URL of company website Presence: Optional. Type: Text. Format: a valid URL with no more than 256 characters.
<account> <company> <partner>	Groups the data of the legal representative of the company.
<account> <company> <partner> <name>	Name of legal representative of company Presence: Optional. Type: Text. Format: Free, restricted to 50 characters.
<account> <seller> <documents> <document> <type> <value>	CPF of seller Presence: Required, if tag document is informed. Type: Number. Format: When the type is CPF, it will accept only valid and unrestricted CPF numbers (in PagSeguro/UOL).
<account> <company> <partner> <birthDate>	Date of birth of Seller Presence: Optional. Type: Text. Format: DD/MM/AAAA.
<account> <address>	Groups the address data of the seller or company. Presence: Optional.
<account> <address> <postalCode>	Postal code of address of seller or company. Presence: Optional. Type: Number. Format: An 8-digit number corresponding to a valid postal code.

XML PARAMETER	DESCRIPTION
<account> <address> <street>	Street name of address of seller or company. Presence: Optional. Type: Text. Format: Text with numbers, letters (no accent), spaces and characters "." (dot) and "-" hyphen, restricted to 80 characters. The value of this field will only be registered when the postal code informed does not have a street name linked to it.
<account> <address> <number>	Number of address of seller or company. Presence: Optional. Type: Text. Format: Free text, restricted to 20 characters.
<account> <address> <complement>	Complement of address of seller or company. Presence: Optional. Type: Text. Format: Text with numbers, letters (no accent), spaces and characters "." (dot) and "-" hyphen, restricted to 40 characters.
<account> <address> <district>	District of address of seller or company. Presence: Optional. Type: Text. Format: Text with numbers, letters (no accent), spaces and characters "." (dot) and "-" hyphen, restricted to 60 characters. The value of this field will only be registered when the postal code informed does not have a district name linked to it.
<account> <address> <city>	City of address of seller or company. Presence: Optional. Type: Text. Format: Free text. The city linked to the postal code informed will be registered.
<account> <address> <state>	State of address of seller or company. Presence: Optional. Type: Text. Format: Free text. The state linked to the postal code informed will be registered.

XML PARAMETER	DESCRIPTION
<code><account></code> <code><address></code> <code><country></code>	ISO code of country of address of seller or company. Presence: Optional. Type: Text. Format: from 2 to 10 numbers, letters and the character “-“ (hyphen).

Response of Authorization API

The response is given in XML format. The example below shows a successful response to a call made to the authorization API:

```

1. <authorizationRequest>
2.   <code>D8DD848AC9C98D9EE44C5FB3A1E53913</code>
3.   <date>2011-02-25T11:40:50.000-03:00</date>
4. </authorizationRequest>
    
```

The tables below describe the returned parameters.

PARAMETER	DESCRIPTION
<code><authorizationRequest></code>	Root of XML response file. Contains the data of the created authorization code.
<code><authorizationRequest></code> <code><code></code>	Redirect code created. This code must be used to direct the buyer to the authorization flow Type: Text. Format: A string of 32 characters.
<code><authorizationRequest></code> <code><date></code>	Request date. Type: Date/Time. Format: YYYY-MM-DDThh:mm:ss.STZD.

Should an error occur in the call to the Authorization API, an error response will be returned, as shown below. It will indicate all the errors identified in the call:

```

1. <errors>
2.   <error>
3.     <code>11064</code>
4.     <message>redirectURL must have the same domain as application
       URL.</message>
5.   </error>
6. </errors>
    
```

The table below describe the parameters returned.

PARAMETER	DESCRIPTION
<errors>	List of errors.
<errors> <error>	Data of error found.
<errors> <error> <code>	Error code. Type: Text. Format: See Table of Errors on page 34.
< errors > <error > <message>	Descriptive message. Type: Text. Format: See Table of Errors on page 34.

Directing the buyer to the authorization flow

After making a successful call to the API, you must direct the buyer to the authorization flow, using the request code returned. The example below shows an assembled URL for the user to start the authorization flow.

```
https://pagseguro.uol.com.br/v2/authorization/request.jhtml?code={requestCode}
```

The table below describes the parameter used

PARAMETER	DESCRIPTION
Code	Request code returned by call to Authorization API of PagSeguro Presence: Required.

Authorization Flow

By making a successful call to the authorization API and redirecting the client to PagSeguro, a screen based on the information that you sent in the call will be displayed.

If you sent no client data or sent the data and PagSeguro confirmed that this client has no PagSeguro account, a screen proposing the creation of a primary account below the option of logging into PagSeguro as shown in image 6 below:



Você precisa de uma conta PagSeguro para continuar

Crie uma conta PagSeguro

É fácil e rápido!

Pessoa física

Tipo vendedor - requer CPF

Pessoa jurídica

Tipo empresarial - requer CNPJ

Já tem uma conta PagSeguro?



Entre com seu email e senha

Image 6

If you sent the data and PagSeguro confirmed that this client has a PagSeguro account, the fields where he/she can log into PagSeguro will be displayed and below the option proposing the creation of an account as shown in image 7 below:



Você já está cadastrado no PagSeguro

Informe sua senha para prosseguir com o cadastro de vendedor no PagSeguro

É fácil e rápido!

E-mail

email-do-vendedor@uol.com.br

Senha

Para sua segurança, a senha deve possuir entre 5 e 8 caracteres misturando letras e números.

[Esqueci a minha senha](#)

Entrar

Quer criar uma nova conta?

É fácil e rápido!



[Cadastre uma nova conta](#)

Image 7

After having created the account or having typed in your password, a screen informing the client that your app wishes to gain access to the permissions sent in the authorization call will be displayed. The client also receives an explanation of each permission and the option to authorize or not the app as shown in Image 8 below:



Image 8

After the client's decision, by clicking on Authorize or Do not Authorize, he/she will be redirected to your return URL. In this return, PagSeguro will send via GET, the notification code of the authorization so you can immediately check the result of this authorization.

The return will be carried out as follows:

<http://www.seusite.com.br/retorno?notificationCode={notificationCode}>

Additionally, PagSeguro will send a notification to your website via POST.

Notifications

After the buyer authorizes the app, PagSeguro will send via POST a notification to your system with the authorization status.

Image 9 illustrates the operation of the notification. Please note that it is PagSeguro that initiates the notification process by sending a code to your system.

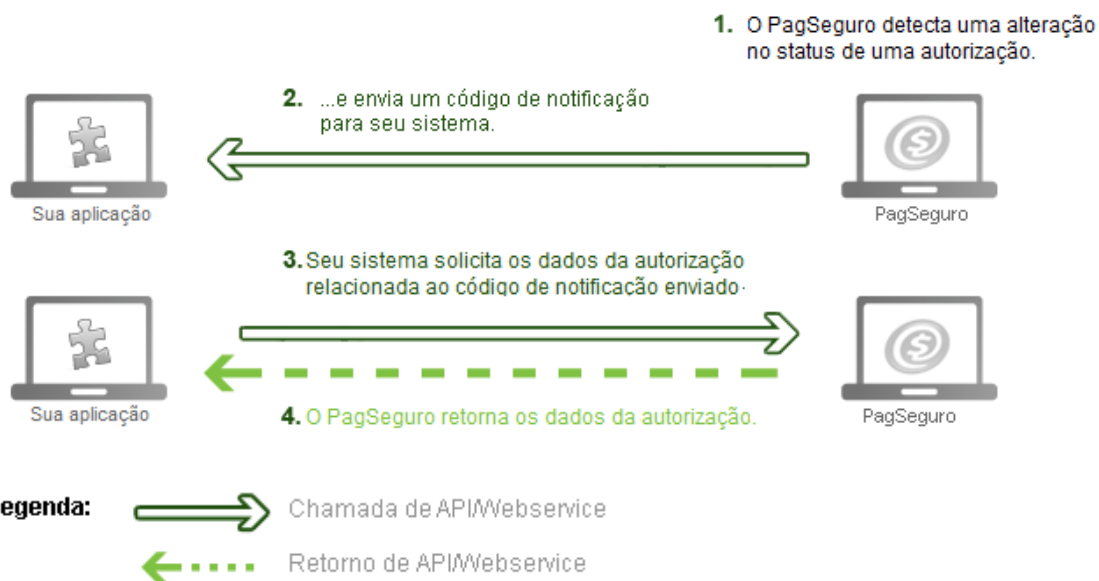


Image 9

Configuring the receipt of notifications

In order to use the Notifications API, you must first have created an app. The address (URL) of the notification is configured at the time of creation of the app, however, it can also be transferred as a parameter in the call as was shown earlier.

To view or change this URL in an already-existing app must be done through the app list page at the <https://pagseguro.uol.com.br/aplicacao/listagem.jhtml>, by clicking on the button **Edit app**.

Receiving a transaction notice

After the address to where PagSeguro will send notifications has been set up, the next step is to prepare the system to receive the notification code.

PagSeguro sends the notifications to the URL that you configured using the HTTP protocol under the **POST** method.

See below an example of a notification sent by PagSeguro (the lines were divided to ease reading).

```
POST http://lojamodelo.com.br/notificacao HTTP/1.1
Host:pagseguro.uol.com.br
Content-Length:85
Content-Type:application/x-www-form-urlencoded
notificationCode=766B9C-AD4B044B04DA-77742F5FA653-E1AB24
&notificationType=applicationAuthorization
```

PARAMETER	DESCRIPTION
notificationCode	<p>The code that identifies the notification. This code must be used to search the notification and get the data of the associated transaction/subscription. Note that the code that identifies the notification is not the same as the code that identifies the transaction.</p> <p>Type: Text. Format: A string of 39 characters.</p>
notificationType	<p>The type of notification sent.</p> <p>Type: Text. Format: For authorization notifications it will be applicationAuthorization</p>

Note that the notification has no information pertaining to the authorization. Therefore, as soon as your system receives a notification, it must search it to obtain the data, as described below.

It is worthwhile noting that, during the time that your system has not searched a notification sent, PagSeguro will send it again **every 2 hours**, up to a **maximum of 5 times**. If your system is unavailable for a period greater than this and did not receive any of the notifications, it is still possible to get the data of your authorizations using the Authorization Search.

Searches

PagSeguro uses a Search API so you can obtain the data of your authorizations easily, swiftly and safely.

See below how to perform a search:

Searching an authorization by notification code

This search must be used to search a notification received through POST sent by PagSeguro or through the GET parameter (notificationCode) sent through the redirect of the authorization page of PagSeguro in order to obtain the authorization data. The call must be made using the **GET** method.

Search URL:

```
https://ws.pagseguro.uol.com.br/v2/authorizations/notifications/{notificationCode}?appId={appId}&appKey={appKey}
```

Authentication parameters

PARAMETER	DESCRIPTION
appId	App ID. Presence: Required. Type: Text. Format: A string of up to 60 characters.
appKey	Specifies the token corresponding to the PagSeguro app that is making the request. Presence: Required. Type: Text. Format: A string of 32 characters.

Request parameters

PARAMETER	DESCRIPTION
notificationCode (after notifications/)	ID code of notification. Informs the notification code that you must search. The code must be informed in the URL path. You must use the code that you received by the notificationCode parameter at the sending of the notification. Presence: Required. Type: Text. Format: A string of 39 characters.

Searching an authorization by its code

This search provides access to all the data of an authorization based on its ID code. The call must be made using the **GET** method.

Search URL:

```
https://ws.pagseguro.uol.com.br/v2/authorizations/{authorizationCode}?appId={appId}&appKey={appKey}
```

Authentication parameters

PARAMETER	DESCRIPTION
appId	App ID. Presence: Required. Type: Text. Format: A string of up to 60 characters.
appKey	Specifies the token corresponding to the PagSeguro app that is making the request. Presence: Required. Type: Text. Format: A string of 32 characters.

Request Parameters

PARAMETER	DESCRIPTION
authorizationCode (after authorizations /)	Code that identifies the authorization to be consulted/cancelled. Presence: Required in the search of an authorization. Type: Text. Format: A string of 32 characters.

For both searches above, the response is given in XML format, as shown below.

```

1. <authorization>
2.   <code>9D7FF2E921216F1334EE9FBEB7B4EBBC</code>
3.   <creationDate>2011-03-30T14:20:13.000-03:00</creationDate>
4.   <reference>ref1234</reference>
5.   <permissions>
6.     <permission>
7.       <code>CREATE_CHECKOUTS</code>
8.       <status>APPROVED</status>
9.       <lastUpdate>2011-03-30T15:35:44.000-03:00</lastUpdate>
10.    </permission>
11.    <permission>
12.      <code>SEARCH_TRANSACTIONS</code>
13.      <status>APPROVED</status>
14.      <lastUpdate>2011-03-30T14:20:13.000-03:00</lastUpdate>
15.    </permission>
16.  </permissions>
17. </authorization>
    
```

The following tables describe the parameters returned by the queries:

PARAMETER	DESCRIPTION
<authorization>	Root of XML response file. Contains the data of the authorization.
<authorization> <code>	Authorization code. Type: Text.
<authorization> <creationDate>	Creation date of authorization Type: Text.
<authorization> <reference>	ID that was used to refer to the authorization at the time of the request. Type: Date/Time. Format: YYYY-MM-DDThh:mm:ss.sTZD.
<authorization> <permissions>	Represents the permissions returned by the authorization. Type: Text.
<authorization> <permissions> <permission>	Data of permission returned by search. Type: Text.

PARAMETER	DESCRIPTION										
<p><authorization> <permissions> <permission> <code></p>	<p>Code of permission. Type: Text.</p> <table border="1" data-bbox="547 383 1482 891"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CREATE_CHECKOUTS</td> <td>The app may direct the buyers to PagSeguro and mediate the payments for you.</td> </tr> <tr> <td>RECEIVE_TRANSACTION_NOTIFICATIONS</td> <td>The app may receive and search the notifications of the transactions that it mediated for you.</td> </tr> <tr> <td>SEARCH_TRANSACTIONS</td> <td>The app may search the transactions that it mediated for you.</td> </tr> <tr> <td>MANAGE_PAYMENT_PRE_APPROVALS</td> <td>The app may search the transactions that it mediated for you.</td> </tr> </tbody> </table>	Value	Description	CREATE_CHECKOUTS	The app may direct the buyers to PagSeguro and mediate the payments for you.	RECEIVE_TRANSACTION_NOTIFICATIONS	The app may receive and search the notifications of the transactions that it mediated for you.	SEARCH_TRANSACTIONS	The app may search the transactions that it mediated for you.	MANAGE_PAYMENT_PRE_APPROVALS	The app may search the transactions that it mediated for you.
Value	Description										
CREATE_CHECKOUTS	The app may direct the buyers to PagSeguro and mediate the payments for you.										
RECEIVE_TRANSACTION_NOTIFICATIONS	The app may receive and search the notifications of the transactions that it mediated for you.										
SEARCH_TRANSACTIONS	The app may search the transactions that it mediated for you.										
MANAGE_PAYMENT_PRE_APPROVALS	The app may search the transactions that it mediated for you.										
<p><authorization> <permissions> <permission> <status></p>	<p>Status of client permission. Type: Text.</p> <table border="1" data-bbox="547 1066 1139 1216"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>PENDING</td> <td>Approval pending</td> </tr> <tr> <td>APPROVED</td> <td>Approved by client</td> </tr> <tr> <td>DENIED</td> <td>Denied by client</td> </tr> </tbody> </table>	Value	Description	PENDING	Approval pending	APPROVED	Approved by client	DENIED	Denied by client		
Value	Description										
PENDING	Approval pending										
APPROVED	Approved by client										
DENIED	Denied by client										
<p><authorization> <permissions> <permission> <lastUpdate></p>	<p>Date/time in which the last change occurred in the permission status. Type: Text.</p>										

Searching all the app authorization

Through this search, you can check all the authorizations linked to your app. The call must be made using the **GET** method.

Search URL:

<https://ws.pagseguro.uol.com.br/v2/authorizations?appId={appId}&appKey={appKe}>

The result is displayed in XML as shown below:

```

1. <authorizationSearchResult>
2.   <date>2011-03-30T11:09:11.000-03:00</date>
3.   <authorizations>
4.     <authorization>
5.       <code>5A220D39B3B31E8BB4E3EFA4FCC4E6A3</code>
6.       <creationDate>2011-03-21T16:32:21.000-03:00</creationDate>
7.       <reference>123</reference>
8.       <permissions>
9.         <permission>
10.          <code>SEARCH_TRANSACTIONS</code>
11.          <status>APPROVED</status>
12.          <lastUpdate>2011-03-21T16:32:21.000-03:00</lastUpdate>
13.        </permission>
14.        <permission>
15.          <code>RECEIVE_TRANSACTION_NOTIFICATIONS</code>
16.          <status>APPROVED</status>
17.          <lastUpdate>2011-03-24T16:15:07.000-03:00</lastUpdate>
18.        </permission>
19.        <permission>
20.          <code>CREATE_CHECKOUTS</code>
21.          <status>APPROVED</status>
22.          <lastUpdate>2011-03-21T16:32:21.000-03:00</lastUpdate>
23.        </permission>
24.      </permissions>
25.    </authorization>
26.  </authorizations>
27. </authorizationSearchResult>

```

The tables below describe the parameters returned by the searches.

PARAMETER	DESCRIPTION
<authorizationSearchResult>	Root of XML response file. Contains the data of the authorization search.
<date>	Informs the date/time in which the search occurred.

PARAMETER	DESCRIPTION										
<authorizationSearchResult> <authorizations> <authorization>	Contains the authorization data.										
<authorizationSearchResult> <authorizations> <authorization> <code>	Authorization code. Type: Text.										
<authorizationSearchResult> <authorizations> <authorization> <creationDate>	Authorization Creation date: Type: Text.										
<authorizationSearchResult> <authorizations> <authorization> <reference>	ID that was used to refer to the authorization at the time of the request. Type: Date/Time. Format: YYYY-MM-DDThh:mm:ss.sTZD.										
<authorizationSearchResult> <authorizations> <authorization> <permissions>	Represents the permissions returned by the authorization. Type: Text.										
<authorizationSearchResult> <authorizations> <authorization> <permissions> <permission>	Data of permission returned by search. Type: Text.										
<authorizationSearchResult> <authorizations> <authorization> <permissions> <permission> <code>	Code of permission. Type: Text. <table border="1" data-bbox="660 1442 1482 2020"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CREATE_CHECKOUTS</td> <td>The app may direct the buyers to PagSeguro and mediate the payments for you.</td> </tr> <tr> <td>RECEIVE_TRANSACTION_NOTIFICATIONS</td> <td>The app may receive and search the notifications of the transactions that it mediated for you.</td> </tr> <tr> <td>SEARCH_TRANSACTIONS</td> <td>The app may search the transactions that it mediated for you.</td> </tr> <tr> <td>MANAGE_PAYMENT_PRE_APPROVALS</td> <td>The app may manage and use payment pre-approvals for you.</td> </tr> </tbody> </table>	Value	Description	CREATE_CHECKOUTS	The app may direct the buyers to PagSeguro and mediate the payments for you.	RECEIVE_TRANSACTION_NOTIFICATIONS	The app may receive and search the notifications of the transactions that it mediated for you.	SEARCH_TRANSACTIONS	The app may search the transactions that it mediated for you.	MANAGE_PAYMENT_PRE_APPROVALS	The app may manage and use payment pre-approvals for you.
Value	Description										
CREATE_CHECKOUTS	The app may direct the buyers to PagSeguro and mediate the payments for you.										
RECEIVE_TRANSACTION_NOTIFICATIONS	The app may receive and search the notifications of the transactions that it mediated for you.										
SEARCH_TRANSACTIONS	The app may search the transactions that it mediated for you.										
MANAGE_PAYMENT_PRE_APPROVALS	The app may manage and use payment pre-approvals for you.										

PARAMETER	DESCRIPTION								
<authorizationSearchResult> <authorizations> <authorization> <permissions> <permission> <status>	Status of client permission. Type: Text. <table border="1" data-bbox="662 383 1254 533"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>PENDING</td> <td>Approval pending</td> </tr> <tr> <td>APPROVED</td> <td>Approved by client</td> </tr> <tr> <td>DENIED</td> <td>Denied by client</td> </tr> </tbody> </table>	Value	Description	PENDING	Approval pending	APPROVED	Approved by client	DENIED	Denied by client
Value	Description								
PENDING	Approval pending								
APPROVED	Approved by client								
DENIED	Denied by client								
<authorizationSearchResult> <authorizations> <authorization> <permissions> <permission> <lastUpdate>	Date/time in which the last change occurred in the permission status. Type: Text.								

If an error occurs in the call to the Search API, in the parameters informed of if a technical failure occurs in the system, an error response will be returned, as shown below. It will indicate all the errors identified in the call:

```

1. <errors>
2.   <error>
3.     <code>13014</code>
4.     <message>maxPageResults invalid value (must be between 1 and
5.       1000).</message>
6.   </error>
7. </errors>
    
```

The response XML fields of the search of a transaction notification are described below.

PARAMETER	DESCRIPTION
<errors>	List of errors.
<errors> <error>	Data of error found.
<errors> <error> <code>	Error code. Type: Text. Format: See Table of Errors on page 34.
<errors> <error> <message>	Descriptive message. Type: Text. Format: See Table of Errors on page 34.

Using APIs of PagSeguro

After getting the authorization, your app can use PagSeguro's services in the name of the seller.

To use PagSeguro's APIs using the authorization granted by the client, simply replace the items **email** and **token** for **appId**, **appKey** and for the **authorizationCode** generated by the app. See below how to use the APIs available in PagSeguro with the App Model:

Payment API

Without the use of the Application Model, the call to PagSeguro is done using the e-mail and token of the client. See below an example of the call without the App Model for the Payment API (the lines have been divided to ease reading):

```
curl https://ws.pagseguro.uol.com.br/v2/checkout/ -d\  
  "email=suporte@lojamodelo.com.br\  
  &token=95112EE828D94278BD394E91C4388F20\  
  &currency=BRL\  
  &itemId=0001\  
  &itemDescription1=Notebook Prata\  
  &itemAmount1=24300.00\  
  &itemQuantity1=1\  
  &itemWeight1=1000\  
  &reference=REF1234\  
  &senderName=Jose Comprador\  
  &senderAreaCode=11\  
  &senderPhone=56273440\  
  &senderEmail=comprador@uol.com.br\  
  &shippingType=1\  
  &shippingAddressStreet=Av. Brig. Faria Lima\  
  &shippingAddressNumber=1384\  
  &shippingAddressComplement=5o andar\  
  &shippingAddressDistrict=Jardim Paulistano\  
  &shippingAddressPostalCode=01452002\  
  &shippingAddressCity=Sao Paulo\  
  &shippingAddressState=SP\  
  &shippingAddressCountry=BRA"
```

With the use of the App Model, the call to PagSeguro is done using the **appId**, the **appKey** and the **authorizationCode** of the client. See below an example of the same call using the App Model (the lines have been divided to ease reading):

```
curl https://ws.pagseguro.uol.com.br/v2/checkout/ -d\  
  "appId=lojamodelo\  
  &appKey=CAD9C79F4141DF222401CF940D6F0682\  
  &authorizationCode=D8DD848AC9C98D9EE44C5FB3A1E53913\  
  &currency=BRL\  
  &itemId=0001\  
  &itemDescription1=Notebook Prata\  
  &itemAmount1=24300.00\  
  &itemQuantity1=1\  
  &itemWeight1=1000\  
  &reference=REF1234\  
  &senderName=Jose Comprador\  
  &senderAreaCode=11"
```

```
&senderPhone=56273440\  
&senderEmail=comprador@uol.com.br\  
&shippingType=1\  
&shippingAddressStreet=Av. Brig. Faria Lima\  
&shippingAddressNumber=1384\  
&shippingAddressComplement=5o andar\  
&shippingAddressDistrict=Jardim Paulistano\  
&shippingAddressPostalCode=01452002\  
&shippingAddressCity=Sao Paulo\  
&shippingAddressState=SP\  
&shippingAddressCountry=BRA"
```

Notification API

The Notification API is the only API that does not require an authorizationCode. See below an example of a call to this API without the App Model (the lines have been divided to ease reading):

```
https://ws.pagseguro.uol.com.br/v2/transactions/notifications  
/9E884542-81B3-4419-9A75-BCC6FB495EF1  
?email=suporte@lojamodelo.com.br  
&token=95112EE828D94278BD394E91C4388F20
```

By using the app model, simply transfer, instead of the email and token of the client, the appId and appKey of your app as shown below (the lines have been divided to ease reading):

```
https://ws.pagseguro.uol.com.br/v2/transactions/notifications  
/9E884542-81B3-4419-9A75-BCC6FB495EF1  
?appId=lojamodelo  
&appKey=D8DD848AC9C98D9EE44C5FB3A1E53913
```

Search API

See below an example of the call for this Transaction Search API without the App Model (the lines have been divided to ease reading):

```
https://ws.pagseguro.uol.com.br/v2/transactions  
/9E884542-81B3-4419-9A75-BCC6FB495EF1  
?email=suporte@lojamodelo.com.br  
&token=95112EE828D94278BD394E91C4388F20
```

By using the app model, simply transfer, instead of the email and token of the client, the appId, appKey and authorizationCode as shown below (the lines have been divided to ease reading):

```
https://ws.pagueseguro.uol.com.br/v2/transactions
/9E884542-81B3-4419-9A75-BCC6FB495EF1
?appId=lojamodelo
&appKey=D8DD848AC9C98D9EE44C5FB3A1E53913
&authorizationCode=D8DD848AC9C98D9EE44C5FB3A1E53913
```

The same process can be applied for searches of Transaction Timeline and for the search of Abandoned Transactions.

Creation of Subscription

See below an example of a call to this Subscription API without the App Model (the lines have been divided to ease reading):

```
curl -k https://ws.pagueseguro.uol.com.br/v2/pre-approvals/request -d\
"email=suporte@lojamodelo.com.br\
&token=95112EE828D94278BD394E91C4388F20\
&reference=REF1234\
&redirectURL=http://www.notebookprata.com.br/retorno.php\
&reviewURL=http://www.notebookprata.com.br/revisao.php\
&preApprovalCharge>manual\
&preApprovalName=Seguro contra roubo do Notebook Prata\
&preApprovalDetails=Seguro contra roubo do Notebook Prata.\
&preApprovalAmountPerPayment=100.00\
&preApprovalPeriod=Monthly\
&preApprovalDayOfMonth=28\
&preApprovalMaxPaymentsPerPeriod=1\
&preApprovalMaxAmountPerPeriod=100.00\
&preApprovalInitialDate=2013-09-01T00:00:00-03:00\
&preApprovalFinalDate=2013-12-01T00:00:00-03:00\
&preApprovalMaxTotalAmount=400.00"
```

With the use of App Model, the call to PagSeguro is done using the appId, appKey and the authorizationCode of the client. See below an example of the same call using the App Model (the lines have been divided to ease reading):

```
curl -k https://ws.pagueseguro.uol.com.br/v2/pre-approvals/request -d\
"appId=lojamodelo\
&appKey=CAD9C79F4141DF222401CF940D6F0682\
&authorizationCode=D8DD848AC9C98D9EE44C5FB3A1E53913\
&reference=REF1234\
&redirectURL=http://www.notebookprata.com.br/retorno.php\
&reviewURL=http://www.notebookprata.com.br/revisao.php\
```



```
&preApprovalCharge>manual\  
&preApprovalName=Seguro contra roubo do Notebook Prata\  
&preApprovalDetails=Seguro contra roubo do Notebook Prata.\  
&preApprovalAmountPerPayment=100.00\  
&preApprovalPeriod=Monthly\  
&preApprovalDayOfMonth=28\  
&preApprovalMaxPaymentsPerPeriod=1\  
&preApprovalMaxAmountPerPeriod=100.00\  
&preApprovalInitialDate=2013-09-01T00:00:00-03:00\  
&preApprovalFinalDate=2013-12-01T00:00:00-03:00\  
&preApprovalMaxTotalAmount=400.00"
```

Other APIs follow the same process:

Revocation of authorization

Your client may revoke at any time the authorization granted to the app. As such, he/she must access the following link, select the app desired and click on Remove authorization as shown in Image 10.

Link: <https://pagseguro.uol.com.br/aplicacao/listarAutorizacoes.jhtml>

APLICAÇÕES AUTORIZADAS

Confira as aplicações autorizadas por você.

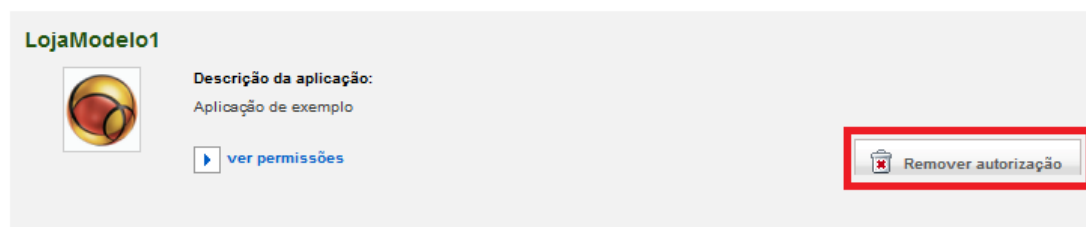


Image 10

Table of Errors

See below the table of errors:

ERROR CODE	DESCRIPTION
12001	appId is required.
12002	appKey is required.
12003	permissions is required.
12004	redirectURL is required.

ERROR CODE	DESCRIPTION
12005	appId invalid length: {0}
12006	appKey invalid length: {0}
12007	reference invalid length: {0}
12008	permissions invalid length: {0}
12009	redirectURL must have the same domain as application URL.
12010	permissions invalid: {0}
12011	inactive application: {0}
12012	redirectURL invalid length: {0}
12013	redirectURL invalid value: {0}
50110	Date must be like yyyy-MM-dd
50128	The telephone does not respect the 8 or 9 digit pattern
50129	The telephone area code must have 2 digits
50130	The postal code must have 8 digits
50132	The CPF must have 11 digits
50133	The CNPJ must have 14 digits
50134	Seller must be over 18 years old
50135	Partner must be over 18 years old
50136	Invalid e-mail
50137	Invalid user type
50140	Email too big. Maximum = 60 characters
50141	Name too big. Maximum = 50 characters
50142	Address too big. Maximum = 80 characters
50143	Address Number too big. Maximum = 20 characters
50144	Address Complement too big. Maximum = 40 characters
50145	Address District too big. Maximum = 60 characters

ERROR CODE	DESCRIPTION
50146	Company Name too big. Maximum = 50 characters
50147	Display Name too big. Maximum = 50 characters
50148	Website URL too big. Maximum = 256 characters