

# SOCIETE GENERALE LUXEMBOURG PSD2 API Solution

**Addressees:**

Business Analysts, Project Managers, Developers, Architects, IT

**Version 1.2, October 17th, 2022**

## Table des matières

<b>1</b>	<b>Introduction.....</b>	<b>3</b>
<b>2</b>	<b>TPP ONBOARDING PREREQUISITES.....</b>	<b>4</b>
<b>3</b>	<b>TPP ONBOARDING.....</b>	<b>4</b>
3.1	Register and Login.....	5
3.2	Upload TPP certificate .....	7
3.3	Certificate Status Validation .....	10
3.4	Creating application .....	11
3.5	Generate key.....	13
3.6	Add TPP Redirect (Callback) URL .....	15
3.7	Add The TPP SECRET.....	16
3.8	Subscribe to API.....	18
<b>4</b>	<b>Postman collection.....</b>	<b>19</b>
4.1	TPP & Client authentication .....	19
4.1.2	Consent Creation .....	24
4.1.3	Account information .....	32
4.2	Regenerate tokens .....	36
4.2.1	Regenerate Access Token.....	36
4.2.2	Regenerate Refresh Token .....	37
<b>5</b>	<b>References .....</b>	<b>39</b>
<b>6</b>	<b>ANNEXES.....</b>	<b>41</b>
6.1	Glossary.....	41

## Document history

Version	Description (remarks)	Date	Author(s)
1.0	Document creation	September 12 <sup>th</sup> , 2022	Naim BERKANI
1.1	Document update	October 14 <sup>th</sup> , 2022	Mina OOULADE & Naim BERKNI
1.2	Document finalization	October 17 <sup>th</sup> , 2022	Naim BERKANI

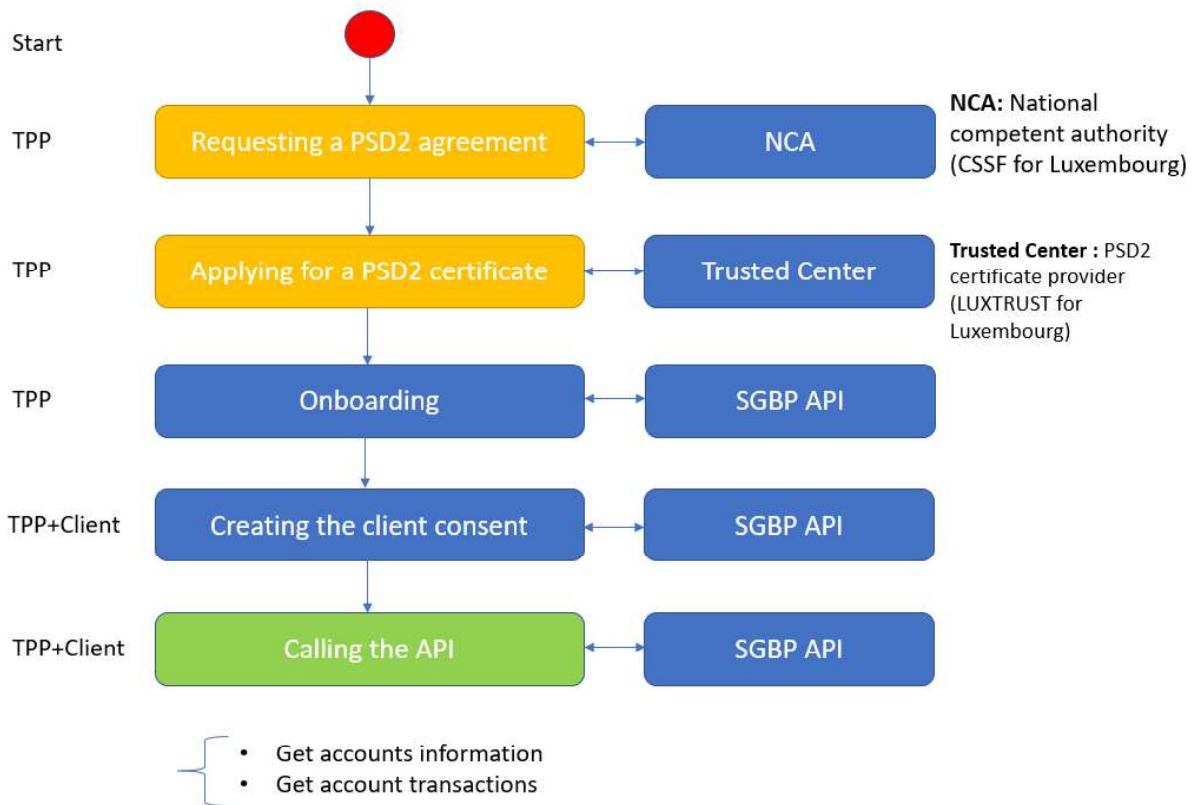
# 1 Introduction

This document describes how Third-Party Providers (TPPs) can connect the PSD2 Solution of SOCIETE GENERALE LUXEMBOURG.

The document assumes that the reader has basic knowledge about Payment Services Directive 2 (PSD2) regulation of the European Union, its terminology and use cases.

The document assumes that TPP is aware about the request for a PSD2 certificate from QTSP (Qualified Trust Service Provider).

The full process allowing TPPs to use the API is :



## 2 TPP ONBOARDING PREREQUISITES

Before sending queries ,TPPs should perform the following actions:

- **Step1:** TPP requests and gets the agreement from the National competent authority (CSSF in LUX),the agreement contains following
- **Step2:**TPP applies and obtains the PSD2 Certificate from a Trusted center (ex:LUX TRUST in LUX)

PSD2 certificate : an EiDAS certificates enriched with the following PSD2 information

1. TPP identifier ("PSD**CC**-**NCA**-**nnnnnnn**)
  - ✓ **CC**: 2 character ISO 3166-1 [8] country code representing the Competent Authority country;
  - ✓ **NCA** : [2-8] character Competent Authority identifier without country code (A-Z uppercase only, no separator)
  - ✓ **nnnnnnn** :identifier (authorization number as specified by the Competent Authority. There are no restrictions on the characters used).  
Exemple: PSD**LU**-**CSSF**-**xxxxxxxx**
    - **LU**: Luxembourg
    - **CSSF**: NCA luxembourg
2. Scope
  - Account information service provider (AISP) and/or
  - Payment initiation service provider (PISP)
3. Validity date
4. Passporting (Geographical area of the agreement)

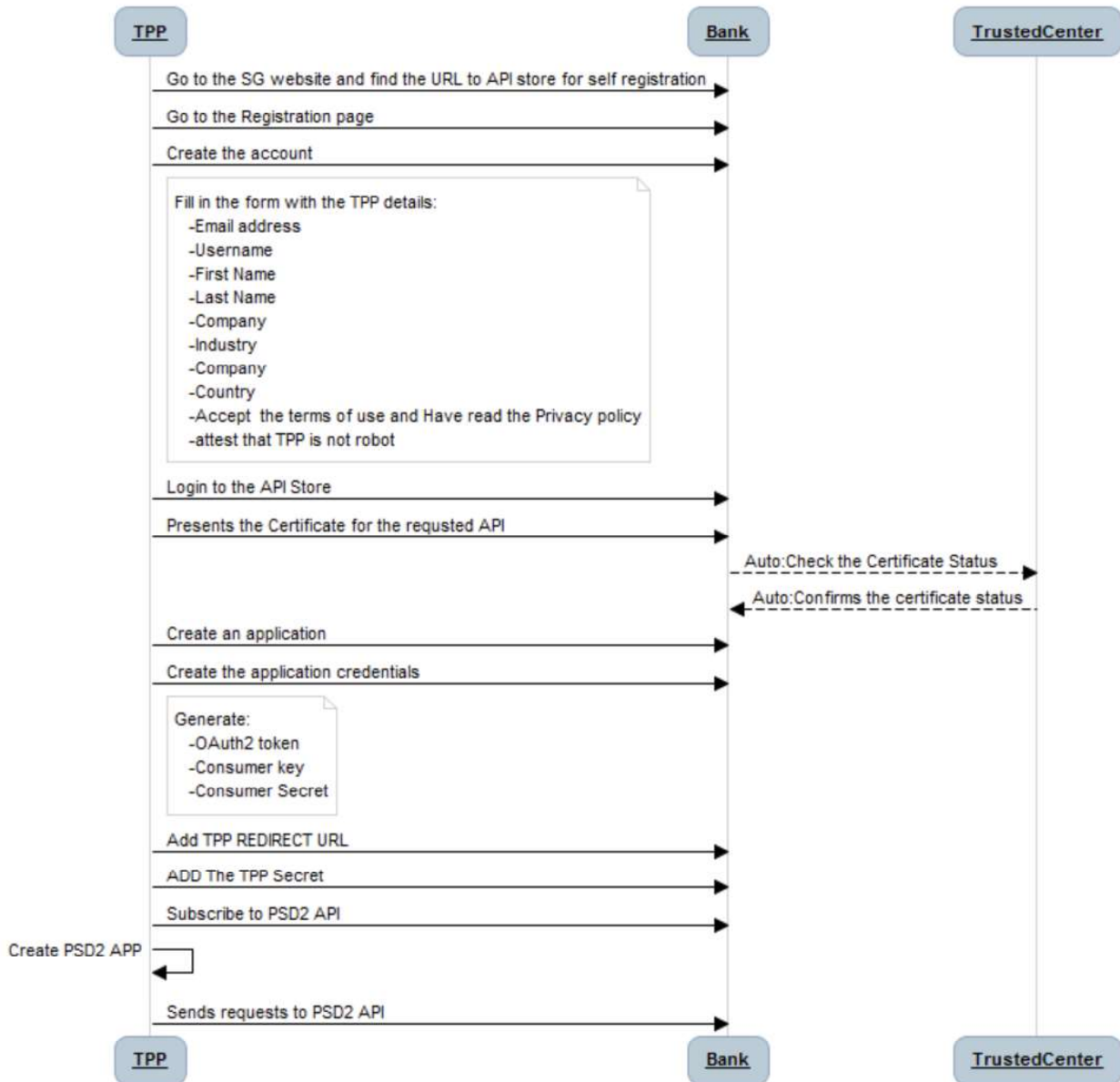
## 3 TPP ONBOARDING

This section explains how to prepare the use of PSD2 API. TPP registration, application creation, certificate management, etc.

Environment preparation process is the same in the non-production and production environment: The returned results (AIS) when a consent is established between a client and the TPP are the same when a client logs directly to the eBanking application. A certificate check will be done against the trusted center having issued it, role check, authorization on the APIs according to the role.

Here is the steps in order to prepare the environment:

## TPP Onboarding



### 3.1 Register and Login

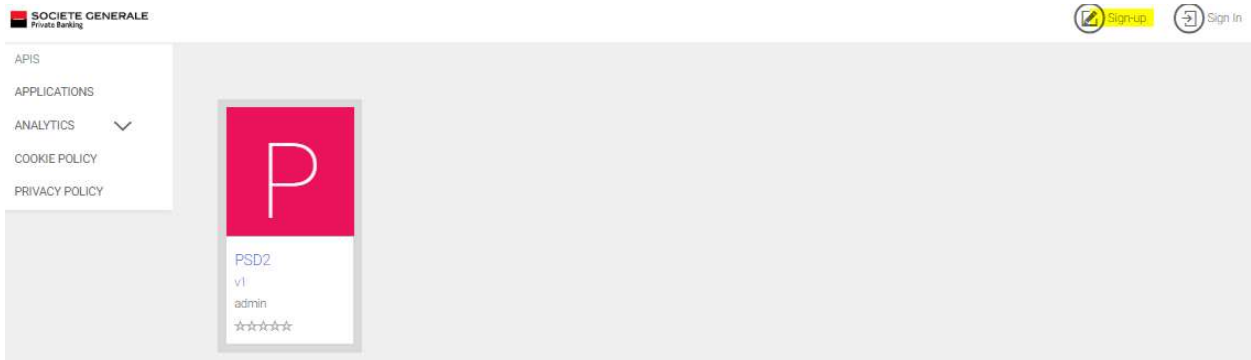
TPP registration is made under API store website

API Store website urls :

NON-PRODUCTION	<a href="https://int-api.privatebanking.societegenerale.lu/ebankingPsd2/store/">https://int-api.privatebanking.societegenerale.lu/ebankingPsd2/store/</a>
PRODUCTION	<a href="https://api.privatebanking.societegenerale.lu/ebankingPsd2/store/">https://api.privatebanking.societegenerale.lu/ebankingPsd2/store/</a>

To be able to work in the API Store, the TPP must be identified and this requires a one-time registration,

To register, please click on the "Sign-up" button at the top of the page. A form will open in which TPP can enter the necessary data.



Fill the following form:

Create your Account

Username \*  
e.g. JohnDoe  
Characters left: 30

Password \*

Re-type Password \*

First Name \*

Last Name \*

Email \*

[View Additional Details](#)

I hereby confirm that I have read and understood the [Privacy Policy](#).

After the registration is completed, TPP can log in to the store. To do this, please use the "Sign-In" button at the top of the page:



TPP will now be asked for login data.

### 3.2 Upload TPP certificate

After logging to the API store, the TPP is redirected to the PSD2 Certificate upload form

- Click on the “Add certificate” button

**Change TPP data**

---

**Third party provider**

TPP-Name\*

TPP-ID

**Roles**

Roles

Account Servicing (PSP\_AS)

Payment Initiation (PSP\_PI)

Account Information (PSP\_AI)

Issuing of card-based payment instruments (PSP\_IC)

**Information**  
By deactivating the checkboxes, the functionalities of the TPP are withdrawn even if the certificate is valid

**Contact Person Data**

First name\*

Last name\*

E-Mail

**TPP Status**

Status\*

\* mandatory fields

- Click on “CHOOSE FILE TO UPLOAD” button

◀ Add Certificate

The screenshot shows a web form titled 'Add Certificate'. It contains several sections: 'Certificate Upload' with a 'CHOOSE FILE TO UPLOAD' button; 'Third party provider' with fields for 'TPP-Name' and 'TPP-ID'; 'Certificate Status' with an 'Issued by' field; 'Roles' with four checkboxes: 'Account Servicing (PSP\_AS)', 'Payment Initiation (PSP\_PI)', 'Account Information (PSP\_AI)', and 'Issuing of card-based payment instruments (PSP\_IC)'; and 'Certificate Validation' with a 'Status\*' dropdown menu set to 'Received' and a 'Last checked' field. At the bottom are 'CANCEL', 'ADD MORE', and 'SAVE' buttons.

Certificate upload button

Informations not yet available

- Go to the file location and select the certificate file

◀ Add Certificate

This screenshot shows the same 'Add Certificate' form as above, but with a Windows File Explorer window overlaid. The File Explorer is open to the path 'GROUPE\_SOCIETE\_GENERALE' and shows a list of files: 'GROUPE\_SOCIETE\_GENERALE\_EV-AIS.crt', 'GROUPE\_SOCIETE\_GENERALE\_EV-AIS.key', 'GROUPE\_SOCIETE\_GENERALE\_EV-AIS.p12', and 'GROUPE\_SOCIETE\_GENERALE\_EV-AIS.pem'. The 'GROUPE\_SOCIETE\_GENERALE\_EV-AIS.crt' file is selected. The 'File name' field at the bottom of the File Explorer contains 'GROUPE\_SOCIETE\_GENERALE\_EV-' and the file type is set to 'All Files'. The 'Open' button is highlighted.

Navigate to the certificate file location

Upload file



- Click on “Open” button

The TPP/Certificate informations will be extracted from the file:

- TPP\_ID
- Cert\_ID
- Certificate issuer
- Valid from date
- Valid to date
- PSD2 role(s)
- Certificate Status: First, the status of the certificate is “received” until the validation job running

### 3.3 Certificate Status Validation

This action is automatically performed with a scheduled job, the solution will call the CRLs: “Certificate Revocation Lists” provided by the Trusted center (these URL is extracted from the certificate ) if the certificate is not revoked, the status of the uploaded certificate will be “VALID”

Third party provider

TPP-Name\*

TPP-ID

Contact Person Data

First name\*

Last name\*

E-Mail

ⓘ In the required fields first name, last name and E-mail the data of the TPP contact person needs to be entered. It is possible to import this data fields from the previous WSO2 registration through the button "import".

TPP Status

Status

Certificates

Cert-ID	Status	Valid from	Valid to	Last checked
3613709580464993324	VALID	2019-05-03	2021-05-03	2020-03-17
0320194398368332333				
993853820				

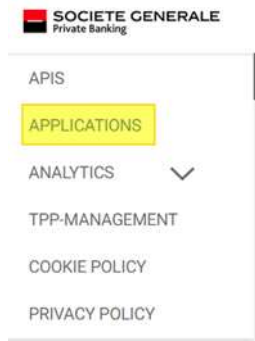
\* mandatory fields

TPP-ID to use in PSD2 requests

### 3.4 Creating application

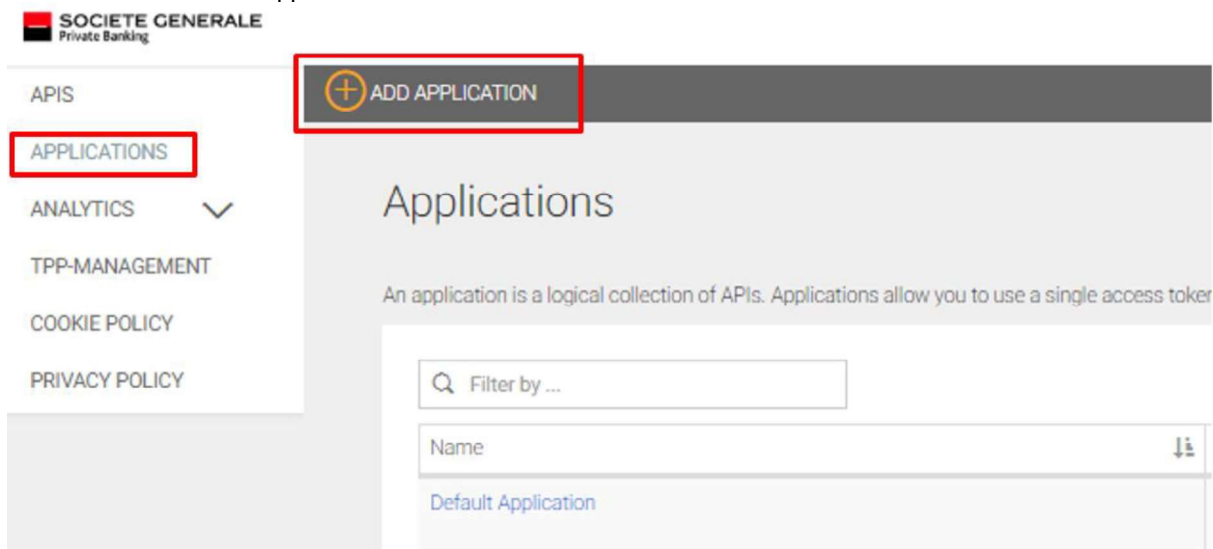
Afterwards TPP must select the application to use in order to "consume" it. This application practically serves as a storage location for the later API.

Please click on the menu entry "APPLICATIONS"



Now another area opens, then an already created entry "DefaultApplication" is displayed. This application has already been automatically added for TPP during the registration process, as a new application will be created the "DefaultApplication" and can be ignored.

TPP Adds the first own application via the button "ADD APPLICATION".



TPP will now be guided through the installation with the following dialog. First give the application a meaningful name such as the TPP company name. Enter this name in the upper field "Name".

TPP is welcome to fill in the other fields if required, but they are not mandatory for using the API.

## Add Application

An application is a logical collection of APIs. Applications allow you to use a single access token to invoke a collection of APIs and to share a single access token across multiple APIs. DefaultApplication is pre-created and allows unlimited access by default.

Name\*

Characters left: 70

Per Token Quota

Unlimited



Allows unlimited requests

This feature allows you to assign an API request quota per access token. Allocated quota will be shared among all the subscribed APIs of the application.

Description

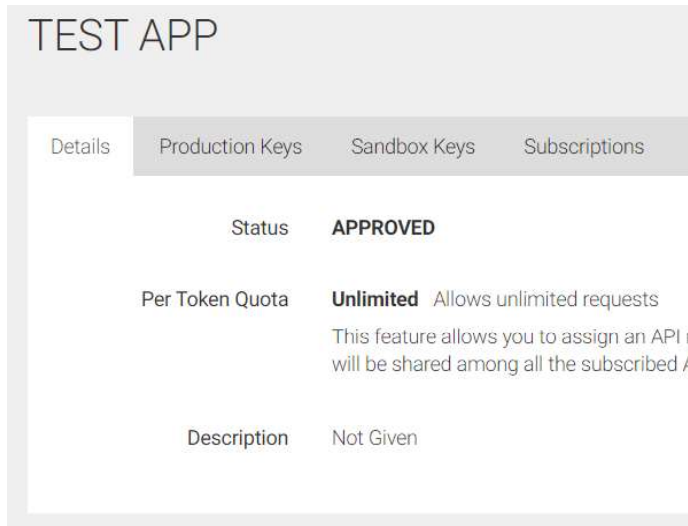
Add

Cancel

The "Add" button completes the process and the application is ready. TPP can now open the newly created application

### 3.5 Generate key

In order to communicate with the API, the system needs keys, here called "Production Keys". These keys must be generated once. Open the newly created application then click on the "Productions keys" tab.



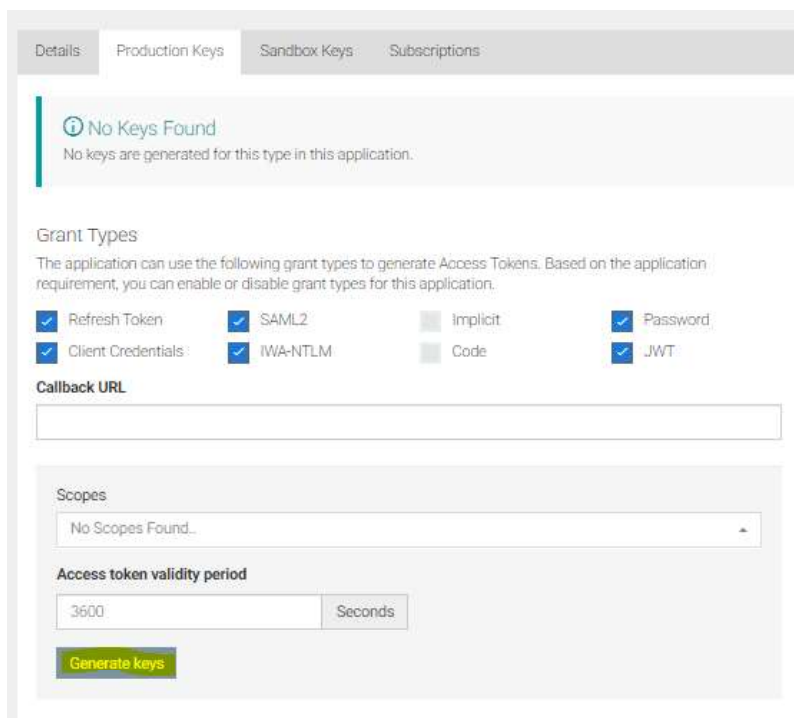
TEST APP

Details Production Keys Sandbox Keys Subscriptions

Status **APPROVED**

Per Token Quota **Unlimited** Allows unlimited requests  
This feature allows you to assign an API re  
will be shared among all the subscribed A

Description Not Given



Details Production Keys Sandbox Keys Subscriptions

**No Keys Found**  
No keys are generated for this type in this application.

**Grant Types**  
The application can use the following grant types to generate Access Tokens. Based on the application requirement, you can enable or disable grant types for this application.

Refresh Token  SAML2  Implicit  Password  
 Client Credentials  IWA-NTLM  Code  JWT

**Callback URL**

Scopes  
No Scopes Found..

**Access token validity period**  
3600 Seconds

**Generate keys**

The button "Generate Keys" initiates the generation. Please click on the button. No need to make any changes to the settings above.

The newly created keys are displayed:

- consumer key
- consumer secret
- access token

BankingApp

Details Production Keys Sandbox Keys Subscriptions

Hide Keys

Consumer Key

y\_t4z8BfgqcirYfz6ZINJXEwKTla

Consumer Secret

PjyOUhN5ohE9Q\_UXaL9mX0xaf0Aa

Details Production Keys Sandbox Keys Subscriptions

Show Keys

Consumer Key

.....

Consumer Secret

.....

Grant Types

The application can use the following grant types to generate Access Tokens. Based on the application requirement, you can enable or disable grant types for this application.

Refresh Token  SAML2  Implicit  Password  
 Client Credentials  IWA-NTLM  Code  JWT

Callback URL

.....

Update

### Generating Access Tokens

The following cURL command shows how to generate an access token using the Password Grant type.

```
curl -k -d "grant_type=password&username=Username&password=Password" \
-H "Authorization: Basic Base64(consumer-key:consumer-secret)" \
https://int-api.privatebanking.societegenerale.lu/ebankingPsd2/token
```

In a similar manner, you can generate an access token using the Client Credentials grant type with the following cURL command.

```
curl -k -d "grant_type=client_credentials" \
-H "Authorization: Basic Base64(consumer-key:consumer-secret)" \
https://int-api.privatebanking.societegenerale.lu/ebankingPsd2/token
```

### Generate a Test Access Token

#### Access Token

.....

Above token has a validity period of **3600** seconds. And the token has ( **am\_application\_scope,default** ) scopes.

Scopes

No Scopes Found..

Validity period

3600 Seconds

Regenerate

### 3.6 Add TPP Redirect (Callback) URL

Redirect URLs are a part of the OAuth flow. After a user successfully authorizes an application, the authorization server will redirect the user back to the application with either an authorization code or access token in the URL.

- Click on “TPP-MANAGEMENT”

You will have to reauthenticate with same credentials.

**SOCIETE GENERALE**  
Private Banking

APIS  
APPLICATIONS  
ANALYTICS  
**TPP-MANAGEMENT**  
COOKIE POLICY  
PRIVACY POLICY

**Change TPP data**

**Third party provider**

TPP-Name\*

TPP-ID PSDLU-CSSF-B00000019

**Contact Person Data**

First name\*

Last name\*

E-Mail

ⓘ In the required fields first name, last name and E-mail the data of the TPP contact person needs to be entered. It is possible to import this data fields from the previous WSO2 registration through the button "import".

**TPP Status**

Status VALID

**Certificates**

Cert-ID	Status	Valid from	Valid to	Last checked
3613709580464593324 0320194398368332333 993853820	VALID	2019-05-03	2021-05-03	2020-03-17

\* mandatory fields

- Click on “ADD REDIRECT URL”

### ⏪ Add Redirect URL

**Redirect URL**

---

Redirect URL

- Enter the URL
- Click on “SAVE” button the save the URL

## 3.7 Add The TPP SECRET

- Click on the “TPP-MANAGEMENT” item

**Change TPP data**

---

**Third party provider**

TPP Name\*

TPP-ID

---

**Contact Person Data**

First name\*

Last name\*

E-Mail

ⓘ In the required fields first name, last name and E-mail the data of the TPP contact person needs to be entered. It is possible to import this data fields from the previous WSO2 registration through the button "import".

---

**TPP Status**

Status

---

**Certificates**

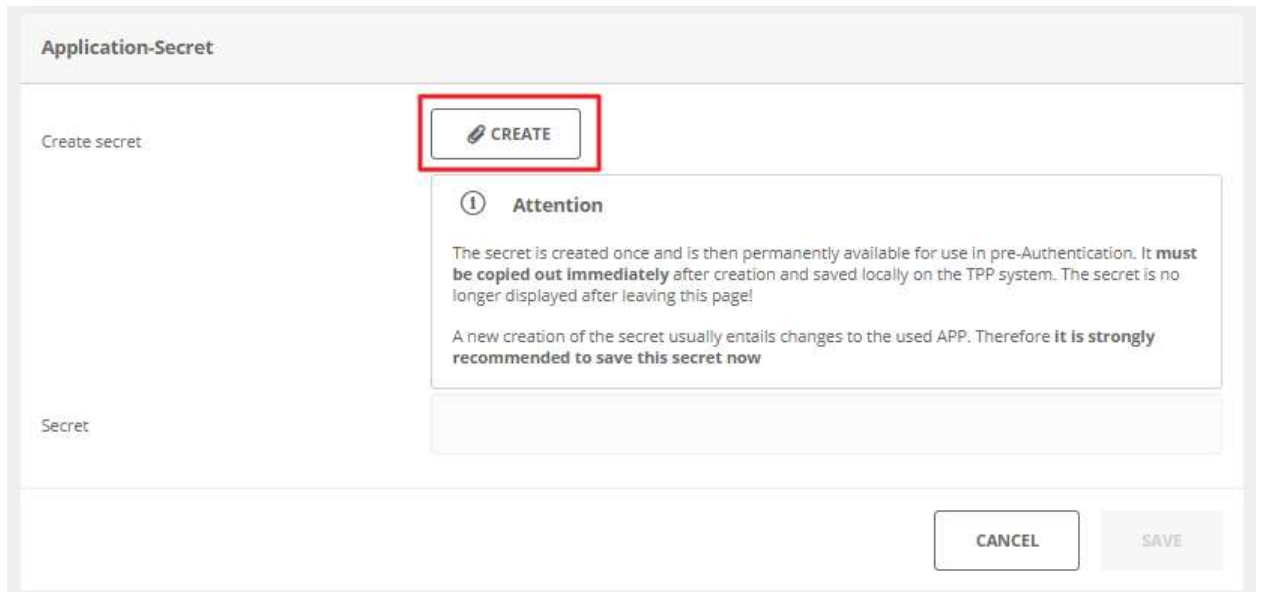
Cert-ID	Status	Valid from	Valid to	Last checked
3613709580464593324	VALID	2019-05-03	2021-05-03	2020-03-17
0320194398368332333				
993853820				

---

\* mandatory fields

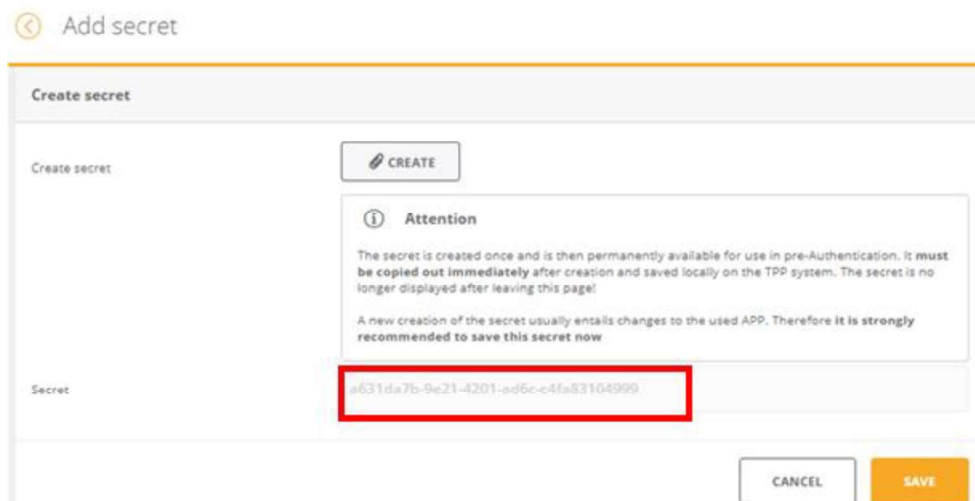


- Click on the “ADD SECRET” button



The screenshot shows a form titled "Application-Secret". On the left, there is a "Create secret" label and a "Secret" input field. On the right, there is a "CREATE" button with a pencil icon, which is highlighted with a red rectangular box. Below the button is an "Attention" warning box with an information icon. The warning text reads: "The secret is created once and is then permanently available for use in pre-Authentication. It **must be copied out immediately** after creation and saved locally on the TPP system. The secret is no longer displayed after leaving this page! A new creation of the secret usually entails changes to the used APP. Therefore it is **strongly recommended to save this secret now**". At the bottom right, there are "CANCEL" and "SAVE" buttons.

- Click on the “Create” button



The screenshot shows the "Create secret" form after the "CREATE" button has been clicked. The "Secret" input field now contains a long alphanumeric string: "a631da7b-9e21-4201-ad6c-c4fa83104999". This string is highlighted with a red rectangular box. The "Attention" warning box is still present. At the bottom right, there are "CANCEL" and "SAVE" buttons.

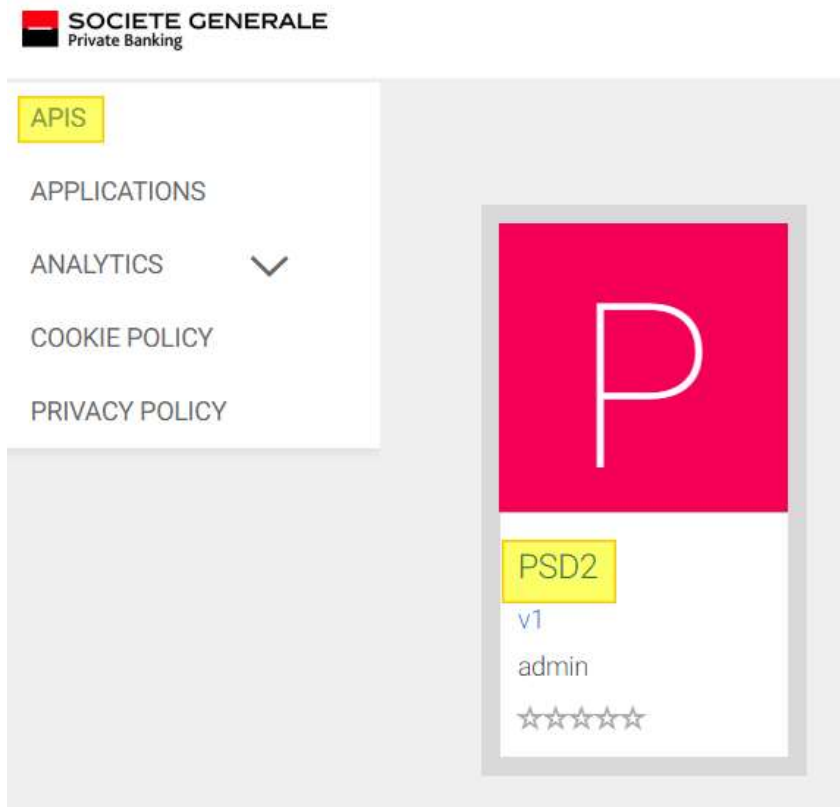
- The secret is created

This secret needs to be stored in a dedicated zone (such as password vault). As it will be used for all consent creation requests, the secret should be stored in a TPP configuration file.

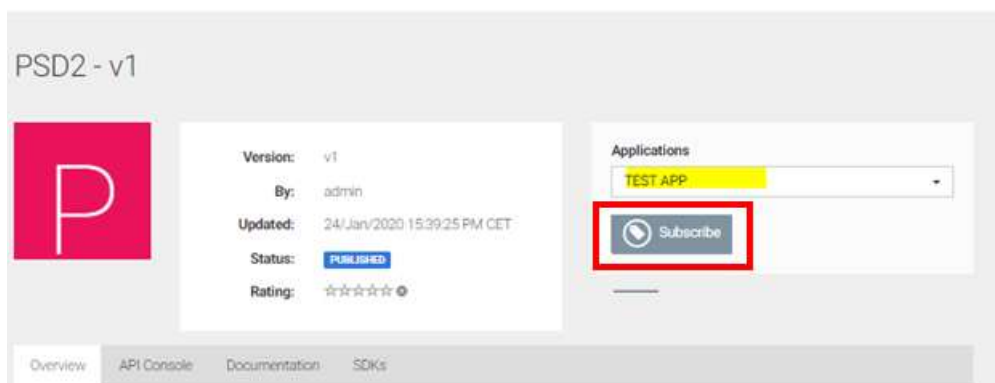
- Click on the “SAVE” button

### 3.8 Subscribe to API

A subscription to the API is mandatory before consuming it. This process also only takes place once. Please click on "APIs" in the left side menu. Then select the PSD2 API by clicking on the colored icon



Select the newly created application and confirm the process with the button "Subscribe".



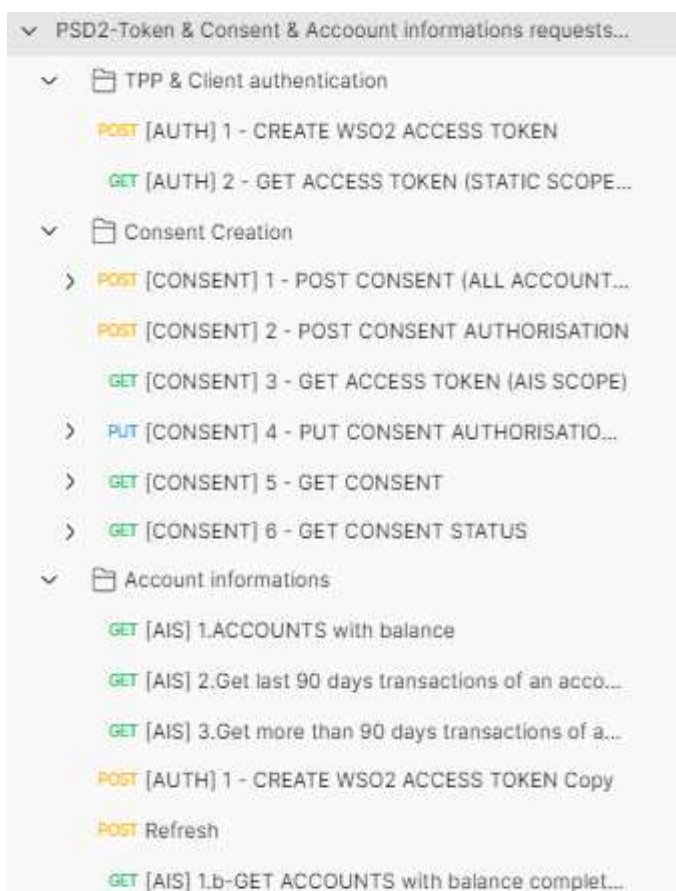
Please close the success message by clicking on the button "Stay on this page".

## 4 Postman collection

In this section it will be described the correspondence of PSD2 API requests with client actions, however, steps 1 and 2 which are managed on the TPP side have no correspondence with API requests.

In the absence of an application with a User Journey adapted to PSD2, the POSTMAN tool was used to perform the tests on the API

On POSTMAN, requests are assembled as a collection which is as follows



VARIABLE	VALUE FOR INT ENV
wso2-url	https://int-api.privatebanking.societegenerale.lu/ebankingPsd2
ASO	https://int-api.privatebanking.societegenerale.lu/ebankingAuthServer/oauth
api_gateway	https://int-api.privatebanking.societegenerale.lu/ebankingPsd2/psd2/v1
tenantId	12

### 4.1 TPP & Client authentication

#### 4.1.1.1 [AUTH] 1 - CREATE WSO2 ACCESS TOKEN

This request allows the API to identify the TPP using the Consumer Key and the Consumer Secret generated in the onboarding process

- **Query type:** POST

- **URL:** {{wso2-url}}/oauth2/token
- **Inputs:**

Field	Section	Value
Username	authorization	<u>wso2-consumer-key</u>
Password	authorization	<u>wso2-consumer-secret</u>
grant_type	Body	client_credentials

- **Action to perform**

Click on **Send** button

The screenshot shows a REST client interface for a POST request to the URL `{{wso2-url}}/oauth2/token`. The request is configured with Basic Auth. The Username field contains `{{wso2-consumer-key(TPP4)}}` and the Password field contains `{{wso2-consumer-secret(TPP4)}}`. The 'Show Password' checkbox is checked. The response is displayed in JSON format:

```

1  {
2    "access_token": "[REDACTED]",
3    "scope": "am_application_scope default",
4    "token_type": "Bearer",
5    "expires_in": 3600
6  }

```

- **Outputs**

Field	Type	Expected Value
Status	Request status	200 OK
access_token	Token	/

#### 4.1.1.2 [AUTH] 2 - GET ACCESS TOKEN (STATIC SCOPES)

This request allows the API to create access token with statistic scope  
Go to authorization Pan

Token Name	<input type="text" value="Enter a token name..."/>
Grant Type	Authorization Code <span style="float: right;">▼</span>
Callback URL <sup>①</sup>	<input type="text" value="{{redirect_uri_tpp}}"/>
	<input type="checkbox"/> Authorize using browser
Auth URL <sup>①</sup>	<input type="text" value="{{ASO}}/{{tenantId}}/oauth/authorize"/>
Access Token URL <sup>①</sup>	<input type="text" value="{{ASO}}/{{tenantId}}/oauth/token"/>
Client ID <sup>①</sup>	<input type="text" value="{{clientIdTPP}}"/>
Client Secret <sup>①</sup>	<input type="text" value="{{clientsecretTPP}}"/>
Scope <sup>①</sup>	<input type="text" value="e.g. read:org"/>
State <sup>①</sup>	<input type="text" value="State"/>
Client Authentication	Send as Basic Auth header <span style="float: right;">▼</span>

 Clear cookies <sup>①</sup>

**Get New Access Token**

Fill the fields as below:

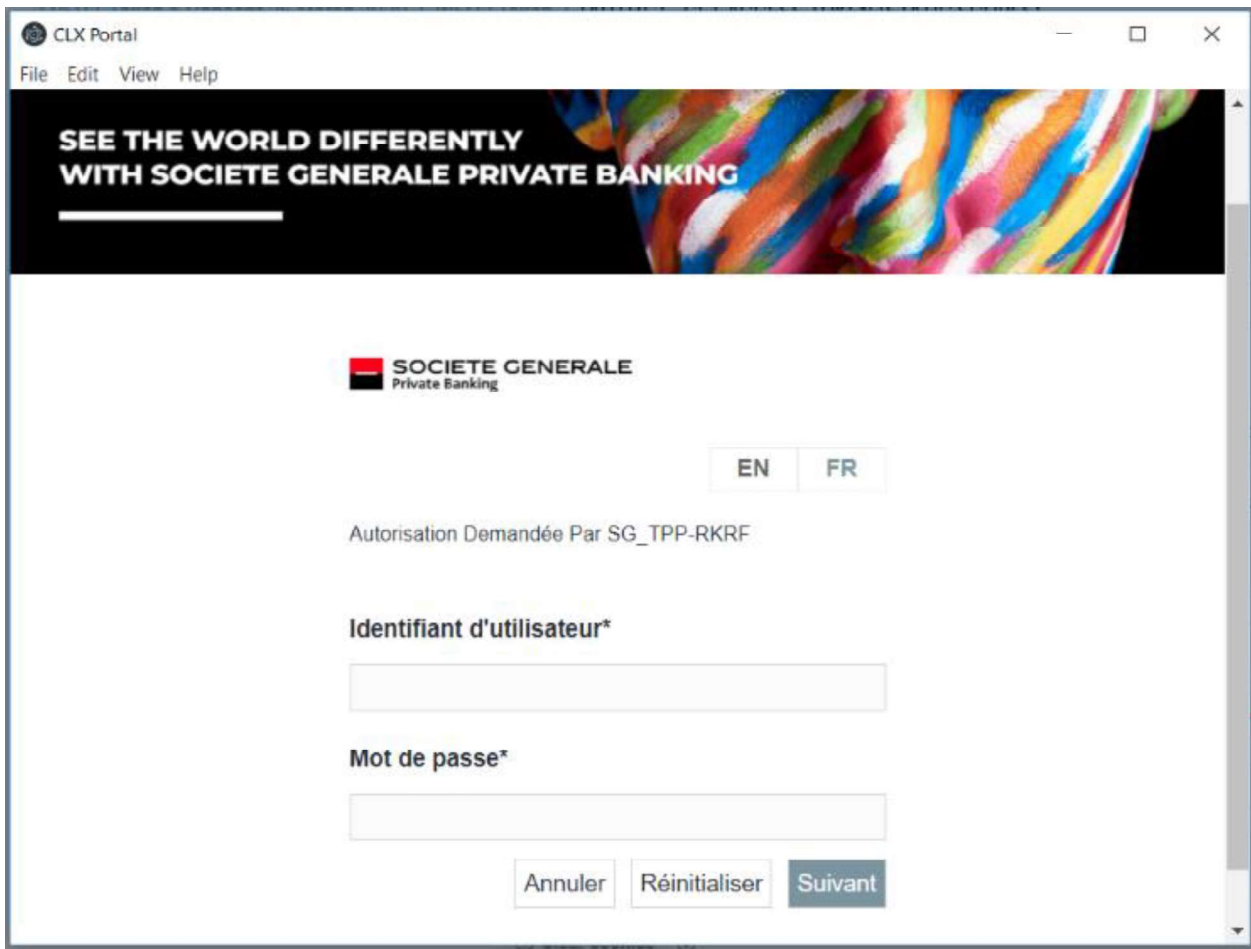
- Inputs:**

Field	Value
Callback URL	<u><a href="#">ADD REDIRECT URL</a></u>
Auth URL	<code>{{ASO}}/{{tenantId}}/oauth/authorize</code>
Access Token URL	<code>{{ASO}}/{{tenantId}}/oauth/token</code>
Client Id	<u><a href="#">clientIdTPP</a></u>
Client secret	<u><a href="#">clientsecretTPP</a></u>

- Action to perform**

Click on **GET NEW ACCESS TOKEN**

The eBanking login page is open,



Perform SCA

- 1<sup>st</sup> factor (contract+Password)
  - **Inputs:**

Field	Value
ContractID	eBanking contractID
Password	eBanking password

- 2<sup>nd</sup> factor (pushTan confirmation)
  - **Inputs:**

Client can use one of the following authentication method

Field	Value
Access_Code	
FingerPrint	If configured
FaceID	If configured

- **Outputs**

The popup with token response is displayed



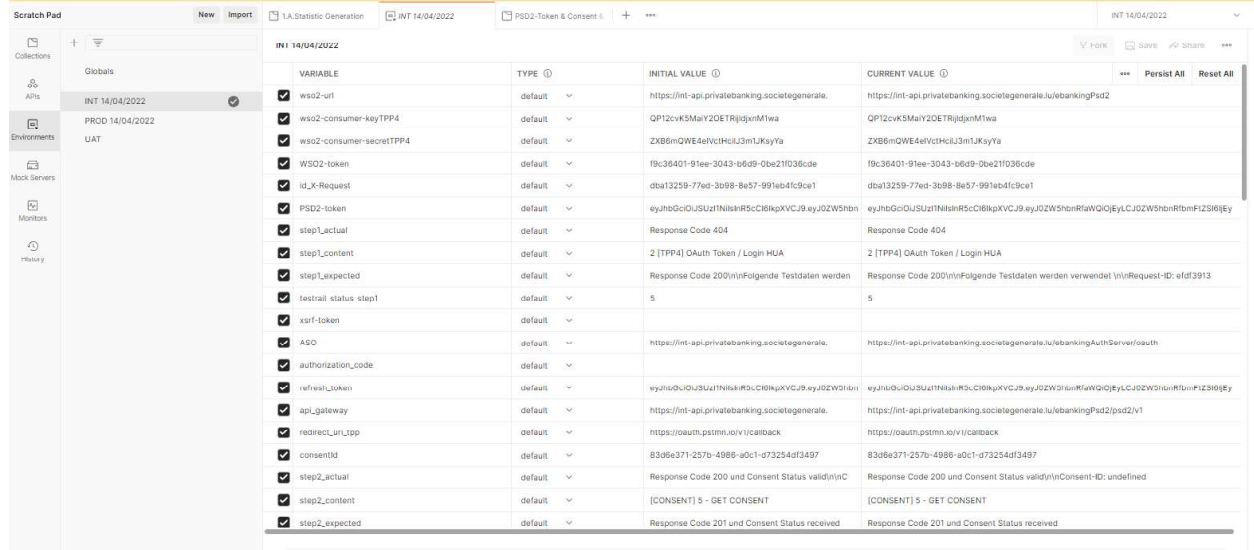


Click on the **USE TOKEN**

Then click on **send** button in postman request

The refresh\_token is not automatically saved

So the value should be copied and saved under the Environment Variable "**refresh\_token**" (CURRENT VALUE column) and click on "Persist All" button and Save.



Field	Type	Expected Value
<a href="#">PSD2-token</a>	Json	
<b>refresh_token</b>	json	

#### 4.1.2 Consent Creation

##### 4.1.2.1 [CONSENT] 1 - POST CONSENT (ALL ACCOUNTS)

- **Query type:** POST
- **URL:** `{{api_gateway}}/v1/consents`
- **Inputs:**

Field	Section	Value
withBalance	Params	True/false
Authorization	Headers	Bearer <code>{{WSO2-token}}</code>
PSD2-AUTHORIZATION	Headers	Bearer <code>{{PSD2-token}}</code>
X-Request-ID	Headers	<code>{{id_X-Request}}</code>
Body	Body	<pre>{   "access": {     "allPsd2": "allAccounts"   },   "recurringIndicator": false,   "validUntil": "2022-12-31",   "frequencyPerDay": 4,   "combinedServiceIndicator": false }</pre>



		}
--	--	---

**validUntil** : should always a future date

- **Action to perform**

Click on **Send** button

- **Outputs**

Field	Type	Expected Value
Status	Status code	201 created
Consent_ID	json	

#### 4.1.2.2 [CONSENT] 2 - POST CONSENT AUTHORISATION

- **Query type:**POST
- **URL:** {{api\_gateway}}/v1/consents/Consent\_ID/authorisations/
- **Inputs:**

Field	Section	Value
Consent-ID	Headers	<u>Consent ID</u>
Authorization	Headers	Bearer {{ <u>WSO2-token</u> }}
PSD2-AUTHORIZATION	Headers	Bearer {{ <u>PSD2-token</u> }}
X-Request-ID	Headers	{{id_X-Request}}

- **Action to perform**

Click on **Send** button

POST `{{(api_gateway)}}/v1/consents/{{(consentId)}}/authorisations/` Send

Params Authorization Headers (15) Body ● Pre-request Script ● Tests ● Settings Cookies

Query Params

KEY	VALUE	DESCRIPTION	...	Bulk Edit
Key	Value	Description		

body Cookies (1) Headers (18) Test Results (2/3) Status: 201 Created Time: 1364 ms Size: 1.39 KB Save Response

Pretty Raw Preview Visualize JSON Copy Search

```

1  {
2    "scaStatus": "failed",
3    "authorisationId": "22eeba75-befa-44c4-8a18-cbf5569b0083",
4    "scaMethods": [],
5    "_links": {
6      "scaStatus": {
7        "href": "/v1/consents/2f647dee-a6c2-49f8-8ee9-d50b9b27b4a1/authorisations/22eeba75-befa-44c4-8a18-cbf5569b0083"
8      },
9      "scaOauth": {
10       "href": "https://api.privatebanking.societegenerale.lu/ebankingAuthServer/oauth/12/oauth/authorize?
           scope=AIS:6f3cca50-5e72-4267-8c94-83b261e51117"
11     }
12   }
13 }

```

• **Outputs**

Field	Type	Expected Value
Status	Status code	201
Datas	Json	See below the json
<a href="#">ais_dynamic_scope</a>		AIS:xxxxxxxx
<a href="#">consent_authorisationId</a>	Json	

4.1.2.3 [CONSENT] 3 - GET ACCESS TOKEN (AIS SCOPE)

This request allows the API to create access token with dynamic scope  
Go to authorization Pan

## Configure New Token

Configuration Options ●

Advanced Options

Token Name	<input type="text" value="Enter a token name..."/>
Grant Type	Authorization Code ▾
Callback URL ⓘ	<input type="text" value="{{redirect_uri_tpp}}"/>
	<input type="checkbox"/> Authorize using browser
Auth URL ⓘ	<input type="text" value="{{ASO}}/{{tenantId}}/oauth/authorize"/>
Access Token URL ⓘ	<input type="text" value="{{ASO}}/{{tenantId}}/oauth/token"/>
Client ID ⓘ	<input type="text" value="{{clientIdTPP}}"/>
Client Secret ⓘ	<input type="text" value="{{clientsecretTPP}}"/>
Scope ⓘ	<input type="text" value="{{ais_dynamic_scope}}"/>
State ⓘ	<input type="text" value="State"/>
Client Authentication	Send as Basic Auth header ▾

Fill the fields as below:

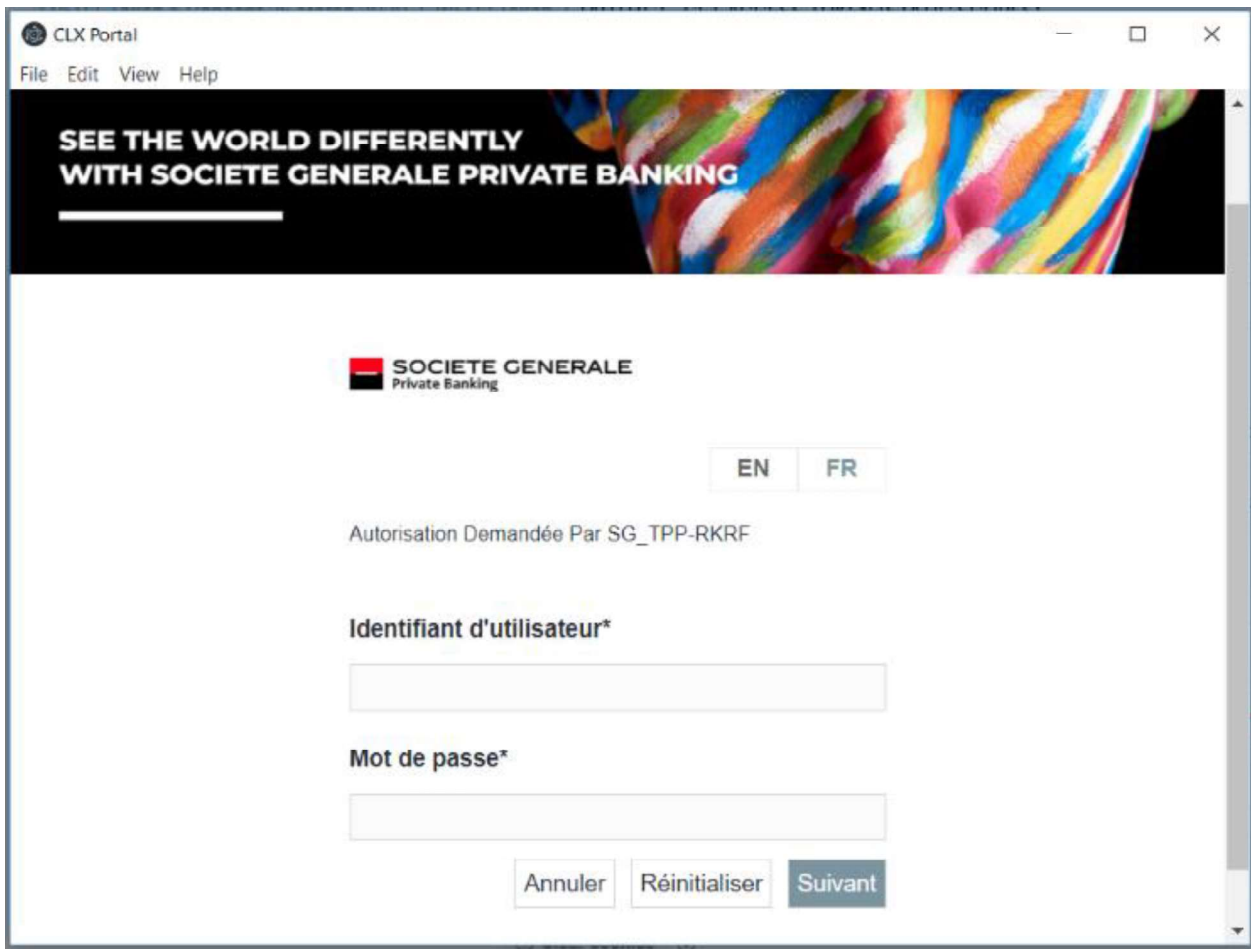
- **Inputs:**

Field	Value
Callback URL	<a href="#">ADD REDIRECT URL</a>
Auth URL	{{ASO}}/{{tenantId}}/oauth/authorize
Access Token URL	{{ASO}}/{{tenantId}}/oauth/token
Client Id	<a href="#">clientIdTPP</a>
Client secret	<a href="#">clientsecretTPP</a>
ais_dynamic_scope	Dynamic scope retrieved in previous step "Post consent authorization" go to <a href="#">here</a>

- **Action to perform**

Click on **GET NEW ACCESS TOKEN**

The eBanking login page is open,



Perform SCA

- 1<sup>st</sup> factor (contract+Password)
  - **Inputs:**

Field	Value
ContractID	eBanking contractID
Password	eBanking password

- 2<sup>nd</sup> factor (pushTan confirmation)
  - **Inputs:**

Client can use one of the following authentication method

Field	Value
Access_Code	
FingerPrint	
FaceID	

- **Outputs**

The popup with token response is displayed



1.PSD2-Token & Consent 26 March 2020 / Consent / [CONSENT] 4 - PUT CONSENT AUTHORISATION (VALIDATION) Save ... 🔗 📄

PUT ▼ `{{api_gateway}}/v1/consents/{{consentId}}/authorisations/{{consent_authorisationId}}` Send ▼

Params Authorization Headers (16) Body ● Pre-request Script Tests Settings Cookies

Query Params

KEY	VALUE	DESCRIPTION	...	Bulk Edit
Key	Value	Description		

---

Body Cookies (1) Headers (18) Test Results Status: 200 OK Time: 1541 ms Size: 1.03 KB Save Response ▼

Pretty Raw Preview Visualize JSON ▼ 🔗 🔍

```

1 |
2 |   "scaStatus": "finalised"
3 |

```

- **Outputs**

Field	Type	Expected Value
Status	Status code	200
scaStatus	Json	Finalized

#### 4.1.2.5 [CONSENT] 5 - GET CONSENT

It allows to check the status and the scope of the consent

- **Query type:** GET
- **URL:** `{{api_gateway}}/v1/consents/{{consentId}}`
- **Inputs:**

Field	Section	Value
withBalance	Params	True/false
<b>Consent-ID</b>	Headers	(see <a href="#">ConsentID</a> )
Authorization	Headers	Bearer <code>{{WSO2-token}}</code>
PSD2-AUTHORIZATION	Headers	Bearer <code>{{PSD2-token}}</code>
X-Request-ID	Headers	<code>{{id_X-Request}}</code>

- **Action to perform**

Click on **Send** button

The screenshot shows a REST client interface with the following details:

- Method:** GET
- URL:** `{{api_gateway}}/v1/consents/{{consentId}}`
- Response Status:** 200 OK, Time: 555 ms, Size: 1.4 / KB
- Response Body (JSON):**

```

1  {
2    "access": {
3      "accounts": [
4        {
5          "iban": "LU900612756733200EUR",
6          "currency": "EUR"
7        },
8        {
9          "iban": "LU750612756733210EUR",
10         "currency": "EUR"
11        }
12       ],
13       "balances": [
14         {
15           "iban": "LU900612756733200EUR",
16           "currency": "EUR"
17         },
18         {
19           "iban": "LU750612756733210EUR",
20           "currency": "EUR"
21         }
22       ]
23     }
24   }

```

• **Outputs**

Field	Type	Expected Value
Status	Status code	200 OK
Response	Json	See the table below

Field	Expected Value
Access	Access scope: List of the contract cash accounts (IBAN+Currency)
Balances	Balances scope: List of the contract cash accounts (IBAN+Currency)
Transactions	Transaction scope: List of the contract cash accounts (IBAN+Currency)
recurringIndicator	false
validUntil	Today <validUntil <Today+90 days
frequencyPerDay	4
consentStatus	valid

4.1.2.6 [CONSENT] 6 - GET CONSENT Status

It allows to check only the status of the consent

- **Query type:** GET
- **URL:** `{{api_gateway}}/v1/consents/{{consentId}}/status`
- **Inputs:**

Field	Section	Value
withBalance	Params	True/false
Consent-ID	Headers	(see <a href="#">ConsentID</a> )
Authorization	Headers	Bearer <code>{{WSO2-token}}</code>
PSD2-AUTHORIZATION	Headers	Bearer <code>{{PSD2-token}}</code>
X-Request-ID	Headers	<code>{{id_X-Request}}</code>

- **Action to perform**

Click on **Send** button

1.PSD2-Token & Consent 26 March 2020 / Consent / [CONSENT] 6 - GET CONSENT STATUS

GET `{{api_gateway}}/v1/consents/{{consentId}}/status` Send

Params Authorization Headers (13) Body Pre-request Script Tests Settings Cookies

Query Params

KEY	VALUE	DESCRIPTION
Key	Value	Description

Body Cookies (1) Headers (18) Test Results (1/1) Status: 200 OK Time: 1370 ms Size: 1.03 KB Save Response

Pretty Raw Preview Visualize JSON

```

1  {
2    "consentStatus": "valid"
3  }

```

- **Outputs**

Field	Type	Expected Value
Status	Status code	200 OK
consentStatus	Json	Valid

#### 4.1.3 Account information

##### 4.1.3.1 [AIS] 1.ACCOUNTS with balance

- **Query type:** GET
- **URL:** <https://int-api.privatebanking.societegenerale.lu/ebankingPsd2/psd2/v1/v1/accounts>
- **Inputs:**

Field	Section	Value
withBalance	Params	<ul style="list-style-type: none"> <li>• <b>true:</b> to retrieve accounts information with balances</li> <li>• <b>false:</b> to retrieve accounts information without balances</li> </ul>
Consent-ID	Headers	(see <a href="#">ConsentID</a> )
Authorization	Headers	Bearer <code>{{WSO2-token}}</code>
PSD2-AUTHORIZATION	Headers	Bearer <code>{{PSD2-token}}</code>
X-Request-ID	Headers	<code>{{id_X-Request}}</code>

- **Action to perform**

Click on **Send** button



GET `{{api_gateway}}/v1/accounts?withBalance=true` Send

Params ● Authorization Headers (14) Body Pre-request Script Tests ● Settings Cookies

Query Params

KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/> withBalance	true			
Key	Value	Description		

Body Cookies (1) Headers (18) Test Results (2/2) Status: 200 OK Time: 1080 ms Size: 1.95 KB Save Response

Pretty Raw Preview Visualize JSON  

```

1  {
2    "accounts": [
3      {
4        "resourceId": "2601d0d5-6fda-4cc3-9ceb-a571600def2e",
5        "iban": "LU900612756733200EUR",
6        "currency": "EUR",
7        "name": "compte perso 2",
8        "cashAccountType": "CACC",
9        "bic": "SGABLULL",
10       "balances": [
11         {
12           "balanceAmount": {
13             "currency": "EUR",
14             "amount": "11.9"
15           }
16         }
17       ],
18       "_links": {
19         "self": {
20           "href": "/v1/accounts/2601d0d5-6fda-4cc3-9ceb-a571600def2e"

```

• **Outputs**

Field	Type	Expected Value
Status	Status code	201
Datas	Json	See below the json

Example

```

{
  "accounts": [
    {
      "resourceId": "fa2a2366-4264-473c-a3bf-df8eb079655d",
      "iban": "LU190615608573380CAD",
      "currency": "CAD",
      "cashAccountType": "CACC",
      "bic": "SGABLULL",
      "balances": [
        {
          "balanceAmount": {
            "currency": "CAD",
            "amount": "0.0"
          }
        }
      ],
      "_links": {
        "self": {
          "href": "/v1/accounts/fa2a2366-4264-473c-a3bf-df8eb079655d"
        },
        "balances": {
          "href": "/v1/accounts/fa2a2366-4264-473c-a3bf-df8eb079655d/balances"
        },
        "transactions": {
          "href": "/v1/accounts/fa2a2366-4264-473c-a3bf-df8eb079655d/transactions"
        }
      }
    }
  ]
}

```

```

    }
  },
  {
    "resourceId": "1d8187b3-933e-4ef6-b033-d4c8155e0367",
    "iban": "LU070615608573380USD",
    "currency": "USD",
    "cashAccountType": "CACC",
    "bic": "SGABLULL",
    "balances": [
      {
        "balanceAmount": {
          "currency": "USD",
          "amount": "39.63"
        }
      }
    ],
    "_links": {
      "self": {
        "href": "/v1/accounts/1d8187b3-933e-4ef6-b033-d4c8155e0367"
      },
      "balances": {
        "href": "/v1/accounts/1d8187b3-933e-4ef6-b033-d4c8155e0367/balances"
      },
      "transactions": {
        "href": "/v1/accounts/1d8187b3-933e-4ef6-b033-d4c8155e0367/transactions"
      }
    }
  }
}

```

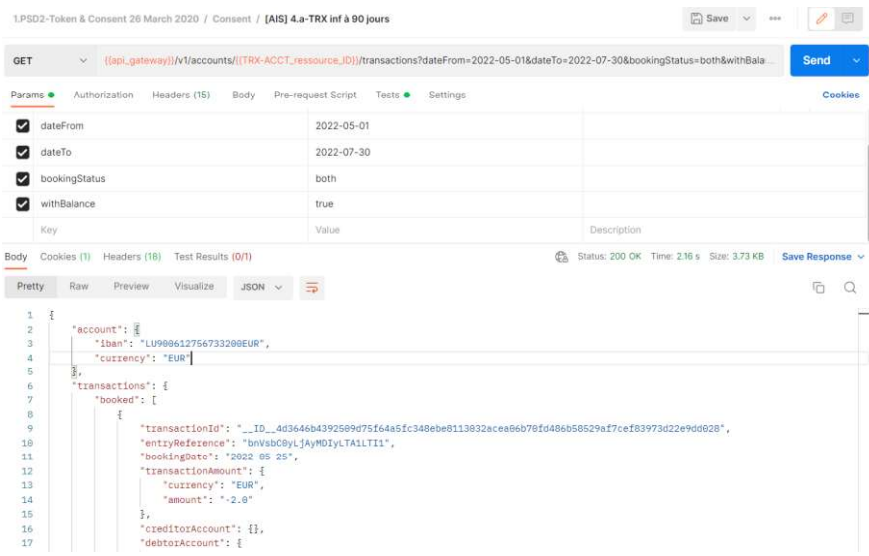
#### 4.1.3.2 [AIS] 2. Get last 90 days transactions of an account

- **Query type:** GET
- **URL:** <https://int-api.privatebanking.societegenerale.lu/ebankingPsd2/psd2/v1/v1/accounts/{{resourceId}}/transactions>
- **Inputs:**

Field	Section	Value
resourceId	URL: ResourceId of the account for which transactions are retrieved	One of resources ID from previous request response (Click to see <a href="#">ResourceID</a> )
dateFrom	Params	Date from to retrieve transactions >=Today-90days
dateTo	Params	Date from to retrieve transactions >= dateFrom
bookingStatus	Params	<b>Both:</b> to retrieve executed and ongoing operations
withBalance	Params	true/false: t0 retrieve or not intermediate balance of account
Consent-ID	Headers	One of resources ID from previous request response (Click to see )
Authorization	Headers	Bearer {{WSO2-token}}
PSD2-AUTHORIZATION	Headers	Bearer {{PSD2-token}}
X-Request-ID	Headers	{{id_X-Request}}

- **Action to perform**

Click on **Send** button



- **Outputs**

Field	Type	Expected Value
Status	Status code	201
Datas	Json	See below the json

#### 4.1.3.3 [AIS] 3. Get more than 90 days transactions of an account

- **Query type:** GET
- **URL:** <https://int-api.privatebanking.societegenerale.lu/ebankingPsd2/psd2/v1/v1/accounts/{{resourceId}}/transactions>
- **Inputs:**

Field	Section	Value
resourceId	URL: ResourceId of the account for which transactions are retrieved	One of resources ID from previous request response
dateFrom	Params	Date from to retrieve transactions < <b>Today-90days</b>
dateTo	Params	Date from to retrieve transactions >= dateFrom
bookingStatus	Params	<b>Both:</b> to retrieve executed and ongoing operations
withBalance	Params	true/false: to retrieve or not intermediate balance of account
Consent-ID	Headers	
Authorization	Headers	Bearer <a href="#">{{WSO2-token}}</a>
PSD2-AUTHORIZATION	Headers	Bearer <a href="#">{{PSD2-token}}</a>
X-Request-ID	Headers	<a href="#">{{id_X-Request}}</a>

- **Action to perform**

Click on **Send** button

- **Outputs**

Field	Type	Expected Value
Status	Status code	401: To retrieve Transactions elder than 90 days ,SCA is required
Datas	Json	See below the json

```

"tppMessages": [
  {
    "category": "ERROR",
    "code": "SERVICE_BLOCKED",
    "path": "/v1/accounts/4e30201f-c14d-487c-9259-ce9f9b2213bc/transactions",
    "text": "Transactions older than 90 days require SCA."
  }
],
"_links": {
  "startAuthorisation": "/v1/consents/TX_f7bb53f3-2dc9-4b21-ba2b-986267015a42/authorisations"
}
}

```

## 4.2 Regenerate tokens

The tokens expire and should be regenerated before relaunching the queries

### 4.2.1 Regenerate Access Token

Go to query: [AUTH] 1 - CREATE WSO2 ACCESS TOKEN and click on "Send" button

- **Query type:** POST
- **URL:** {{wso2-uri}}/oauth2/token
- **Inputs:**

Field	Section	Value
Username	authorization	<a href="#">wso2-consumer-key</a>
Password	authorization	<a href="#">wso2-consumer-secret</a>
grant_type	Body	client_credentials

- **Action to perform**

Click on **Send** button

The screenshot shows a REST client interface with the following details:

- Method:** POST
- URL:** {{wso2-uri}}/oauth2/token
- Auth:** Basic Auth
- Username:** {{wso2-consumer-keyTPP4}}
- Password:** {{wso2-consumer-secretTPP4}}
- Show Password:**
- Status:** 200 OK
- Time:** 5.37 s
- Size:** 625 B
- Response (JSON):**

```

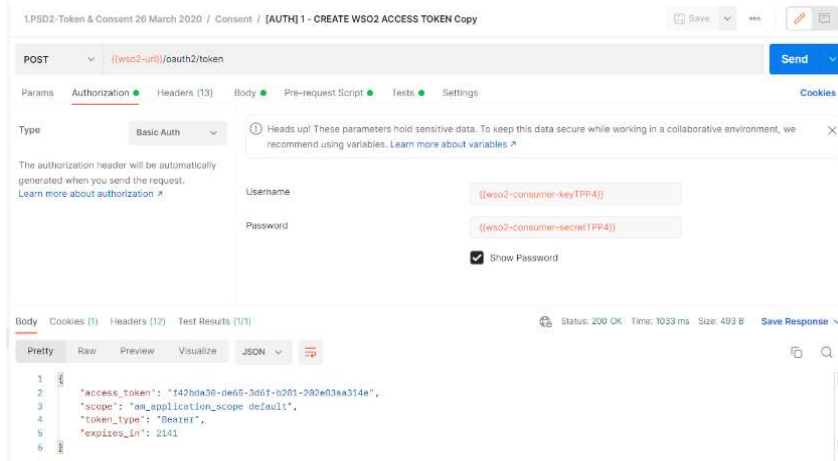
{
  "access_token": "REDACTED",
  "scope": "am_application_scope default",
  "token_type": "Bearer",
  "expires_in": 3600
}

```

- **Outputs**

Field	Type	Expected Value
Status	Request status	200 OK
access_token	Token	/

Example:

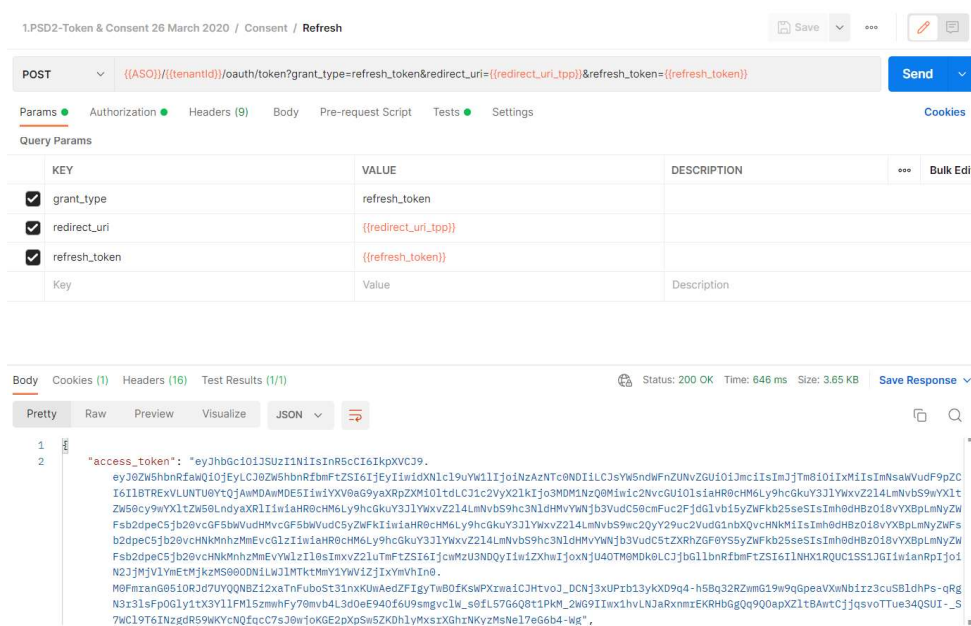


## 4.2.2 Regenerate Refresh Token

Go to query: **REFRESH**

- **Query type:** POST
- **URL:** {{ASO}}/{{tenantId}}/oauth/token?grant\_type=refresh\_token&redirect\_uri={{redirect\_uri\_tpp}}&refresh\_token={{refresh\_token}}
- **Inputs:**

Field	Section	Value
grant_type	Params	'refresh_token'
redirect_uri	Params	<a href="#">redirect_uri_tpp</a>
refresh_token	Params	<a href="#">refresh_token</a>
Username	authorization	<a href="#">wso2-consumer-key</a>
Password	authorization	<a href="#">wso2-consumer-secret</a>



○ **Outputs**

Field	Type	Expected Value
Status	Request status	200 OK
access_token	Token	/
refresh_token	Token	

## 5 References

Description	Hyperlink
Short introduction to PSD2 by Berlin Group Initiative	<a href="https://docs.wix-static.com/ugd/c2914b_c6a8a0dca83e4af8859be266415d3d79.pdf">https://docs.wix-static.com/ugd/c2914b_c6a8a0dca83e4af8859be266415d3d79.pdf</a>
Directive (EU) 2015/2366 of the European parliament and of the council on payment services in the internal market (PSD2) of 25 November 2015	English: <a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366</a>
Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 (RTS document)	<a href="https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2">https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2</a>
Commision delegated regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication	<a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2018:069:TOC">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2018:069:TOC</a>
Consultation on RTS specifying the requirements on strong customer authentication and common and secure communication under PSD2	<a href="https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper">https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper</a>
Discussion on RTS on strong customer authentication and secure communication under PSD2	<a href="https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/discussion-paper">https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/discussion-paper</a>
EBA Fallback document	<a href="https://eba.europa.eu/-/eba-publishes-final-guidelines-on-the-exemption-from-the-fall-back-mechanism-under-the-rt-s-on-sca-and-csc">https://eba.europa.eu/-/eba-publishes-final-guidelines-on-the-exemption-from-the-fall-back-mechanism-under-the-rt-s-on-sca-and-csc</a>
NextGenPSD2 Access to Account Interoperability Framework (Berlin Group Standard) <ul style="list-style-type: none"> <li>• Documentation</li> <li>• Technial documentation / API description</li> <li>• OpenAPI File</li> </ul>	<a href="https://www.berlin-group.org/nextgenpsd2-downloads">https://www.berlin-group.org/nextgenpsd2-downloads</a>
WSO2 API Manager	Description: <a href="https://wso2.com/api-management/">https://wso2.com/api-management/</a>  Documentation: <a href="https://docs.wso2.com/display/AM250/WSO2+API+Manager+Documentation">https://docs.wso2.com/display/AM250/WSO2+API+Manager+Documentation</a>
WSO2 Analytics	<a href="https://docs.wso2.com/display/AM250/Analytics">https://docs.wso2.com/display/AM250/Analytics</a>
WSO2 Admin Guide	<a href="https://docs.wso2.com/display/AM250/Product+Administration">https://docs.wso2.com/display/AM250/Product+Administration</a>

## 6 ANNEXES

### 6.1 Glossary

PSD2 abbreviation	Meaning	Usage
2FA	Two Factor Authentication	
AIS	Account Information Service means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider; according to article 4 (16) of [PSD2] and as regulated by article 67 of [PSD2].	This service may be used by an AISP to request information about the account of a PSU. The account is managed by the ASPSP providing the XS2A Interface. Functionality and restrictions of this service comply with the requirements defined by article 67 of [PSD2].
AISP	Account Information Service Provider means a payment service provider pursuing account information services, according to article 4 (19) and Annex I of [PSD2].	
ASPSP	Account Servicing Payment Service Provider means a payment service provider providing and maintaining a payment account for a payer, according to article 4 (17) of [PSD2]. For example a bank.	
FCS	Fund confirmation service	This service may be used by a PIISP to request a confirmation of the availability of specific funds on the account of a PSU. The account is managed by the ASPSP providing the XS2A Interface. Functionality and restrictions of this service comply with the requirements defined by article 65 of [PSD2].
eIDAS	electronic <b>I</b> dentification, <b>A</b> uthentication and trust <b>S</b> ervices is an EU regulation on electronic identification and trust services for electronic transactions in the internal market. It is a set of standards for electronic identification and trust services for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification and repeals directive 1999/93/EC from 13 December 1999.	
MVP	Minimum Viable Product	Focus on scope in agile development
NA/NCA	National (Competent) Authority. Holds a list of TPPs registered in that particular country.	
PIS	Payment Initiation Service means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider	This service may be used by a PISP to initiate a single payment on behalf of a PSU using a given account of that PSU. The account is managed by the ASPSP



	according to article 4 (15) of [PSD2] and as regulated by article 66 of [PSD2].	providing the XS2A Interface. Functionality and restrictions of this service comply with the requirements defined by article 66 of [PSD2].
PISP	Payment initiation service provider means a payment service provider offering a PIS to its customer, according to article 4 (18) and point (7) of Annex I of [PSD2].	
PIISP	Payment Instrument Issuer Service Provider according to article 4 (14) and 45) of [PSD2]. A PIISP can use the service "Confirmation on the availability of funds" as regulated by article 65 of [PSD2].	
PSU	Payment Service User means a natural or legal person making use of a payment service in the capacity of payer, payee, or both according to article 4 (10) of [PSD2].	
QTSP	Qualified Trust Service Provider, e.g. a trust centre issuing qualified certificates. Luxembourg: LuxTrust S.A.	
SCA	Strong Customer Authentication – authentication procedure based on two factors compliant with the requirements of [PSD2] and [EBA-RTS].	
TPP	Third Party Provider – generic term for AISP/PIISP/PISP.	
TSP/QTSP	Trust Service Provider according to [eIDAS]. Within the context of the XS2A interface specification only qualified TSPs (QTSPs) according to section 3 of [eIDAS] issuing qualified certificates for electronic seals and/or qualified certificates for website authentication which are compliant with the requirements of [EBA-RTS] are relevant.	
XS2A	Access to account interface – interface provided by an ASPSP to TPP for accessing accounts.	
QSealC	Qualified Electronic Seal Certificates	
QWAC	Qualified Website Authentication Certificates	