PSD2 Third Party Registering & Authorising Process Manual SK

Change log

Date of publishing	Version	Date of effectiveness	Description
20.5.2020	1	25.5.2020	Document edit
3.6.2021	2	1.7.2021	In Request body parameters & Response body parameters: (chapters 1. - 3.): email "contact" and other parameters are now mandatory In chapter 6. changed link to bank authorization server (KB SK uses login.kb.cz, where KB has centralized CAAS services)

Differences from the Czech Open Banking Standard are highlighted yellow.

Contents

TPP Authentication

A third party that wishes to use the services defined in PSD2 must obtain a license from a national regulator and an applicable certificate issued for PSD2 services.

To make the authentication successful, a QSEAL-type (electronic seal) or QWAC-type (qualified website authentication certificate) qualified certificates issued by I.CA (or other QTSP from EBA list and which is onboarded by Komerční banka (KB) – must be verified at api@kb.cz) according to ETSI standard must be used for identifying the third-party communicator (also the third party provider, hereinafter TPP).

A precondition for using the PSD2 services in KB is sending an application for connecting to api@kb.cz mailbox, including a public certificate without a private key.

The differences from the previous version of the manual are marked in yellow.

A third party authentication certificate is required on establishing a secured commotion with the bank (ASPSP) using the TLS communication protocol.

Authentication is required for all resources except for the client authorisation – see Chapter *Authorising Resource – Request Characteristics*, which initiates the federated authentication process of KB.

How to proceed when exchanging a PSD2 certificate

When exchanging a PSD2 certificate, you need to register / verify a new certificate (preferably well in advance of the expiration of the original PSD2 certificate to ensure the continuity of consumption of PSD2 services) as follows:

1. A necessary condition for the further use of PSD2 services in KB is that **TPP sends a new PSD2 certificate** to the mailbox api@kb.cz **for manual registration** – i.e. **only the public part of the new PSD2 certificate without the private key**, it is ideal to also communicate the initial validity date of the new certificate or its serial number at the same time.
2. **KB** will then confirm a certificate registration to the TPP from the same email box (api@kb.cz).
3. **TPP** calls with the new certificate the entire AISP / PISP flow (depending on the scope according to the license) and the process of consuming PSD2 services is renewed / continues “seamlessly” (uninterruptedly).
4. Depending on the concurrence of both certificates (existing and new one), TPP can use both certificates simultaneously (during their validity).
5. When using a new certificate does not mean that you have to generate new TPP credentials (clientId, clientSecret, or apiKey).
6. Only in the event that the exchange of PSD2 certificates is not successful, TPP will report KB any errors to the email box api@kb.cz

Error reporting

Reporting production errors or errors within particular calling always takes place via the mailbox api@kb.cz. The e-mail sent must contain the following information, in case the required information is missing, it will not be possible to process the query or error.

The following must be specified:
PSD2 API domain: ***CZ*** *or* ***SK***
Environment: ***Sandbox*** *or* ***Production***
Whether it was called from FE Sandbox, incl. the type and version of the browser used or, in the case of a BE call, the name and version of the program for the BE call
Request type (type of PSD2 service)
Date and time of the call
IP address
The error specification and its most accurate description (incl.. „***x-request-id***“), which can be supplemented with the appropriate screenshot.

Without the above values, it is not possible to solve the reported error and KB may ask you to complete the necessary information (it may prolong the fixing the error).

Registering and Authenticating Resource Issued by the Bank

The client enrolment process that is necessary for understanding the application registering and work with the tokens is described in detail in the Czech open banking standard documentation (specifically in the Chapter “Flow in the Process of the Client Enrolment into the TPP Application”) – Czech Open Banking Standard.

The third party’s application should be registered so that the Payment Initiation Service (PIS) and Account Information Service (AIS) can be used (see the following Chapter).

1. Initializing/Registering – Resource Characteristics

By calling this resource, the TPP asks for the dynamic registration of its application (client_id in the OAuth terminology). A valid certificate should be used to call the resource. The client_id and client_secret parameters are the outputs that the TPP needs to start and go through the user (bank client) authentication process. Komerční banka does not support the API key.

URI: /register
HTTP Method: POST
Request URL: https://api.koba.sk/serverapi/oauth2/v1/register
Authorization: the request **requires** the user/client authorisation as part of the API calling
Certification: the request **requires** the use of the third party qualified certificate.

Supported encoding: `charset=UTF-8`

Request header parameters:

Parameter	Values	Mandatory (yes/no)	Description
Tpp_id	string	y	Registration number of the particular TPP.

Request body parameters:

Parameter	Values	Mandatory (yes/no)	Description
application_type	web, native	y	A type of the application using client_id. The `web` type requires defining the rediect_uris in the web uri format, in the form of http/s scheme. The `native` type allows for inputting e.g. an application package or own format in redirect_uris. ***Note: native is not supported by Komerční banka.***
redirect_uris	Field containing strings, e.g. in the URL format `[Max 3x 2047 B]`	y	A listing of URL to which the flow authentication is redirected in the end. The authorizing request must contain exactly one of those registered URI in a precise format.
client_name	string `[Max 255 B]`	y	The client application name.
client_name#en-US	string `[Max 1024 B]`	n	The client application name in the relevant language or encoding.
logo_uri	URI `[Max 2047 B]`	y	The application logo URI (or the location from which it can be downloaded during registering).
contact	string e-mail `[Max 320 B]`	y	A contact E-mail to a competent person on the side of the client application.
scopes	String field `[Max 10x 255 B]`	y	A field of scopes required by the application. The scopes are validated against the contents of the used certificate during registering. The field is case sensitive with "aisp" and "pisp" being the allowed values.

Example of a request:

```
POST https://api.koba.sk/serverapi/oauth2/v1/register HTTP/1.1
Accept-Encoding: gzip,deflate
x-request-id: 4512345
Content-Type: application/json; charset=UTF-8
Host: api.koba.sk

{
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.sk/start",
      "https://www.mymultibank.sk/start2"],
   "client_name": "Moje_univerzalni_banka",
   "client_name#en-US": "My_cool_bank",
   "logo_uri": "https://www.mybank.sk/logo.png",
   "contact": "info@mybank.sk",
   "scopes": ["aisp","pisp"]
}
```

Response header parameters:

Parameter	Values	Mandatory (yes/no)	Description
Content-Type	String	y	A specification of the required transfer format. Based on the prerequisites of the technical specification of this API standard, in this case the **application/json** format is primarily supported.
x-request-id	String	n	An optional parameter for TPP request / response identification (pairing).

Response body parameters:

Parameter	Values	Mandatory (yes/no)	Description
client_id	string	y	The `client_id` assigned to the application. This ID launches the authentication process and decoded communication during the exchange of the `code` and `refresh_token`.
client_secret	string	y	Client secret – a password/token issued by the bank IDP for the (`client_id`) TPP application.
api_key	string	y	The API key used by the application when communicating with the bank API. If the given bank does not support API keys, the field returns “NOT_PROVIDED”.
application_type	web	y	A type of the application using client_id. The `web` type requires defining the rediect_uris in the web uri format, in the form of http/s scheme.
redirect_uris	Field containing strings, e.g. in the URL format `[Max 3x 2047 B]`	y	A listing of URL to which the flow authentication is redirected in the end. The authorizing request must contain exactly one of those registered URI in a precise format.
client_name	string `[Max 255 B]`	y	The client application name.
client_name#en-US	string `[Max 1024 B]`	y	The client application name in the relevant language or encoding.

logo_uri	URI [Max 2047 B]	y	The application logo URI (or the location from which it can be downloaded during registering).
contact	string e-mail [Max 320 B]	y	A contact E-mail to a competent person on the part of the client application.
scopes	String field [Max 10x 255 B]	y	A field of scopes required by the application. The scopes are validated against the contents of the used certificate during registering.

Example of an error-free response:

```
HTTP/1.1 201 Created
Content-Type: application/json; charset=UTF-8
Accept-Encoding: gzip,deflate
x-request-id: 4512345
Host: api.koba.sk
Conncetion: Keep-Alive
Transfer-Encoding: chunked

{
   "client_id": "Moje_univerzalni_banka-1234",
   "client_secret":
     "AAjkk45sd78ad454gddd8712_4555g5g5g5gg",
   "client_secret_expires_at": 0,
   "api_key": "NOT_PROVIDED",
   "application_type": "web",
   "redirect_uris":
      ["https://www.mymultibank.sk/start",
       "https://www.mymultibank.sk/start2"],
   "client_name": "Moje_univerzalni_banka",
   "client_name#en-US": "My_cool_bank",
   "logo_uri": "https://www.mybank.sk/logo.png",
   "contact": "info@koba.sk",
   "scopes":[
      "pisp",
      "aisp"]
}
```

Error codes:

HTTP Status	Code	Description
400	**invalid_request**	Invalid request. It is missing a mandatory field or its format is inappropriate / invalid.
401	**invalid_client**	Invalid client_id.
401	**unauthorized_client**	The client is not authorised to execute this query.
401	**access_denied**	Access denied by the authorising server.
500, 503	**server_error**	Authorising server error.

2. Information on Application Registering Data – Resource Characteristics

By calling this resource, the TPP may ask for an overview of the registering data related to a particular application. To call the resource, a valid certificate and client_id issued for this TPP should be used. An overview of the registering data is the output.

URI: /register/{client_id}
HTTP Method: GET
Request URL: https://api.koba.sk/serverapi/oauth2/v1/register/{client_id}
Authorization: the request **requires** the user/client authorisation as part of the API calling
Certification: the request **requires** the use of the third party qualified certificate.

Supported encoding: `charset=UTF-8`

Example of a request:

```
GET
https://api.koba.sk/serverapi/oauth2/v1/register/Moje_univerzalni_banka
-1234 HTTP/1.1
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
x-request-id: 112233
Host: api.koba.sk
Connection: Keep-Alive
```

Response parameters:

Parameter	Values	Mandatory (yes/no)	Description
client_id	string	y	The `client_id` assigned to the application. This ID launches the authentication process and decoded communication during the exchange of the `code` and `refresh_token`.
client_secret	string	y	Client secret – a password/token issued by the bank IDP for the (`client_id`) TPP application.
api_key	string	y	The API key used by the application when communicating with the bank API. If the given bank does not support API keys, the field returns “NOT_PROVIDED”.
application_type	web	y	A type of the application using client_id. The `web` type requires defining the rediect_uris in the web uri format, in the form of http/s scheme.
redirect_uris	Field containing strings, e.g. in the URL format	y	A listing of URL to which the flow authentication is redirected in the end. The authorizing request must contain exactly one of those registered URI in a precise format.
client_name	string	y	The client application name.
client_name#en-US	string	y	The client application name in the relevant language or encoding.
logo_uri	URI	y	The application logo URI (or the location from which it can be downloaded during registering).
contact	string e-mail	y	A contact E-mail to a competent person on the part of the client application.
scopes	String field	y	A field of scopes required by the application. The scopes are validated against the contents of the used certificate during registering.

Example of an error-free response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
x-request-id: 112233
Host: api.koba.sk
Accept-Encoding: gzip,deflate
Content-Language: cs
Conncetion: Keep-Alive

{
   "client_id": "Moje_univerzalni_banka-1234",
   "client_secret":
     "AAjkk45sd78ad454gddd8712_4555g5g5g5gg",   "api_key": "NOT_PROVIDED",
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.sk/start",
      "https://www.mymultibank.sk/start2"],
   "client_name": "Moje_univerzalni_banka",
   "client_name#en-US": "My_cool_bank",
   "logo_uri": "https://www.mybank.sk/logo.png",
   "contact": "info@mybank.sk",
   "scopes": ["aisp","pisp"]
}
```

Error codes:

HTTP Status	Code	Description
400	invalid_request	Invalid request. It is missing a mandatory field or its format is inappropriate / invalid.
401	invalid_client	Invalid client_id.
401	unauthorized_client	The client is not authorised to execute this query.
401	access_denied	Access denied by the authorising server.
500, 503	server_error	Authorising server error.

3. Changing the Registering Data – Resource Characteristics

By calling this resource, the TPP may ask for changing the registering data related to a particular application. To call the resource, a valid certificate and client_id issued for this TPP should be used. An overview of the changed data is the output.

URI: /register/{client_id}
HTTP Method: PUT
Request URL: https://api.koba.sk/serverapi/oauth2/v1/register/{client_id}
Authorization: the request **requires** the user/client authorisation as part of the API calling
Certification: the request **requires** the use of the third party qualified certificate.

Supported encoding: `charset=UTF-8`

Request header parameters:

Parameter	Values	Mandatory (yes/no)	Description
client_id	string	y	Registration number of the particular TPP.
x-request-id	String	n	An optional parameter for TPP request / response identification (pairing).

Request body parameters:

Parameter	Values	Mandatory (yes/no)	Description
application_type	web	y	A type of the application using client_id. The `web` type requires defining the redirect_uris in the web uri format, in the form of http/s scheme.
redirect_uris	Field containing strings, e.g. in the URL format `[Max 3x 2047 B]`	y	A listing of URL to which the flow authentication is redirected in the end. The authorizing request must contain exactly one of those registered URI in a precise format.
client_name	string `[Max 255 B]`	y	The client application name.
client_name#en-US	string `[Max 1024 B]`	n	The client application name in the relevant language or encoding.
logo_uri	URI `[Max 2047 B]`	y	The application logo URI (or the location from which it can be downloaded during registering).
contact	string e-mail `[Max 320 B]`	y	A contact E-mail to a competent person on the part of the client application.
scopes	String field `[Max 10x 255 B]`	y	A field of scopes required by the application. The scopes are validated against the contents of the used certificate during registering. **`["aisp","pisp"]`**

Example of a request:

```
POST
https://api.koba.sk/serverapi/oauth2/v1/register/Moje_univerzalni_banka
-1234 HTTP/1.1
Content-Type: application/json;charset=UTF-8
X-request-id: 235144
Host: api.koba.sk
Connection: Keep-Alive
Accept-Encoding: gzip,deflate

{
   "application_type": "web",
   "redirect_uris":
```

```
     ["https://www.mymultibank.sk/start",
      "https://www.mymultibank.sk/start2"],
   "client_name": "Moje_nejlepsi_banka",
   "client_name#en-US": "My_best_bank",
   "logo_uri": "https://www.mybank.sk/logo.png",
   "contact": "info@mybank.sk",
   "scopes": ["aisp"]
}
```

Response header parameters:

Parameter	Values	Mandatory (yes/no)	Description
Content-Type	string	y	A specification of the required transfer format. From the precondition of technical specification of this API standard, in this case, **application/json** format is primarily supported.
x-request-id	String	n	An optional parameter for TPP request / response identification (pairing).

Response body parameters:

Parameter	Values	Mandatory (yes/no)	Description
client_id	ID TPP application	y	A unique identifier of the TPP application issued by the bank, or the bank IDP, e.g., by using the *"0. Initializing/registering resource"*.
application_type	web	y	A type of the application using client_id. The `web` type requires defining the rediect_uris in the web uri format, in the form of http/s scheme.
redirect_uris	Field containing strings, e.g. in the URL format	y	A listing of URL to which the flow authentication is redirected in the end. The authorizing request must contain exactly one of those registered URI in a precise format.
client_name	string	y	The client application name.
client_name#en-US	Arbitrary string	y	The client application name in the relevant language or encoding.
logo_uri	URI	y	The application logo URI (or the location from which it can be downloaded during registering).
contact	string e-mail	y	A contact E-mail to a competent person on the part of the client application.
scopes	String field	y	A field of scopes required by the application. The scopes are validated against the contents of the used certificate during registering.

Example of an error-free response:

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
x-request-id: 235144
Host: api.koba.sk
Accept-Encoding: gzip,deflate
Content-Language: cs
Connection: Keep-Alive

{
 "client_id": " Moje_univerzalni_banka-1234",    "application_type": "web",
   "redirect_uris":
```

```
     ["https://www.mymultibank.sk/start",
      "https://www.mymultibank.sk/start2"],
   "client_name": "Moje_nejlepsi_banka",
   "client_name#en-US": "My_best_bank",
   "logo_uri": "https://www.mybank.sk/logo.png",
   "contact": "info@mybank.sk",
   "scopes": ["aisp"]
}
```

Error codes:

HTTP Status	Code	Description
400	invalid_request	Invalid request. It is missing a mandatory field or its format is inappropriate / invalid.
401	invalid_client	Invalid client_id.
401	unauthorized_client	The client is not authorised to execute this query.
401	access_denied	Access denied by the authorising server.
500, 503	server_error	Authorising server error.
400	invalid_scope	Invalid request scope.
403	insufficient_scope	E.g. insufficient authorisation to use the required scope.
400	invalid_redirect_uri	The value(s) of one or more redirect uris is/are not valid.

4. Deleting the Application – Resource Characteristics

By calling this resource, the TPP may ask for deleting data and access to a particular application. To call the resource, a valid certificate and client_id issued for this TPP should be used. A confirmation of the deletion is the output.

URI: /register/{client_id}
HTTP Method: DELETE
Request URL: https://api.koba.sk/serverapi/oauth2/v1/register/{client_id}
Authorization: the request **requires** the user/client authorisation as part of the API calling
Certification: the request **requires** the use of the third party qualified certificate.

Supported encoding: `charset=UTF-8`

Example of a request:

```
DELETE
https://api.koba.sk/serverapi/oauth2/v1/register/Moje_univerzalni_banka
-1234 HTTP/1.1
Content-Type: application/json;charset=UTF-8
x-request-id:541261
Host: api.koba.sk
Connection: Keep-Alive
Accept-Encoding: gzip,deflate
```

Example of a response:

```
HTTP/1.1 201 Created
x-request-id: 541261
Accept-Encoding: gzip,deflate
Content-Language: cs
Content-Type: application/json;charset=UTF-8
Connection: Keep-Alive
```

Error codes:

HTTP Status	Code	Description
401	invalid_client	Invalid client_id.
401	unauthorized_client	The client is not authorised to execute this query.
401	access_denied	Access denied by the authorising server.
500, 503	server_error	Authorising server error.

5. Requesting a New client_secret – Resource Characteristics

By calling this resource, the TPP may ask for issuing a new client_secret. To call the resource, a valid certificate and client_id issued for this TPP should be used. The previous client_secret will be invalidated by this request.

URI: /register/{client_id}
HTTP Method: POST
Request URL: https://api.koba.sk/serverapi/oauth2/v1/register/{client_id}
Authorization: the request **requires** the user/client authorisation as part of the API calling
Certification: the request **requires** the use of the third party qualified certificate.

Supported encoding: `charset=UTF-8`

Example of a request:

```
POST
https://api.koba.sk/serverapi/oauth2/v1/register/Moje_univerzalni_banka
-1234 HTTP/1.1
Content-Type: application/json;charset=UTF-8
x-request-id: 245687
Host: api.koba.sk
Accept-Encoding: gzip,deflate
Connection: Keep-Alive
```

Response parameters:

Parameter	Values	Mandatory (yes/no)	Description
client_id	string	y	The `client_id` assigned to the application. This ID launches the authentication process and decoded communication during the exchange of the `code` and `refresh_token`.
client_secret	string	y	Client secret – a password/token issued by the bank IDP for the (`client_id`) TPP application.

Example of an error-free request:

```
HTTP/1.1 200 OK
x-request-id: 245687
Host: api.koba.sk
Accept-Encoding: gzip,deflate
Content-Type: application/json;charset=UTF-8
Connection: Keep-Alive

{
   "client_id": " Moje_univerzalni_banka-1234",
   "client_secret": "BBjkk45sd78ad454gddd8712_4555g5g5g5gg"
}
```

Error codes:

HTTP Status	Code	Description
400	invalid_request	Invalid request. It is missing a mandatory field or its format is inappropriate / invalid.
401	invalid_client	Invalid client_id.
401	unauthorized_client	The client is not authorised to execute this query.
401	access_denied	Access denied by the authorising server.
500, 503	server_error	Authorising server error.

6. Authorising Resource – Request Characteristics

The Resource is used for obtaining the user's authorisation code, which is a prerequisite for getting an access token. A third party application can start the authorising process by redirecting its user's web browser to the banks authorisation server (KB SK uses login.kb.cz, where KB has centralized CAAS services). During the authorising process, the user is asked to enter his/her KB SK Internet banking login information. After logging in, a list of authorisations is displayed (specified by the scope, e.g. AISP and/or PISP), for which the user is entitled to grant consents to a third party. If the user allows selected access for an application, he/she will receive a TPP authorisation code as a parameter as part of the redirection to the URL callback (the address specified upon the application registering).

URI: /ssologin
HTTP Method: GET
Request URL: https://login.kb.cz/autfe/ssologin
Authorization: the request **requires** the user/client authorisation as part of the API calling
Certification: the request **does not require** the use of the third party qualified certificate.

Supported encoding: `charset=UTF-8`

Request parameters:

Parameter	Values	Mandatory (yes/no)	Description
response_type	code	y	A mandatory parameter determining the authentication flow that has been used (code grant in this case). In terms of the authentication process it means that a one-time code is expected instead of the access_token as a result of a successful identification and authentication.
client_id	ID TPP application	y	A unique identifier of the TPP application issued by the bank, or the bank IDP, e.g., by using the "*0. Initializing/registering resource"*.
redirect_uri	URL	y	An URL to which the authentication flow is redirected in the end. This URL is already determined while the client_id is issued, and this parameter is validated as part of the authentication against the URL introduced for the client_id on the bank's IDP system. The value should be identical to one of the values introduced by using the "*0. Initializing/registering resource".*
scope	aisp or pisp value	n	A limiting attribute of a required scope (authorisation). For PSD2, it may be the "aisp" or "pisp" roles (case sensitive). If the "scope" attribute is not specified at all, the relevant scope is taken over from the registered application (implicit value). E.g., if the TPP application is a holder of both authorisations, it may limit the scope of its specific transaction to one role (see the example of the request).
state	Arbitrary string	n	Redirect_uri can be supplemented with this parameter when redirected. It conveys information from the application via the authentication flow. (It can also be used for the query request/response pairing.)

Example of a request:

```
GET https://login.kb.cz/autfe/ssologin HTTP/1.1
Host: login.kb.cz
Content-Type: application/x-www-form-urlencoded

client_id=Moje_univerzalni_banka-1234&
redirect_uri=https://www.mymultibank.sk/start&
response_type=code&
scope=aisp&
state=12345678
```

Example of a call performed via the browser command line (only applicable to AISP scope here)
The highlighted values (client_id, redirect_uri) in the link below should be filled in. The scope attribute needs not to be specified at all; the application scope is taken over in full (aisp and pisp). Only one of the values, either “aisp” or “pisp”, can be used to reduce the require length of the scope (multiple values are inadmissible):

https://login.kb.cz/autfe/ssologin?response_type=code&client_id=ADD_client_id&redirect_uri=ADD_redirect_uri&state=12345678&scope=aisp

Response parameters:

Parameter	Description
code	Authorisation code (JWT token type, consisting of 3 parts separated with ‘.’ (i.e. dot)).
state	A state parameter from the TPP request.

Example of an error-free response:

```
content-type: application/x-www-form-urlencoded
date: Wed, 8 Mar 2017 20:56:28 GMT
location: https://www.mymultibank.sk/start?
          code=a200234062baa2ada828bbd33c1f6054&
          state=12345678
status: 302
```

Error codes:

HTTP Status	Code	Description
302	invalid_request	Invalid request. It is missing a mandatory field or its format is inappropriate / invalid.
302	unauthorized_client	The client is not authorised to execute this query.
302	access_denied	Access denied by the authorising server.
500, 503	server_error	Authorising server error.
302	invalid_scope	Invalid request scope.

Example of an error response:

```
HTTP/1.1 302 Found
Location: https://www.mymultibank.com/login?
    error=invalid_request
    &error_description=Unsupported%20response_uri
    &state=login_sk
```

7. Obtaining/Issuing the Token – Request Characteristics

Having received the authorisation code, your application may subsequently swap it for an access token or refresh token.

URI: /token
HTTP Method: POST
Request URL: https://api.koba.sk/serverapi/oauth2/v1/token
Authorization: the request **requires** the user/client authorisation as part of the API calling
Certification: the request **requires** the use of the third party qualified certificate.

Supported encoding: `charset=UTF-8`

Request parameters:

Parameter	Values	Mandatory (yes/no)	Description
code	string	n (mandatory in the case of obtaining the access token)	An authorisation code returned from the original request.
refresh_token	string	n (mandatory in the case of refreshing the access token)	A refresh token string.
grant_type	string	y	Valid values of the authorisation code. Permitted values of authorization_code, refresh_token.
redirect_uri	string	n (mandatory in the case of obtaining the access token)	The authorisation code will be sent to this URL as a parameter. It should be identical to one URL registered during the application registering. By default, the value is set to the first URI that has been configured for the client.
client_id		n (mandatory in the case of obtaining the access token)	The Client_ID is obtained while the application is being registered, TPP application ID.
client_secret	string	n (mandatory in the case of obtaining the access token)	Client secret – password/token issued by the bank IDP for the (`client_id`) TPP application.
x-request-id	String	n	An optional parameter for TPP request / response identification (pairing).

Example of a request:

```
POST https://api.koba.sk/serverapi/oauth2/v1/token HTTP/1.1
Host: api.koba.sk
Content-Type: application/x-www-form-urlencoded
x-request-id: 548795

code=a200234062baa2ada828bbd33c1f6054&
client_id=Moje_univerzalni_banka-1234&
client_secret=BBjkk45sd78ad454gddd8712_4555g5g5g5gg&
redirect_uri=https://www.mymultibank.sk/start&
grant_type=authorization_code
```

Response parameters:

Parameter	Values	Mandatory (yes/no)	Description
token_type	string	y	The inputted token type. The value does not distinguish between capital and lower-case letters. An example of the token type: “Bearer”
access_token	string	y	An access token issued by the authorising server.
refresh_token	string	n	Refresh tokens are authorisations used for obtaining new access tokens after they have been authorised.
expires_in	integer($int64)	y	A life time of the access token expressed in seconds.
scope	string	y	Scope of the issued JWT token, e.g. aisp, pisp

Example of an error-free response:
A successfully processed request generates a response with the JSON payload defined as follows:

```
{
   "scope": "aisp pisp",
   "expires_in": 3600,
   "token_type": "Bearer",
   "access_token": "ae9eef9b0af42c674d0b1c1128c37c2d"
   "refresh_token": "be9eef9b0af42c674d0b1c1128c37c2g"
}
```

Error codes:

HTTP Status	Code	Description
400	invalid_request invalid_client invalid_grant unauthorized_client	Invalid request. It is missing a mandatory field or its format is inappropriate / invalid. Invalid client (user). Invalid grant (authorisation). The client (user) is not entitled to use the authorisation type.
401	Access_denied	Access denied.
403	Forbidden	The client is not authorised to execute this query.
404	Not found	The entered query has not been found.
429	Too many requests	The system capacity has been exceeded by inputting too many requests.
500	Internal server error	Server error.

8. Invalidating the Token – Request Characteristics

The API invalidating the refresh token.

URI: /revoke
HTTP Method: POST
Request URL: https://api.koba.sk/serverapi/oauth2/v1/revoke
Authorization: the request **requires** the user/client authorisation as part of the API calling
Certification: the request **requires** the use of the third party qualified certificate.

Supported encoding: `charset=UTF-8`

Request parameters:

Parameter	Description
token	OAuth2 refresh token obtained during the authentication process after its exchange (swap) for the code.

Example of a request:

```
POST https://api.koba.sk/serverapi/oauth2/v1/revoke HTTP/1.1
Host: api.koba.sk
x-request-id: 897145
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

token=be9eef9b0af42c674d0b1c1128c37c2g&client_id=Moje_univerzalni_banka-1234&
client_secret=BBjkk45sd78ad454gddd8712_4555g5g5g5g
```

Error codes:

HTTP Status	Code	Description
302	Invalid_request Invalid_client Access_denied	Invalid request or invalid client; access denied.
400	invalid_request Invalid_client TODO validations with CAAS, taken over	Invalid request. It is missing a mandatory field or its format is inappropriate / invalid.
401	Invalid_grant Invalid_token	Invalid client, invalid grant, or invalid token.
403	Forbidden	The client is not authorised to execute this query.
404	Not found	The entered query has not been found.
429	Too many requests	The system capacity has been exceeded by inputting too many requests.
500	Internal server error	Server error.