

Sandbox příručka API OAUTH2

Change log

Date	Version	Description
10.02.2020	7	Oprava chybně uvedeného hesla v Přihlášení
26.02.2020	8	Aktualizace dokumentu a printscreenů
22.05.2020	9	Úprava dokumentu
09.03.2021	10	Odstranění varianty přímého volání (vybraných resource) - pro registraci, změnu nebo smazání aplikace, vč. požadavku na client secret prostřednictvím přímého volání - tj. odstranění podkapitol 2.1 až 2.5 ve srovnání s předchozí verzí dokumentu č. 9 a přečíslování zbývajících podkapitol v kapitole 2.
30.05.2024	11	Doplnění úpravy odkazu na identity server v rámci 1 SCA flow na straně 10.
20.08.2024	12	Úprava příručky (zejména aktualizace printscreenů) pro nový API store – nové prostředí pro klienty.
06.03.2025	13	Úprava příručky z důvodu změny funkcionality a designu webu

Obsah

Sandbox příručka	1
API OAuth2.....	1
Hlášení chyb	4
1 Stažení a import certifikátu pro sandbox	4
2 Postup vygenerování authorization_code a access/refresh_token pro aplikaci.....	5
3 Revoke token	11
4 Postup přístupu do aplikace přes přímé volání.....	13
4.1 Charakteristika requestu Získání/vystavení tokenu.....	13
4.2 Charakteristika requestu Zneplatnění tokenu.....	17

Hlášení chyb

Hlášení chyb Sandboxu nebo jeho volání probíhá vždy pomocí emailové schránky api@kb.cz. Odeslaný email musí obsahovat níže uvedené náležitosti. V případě chybějící požadované informace nebude možné dotaz nebo chybu zpracovat.

PSD2 API: CZ, SK

Prostředí: Sandbox, Produkce

Zda bylo voláno z FE Sandbox vč. typu a verze použitého prohlížeče nebo v případě BE volání název a verzi programu pro BE volání

Typ volání

Datum a čas uskutečněného volání

IP adresu

Chybu a její co nejpřesnější popis, který může být doplněn o příslušný otisk obrazovky

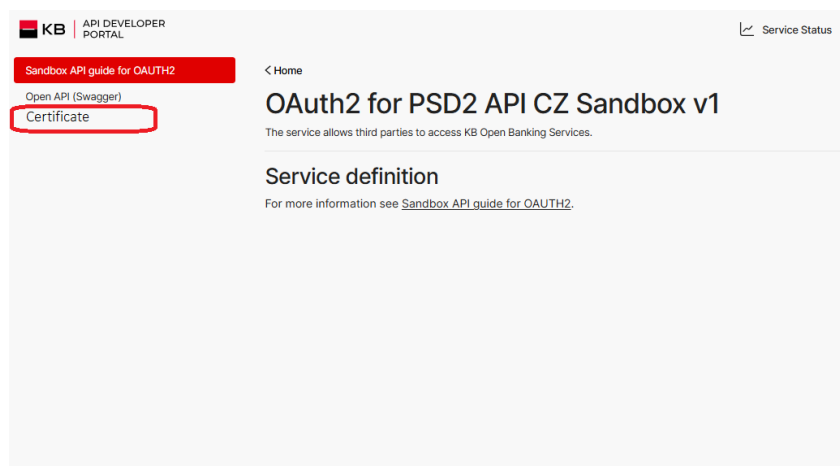
Bez výše uvedených hodnot se není možné hlášenou chybou zabývat.

1 Stažení a import certifikátu pro sandbox

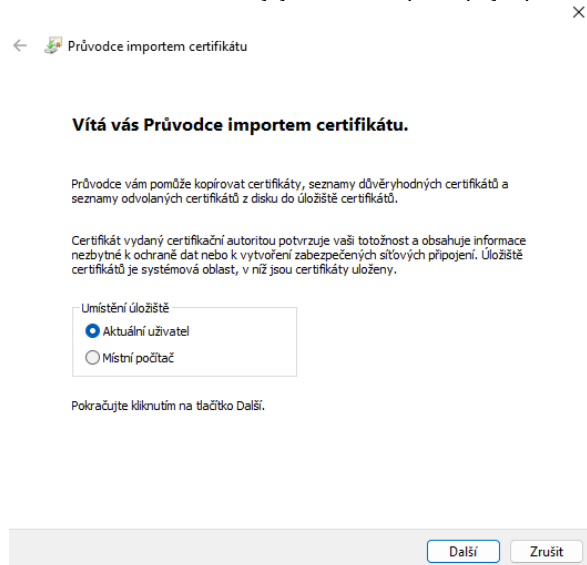
Pro provolání endpointů je potřeba mít stažený a podepsaný certifikát pro sandbox.

Prerekvizita pro stažení certifikátu je být zaregistrován a přihlášen na developerském portálu (bez přihlášení není viditelná možnost stažení certifikátu)

Certifikát ke stažení a heslo k němu je přístupné na developerském portálu po kliknutí na "Certificate" možnost v menu dev portálu:



Po stažení certifikátu si jej otevřete a postupujete podle průvodce pro úspěšný import certifikátu:



2 Postup vygenerování authorization_code a access/refresh_token pro aplikaci

Je potřeba vygenerovat kód (authorization code), který je potřebný pro následné vygenerování access/refresh tokenů. Kód si vygenerujete pomocí odkazu: https://api-gateway.kb.cz/sandbox/oauth2-authorization-ui/v3/?response_type=code&client_id=ExampleClient-6303&redirect_uri=http://kb.cz/&scope=aisp%20pisp&state=xyz

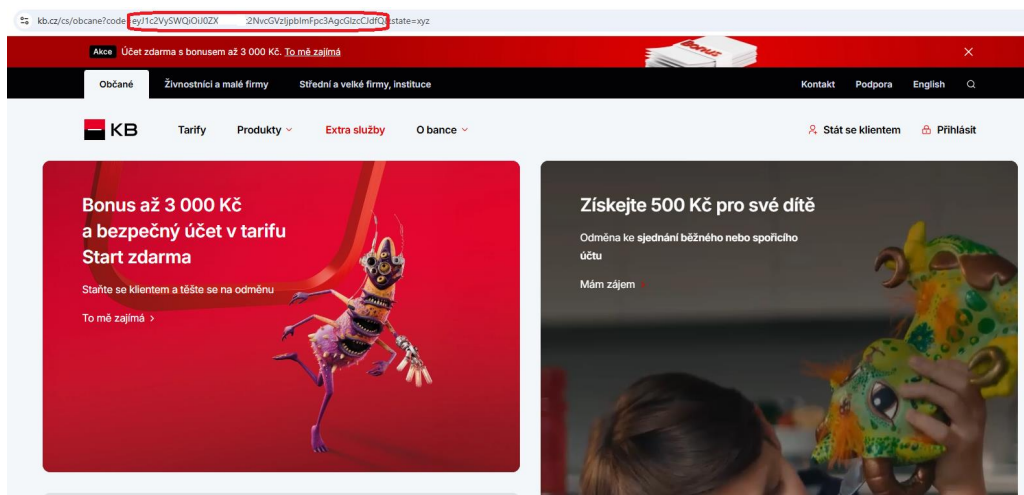
Po otevření odkazu napište například název vašeho testovacího klienta a stiskněte „Generate authorization code“:

Client authentication – test version

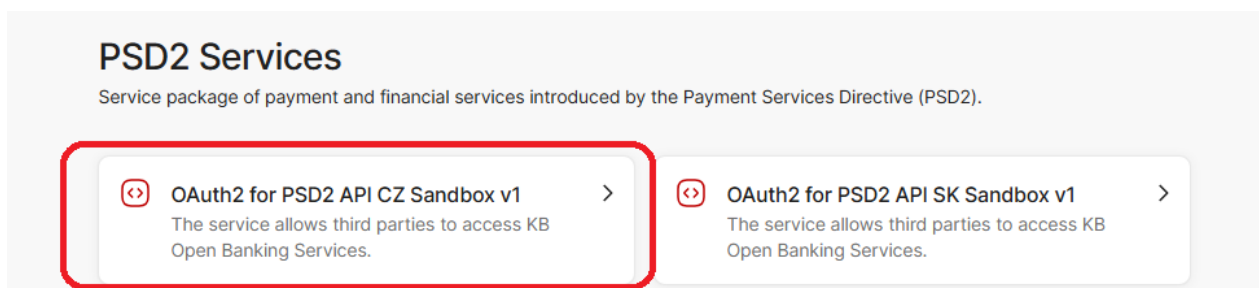
Note: This is a test page for the sandbox API. The authorization code is generated from the entered data (name of a test client). Use the authorization code in related API services (see the sandbox manual of related API services).

Generate authorization code

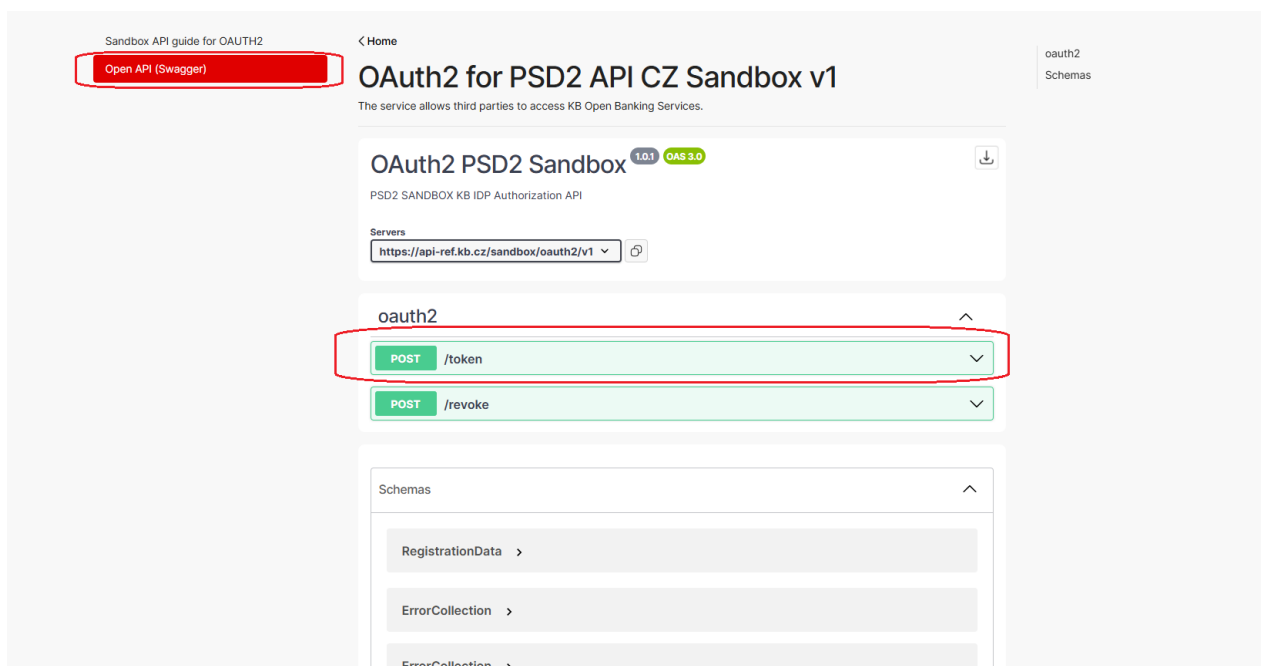
Po stisku „Generate authorization code“ se Vám zobrazí web kb.cz, ale vás zajímá url. Odtud zkopírujte kód, který je ohraničen zleva "code=" a zprava "&state" (tohle ohraničení nekopírujte). Zkopírovaný kód si uložte.



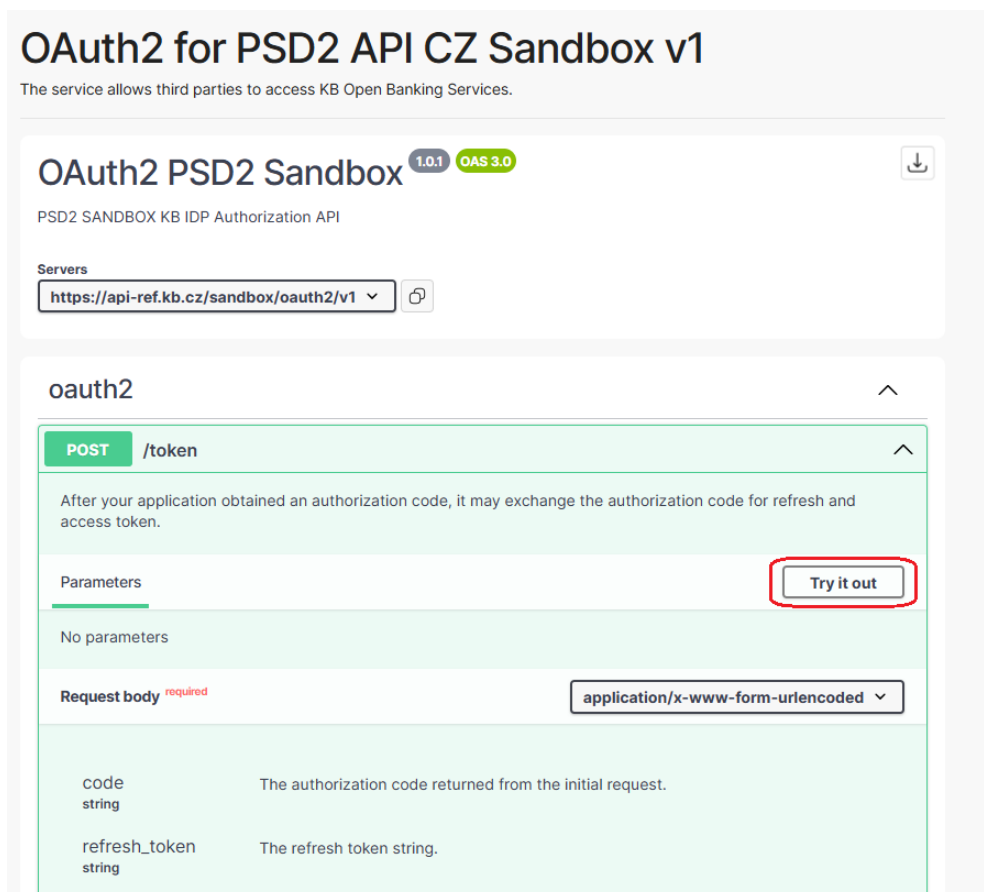
Vraťte se na hlavní stránku developerského portálu a přejděte na sekci pro PSD2. Otevřete si OAuth2 for PSD2 API CZ Sandbox v1.



V levé části obrazovky stiskněte „OPEN API (Swagger)“ a poté na /token endpoint:



Stiskněte „Try it out“:



Vyplňte pole code hodnotou, kterou jste zkopírovali z url (authorization code) a potom stiskněte „Execute“.

POST /token

After your application obtained an authorization code, it may exchange the authorization code for refresh and access token.

Parameters Cancel Reset

No parameters

Request body required application/x-www-form-urlencoded

code string The authorization code returned from the initial request.
eyJ1c2VySWQlOIJUR. ic2NvcGVzljpbmFp
☐ Send empty value

refresh_token string The refresh token string.
string
☐ Send empty value

grant_type required string Valid values: authorization_code.
authorization_code

redirect_uri string The authorization code will be sent to this callback URL as a parameter. It must match one of the URLs registered during application registration. The value defaults to the first redirect URI configured for the client.
string
☐ Send empty value

client_id string The client ID obtained during application registration.
string
☐ Send empty value

client_secret string The client application secret.
string
☐ Send empty value

Execute

Po stisku tlačítka „Execute“ vás systém požádá o výběr certifikátu. Vyberte příslušný certifikát a stiskněte „OK“

Vyberte certifikát

Vyberte certifikát pro ověření na serveru api-ref.kb.cz:443

Předmět	Vydavatel	Sériové číslo
Vase Pokladna	Test CA KB 2	

Informace o certifikátu OK Zrušit

Chcete této aplikaci povolit přístup ke svému privátnímu klíči?

Popis klíče : Privátní klíč CryptoAPI



Povolit

Nepovolovat

[illegible]

Vygenerovaný access token a refresh token si zkopírujte a uložte.

V případě, že došlo k nějaké chybě (například neplatný authorization code), dostanete v odpovědi jednu z možných error hlášek (s kódem: 400, 401, 403, 404, ...), které jsou znázorněny ve swaggeru v části Responses

Responses		
Code	Description	Links
200	OK	No links
Media type		
application/json		
Controls Accept header.		
Example Value Schema		
<pre>{ "token_type": "string", "access_token": "string", "refresh_token": "string", "expires_in": 0, "acr": 0 }</pre>		
400	Invalid_request Invalid_scope	No links
Media type		
application/json		
Example Value Schema		
<pre>{ "errors": [{ "error": "ERR_CODE_400" }] }</pre>		
401	Unauthorized_client Access_denied	No links
Media type		
application/json		
Example Value Schema		
<pre>{ "errors": [{ "error": "ERR_CODE_401" }] }</pre>		

Vygenerovaný access token a refresh token mají obou platnost 1 hodinu.

Pro obnovení access tokenu je třeba mít splněn bod 2 – vygenerování access token. Při vygenerování access token vám vygeneruje zároveň i refresh token. Ten slouží k obnovení platnosti access tokenu.

Endpoint pro obnovení access tokenu je stejný jako ten použitý pro jeho vygenerování:

Sandbox API guide for OAUTH2
Open API (Swagger)

Home
OAuth2 for PSD2 API CZ Sandbox v1
The service allows third parties to access KB Open Banking Services.

oauth2
Schemas

OAuth2 PSD2 Sandbox 1.0.1 OAS 3.0

PSD2 SANDBOX KB IDP Authorization API

Servers
https://api-ref.kb.cz/sandbox/oauth2/v1

oauth2

POST /token

POST /revoke

- Do pole refresh_token vložte refresh token
- Rozklikněte parametr grant_type a zvolte možnost refresh_token

oauth2

POST

/token

After your application obtained an authorization code, it may exchange the authorization code for refresh and access token.

Parameters

CancelReset

No parameters

Request body required

application/x-www-form-urlencoded

code
string

The authorization code returned from the initial request.

☒ Send empty value

refresh_token
string

The refresh token string.

☐ Send empty value

grant_type * required
string

Valid values: authorization_code,
refresh_token
authorization_code
refresh_token

redirect_uri
string

To this callback URL as a parameter. It must
during application registration. The value defaults
to the first redirect URI configured for the client.

☐ Send empty value

client_id
string

The client ID obtained during application registration.

☐ Send empty value

Stiskněte tlačítko „Execute“.

V případě, že refresh token byl validní, tak dostanete odpověď 200, která bude obsahovat obnovený access token.

[illegible]

Pokud nastane nějaká chyba nebo jste vyplnili nesprávný nebo neplatný refresh token, v odpovědi dostanete jednu z error hlášek, jejich vzor je ukázán ve swagger:

Code	Description	Links
200	OK	No links
Media type application/json		
Controls Accept header.		
Example Value Schema		
<pre>{ "token_type": "string", "access_token": "string", "refresh_token": "string", "expires_in": 0, "acr": 0 }</pre>		
400	Invalid_request Invalid_scope	No links
Media type application/json		
Example Value Schema		
<pre>{ "errors": [{ "error": "ERR_CODE_400" }] }</pre>		
401	Unauthorized_client Access_denied	No links
Media type application/json		
Example Value Schema		

3 Revoke token

Revoke token slouží ke zrušení platnosti refresh tokenu. To znamená, že pokud provedete na validní a platný refresh token endpoint revoke, následně již nebude refresh token platný a nebude se moci použít k vytvoření nového access tokenu.

Pro provedení revoke nad refresh tokenem zvolte endpoint revoke:

Sandbox API guide for OAUTH2

Open API (Swagger)

OAuth2 for PSD2 API CZ Sandbox v1

The service allows third parties to access KB Open Banking Services.

OAuth2 PSD2 Sandbox 1.0.1 OAS 3.0

PSD2 SANDBOX KB IDP Authorization API

Servers

https://api-ref.kb.cz/sandbox/oauth2/v1

oauth2

POST /token

POST /revoke

- Vyplňte pole token: vložte validní a platný refresh token
- Stiskněte „Execute“

POST /revoke

The API to revoke refresh token and/or access token.

Parameters

No parameters

Request body **required** application/x-www-form-urlencoded

token * **required** string The value of refresh or access token.
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdV

client_id * **required** string The client ID obtained during application registration.
string

client_secret * **required** string The client application secret.
string

Execute Clear

V případě že jste vložili validní a platný refresh token tak v odpovědi obdržíte response 204 (OK) - tato odpověď neobsahuje žádnou dodatečnou zprávu v response body.
Refresh token již nebude možné použít k obnově access tokenu.

Responses

Curl

```
curl -X 'POST' \
  'https://api-ref.kb.cz/sandbox/oauth2/v1/revoke' \
  -H 'accept: */*' \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -d 'token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdV'
```

Request URL

https://api-ref.kb.cz/sandbox/oauth2/v1/revoke

Server response

Code	Details
204	Response headers <pre>cache-control: no-cache,no-store,max-age=0,must-revalidate,no-store expires: 0 pragma: no-cache</pre>

V případě že nastala nějaká chyba nebo byl vložen nesprávný/neplatný refresh token, v odpovědi dostanete error hlášku. Jejich vzor je ukázán ve swagger:

Responses		
Code	Description	Links
204	OK Media type Controls Accept header.	No links
302	Invalid_request Invalid_client Access_denied Media type	No links
400	Invalid_request Invalid_scope Media type application/json Example Value Schema <pre>{ "errors": [{ "error": "ERR_CODE_400" }] }</pre>	No links
401	Unauthorized_client Access_denied Media type application/json Example Value Schema <pre>{ "errors": [{ "error": "ERR_CODE_401" }] }</pre>	No links
403	Forbidden_Insufficient_scope Media type application/json	No links



4 Postup přístupu do aplikace přes přímé volání

4.1 Charakteristika requestu Získání/vystavení tokenu

Je potřeba vygenerovat autorizační kód (authorization code), který je potřebný pro následné vygenerování access/refresh rokenů.

Kód si vygenerujete pomocí odkazu: https://api-gateway.kb.cz/sandbox/oauth2-authorization-ui/v3/?response_type=code&client_id=ExampleClient-6303&redirect_uri=http://kb.cz/&scope=aisp%20pisp&state=xyz

Po otevření odkazu napište například název vašeho testovacího klienta a stiskněte „Generate authorization code“

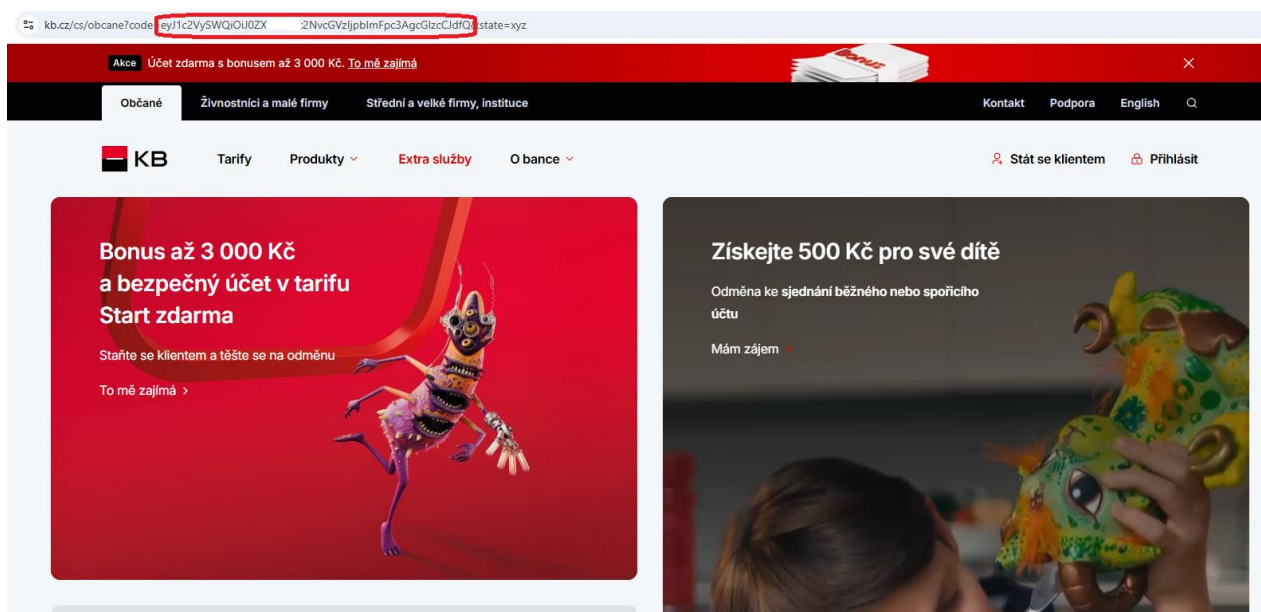
Client authentication – test version

Note: This is a test page for the sandbox API. The authorization code is generated from the entered data (name of a test client).
Use the authorization code in related API services (see the sandbox manual of related API services).

Enter name of test client (i.e. Klient 1)

Generate authorization code

Po stisku „Generate authorization code“ se Vám zobrazí web kb.cz, ale vás zajímá url. Odtud zkopírujte kód, který je ohraničen zleva "code=" a zprava "&state" (tohle ohraničení nekopírujte). Zkopírovaný kód si uložte.



URI: /token
 HTTP Metoda: POST
 Request URL: <https://api.kb.cz/sandbox/oauth2/v1/token>
 Certification: request **vyžaduje** použití kvalifikovaného certifikátu třetí strany.

Podporované kódování: charset=UTF-8

Parametry requestu:

Parametr	Hodnoty	Povinný	Popis
code	string	n (pokud se jedná o získání access tokenu pak je povinný)	Vygenerovaný authorization code
refresh_token	string	n (pokud se jedná o obnovení access tokenu pak je povinný)	Řetězec refrešovacího tokenu..
grant_type	string	y	Validní hodnoty autorizačního kódu Povolené hodnoty : authorization_code, refresh_token
redirect_uri	string	n (pokud se jedná o získání access tokenu pak je povinný)	Autorizační kód bude zaslán na toto URL jako parametr. Musí se shodovat s jedním URL zaregistrovaným během registrace aplikace. Hodnota je defaultně nastavena na první URI, které bylo klientovi nakonfigurováno.
client_id		n (pokud se jedná o získání access tokenu pak je povinný)	Client_ID je získáno během registrace aplikace, ID aplikace TPP.

		je povinný)	
client_secret	string	n (pokud se jedná o získání access tokenu pak je povinný)	Client secret - password/token vydaný IDP banky/bance pro aplikaci (<code>client_id</code>) TPP

Příklad requestu:

```
POST /oauth2/token HTTP/1.1
Host: idp.banka.cz
Content-Type: application/x-www-form-urlencoded

code=a200234062baa2ada828bbd33c1f6054&
client_id=MyPFM&
client_secret={client_secret}&
redirect_uri=https://www.mypfm.cz/start&
grant_type=authorization_code
```

Parametry response:

Parametr	Hodnoty	Povinný	Popis
token_type	string	y	Typ zadaného tokenu. Hodnota nerozlišuje velká písmena. Typ tokenu například "Bearer"
access_token	string	y	Přístupový token vydaný autorizačním serverem.
refresh_token	string	n	Refreshovací tokeny jsou pověřeni užívaná k obstarání nových přístupových tokenů když už byly autorizovány.
expires_in	integer(\$int64)	y	Životnost přístupového tokenu, uvádí se v sekundách.
acr	integer(\$int64)	n	Úroveň zabezpečení autentizace. Nabývá hodnot 0 až 4. Default 3. Hodnota „0“ znamená nonSCA.

Příklad response bez chyby:

Úspěšně zpracovaný request odpoví response s takto definovaným JSON payloadem:

```
{
  "expires_in": 3600,
  "token_type": "Bearer",
  "access_token": "ae9eef9b0af42c674d0b1c1128c37c2d",
  "refresh_token": "be9eef9b0af42c674d0b1c1128c37c2g",
  "acr": "0"
}
```

Chybové kódy:

HTTP Status	Kód	Popis
400	invalid_request	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu.
401	Unauthorized_client Access_denied	Chybná autorizace na straně klienta, přístup odepřen
403	Forbidden	Klient není oprávněný provádět tento dotaz.
404	Not found	Zadaný dotaz se nepodařilo najít
429	Too many requests	Kapacita systému byla překročena zadáním přílišného množství requestů.
500	Internal server error	Chyba serveru

4.2 Charakteristika requestu Zneplatnění tokenu

API sloužící ke zrušení platnosti refresh nebo access tokenu.

URI: /revoke
 HTTP Metoda: POST
 Request URL: <https://api.kb.cz/sandbox/oauth2/v1/revoke>
 Certification: request **vyžaduje** použití kvalifikovaného certifikátu třetí strany.

Podporované kódování: charset=UTF-8

Parametry requestu:

Parametr	Popis
token	OAuth2 access nebo refresh token získaný na základě autentizačního procesu po výměně za code resp. refresh token (v případě access_tokenu)

Příklad requestu:

```
POST /oauth2/revoke HTTP/1.1
Host: idp.banka.cz
Content-Type: application/x-www-form-urlencoded

token=be9eef9b0af42c674d0b1c1128c37c2g
```

Chybové kódy:

HTTP Status	Kód	Popis
302	Invalid_request Invalid_client Access_denied	Nevalidní request nebo nevalidní klient, přístup odepřen.
400	invalid_request	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu.
401	Invalid_client Invalid_grant Invalid_token	Nevalidní klient, nevalidní oprávnění nebo nevalidní token.
403	Forbidden	Klient není oprávněný provádět tento dotaz.
404	Not found	Zadaný dotaz se nepodařilo najít
429	Too many requests	Kapacita systému byla překročena zadáním přílišného množství requestů.
500	Internal server error	Chyba serveru