NA PARTNERSTVÍ ZÁLEŽÍ

KB

Příručka registrační a autorizační postup PSD2 pro třetí strany

Obsah

Autentizace TPP

Třetí strana, která chce využívat služby definované v PSD2 musí mít licenci od národního regulátora a příslušný certifikát vydaný pro služby PSD2.

Předpokladem úspěšné autentizace je pak použití kvalifikovaného certifikátu typu QSEAL (elektronická pečeť) vydaného dle normy ETSI od společnosti I.CA pro identifikaci komunikující třetí strany (také third party provider, dále TPP).

Nutnou podmínkou využití služeb PSD2 v KB je zaslání žádosti o připojení do schránky api@kb.cz včetně certifikátu bez privátního klíče.

Použití certifikátu pečeti znamená vyžadovat podepisování requestu TPP při komunikaci s bankou (ASPSP). TPP je ověřena vyhodnocením platnosti podpisu zprávy a obsahem veřejného klíče zaslaného spolu s podpisem (např. podle normy CAdES).

Použití certifikátu třetích stran je vyžadováno u všech popsaných resources až na „1. Autorizační resource“, který zahajuje přesměrování na federovaný autentizační proces banky.

Registrační a autentizační resource vystavené bankou

Proces enrollmentu klienta nutný pro pochopení registrace aplikace a práce s tokeny je detailně popsán v dokumentaci českého open banking standardu (konkrétně v kapitole Flow v procesu enrollmentu klienta do aplikace TPP) Czech Open Banking Standard.

Nutnou podmínkou pro využívání služeb Iniciování platby (PIS) a Informace o účtu (AIS) je registrace aplikace třetí strany (viz následující kapitola).

1.Charakteristika inicializační/registrační resource

Zavoláním tohoto resource požádá TPP o dynamickou registraci client_id. Pro zavolání resource je potřeba použít platný certifikát. Výstupem jsou parametry client_id a client_secret, které TPP potřebuje pro nastartování a průchod autentizačním procesem uživatele (klienta banky). API klíč není v Komerční bance podporován.

URI: /register
HTTP Metoda: POST
Request URL: https://api.kb.cz/serverapi/oauth2/v1/register
Authorization: request **vyžaduje** autorizaci uživatele/klienta jako součást volání API
Certification: request **vyžaduje** použití kvalifikovaného certifikátu třetí strany.

Podporované kódování: `charset=UTF-8`

Parametry hlavičky (header) requestu:

Parametr	Hodnoty	Povinný	Popis
Tpp_id	string	y	Registrační číslo určitého TPP.

Parametry těla (body) requestu:

Parametr	Hodnoty	Povinný	Popis
application_type	web, native	y	Typ aplikace, která bude používat client_id. V případě typu `web` je požadováno definování rediect_uris ve formátu webového uri v podobě http/s schéma. U typu `native` je možné v redirect_uris zadat např. application package, resp. vlastní formát.
redirect_uris	Pole obsahující řetězce např. ve formátu URL `[Max 3x 2047 B]`	y	Výčet URL kam je na konci přesměrováno flow autentizace. Autorizační request musí obsahovat právě jedno z těchto zaregistrovaných URI v přesném formátu.
client_name	string `[Max 255 B]`	y	Jméno klientské aplikace
client_name#en-US	string `[Max 1024 B]`	n	Jméno klientské aplikace v příslušném jazyce/kódování.
logo_uri	URI `[Max 2047 B]`	n	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)
contact	string e-mail `[Max 320 B]`	n	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů `[Max 10x 255`	n	Pole aplikací požadovaných scopes. Při registraci jsou scopes validovány proti obsahu použitého certifikátu.

	B]		

Příklad requestu:

```
POST /oauth2/register HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: idp.banka.cz

{
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje univerzální banka",
   "client_name#en-US": "My cool bank",
   "logo_uri": "https://www.mybank.cz/logo.png",
   "contact": "info@mybank.cz",
   "scopes": ["aisp", "pisp"]
}
```

Parametry hlavičky (header) response:

Parametr	Hodnoty	Povinný	Popis
Content-Type	string	y	Specification of required transfer format. From the precondition of technical specification of this API standard, in this case, **application/json** format is primarily supported.

Parametry těla (body) response:

Parametr	Hodnoty	Povinný	Popis
client_id	string	y	Aplikaci přiřazené `client_id`. Tímto ID je startován autentizační proces a dekorována komunikace při výměně `code` a `refresh_tokenu`.
client_secret	string	y	Client secret - password/token vydaný IDP banky pro aplikaci (`client_id`) TPP
client_secret_expires_at	Time	n	Defaultní hodnota je 0 (`client_id` nikdy neexpiruje). V opačném případě je uvedena hodnota v sekundách od data 1970-01-01T0:0:0Z
api_key	string	y	API klíč, který aplikace používá při komunikaci s API banky. Pokud banka API klíče nepodporuje, vrátí hodnotu „NOT_PROVIDED“
application_type	web, native	y	Typ aplikace, která bude používat client_id. V případě typu `web` je požadováno definování rediect_uris ve formátu webového uri v podobě http/s schéma. U typu `native` je možné v redirect_uris zadat např. application package, resp. vlastní formát.
redirect_uris	Pole obsahující	y	Výčet URL kam je na konci přesměrováno flow

	řetězce např. ve formátu URL [Max 3x 2047 B]		autentizace. Autorizační request musí obsahovat právě jedno z těchto zaregistrovaných URI v přesném formátu.
client_name	string [Max 255 B]	y	Jméno klientské aplikace
client_name#en-US	string [Max 1024 B]	n	Jméno klientské aplikace v příslušném jazyce/kódování.
logo_uri	URI [Max 2047 B]	n	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)
contact	string e-mail [Max 320 B]	n	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů [Max 10x 255 B]	n	Pole aplikací požadovaných scopes. Při registraci jsou scopes validovány proti obsahu použitého certifikátu.

Příklad response bez chyby:

```
HTTP/1.1 201 Created
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
   "client_id": "a0b25291f0",
   "client_secret":
     "AAjkk45sd78ad454gddd8712_4555g5g5g5gg",
   "client_secret_expires_at": 0,
   "api_key":
     "00000000-1212-0f0f-a0a0-123456789abc",
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje univerzální banka",
   "client_name#en-US": "My cool bank",
   "logo_uri": "https://www.mybank.cz/logo.png",
```

Chybové kódy:

HTTP Status	Kód	Popis
400	**invalid_request**	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu.
401	**invalid_client**	Nevalidní client_id.
401	**unauthorized_client**	Klient není oprávněný provádět tento dotaz.
401	**access_denied**	Autorizační server odmítl přístup.
500, 503	**server_error**	Chyba autorizačního serveru.

2.Charakteristika resource Informace o registračních údajích aplikace

Zavoláním tohoto resource může TPP požádat o přehled registračních údajů pro konkrétní aplikaci. Pro zavolání resource je potřeba použít platný certifikát a client_id, které je vydáno k tomuto TPP. Výstupem je přehled registračních údajů.

URI: /register/{client_id}
HTTP Metoda: GET
Request URL: https://api.kb.cz/serverapi/oauth2/v1/register/{client_id}
Authorization: request **vyžaduje** autorizaci uživatele/klienta jako součást volání API
Certification: request **vyžaduje** použití kvalifikovaného certifikátu třetí strany.

Podporované kódování: `charset=UTF-8`

Příklad requestu:

```
GET /oauth2/register/a0b25291f0 HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: idp.banka.cz
```

Parametry response:

Parametr	Hodnoty	Povinný	Popis
client_id	string	y	Aplikaci přiřazené `client_id`. Tímto ID je startován autentizační proces a dekorována komunikace při výměně `code` a `refresh_tokenu`.
client_secret	string	y	Client secret - password/token vydaný IDP banky pro aplikaci (`client_id`) TPP
client_secret_expires_at	Time	n	Defaultní hodnota je 0 (`client_id` nikdy neexpiruje). V opačném případě je uvedena hodnota v sekundách od data 1970-01-01T0:0:0Z
api_key	string	y	API klíč, který aplikace používá při komunikaci s API banky. Pokud banka API klíče nepodporuje, vrátí hodnotu „NOT_PROVIDED“
application_type	web, native	y	Typ aplikace, která bude používat client_id. V případě typu `web` je požadováno definování rediect_uris ve formátu webového uri v podobě http/s schéma. U typu `native` je možné v redirect_uris zadat např. application package, resp. vlastní formát.
redirect_uris	Pole obsahující řetězce např. ve formátu URL	y	Výčet URL kam je na konci přesměrováno flow autentizace. Autorizační request musí obsahovat právě jedno z těchto zaregistrovaných URI v přesném formátu.
client_name	string	y	Jméno klientské aplikace
client_name#en-US	string	n	Jméno klientské aplikace v příslušném jazyce/kódování.
logo_uri	URI	n	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)

contact	string e-mail	n	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů	n	Pole aplikací požadovaných scopes. Při registraci jsou scopes validovány proti obsahu použitého certifikátu.

Příklad response bez chyby:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
   "client_id": "a0b25291f0",
   "client_secret":
     "AAjkk45sd78ad454gddd8712_4555g5g5g5gg",
   "client_secret_expires_at": 0,
   "api_key":
     "00000000-1212-0f0f-a0a0-123456789abc",
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje univerzální banka",
   "client_name#en-US": "My cool bank",
   "logo_uri": "https://www.mybank.cz/logo.png",
   "contact": "info@mybank.cz",
   "scopes": ["aisp", "pisp"]
}
```

Chybové kódy:

HTTP Status	Kód	Popis
400	**invalid_request**	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu.
401	**invalid_client**	Nevalidní client_id.
401	**unauthorized_client**	Klient není oprávněný provádět tento dotaz.
401	**access_denied**	Autorizační server odmítl přístup.
500, 503	**server_error**	Chyba autorizačního serveru.

3.Charakteristika resource Změna registračních údajů

Zavoláním tohoto resource může TPP požádat o změnu registračních údajů pro konkrétní aplikaci. Pro zavolání resource je potřeba použít platný certifikát a client_id, které je vydáno k tomuto TPP. Výstupem je přehled změněných údajů.

URI: /register/{client_id}
HTTP Metoda: PUT
Request URL: https://api.kb.cz/serverapi/oauth2/v1/register/{client_id}
Authorization: request **vyžaduje** autorizaci uživatele/klienta jako součást volání API
Certification: request **vyžaduje** použití kvalifikovaného certifikátu třetí strany.

Podporované kódování: `charset=UTF-8`

Parametry hlavičky (header) requestu:

Parametr	Hodnoty	Povinný	Popis
client_id	string	y	Registrační číslo určitého TPP.

Parametry těla (body) requestu:

Parametr	Hodnoty	Povinný	Popis
application_type	web, native	y	Typ aplikace, která bude používat client_id. V případě typu `web` je požadováno definování rediect_uris ve formátu webového uri v podobě http/s schéma. U typu `native` je možné v redirect_uris zadat např. application package, resp. vlastní formát.
redirect_uris	Pole obsahující řetězce např. ve formátu URL `[Max 3x 2047 B]`	y	Výčet URL kam je na konci přesměrováno flow autentizace. Autorizační request musí obsahovat právě jedno z těchto zaregistrovaných URI v přesném formátu.
client_name	string `[Max 255 B]`	y	Jméno klientské aplikace
client_name#en-US	string `[Max 1024 B]`	n	Jméno klientské aplikace v příslušném jazyce/kódování.
logo_uri	URI `[Max 2047 B]`	n	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)
contact	string e-mail `[Max 320 B]`	n	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů `[Max 10x 255 B]`	n	Pole aplikací požadovaných scopes. Při registraci jsou scopes validovány proti obsahu použitého certifikátu. **`[ aisp, pisp ]`**

Příklad requestu:

```
POST /oauth2/register/a0b25291f0 HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: idp.banka.cz

{
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje univerzální banka",
   "client_name#en-US": "My cool bank",
   "logo_uri": "https://www.mybank.cz/logo.png",
   "contact": "info@mybank.cz",
   "scopes": ["aisp", "pisp"]
}
```

Parametry hlavičky (header) response:

Parametr	Hodnoty	Povinný	Popis
Content-Type	string	y	Specification of required transfer format. From the precondition of technical specification of this API standard, in this case, **application/json** format is primarily supported.

Parametry těla (body) response:

Parametr	Hodnoty	Povinný	Popis
client_id	ID aplikace TPP	y	Jedinečný identifikátor aplikace TPP vydaný bankou, resp IDP banky. Např. použitím resource *„0. Inicializační/registrační resource“*
client_secret_expires_at	Time	n	Defaultní hodnota je 0 (`client_id` nikdy neexpiruje). V opačném případě je uvedena hodnota v sekundách od data 1970-01-01T0:0:0Z
application_type	web, native	y	Typ aplikace, která bude používat client_id. V případě typu `web` je požadováno definování rediect_uris ve formátu webového uri v podobě http/s schéma. U typu `native` je možné v redirect_uris zadat např. application package, resp. vlastní formát.
redirect_uris	Pole obsahující řetězce např. ve formátu URL	y	Výčet URL kam je na konci přesměrováno flow autentizace. Autorizační request musí obsahovat právě jedno z těchto zaregistrovaných URI v přesném formátu.
client_name	string	y	Jméno klientské aplikace
client_name#en-US	Libovolný string	n	Jméno klientské aplikace v příslušném jazyce/kódování.
logo_uri	URI	n	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)

contact	string e-mail	n	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů	n	Pole aplikací požadovaných scopes. Při registraci jsou scopes validovány proti obsahu použitého certifikátu.

Příklad response bez chyby:

```
HTTP/1.1 200
Content-Type: application/json

{
   "client_id": "a0b25291f0",
   "client_secret_expires_at": 0,
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje univerzální banka",
   "client_name#en-US": "My cool bank",
   "logo_uri": "https://www.mybank.cz/logo.png",
   "contact": "info@mybank.cz",
   "scopes": ["aisp", "pisp"]
}
```

Chybové kódy:

HTTP Status	Kód	Popis
400	**invalid_request**	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu.
401	**invalid_client**	Nevalidní client_id.
401	**unauthorized_client**	Klient není oprávněný provádět tento dotaz.
401	**access_denied**	Autorizační server odmítl přístup.
500, 503	**server_error**	Chyba autorizačního serveru.
400	**invalid_scope**	Neplatný scope požadavku.
403	**insufficient_scope**	Např. nedostatečné oprávnění pro použití požadovaného scope.
400	**invalid_redirect_uri**	Hodnota jednoho nebo více redirect uri není validní.

4.Charakteristika resource Smazání aplikace

Zavoláním tohoto resource může TPP požádat o smazání údajů a přístupu konkrétní aplikaci. Pro zavolání resource je potřeba použít platný certifikát a client_id, které je vydáno tomuto TPP. Výstupem je potvrzení o smazání.

URI: /register/{client_id}
HTTP Metoda: DELETE
Request URL: https://api.kb.cz/serverapi/oauth2/v1/register/{client_id}
Authorization: request **vyžaduje** autorizaci uživatele/klienta jako součást volání API
Certification: request **vyžaduje** použití kvalifikovaného certifikátu třetí strany.

Podporované kódování: `charset=UTF-8`

Příklad requestu:

```
DELETE /oauth2/register/a0b25291f0 HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: idp.banka.cz
```

Příklad response:

```
HTTP/1.1 201 Created
```

Chybové kódy:

HTTP Status	Kód	Popis
401	**invalid_client**	Nevalidní client_id.
401	**unauthorized_client**	Klient není oprávněný provádět tento dotaz.
401	**access_denied**	Autorizační server odmítl přístup.
500, 503	**server_error**	Chyba autorizačního serveru.

5.Charakteristika resource Žádost o nový client_secret

Zavoláním tohoto resource může TPP požádat o vydání nového client_secret. Pro zavolání resource je potřeba použít platný certifikát a client_id, které je vydáno tomuto TPP. Původní client_secret bude tímto requestem zneplatněn.

URI: /register/{client_id}
HTTP Metoda: POST
Request URL: https://api.kb.cz/serverapi/oauth2/v1/register/{client_id}
Authorization: request **vyžaduje** autorizaci uživatele/klienta jako součást volání API
Certification: request **vyžaduje** použití kvalifikovaného certifikátu třetí strany.

Podporované kódování: `charset=UTF-8`

Příklad requestu:

```
POST /oauth2/register/a0b25291f0/renewSecret HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: idp.banka.cz
```

Parametry response:

Parametr	Hodnoty	Povinný	Popis
client_id	string	y	Aplikaci přiřazené `client_id`. Tímto ID je startován autentizační proces a dekorována komunikace při výměně `code` a `refresh_token`u.
client_secret	string	y	Client secret - password/token vydaný IDP banky pro aplikaci (`client_id`) TPP
client_secret_expires_at	Time	n	Defaultní hodnota je 0 (`client_id` nikdy neexpiruje). V opačném případě je uvedena hodnota v sekundách od data 1970-01-01T0:0:0Z

Příklad response bez chyby:

```
HTTP/1.1 200 OK

{
   "client_id": "a0b25291f0",
   "client_secret": "BBjkk45sd78ad454gddd8712_4555g5g5g5gg",
   "client_secret_expires_at": 0
}
```

Chybové kódy:

HTTP Status	Kód	Popis
400	**invalid_request**	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu.
401	**invalid_client**	Nevalidní client_id.
401	**unauthorized_client**	Klient není oprávněný provádět tento dotaz.
401	**access_denied**	Autorizační server odmítl přístup.
500, 503	**server_error**	Chyba autorizačního serveru.

6.Charakteristika requestu na Autorizační resource

Když váš klient/aplikace není autorizován, musí si obstarat autorizační kód, předtím než si zažádá o přístupový token. Vaše aplikace může zahájit autorizační proces tím, že přesměruje webový prohlížeč svého uživatele na bankovní autorizační server. Server poté bude po uživateli požadovat jeho údaje. Uživateli se zobrazí povolení specifikovaná scopem a seznam bankovních a platebních služeb a účtů, ze kterých může uživatel vybírat. Pokud uživatel povolí vaší aplikaci přístup k něčemu z toho, server zašle autorizační kód na callback URL tím, že přesměruje prohlížeč na redirect_uri.

URI: /ssologin
HTTP Metoda: GET
Request URL: https://login.kb.cz/autfe/ssologin
Authorization: request **vyžaduje** autorizaci uživatele/klienta jako součást volání API
Certification: request **vyžaduje** použití kvalifikovaného certifikátu třetí strany.

Podporované kódování: `charset=UTF-8`

Parametry requestu:

Parametr	Hodnoty	Povinný	Popis
response_type	code	y	Povinný parametr. Určuje použité autentizační flow. V tomto případě code grant. Pro autentizační proces to znamená, že jako výsledek úspěšné identifikace a autentizace je očekáván jednorázový code na místo access_tokenu.
client_id	ID aplikace TPP	y	Jedinečný identifikátor aplikace TPP vydaný bankou, resp IDP banky. Např. použitím resource *„0. Inicializační/registrační resource“*
redirect_uri	URL	y	URL kam je na konci přesměrováno flow autentizace. Toto URL je stanoveno již při vydání client_id a v rámci autentizace je tento parametr validován proti URL zavedenému k client_id v systému IDP banky. Hodnota by se měla shodovat s jednou z hodnot zavedených použitím resource *„0. Inicializační/registrační resource“.*
scope	Seznam oprávnění oddělený mezerou	n	Jedná se o pole aplikací požadovaných scope (oprávnění). V případě PSD2 to mohou být role aisp a pisp. Např. pokud je TPP držitelem obou oprávnění může zde pro svoji aplikaci požádat jen o jedno z nich nebo oboje viz příklad requestu
state	Libovolný string	n	Tímto parametrem je možné obohatit redirect_uri při přesměrování. Slouží k předání informací z aplikace přes autentizační flow.

Příklad requestu:

```
GET /oauth2/authfe/ssologin HTTP/1.1
Host: idp.banka.cz
Content-Type: application/x-www-form-urlencoded

client_id=MyPFM&
redirect_uri=https://www.mypfm.cz/start&
response_type=code&
scope=aisp pisp&
state=balance
```

Příklad volání přes příkazovou řádku prohlížeče
V linku
https://login.kb.cz/autfe/ssologin?response_type=code&client_id=DOPLNIT_client_id&redirect_uri=DOPLNIT_redirect_uri&state=12345678&scope=aisp
) je nutno změnit hodnotu client_id dle požadované hodnoty, dále redirect_uri a požadovaný scope ve formě „aisp“, „pisp“ (více hodnot je odděleno čárkami).

Parametry response:

Pole	Popis
code	Autorizační code
state	Parametr state z requestu TPP

Příklad response bez chyby:

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

Chybové kódy:

HTTP Status	Kód	Popis
302	**invalid_request**	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu.
302	**unauthorized_client**	Klient není oprávněný provádět tento dotaz.
302	**access_denied**	Autorizační server odmítl přístup.
500, 503	**server_error**	Chyba autorizačního serveru.
302	**invalid_scope**	Neplatný scope požadavku.

Příklad error response:

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

7.Charakteristika requestu Získání/vystavení tokenu

Poté co vaše aplikace obdrží autorizační kód, může ho následně vyměnit za access nebo refresh token.

URI: /token
HTTP Metoda: POST
Request URL: https://api.kb.cz/serverapi/oauth2/v1/token
Authorization: request **vyžaduje** autorizaci uživatele/klienta jako součást volání API
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)	Autorizační kód vrácený z původního requestu.
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 URl, 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.
client_secret	string	n (pokud se jedná o získání access tokenu pak je povinný)	Client secret - password/token vydaný IDP banky pro aplikaci (`client_id`) 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 pověření 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

8.Charakteristika requestu Zneplatnění tokenu

API sloužící ke zrušení platnosti refresh nebo access tokenu.

URI: /revoke
HTTP Metoda: POST
Request URL: https://api.kb.cz/serverapi/oauth2/v1/revoke
Authorization: request **vyžaduje** autorizaci uživatele/klienta jako součást volání API
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