Příručka registrační a autorizační postup PSD2 pro třetí strany

Datum zveřejnění	Verze	Datum účinnosti	Popis
7.7.2020	4	8.7.2020	Úprava dokumentu
3.6.2021	5	1.7.2021	Parametry těla (body) requestu & Parametry těla (body) response (kap. 1. až 3.): email „contact“ a další jsou nově mandatorní

Poznámka: Přeškrtnuté a žlutě podbarvené jsou změny oproti ČOBS.

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) nebo QWAC (kvalifikovaný certifikát pro webové stránky) vydaného dle normy ETSI od společnosti I.CA (nebo jiného QTSP ze seznamu EBA, který je už akceptován Komerční bankou (KB) – potřeba ověřit na api@kb.cz) 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 veřejného certifikátu bez privátního klíče.

Rozdíly oproti předchozí verzi příručky jsou rovněž označeny žlutě.

Autentizační certifikát třetí strany je vyžadován při navázaní zabezpečeného spojení s bankou (ASPSP) komunikačním protokolem TLS.

Autentizace je vyžadována u všech resources, kromě autorizace klienta viz. kapitola *Charakteristika requestu na Autorizační resource*, který zahajuje federovaný autentizační proces KB.

Jak postupovat při výměně PSD2 certifikátu

Při výměně certifikátu potřeba provést registraci/ověření nového certifikátu (nejlépe v dostatečném předstihu před expirací původního PSD2 certifikátu, aby byla zajištěna kontinuita konzumace PSD2 služeb) je potřeba postupovat takto:

1) Nutnou podmínkou pokračování využití PSD2 služeb v KB je, že **TPP zašle k manuální registraci nový PSD2 certifikát** do schránky **api@kb.cz** - tzn. jen **veřejnou část nového PSD2 certifikátu bez privátního klíče**, ideální je současně sdělit též počáteční datum platnosti nového certifikátu nebo jeho sériové číslo.

2) **KB** následně zašle TPP ze stejné emailové schránky (api@kb.cz) **potvrzení o registraci certifikátu**.

3) **TPP provolá s novým certifikátem celé AISP / PISP flow** (v závislosti na scopu dle licence) a proces konzumace PSD2 služeb je obnoven/kontinuálně pokračuje (tzv. bezvýpadkově).

4) V závislosti na souběhu obou certifikátů (existujících i nových) může TPP používat oba certifikáty současně (během jejich platnosti).

5) Použití nového certifikátu neznamená, že musíte vygenerovat nové identifikační údaje TPP (clientId, clientSecret nebo apiKey).

6) Pouze v případě, že by výměna neproběhla v pořádku, TPP nahlásí případné chyby KB na emailovou schránku api@kb.cz

Hlášení chyb

Hlášení chyb na PSD2 produkci probíhá vždy pomocí mailové schránky api@kb.cz. Odeslaný mail musí obsahovat níže uvedené náležitosti v případě chybějící požadované informace nebude možné dotaz nebo chybu zpracovat.

Je potřeba specifikovat následující:
PSD2 API doménu: ***CZ**, nebo **SK***
Prostředí: ***Sandbox**, nebo **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 (kterou PSD2 službu)
Datum a čas uskutečněného volání
IP adresu
Chybu a její co nejpřesnější popis (vč. „***x-request-id***“), který může být doplněn o příslušný otisk obrazovky.

Bez výše uvedených hodnot není možné hlášenou chybou bezprostředně zabývat a KB vás může požádat o doplnění nezbytných informací (může to opravu chyby prodloužit).

Registrační a autentizační resource vystavený 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 žádá TPP o dynamickou registraci svojí aplikace (v terminologii OAuth je to 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. ***Poznamka – native není v Komerční bance podporován***
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]`	y	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)
contact	string e-mail `[Max 320 B]`	y	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů `[Max 10x 255 B]`	y	Pole aplikací požadovaných scopes. Při registraci jsou scopes validovány proti obsahu použitého certifikátu. Pole je case-sensitive a povolené hodnoty jsou "aisp" a "pisp".

Příklad requestu:

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

{
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje_univerzalni_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.
x-request-id	String	n	Volitelný parametr pro identifikaci (spárování) TPP request / response

Parametry těla (body) response:

Parametr	Hodnoty	Povinný	Popis
client_id	String	y	Aplikaci přiřazené `client_id`. Tímto ID je startován autentizační proces a dekodována komunikace při výměně `code` a `refresh_tokenu`.
client_secret	String	y	Client secret - password/token vydaný IDP banky pro aplikaci (`client_id`) TPP
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	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.
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]`	y	Jméno klientské aplikace v příslušném jazyce/kódování.
logo_uri	URI `[Max 2047 B]`	y	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)
contact	string e-mail	y	E-mail jako kontakt na zodpovědnou osobu na straně

	[Max 320 B]		klientské aplikace.
scopes	Pole stringů [Max 10x 255 B]	y	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; charset=UTF-8
Accept-Encoding: gzip,deflate
x-request-id: 4512345
Host: api.kb.cz
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.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje_univerzalni_banka",
   "client_name#en-US": "My_cool_bank",
   "logo_uri": "https://www.mybank.cz/logo.png",
   "contact": "info@kb.cz",
   "scopes":[
      "pisp",
      "aisp"]
}
```

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
https://api.kb.cz/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.kb.cz
Connection: Keep-Alive
```

Parametry response:

Parametr	Hodnoty	Povinný	Popis
client_id	string	Y	Aplikaci přiřazené `client_id`. Tímto ID je startován autentizační proces a dekodována komunikace při výměně `code` a `refresh_tokenu`.
client_secret	string	Y	Client secret - password/token vydaný IDP banky pro aplikaci (`client_id`) TPP
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	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.
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	Y	Jméno klientské aplikace v příslušném jazyce/kódování.
logo_uri	URI	Y	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)
contact	string e-mail	Y	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů	Y	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; charset=UTF-8
x-request-id: 112233
Host: api.kb.cz
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.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje_univerzalni_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.
x-request-id	String	n	Volitelný parametr pro identifikaci (spárování) TPP request / response

Parametry těla (body) requestu:

Parametr	Hodnoty	Povinný	Popis
application_type	web	y	Typ aplikace, která bude používat client_id. V případě typu `web` je požadováno definování redirect_uris ve formátu webového uri v podobě http/s schéma.
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]`	y	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)
contact	string e-mail `[Max 320 B]`	y	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů `[Max 10x 255 B]`	y	Pole aplikací požadovaných scopes. Při registraci jsou scopes validovány proti obsahu použitého certifikátu. **`["aisp","pisp"]`**

Příklad requestu:

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

{
   "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.cz/start",
      "https://www.mymultibank.cz/start2"],
```

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

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.
x-request-id	String	n	Volitelný parametr pro identifikaci (spárování) TPP request / response

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“*
application_type	web	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.
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	y	Jméno klientské aplikace v příslušném jazyce/kódování.
logo_uri	URI	y	URI loga aplikace (resp. místo odkud je možné ho při registraci stáhnout)
contact	string e-mail	y	E-mail jako kontakt na zodpovědnou osobu na straně klientské aplikace.
scopes	Pole stringů	y	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;charset=UTF-8
x-request-id: 235144
Host: api.kb.cz
Accept-Encoding: gzip,deflate
Content-Language: cs
Connection: Keep-Alive

{
 "client_id": " Moje_univerzalni_banka-1234",     "application_type": "web",
   "redirect_uris":
     ["https://www.mymultibank.cz/start",
      "https://www.mymultibank.cz/start2"],
   "client_name": "Moje_nejlepsi_banka",
   "client_name#en-US": "My_best_bank",
```

```
   "logo_uri": "https://www.mybank.cz/logo.png",
   "contact": "info@mybank.cz",
   "scopes": ["aisp"]
}
```

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

Příklad 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
```

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

Parametry response:

Parametr	Hodnoty	Povinný	Popis
client_id	string	y	Aplikaci přiřazené `client_id`. Tímto ID je startován autentizační proces a dekodována komunikace při výměně `code` a `refresh_tokenu`.
client_secret	string	y	Client secret - password/token vydaný IDP banky pro aplikaci (`client_id`) TPP

Příklad response bez chyby:

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

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

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

Resource slouží na získaní autorizačního kódu uživatele (code), který je nutnou podmínkou pro získaní přístupového tokenu. Aplikace třetí strany může zahájit autorizační proces tím, že přesměruje webový prohlížeč svého uživatele na bankovní autorizační server. V rámci autorizačního procesu budou od uživatele vyžadovány jeho přihlašovací údaje do internetového bankovnictví KB. Uživateli se po přihlášení zobrazí výčet povolení (specifikovaných scopem např. AISP a/nebo PISP), pro které může udělit souhlas třetí straně. Pokud uživatel povolí aplikaci vybraný přístup, obdrží TPP autorizační kód jako parametr v rámci přesměrování na callback URL (adresa uvedená při registraci aplikace).

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 **nevyžaduje** 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	hodnota aisp nebo pisp	n	Atribut pro omezení požadovaného scope (oprávnění). V případě PSD2 to může být role "aisp“ nebo "pisp“ (case-sensitive). Pokud se atribut „scope“ neuvede vůbec, přebírá se scope z registrované aplikace (implicitní hodnota). Např. pokud je aplikace TPP držitelem obou oprávnění může zde pro svoji konkrétní operaci omezit scope požádat pouze na jednu roli 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. (může sloužit i pro spárování request/response dotazu)

Příklad requestu:

```
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.cz/start&
response_type=code&
scope=aisp&
state=12345678
```

Příklad volání přes příkazovou řádku prohlížeče (zde pouze pro scope AISP)

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

Hodnoty barevných částí (client_id, redirect_uri) je nutné doplnit. Atribut scope není nutné uvádět vůbec, přebere se scope aplikace v plném rozsahu (aisp a pisp). Pro omezení požadovaného rozsahu scope, lze uvést pouze jednu z hodnot „aisp“ nebo „pisp“ (více hodnot není přípustných).

Parametry response:

Pole	Popis
code	Autorizační code (typu JWT token skládající se ze 3 částí oddělených tečkou)
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.mymultibank.cz/start?
          code=a200234062baa2ada828bbd33c1f6054&
          state=12345678
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 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.
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
x-request-id	String	n	Volitelný parametr pro identifikaci (spárování) TPP request / response

Příklad requestu:

```
POST https://api.kb.cz/serverapi/oauth2/v1/token HTTP/1.1
Host: api.kb.cz
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.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.
scope	string	y	Scope vystaveného JWT tokenu např. aisp, pisp

Příklad response bez chyby:
Úspěšně zpracovaný request odpoví response s takto definovaným JSON payloadem:

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

Chybové kódy:

HTTP Status	Kód	Popis
400	invalid_request invalid_client invalid_grant unauthorized_client	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu. Nevalidní uživatel. Neplatné pověření. Uživatel není oprávněný používat autorizační typ.
401	Access_denied	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 https://api.kb.cz/serverapi/oauth2/v1/revoke HTTP/1.1
Host: api.kb.cz
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
```

Chybové kódy:

HTTP Status	Kód	Popis
302	Invalid_request Invalid_client Access_denied	Nevalidní request nebo nevalidní klient, přístup odepřen.
400	invalid_request Invalid_client TODO validace s CAAS, přebírame	Nevalidní request. V dotazu chybí povinné pole nebo je v nevhodném / nevalidním formátu.
401	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