OTEVŘENÉ BANKOVNICTVÍ

Fio banka

Verze 1.2

OBSAH

1 POPIS

Pro provádění volání API je nejprve nutné získat platný přístupový token. Jeho získání probíhá pomocí mechanismu OAuth2 tak, jak je popsán v Českém standardu pro Open Banking. Následující návod slouží k rychlejšímu seznámení s použitým autentikačním mechanismem.

2 JAK ZAČÍT (SANDBOX)

Nejprve je nutné zaregistrovat TPP do sandbox prostředí prostřednictvím webového formuláře na adrese https://developers.fio.cz/oauth2/register. Po registraci obdržíte údaje client-id, client-secret a API key, které budou potřebné v dalších krocích autentikace.

Přihlašovací údaje uživatelů dostupných v sandbox prostředí jsou uvedeny na adrese https://developers.fio.cz.

Sandbox prostředí se nachází na URL https://developers.fio.cz/api/
Sandbox nevyžaduje klientský SSL certifikát pro HTTPS spojení.

2.1 Povolení přístupu klienta banky

Zaregistrovaný TPP může vyžádat souhlas klienta s přístupem k bankovním účtům prostřednictvím POST požadavku:

https://developers.fio.cz/api/cz/v1/oauth/auth?response_type=code&client_id=${client_id}&redirect_uri=${redirectUrl}&state=${state}&scope=${scope}

Content-Type je application/x-www-form-urlencoded

Vstupy:

response_type	definuje použité autentikační flow, zde použita hodnota "code"
client_id	identifikátor TPP z registrace
redirect_uri	návratová URL OAuth2 autentikacie, musí odpovídat jedné z hodnot vyplněné při registraci TPP
state	libovolný řetězec definovný TPP, který bude v nezměněné formě předán při přesměrování
scope	mezerou oddělený seznam požadovaných oprávnění (možné hodnoty "aisp", "pisp", "cisp") - není možné vyžadovat oprávnění, které nebylo nastaveno při registraci TPP

Příklad:

```
https://developers.fio.cz/api/cz/v1/oauth/auth?response_type=code&client_id=Q1pf
XzAzYmQ3N2U0LWE2NTQtNDJjOC04NGM4LWVjNmViMDk2Y2U4OQ%3D%3D&redirect_uri=https%3A%2
F%2Fdevelopers.fio.cz%2Fwebjars%2Fspringfox-swagger-ui%2Foauth2-
redirect.html&state=tpp_special_value&scope=aisp+cisp+pisp
```

Po vyplnění přihlašovacích údajů klienta banky (reprezentující udělení souhlasu klienta s přístupem) dojde k přesměrování (HTTP redirect) na zadanou redirect_uri s parametry:

- code - jednorázový kód, slouží k výměně za refresh a access token
- state - zopakovaná hodnota ze vstupu generovaná TPP

```
https://developers.fio.cz/webjars/springfox-swagger-ui/oauth2-
redirect.html?code=kCot-0gbWhsnSkzVg7IwI-
r0OGa38P2QLDFIe_AqJ_A%3D&state=tpp_special_value
```

2.2 Výměna authorization code za refresh token a access token

V dalším kroku je nutné vyměnit získaný jednorázový kód za přístupové tokeny pomocí POST požadavku na URL https://developers.fio.cz/api/cz/v1/oauth/token

Autorizačním kódem se nemyslí obsah SMS kterou banka zašle klientovi, k autorizaci přístupu TPP, ale kód který vrátí banka v URL.

Vstupy:
Content-Type je application/x-www-form-urlencoded

grant_type	konstanta "authorization_code" dle standardu OAuth2
code	výstupní parametr code z OAuth2 autentikace v předchozím kroku
client_id	identifikator TPP z registrace
client_secret	secret TPP z registrace
redirect_uri	návratová URL OAuth2 autentikace, musí odpovídat hodnotě použité v předchozím kroku

Výstupem je dokument ve formátu JSON s následujícími elementy:

access_token	krátkodobý přístupový token k volání API
expires_in	expirace access tokenu v sekundách
token_type	konstanta "Bearer" dle standardu OAuth2
refresh_token	dlouhodobý token sloužící k obnovení krátkodobého přístupového tokenu
refresh_expires_in	expirace refresh tokenu v sekundách

Příklad volání pomocí nástroje curl:

```
curl -s --insecure -X POST -H 'Content-Type: application/x-www-form-urlencoded'
-d
'grant_type=authorization_code&client_id=Q1pfXzAzYmQ3N2U0LWE2NTQtNDJjOC04NGM4LWV
jNmViMDk2Y2U4OQ%3D%3D&client_secret=M2Q1YzJhNmEtZTg5ZS00Y2VkLWFjMzUtYmVjYjJkMGJm
ZTQz&redirect_uri=https%3A%2F%2Fdevelopers.fio.cz%2Fwebjars%2Fspringfox-swagger-
ui%2Foauth2-redirect.html&code=XBgCUQiWwR3v8sEHsacS4Oyp4Uu7otnNo7Gt81lTEQE%3D'
https://developers.fio.cz/api/cz/v1/oauth/token
```

Výstup:

```
{
"access_token":"Y2FjNTI0NjYtYjY3NS00NTg4LWE2NjItNTBjZmFiM2M1MmVj",
"refresh_token":"YWIyNjI5MmYtYzNjOC00ZGNkLWFjOGEtMjEzMzQ1ODU4MTU2",
"token_type":"Bearer",
"refresh_expires_in":7776000,
"expires_in":3599
}
```

2.3 Výměna refresh tokenu za access token

Po vypršení platnosti access tokenu je možné požádat o nový access token prostřednictvím platného refresh tokenu.

POST požadavek na URL https://developers.fio.cz/api/cz/v1/oauth/token

Vstupy:

Content-Type je application/x-www-form-urlencoded

grant_type	konstanta "refresh_token"
client_id	identifikátor TPP z registrace
client_secret	secret TPP z registracie
refresh_token	refresh_token

Výstupem je dokument ve formátu JSON s následujícími elementy:

access_token	krátkodobý přístupový token k volání API
expires_in	expirace access tokenu v sekundách
token_type	konstanta "Bearer" dle standardu OAuth2
refresh_token	dlouhodobý token sloužící k obnovení krátkodobého přístupového tokenu
refresh_expires_in	expirace refresh tokenu v sekundách

Příklad:

```
curl -s --insecure -X POST -H 'Content-Type: application/x-www-form-urlencoded'
-d
'grant_type=refresh_token&client_id=Q1pfXzAzYmQ3N2U0LWE2NTQtNDJjOC04NGM4LWVjNmVi
MDk2Y2U4OQ%3D%3D&client_secret=M2Q1YzJhNmEtZTg5ZS00Y2VkLWFjMzUtYmVjYjJkMGJmZTQz&
refresh_token=YWIyNjI5MmYtYzNjOC00ZGNkLWFjOGEtMjEzMzQ1ODU4MTU2'
https://developers.fio.cz/api/cz/v1/oauth/token
```

2.4 Použití access tokenu pro volání API

Pro volání autentikovaných endpointů API musí být v požadavku vyplněné následující hodnoty HTTP header (hlavičky):

Authorization: Bearer {access_token}

Příklad:

```
curl --insecure -H "Authorization: Bearer
Y2FjNTI0NjYtYjY3NS00NTg4LWE2NjItNTBjZmFiM2M1MmVj"
https://developers.fio.cz/api/cz/v1/accounts
```

Výstup:

```
{
"pageNumber":0,
"pageCount":1,
"pageSize":2,
"totalCount":2,
"accounts":[
  {§é
    "id":"1",
    "identification":
      {
        "iban":"CZ2020100000001234567890",
        "other":"1234567890/2010"
      },
    "currency":"CZK",
    "servicer":
      {
        "bankCode":"2010",
        "bic":"FIOBCZPP"
      },
    "nameI18N":"Osobni ucet",
    "productI18N":"Osobni konto"
  },
```

```
  {
    "id":"2",
    "identification":
      {
        "iban":"CZ2020100000004444444444",
        "other":"4444444444/2010"
      },
    "currency":"CZK",
    "servicer":
      {
        "bankCode":"2010",
        "bic":"FIOBCZPP"
      },
     "nameI18N":"Podnikatelsky ucet",
     "productI18N":"Podnikatelske konto"
  }]
}
```

3 ŽÁDOST O PŘÍSTUP DO PRODUKČNÍHO PROSTŘEDÍ

Požadavek o přístup zašlete na adresu api@fio.cz. Do žádosti uveďte.

Název žádajícího subjektu:

Hlavní kontakt:
Jméno a příjmení:
E-mail:
Telefon:

Technický kontakt:
Jméno a příjmení:
E-mail:
Telefon:

Identifikátor společnosti získané od národního regulátora:
URL s logem:
Návratové URL pro OAuth2 (je možné i více hodnot):
Požadovaná přístupová práva [AISP/CISP/PISP]:

V příloze:

1. Vaše veřejná část PGP klíče.
   PGP klíč bude sloužit k bezpečnému předání dat (clientId, clientSecret, webApiKey) vaší společnosti po zpracování žádosti a přidání do produkčního prostředí.
2. QWAC certifikát ve formátu PEM a včetně seznamu jeho nadřízených certifikátů až k root CA.

4 PRODUKČNÍ KONCOVÉ BODY (ENDPOINTS)

Při vytváření SSL spojení používejte plný řetězec klientských certifikátů od QWAC až k root CA.

AISP endpoint: https://api.fio.cz/api/cz/v1/accounts

CISP endpoint: https://api.fio.cz/api/cz/v1/accounts/balanceCheck

PISP endpoint: https://api.fio.cz/api/cz/v1/payments

Auth endpoint: https://api.fio.cz/api/cz/v1/oauth/auth

Token endpoint: https://api.fio.cz/api/cz/v1/oauth/token

Token revoke endpoint: https://api.fio.cz/api/cz/v1/oauth/revoke

Connection test controller https://api.fio.cz/api/cz/v1/test

5 TEST FUNKČNOSTI A OBNOVA CERTIFIKÁTU

QWAC certifikát má dobu platnosti. Minimálně 15 dní před vypršením certifikátu doporučujeme si obnovený certifikát otestovat a vyzkoušet, jestli komunikace mezi třetí stranou a Fio bankou nepřestane fungovat.

Pro zajištění bezproblémové komunikace, před nasazením QWAC certifikátu na produkčních serverech třetí strany, doporučujeme ověřit funkčnost obnoveného QWAC certifikátu na endpointu https://api.fio.cz/api/cz/v1/test.

Vrátí-li endpoint stejný identifikátor společnosti (OrganizationIdentifier) stejný jako v původním certifikátu, tak není potřeba kontaktovat Fio banku pro výměnu certifikátu. Obnovu lze možné provést bez součinnosti pracovníků banky.

Pokud endpoint vrátí chybu "No client certificate used" nebo jinou chybu, tak je nutné kontaktovat Fio banku, se žádostí o výměnu a zaslat nový QWAC certifikát společně s popisem chyby.

6 KONTAKTY

V případě jakýchkoliv dotazů se na nás můžete obrátit na adrese **api@fio.cz**

7 ZNÁMÉ CHYBY

7.1 SSL error 48

Při dotazech nepoužíváte plný SSL client certificate chain.

8 ZMĚNY VE VERZÍCH DOKUMENTACE

Verze	Datum	Obsah	Změna z	Změna na
1.00	10.06.2019			Vytvoření dokumentu
1.01	22.10.2019	4		Přidání informací o PGP klíči
1.02	29.10.2019	5		Zpřehlednění informací o Endpoints
1.03	30.01.2020	5		Přidání informace o token revoke endpoint

1.04	17.06.2020	7		Přidání sekce Známé chyby
1.1	24.06.2020	5		Doplněna nová pátá sekce Výměna certifikátu
1.2	11.9.2020	4		Nově vyžadujeme celý řetězec certifikátů od QWAC po root CA
1.2	11.9.2020	5	Nadpis: Výměna certifikátu	Test funkčnosti a obnova certifikátu
1.2.	11.9.2020	2,3	Sloučení bodů 2 a 3	Nově je pouze bod 2