# OTEVŘENÉ BANKOVNICTVÍ

Fio banka

**Verze 1.8.4**

## OBSAH


**1 POPIS ..... 3**

**2 REGISTRACE DO SANDBOX PROSTŘEDÍ ..... 4**

2.1 Žádost o přístup do testovacího prostředí ..... 4

2.1.1 Vygenerování vlastního testovacího QWAC PSD2 certifikátu do sandbox prostředí ..... 4

2.1.1.1 Vytvoření certifikátu a soukromý klíč certifikační autority: ..... 4

2.1.1.2 Vytvoření soukromého klíče k budoucímu vlastnímu QWAC PSD2 certifikátu: ..... 4

2.1.1.3 Vytvoření žádosti o certifikát ..... 5

2.1.1.4 Zpracování žádosti o QWAC jako certifikační autorita ..... 6

**3 TESTOVÁNÍ ..... 7**

3.1 Povolení přístupu klienta banky ..... 7

3.2 Výměna authorization code za refresh token a access token ..... 8

3.3 Výměna refresh tokenu za access token ..... 8

3.4 Použití access tokenu pro volání API – AISP ..... 9

3.5 Postup podání pokynu – PISP ..... 13

**4 ŽÁDOST O PŘÍSTUP DO PRODUKČNÍHO PROSTŘEDÍ ..... 15**

**5 PRODUKČNÍ KONCOVÉ BODY (ENDPOINTS) ..... 16**

5.1 Koncové body nad rámec ČOBS standardu ..... 16

5.1.1 Přehled transakcí od ID transakce ..... 16

5.1.2 Ověření planosti certifikátu ..... 17

**6 TEST FUNKČNOSTI A OBNOVA CERTIFIKÁTU ..... 18**

**7 KONTAKTY A HLÁŠENÍ CHYB ..... 19**

**8 ZNÁMÉ CHYBY ..... 20**

8.1 tlsv1 alert unknown ca / SSL alert number 48 ..... 20

8.2 BAD_REQUEST – FIELD INVALID – „productI18N“: „Fio konto“ ..... 20

8.3 Chyba 422 Unprocessable entity ..... 20

8.4 Chyba 400 Error FF01 ..... 20

**9 ZMĚNY VE VERZÍCH DOKUMENTACE ..... 21**

# 1 POPIS

Dokument popisuje postupy, jak se napojit na rozhraní PSD2 API u Fio banky a jaké jsou pro to nutné požadavky. Tento dokument je platný pro Fio banku v České i Slovenské republice.

Produkční prostředí využívá standardu ČOBS ve verzi 4.1.

# 2 REGISTRACE DO SANDBOX PROSTŘEDÍ

Před využitím sandbox rozhraní musíte být zaregistrováni v testovacím prostředí Fio banky. Žádost o přístup se provede odesláním požadavku na email api@fio.cz

## 2.1 Žádost o přístup do testovacího prostředí

Žádající subjekt musí v žádosti přiložit svůj QWAC certifikát. Nemáte-li QWAC certifikát, tak je nutné si jej vytvořit podle postupu 2.1.1

V žádosti uveďte:

Předmět: SANBOX žádost o přístup

Tělo:
Název žádajícího subjektu:

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:
QWAC certifikát ve formátu PEM a včetně jeho nadřízených a mezilehlých certifikátů až k root CA

* Obecná e-mailová adresa sloužící pro technickou komunikaci
** Návratové URL musí být zabezpečený protokol https:// a nemůže být „localhost“.

Podle zaslaných údajů založíme novou třetí stranu do našeho testovacího prostředí a zašleme vám zpět emailem přístupové údaje:

- client id
- client secret
- api key

### 2.1.1 Vygenerování vlastního testovacího QWAC PSD2 certifikátu do sandbox prostředí

Pokud **nejste licencovaný subjekt** a QWAC PSD2 certifikát nevlastníte, tak je možné si vytvořit pro účely testování vlastní certifikát. Podle návodu níže si vytvoříte vlastní certifikační autoritu a vydáte si testovací QWAC PSD2 certifikát sami. Budete k tomu potřebovat openssl software (https://www.openssl.org/)

#### *2.1.1.1 Vytvoření certifikátu a soukromý klíč certifikační autority:*

```
openssl req -x509 -newkey rsa:4096 -keyout ca-key.pem -out ca-cert.pem -days
7300 -nodes
```

Soubor s certifikátem certifikační autority (`ca-cert.pem`) budete zasílat spolu s dále vygenerovaným certifikátem v žádosti o přístup do testovacího prostředí. Bude se také využívat pro jednotlivá volání endpointů, spolu s vlastním certifikátem, který vznikne v dalších krocích.

#### *2.1.1.2 Vytvoření soukromého klíče k budoucímu vlastnímu QWAC PSD2 certifikátu:*

```
openssl genrsa -out dummy.key 4096
```

Soubor se soukromým klíčem (`dummy.key`) také budete následně potřebovat. Nejen k podepsání vlastní žádosti o QWAC PSD2 certifikát, ale i pro jednotlivá volání endpointů.

### 2.1.1.3 Vytvoření žádosti o certifikát

```
openssl req -new -key dummy.key -out dummy.csr -subj
/C=XX/CN=dummy/organizationIdentifier=PSDCZ-TST-123456 -config qc.conf
```

V tomto příkazu je několik klíčových parametrů, které musíte zohlednit:

Subject certifikátu: -subj /C=XX/CN=dummy/organizationIdentifier=PSDCZ-TST-123456 – do položky organizationIdentifier je třeba uvést unikátní hodnotu, kterou dále uvedete v žádosti o přístup do testovacího prostředí (v položce „Identifikátor společnosti získané od národního regulátora:“).

Doporučujeme zadat např. „PSDCZ-TST-vaše IČO“ nebo místo IČO jinou pravděpodobně unikátní hodnotu. Pokud by došlo k duplicitě a vámi zadaná hodnota bude už v testovacím prostředí používána, budeme vás kontaktovat. V takovém případě bude třeba provést generování nového certifikátu.

S ohledem na parametr -config qc.conf je nutné připravit si specifický soubor qc.conf. který bude mít podobu:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = qcStatements

[req_distinguished_name]

[qcStatements]
1.3.6.1.5.5.7.1.3=ASN1:SEQUENCE:qcStatement

[qcStatement]
etsiQcsCompliance=SEQUENCE:etsiQcsCompliance
qcs-QcPDS=SEQUENCE:qcs-QcPDS
id-qc-statement=SEQUENCE:id-qc-statement
qcs-QcType=SEQUENCE:qcs-QcType
[etsiQcsCompliance]
statementId=OID:0.4.0.1862.1.1
[qcs-QcPDS]
statementId=OID:0.4.0.1862.1.5
QcPDS-List=SEQUENCE:QcPDS-List
[QcPDS-List]
QcPDS1=SEQUENCE:QcPDS1
[QcPDS1]
url=IA5STRING:https://example.org/pkidisclosure
description=PRINTABLESTRING:example

[id-qc-statement]
statementId=OID:0.4.0.19495.2
statementInfo=SEQUENCE:id-qc-statement-Info
[id-qc-statement-Info]
rolesOfPSP=SEQUENCE:rolesOfPSP
nCAName=UTF8String:Dummy Financial Supervision Authority
nCAId=UTF8String:XX-DFSA
[rolesOfPSP]
PSP_AI=SEQUENCE:PSP_AI
PSP_AS=SEQUENCE:PSP_AS
PSP_PI=SEQUENCE:PSP_PI
PSP_IC=SEQUENCE:PSP_IC
[PSP_AI]
```

```
roleOfPspOid=OID:0.4.0.19495.1.3
roleOfPspName=UTF8String:PSP_AI
[PSP_AS]
roleOfPspOid=OID:0.4.0.19495.1.1
roleOfPspName=UTF8String:PSP_AS
[PSP_PI]
roleOfPspOid=OID:0.4.0.19495.1.2
roleOfPspName=UTF8String:PSP_PI
[PSP_IC]
roleOfPspOid=OID:0.4.0.19495.1.4
roleOfPspName=UTF8String:PSP_IC
[qcs-QcType]
statementId=OID:0.4.0.1862.1.6
statementInfo=SEQUENCE:qcs-QcType-Info
[qcs-QcType-Info]
qct-esign=OID:0.4.0.1862.1.6.1
qct-eseal=OID:0.4.0.1862.1.6.2
qct-web=OID:0.4.0.1862.1.6.3
```

To zajistí, že certifikát bude obsahovat vyplněné všechny role PSP – AISP, PISP i CISP a bude tedy možné testovat všechny funkčnosti. V tomto kroku můžete narazit na problém, že dostanete chybu „Subject Attribute organizationIdentifier has no known NID, skipped“. V takovém případě bude potřeba použít novější verzi openssl (například z aktuálního ubuntu nebo aktuálního cygwin).

#### *2.1.1.4 Zpracování žádosti o QWAC jako certifikační autorita*

```
openssl x509 -req -days 1460 -in dummy.csr -CA ca-cert.pem -CAkey ca-key.pem -
CAcreateserial -out dummy.crt -sha256 -extensions qcStatements -extfile qc.conf
```

Tímto získáme soubor dummy.crt s naším testovacím QWAC PSD2 certifikátem.

**Shrnutí, jak získané soubory použít:**

- ca-cert.pem – certifikát root certifikační autority – přiložit do žádosti o přístup do testovacího prostředí jako přílohu.
- dummy.crt – testovací QWAC PSD2 certifikát – přiložit do žádosti o přístup do testovacího prostředí jako přílohu. Bude také potřeba pro jednotlivá volání endpointů.
- dummy.key – soukromý klíč k testovacímu QWAC PSD2 certifikátu – dobře si uschovat, bude potřeba pro jednotlivá volání endpointů.

Ostatní vytvořené soubory už pro další práci s testovacím PSD2 API nebudeme potřebovat. Budou se samozřejmě hodit, pokud bychom někdy potřebovali generovat další certifikát.

Důležitá je ještě hodnota

- **organizationIdentifier** z kroku 3.

Ta se použije v žádosti o přístup do testovacího prostředí, kde ji uvedete do položky „Identifikátor společnosti získané od národního regulátora“.

# 3 TESTOVÁNÍ

Po potvrzení o zavedení do testovacího prostředí je možné zahájit testování. E-mailem obdržíte přístupové údaje pro sandbox prostředí:

- client id
- client secret
- api key

## 3.1 Povolení přístupu klienta banky

Zaregistrovaná třetí strana do testovacího prostředí si musí vyžádat souhlas klienta (PSU) s přístupem k bankovním účtům prostřednictvím GET požadavku:

https://developers.fio.cz/api/cz/v2/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 autentikace, musí odpovídat jedné z hodnot vyplněné při registraci TPP |
| state | libovolný řetězec definovaný 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/v2/oauth/auth?response_type=code&client_id=Q1pfXzAzYmQ3N2U0LWE2NTQtNDJjOC04NGM4LWVjNmViMDk2Y2U4OQ%3D%3D&redirect_uri=https%3A%2F%2Fdevelopers.fio.cz%2Fwebjars%2Fspringfox-swagger-ui%2Foauth2-redirect.html&state=tpp_special_value&scope=aisp+cisp+pisp
```

Po vyplnění přihlašovacích údajů klienta banky (dostupné v další kapitole, reprezentuje 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
```

**Klienti v testovacím prostředí**

| **Login:** | **Heslo:** |
|---|---|
| psd_novak | Heslo001 |
| psd_tvolny | Heslo001 |
| psd_ticha | Heslo001 |
| psd_bernolakova | Heslo001 |

Tyto osoby jsou specificky nakonfigurované, aby nebyl při SCA vyžadován druhý faktor (autorizace pomocí mobilní aplikace či SMS), protože realizovat druhý faktor v testovacím prostředí by bylo nepraktické.

## 3.2 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/v2/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 --cert ./muj_certifikat.pem --key ./klic.key -X POST -H
'Content-Type: application/x-www-form-urlencoded' -d
'grant_type=authorization_code&client_id=Q1pfXzAzYmQ3N2U0LWE2NTQtNDJjOC04NGM4L
WVjNmViMDk2Y2U4OQ%3D%3D&client_secret=M2Q1YzJhNmEtZTg5ZS00Y2VkLWFjMzUtYmVjYjJk
MGJmZTQz&redirect_uri=https%3A%2F%2Fdevelopers.fio.cz%2Fwebjars%2Fspringfox-
swagger-ui%2Foauth2-
redirect.html&code=XBgCUQiWwR3v8sEHsacS4Oyp4Uu7otnNo7Gt81lTEQE%3D'
https://developers.fio.cz/api/cz/v2/oauth/token
```

Výstup:

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

Vydané refresh tokeny mají platnost 180 dní. V "refresh_expires_in" tedy u nového refresh tokenu přijde hodnota 15552000.

## 3.3 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/v2/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 registrace |
| 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 --cert ./muj_certifikat.pem --key ./klic.key -X POST -H
'Content-Type: application/x-www-form-urlencoded' -d
'grant_type=refresh_token&client_id=Q1pfXzAzYmQ3N2U0LWE2NTQtNDJjOC04NGM4LWVjNm
ViMDk2Y2U4OQ%3D%3D&client_secret=M2Q1YzJhNmEtZTg5ZS00Y2VkLWFjMzUtYmVjYjJkMGJmZ
TQz&refresh_token=YWIyNjI5MmYtYzNjOC00ZGNkLWFjOGEtMjEzMzQ1ODU4MTU2'
https://developers.fio.cz/api/cz/v2/oauth/token
```

## 3.4 Použití access tokenu pro volání API – AISP

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

Authorization: Bearer {access_token}

Příklad:

```
curl --insecure --cert ./muj_certifikat.pem --key ./klic.key -H
"Authorization: Bearer Y2FjNTI0NjYtYjY3NS00NTg4LWE2NjItNTBjZmFiM2M1MmVj"
https://developers.fio.cz/api/cz/v2/accounts
```

Výstup:

```
{
"pageNumber":0,
"pageCount":1,
"pageSize":2,
"totalCount":2,
"accounts":[
  {
    "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"
  }]
}
```


Jako další příklad uvádíme endpoint pro získání zůstatku: https://developers.fio.cz/api/cz/v2/accounts/{id}/balance. Hodnotu {id} v tomto případě získáme z jednotlivých položek accounts.id z odpovědi na dotaz na seznam účtů (https://developers.fio.cz/api/cz/v2/accounts). Pro získání zůstatku jednoho z účtů z předchozího příkladu se zavolá https://developers.fio.cz/api/cz/v2/accounts/1/balance nebo https://developers.fio.cz/api/cz/v2/accounts/2/balance (id je obvykle desetimístné číslo).

Příklad:

```
curl --header 'Authorization: Bearer
.oaCOnzCaYrF3xsL.y3yQ7xPl/qqxyA30h0NRgXeWWWE2ozB5q' --cert ./dummy.crt --key
./dummy.key --insecure --request GET
'https://developers.fio.cz/api/cz/v2/accounts/2400862979/balance'
```

Výstup:


```
{
    "balances": [
        {
            "type": {
                "codeOrProprietary": {
                    "code": "CLAV"
                }
            },
            "amount": {
                "value": 5916774.2200,
                "currency": "CZK"
            },
            "creditDebitIndicator": "CRDT",
            "date": {
                "dateTime": "2022-01-17T13:56:50.322+01:00"
            }
        },
        {
            "type": {
                "codeOrProprietary": {
                    "code": "CLBD"
                }
```

```
            },
            "amount": {
                "value": 5916874.2200,
                "currency": "CZK"
            },
            "creditDebitIndicator": "CRDT",
            "date": {
                "dateTime": "2022-01-17T13:56:50.322+01:00"
            }
        }
    ]
}
```


ČOBS standard rozeznává 4 typy zůstatků, takže položka type.codeOrProprietary.code může mít tyto hodnoty:

- CLAV ClosingAvailable - Available balance
- PRCD PreviouslyClosedBooked - Opening balance
- CLBD ClosingBooked - Closing balance
- ITBD InterimBooked - Intermediate balance

V současné době zobrazujeme pouze zůstatky typu CLAV a CLBD.

Při získávání přehledu transakcí mohou nastat dvě rozdílné situace. Rozhodující je hodnota fromDate v requestu. Např:

```
curl --location 'https://developers.fio.cz/api/cz/v2/accounts/2400862979/transactions?fromDate=2022-01-01&toDate=2022-12-31' --header 'Authorization: Bearer SIX9a XT2uSYpAcZCPDZCEYH9NH06k/XxpvQvg3pkcRwGHDGoLKQ7OHNFLKOvBhxdkqdV5JOKgIObE9ECE IYLJIrJClzoO/8RwoAf' --cert ./dummy.crt --key ./dummy.key
```

Pokud je hodnota fromDate méně jak 90 dní v minulosti (to platí i pokud není uvedena vůbec, v takovém případě se použije dnešní datum), odpověď přijde bez dalšího ověření a vypadá např takto:


```
{
    "pageNumber": 0,
    "pageCount": 1,
    "pageSize": 141,
    "totalCount": 141,
    "transactions": [
        {
            "entryReference": "15795914962",
            "amount": {
                "value": 4742.99,
                "currency": "CZK"
            },
            "creditDebitIndicator": "DBIT",
            "reversalIndicator": false,
            "status": "BOOK",
            "bookingDate": {
                "date": "2022-12-23T00:00:00.000+01:00"
            },
            "valueDate": {
                "date": "2022-12-23T00:00:00.000+01:00"
            },
            "bankTransactionCode": {
                "proprietary": {
```

```
                    "code": "10000101000",
                    "issuer": "CBA"
                }
            },
            "entryDetails": {
                "transactionDetails": {
                    "references": {
                        "instructionIdentification": "d5e888a2-9b9f-44f5-8a90-
8d5c7bb76cf",
                        "endToEndIdentification": "/VS/511833641/SS//KS/0308"
                    },
                    "amountDetails": {
                        "instructedAmount": {
                            "amount": {
                                "value": 4742.99,
                                "currency": "CZK"
                            }
                        }
                    },
                    "relatedParties": {
                        "creditorAccount": {
                            "identification": {
                                "other": {
                                    "identification": "2300427152/2010"
                                }
                            }
                        }
                    },
                    "relatedAgents": {
                        "creditorAgent": {
                            "financialInstitutionIdentification": {
                                "clearingSystemMemberIdentification": {
                                    "memberIdentification": "2010"
                                }
                            }
                        }
                    },
                    "remittanceInformation": {
                        "unstructured": "5d81c7b7942c469998ced548a401a85a",
                        "structured": {
                            "creditorReferenceInformation": {
                                "reference": [
                                    "VS:511833641",
                                    "KS:0308"
                                ]
                            }
                        }
                    },
                    "additionalRemittanceInformation": "5d81c7b7942c469998ced548a401a85a"
                }
            }
        },
```

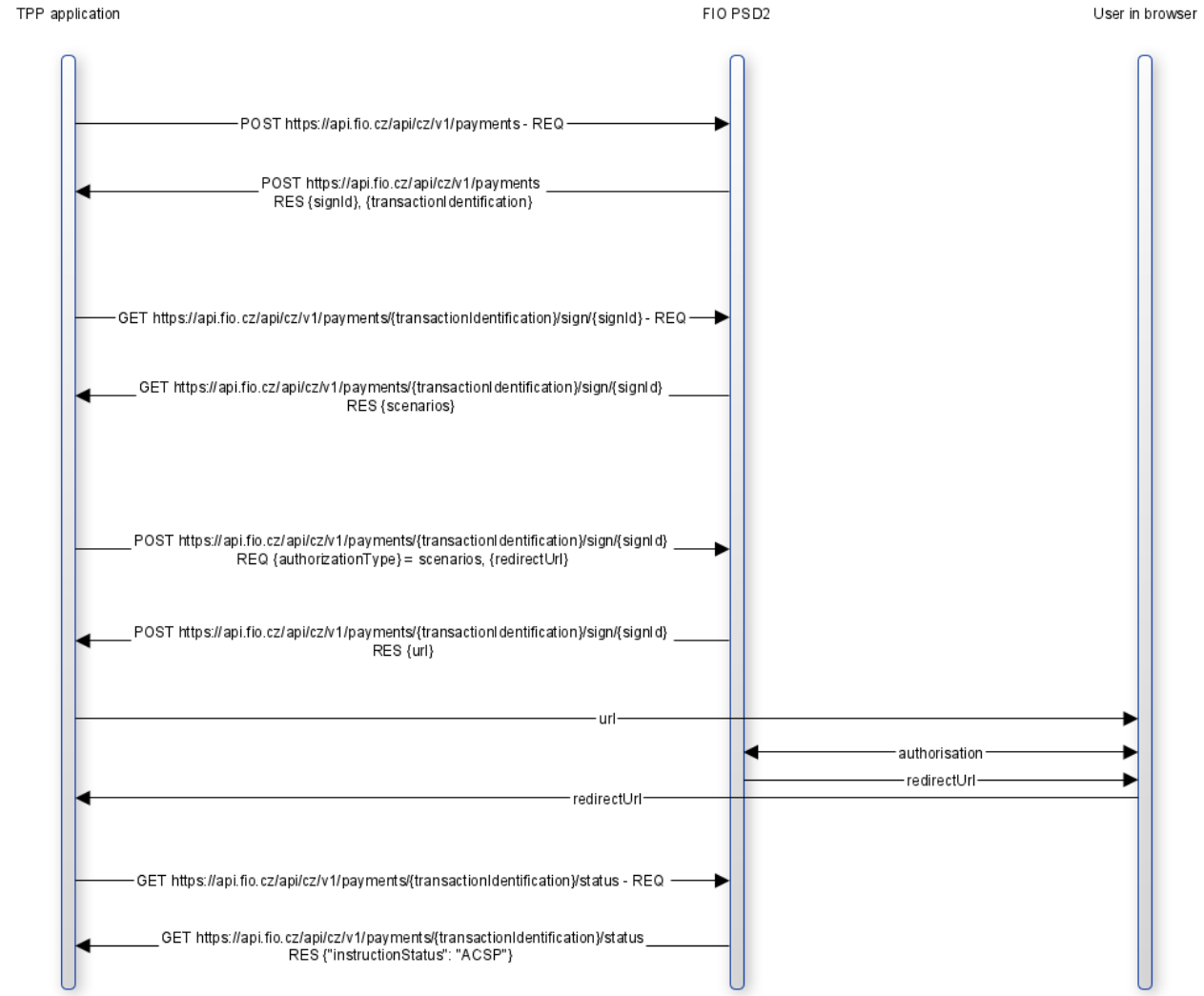
Pokud je však fromDate více jak 90 dní v minulosti, přijde nejdříve chyba 422. V takovém případě je klient upozorněn, že mu nemůžeme poskytnout data ke zvolenému období. Omezení a nezbytnost silné autorizace podléhá platné legislativě EU 2018/389, Kapitola III, Článek 10.
Pro poskytnutí dat je potřeba použít nový refresh token vygenerovaný z jednorázového code viz bod 3.2 Výměna authorization code za refresh token a access token

Platnost silného ověření (SCA) je 5 minut od vzniku refresh tokenu. Během této doby je možné získat transakční historii starší 90 dní. Poté je třeba proces opakovat a znovu vygenerovat refresh token.

Pro získávání informací o pohybech na účtu platí omezení, že v odpovědi na jeden dotaz (bez ohledu na stránkování) je možné vrátit maximálně 10 000 pohybů. Pro jednodušší (postupné) získávání většího množství pohybů je možné využít endpoint accounts/{id}/transactionsFromEntryReference popsaný v kapitole 5.1.1.

## 3.5 Postup podání pokynu – PISP

Volání endpointů pro podání pokynu probíhá v tomto pořadí:




Aplikace třetí strany odešle data o požadované platbě pomocí POST na endpoint https://api.fio.cz/api/cz/v2/payments. Zpět se v odpovědi vrátí doplněná data o platbě. Pro další použití jsou důležité tyto hodnoty:

- signId (ve skupině signInfo) – jeho hodnota se v dalších voláních používá v url a identifikuje konkrétní podepisování
- transactionIdentification (ve skupině paymentIdentification) - jeho hodnota se v dalších voláních používá v url a identifikuje konkrétní platbu

Následně aplikace třetí strany zjistí stav platby a použitelný autorizační scénář pomocí GET na endpoint https://api.fio.cz/api/cz/v2/payments/{transactionIdentification}/sign/{signId}. Pokud nedojde k chybě, je odpověď v této fázi procesu vždy v této podobě:

```
{
  "scenarios": [
    "USERAGENT_REDIRECT"
  ],
  "signInfo": {
    "signId": "string s hodnotou {signId}",
    "state": "OPEN"
  }
}
```

Hodnotu z položky scenarios (tedy řetězec USERAGENT_REDIRECT) pak následně aplikace třetí strany použije ve svém POST requestu na https://api.fio.cz/api/cz/v2/payments/{transactionIdentification}/sign/{signId}, kde ji vloží do položky authorizationType. V tomto requestu je také nutné specifikovat redirectUrl, kam bude uživatel přesměrován poté, co dokončí autorizaci. Request tedy vypadá například takto:

```
{
  "authorizationType": "USERAGENT_REDIRECT",
  "redirectUrl": "https://ourtppaplication.com/return-from-auth-example-url"
}
```

V odpovědi na tento request je vrácena url, kam má být uživatel přesměrován, aby mohl platbu autorizovat:

```
{
  "authorizationType": "USERAGENT_REDIRECT",
  "href": {
    "url": "https://api.fio.cz/example-url-for-auth"
  },
  "signInfo": {
    "signId": "string s hodnotou {signId}",
    "state": "OPEN"
  }
}
```

Aplikace třetí strany tedy uživatele přesměruje na tuto adresu (hodnota url), uživatel tam provede autorizaci a poté je vrácen zpět do aplikace třetí strany na url specifikovanou v hodnotě redirectUrl z requestu.

Poté už zbývá jen ověřit stav platby pomocí GET na endpoint https://api.fio.cz/api/cz/v2/payments/{transactionIdentification}/status. Na tento request se vrátí jednoduchá odpověď v této podobě:

```
{
  "instructionStatus": "ACSP"
}
```

Položka instructionStatus může mít tyto hodnoty:

- ACTC – platba čeká na autorizaci nebo autorizace právě probíhá
- ACSP – platba byla úspěšně autorizována, finální stav
- RJCT – platba byla odmítnuta nebo došlo k chybě, finální stav

# 4 ŽÁDOST O PŘÍSTUP DO PRODUKČNÍHO PROSTŘEDÍ

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

V žádosti uveďte:
Předmět: PSD2 API – žádost o přístup – produkční prostředí

Tělo:
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 a mezilehlých certifikátů až k root CA.

* Obecná e-mailová adresa sloužící pro technickou komunikaci
** Návratové URL musí být zabezpečený protokol https:// a nemůže být „localhost“.

# 5 PRODUKČNÍ KONCOVÉ BODY (ENDPOINTS)

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

Verze v2 odpovídá specifikaci ČOBS 4.1

| |
|---|
| **AISP endpoints:** |
| https://api.fio.cz/api/cz/v2/accounts |
| https://api.fio.cz/api/cz/v2/accounts/balance |
| https://api.fio.cz/api/cz/v2/accounts/{id}/transactions |
| https://api.fio.cz/api/cz/v2/accounts/{id}/transactionsFromEntryReference |
| **CISP endpoints:** |
| https://api.fio.cz/api/cz/v2/accounts/balanceCheck |
| **PISP endpoints:** |
| https://api.fio.cz/api/cz/v2/batchpayments |
| https://api.fio.cz/api/cz/v2/batchpayments/{transactionIdentification} |
| https://api.fio.cz/api/cz/v2/batchpayments/{transactionIdentification}/sign/{signId} |
| https://api.fio.cz/api/cz/v2/batchpayments/{transactionIdentification}/status |
| https://api.fio.cz/api/cz/v2/payments |
| https://api.fio.cz/api/cz/v2/payments/balanceCheck |
| https://api.fio.cz/api/cz/v2/payments/{id} |
| https://api.fio.cz/api/cz/v2/payments/{id}/sign/{signId} |
| https://api.fio.cz/api/cz/v2/payments/{id}/status |
| https://api.fio.cz/api/cz/v2/standingorders |
| https://api.fio.cz/api/cz/v2/standingorders/{transactionIdentification} |
| https://api.fio.cz/api/cz/v2/standingorders/{transactionIdentification}/sign/{signId} |
| https://api.fio.cz/api/cz/v2/standingorders/{transactionIdentification}/status |
| **Auth endpoints:** |
| https://api.fio.cz/api/cz/v2/oauth/auth |
| **Token endpoints:** |
| https://api.fio.cz/api/cz/v2/oauth/token |
| **Token revoke endpoint:** |
| https://api.fio.cz/api/cz/v2/oauth/revoke |
| **Connection test controller** |
| https://api.fio.cz/api/cz/v2/test |

## 5.1 Koncové body nad rámec ČOBS standardu

### 5.1.1 Přehled transakcí od ID transakce

Endpoint https://api.fio.cz/api/cz/v2/accounts/{id}/transactionsFromEntryReference se použiteje pro získávání nových pohybů na účtu od posledního stažení nebo k postupnému získání velkého množství pohybů. Jde také o praktický způsob, jak získat informace o pohybech na účtu, když za jeden den proběhlo více > 10 000 pohybů. V odpovědi na GET požadavek se vrací všechny pohyby, které se na účtu odehrály po pohybu, jehož entryReference zašlete na vstupu.
V odpovědi na dotaz vrací tento endpoint všechny pohyby na účtu s vyšším entryReference než je entryReference zaslané v dotazu jako parametr (např. takto: /accounts/{{account_id}}/transactionsFromEntryReference?entryReference=49937000157). Vrací pouze zaúčtované pohyby, v odpovědi tedy nebudou například dosud nezaúčtované karetní transakce. Pokud je mezi vracenými pohyby nějaký pohyb starší 90 dnů, je vyžadováno SCA, pokud jsou všechny pohyby staré 90 dní nebo méně, SCA vyžadováno není.

Hlavní odlišností proti endpointu /transactions, který vrací transakce podle data je to, že pokud je výsledkem dotazu více jak 10 000 transakcí, nevrátí se chyba, ale prvních 10 000 transakcí z výsledku. V odpovědi tedy

získáme novou hodnotu „posledního“ entryReference a můžeme pokračovat v získávání dat novým dotazem. Takto pokračujeme, dokud v položce totalCount nepřijde hodnota nižší než 10 000. To značí, že už jsme se dostali na konec a žádné novější pohyby na účtu aktuálně nejsou. Ve výchozím stavu jsou jednotlivé pohyby řazené za sebou právě podle entryReference vzestupně, nejnovější pohyb je tedy v odpovědi poslední.

Tento endpoint je také možné využít ke stahování pouze nových pohybů od posledního stažení. Pomocí volání, když jako hodnotu parametru entry\Reference zadáme 0 (/accounts/{{account_id}}/transactionsFromEntryReference?entryReference=0) získáme aktuálně poslední pohyb na účtu. Následně pak můžeme ve zvolené periodě provést vždy volání s posledním získaným entryReference a tak stahovat pouze nové pohyby.

Výjimečně mohou nastat situace, kdy pohyb s vyšším entryReference časově předchází pohyb s nižším entryReference, Jedná se zejména o různé opravné pohyby.

GET
https://developers.fio.cz/api/cz/v2/accounts/{{account_id}}/transactionsFromEntryReference?entryReference={{entryReference}}

Vstupy:

| | |
|---|---|
| account_id | Identifikátor účtu – číslo účtu ve formátu BBAN bez kódu banky |
| entryReference | Identifikátor platby (na výstupu zde a u /transactions endpointu k dispozici pro každý pohyb v poli entryReference). V případě že je použita hodnota 0, vrací se ve výstupu poslední (právě jeden) pohyb na účtu. Při použití konkrétního entryReference ve výstupu přijdou všechny pohyby s vyšším entryReference. Pokud tedy pošleme entryReference aktuálně posledního pohybu, v odpovědi žádný pohyb nebude. |

### 5.1.2 Ověření planosti certifikátu

Endpoint https://api.fio.cz/api/cz/v2/test sloužící k otestování platnosti obnoveného QWAC certifikátů více viz bod 6.

# 6 TEST FUNKČNOSTI A OBNOVA CERTIFIKÁTU

Obnovené certifikáty QWAC se musí nahrát do registru pro kontrolou jejich platnosti podle prostředí. Celý řetězec certifikátů od QWAC včetně mezilehlého až po root CA nahrajte zde:
Produkční prostředí – https://developers.fio.cz/upload/

Každý QWAC certifikát má dobu platnosti. Minimálně 15 dní před vypršením certifikátu doporučujeme obnovený certifikát řádně otestovat, jestli komunikace mezi třetí stranou a Fio bankou nepřestane fungovat. Pro zajištění bezproblémové komunikace, před nasazením QWAC certifikátu na produkčních serverech třetí strany, jsme umožnili ověřit funkčnost obnoveného QWAC certifikátu na endpointu https://api.fio.cz/api/cz/v2/test.

```
curl --insecure --cert muj_certifikat.pem –key klic.key -X GET
„https://api.fio.cz/api/cz/v2/test“ -H „accept: application/json“
```

Vrátí-li endpoint stejný identifikátor společnosti (OrganizationIdentifier) stejný jako v původním certifikátu, tak není potřeba kontaktovat Fio banku pro výměnu certifikátu. Výměnu certifikátu je 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.

# 7 KONTAKTY A HLÁŠENÍ CHYB

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

Pro správné vyřízení nahlášených chyb je potřeba uvést co nejvíce informací, které nám pomohou s jejich vyhodnocením a opravou.

Hlášení chyb by mělo ideálně obsahovat:

- Datum a čas provedeného volání
- Přepis JSON volání
- Chyba a její podrobný popis
- Screenshot chyby
- Další relevantní informace vztahující se k chybě, jejímu vzniku a co jí předcházelo

# 8 ZNÁMÉ CHYBY

## 8.1 tlsv1 alert unknown ca / SSL alert number 48

Volání neobsahuje QWAC certifikát ve formátu PEM včetně jeho nadřízených a mezilehlých certifikátů až k root CA viz bod 4 Žádost o přístup do produkčního prostředí

## 8.2 BAD_REQUEST – FIELD INVALID – „productI18N“: „Fio konto“

Pro účty typu Fio konto je zavedeno omezení a prostředky je možné posílat pouze na jiné účty stejného vlastníka nebo na nastavený cílový účet. Na jiné účty není možné provádět platby a při pokusu přijde jedna z těchto chyb:

- „Zadaný účet příjemce neodpovídá aktuálně nastavenému povolenému externímu cílovému účtu.“
- „Pro zvolený spořící účet není k datu platby zadán povolený cílový účet.“

Více zde https://www.fio.cz/docs/cz/OP_FB_ramcova_smlouva.pdf článek VI. – B spořící účty

## 8.3 Chyba 422 Unprocessable entity

Klient se dožaduje dat starších víc než 90dní bez silné autorizace viz bod 3.4 Použití access tokenu pro volání API – AISP

## 8.4 Chyba 400 Error FF01

Neplatný formát JSON nebo jiný technický problém se zpracováním dotazu. Příklady správných formátů JSON naleznete v aktuální dokumentaci ČOBS viz bod 1 Popis

# 9 ZMĚNY VE VERZÍCH DOKUMENTACE

| Verze | Datum | Obsah | Změna z | Změna na |
|---|---|---|---|---|
| 1.00 | 10.6.2019 | | | 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 | 30.1.2020 | 5 | | Přidání informace o token revoke endpoint |
| 1.04 | 17.6.2020 | 7 | | Přidání sekce Známé chyby |
| 1.1 | 24.6.2020 | 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 |
| 1.3. | 30.6.2021 | 4 | | Doplnění endpointů v2 |
| 1.4. | 24.8.2021 | 2.5 | | Přidání nového kapitoly Postup podání pokynu – PISP |
| 1.5. | 20.12. 2021 | 2.1,2.2,2.3.,2.4 | | Nový způsob registrace do sandboxu |
| 1.6 | 17.1. 2022 | 3.1, 3.4 | | Přidání dalších klientů v testovacím prostředí, další příklad pro AISP |
| 1.7 | 22.5. 2023 | 3.2, 3.4, 5, 8 | | Prodloužení platnosti refresh tokenu. SCA pro informace o transakcích starších 90 dní. Dostupnost v1 endpointů do konce roku 2023 |
| 1.7.1 | 13.7.2023 | 3.4 | | Doplnění autorizačních kroků |
| 1.8 | 6.9.2023 | 2.1, 3.4, 3.5, 4, 8.1, 8.2, 8.3, | | Doplnění „mezilehlých“ certifikátů do definic. Úprava definic 8.1 a 8.2, nová známá chyba |
| 1.8.1 | 9.1.2024 | 2.1, 3.4, 4, 6, 7, 8.4 | | Podmínky návratového URL, úprava SCA, doplnění kontroly platnosti QWAC, hlášení chyb, nová známá chyba |
| 1.8.2 | 19.3.2024 | 5 | | Odstranění endpointů v1 |
| 1.8.3 | 19.9.2024 | 6 | | Změna data pro zneplatnění neregistrovaných certifikátů na 13.1.2025 |
| 1.8.4 | 27.2. 2025 | 3.4, 5, 5.1 | | Doplnění chování pro stažení transakční historie nad 10 000 pohybů za den<br>Aktualizace endpointů<br>Přidání popisu endpointu transactionsFromEntryReference |