



# FORTIPAY OPENBANKING API

DOKUMENTACE ROZHRANÍ KE SLUŽBÁM FORTIPAY OPENBANKING API

**FORTISSIMO, spol. s r.o.**  
Lidická 1264, 739 61 Třinec

Telefon: +420 558 330 000  
E-mail: [info@devizy.cz](mailto:info@devizy.cz)  
Web: [www.devizy.cz](http://www.devizy.cz)

**OBSAH**

Úvod .....	3
Bezpečnost .....	4
Bezpečnostní klíč .....	4
Udělení souhlasu .....	5
Služby FortiPay OpenBanking API .....	6
Registrace aplikace třetí strany .....	6
Oprávnění .....	7
Autorizace transakcí .....	8
Ošetření chyb .....	9
Deklarované chyby .....	9
Neočekávané chyby .....	9
Bezpečnostní chyby .....	9
Chyby autorizace transakce .....	9

## ÚVOD

Rozhraní FortiPay OpenBanking API (dále jen „API“) poskytuje přístup k rozhraní služeb spojených s klientskými účty a jejich transakcemi vedenými u platební instituce Fortissimo v souladu se směrnicí Evropské unie o platebních službách PSD2.

Cílem API je zvýšení možností správy účtů a otevření brány vývojářům třetích stran.

Služby dostupné dle PSD2:

- získání informace o aktuálním zůstatku na účtu
- nahlédnutí na pohyby na účtu
- zadání odchozí platby

## BEZPEČNOST

Bezpečnost otevřeného bankovníctví je ošetřena regulatorními technickými standardy (RTS), které jsou zaměřeny na silné ověření klientů. Definují oblasti jako je zabezpečení, autentizace, výměna informací či metodická spolupráce v oblasti dohledu či komunikace s centrálním elektronickým registrem.

API poskytuje online služby dostupné na internetu přes zabezpečený protokol HTTPS. Komunikace proto mezi klientským systémem a API vyžaduje zabezpečení pomocí SSL protokolu s minimálně 128 bitovým šifrováním. Konkrétně je požadována vzájemná (two-way) SSL autentizace a pro navázání spojení musí klientská aplikace použít kvalifikovaný certifikát pro autentizaci webových serverů (QWAC) nebo elektronickou pečeť (QSEAL) dle eIDAS.

## BEZPEČNOSTNÍ KLÍČ

Bezpečnostní model pro přístup k API je založený na protokolu OAuth2. Bezpečnostní klíč vzniká udělením souhlasu uživatelem v procesu, kdy je uživatel přesměrován z partnerské aplikace do internetového bankovníctví ePay24, kde se přihlásí, udělí souhlas, který autorizuje bezpečnostním prvkem a následně je přesměrován zpět do aplikace partnera.

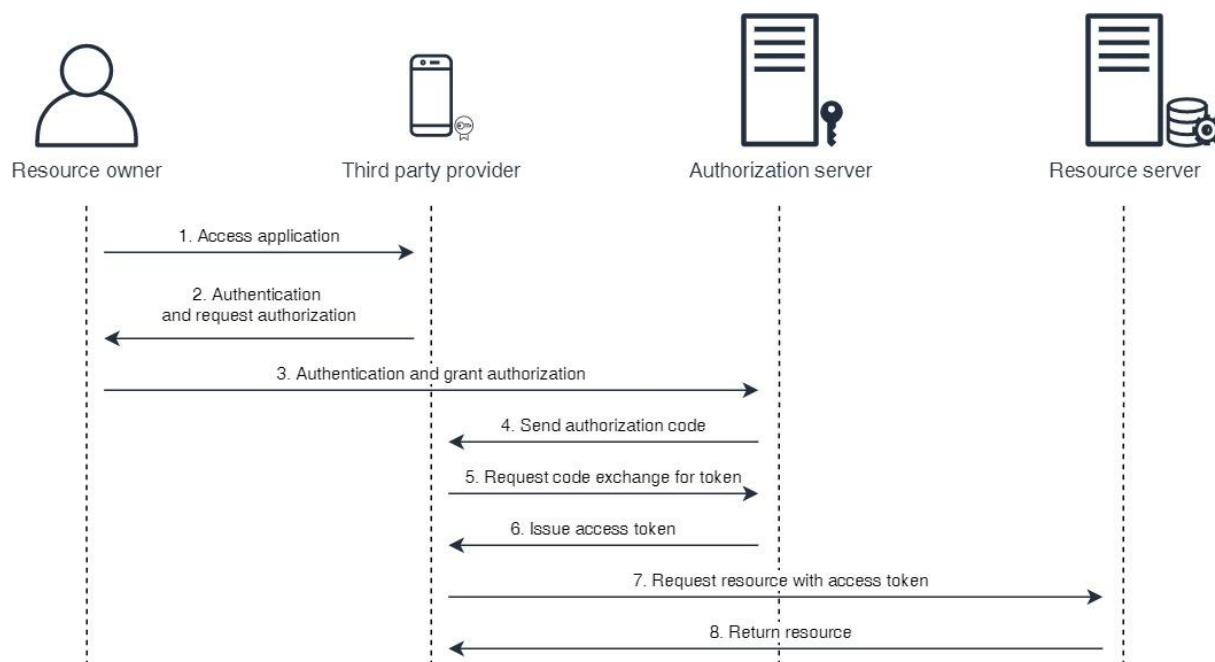
API poskytuje dle OAuth2 specifikace následující endpointy:

- <https://www.epay24.eu/OAuth2Authorize> - vytvoření souhlasu přístupu k API
- <https://www.epay24.eu/OAuth2Token> - generování bezpečnostního klíče (access a refresh token)
- <https://www.epay24.eu/OAuth2Revoke> - zneplatnění bezpečnostního klíče

Požadavek na udělení souhlasu musí obsahovat požadované OAuth2 oprávnění (scope).

Schéma udělení souhlasu a vygenerování klíče pomocí OAuth2 autorizačního kódu.

Komunikace probíhá dle internetového standardu RFC 6749 (viz. <https://tools.ietf.org/html/rfc6749>).



Obrázek 1 - Bezpečnostní klíč – sekvenční diagram získání bezpečnostního klíče

## UDĚLENÍ SOUHLASU

Aby aplikace třetí strany měla přístup k datům uživatele, musí uživatel této aplikaci udělit souhlas spolu s rozsahem oprávnění ke správě jeho účtů a plateb.

1. Aplikace uživatele přeměruje do internetového prohlížeče s potřebnými parametry dle standardu OAuth2 (id aplikace, návratová url do aplikace, požadovaná oprávnění).
2. Pokud uživatel není v prohlížeči přihlášen ke svému Fortissimo účtu, je vyzván k přihlášení. Pro přihlášení je uživatel vyzván k zadání autorizačního SMS kódu, jako je tomu u přihlášení do ePay24. V případě, že uživatel byl již přihlášen, pokračuje rovnou bodem 3.

Obrázek 2 - Přihlášení

Obrázek 3 - Zadání autorizačního SMS kódu

3. Uživatel bude vyzván ke kontrole údajů a aplikace, které zvolené oprávnění povoluje. Úroveň oprávnění může uživatel v seznamu změnit.

Obrázek 4 - Kontrola a přidělení oprávnění aplikaci

4. Stisknutím tlačítka „Povolit“ uživatel dává svolení k přístupu aplikací třetí strany ke svým účtům či platbám.

### Kdy probíhá proces udělení oprávnění?

Oprávnění se aplikaci třetí strany uděluje při prvním přihlášení uživatele nebo v případě vypršení platnosti či zneplatnění bezpečnostního klíče.

## SLUŽBY FORTIPAY OPENBANKING API

Technický popis služeb poskytovaných v rámci API je dostupný online na adrese <https://connect.epay24.eu/specs/openbanking/v1/ui/index>.

Základní adresa pro připojení k rozhraní  
<https://connect.epay24.eu/api/openbanking>

Základní adresa pro připojení k testovacímu rozhraní  
<https://connect.epay24.eu/sandbox/api/openbanking>

Třetí strana, která chce využívat služeb FortiPay OpenBanking API rozhraní, musí mít platnou licenci od národního regulátora a příslušný certifikát. Nutnou podmínkou je také registrace aplikace pomocí API rozhraní, podepsaná příslušným certifikátem.

Při komunikaci s API je nutné každý požadavek podepsat příslušným certifikátem, který byl použit při registraci aplikace. Certifikát je kontrolován na platnost u jeho vydavatele a zároveň jsou kontrolována data určující roli dle směrnice PSD2.

### REGISTRACE APLIKACE TŘETÍ STRANY

Registrace aplikace třetí strany probíhá na příslušném rozhraní služby a její adrese */registration/create*.

Pro volání služby registrace se využívá volání POST požadavku podepsaného příslušným certifikátem spolu s JSON daty v následující struktuře:

Atribut	Datový typ	Popis
<i>Appld</i>	string	Přihlašovací jméno aplikace (client_id)
<i>Password</i>	string	Heslo aplikace (client_secret)
<i>Name</i>	string	Název aplikace
<i>Description</i>	string	Popis aplikace
<i>Email</i>	string	Email (pro potvrzení registrace, kontakt administrátorů)
<i>PhoneNumber</i>	string	Telefonní číslo (pro kontakt administrátorů)

Po úspěšné registraci bude na uvedený email položky *Email* zaslaná zpráva s odkazem pro potvrzení registrace aplikace.

#### *Změna certifikátu aplikace*

Změnu certifikátu při vypršení nebo zneplatnění předchozího, je možné provést pomocí volání POST požadavku podepsaného novým certifikátem na adrese */registration/certificate*.

Atribut	Datový typ	Popis
<i>Appld</i>	string	Přihlašovací jméno aplikace (client_id)
<i>Password</i>	string	Heslo aplikace (client_secret)
<i>PreviousCertificatePEM</i>	base64	Předchozí certifikát (formát PEM)

## OPRÁVNĚNÍ

Aplikace třetí strany si vždy vyžádá rozsah potřebných oprávnění a klient při udělení souhlasu oprávnění může tuto sadu omezit.

Při udělení souhlasu je možné aplikaci přidělit tato oprávnění:

- Získání informací o účtech (product\_info)
- Získání informací o zůstatcích (balance\_info)
- Přístup do historie transakcí (transaction\_info)
- Možnost realizace platby (payment)

Dané oprávnění se aplikuje na veškeré účty klienta pro danou aplikaci třetí strany. Dále s daným oprávněním je svázána skupina služeb, které tuto oblast obsluhují.

Popis služby	Oprávnění	Adresa služby
Získání informací o účtech	product_info	GET /aisp/account/list
Získání informací o zůstatku	balance_info	GET /aisp/account/balance/get
Ověření zůstatku na účtu	balance_info	GET /pisp/account/balance/check
Získání historie transakcí	transaction_info	GET /aisp/account/transaction/list
Ověření stavu platby	payment	GET /pisp/payment/status/get
Vytvoření domácí platby	payment	POST /pisp/payment/domestic/create
Vytvoření zahraniční platby	payment	POST /pisp/payment/foreign/create
Vytvoření SEPA platby	payment	POST /pisp/payment/sepa/create

Tabulka 1 - Dostupné služby

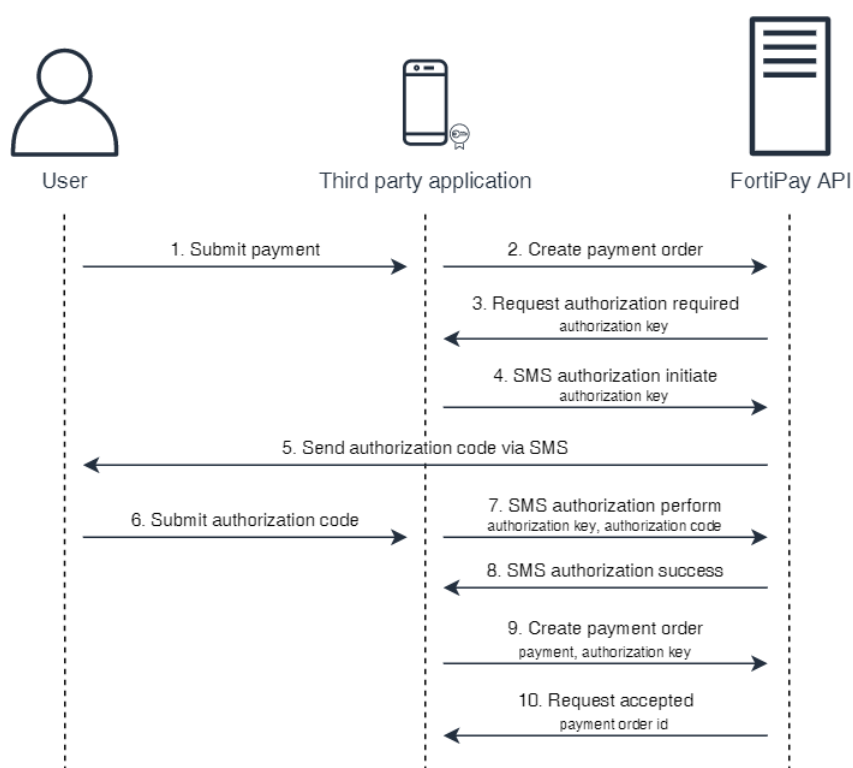
## AUTORIZACE TRANSAKČÍ

Každý požadavek na API vyžaduje platný access token přidělený v procesu OAuth2 autorizace. Pro zajištění toho, aby bezpečnostní klíč aplikace třetí strany nezneužila, je v některých případech nutné ověřit, že daný požadavek je vygenerován na popud uživatelské akce a je vyžádána autorizace pomocí dalšího bezpečnostního prvku – v současné době SMS OTP (One-Time Password).

Principem vytvoření transakce je zaslání požadavku na vytvoření platby aplikací třetí strany, kdy API buď platební příkaz přijme a zpracuje anebo vrátí chybu, ve které popisuje, že vyžaduje další ověření bezpečnostním prvkem. Po úspěšném ověření aplikace opakuje původní požadavek na zadání platby, se kterým odešle i autorizační klíč. Server API ověří platnost autorizačního klíče, zkontroluje, že se zadání platby shoduje s původním požadavkem a příkaz zpracuje. Následující diagram popisuje proces autorizace platby za pomoci SMS OTP.

Specifické operace pro inicializaci bezpečnostního prvku a jeho ověření

- /authorization/smsotp/initiate – odešle jednorázové heslo na autorizační telefonní číslo uživatele
- /authorization/smsotp/perform – ověří jednorázové heslo pro autorizaci



Obrázek 5 - Autorizace transakcí - sekvenci diagram autorizace platby

1. Uživatel potvrdí zadání platby v aplikaci třetí strany
2. Aplikace třetí strany odešle požadavek na založení platebního příkazu
3. Aplikaci třetí strany se vrátí stavový kód 500 s popisem chyby OAM\_TRANSACTION\_AUTHORIZATION\_EXCEPTION obsahující autorizační klíč pro SMS OTP autorizaci
4. Aplikace třetí strany zažádá o autorizaci klíče pomocí SMS OTP a vyzve uživatele k zadání ověřovacího kódu z SMS, která mu v zápětí dorazí
5. Server API odešle uživateli SMS s ověřovacím kódem na autorizační telefonní číslo uživatele
6. Uživatel zadá ověřovací kód z SMS do aplikace třetí strany
7. Aplikace třetí strany odešle autorizační klíč spolu s kódem zadaným uživatelem pro jeho ověření
8. Server API ověří klíč vůči kódu a vrátí výsledek operace
9. Aplikace třetí strany znovu odešle původní platbu nyní spolu s autorizačním klíčem, následně server API zkontroluje, zda platba souhlasí s původním zadáním, zda je autorizační klíč ověřen a založí platební příkaz
10. Aplikace třetí strany přijme identifikaci nově zadané platby



## OŠETŘENÍ CHYB

Přístup k API může mít za následek vyvolání některé z aplikačních chyb:

- Deklarované chyby – specifické chyby definované konkrétní operací služby
- Neočekávané chyby – nedeklarovaná chyba na straně serveru
- Bezpečnostní chyby – neplatný klíč, certifikát, neoprávněný přístup
- Chyby autorizace transakce

### DEKLAROVANÉ CHYBY

Server API vrátí stavový kód 500, v těle odpovědi obsahuje JSON strukturu s chybou. Typický případ je validační chyba - SYS\_VALIDATION\_EXCEPTION, která navíc obsahuje pole s úplným výčtem chyb při validaci.

```
{
  "Name": "SYS_VALIDATION_EXCEPTION",
  "Message": "Validation exception containing (1) errors",
  "ErrorValidationData": [
    {
      "Parameter": "Amount",
      "Message": "Amount is required!"
    }
  ]
}
```

### NEOČEKÁVANÉ CHYBY

Server API vrátí stavový kód 500 a v těle odpovědi JSON strukturu s názvem SYS\_UNEXCEPTED\_EXCEPTION.

```
{
  "Name": "SYS_UNEXCEPTED_EXCEPTION",
  "Message": "Unknown error occurred "
}
```

### BEZPEČNOSTNÍ CHYBY

Server API vrátí stavový kód 401 – Unauthorized.

### CHYBY AUTORIZACE TRANSAKCE

Server API vrátí stavový kód 500 a v těle odpovědi autorizační klíč k platbě se seznamem možností autorizace.

```
{
  "Name": "OAM_TRANSACTION_AUTHORIZATION_EXCEPTION",
  "Message": "Authorization Required",
  "ErrorTransactionAuthorizationData": {
    "AuthorizationKey": "7cdyz6pxhbrsta39jbfxfmsu7mf9s5",
    "AuthorizationMethods": [
      "SMS"
    ]
  }
}
```

V Třinci 5.11.2021