HPB PSD2 API

FAQ

SUMMARY

IMPORTANT!!

We have structured this document in a form of hints whose source was compilation of emails (questions and answers) and arranged them into different categories to help end users find their way around our API and also to help them solve potential problems. Also, important keywords are bolded for better end user experience and faster search.

➢ GENERAL

About HPB API:

- An application programming interface (**API**) is set of protocols for building applications. APIs allow other parties to access data or features of an application over the HTTP protocol using the JSON format
- Product types:
  - ○ AIS
  - ○ PIS (foreign, target2 and sepa)
- Payment services:
  - ○ Periodic
  - ○ Bulk only for sepa payments
- **PSU-ID:**
  - ○ Unique user identifier and it is mandatory field-> it is created through Developer Portal-> in production environment PSU-ID is OIB
  - ○ PSU-ID Type is also mandatory field (customerNumber)
- **Current API version:**
  - ○ v1.3.4.
- Payment cancellation supported for:
  - ○ payments/sepa-credit-transfers
  - ○ payments/target-2-payments
  - ○ payments/cross-border-credit-transfers
  - ○ payments/domestic-credit-transfers

Other:

- Our API supports Multilevel SCA for Payment Initiation, Consent Establishment and Signing Baskets
- AIS/PIS APIs are ready and tested with standard NISP test collection
- PSU-Corporate-ID i PSU-Corporate-ID-Type is not mandatory field because all accounts are linked to PSU-ID
- **URL for HPB API portal**
  - ○ https://www.hpb.hr/hpb-open-api-portal
- **scaAuthenticationData** represent token value which you get after authorization through IAM portal and result needs to be placed in the body of PUT request. Alternatevely, for sandbox and testing purposes you can speed up whole process by puting hardcoded values „12345" in request body, but this is not recomended because then you are not testing complete oAuth2 SCA flow
- **oAuth2**:
  - ○ oAuth2 flow is used for authentication An Introduction to OAuth 2 | DigitalOcean)
  - ○ An access token is generated in the OAuth 2.0 flow, and is triggered by the user giving consent to access dana. These tokens ensure access only to those protected resources granted by the user.

➢ SANDBOX ENVIRONMENT

GETTING STARTED in a few words:

1. Register on Developer Portal
2. Create an App and generate a certificate
3. Import certificate to Postman
4. Modify collection variables
5. Make a request
6. Authorize via IAM Portal

Registration:

- More informations on **NextGenPSD2XS2AFrameworkforCroatia** document: https://api.sandbox.openbanking.hpb.hr/apidocumentation?api=1042
- After registration done on https://iam.sandbox.openbanking.hpb.hr/connect/register TPP must create a V1/consent request through Postman or similar software

Certificate:

- First step is registration on developer portal (https://developer.sandbox.openbanking.hpb.hr/) -> creation of new TPP, app and certificate
- **Certificate details:**
  - o can be sent in request header
  - o imported (.crt and -key) to Postman
  - o Certificates are issued by MeDirect
- TPP-Authentication-Certificate doesn't have to be defined as variable (if you do, then you have to define it in collection variables)
- TPPs that have CRT and KEY files should not use PFX file and Passphrase fields, also, TPPs that have certificate in PFX format should not use CRT file and KEY file fields

AIS:

- For debit accounts use one from GetAccounts list, for creditor accounts use any valid IBAN
- **ConsentID**
  - o Scope parametar for AIS
  - o Needs to be forwarded in Header
  - o User can give consent for more than one account if he creates consents for allAccounts. If user give consent for one account, next consent will overwrite consent given before

PIS:

- **PaymentID**
  - Scope parametar for PIS
  - Check transactionStatus doesn't have time limit so it can be requested anytime with proper payment ID as parameter
  - Unique identifier for every payment
- Only bookedTransaction are shown in reponse code
- Openid has to be removed from scope for request to work
- Field **remittanceInformationUnstructured** is currently in testing phase
- **500 Internal Server Error**
  - problem can be found in payer's account ("debtorAccount"), because it is possible that corresponding account does not support this type of payment because it is not categorized as transactions account
- According to the API specification, within the chapter for PIS (p.4) the PUT request is specified which should be called („/ v1 / {payment-service} / {paymentproduct} // {paymentId} / authorizations / {authorisationId}"). After a successful PUT request, the response returns **status = "finalized"** and only then is the authorization completed.

Other:

- **Redirect_URI**
  - Can be changed through Developer portal
  - In the connect/authorize endpoint request must match the one registered on the Developer Portal

Example of sandbox flow:

- Import certificate (.crt .pfx and .key files…and passphrase)
- After that, create variables (on collection level):
o BaseURL: https://api.sandbox.openbanking.hpb.hr
o PSU-ID: 2019110700008000058
o ClientSecret: 378a9044-0403-4636-baa5-81c5416deaaf
o X-Request-ID: {{$guid}}
o PSU-IP-Port: 80
o PSU-ID-Type: customerNumber
o TPP-Redirect-URI: https://api.sandbox.psd2cloud.asseco-see.hr

After that, please try to make request. Before you send request, make sure that you have defined following in the header:
- Content-Type: application/json
- PSU-ID-Type: {{PSU-ID-TYPE}}
- X-Request-ID: {{X-Request-ID}}
- PSU-ID: {{PSU-ID}}
- PSU-IP-Address: {{PSU-IP-Address}}

![HPB logo]

Additional information:

ClientID: 8.clientname22
Username: 8.retail.customer1

➢ PRODUCTION ENVIRONMENT

AIS:
- In getTransactions endpoint if you don't send dateFrom, dateTo you only fetch transactions in last month. If you send those parameters you fetch all transactions which was defined by that parameters
- User can give consent for more than one account if he creates consents for allAccounts. If user give consent for one account, next consent will overwrite consent given before
- For Corporate accounts user has to send his OIB as PSU-ID to get all available accounts

PIS:
- For transaction cancellation (DELETE v1/payments/{paymentProduct}/{paymentID}), **payment ID** is important for referencing
- **transactionID**
  - o Unique identifier for every transaction
- According to the API specification, within the chapter for PIS (p.4) the PUT request is specified which should be called („/ v1 / {payment-service} / {paymentproduct} / {paymentId} / authorizations / {authorisationId}"). After a successful PUT request, the response returns status = "finalized" and only then the authorization is completed

Other:
- **Production URLs:**
  - o https://iam.openbanking.hpb.hr/
  - o https://api.openbanking.hpb.hr/
- **Access Tokens**
  - o If you use **MTLS**, token must be fetched from /connect/token/mtls endpoint where client_secret is not sent through field but MTLS auth need to be completed via TPP certificate
  - o Flag –cacert is not needed because FQDN iam.openbanking.hpb.hr has valid public certificate
  - o Refresh_token is not supported
- Client certificate need to be added to trusted list
- **Redirect_URI**

- o For changing redirect_uri you need to inform HPB support team because it needs manual work
- o Redirect_uri field can have multiple values but it has to be in an array

Regulation:

- Banks within the EU are regulated in the same way for all member states and are obliged to open their API in the manner prescribed by the PSD2 Directive (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/? uri = CELEX: 32015L2366 & from = EN # d1e5044-35-1) which was transferred to the valid Payment Transactions Act in the Republic of Croatia. The technical and security prerequisites for the operation of the interface are further defined by the Commission Delegated Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389&from=en#d1e1177-23-1 which is directly applicable in HR legislation. Hrvatska poštanska Banka d.d. maintains a dedicated interface that complies with the above regulations, as a regular channel of access to user payment accounts, together with the channels of Internet and mobile banking and does not provide other remote access options.

➢ **KEYWORDS AND TERMS**

Abbreviation / Term	Expansion / Description
TPP	Third party provider. A legal entity acting either as AISP, PISP or both
AIS	Account information services
PIS	Payment instruction services
User	Individual that is registered at both TPP and Bank and has granted consent to TPP
IAM	Identity access manager
CA	Certification authority
OAuth 2	Industry-standard protocol for authorization
SCA	Strong customer authentication

➢ **REFERENCES**

1. https://www.hpb.hr/hpb-open-api-portal
2. https://api.sandbox.openbanking.hpb.hr/apidocumentation?api=1042
3. https://iam.sandbox.openbanking.hpb.hr/connect/register
4. https://developer.sandbox.openbanking.hpb.hr/
5. https://iam.openbanking.hpb.hr
6. https://api.openbanking.hpb.hr/
7. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389&from=en#d1e1177-23-1

➢ **OTHER SOURCES**

1. An Introduction to OAuth 2 | DigitalOcean)