PSD2 API

API Technical Overview

Version

Version	Date	Author	Modifications
0.1	2018-19-21	Michal Bureš	Initialization
1.0	2018-12-17	Michal Bureš	Final version
1.1	2019-09-06	Michal Bureš	Sequence diagrams added
1.2	2020-02-26	Michal Bureš	Updated with respect to COBS v3.1

Referenced Documents

Ref.	Date or Version	Document name
[PSD2 RTS]		Regulatory Technical Specification for PSD2
[COBS]		The Czech Open Banking Standard
[XS2A]		Berlin Group Standard for PSD2 XS2A
[TS 119 495]		Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU

1 PSD2 API OVERVIEW

1.1 Introduction

Welcome to BNP Paribas Personal Finance CEE APIs! The APIs can be used for API-banking, as defined in PSD2 RTS.

1.2 Technical Standards

The APIs are mostly based on the Czech Open Banking Standard (COBS), with some customizations. However, some of the APIs are based on the Berlin Group Standard for PSD2 XS2A or custom-built for our purposes.

The APIs use REST notation, using HTTPS as transport protocol and JSON as payload.

1.3 Available APIs

BNP Paribas Personal Finance exposes the following APIs:

API	Standard	Allowed Consumers	Comment
TPP_Registration_COBS	Customized COBS v3.1	All PSD2 PSPs	Initiation of the cooperation with BNP Paribas PF CEE
TPP_Information	Custom	Public API	Supplementary API for TPP management
oAuth2_COBS	COBS v3.1	All PSD2 PSPs	Client enrolment for Account Information and Payment Initiation
Consent_Management_BG	XS2A (Berlin Group)	Internal, not for TPPs	For the moment, the API is for our internal use only
Balance_Check_COBS	COBS v3.1	PSD2 CISPs and PISPs	Balance check of the account (no blocking of the amount)
Account_Information_COBS	COBS v3.1	PSD2 AISPs List of accounts also for PISPs	List of authorized accounts, account balance, transaction history
Payment_Initiation_COBS	COBS v3.1, extensions	PSD2 PISPs	Initiation of payment orders
Standing_Orders_COBS	COBS v3.1	Active operations for PISPs Passive operations for AISPs	Information about and initiation of standing orders
Direct_Debit	Custom	Internal, not for TPPs	For the moment, the API is for our internal use only

BNP Paribas Personal Finance consists of a number of national branches across Europe. This API serves the following national entities:

- HelloBank.CZ, a brand operated by BNP Paribas Personal Finance SA, odštěpný závod, Czech Republic, on https://api2.hellobank.cz
- Cetelem Hungary on https://api.cetelem.hu

1.4 Mandatory HTTP Headers

Our APIs require the callers to provide the following HTTP headers defined in the Czech Open Banking Standard version 3.1 (COBS v3.1).

Header	Comment
User-User-Agent	End-user's browser information based as comes in User-Agent HTTP header
User-IP-Address	IP address of the end-user's device
User-Geo-Location	End-user's GPS coordinates (if available)
Action-ID	Unique identification of business transaction. Should be the same for multiple related REST calls
X-Request-ID	Unique identification of technical call. Each call must be assigned a unique request-ID.
Date	Current date and time

2 HOW TO START

2.1 For Developers

The API documentation is publicly available on https://www.cee.bnpparibas-pf.com.

Also, any developer can register to our API Portal at https://www.cee.bnpparibas-pf.com/sign-in. Upon registration, anyone can get access to our support and community.

Developers require a testing PSD2 certificate. Such certificate can be issued by První certifikační autorita, a.s. (I.CA), see https://ica.cz/. HelloBank Sandbox API accepts either qualified PSD2 certificates issued by any eIDAS certificate authority (see chapters 2.2 and 3.1) or PSD2 testing certificates issued by I.CA. No other types of certificates can be accepted.

2.2 For Licenced Payment Service Providers

For TPPs to start integration with HelloBank, TPPs must register using TPP_Registration_COBS API. A PSD2-compliant certificate based on specification TS 119 495 is required to initiate your registration.

An official TPP account will be created upon TPP registration via API. This account can be used to provide support of the API operations, get operational information etc. Along with the account creation, a TPP will get an "organization code". Whenever a new TPP employee registers to our API Portal, he or she will provide the organization code in order to join his or her organization.

There are some deviations from the Czech Open Banking Standard in our implementation:

- TPP should register just once. In contrary to COBS, we do not support multiple applications per TPP.
- There is no support for client_secret in oAuth2 flow. Instead, we fully rely on eIDAS TLS certificates.

3 SECURITY ELEMENTS

3.1 PSP Qualified Certificates

TPPs must use mutually-authenticated HTTPS connection. Protocol TLS 1.2 will be requested.

The client certificate must be a qualified eIDAS certificate for web-site authentication (QWAC based on EU regulation 910/2014) with extensions for PSD2 defined in technical standard ETSI TS 119 495 version 1.1.1.

TPP's qualified certificate for web-site authentication used as a client TLS certificate must comply with the following rules:

- Issuing qualified certification authority has to provide OCSP service with electronic seal including date and time, using certificate fulfilling ETSI TS 119 312 for 3 years durability. In the case, when OCSP service will not be available to validate certificate for particular request, request will be not authorized.
- QCA policies related with certificates has to be available in English, Czech, Slovak or Hungarian language.
- Qualified certificate with QWAC profile must fulfil ETSI TS 119 312 requirements for 1 year durability.

3.2 PSP Qualified Seals

The qualified seals are not supported by our API yet. We assume using seals based on Berlin Group XS2A standard.

The signing certificate must be a qualified eIDAS certificate for electronic seals (QSealC based on EU regulation 910/2014) with extensions for PSD2 defined in technical standard ETSI TS 119 495 version 1.1.1.

TPP's certificate for qualified electronic seals must comply with the following rules:

- Issuing qualified certification authority has to provide OCSP service with electronic seal including date and time, using certificate fulfilling ETSI TS 119 312 for 3 years durability. In the case, when OCSP service will not be available to validate certificate for particular request, request will be not authorized.
- QCA policies related with certificates has to be available in English, Czech, Slovak or Hungarian language.
- TPP will use qualified certificate with QsealC profile and fulfilling ETSI TS 119 312 requirements for 3 years durability.

3.3 oAuth2 Tokens

See Czech Open Banking Standard for further details about oAuth2 flows.

4 CUSTOMIZATION OF THE API

This chapter clarifies some implementation details about the exposed API.

4.1 Account Numbers

Banks are requested to open API for all payment accounts. This includes current accounts, savings accounts, as well as revolving accounts.

The accounts are identified as following:

- Current accounts by IBAN
- Savings accounts by IBAN
- Revolving accounts (credit cards) in
  - HelloBank.CZ by credit case number specified in “other/identification” field
  - Cetelem Hungary by IBAN

Example of identification of a revolving account in HelloBank.CZ:

```
"debtorAccount": {
    "identification": {
      "iban": "NOTPROVIDED",
      "other":    {
           "identification": "412345678900"
       }
   }
},
```

5 API SANDBOX

5.1 Basic Information

As per PSD2 regulation, banks are required to provide testing PSD2 APIs for licenced third parties, a sandbox. It provides a basic simulation of the PSD2 APIs in terms of input and output data, including positive and negative scenarios.

However, in order to allow using the sandbox by a broad audience of developers, it is not protected by any authentication mechanisms such as certificates. Hence, the sandbox can be used by any registered developer, it does not require PSD2 licence. Neither, non-functional characteristics of the API (such as response latency) is simulated.

Only some of the PSD2 APIs are sandboxed. Please refer to API documentation whether a corresponding sandbox API is available. Some APIs are publicly available without any restrictions, so herein the developers can use directly these APIs.

5.2 Using Sandbox

If sandboxed API is available, it is published with URL prefix /sandbox. For example, list of accounts resource in Account Information Service is available on https://api2.hellobank.cz/api/v1/my/accounts. Then sandbox API for the same is published on https://api2.hellobank.cz/sandbox/api/v1/my/accounts.

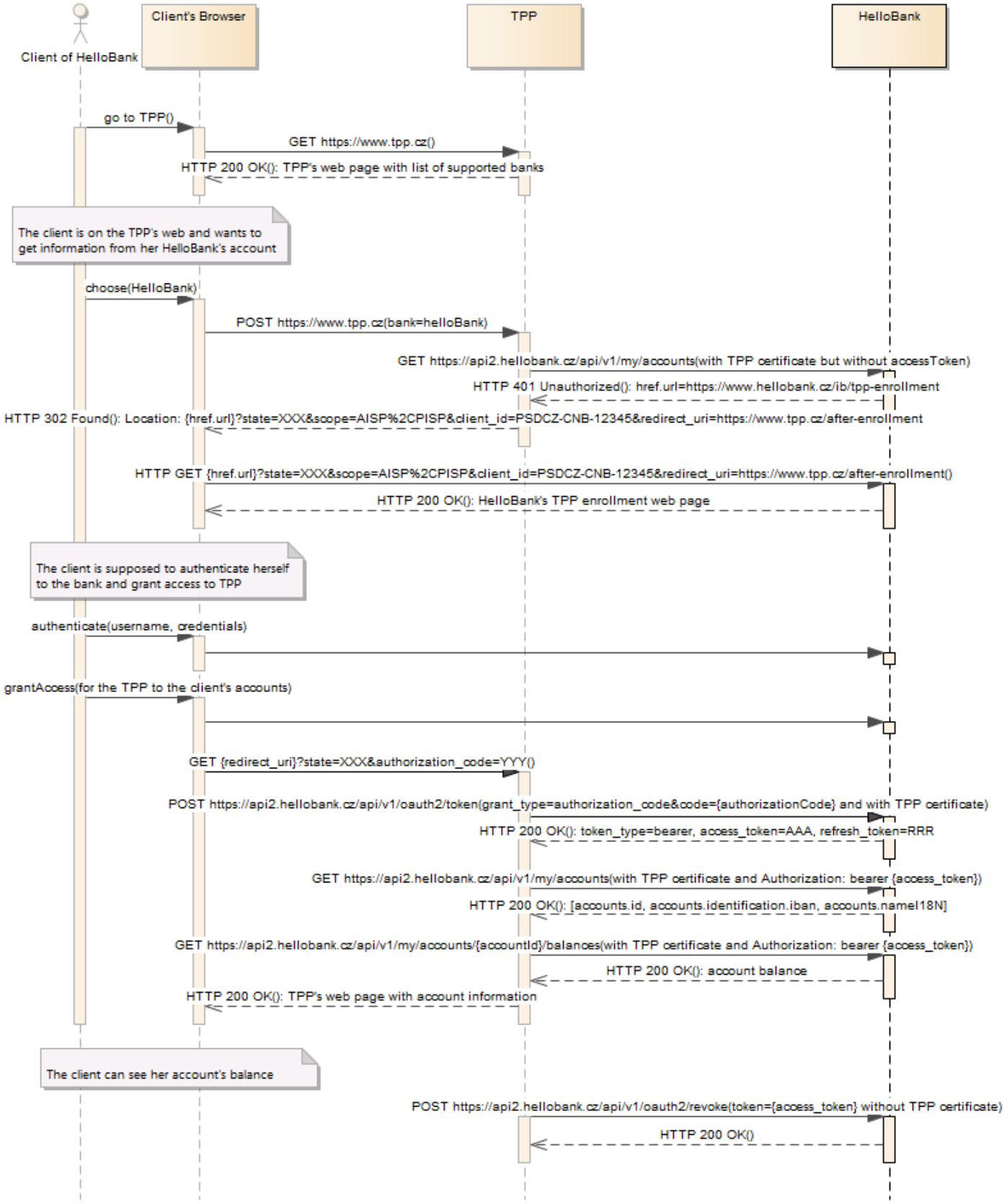
5.3 Sandbox Data

The data provided by the sandbox is an anonymised version of a real data. It should offer the developers full range of various payment transaction types etc.

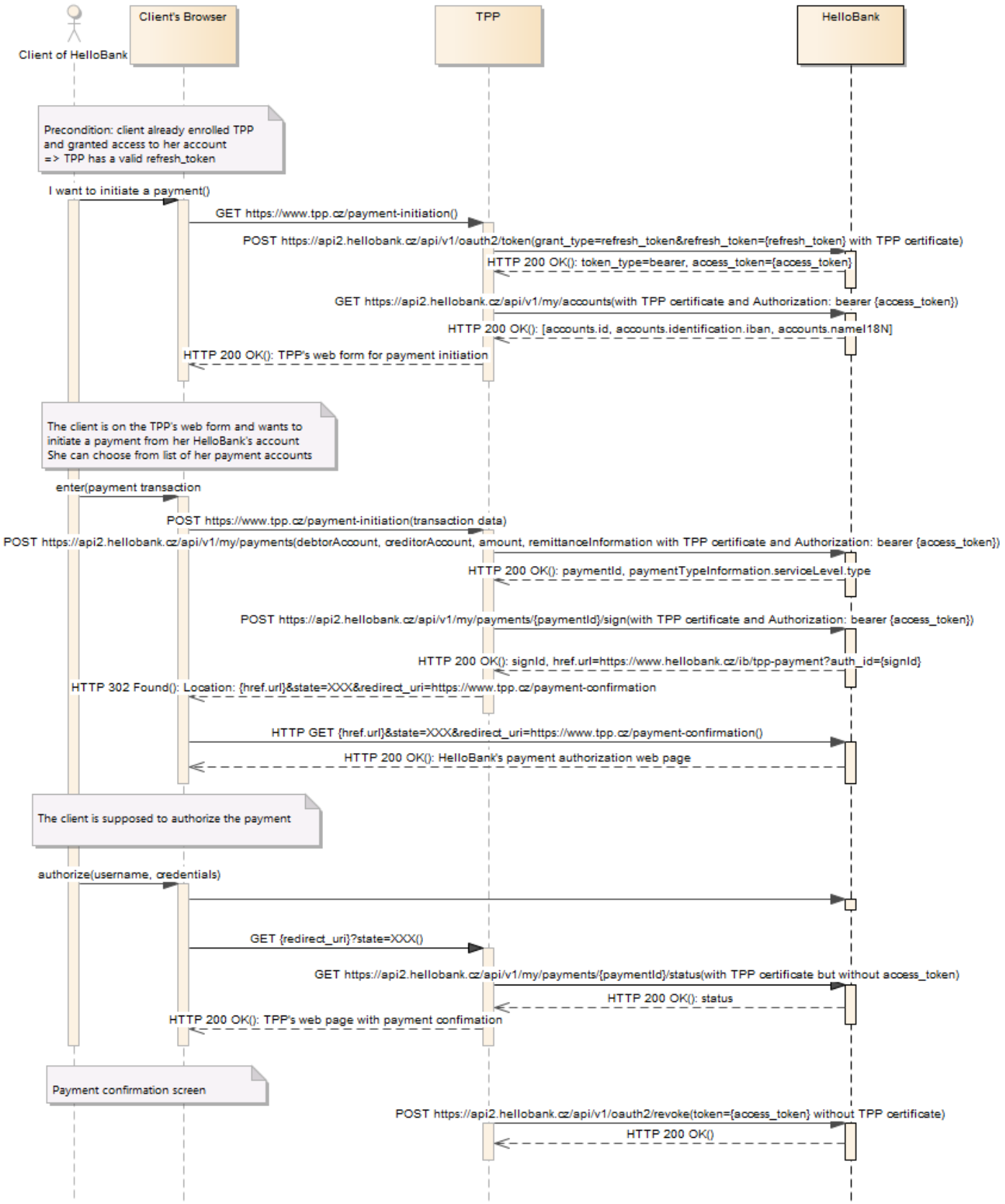
In order to get simulated account numbers, please use https://api2.hellobank.cz/sandbox/api/v1/my/accounts and get list of available sandbox accounts. Simply skip the challenge to provide TLS client certificate and you will receive a testing data set.

6 BASIC API FLOWS

6.1 Client TPP Enrolment and Account Information



6.2 Payment Initiation by TPP



========== End of the document ==========