The Sandbox SK Manual on Validation of Balances to Card-Based Payment Instrument Issuers

Change log

Date	Version	Description
29.01.2020	1	First document version
21.05.2020	2	Document edit

Contents

1. Sufficient Funds Query (POST /accounts/balanceCheck) 4
2. Sufficient Funds Query (CIS) Calling API Sandbox 4
3. Issuing a Certificate 4
4. Definition of Test Accounts for CIS Calling 4
5. Definition of the Mock 4
6. Error reporting 6
7. API CIS Mock Calling Methods 7

API CIS mock calling through the console 7
Filling in the required fields 9
Error message 10

8. Access to the Sandbox through API Direct Calling 11

Sufficient Funds Query (POST /accounts/balanceCheck) 11
Characteristics of the Resource 11

9. PSD2 glossary – selected terms 16

1. Sufficient Funds Query (POST /accounts/balanceCheck)

The service serves to verify sufficient funds in a specific account that the client manages through his/her internet or mobile banking.
The bank's response consists in a confirmation or non-confirmation of the sufficiency of funds as against the amount stated in the query. The answer is yes/no only – see below for details. In this case, the bank does not provide information about the specific amount of the balance in the client's account.

The service is not authorised by the account holder directly through the authorisation resource.
Komerční banka has based its approach on the unified structure and format of information defined by the Czech Banking Association in the Czech Open Banking Standard.
The information provided through API Open Banking is in both Czech and English.
The allowed character set is based exclusively on the SWIFT character set (i.e., exclusively without diacritics).
The "debtorAccount.identification.iban" data element requires an account number in the IBAN format as defined by the ISO 13616 international standard.

Only one query can be sent and processed during a single call.

2. Sufficient Funds Query (CIS) Calling API Sandbox

Through the Sandbox, third parties may have a trial (mock) of a service verifying the availability of funds in a specific payment account of a client of Komerční banka, branches of the foreign bank (hereinafter referred to as Komeční banky).

Any entities, not only the third parties with a PSD2 services licence, may access the API Sandbox. However, they must register at KB's API portal https://api.koba.sk/portal/?tenant=api.kb.sk. Failing this, they cannot utilize the Sandbox services. The procedure for registration is described in the document API Sandbox Registration_v1.doc.

3. Issuing a Certificate

A certificate is necessary for the production calling and PSD2 Sandbox. After the registration, Komerční banka will provide the third parties with certificates to be used on the Sandbox, **based on their request sent at the electronic address** api@kb.cz . The Sandbox certificates are not intended for production use. The production unit will reject and monitor such calls. The procedure for registration is described in the document *API Sandbox Registration_v1.doc.* Qualified PSD2 certificates issued by a qualified certification authority according to the EU QTSP list at https://webgate.ec.europa.eu/tl-browser/

4. Definition of Test Accounts for CIS Calling

- IBAN – account test number for CIS mock calling in the IBAN format.
- Currency – currency in which the account is denominated.
- Available balance – amount to which the query relates.
- Authorization – information whether or not CIS is allowed for the given account. It simulates the client's consent granted to a third party.
- Account category – information whether CIS calling is possible in KB for the given account (or account type).

IBAN	Currency	Available balance	Authorization	Account category
SK7481000000435300270267	EUR	33.30	YES	YES

5. Definition of the Mock

Parameters of dynamic calling are defined, which a third party can change within calling. Appropriate responses or, as the case may be, error codes are returned depending on the request parameters used.

KB makes it possible to call the CIS service in the Sandbox with the below parameters and logics:

Parameter	CISP Parameter	Input values	Activity/Response	Error Code
Certificate	AISP service calling certificate	KB test certificates (those issued by I.CA are allowed for the time being), with a given scope.	If the provided certificate is used, the balance is returned (depending on the validations below).	-
		Any other certificate than that issued by I.CA as the authorised issuer.	If any other certificate is used, an error is returned - Authentication with an invalid certificate.	403 FORBIDDEN - Invalid certificate or token.
		Calling without a certificate.	If TPP uses no certificate, an error is returned - Missing certificate or access token.	401 UNAUTHORISED - Missing certificate or access token.
Account number	debtorAccount, - identification - iban	IBAN of the account - see the Definition of test accounts for CIS calling.	Balance (depending on the validations below).	-
		An account for which no consent has been set.	Error - no consent has been set.	AG01 TransactionForbidden
		An account that is not categorized for CISP by KB.	Error - no CIS calling is allowed for this account in KB.	AC12 InvalidAccountType
		Any other account at the input.	Error - the account is not in the IBAN format.	AC02 InvalidDebtorAccountNumber
Account currency	debtorAccount - identification - currency	Currency of the account	Account currency validation. If the currency is different from the KB account currency, an error is returned.	AC09 InvalidAccountCurrency
Query currency	transactionDetails - currency	CZK, EUR	If the transaction currency is different from the account currency: • Account denominated in CZK and the transaction in EUR - the amount will be converted using the KB mean rate as of 01 Dec 2017 (EUR 1.00 = CZK 25.5073) • Account denominated in EUR and the transaction in CZK - the amount will be converted using the KB mean rate as of 01 Dec 2017 (EUR 1.00 = CZK 25.5073)	
			If the transaction currency is different from CZK/EUR, an error is returned – The transaction currency is not listed on the bank's exchange list.	AM11 InvalidTransactionCurrency
Query amount	transactionDetails - totalAmount	Value	The value is greater than zero - an answer is returned (if the query passes all the other validations).	-
			The value is less than or equal to zero - an error is returned – Invalid amount, e.g., too low or high amount or a wrong number format in terms of the number of decimal places according to ISO 4217.	AM12 InvalidAmount

Other Parameterisable and Non-Parameterisable (Static) Values of Calling and their Validation

The third party/calling party will be able to fill in the parametrisable values of calling according to his/her needs. KB will validate the type / length and format of these values in the same manner like during real-life validations performed in the production API – see the Czech Open Banking Standard ČBA specification.

The table below contains other attributes that are also part of the sufficient funds query. This information identifies the merchant who makes the CIS calling. Any fictional data can be inputted in the Sandbox. KB will validate the **obligation** and **format of the field**.

Parameter description	Query parameter	Type	Mandatory (Yes / No)	Form
Unique identification of the payment transaction (by the card issuer)	exchangeIdentification	number	Yes	IntMax18Digits
Name of the debtor - cardholder	debtor.name	string	No	Max140Text
Currency code as additional identification of multicurrency accounts	currency	string	No	CurrencyCode ISO 4217 (Max3Text)
Cardholder authentication method taken from the AuthenticationMethod5Code list according to the ISO 20022 of the CAAA.002 message.	authenticationMethod	string	No	AuthenticationMethod 5Code
Identification of the merchant, e.g. IČ.	identification	string	Yes	Max35Text
Short name of the merchant.	shortName	string	Yes	Max35Text
Name of the merchant as stated on the receipt.	commonName	string	Yes	Max70Text
Address of the merchant.	address	string	No	Max140Text
Country code according to the ISO 3166-1 alpha-2 country code list.	countryCode	string	Yes	Min3Max4Text
Merchant category according to the ISO 18240 code list.	merchantCategoryCode	string	Yes	Min3Max4Text

6. Error reporting

Reporting quarantined errors or calling them always takes place via the mailbox api@kb.cz. The e-mail sent must contain the following information, in case the required information is missing, it will not be possible to process the query or error.

PSD2 API: CZ, SK
Environment: Sandbox, Production
Whether it was called from FE Sandbox incl. the type and version of the browser used or, in the case of a BE call, the name and version of the program for the BE call
Request type
Date and time of the call
IP address
The error and its most accurate description, which can be supplemented with the appropriate screenshot

Without the above values, it is not possible to solve the reported error.

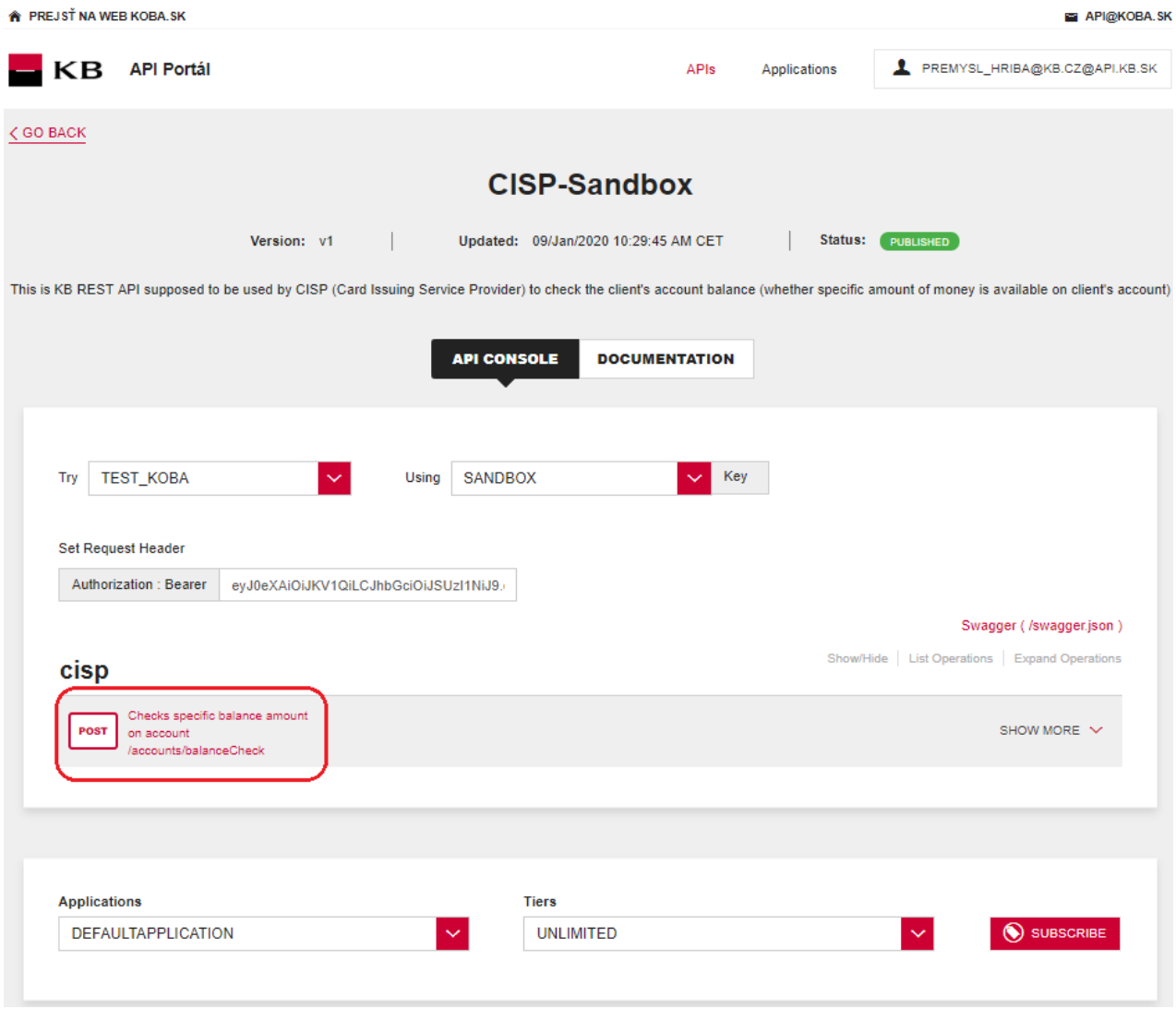
7. API CIS Mock Calling Methods

- API CIS direct calling

API CIS mock calling through the console

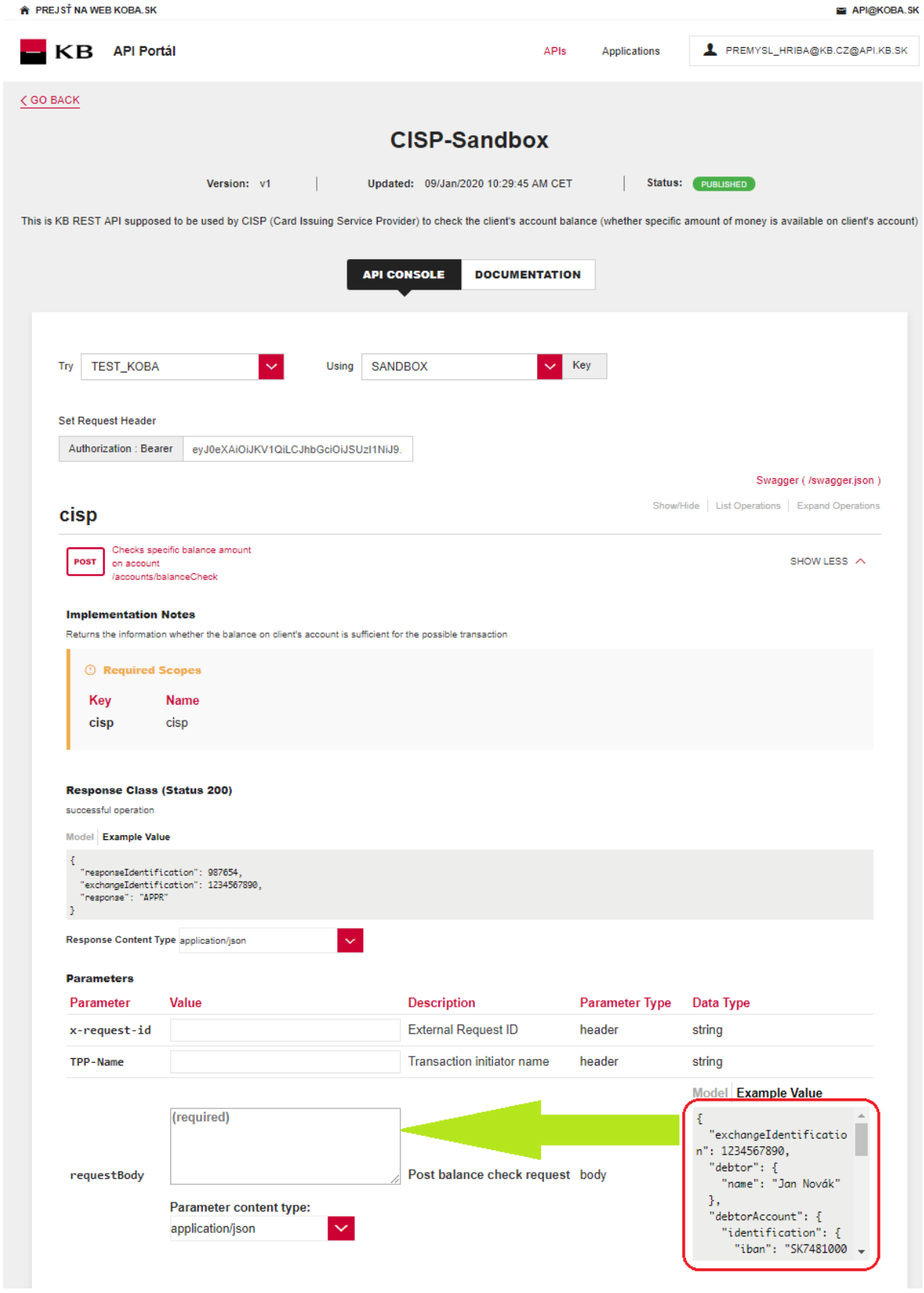
In the Sandbox, it means calling the operation entitled “Checks specific balance amount on account”.

The user chooses an operation he/she wishes to test. In this case, it is “Checks specific balance amount on account”. This operation will provide information about availability of funds in the client’s account.


PREJSŤ NA WEB KOBA.SK
API@KOBA.SK
KB API Portál
APIs
Applications
PREMYSL_HRIBA@KB.CZ@API.KB.SK
GO BACK
CISP-Sandbox
Version: v1
Updated: 09/Jan/2020 10:29:45 AM CET
Status: PUBLISHED
This is KB REST API supposed to be used by CISP (Card Issuing Service Provider) to check the client's account balance (whether specific amount of money is available on client's account)
API CONSOLE
DOCUMENTATION
Try TEST_KOBA
Using SANDBOX
Key
Set Request Header
Authorization : Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
Swagger (/swagger.json)
Show/Hide
List Operations
Expand Operations
cisp
POST
Checks specific balance amount on account /accounts/balanceCheck
SHOW MORE
Applications
DEFAULTAPPLICATION
Tiers
UNLIMITED
SUBSCRIBE

Filling in the required fields

For requestBody, just click on the displayed example to copy it to the appropriate field. If any of mandatory fields is not filled in, the report is not displayed and the blank fields are highlighted in red.



Error message

If any value has been entered incorrectly, one of the following error messages or an error specified in the mock definition will be displayed after pressing the "TRY IT OUT" button, otherwise the result statement will be displayed.

Response Messages

HTTP Status Code	Reason	Response Model	Headers
400	Input parameter is invalid	Model | **Example Value**	
401	Missing certificate or access token	Model | **Example Value**	
403	Invalid certificate or token	Model | **Example Value**	
415	Invalid message charset	Model | **Example Value**	
500	Unexpected error occured	Model | **Example Value**	

```
{
  "errors": [
    {
      "error": "ERR_CODE_400",
      "scope": "x-request-id",
      "message": "Value of parameter x-request-id is wrong"
    }
  ]
}
```

```
{
  "errors": [
    {
      "error": "ERR_CODE_401",
      "message": "Missing certificate or access token"
    }
  ]
}
```

```
{
  "errors": [
    {
      "error": "ERR_CODE_403",
      "message": "Invalid certificate or token"
    }
  ]
}
```

```
{
  "errors": [
    {
      "error": "RR10",
      "message": "InvalidCharacterSet"
    }
  ]
}
```

```
{
  "errors": [
    {
      "error": "ERR_CODE_500",
      "message": "Internal Server Error"
    }
  ]
}
```

TRY IT OUT

8. Access to the Sandbox through API Direct Calling

Sufficient Funds Query (POST /accounts/balanceCheck)

This is the resource for sending a sufficient funds query regarding a debtor's particular payment account. This resource is not authorized by the account holder directly through the authorisation resource. The consent to access to information must be granted by the client outside the interaction of this API before the resource is used.

Characteristics of the Resource

URI:	/accounts/balanceCheck
HTTP Method:	POST
Request URL:	https://api.koba.sk/sandbox/cisp/v1/accounts/balanceCheck
Authorization:	the request **does not require** any authorisation by the user/client as part of the API call
Certification:	the request **requires** the use of the third party qualified certificate. The API call may not be successful unless the certificate contains the scope "**cisp**" scope permission**!**
Pagination:	no
Sorting:	no
Filtering:	no
Supported encoding:	`charset=UTF-8`

Query parameters of the request: **not defined**

Example of the API call curl:

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --he
ader 'x-request-id: 123' --header 'x-client-cert: TPP_CERT' --header 'Authorization: Bearer ' -
d '{ \
   "exchangeIdentification": 1234567890, \
   "debtor": { \
     "name": "Jan Novák" \
   }, \
   "debtorAccount": { \
     "identification": { \
       "iban": "SK7481000000435300270267" \
     }, \
     "currency": "EUR" \
   }, \
   "authenticationMethod": "NPIN", \
   "merchant": { \
     "identification": "47116129", \
     "shortName": "NOOLUXOR", \
     "commonName": "NOOLUXOR s.r.o", \
     "address": "Hlavní 5, Praha 1", \
     "countryCode": "CZ", \
     "merchantCategoryCode": 5192 \
   }, \
   "transactionDetails": { \
     "currency": "EUR", \
     "totalAmount": 15.3 \
   } \
}' 'https://api.koba.sk/sandbox/cisp/v1/accounts/balanceCheck'
```

Table 1 Request header parameters

PARAMETER	TYPE	MANDA-TORY	PURPOSE
Content-Type	Text	Yes	A specification of the required transfer format. Based on the prerequisites of the technical specification of this API standard, in this case the **application/json** format is primarily supported.
API-key	Text	No	An optional string issued to a communicating third party as the call identifier of that party primarily serving as the configuration element of communication.
x-request-id	Text	Yes	A unique identification of the caller's each particular query. The value of this parameter should therefore be generated randomly, and the individual x-request-ids of the same caller within a short time interval should not be identical. This parameter service returns responses to the calling system within response headers.
x-client-cert	Text	Yes	A qualified certificate for establishing two-way TLS communication. The third party is identified by verifying the validity and contents of the certificate.

Example of request headers:

```
{
  "Accept": "application/json",
  "x-request-id": "123",
  "x-client-cert": "TPP_CERT"
}
```

Table 2 Response header parameters

PARAMETER	TYPE	MANDA-TORY	PURPOSE
Content-Type	Text	Yes	A specification of the required transfer format. Based on the prerequisites of the technical specification of this API standard, in this case the **application/json** format is primarily supported.
x- request -id	Text	Yes	Returns the original request id of the API call.

Example of response headers:

```
{
  "date": "Fri, 23 Feb 2018 12:51:46 GMT",
  "cookie": "i18next=sk-SK",
  "x-request-id": "123",
  "accept": "application/json",
  "x-forwarded-host": "api.koba.sk",
  "host": "api.koba.sk",
  "accept-encoding": "gzip, deflate",
  "cache-control": "no-cache",
  "x-forwarded-server": "api.koba.sk",
  "content-type": "application/json; charset=UTF-8",
  "keep-alive": "timeout=60, max=100",
  "connection": "Keep-Alive",
  "transfer-encoding": "chunked",
  "strict-transport-security": "max-age=16070400; includeSubDomains",
}
```

Komerční banka provides information on the availability of funds within the following structure and contents of the POST request.

Table 3 Sufficient funds query – BASIC ELEMENTS OF THE REQUEST

LEVEL	MESSAGE ELEMENT	OCCURRENCE	FORMAT TYPE	PRESENTATION
+	exchangeIdentification	[1..1]	Max18Text	Unique identification of the query
+	debtor	[0..1]	±	Identification of the debtor – cardholder
++	name	[1..1]	Max140Text	Transaction debtor's (cardholder's) name
+	debtorAccount	[1..1]	±	Debtor's account
++	identification	[1..1]	±	Debtor's account identification
+++	iban	[1..1]	IBAN2007Identifier	IBAN
++	currency	[0..1]	CurrencyCode, ISO 4217	Debtor's account currency
+	authenticationMethod	[0..1]	CodeSet	Client authentication method
+	merchant	[0..1]	±	Merchant carrying out the transaction
++	identification	[1..1]	Max35Text	Merchant's identification
++	type	[0..1]	Code	Merchant's type
++	shortName	[1..1]	Max35Text	Merchant's name
++	commonName	[1..1]	Max70Text	Merchant's name as given in the payment slip
++	address	[0..1]	Max140Text	Merchant's address
++	countryCode	[0..1]	CountryCode, ISO 3166	Merchant's country
++	merchantCategoryCode	[1..1]	Min3Max4Text, ISO 18245	Merchant's code depending on the type of the transaction
+	transactionDetails	[1..1]	±	Transaction details
++	currency	[1..1]	CurrencyCode, ISO 4217	Balance query currency
++	totalAmount	[1..1]	Max18.5Amount	Balance query amount

JSON – example of a requestBody:

```
{
        "exchangeIdentification": 103149078,
        "debtor": {
                "name": "Jan Novak"
        },
        "debtorAccount": {
                "identification": {
                        "iban": "SK7481000000435300270267"
                },
                "currency": "EUR"
        },
        "authenticationMethod": "NPIN",
               "merchant": {
                "identification": 47116129,
                "shortName": "NOOLUXOR",
                "commonName": "NOOLUXOR s.r.o",
                "address": "Hlavni 5, Praha 1",
                "countryCode": "CZ",
                "merchantCategoryCode": 5192
        },
        "transactionDetails": {
                "currency": "EUR",
                "totalAmount": 15.3
        }
}
```

Table 4 Sufficient funds query – RESPONSE ELEMENTS

LEVEL	MESSAGE ELEMENT	OCCURRENCE	FORMAT TYPE	PRESENTATION
+	responseIdentification	[1..1]	Celé číslo	A unique identification of a response to the sufficient funds query (from ASPSP).

+	exchangeIdentification	[1..1]	IntMax18Digits	A repeated identification of the payment transaction (sufficient funds query) by the card issuer, to which the sufficient funds query relates.
+	response	[1..1]	Code set	A response to the sufficient funds query.

JSON – example of a response:

```
{
   "responseIdentification": 41657765434736200,
   "exchangeIdentification": 103149078,
   "response": "APPR"
}
```

Table 5 "Response" parameter return codes

CODE	DESCRIPTION
APPR	Sufficient funds in the account.
DECL	Insufficient funds in the account.

Table 6 CBA-standard defined error codes for the Sufficient Funds Query POST service

HTTP STATUS CODE	ERROR CODE	ERROR CODE DESCRIPTION	PURPOSE
401	UNAUTHORISED	Chybějící certifikát nebo access token.	Missing certificate or access token.
403	FORBIDDEN	Nevalidní certifikát nebo token.	Authentication made with an invalid certificate or expired access token, or a call that does not correspond to the third party's licence.
400	FIELD_MISSING	Chybějící povinné pole.	Missing mandatory field in the request.
400	FIELD_INVALID	Hodnota pole není validní.	The value of the field is not valid.
400	AC02	InvalidDebtorAccountNumber	Incorrect account number format.
400	AC09	InvalidAccountCurrency	The declared account currency does not correspond to the currency in which the client's account held with the bank under the given number is denominated.
403	AG01	TransactionForbidden	The account type does not match the allowed account types (e.g. a non-paying account).
400	AM11	InvalidTransactionCurrency	The payment currency is not listed in the bank's exchange list.
400	AM12	InvalidAmount	The amount of the transaction is invalid, i.e. is too low/high, the account number is incorrect, or the number of decimal places is wrong according to ISO 4217.
400	FF01	InvalidFileFormat	The payload has not been sent under JSON or other technical issue occurred.
400, 50x	NARR	Narrative	The payment has been rejected on general grounds, which will be explained in the narrative. This may be a technical issue.
400	RF01	NotUniqueTransactionReference	The sufficient funds query reference is not unique.
400	RR10	InvalidCharacterSet	Illegal characters have been used (e.g. Chinese characters, diacritic, unauthorised symbols etc.).

JSON – example of an error message body:

```
{
    "errors": [{
     "error": "UNAUTHORISED",
     "message": "Missing certificate or access token"
     }]
}
```

9. PSD2 glossary – selected terms

API – Application Programing Interface
REST – (Representational State Transfer) is an API architecture, which allows for accessing the data and execute CRUD operations. It usually uses the HTTP/HTTPS protocol. REST is stateless, which makes communication with the API much easier and allows for the parallel processing of its contents. At the same time, it can be easily used with HTTP, which is a widely used protocol. Last not least, it provides a standard of a kind so we can easily use an API created by somebody else or offer our API to a number of other users. The REST interface supports uniform and easy access to resources. Such resources can be data or application states (as long as they can be described using specific data). All resources have their URI identifier. REST defines four basic methods of access (GET, PUT, POST, and DELETE). The HTTP Verbs have the following meaning:

- GET – obtaining the data
- POST – creating
- PUT – editing (like SET, it edits an entire resource)
- DELETE – deleting
- PATCH – partial editing

REST API – Distributed environment interface oriented on data, not on calling procedures like RPC (XML-RPC) or SOAP. Web services define remote procedures and their calling protocol; REST decides how the data should be approached. REST API uses HTTP methods, such as @GET, @PUT, @POST, @DELETE, @PATCH.
TPP – Third Party Provider (a third party registered with the Slovak National Bank or another official authority within the EU)
AIS – Account Information Service
AISP – Account Information Service Provider
PIS – Payment Initiation Service
PISP – Payment Initiation Service Provider
CIS – Card-based Payment Instrument Issuance Service
CISP – Card-based Payment Instrument Issuance Service Provider
ASPSP – Account Servicing Payment Service Provider (a bank holding the debtor's payment account)