CAF API

PSD2 interface CAF de Volksbank

November 21 2019

Colophon

Label	Data
Owner	Service Centre KBS de Volksbank N.V.
Authors	ITC VO KWB Open Banking
Status	CAF BG final
Project	PSD2

Version

Version	Date	Changes
1.0	2019-09-12	Final version
1.1	2019-11-21	Change log: - Updated response headers CAF consent request call.

References

Version	Date	Description	Author	Reference
	October 2012	The OAuth 2.0 Authorization Framework	D. Hardt, Ed.	RFC 6749
		OAuth 2.0 Servers	Aaron Parecki	
	2014-07-21	An Introduction to OAuth 2	Mitchell Anicas	
	2015-07-03-07	OAuth 2.0 Token Introspection	J. Richer, Ed.	RFC 7662
1.1	2009-12-18	Sepa Requirements For An Extended Character Set	European Payments Council (EPC)	EPC217-08

TABLE OF CONTENTS

1 Introduction

This document describes the CAF (Confirmation of the Availability of Funds) interface offered by de Volksbank under PSD2. This funds confirmation service complies with Berlin Group standards (NextGenPSD2 XS2A Framework Implementation Guidelines V1.3). Note that before the funds confirmation service can be used, a PSU (Payment Service User) has to give explicit consent that a PIISP (Payment Instrument Issuing Service Provider) can request a funds confirmation. This is a de Volkbank-specific flow that is based on the AIS (Account Information Services) consent flow as described by the Berlin Group.

This document explains the process of the consent a PSU is required to give for letting a TPP (Third Party Provider) in the role of PIISP check the funds availability, followed by an explanation of the actual funds confirmation service.

The remainder of this document will be organized as follows:

- Chapter 2 describes the conditions de Volksbank applies to the use of its CAF services, the character set used to be exchanged between the TPP and de Volksbank in its role as ASPSP (Account Servicing Payment Service Provider), the datatypes defined for the individual pieces of information and the URLs to be used by the TPP for the different brands of de Volksbank;
- Chapter 3 sheds some light on the chosen consent flow;
- Chapter 4 explains the fine details of the consent flow;
- Chapter 5 contains an explanation of the actual confirmation of the availability of funds service.

2 CAF services as offered by de Volksbank

2.1 Conditions on the use of de Volksbank's CAF services

The following conditions apply on the usage of the CAF services:

1. The authorization code is valid for a duration of **10** minutes;
2. The access token is valid for a duration of **10** minutes;
3. Each consent granted by a PSU to a PIISP is valid for the duration as indicated by the PIISP in the field *validUntil*, submitted in the CAF consent request. The refresh token is valid for **90** days;
4. Requirements pertaining to the CAF services retrieving information on funds availability:
    a. The CAF services retrieving information on funds availability can only apply to **one** specific account per call.
    b. The CAF services are only allowed for **euro** payments.

2.2 Character set

The used character set is the Latin character set of the UTF-8 character encoding standard. This is in accordance with the character set as defined by the European Payments Council (EPC) Implementation Guidelines (EPC217-08). This character set is defined below:

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
/ - ? : ( ) . , ' +
Space

2.3 Data types

The APIs as defined by de Volksbank N.V. consume and produce JSON (Java Script Object Notation) structures. JSON accepts the following data types:

1. A string;
2. A number;
3. An object (JSON object);
4. An array;
5. A boolean.

2.4 URLs

De Volksbank supports PSD2 APIs for three different brands: ASN Bank, RegioBank and SNS. There is one specific URL per brand.

- URL for access granting
  - for TPPs in the role of PIISP to start the access granting process for the PSU, use:
    psd.bancairediensten.nl/psd2/asnbank/v1/authorize
    psd.bancairediensten.nl/psd2/regiobank/v1/authorize
    psd.bancairediensten.nl/psd2/snsbank/v1/authorize

  - for TPPs in the role of PIISP to redeem an authorization code for an access token, use:
    psd.bancairediensten.nl/psd2/asnbank/v1/token
    psd.bancairediensten.nl/psd2/regiobank/v1/token
    psd.bancairediensten.nl/psd2/snsbank/v1/token

- URL for executing permission, the so-called bank-URL:
  - for ASN Bank, use: **api.asnbank.nl**
  - for RegioBank, use: **api.regiobank.nl**
  - for SNS, use: **api.snsbank.nl**

Attention:
Known Android problem

On some android phones it is possible that the customer is requested to install a certificate for the authorize request. This is a reaction from the browser to the possibility to use a client certificate on our standard HTTPS port 443. If the authorize request is send from a server the standard TLS connection takes care of this issue, but the browser does not. If the request is initiated from the browser of the customer, you have to use port 10443 for the authorize requests only, to avoid the client certificate question.

With respect to the data types, de Volksbank adheres closely to the datatypes and formats used in pain messages as defined by the ISO 20022 norm and adopted by the EPC for SEPA payments. This means that for alpha-numerical, decimal and date fields the datatype **string** with some additional formatting will be used:

Datatype	Length/Format	Description
String	Maxtext34	Maximum length of the alpha-numerical string is 34
	Maxtext35	Maximum length of the alpha-numerical string is 35
	Maxtext70	Maximum length of the alpha-numerical string is 70
	Maxtext140	Maximum length of the alpha-numerical string is 140
	ISO 8601 date format	Dates are of the data type string, but must comply with the ISO 8601 date format. This implies that dates have the following format: **YYYY-MM-DD**.
	ISO 8601 datetime format	Dates are of the data type string, but must comply with the ISO 8601 datetime format.
String	Decimal format	Amount fields are of the data type *string*, but have the format of a *decimal* where the following format requirements hold: 1. The number of fractional digits must comply with the ISO 4217 minor unit of currency (for instance, the number of fractional

		digits for the currency EUR is 2); 2. The digits denoting integers and the digits denoting fractions are separated by a **dot**.
Number	Integer format	Number is an integer starting at 0, 1, 2, ...

3 Access

The PIISP can only use the PSD2 APIs as authorized by de Volksbank. The PIISP must be registered with the Competent Authority with a license for CAF services (refer to the payment service 5 as described in Annex I of the Payment Services Directive (2015/2366)).
PIISPs that wish to use the PSD2 APIs of de Volksbank are required to go through an onboarding process. Part of this onboarding process is the exchange of a so-called **client_id**, **client_secret** and **redirect_uri.** The redirect_uri is needed to return the response to the consent request, the subsequent authorization request and token exchange request to the appropriate address of the PIISP.

3.1 Certificates

The connections between the TPP and de Volksbank endpoints are secured by a mutual TLS authentication, as required in the PSD2 regulations. This means that the TLS connection can only be established including client (i.e. TPP) authentication. For this authentication the TPP has to use a qualified certificate for website authentication. This qualified certificate has to be issued by a qualified trusted service provider (QTSP) according to the eIDAS regulation [eIDAS].
The content of the certificate has to be compliant with the requirements as specified in article 34 of the EBA Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under article 98 of Directive 2015/2366 (PSD2).

The public key of this certificate has to be presented to de Volksbank during the onboarding process of the TPP.

3.2 Authentication by OAuth2

De Volksbank has chosen the OAuth2 authentication method for its PSD2 interface, an authentication method that does not require users to share their bank passwords with third-party apps. More details on the OAuth2 authentication method can be found in the standard OAuth2 flows or in one of the many tutorials on the internet.

3.3 Authorization

De Volksbank is using the so-called a*uthorization code* grant flow. The authorization code grant type is used to obtain both access tokens and refresh tokens and is optimized for confidential clients.

The ASPSP (the PSU's bank) delivers an authorization code to the TPP on behalf of the customer. The code is issued only once by the ASPSP and is needed for using the PSD2 functions. Next, the TPP will exchange the authorization code for an access and refresh token. The access token is subsequently used in each PSD2 API service.

4 The APIs for granting access to the CAF service

The PIISP must use the following APIs for gaining access to the CAF service:

1. Consent request (creation of a consent ID);
2 and 3. Authorization request and approval of the PSU;

   Please note that currently between the creation of a consent ID and the approval of the PSU a time window of 10 minutes is defined. If after these 10 minutes we (as an ASPSP) have not received an approval of the PSU the consent is automatically expired.

4. Access token request: access token and refresh token based on authorization code;
5. New access token request: new access and refresh tokens based on refresh token.

The API endpoints usually consist of the following elements:

1. Method and URL;
2. Path parameters;
3. Query parameters;
4. Request header;
5. Request body;
6. Response code;
7. Response header;
8. Response body.

We will discuss these elements for every endpoint de Volksbank offers.

4.1 CAF consent request: PIISP requests permission to check availability of funds of the PSU

By issuing a CAF consent request, the PIISP seeks to get permission from an ASPSP to check the availability of funds of a PSU at the addressed ASPSP.

The next sub-sections discuss the parts which make up the CAF consent request.

4.1.1 Method and URL

Method	URL	Description
POST	https://psd.bancairediensten.nl/psd2/ [snsbank|asnbank|regiobank]/v1/funds-confirmation	CAF consent request endpoint as defined by de Volksbank.

Note that this endpoint URL is identical to the endpoint the Berlin Group describes for the actual funds confirmation service, not for a consent. For the actual funds confirmation service, de Volksbank offers a different endpoint, as described in chapter 5.

4.1.2 Path parameters

The CAF consent request endpoint does not have any path parameters.

4.1.3 Query parameters

The CAF consent request endpoint does not have any query parameters.

4.1.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Invariably filled with the value "*application/json*".
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the PIISP).
Authorization	String	Y	Attribute consists of *client_id*: Identification of the PIISP as registered with de Volksbank.

4.1.5 Request body

Attribute	Type	Mandatory	Description
access accounts balances transactions	Account Access object String String String	Y	This attribute is part of the object *Account Access*. Sub-attributes *accounts*, *balances* and *transactions* must be empty, because de Volksbank only supports consent requests without explicitly mentioning the accounts.
recurringIndicator	Boolean	Y	The value of the attribute *recurringIndicator* is to be set to *true*, if the consent is for a recurring access to the information on funds availability. The value of the attribute *recurringIndicator* is to be set to *false*, if the consent is for a one-off access to the information on funds availability.
validUntil	String	Y	The attribute *validUntil* contains the date indicating until when a CAF consent is valid. The attribute has the ISO 8601 Date format (YYYY-MM-DD).
frequencyPerDay	Number	Y	This field indicates the requested maximum frequency for a CAF call per day. For a one-off access this attribute is set to "1". The value should be 1 or greater.
combinedService Indicator	Boolean	Y	Set to *true* this value indicates that a CAF service will be addressed in the same "session" as another service. De Volksbank only supports the option **false**.

Attribute	Type	Mandatory	Description
account	Account Reference Object	Y	Account details of the debtor. iban: Attribute *iban* is part of the object *Account Reference* as defined by the Berlin Group. ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}. currency: Attribute *currency* is part of the object *Account Reference* as defined by the Berlin Group. SO 4217 Alpha 3 currency code. Only EUR is supported.
iban	String	Y	
currency	String	N	

4.1.6 Example CAF consent request

The CAF consent request is illustrated below:

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v1/funds-confirmation
Content-Type:        application/json
X-Request-ID:        99391c7e-ad88-49ec-a2ad-99ddcb1f7756
Authorization:       l72b095e702f4042e881384c746532defe
{
   "access":
      { "accounts": [],
        "balances": [],
        "transactions": [] },
   "recurringIndicator": true,
   "validUntil": "2020-01-31",
   "frequencyPerDay": 6,
   "combinedServiceIndicator": false,
   "account": {"iban": "NL64ASNB0948305290", "currency": "EUR"}
 }
```

4.1.7 Response code

Code	Description
201	Created

4.1.8 Response header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute invariably filled with the value "*application/json*".

Attribute	Type	Mandatory	Description
Location	String	Y	Attribute contains the location of the created resource.
X-Request-ID	String	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the PIISP).
ASPSP-SCA-Approach	String	Y	Attribute is filled with the value "*REDIRECT*".

4.1.9 Response body

Attribute	Type	Mandatory	Description
consentStatus	Consent Status	Y	In case of a successful consent request (HTTP status code 201), only the status "received", as defined by the Berlin Group, is supported.
consentId	String	Y	Attribute contains the unique identification of the consent.
_links	Links	Y	URL where the TPP can execute the Authorize call (see next section). De Volksbank has opted for the SCA OAuth2 Approach, where the ASPSP transmits the URI where the configuration of the Authorisation Server can be retrieved. The configuration follows the OAuth 2.0 Authorisation Server Metadata specification.

4.1.10 Example CAF consent response

The CAF consent response is illustrated below:

```
HTTP/1.x 201 Created
Content-Type:       application/json
Location:
https://psd.bancairediensten.nl/psd2/snsbank/v1/funds-
confirmation/SNS0123456789012
X-Request-ID:       99391c7e-ad88-49ec-a2ad-99ddcb1f7756
ASPSP-SCA-Approach: REDIRECT
{
   "consentStatus": "received",
   "consentId": "SNS0123456789012",
   "_links": { "scaOAuth": {"href": "
https://psd.bancairediensten.nl/psd2/snsbank/v1/authorize"} }
}
```

4.2 Authorization request: PSU authorizes use of CAF services to the PIISP

The PIISP issues a request with the purpose to receive a URL which re-directs the PSU to the local bank environment in order to allow the PSU to authorize its bank, the ASPSP, to grant the PIISP permission to use the Funds Confirmation call.

In the next sub-sections, we will take a closer look at the elements which constitute the authorization endpoint.

4.2.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/authorize?	Authorization endpoint as defined by de Volksbank.

4.2.2 Path parameters

The authorization endpoint does not have any path parameters.

4.2.3 Query parameters

Attribute	Type	Mandatory	Description
response_type	String	Y	Attribute invariably filled with the value "*code*".
consentId	String	Y	Attribute filled with the value of the consentId as received in the response body to the *POST /v1/funds-confirmation* request. Example: "SNS012345678912"
client_id	String	Y	Attribute filled with the value of the client_id
scope	String	Y	Attribute specifies the level of access that the application is requesting. Invariably filled with the value "*CAF*".
state	String	Y	Attribute contains the unique identification of the request issued by the PIISP. The Berlin Group refers to this attribute as *X-Request-ID*.
redirect_uri	url	Y	Attribute filled with the value where the service redirects the user-agent to after granting the authorization code. No wildcards can be used in the callback URL. De Volksbank validates the exact callback URL.

4.2.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Description filled with the value "*application/x-www-form-urlencoded*".

4.2.5 Request body

The authorize endpoint does not have a request body.

4.2.6 Example authorize request

The authorize request is illustrated below:

```
GET
https://psd.bancairediensten.nl/psd2/snsbank/v1/authorize?response_type=code&consentId=SNS012345678912&client_id=<client_id>&scope=CAF&state=111111&redirect_uri=https://thirdparty.com/callback
Content-Type: application/x-www-form-urlencoded
```

4.2.7 Response code

Code	Description
302	Redirect

4.2.8 Response header

Attribute	Type	Mandatory	Description
location	String	Y	This attribute contains: 1. The URL leading to the login page of the ASPSP; 2. Session data stored in a JWT object (JWT stands for *Json WebToken*).
Content-Type	String	Y	Attribute invariably filled with the value "*text/plain*".

4.2.9 Response body

The authorize endpoint does not have a response body.

4.2.10 Example authorize response

The authorize response is illustrated below:

```
HTTP/1.x 302
location:
https://api.snsbank.nl/online/toestemminggeven/#/login?action=display&sessionID=<sessionID>&sessionData=<sessionData>
Content-Type : text/plain
```

4.3 PSU approving the consent request

PSUs clicking on the link leading them to the ASPSP, will log on to the service to authenticate their identity. Next, the PSU approves the PIISP's request to confirm funds. In cases of success, the service returns an authorization code and redirects the user-agent to the application redirect URI.

The PSU's authentication and the PSU's approval are processes internal to de Volksbank, which we will not describe here. The return of the authorization code, though, we will discuss below.

4.3.1 Response code

Code	Description
302	Redirect

4.3.2 Response parameters

Attribute	Type	Mandatory	Description
code	String	Y	Attribute filled with the authorization code needed to obtain an access and a refresh token. This code can only be used once and exchanged within a configurable time window (currently set to 10 minutes).
state	String	Y	This attribute is filled with the value which the PIISP has delivered in the attribute **state** in the **Authorize** request

The authorization code is then passed on to the PIISP via the re-direct URL the PSU has to its disposition.

4.3.3 Example authorization response

The authorization response is illustrated below:

```
HTTP/1.x 302

https://fintechapplication/redirect?code=869af7df-4ea4-46cf-8bed-
3de27624b29e&state=12345
```

4.4 Access token request: PIISP requesting an access token

The access token and the refresh token are provided on the basis of the authorization code. The PIISP requests an access token from the API, by passing the authorization code along with authentication details, including the client secret, to the API token endpoint.

4.4.1 Method and URL

Method	URL	Description
POST	https://psd.bancairediensten.nl/psd2/ [snsbank|asnbank|regiobank]/v1/token?	Token endpoint as defined by de Volksbank.

4.4.2 Path parameters

The token endpoint does not have any path parameters.

4.4.3 Query parameters

Attribute	Type	Mandatory	Description
grant_type	String	Y	Attribute invariably filled with the value "*authorization_code*"; defines the OAuth2 flow.
code	String	Y	Authorization code needed to obtain an access and a refresh token.
redirect_uri	String	Y	The service redirects the user-agent to the application redirect URI. No wildcards can be used in the callback URL. De Volksbank validates the exact callback URL.

4.4.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute invariably filled with the value "*application/x-www-form-urlencoded*".
X-Request-ID	String	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the PIISP).
Authorization	String	Y	Consist of *client_id* and *client_secret* separated by a colon (**:**) in a **base64** encoded string. – Format: Basic base64 (<client_id>:<client_secret>); – client_id: Identification of the PIISP as registered with de Volksbank; – client_secret: secret agreed between the PIISP and de Volksbank.

4.4.5 Request body

The token endpoint does not have a request body.

4.4.6 Example token request

The token request is illustrated below:

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v1/token?grant_type=authorization_code&code=<authorization_code>&redirect_uri=https://thirdparty.com/callback
Content-Type: application/x-www-form-urlencoded
X-Request-ID: fdb9757d-8f27-4f9e-9be0-0eadacc89012
Authorization: Basic base64(<client_id>:<client_secret>)
```

4.4.7 Response code

If the authorization is valid, the ASPSP will return a response containing an access token and a refresh token to the application. The response will look like this:

Code	Description
200	Ok

4.4.8 Response header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute is invariably filled with the value "*application/json*".

4.4.9 Response body

Attribute	Type	Mandatory	Description
access_token	String	Y	Attribute filled with the access token needed to call the PSD2 interface, in this case CAF.
token_type	String	Y	Attribute filled with the fixed value "*Bearer*".
expires_in	Number	Y	Attribute filled with the lifetime in seconds of the access token.
refresh_token	String	Y	Value in the attribute can be used to obtain a new access token using the same authorization grant in the situation where the current token has expired.
scope	String	Y	Attribute filled with the scope of the access token. In this context *"CAF".*

4.4.10 Example token response

The token response is illustrated below:

```
HTTP/1.x 200
Content-Type: application/json
   {
     "access_token": "<ACCESS_TOKEN>",
     "token_type": "Bearer",
     "expires_in": 600,
     "refresh_token": "<REFRESH_TOKEN>",
     "scope": "CAF"
   }
```

At this point, the PIISP has been authorized. It is allowed use the token to request a confirmation of funds on the user's account via the service API, limited to the scope of access, until the token expires or is revoked. A refresh token may be used to request new access tokens if the original token has expired.

4.5 New access token request: PIISP requesting a new access token

When the original token has expired, the PIISP can request a new access token. A PIISP using an expired token in a funds confirmation request will receive an "Invalid Token Error" response. When this happens, the refresh token can be used to request a fresh access token from the authorization server. The authorization server issues a new refresh token, in which case the client must dispose of the old refresh token and replace it with the new refresh token.

4.5.1 Method and URL

Method	URL	Description
POST	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/token?	Token endpoint as defined by de Volksbank

4.5.2 Path parameters

The token endpoint does not have any path parameters.

4.5.3 Query parameters

Attribute	Type	Mandatory	Description
grant_type	String	Y	Attribute invariably filled with value "*refresh_token*"; defines the OAuth2 flow.
refresh_token	String	Y	Refresh token code needed to obtain the new access and refresh token.
redirect_uri	String	Y	The service redirects the user-agent to the application redirect URI. No wildcards can be used in the callback URL. De Volksbank validates the exact callback URL.

4.5.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute invariably filled with the value "*application/x-www-form-urlencoded*".
X-Request-ID	String	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the PIISP).
Authorization	String	Y	Consist of *client_id* and *client_secret* separated by a colon (**:**) in a **base64** encoded string. – Format: Basic base64 (<client_id>:<client_secret>); – client_id: Identification of the PIISP as registered with de Volksbank; – client_secret: secret agreed between the PIISP and de Volksbank.

4.5.5 Request body

The token endpoint does not have a request body.

4.5.6 Example token request

The token request is illustrated below:

```
POST
https://psd.bancairediensten.nl/psd2/snsbank/v1/token?grant_type=refresh_token&refresh_token=<REFRESH_TOKEN>&redirect_uri=https://thirdparty.com/callback
Content-Type: application/x-www-form-urlencoded
X-Request-ID: fdb9757d-8f27-4f9e-9be0-0eadacc89012
Authorization: Basic base64(<client_id>:<client_secret>)
```

4.5.7 Response code

If the authorization is valid, the ASPSP will return a response containing the access token and a refresh token to the application. The response will look like this:

Code	Description
200	Ok

4.5.8 Response header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute is invariably filled with the value "*application/json*".

4.5.9 Response body

Attribute	Type	Mandatory	Description
access_token	String	Y	Attribute filled with the access token needed to call the PSD2 interface, in this case CAF.
token_type	String	Y	Attribute filled with the fixed value "*Bearer*".
expires_in	Number	Y	Attribute filled with the lifetime in seconds of the access token.
refresh_token	String	Y	Value of the attribute can be used to obtain a new access token using the same authorization grant in the situation where the current token has expired.
scope	String	Y	Attribute filled the scope of the access token. In this context "*CAF*".

4.5.10 Example token response

The token response is illustrated below:

```
HTTP/1.x 200
Content-Type: application/json
   {
     "access_token": "<ACCESS_TOKEN>",
     "token_type": "Bearer",
     "expires_in": 600,
     "refresh_token": "<REFRESH_TOKEN>",
     "scope": "CAF"
   }
```

Now, the PIISP has been authorized again.

5 De Volksbank CAF Services

The Confirmation of the Availability of Funds service (CAF) de Volksbank supports requires an access token in its service call. This access token is delivered in the attribute *Authorization* in the header of the request. When an OAuth 2.0 client submits the request to the resource server, the resource server needs to verify the access token. Only if the access token is valid, the response to this request will be successful.

5.1 Confirmation of Funds

The CAF service call returns a response with a confirmation of the funds of the customer. The response consists solely of a boolean (*true* or *false*), and does not give any additional information about the account. The response is per IBAN, as granted by the consent.

5.1.1 Method and URL

Method	URL	Description
POST	https://psd.bancairediensten.nl/psd2/ [snsbank|asnbank|regiobank]/v1/ funds-confirmation/{consent-id}	Confirmation of funds endpoint.

5.1.2 Path parameters

Attribute	Type	Mandatory	Description
consent-id	String	Y	Attribute contains the unique identification of the consent.

5.1.3 Query parameters

The confirmation of funds request endpoint does not have any query parameters.

5.1.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute invariably filled with the value "*application/json*".
X-Request-ID	String	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the PIISP).
Authorization	String	Y	Attribute filled with the access-token as obtained in the token request call.

5.1.5 Request body

Attribute	Type	Mandatory	Description

Attribute	Type	Mandatory	Description
account iban currency	Account Reference Object String String	Y Y N	Account details of the debtor. iban: Attribute *iban* is part of the object *Account Reference* as defined by the Berlin Group. ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}. currency: Attribute *currency* is part of the object *Account Reference* as defined by the Berlin Group. SO 4217 Alpha 3 currency code.
instructedAmount currency amount	Amount Object String String	Y Y Y	Transaction amount to be checked within the funds check mechanism. currency: Attribute currency is part of the object Amount as defined by the Berlin Group. ISO 4217 Alpha 3 currency code. Only EUR is supported. amount: Attribute amount is part of the object Amount as defined by the Berlin Group. Amount should be in euro. The amount is given with fractional digits, if needed. The decimal separator is a dot (.). The number of fractional digits (or minor unit of currency) must comply with ISO 4217.

5.1.6 Example confirmation of funds request

The confirmation of funds request is illustrated below:

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v1/funds-confirmation/
SNS012345678912
Content-Type:        application/json
X-Request-ID:        fdb9757d-8f27-4f9e-9be0-0eadacc89012
Authorization:       Bearer "<ACCESS-TOKEN>"
{
      "account": {"iban": "NL64ASNB0948305290", "currency": "EUR"},
       "instructedAmount": {"currency": "EUR", "amount": "123.50"}
}
```

5.1.7 Response code

The response will look like this:

Code	Description
200	Ok

5.1.8 Response header

Attribute	Type	Mandatory	Description

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute is invariably filled with the value "*application/json*".
X-Request-ID	String	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the PIISP).

5.1.9 Response body

Attribute	Type	Mandatory	Description
fundsAvailable	boolean	Y	Equals true if sufficient funds are available at the time of the request, false otherwise.

5.1.10 Example confirmation of funds response

The confirmation of funds response is illustrated below:

```
HTTP/1.x 200 Ok
Content-Type:   application/json
X-Request-ID:   fdb9757d-8f27-4f9e-9be0-0eadacc89012
{
    "fundsAvailable": "true"
}
```

5.2 Error handling

5.2.1 HTTP error codes

The possible HTTP error codes that are returned and their meaning can be found in the table below.

Code	Description
400	Bad request The server cannot or will not process the request due to something that is perceived to be a client error (e.g., malformed request syntax, invalid request message framing, or deceptive request routing).
401	Unauthorized The request has not been applied because it lacks valid authentication credentials for the target resource.
403	Forbidden The server understood the request but refuses to authorize it.
404	Not found The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.
406	Not acceptable Cannot generate the content that is specified in the Accept header.
415	Unsupported media type The supplied media type is not supported.

Code	Description
500	Internal server error The server encountered an unexpected condition that prevented it from fulfilling the request.

5.2.2 Additional error information

Errors will be accompanied by additional information in the form of tppMessages. These look like this:

```
{ "tppMessages": [
                    { "category": "ERROR",
                      "code": "ERROR_CODE",
                      "text": "additional text information of the ASPSP up
                       to 512 characters"
                    }
                  ]
}
```

The table below shows the various codes and texts that might be returned.

HTTP status	Category	Code	Text
400	ERROR	FORMAT_ERROR	The format of the X-REQUEST-ID is not valid.
400	ERROR	FORMAT_ERROR	The format of the input is not valid.
400	ERROR	FORMAT_ERROR	One or more input fields are invalid.
400	ERROR	INVALID_ACCOUNT_ NUMBER_FORMAT	The format of the account number is not valid.
400	ERROR	INVALID_INPUT	The parameter is not supported.
400	ERROR	PERIOD_INVALID	The requested time period is out of bounds.
401	ERROR	INVALID_JWT_TOKEN	JWT token is invalid.
401	ERROR	CONSENT_INVALID	The mandate could not be found.
401	ERROR	CONSENT_INVALID	The mandate is revoked.
401	ERROR	CONSENT_INVALID	The mandate has an invalid status.
401	ERROR	CONSENT_INVALID	The entered digipass credentials are invalid.
401	ERROR	CONSENT_INVALID	The selected digipass token is invalid.
401	ERROR	CONSENT_INVALID	The account is not within the contract.
401	ERROR	CONSENT_INVALID	The mandate could not be granted.
401	ERROR	CONSENT_INVALID	The consent is not valid for this service.
401	ERROR	CONSENT_INVALID	The age is not allowed.
401	ERROR	CONSENT_EXPIRED	The expiration date of the mandate has been expired.
401	ERROR	CONSENT_EXPIRED	The consent should be executed once within 10 minutes.
403	ERROR	SERVICE_BLOCKED	The requested service is not allowed for this account.
403	ERROR	SERVICE_BLOCKED	This account's master switch is switched off.
403	ERROR	RESOURCE_UNKNOWN	The account could not be found.
500	ERROR	INTERNAL_SERVER_ERROR	An internal server error occurred.