AIS API

PSD2 interface AIS de Volksbank

January 2019

Colophon

Label	Gegevens
Owner	Service Centre KBS de Volksbank N.V.
Authors	ITC VO KWB Open Banking
Status	AIS ready
Project	PSD2

Version

Version	Date	Changes
1.0	2019-01-18	Final version

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

The document at hand describes the AIS (Account Information Services) interface offered by de Volksbank under PSD2. It explains the process of the consent a PSU (Payment Service User) is required to give for letting a TPP (Third Party Provider) in its role as AISP (Account Information Service Provider) access its account information and the actual account information services for which a consent is given.

The remainder of this document will be organized as follows:

Chapter 2 describes the character set used for the account information to be exchanged between the AISPs and de Volksbank in its role as ASPSP, the datatypes defined for the individual pieces of information and the URLs to be used by the AISPS for the different brands of de Volksbank. Chapter 3 sheds some light on the chosen consent flow. Chapter 4 lays out the fine details of the consent flow and, finally, chapter 5 contains an in-depth explanation of the actual account information services.

2 Account Information Services as offered by de Volksbank

2.1 Conditions on the use of de Volksbank's account information services

The following conditions apply on the usage of the account information services:

1. The first call to any of the account information services currently supported by de Volksbank should be initiated within **10** minutes after the consent has been given by the PSU to the AISP;
2. Each consent granted by a PSU to an AISP is valid for **90** days in accordance with the PSD2 RTS requirements on strong customer authentication;
3. Requirements pertaining to the account information services retrieving information on transactions:
    a. The account information services retrieving information on transactions can only apply to **one** specific account per call;
    b. Only information on transactions dating back to a maximum of **2** years can be retrieved;
    c. Every **next call** returns transactions newer than the previous ones;
    d. Maximum number of transactions in one response has been set to **2000**;
    e. If the AISP does not provide a maximum number of transactions in the call, de Volksbank will use a default value of **1000** transactions.

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 its three different brands: ASN Bank, RegioBank and SNS.

- URL for access granting
  - for TPPs in the role of AISP 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 AISP 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; per brand one specific URL, the so-called bank-URL:
  - for ASN Bank, use: **api.asnbank.nl**
  - for RegioBank, use: **api.regiobank.nl**
  - for SNS Bank, use: **api.snsbank.nl**

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. This implies that dates have the following format: Format: **YYYY-MM-DDThh:mm:ss**.
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 TPP can only use the PSD2 APIs as authorized by de Volksbank. The TPP must be registered with the Competent Authority with a license to perform Account information services (refer to payment service 8 as described in Annex of the Payment Services Directive (2015/2366),
AISPS, 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 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 TPP.

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 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)[1].

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 *Authorization 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.

[1] At this moment these kind of specific PSD2 Certificates cannot be issued by a qualified trusted service provider. As soon as these kind of PSD2 Certificates will become available, de Volksbank will ask for these certificates.

4 The APIs for granting access to account information

The AISPs must use the following APIs for gaining access to account information:

1. consent request;
2. authorization request;
3. access token request: access token and refresh token based on authorization code;
4. new access token request: new access and refresh tokens based on refresh token.

4.1 Consent request: AISP requests permission to use account information of the PSU

By issuing a consent request, the AISP seeks permission from an AISP to access the account information a PSU is holding with the addressed ASPSP on behalf of that particular PSU.

This **consent request** call is illustrated below:

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v1/consents
Content-Type:        application/json
X-Request-ID:        99391c7e-ad88-49ec-a2ad-99ddcb1f7756
Authorization:       <Basic client_id>:<client_secret>
TPP-Redirect-URI:    redirect_uri=https://thirdparty.com/callback

{
   "access":
      { "accounts": [],
        "balances": [],
        "transactions": [] },
   "recurringIndicator": true,
   "validUntil": "2019-01-01",
   "frequencyPerDay": 6,
   "combinedServiceIndicator": false
 }
```

The next table explains the attributes of the **consent request** interface. There are three possible values in the column *Mandatory*:

- Y the attribute is mandatory for that scope
- O the attribute is optional for that scope
- N the attribute is not permitted for that scope

Attribute	Type	Mandatory	Description
url	url	Y	The API consent endpoint.
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 AISP).
Authorization	String	Y	Consist of *client_id* and *client_secret* separated by a colon (**:**) in a **base64** encoded string. – Format: Basic B64(<client_id>:<client_secret>); – client_id: Identification of the AISP as registered with de Volksbank; – client_secret: secret agreed between the AISP and de Volksbank.
TTP_redirect_uri	url	Y	URI of the TPP, where the transaction flow is redirected to after a Redirect.
accounts	String	Y	This attribute is part of the array *Access* and refers to the requested access services. Sub-attributes *accounts*, *balances* and *transactions* must be empty, because de Volksbank only supports consent requests without explicitly mentioning the accounts.
balances	String	Y	Idem.
transactions	String	Y	Idem.
recurringIndicator	Boolean	Y	The value of the attribute *recurringIndicator* is to be set to *true*, if the consent is for recurring access to the account data. The value of the attribute *recurringIndicator* is to be set to *false*, if the consent is for one-off access to the account data.
validUntil	String	Y	The attribute *validUntil* contains a date. The attribute has the ISO 8601 Date format (YYYY-MM-DD). N.B.: the value in this attribute must meet the requirement that *each consent granted by a PSU to an AISP is valid for 90 days in accordance with the PSD2 RTS requirements on strong customer authentication* (see also section2.1.).
frequencyPerDay	Number	Y	This field indicates the requested maximum frequency for an access per day. For a one-off access this attribute is set to "1".
combinedService Indicator	Boolean	Y	Set to *true* this value indicates that a payment initiation service will be addressed in the same "session" as an account information service. De Volksbank only supports the option **false**.

The response of the service **Consent Request** is illustrated below:

```
HTTP/1.x 200 Ok
Content-Type:        application/json
Location:            v1/consents/6ba7b811-9dad-11d1-80b4-00c04fd430c8
X-Request-ID:        99391c7e-ad88-49ec-a2ad-99ddcb1f7756
ASPSP-SCA-Approach: REDIRECT
```

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Invariably filled with the value "*application/json*".
Location	String	Y	Location of the created resource
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
ASPSP-SCA-Approach	String	Y	The field *ASPSP-SCA-Approach* I invariably filled with the value REDIRECT.

4.2 Authorization request: PSU authorizes use of account information to the AISP

The AISP 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 AISP access to the account information of the PSU.

This request call is illustrated below:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1/authorize?
Content-Type:        application/json
Authorization:       <Basic client_id>:<client_secret>
{
   response_type=code&
   consent_id=SNS012345678912&
   scope=AIS&
   state=111111&
   redirect_uri=https://thirdparty.com/callback&
}
```

The next table explains the attributes of the **authorization request** interface. There are three possible values in the column *Mandatory*:

- Y the attribute is mandatory for that scope
- O the attribute is optional for that scope
- N the attribute is not permitted for that scope

Attribute	Type	Mandatory	Description
url	url	Y	the API authorization endpoint.
Content-Type	String	Y	Invariably filled with the value "*application/json*".
Authorization	String	Y	Consist of *client_id* and *client_secret* separated by a colon (**:**) in a **base64** encoded string. – Format: Basic B64(<client_id>:<client_secret>); – client_id: Identification of the AISP as registered with de Volksbank; – client_secret: secret agreed between the AISP and de Volksbank.
response_type	String	Y	Invariably filled with the value "*code*".
consentId	String	Y	Filled with the value of the *consentId* as received in the response to the *POST /v1/consents* request. Example: "SNS012345678912"
scope	String	Y	Specifies the level of access that the application is requesting. Invariably filled with the value "*AIS*".
state	String	Y	Unique identification of the request issued by the TPP. The Berlin Group calls this attribute *X-Request-ID*.
redirect_uri	url	Y	Where the service redirects the user-agent after an authorization code is granted. No wildcards can be used in the call-back URL. De Volksbank validates the exact call-back URL.

The next table explains the attributes of the **authorization response** interface. There are three possible values in the column *Mandatory*:

- Y the attribute is mandatory for that scope
- O the attribute is optional for that scope
- N the attribute is not permitted for that scope

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Invariably filled with the value "*application/json*".
location	String	Y	This attribute contains: 1. The URL leading to the login page of the ASPSP; 2. Session data (JWT, Json WebToken).

The PSU clicking the link to the ASPSP, must first log on to the service to authenticate its identity. Next, the PSU approves the AISP's request to access the PSU's account information. In cases of success, the service returns an authorization code and redirects the user-agent to the application redirect URI.

PSU receives an authorization code.

```
HTTP/1.x 200 Ok
Content-Type: application/json
Location:     https://thirdparty.com/callback
    {
        "grant_type": "authorization_code",
        "code": "<AUTHORIZATION_CODE>"
    }
```

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Invariably filled with the value "*application/json*".
Location	String	Y	URL where the AISP wants to receive the authorization code; in this example https://thirdparty.com/callback.
grant_type	String	Y	Invariably filled with the value "*authorization code*".
code	String	Y	<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).

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

4.3 Access token request: AISP requesting an access token

An access token and a refresh token are provided based on an authorization code. The AISP 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.

Application requests access token.

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v1/token?
Content-Type: application/json
Authorization: <Basic client_id>:<client_secret>
    {
       "grant_type": "authorization_code",
       "code": "<AUTHORIZATION_CODE>"
       "redirect_uri"="https://thirdparty.com/callback"
    }
```

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Filled with the fixed value "*application/json*".
Authorization	String	Y	Consists of client_id and client_secret separated by a colon in a base64 encoded string. – Format: Basic B64(<client_id>:<client_secret>); – client_id: Identification of the AISP as registered with de Volksbank; – client_secret: secret agreed between the AISP and de Volksbank.
grant_type	String	Y	Filled with the fixed 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 call back URL. De Volksbank validates the exact call back URL.

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

Application receives access token.

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

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Filled with the fixed value "*application/json*".
access_token	String	Y	Access token needing to call PSD2 interface, in this case AIS.
token_type	String	Y	Filled with the fixed value "*bearer*".
expires_in	Number	Y	The lifetime in seconds of the access token.
refresh_token	String	Y	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	The scope of the access token. In this context *AIS*.

At this point, the AISP has been authorized. It is allowed use the token to access 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.

4.4 New access token request: AISP requesting a new access token

When the original token has expired, the AISP can request a new access token. An AISP using an expired token in an account information request will receive in 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.

Application requests new access token.

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v1/token?
Content-Type: application/json
Authorization: <Basic client_id>:<client_secret>
   {
      "grant_type": " refresh_token",
      "code": "<REFRESH_TOKEN>"
      "redirect_uri"="https://thirdparty.com/callback"
   }
```

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Filled with the fixed value "*application/json*".
Authorization	String	Y	Consist of client_id and client_secret separated by a colon in a base64 encoded string. – Format: Basic B64(<client_id>:<client_secret>); – client_id: Identification of the AISP as registered with de Volksbank; – client_secret: secret agreed between the AISP and de Volksbank.
grant_type	String	Y	Filled with the fixed value "*refresh_token*"; defines the oauth2 flow.
code	String	Y	Refresh code needing to obtain 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 call back URL. De Volksbank validates the exact call back URL.

If the authorization is valid, the API will send a response containing the access token (and optionally, a refresh token) to the application. The entire response will look like this:

AISP receiving a new access and refresh token.

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

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Filled with the fixed value "*application/json*".
access_token	String	Y	Access token needing to call PSD2 interface, in this case AIS.
token_type	String	Y	Fixed value "*bearer*".
expires_in	Number	Y	The lifetime in seconds of the access token.
refresh_token	String	Y	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	The scope of the access token. In this context *AIS*.

Now, the AISP has been authorized again.

4.5 Error handling

Code	Description
200	Successful operation The request has succeeded.
302	Redirect The target resource resides temporarily under a different URI. Since the redirection might be altered on occasion, the client ought to continue to use the effective request URI for future requests.
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.
500	Internal server error The server encountered an unexpected condition that prevented it from fulfilling the request.

5 De Volksbank AIS Information Services

The Account Information Services (AIS) de Volksbank supports all require an access token in their 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.

The AIS API service calls will return a response with the account information of the customer. The account information consists of IBAN, balance information of the account or transactional information of that account. The response is per IBAN, as granted by the consent. The maximum time period for which transaction history can be shown is currently set at **two** years.

De Volksbank currently supports 3 AIS services which have also been defined by the Berlin Group. These services are the following:

1. Read Account list;
2. Read Balance;
3. Read Transaction List.

The first call should be initiated within **10** minutes after the mandate has been granted.

The services listed above are described in more detail in the following sections.

5.1 Read Account List

5.1.1 Summary

The Account Information Service call **Read Account List** provides information about a PSU's account uniquely identified by an IBAN. Out of a list of account data defined by the Berlin Group, de Volksbank offers the following attributes:

1. IBAN;
2. Currency;
3. Name;
4. Product;
5. BIC.

5.1.2 Service structure

5.1.2.1 Request

The request call of the service **Read Account List** looks like this:

```
GET https://psd.acc.bancairediensten.nl/psd2/snsbank/v1/accounts
Content-Type:       application/json
X-Request-ID:       fdb9757d-8f27-4f9e-9be0-0eadacc89012
Consent-ID:         ABC5678901234567
Authorization:      bearer ACCESS-TOKEN
```

The attributes in the example shown above are defined below:

Attribute	Type	Mandatory	Description
withBalance	Boolean	N	The attribute *withBalance* is a query parameter. The Berlin Group Implementation guide version 1.3 states the following about this parameter: *If contained, this function reads the list of accessible payment accounts including the booking balance, if granted by the PSU in the related consent and available by the ASPSP. This parameter might be ignored by the ASPSP.* N.B.: At the moment, this query parameter cannot be processed by de Volksbank. It should be left out.
Content-Type	String	Y	Filled with the fixed value "*application/json*".
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
Consent-ID	String	Y	Filled with the value of Consent-ID obtained in the consent request call.
Authorization	String	Y	Filled with the access-token as obtained in the token request call.

5.1.2.2 Response

The response of the service **Read Account List** is illustrated below:

```
HTTP/1.x 200 Ok
Content-Type:   application/json
X-Request-ID:   fdb9757d-8f27-4f9e-9be0-0eadacc89012
{"accounts":
    [ { "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",
        "iban": "NL79RBRB0230400868",
        "currency": "EUR",
        "name": "Huishoudpot",
        "product": "Plus Betalen",
        "bic": "RBRBNL21"
      }
    ]
}
```

The attributes in the example shown above are defined below:

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Filled with the fixed value "*application/json*".
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
resourceId	String	Y	A universally unique identifier (UUID), a 128-bit number used to identify the account. This identifier is determined by the ASPSP.
iban	String	N	Unique identification of the account. Format: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}
currency	String	Y	ISO 4217 Alpha 3 currency code.
name	String	N	Name of the account given by the bank or the PSU in Online-Banking.
product	String	N	Product name of the Bank for this account, proprietary definition.
bic	String	N	The BIC associated to the account. Format: [A-Z]{6,6}[A-Z2-9][A-NP-Z0-9]([A-Z0-9]{3,3}){0,1}

5.2 Read Balance

5.2.1 Summary

The Account Information Service **Read Balance** provides information about the balance on a PSU's account uniquely identified by an IBAN. The following balance information is shown:

1. IBAN;
2. Currency;
3. Name;
4. Product;
5. Bic.

For every single call, the service **Read Balance** returns the balance of only one IBAN.

5.2.2 Service structure

5.2.2.1 Request

The request call of the service **Read Balance** looks like this:

```
GET
https://psd.acc.bancairediensten.nl/psd2/snsbank/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/balances
Content-Type:       application/json
X-Request-ID:       fdb9757d-8f27-4f9e-9be0-0eadacc89012
Consent-ID:         ABC5678901234567
Authorization:      bearer ACCESS-TOKEN
```

The attributes in the example shown above are defined below:

Attribute	Type	Mandatory	Description
account-id	String	Y	The UUID identifying the account as returned by the service *Read Account List*. This attribute is used as a **path parameter** in the service call.
Content-Type	String	Y	Filled with the fixed value "*application/json*".
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
Consent-ID	String	Y	Filled with the value of Consent-ID obtained in the consent request call.
Authorization	String	Y	Filled with the access-token as obtained in the token request call.

5.2.2.2 Response

The response of the service **Read Balance** is illustrated below:

```
HTTP/1.x 200 Ok
Content-Type:   application/json
X-Request-ID:   fdb9757d-8f27-4f9e-9be0-0eadacc89012
{
"balances":
    [ { "balanceType": "interimAvailable",
        "balanceAmount": {"currency": "EUR", "amount": "500.00"},
        "lastChangeDateTime": "2017-10-25T15:30:35.035Z"
    } ]
}
```

The attributes in the example shown above are defined below:

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Filled with the fixed value "*application/json*".
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
iban	String	N	Attribute is part of the array *Account Reference* as defined by the Berlin Group. This attribute is optional and, therefore, de Volksbank does not return it.
balanceType	String	Y	De Volksbank only supports the balance type *interimAvailable*
currency	String	Y	Attribute is part of the array *Amount* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code

Attribute	Type	Mandatory	Description
amount	String	Y	Attribute is part of the array *Amount* as defined by the Berlin Group. The amount 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. totalDigits: 18 fractionDigits: 5.
lastChangeDateTime	String	N	Required format is ISODateTime

5.3 Read Transaction List

5.3.1 Summary

The Account Information Service **Read Transaction List** provides transaction detail information about a PSU's account uniquely identified by an IBAN. The following transaction information is shown:

1. Transaction status: de Volksbank only delivers account information on booked transactions;
2. entryReference;
3. endToEndId;
4. mandateId;
5. creditorId;
6. bookingDate;
7. valueDate;
8. transactionAmount;
9. creditorName;
10. creditorAccount;
11. debtorName;
12. debtorAccount;
13. remittanceInformationUnstructured;
14. purposeCode;
15. bankTransactionCode;
16. proprietaryBankTransactionCode.

For every single call, the service **Read Transaction List** returns the balance of only one IBAN submitted in the path parameter account in the request.

5.3.2 Service structure

5.3.2.1 Request

The request call of the service **Read Transaction List** looks like this:

```
GET
https://psd.acc.bancairediensten.nl/psd2/snsbank/v1/accounts/mdw3456reqeng7890/transactions?dateFrom=2018-11-24&dateTo=2018-11-24&entryReferenceFrom=201823999&bookingStatus="booked"&limit=1000&pageDirerction="next"
Content-Type:  application/json
X-Request-ID:  fdb9757d-8f27-4f9e-9be0-0eadacc89012
```

```
Consent-ID:    ABC5678901234567
Authorization: bearer ACCESS-TOKEN
```

Attribute	Type	Mandatory	Description
account-id	String	Y	The UUID identifying the account as returned by the service *Read Account List*. This attribute is used as a **path parameter** in the service call.
dateFrom	String	N	Start date of the period for which an account statement is requested. Attribute has the ISO 8601 Date format (YYYY-MM-DD).
dateTo	String	N	End date of the period for which an account statement is requested. Attribute has the ISO 8601 Date format (YYYY-MM-DD).
entryReferenceFrom	String	N	The attribute *entryReferenceFrom* is a concatenation of journaldate and a sequence number. The format is YYYYMMDD-XXXXXXXXXXX. The journal date has the format is YYYYMMDD. The sequence number has the format XXXXXXXXXXX. It is a numerical string with a maximum of 12 digits without leading zeros.
bookingStatus	String	Y	The Berlin Group Implementation guide version 1.3 states the following: *Permitted codes are "booked", "pending" and "both". "booked" shall be supported by the ASPSP. To support the "pending" and "both" feature is optional for the ASPSP, Error code if not supported in the online banking frontend.* De Volksbank accepts the values “**booked**” and “**both**”, but de Volksbank will only return transactions with the status “**booked**”.
limit	Number	N	Maximum number of transactions in the response. De Volksbank has set the **maximum** limit to **2000** transactions. De Volksbank has set the **default** limit to **1000** transactions.
pageDirection	String	N	The attribute *pageDirection* refers to the direction of the search. Starting point is the value in the attribute *entryReferenceFrom*. The allowable values are “**previous**” and “**next**”. This attribute is used to build up the 'previous' and 'next' links in the attribute *_links* of the response.
Content-Type	String	Y	Filled with the fixed value "*application/json*".
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
Consent-ID	String	Y	Filled with the value of Consent-id obtained in the consent request call.
Authorization	String	Y	Filled with the access-token as obtained in the token request call.

5.3.2.2 Response

The response of the service **Read Transaction List** is illustrated below:

```
HTTP/1.x 200 Ok
Content-Type:  application/json
X-Request-ID:  fdb9757d-8f27-4f9e-9be0-0eadacc89012
{ "account":{
     "iban":"NL86SNSB0256012733",
     "currency":"EUR"
  },
  "transactions":{
   "booked":[
      {
      "entryReference":"20190101-33263746",
      "endToEndId":"12345678901234567890123456789012345",
      "mandateId":"",
      "creditorId":"",
      "bookingDate":"2017-10-25",
      "valueDate":"2017-10-25",
      "transactionAmount":{"currency":"EUR","amount":"256.67"},
      "creditorName":"Constant Kaanen",
      "creditorAccount":{"iban":"NL64SNSB0123456789","currency":"EUR"},
      "debtorName":"",
      "debtorAccount":{"iban":"","currency":"EUR"},
      "remittanceInformationUnstructured":"Uw toelage",
      "purposeCode":"",
      "bankTransactionCode":"3723",
      "proprietaryBankTransactionCode":"FNGI"}
],
      "_links":{
         "account":{
            "href":"/psd/v1/accounts/3fdb8946-52ee-4a6d-8a0c-
c7ba6f4a45ed"
         },
         "next":{
            "href":"/psd/v1/accounts/3fdb8946-52ee-4a6d-8a0c-
c7ba6f4a45ed/transactions?bookingStatus=booked&limit=2000&pageDirection=n
ext&entryReferenceFrom=20190105-30026081"
         },
```

```
          "previous":{
             "href":"/psd/v1/accounts/3fdb8946-52ee-4a6d-8a0c-
c7ba6f4a45ed/transactions?bookingStatus=booked&limit=2000&pageDirection=p
revious&entryReferenceFrom=20170117-30000010"
          }
       }
    }
}
```

The list of attributes used in the example above is defined below:

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Filled with the fixed value "*application/json*".
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
account	Account Reference array	N	iban: ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30} currency: ISO 4217 Alpha 3 currency code
entryReference	String	N	The attribute *entryReference* is a concatenation of journaldate and a sequence number. The format is YYYYMMDD-XXXXXXXX. The journal date has the format is YYYYMMDD. The sequence number has the format XXXXXXXX. It is a numerical string with a maximum of 8 digits without leading zeros.
endToEndId	String	N	Unique end to end id as provided by the TPP. The ISO 20022 length of is Max35Text.
mandateId	String	N	The attribute *mandateId* contains the unique identification, as assigned by the creditor, to unambiguously identify the mandate belonging to a direct debit agreement. The ISO 20022 length of the *mandateId* value is Max35Text.
creditorId	String	N	EPC rulebook attribute AT-02 for SEPA Direct Debits: Identifier of the Creditor. Max35Text
bookingDate	String	N	The date when an entry is posted to an account on the ASPSPs books. Format is YYYYMMDD
valueDate	String	N	The date at which assets become available to the account owner in case of a credit. Format is YYYYMMDD

Attribute	Type	Mandatory	Description
transactionAmount: currency amount	Amount array String String	Y	Attribute *currency* is part of the array *Amount* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code Attribute *amount* is part of the array *Amount* as defined by the Berlin Group. 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. totalDigits 18 fractionDigits 5.
creditorName	String	N	Party to which an amount of money is due. Max70Text
creditorAccount iban currency	Account Reference array String	N	iban: ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30} currency: ISO 4217 Alpha 3 currency code
debtorName	String	N	Party that owes an amount of money to the (ultimate) creditor. Max70Text
debtorAccount iban currency	Account Reference array String	N	iban: ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30} currency: ISO 4217 Alpha 3 currency code
remittanceInformationUnstructured	String	N	Max140Text.
purposeCode	String	N	Filled with a value belonging to the ISO 20022 ExternalPurpose1Code set.
bankTransactionCode	String	N	Filled with a value belonging to the ISO 20022 ExternalPaymentTransactionStatus1Code set. Note.: De Volksbank will fill in a numerical code, as de Volksbank does not use the ISO 20022 codes.
proprietaryBankTransactionCode	String	N	The proprietary transaction code used by de Volksbank. Max35Text
_links	Links	N	A list of hyperlinks to be recognised by the TPP.
link.	String	N	Values used by de Volksbank: 1. account; 2. next; 3. previous;
href	String	Y	No specific length defined by the Berlin Group.

5.4 Error handling

Code	Description
200	Successful operation The request has succeeded.
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.
500	Internal Server Error The server encountered an unexpected condition that prevented it from fulfilling the request.

APPENDIX A: List of bank TransactionCode and *proprietaryBankTransactionCodes* used by de Volksbank

Debit entries

Product / Channel	Domain	bank Transaction Code	proprietary Bank Transaction Code "FXXX"
Credit Transfers outgoing (minus/debit) <SEPA SCT & SCTInstant>			
Internet	Own accounts	3724	NGI
	SCT within a bank brand	3723	NGI
	SCTinst within the bank / brands	9930	IOI
	SCT within the Nederlands	9720	NGI
	SCTinst within the Netherlands	9933	IOI
	SCT SEPA (excl. NL)	9747	OVS
Corporate Internet Banking batch booking	Own accounts, within the bank, the Nettherlands, SEPA	9722	OVS
Mobile app	Own accounts	3754	NGM
	SCT within a bank brand	3753	NGM
	SCTinst within the bank / brands	9932	IOM
	SCT within the Nederlands	9755	NGM
	SCTinst within the Netherlands	9935	IOM
	SCT SEPA (excl. NL)	9747	OVS
Payment with Payconiq (app)	SCT within a bank brand	3719	PCQ
	SCT within the Netherlands / SEPA	9719	PCQ
Via third party (TPP PSD2)	Own accounts	3758	TPP
	SCT within a bank brand	3757	TPP
	SCTinst within the bank / brands	9931	ITP
	SCT within the Nederlands	9759	TPP
	SCTinst within the Netherlands	9934	ITP
	SCT SEPA (excl. NL)	9747	OVS
Paper based payment	Within the bank / the Netherlands	9846	OVS
(Optical readable form)	SCT SEPA (excl. NL)	9747	OVS
Via IVR (phone)	Own accounts	3795	OVS
Via local office or headoffice	Own accounts	3025	OVS
	SCT within a bank brand	3026	OVS
	SCT within the Netherlands / SEPA	9801	OVS
Recall (error bank)	Within the bank and the Netherlands	9718	RTI
Acceptgiro Outgoing (minus/debit) <SEPA SCT, Local instrument = ACCEPT>			
Internet	SCT within the Netherlands	9721	NGI
Mobile app	SCT within the Netherlands	9756	NGM
Paper based payment (optical readable)	SCT within the Netherlands	9844	ACC
iDEAL outgoing (minus/debit) <SEPA SCT, Local instrument = IDEAL>			
Internet	SCT within the Netherlands / SEPA	9806	IDE
Mobile appl	SCT within the Netherlands / SEPA	9856	IDM
Dutch Urgent payments / TNS outgoing (minus/debit)			
Internet	the Netherlands	9729	OVS

Product / Channel	Domain	bank Transaction Code	proprietary Bank Transaction Code "FXXX"
Local office with charges	the Netherlands	9772	OVS
Local office without charges	the Netherlands	9773	OVS
Foreign payments (NON SEPA) outgoing (minus/debit)			
Internet	World	7727	OVS
Local office	World	7761	OVS
SEPA Direct Debets (minus/debit)			
CORE SDD	the Netherlands and SEPA	9714	EIC
B2B SDD	the Netherlands and SEPA	9827	EIC
Overheidsvordering (Govermental debit)	the Netherlands	9885	MSC
SDDReturn	the Netherlands and SEPA	9715	RTI
SDD Refund	the Netherlands and SEPA	9716	RTI
SDD Reversal	the Netherlands and SEPA	9717	RTI
SDD Reject	by creditor bank	9842	RTI
Automated credit transfers outgoing (minus/debit)			
Automated deposits (internet)	Own accounts, fixed amount	3700	POV
	Own accounts, cash pooling	3701	POV
Standing orders (internet, mobile app, local office)	Bank/Nederland/SEPA	9802	POV
Cash withdrawel (minus/debit)			
Local office	RegioBank	1002	KAS
ATM SNS	SNS	1003 / 7008	GEA
ATM NL (Meastro)	the Netherlands	7900 / 9900	GEA
ATM NL (VPay)	the Netherlands	7910 / 9910	GEA
ATM EU (Meastro)	Europe	7901 / 9901	GEA
ATM EU (VPay)	Europe	7911 / 9911	GEA
ATM World (Meastro)	World	9902	GEA
ATM World (VPay)	World	9912	GEA
POS Card payments (minus/debit)			
POS NL (Meastro)	the Netherlands	7903 / 9903	BEA
POS NL (VPay)	the Netherlands	7913 / 9913	BEA
POS EU (Meastro)	Europe	7904 / 9904	BEA
POS EU (VPay)	Europe	7914 / 9914	BEA
POS World (Meastro)	World	9905	BEA
POS World (VPay)	World	9915	BEA
Mobile payments / NFC (minus/debit)			

Product / Channel	Domain	bank Transaction Code	proprietary Bank Transaction Code "FXXX"
NFC NL (Meastro)	the Netherlands	7906 / 9906	BEA
NFC NL (VPay)	the Netherlands	7916 / 9916	BEA
NFC EU (Meastro)	Europe	7907 / 9907	BEA
NFC EU (VPay)	Europe	7917 / 9917	BEA
NFC World (Meastro)	World	9908	BEA
NFC World (VPay)	World	9918	BEA
Interest, commissions & charges (minus/debit)			
Interest accumulated		7606	AFB
Interest accumulated (when account closing)		7618	AFB
Interest capitalized		7600	MSC
Interest (to be transfered to other account)		7602	MSC
Interest capatalized (when account closing)		7604	MSC
Interest correction		7225	AFB
Interest, commissions & charges corporate accounts		7617	AFB
Interest, commissions & charges corporate accounts (account closing)		7628	AFB
Commission account usage		7241	MSC
Charges usage card		7227	AFB
Commissions Corporate Internet Banking		7734	MSC
Transaction downloading costs Corporate Internet Banking		7737 / 7738	MSC
Charges sending paper statement		7236	AFB
Charges paper based credit transfers		7240	MSC
Charges Dutch Urgent payments		7237	MSC
Charges ATM		7921 / 9921	MSC
Charges POS		7922 / 9922	BEA

Credit entries

Product / Channel	Domain	bank Transaction Code	proprietary Bank Transaction Code "FXXX"
Credit Transfers Incoming (plus/credit) <SEPA SCT & SCTInstant>			
Own accounts	Internet	2724	NGI
	Mobile app	2754	NGM
	Via third party (TPP PSD2)	2758	TPP
	IVR (phone)	2795	OVS
	Via local office or headoffice	2025	OVS
Within a bank brand of de Volksbank	Internet	2723	NGI
	Internet batch booking	8722	OVS

Product / Channel	Domain	bank Transaction Code	proprietary Bank Transaction Code "FXXX"
	Mobile app	2753	NGM
	Payment with Payconiq (app)	2719	PCQ
	Via third party (TPP PSD2)	2757	TPP
	Via local office or headoffice	2026	OVS
	SCTInst Internet/mobile/third party	8948	IOS
Payment request (credit via iDEAL)	Mobile app	6853	BVZ
Between brands of de Volksbank	SCT Internet/mobile/third party	8746	OVS
	Via local office or headoffice	8743	OVS
	SCTInst Internet/mobile/third party	8948	IOS
the Nederlands and SEPA	All channels (SCT)	8809	OVS
	Alle channeld (SCTInst)	8949	IOS
SCT Return	Return posting received	8749	RTI
Acceptgiro incoming (plus/credit) <SEPA SCT, local instrument = ACCEPT>			
the Nederlands	All channels (SCT)	8845	ACC
iDEAL incoming (plus/credit) <SEPA SCT, Local instrument = IDEAL>			
Netherlands/SEPA	Internet/Mobile	8806	IDE
Netherlands/SEPA batch booking	Internet/Mobile	2806	IDE
Dutch Urgent Payments / TNS incoming (plus/credit)			
Between brands of de Volksbank	All channels	8783	OVS
the Netherlands	All channels	8872	OVS
Foreign payments (NON SEPA) incoming (plus/credit)			
World	All channels	6761	OVS
SEPA Direct Debets (plus/credit)			
SDD Return	by debtor bank	8715	RTI
SDD Refund	Internet/mobile app/local office	8716	RTI
SDD Reversal		8717	RTI
SDD Core one-off	Corporate internet banking	8820	EIC
SDD Core recurring	Corporate internet banking	8821	EIC
SDD Reject	by creditor bank	8842	RTI
Automated credit transfers incoming (plus/credit)			
Own accounts, fixed amount	Internet	2700	POV
Own accounts, cash pooling	Internet	2701	POV
Standing order within a bank brand of de Volksbank	Internet/Mobile app/ Local office	8706	POV

Product / Channel	Domain	bank Transaction Code	proprietary Bank Transaction Code "FXXX"
Standing order between brands of de Volksbank	Internet/Mobile app/ Local office	8744	POV
Cash deposit (plus/credit)			
Local office	RegioBank	0001	KAS
ATM NL (Meastro), credit correction	the Netherlands	6900 / 8900	GEA
ATM NL (VPay), credit correction	the Netherlands	6910 / 8910	GEA
ATM EU (Meastro), credit correction	Europe	6901 / 8901	GEA
ATM EU (VPay), credit correction	Europe	6911 / 8911	GEA
ATM World (Meastro), credit correction	World	8902	GEA
ATM World (VPay), credit correction	World	8912	GEA
POS Card payment (plus/credit)			
POS NL (Meastro), credit correction	the Netherlands	6903 / 8903	BEA
POS NL (VPay), credit correction	the Netherlands	6913 / 8913	BEA
POS EU (Meastro), credit correction	Europe	6904 / 8904	BEA
POS EU (VPay), credit correction	Europe	6914 / 8914	BEA
POS World (Meastro), credit correction	World	8905	BEA
POS World (VPay), credit correction	World	8915	BEA
POS Card Refund (plus/credit)			
POS (Maestro)		8909	RTI
POS (Vpay)		8920	RTI
Mobile payments / NFC (plus/credit)			
NFC NL (Meastro), credit correction	the Netherlands	6906 / 8906	BEA
NFC NL (VPay), credit correction	the Netherlands	6916 / 8916	BEA
NFC EU (Meastro), credit correction	Europe	6907 / 8907	BEA
NFC EU (VPay), credit correction	Europe	6917 / 8917	BEA
NFC World (Meastro), credit correction	World	8908	BEA
NFC World (VPay), credit correction	World	8918	BEA
Interest, commissions & charges (plus/credit)			
Interest accumulated		6607	BIJ
Interest accumulated (when account closing)		6619	BIJ
Interest capitalized		6600	MSC
Interest (to be transfered to other account)		6602	MSC
Interest capatalized (when account closing)		6604	MSC
Interest, commissions & charges corporate accounts		6617	AFB

Product / Channel	Domain	bank Transaction Code	proprietary Bank Transaction Code "FXXX"
Interest, commissions & charges corporate accounts (account closing)		6628	AFB
Corrections		6230	AFB