

# AIS API

PSD2 interface AIS de Volksbank

July 2019

## Colophon

Label	Data
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
1.1	2019-04-23	Change log: <ul style="list-style-type: none"><li>– The document structure has been adapted to the structure of the PIS API document for reasons of consistency;</li><li>– The chapters about the Authorize and Token endpoints have been updated.</li></ul>
1.2	2019-07-05	Change log: Updated request and response objects and headers (4).

## References

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

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION</b>	<b>6</b>
<b>2</b>	<b>ACCOUNT INFORMATION SERVICES AS OFFERED BY DE VOLKSBANK</b>	<b>7</b>
2.1	CONDITIONS ON THE USE OF DE VOLKSBANK'S ACCOUNT INFORMATION SERVICES	7
2.2	CHARACTER SET	7
2.3	DATA TYPES	7
2.4	URLS	8
<b>3</b>	<b>ACCESS</b>	<b>9</b>
3.1	CERTIFICATES	9
3.2	AUTHENTICATION BY OAUTH2	9
3.3	AUTHORIZATION	9
<b>4</b>	<b>THE APIS FOR GRANTING ACCESS TO ACCOUNT INFORMATION</b>	<b>10</b>
4.1	CONSENT REQUEST: AISP REQUESTS PERMISSION TO USE ACCOUNT INFORMATION OF THE PSU	10
4.1.1	<i>Method and URL</i>	10
4.1.2	<i>Path parameters</i>	10
4.1.3	<i>Query parameters</i>	10
4.1.4	<i>Request header</i>	11
4.1.5	<i>Request body</i>	11
4.1.6	<i>Example consent request</i>	11
4.1.7	<i>Response code</i>	12
4.1.8	<i>Response header</i>	12
4.1.9	<i>Response body</i>	12
4.1.10	<i>Example consent response</i>	13
4.2	AUTHORIZATION REQUEST: PSU AUTHORIZES USE OF ACCOUNT INFORMATION TO THE AISP	13
4.2.1	<i>Method and URL</i>	13
4.2.2	<i>Path parameters</i>	13
4.2.3	<i>Query parameters</i>	13
4.2.4	<i>Request header</i>	14
4.2.5	<i>Request body</i>	14
4.2.6	<i>Example authorize request</i>	14
4.2.7	<i>Response code</i>	14
4.2.8	<i>Response header</i>	14
4.2.9	<i>Response body</i>	14
4.2.10	<i>Example authorize response</i>	14
4.3	PSU APPROVING THE CONSENT REQUEST	15
4.3.1	<i>Response code</i>	15
4.3.2	<i>Response parameters</i>	15
4.3.3	<i>Example authorization response</i>	15
4.4	ACCESS TOKEN REQUEST: AISP REQUESTING AN ACCESS TOKEN	15
4.4.1	<i>Method and URL</i>	16
4.4.2	<i>Path parameters</i>	16
4.4.3	<i>Query parameters</i>	16
4.4.4	<i>Request header</i>	16

4.4.5	<i>Request body</i> .....	16
4.4.6	<i>Example token request</i> .....	16
4.4.7	<i>Response code</i> .....	17
4.4.8	<i>Response header</i> .....	17
4.4.9	<i>Response body</i> .....	17
4.4.10	<i>Example token response</i> .....	17
4.5	<b>NEW ACCESS TOKEN REQUEST: AISP REQUESTING A NEW ACCESS TOKEN</b> .....	18
4.5.1	<i>Method and URL</i> .....	18
4.5.2	<i>Path parameters</i> .....	18
4.5.3	<i>Query parameters</i> .....	18
4.5.4	<i>Request header</i> .....	18
4.5.5	<i>Request body</i> .....	19
4.5.6	<i>Example token request</i> .....	19
4.5.7	<i>Response code</i> .....	19
4.5.8	<i>Response header</i> .....	19
4.5.9	<i>Response body</i> .....	19
4.5.10	<i>Example token response</i> .....	20
<b>5</b>	<b>DE VOLKSBANK ACCOUNT INFORMATION SERVICES</b> .....	<b>21</b>
5.1	<b>READ ACCOUNT LIST</b> .....	21
5.1.1	<i>Method and URL</i> .....	21
5.1.2	<i>Path parameters</i> .....	21
5.1.3	<i>Query parameters</i> .....	22
5.1.5	<i>Request body</i> .....	22
5.1.6	<i>Example Read Account List request</i> .....	22
5.1.7	<i>Response code</i> .....	22
5.1.8	<i>Response header</i> .....	22
5.1.9	<i>Response body</i> .....	23
5.1.10	<i>Example Read Account List response</i> .....	23
5.2	<b>READ BALANCE</b> .....	24
5.2.1	<i>Method and URL</i> .....	24
5.2.2	<i>Path parameters</i> .....	24
5.2.3	<i>Query parameters</i> .....	24
5.2.5	<i>Request body</i> .....	24
5.2.6	<i>Example Read Balance request</i> .....	24
5.2.7	<i>Response code</i> .....	25
5.2.8	<i>Response header</i> .....	25
5.2.9	<i>Response body</i> .....	25
5.2.10	<i>Example Read Balance response</i> .....	26
5.3	<b>READ TRANSACTION LIST</b> .....	26
5.3.1	<i>Method and URL</i> .....	27
5.3.2	<i>Path parameters</i> .....	27
5.3.3	<i>Query parameters</i> .....	27
5.3.5	<i>Request body</i> .....	28
5.3.6	<i>Example Read Transaction List request</i> .....	28
5.3.7	<i>Response code</i> .....	28
5.3.8	<i>Response header</i> .....	28
5.3.9	<i>Response body</i> .....	29
5.3.10	<i>Example Read Transaction List response</i> .....	32
5.4	<b>HTTP CODES FOR FAILURE (ERROR HANDLING)</b> .....	33

**APPENDIX A: LIST OF BANK TRANSACTIONCODE AND PROPRIETARYBANKTRANSACTIONCODES  
USED BY DE VOLKSBANK..... 34**

# 1 Introduction

This document 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 of AISP (Account Information Service Provider) access its account information and the actual account information services for which a consent is given.

It should be noted that this interface complies with Berlin Group standards (NextGenPSD2 XS2A Framework Implementation Guidelines V1.3);

The remainder of this document will be organized as follows:

- Chapter 2 describes the conditions de Volksbank applies to the use of its account initiation services, 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;
- 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 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 an AISP is valid for **90** days in accordance with the PSD2 RTS requirements on strong customer authentication. The refresh token is as such valid for 90 days.
4. 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 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 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, 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 <u>date</u> format. This implies that dates have the following format: <b>YYYY-MM-DD</b> .
	ISO 8601 datetime format	Dates are of the data type string, but must comply with the ISO 8601 <u>datetime</u> format.
String	Decimal format	Amount fields are of the data type <i>string</i> , but have the format of a <i>decimal</i> where the following format requirements hold: <ol style="list-style-type: none"> <li>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);</li> <li>2. The digits denoting integers and the digits denoting fractions are separated by a <b>dot</b>.</li> </ol>
Number	Integer format	Number is an integer starting at 0, 1, 2, ...



## 3 Access

The AISP can only use the PSD2 APIs as authorized by de Volksbank. The AISP 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 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 AISP.

### 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 *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.

## 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 (creation of a consent id);
2. 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) do not receive an approval of the PSU the consent is automatically expired.

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.

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.

For every individual endpoint de Volksbank offers, we will point out which of these elements they have and explain them in depth.

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

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

In the sub-sections to come, we will discuss at length the parts which make up the consent request.

#### 4.1.1 Method and URL

Method	URL	Description
POST	<a href="https://psd.bancairediensten.nl/psd2/[snsbank asnbank regiobank]/v1/consents">https://psd.bancairediensten.nl/psd2/[snsbank asnbank regiobank]/v1/consents</a>	Consent request endpoint as defined by the Berlin Group in the implementation guide version 1.3.

#### 4.1.2 Path parameters

The consent request endpoint does not have any path parameters.

#### 4.1.3 Query parameters

The 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 " <i>application/json</i> ".
X-Request-ID	String	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
Authorization	String	Y	Attribute consists of <i>client_id</i> : identification of the AISP as registered with de Volksbank.

#### 4.1.5 Request body

Attribute	Type	Mandatory	Description
access	Account Access object	Y	This attribute is part of the object <i>Account Access</i> and refers to the requested access services. Sub-attributes <i>accounts</i> , <i>balances</i> and <i>transactions</i> must be empty, because de Volksbank only supports consent requests without explicitly mentioning the accounts.
accounts	String		
balances	String		
transactions	String		
recurringIndicator	Boolean	Y	The value of the attribute <i>recurringIndicator</i> is to be set to <i>true</i> , if the consent is for a recurring access to the account data. The value of the attribute <i>recurringIndicator</i> is to be set to <i>false</i> , if the consent is for a one-off access to the account data.
validUntil	String	Y	The attribute <i>validUntil</i> 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 section 2.1).
frequencyPerDay	Number	Y	This field indicates the requested maximum frequency for an access per day. For example: for a one-off access this attribute is set to "1".
combinedService Indicator	Boolean	Y	Set to <i>true</i> 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 <b>false</b> .

#### 4.1.6 Example consent request

The **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: 171bc95e703f6042e881384c746532dcfe

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

#### 4.1.7 Response code

Code	Description
201	Created POST response code where consent request was correctly performed.

#### 4.1.8 Response 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 AISP).

#### 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 BerlinGroup is supported.
consentId	String	Y	Attribute contains the unique identification of the consent.
_links	Links	Y	All links can be relative or full links. The choice to be made is up to the discretion of the ASPSP.  " <b>scaOAuth</b> ": In case of a SCA OAuth2 Approach, the ASPSP is transmitting 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 consent response

The response to the service **consent request** is illustrated below:

```
HTTP/1.x 201 Created
Content-Type:      application/json
X-Request-ID:     99391c7e-ad88-49ec-a2ad-99ddcb1f7756
{
  "consentStatus": "received",
  "consentId": "SNS0123456789012",
  "_links": { "scaOAuth": {"href": "https://oauth-
client.devolksbank.nl/auth-srv/oauth/authorize"} }
}
```

## 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.

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".
scope	String	Y	Attribute specifies the level of access that the application is requesting. Invariably filled with the value "A/S".
state	String	Y	Attribute contains the unique identification of the request issued by the AISP.
consentId	String	Y	Attribute contains the unique identification of the consent.

Attribute	Type	Mandatory	Description
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 call-back URL.  De Volksbank validates the exact call-back URL.
client_id	String	Y	Attribute filled with the value of the client_id

#### 4.2.4 Request header

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

#### 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=c
ode&scope=AIS&state=111111&consentId=SNS0123456789012&redirect_uri=https:
//thirdparty.com/callback&client_id=<client_id>
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: <ol style="list-style-type: none"> <li>The URL leading to the login page of the ASPSP;</li> <li>Session data stored in a JWT object (JWT stands for <i>Json WebToken</i>).</li> </ol>
Content-Type	String	Y	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 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.

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 AISP has delivered in the attribute <b>state</b> in the <b>Authorize</b> request

The authorization code is then passed on to the AISP 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: AISP requesting an access token

The access token and the refresh token are provided on the basis of the 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.

#### 4.4.1 Method and URL

Method	URL	Description
POST	<a href="https://psd.bancairediensten.nl/psd2/[snsbank asnbank regiobank]/v1/token?">https://psd.bancairediensten.nl/psd2/[snsbank asnbank regiobank]/v1/token?</a>	Authorization 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	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.

#### 4.4.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	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 AISP).
Authorization	String	Y	Consist of <i>client_id</i> and <i>client_secret</i> separated by a colon (:) in a <b>base64</b> encoded string. – Format: Basic base64 (<client_id>:<client_secret>); – <i>client_id</i> : Identification of the AISP as registered with de Volksbank; – <i>client_secret</i> : secret agreed between the AISP 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=AUTORIZATION\_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 "AIS".
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 "AIS".

#### 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": "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.

## 4.5 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 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?	Authorization 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 filled with filled with the fixed value "refresh_token"; defines the OAuth2 flow.
code	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 call back URL. De Volksbank validates the exact call back URL.

### 4.5.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	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 AISP).

Attribute	Type	Mandatory	Description
Authorization	String	Y	Consist of <i>client_id</i> and <i>client_secret</i> separated by a colon (:) in a <b>base64</b> encoded string. - Format: Basic base64 (<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.

#### 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&code=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 " <i>application/json</i> ".

#### 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 "A/S".
token_type	String	Y	Attribute filled with the fixed value " <i>bearer</i> ".
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 "A/S".
-------	--------	---	--

#### 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": "AIS"
}
```

Now, the AISP has been authorized again.

## 5 De Volksbank Account 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 three 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 to any of these services 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

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.

#### 5.1.1 Method and URL

Method	URL	Description
GET	<a href="https://psd.bancairediensten.nl/psd2/[snsbank asnbank regiobank]/v1/accounts">https://psd.bancairediensten.nl/psd2/[snsbank asnbank regiobank]/v1/accounts</a> {query parameters}	Account information endpoint as defined by the Berlin Group in the implementation guide version 1.3.

#### 5.1.2 Path parameters

The Read Account List endpoint does not have any path parameters.

### 5.1.3 Query parameters

Attribute	Type	Mandatory	Description
withBalance	Boolean	N	<p>The Berlin Group Implementation guide version 1.3 states the following about the attribute <i>withBalance</i>:</p> <p><i>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.</i></p> <p><b>N.B.:</b> At the moment, this query parameter cannot be processed by de Volksbank. It should be left out.</p>

### 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 AISP).
ConsentId	String	Y	Attribute filled with the value of the ConsentId obtained in the consent request call.
Authorization	String	Y	Attribute filled with the access-token as obtained in the token request call.

### 5.1.5 Request body

The Read Account List endpoint does not have a request body.

### 5.1.6 Example Read Account List request

The Read Account List request is illustrated below:

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

### 5.1.7 Response code

The response will look like this:

Code	Description
200	Ok

### 5.1.8 Response header

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

Attribute	Type	Mandatory	Description
X-Request-ID	String	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the AISP).

### 5.1.9 Response body

Attribute	Type	Mandatory	Description
accounts	Account Details object	Y	resourceId: A universally unique identifier (UUID), a 128-bit number used to identify the account. This identifier is determined by the ASPSP.
resourceId	String	Y	
iban	String	N	
currency	String	Y	
name	String	N	iban:
product	String	N	Unique identification of the account.
bic	String	N	Format: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}
			currency: ISO 4217 Alpha 3 currency code.
			name: Name of the account given by the bank or the PSU in Online-Banking.
			product: Product name of the Bank for this account, proprietary definition.
			bic: 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}

### 5.1.10 Example Read Account List response

The Read Account List response 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"
    }
]
}

```

## 5.2 Read Balance

The Account Information Service **Read Balance** provides information about the balance on a PSU's account uniquely identified by an IBAN. For every single call, the service **Read Balance** returns the balance of only one IBAN.

### 5.2.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank asnbank regiobank]/v1/accounts/{account-id}/balances	Balance information endpoint as defined by the Berlin Group in the implementation guide version 1.3.

### 5.2.2 Path parameters

Attribute	Type	Mandatory	Description
account-id	String	Y	The UUID identifying the account as returned by the service <i>Read Account List</i> .

### 5.2.3 Query parameters

The Read Balance endpoint does not have any query parameters.

### 5.2.4 Request header

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

### 5.2.5 Request body

The Read Balance endpoint does not have a request body.

### 5.2.6 Example Read Balance request

The Read Balance request is illustrated below:

```

GET https://psd.bancairediensten.nl/psd2/snsbank/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/balances
Content-Type:      application/json

```



X-Request-ID:	fdb9757d-8f27-4f9e-9be0-0eadacc89012
ConsentId:	ABC5678901234567
Authorization:	bearer ACCESS-TOKEN

### 5.2.7 Response code

The response will look like this:

Code	Description
200	Ok

### 5.2.8 Response header

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

### 5.2.9 Response body

Attribute	Type	Mandatory	Description
account	Account Reference object	N	iban: Attribute is part of the <i>Account Reference</i> object as defined by the Berlin Group. This attribute is optional and, therefore, de Volksbank does <u>not</u> return it.
iban	String		
balances	Balance object	Y	balanceType: De Volksbank only supports the balance type <i>interimAvailable</i>  currency: Attribute is part of the array <i>Amount</i> as defined by the Berlin Group. ISO 4217 Alpha 3 currency code  amount: Attribute is part of the array <i>Amount</i> 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: Required format is <i>ISODateTime</i>
balanceType	String	Y	
balanceAmount	Amount object	Y	
currency	String	Y	
amount	String	Y	
lastChangeDateTime	String	N	

### 5.2.10 Example Read Balance response

The Read Balance response 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"
      } ]
}
```

## 5.3 Read Transaction List

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. mandatId;
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.

### 5.3.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank asnbank regiobank/v1/accounts/{account-id}/transactions {query-parameters}	Transaction information endpoint as defined by the Berlin Group in the implementation guide version 1.3.

### 5.3.2 Path parameters

Attribute	Type	Mandatory	Description
account-id	String	Y	The UUID identifying the account as returned by the service <i>Read Account List</i> .

### 5.3.3 Query parameters

Attribute	Type	Mandatory	Description
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 <i>entryReferenceFrom</i> is a concatenation of journaldate and a sequence number. The format is YYYYMMDD-XXXXXXXXXXXX. The journal date has the format is YYYYMMDD. The sequence number has the format XXXXXXXXXXXX. It is a numerical string with a maximum of 12 digits <u>without</u> leading zeros.
bookingStatus	String	Y	The Berlin Group Implementation guide version 1.3 states the following:  <i>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.</i>  De Volksbank accepts the values <b>"booked"</b> and <b>"both"</b> , but de Volksbank will only return transactions with the status <b>"booked"</b> .
limit	Number	N	Maximum number of transactions in the response. De Volksbank has set the <b>maximum</b> limit to <b>2000</b> transactions. De Volksbank has set the <b>default</b> limit to <b>1000</b> transactions.

Attribute	Type	Mandatory	Description
pageDirection	String	N	The attribute <i>pageDirection</i> refers to the direction of the search. Starting point is the value in the attribute <i>entryReferenceFrom</i> . The allowable values are “ <b>previous</b> ” and “ <b>next</b> ”. This attribute is used to build up the 'previous' and 'next' links in the attribute <i>_links</i> of the response.

### 5.3.4 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 AISP).
ConsentId	String	Y	Attribute filled with the value of the ConsentId obtained in the consent request call.
Authorization	String	Y	Attribute filled with the access-token as obtained in the token request call.

### 5.3.5 Request body

The Read Transaction List endpoint does not have a request body.

### 5.3.6 Example Read Transaction List request

The Read Transaction List request is illustrated below:

```
GET
https://psd.bancairediensten.nl/psd2/snsbank/v1/accounts/mdw3456reqeng7890/transactions?dateFrom=2018-11-24&dateTo=2018-11-24&entryReferenceFrom=201823999&bookingStatus="booked"&limit=1000&pageDirection="next"
Content-Type: application/json
X-Request-ID: fdb9757d-8f27-4f9e-9be0-0eadacc89012
ConsentId: ABC5678901234567
Authorization: bearer ACCESS-TOKEN
```

### 5.3.7 Response code

The response will look like this:

Code	Description
200	Ok

### 5.3.8 Response header

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

Attribute	Type	Mandatory	Description
X-Request-ID	String	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the AISP).

### 5.3.9 Response body

Attribute	Type	Mandatory	Description
account	Account Reference object	N	iban:
iban	String	N	ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}
currency	String	N	currency:
			ISO 4217 Alpha 3 currency code

transactions	Account Report object	N	JSON based account report.
booked	Transactions object		
entryReference	String		entryReference: The attribute <i>entryReference</i> is a concatenation of journaldate and a sequence number.
endToEndId	String	N	The format is YYYYMMDD-XXXXXXX.
mandateId	String	N	The journal date has the format YYYYMMDD. The sequence number has the format XXXXXXXX. It is a numerical string with a maximum of 8 digits <u>without</u> leading zeros.
creditorId	String	N	
bookingDate	String	N	
valueDate	String	N	
transactionAmount:	Amount object	N	
currency	String	Y	
amount	String	Y	
creditorName	String	N	
creditorAccount	Account Reference object		endToEndId: Unique identification as provided by the TPP.
iban	String	N	The ISO 20022 length of the attribute is Max35Text.
currency	String	N	
debtorName	String	N	
debtorAccount	Account Reference object		mandateId: The attribute <i>mandateId</i> contains the unique identification, as assigned by the creditor,
iban	String	N	to unambiguously identify the mandate belonging to a direct debit agreement.
currency	String	N	The ISO 20022 length of the <i>mandateId</i> value is Max35Text.
remittanceInformationUnstructured	String	N	
purposeCode	String	N	
bankTransactionCode	String	N	
ProprietaryBankTransactionCode	String	N	
			creditorId: EPC rulebook attribute AT-02 for SEPA Direct Debits: Identifier of the Creditor. Max35Text
			bookingDate: The date when an entry is posted to an account on the ASPSPs books. Format is YYYYMMDD
			valueDate: The date at which assets become available to the account owner in case of a credit. Format is YYYYMMDD
			currency: Attribute <i>currency</i> is part of the array <i>Amount</i> as defined by the Berlin Group. ISO 4217 Alpha 3 currency code

		<p><b>amount:</b>  Attribute <i>amount</i> is part of the array <i>Amount</i> 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.</p> <p><b>creditorName:</b>  Party to which an amount of money is due.  Max70Text</p> <p><b>iban:</b>  ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}</p> <p><b>currency:</b>  ISO 4217 Alpha 3 currency code</p> <p><b>debtorName:</b>  Party that owes an amount of money to the (ultimate) creditor.  Max70Text</p> <p><b>remittanceInformationUnstructured:</b>  Max140Text</p> <p><b>purposeCode:</b>  Filled with a value belonging to the ISO 20022 ExternalPurpose1Code set.</p> <p><b>bankTransactionCode:</b>  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.</p> <p><b>proprietaryBankTransactionCode:</b>  The proprietary transaction code used by de Volksbank.  Max35Text</p>
--	--	--

Attribute	Type	Mandatory	Description
_links	Links object	N	A list of hyperlinks to be recognised by the TPP.
account	Href type		
href	String	N	
next	Href type	Y	href:
href	String	N	No specific length defined by the Berlin Group.
previous	Href type	Y	
href	String	N	
		Y	

### 5.3.10 Example Read Transaction List response

The Read Transaction List response 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":{

```





## 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"
<b>Credit Transfers outgoing (minus/debit) &lt;SEPA SCT &amp; SCTInstant&gt;</b>			
Internet	Own accounts	3724	NGI
	SCT within a bank brand	3723	NGI
	SCTinst within the bank / brands	9930	IOI
	SCT within the Netherlands	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 Netherlands, 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 Netherlands	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 Netherlands	9759	TPP
	SCTinst within the Netherlands	9934	ITP
	SCT SEPA (excl. NL)	9747	OVS
Paper based payment (Optical readable form)	Within the bank / the Netherlands	9846	OVS
	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
<b>Acceptgiro Outgoing (minus/debit) &lt;SEPA SCT, Local instrument = ACCEPT&gt;</b>			
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
<b>iDEAL outgoing (minus/debit) &lt;SEPA SCT, Local instrument = IDEAL&gt;</b>			
Internet	SCT within the Netherlands / SEPA	9806	IDE
	SCT within the Netherlands / SEPA	9856	IDM
<b>Dutch Urgent payments / TNS outgoing (minus/debit)</b>			
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
<b>Foreign payments (NON SEPA) outgoing (minus/debit)</b>			
Internet	World	7727	OVS
Local office	World	7761	OVS
<b>SEPA Direct Debets (minus/debit)</b>			
CORE SDD	the Netherlands and SEPA	9714	EIC
B2B SDD	the Netherlands and SEPA	9827	EIC
Overheidsvordering (Governmental 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
<b>Automated credit transfers outgoing (minus/debit)</b>			
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
<b>Cash withdrawel (minus/debit)</b>			
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
<b>POS Card payments (minus/debit)</b>			
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
<b>Mobile payments / NFC (minus/debit)</b>			

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
<b>Interest, commissions &amp; charges (minus/debit)</b>			
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"
<b>Credit Transfers Incoming (plus/credit) &lt;SEPA SCT &amp; SCTInstant&gt;</b>			
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
<b>Acceptgiro incoming (plus/credit) &lt;SEPA SCT, local instrument = ACCEPT&gt;</b>			
the Nederlands	All channels (SCT)	8845	ACC
<b>iDEAL incoming (plus/credit) &lt;SEPA SCT, Local instrument = IDEAL&gt;</b>			
Netherlands/SEPA	Internet/Mobile	8806	IDE
Netherlands/SEPA batch booking	Internet/Mobile	2806	IDE
<b>Dutch Urgent Payments / TNS incoming (plus/credit)</b>			
Between brands of de Volksbank	All channels	8783	OVS
the Netherlands	All channels	8872	OVS
<b>Foreign payments (NON SEPA) incoming (plus/credit)</b>			
World	All channels	6761	OVS
<b>SEPA Direct Debets (plus/credit)</b>			
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
<b>Automated credit transfers incoming (plus/credit)</b>			
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

<b>Product / Channel</b>	<b>Domain</b>	<b>bank Transaction Code</b>	<b>proprietary Bank Transaction Code "FXXX"</b>
Standing order between brands of de Volksbank	Internet/Mobile app/ Local office	8744	POV
<b>Cash deposit (plus/credit)</b>			
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
<b>POS Card payment (plus/credit)</b>			
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
<b>POS Card Refund (plus/credit)</b>			
POS (Maestro)		8909	RTI
POS (Vpay)		8920	RTI
<b>Mobile payments / NFC (plus/credit)</b>			
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
<b>Interest, commissions &amp; charges (plus/credit)</b>			
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