AIS API

PSD2 interface AIS de Volksbank

Date: April 23 2024
Version: 1.21

Colophon

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

Version

Version	Date	Changes
1.0	2019-01-18	Initial version
1.1	2019-04-23	- The document structure has been adapted to the structure of the PIS API document for reasons of consistency. - The chapters about the Authorize and Token endpoints have been updated.
1.2	2019-07-05	- Updated request and response objects and headers (4).
1.3	2019-08-02	- Added error information. - Chapters on Get Consent Status, Get Consent and Delete Consent endpoints have been added.
1.4	2019-09-12	- Added information about Android problem in 2.4. - Updated path parameters for refresh token call. - Updated request headers getAccounts, getBalances and getTransactions calls.
1.5	2019-11-21	- Updated response headers consent request call.
1.6	2020-04-29	- Updated certificates paragraph.
1.7	2020-05-12	- Added missing descriptions in paragraphs 5.2.9 and 5.3.9.
1.8	2020-07-14	- Removed unnecessary redirect uri paragraph. - Changed redirect uri in example response to new redirect uri.
1.9	2020-08-05	- Added field ownerName to Read Account List response.
1.10	2021-02-04	- Added TPP-Notification-URI and TPP-Content-Preferred headers to consent request call.
1.11	2021-08-02	- Updated incorrect field name bic to customerBic in Read Account List v1. - Added v1.1 descriptions for Read Account List, Read Balance and Read Transaction List.
1.12	2021-08-25	- Improved description for the use of the accountId/resourceId.
1.13	2022-01-10	- Fixed error in example response Read Transaction List v1.1 and expanded explanation about field information for debit and credit transfers.
1.14	2022-06-08	- Updated Consent request with additional information for access, recurringIndicator, and validUntil fields. - Removed Read Account List v1.0, Read Balance v1.0 and Read Transaction List v1.0. - Added general information about filtering in 2.5. - Added filtering example to readTransactionsList.
1.15	2022-11-14	- Updated Consent request with additional information for recurringIndicator field. - Changed consentIds to UUID format. - Updated list of possible HTTP error codes. - Updated Appendix A, list of bank transaction codes.

1.16	2023-01-16	- Added information about renewing a consent.
1.17	2023-01-17	- Added information about redirect error codes. - Updated Appendix A with the following value: KYC charges business accounts. - Add usage to read accounts list response body.
1.18	2023-04-20	- Update datatypes for X-Request-ID, Account-ID and Consent-ID.
1.19	2023-05-22	- Changed SCA expiration period from 90 days to 180 days. This change comes into effect from 25th July 2023.
1.20	2024-03-07	- Removed port 10443 from authorize endpoint.
1.21	2024-04-23	- Added support for the optional attribute commercialNameAssetUser.

References

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

TABLE OF CONTENTS

1 Introduction

This document describes the 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. The refresh token is valid for a duration of **90** days;
4. Each consent granted by a PSU to an AISP is valid for a maximum of **180** days in accordance with the PSD2 RTS requirements on strong customer authentication;
5. 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. Maximum number of transactions in one response has been set to **2000**;
    d. 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

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

Datatype	Length/Format	Description
String	Maxtext34	Maximum length of the alpha-numerical string is 34
	Maxtext35	Maximum length of the alpha-numerical string is 35
	Maxtext70	Maximum length of the alpha-numerical string is 70
	Maxtext140	Maximum length of the alpha-numerical string is 140
	ISO 8601 date format	Dates are of the data type string, but must comply with the ISO 8601 date format. This implies that dates have the following format: **YYYY-MM-DD**.
	ISO 8601 datetime format	Dates are of the data type string, but must comply with the ISO 8601 datetime format.
String	Decimal format	Amount fields are of the data type *string*, but have the format of a *decimal* where the following format requirements hold: 1. The number of fractional digits must comply with the ISO 4217 minor unit of currency (for instance, the number of fractional digits for the currency EUR is 2); 2. The digits denoting integers and the digits denoting fractions are separated by a **dot**.
Number	Integer format	Number is an integer starting at 0, 1, 2, ...

2.5 Filtering response data

Filtering may be used on the APIs to limit the amount of data returned in an API response. To support server side filtering the *fields* query parameter may be used. Fields can be filtered by including and/or excluding fields:

```
?fields=(field_a(field_b,field_c),field_d!(field_e))
```

Considering the following example response to an endpoint:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1/example
{
   "accounts": [
      {
         "name": "value1",
         "iban": "value2"
      },
      {
         "name": "value1",
         "iban": "value2"
      }
   ]
}
```

To include only the iban fields:

```
GET
https://psd.bancairediensten.nl/psd2/snsbank/v1/example?fields=(accounts(iban))
{
   "accounts": [
      {
         "iban": "value2"
      },
      {
         "iban": "value2"
      }
   ]
}
```

To exclude the iban fields:

```
GET
https://psd.bancairediensten.nl/psd2/snsbank/v1/example?fields=(accounts!(iban))
{
   "accounts": [
      {
            "name": "value1"
        },
        {
            "name": "value1"
        }
    ]
}
```

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).

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[1] use the following APIs for gaining access to account information:

1. Consent request (creation of a consent ID);

2 and 3. Authorization request and approval of the PSU;

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

4. Get consent status request;
5. Access token request: access token and refresh token based on authorization code;
6. New access token request: new access and refresh tokens based on refresh token;
7. Get consent request;
8. Delete consent request.

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	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/consents	Consent request endpoint as defined by the Berlin Group in the implementation guide version 1.3.

[1] The APIs 4, 7 and 8 are optional: an AISP can use these APIs to get information about the status of a consent (4 and 7) or to send a request to delete a consent given by the PSU (8).

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 "*application/json*".
X-Request-ID	UUID	Y	ID of the request, unique to the call, as determined by the initiating party (the AISP).
Authorization	String	Y	Attribute consists of *client_id:* identification of the AISP as registered with de Volksbank.
TPP-Notification-URI	String	N	The URI of the TPP-API where notifications about the consent status will be send towards. The URI should match with the common name or one of the domains of the QWAC certificate.
TPP-Notification-Content-Preferred	String	N	Only SCA is supported by de Volksbank. Other options are currently ignored. We support 2 events: - SCA Consent is valid for 180 days. 5 calendar days before expiry date of the consent you will receive a notification. - Consent given with SCA is revoked by the PSU in his online banking environment. When the Consent is revoked by the PSU you will receive a notification.

4.1.5 Request body

Attribute	Type	Mandatory	Description
access	Account Access object	Y	This attribute is part of the object *Account Access* and refers to the requested access services. Sub-attributes *accounts*, *balances* and *transactions* must be empty arrays, because de Volksbank only supports consent requests without explicitly mentioning the accounts. All the sub-attributes are optional, but at least one is required. The consent will only give access for the given attributes. Please note that a "balances" or "transactions" access right implicitly also gives access to the accounts endpoint.
accounts	array of Account Reference	N	
balances		N	
transactions		N	

Attribute	Type	Mandatory	Description
recurringIndicator	Boolean	Y	The value of the attribute *recurringIndicator* is to be set to *true*, if the consent is for a recurring access to the account data. The value of the attribute *recurringIndicator* is to be set to *false*, if the consent is for a one-off access to the account data. Since it is possible that the Read Transaction List call has to be executed several times (due to a result limit), this call can be executed several times even when *recurringIndicator* is set to *false*. For one-off access to transaction information, the TPP will have ten minutes, starting from the moment of the first Read Transaction List call, for requesting the transaction data.
validUntil	Date	Y	The attribute *validUntil* contains the date until when a consent is valid. The attribute has the ISO 8601 Date format (YYYY-MM-DD) and cannot be in the past. N.B.: Each consent granted by a PSU to an AISP is valid for a maximum of 180 days in accordance with the PSD2 RTS requirements on strong customer authentication (see also section 2.1). If the validUntil value is below the 180 days then that value will be used, otherwise the date 180 days after initiation will be used.
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**.

Attribute	Type	Mandatory	Description
commercialNameAssetUser	String	N	When the consent is meant for another party (the asset user) using the services of an AISP, e.g. in a License-as-a-Service (LaaS) context, this field can be used to provide the asset user's commercial name. When provided, the commercial name will be shown to the PSU on the SCA redirect screen and their permissions dashboard. This will provide more transparency as to who will be receiving their data, and help the PSU recognize different permissions given to same (LaaS) AISP. Using this attribute will also ensure that a PSU's existing consents remain valid when a new consent for the same AISP but a different asset user is created.

4.1.6 Example consent request

The consent request 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

4.1.8 Response header

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

4.1.9 Response body

Attribute	Type	Mandatory	Description
consentStatus	Consent Status	Y	In case of a successful consent request (HTTP status code 201), only the status "received", as defined by the BerlinGroup is supported.
consentId	UUID	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. "**scaOAuth**": 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 consent response is illustrated below:

```
HTTP/1.x 201 Created

Content-Type:        application/json

Location:
https://psd.bancairediensten.nl/psd2/snsbank/v1/consents/05873005-99c2-
42ed-810e-99e6a91ce335/status

X-Request-ID:        99391c7e-ad88-49ec-a2ad-99ddcb1f7756

ASPSP-SCA-Approach: REDIRECT

{

   "consentStatus": "received",

   "consentId": "05873005-99c2-42ed-810e-99e6a91ce335",

   "_links": { "scaOAuth": {"href":
"https://psd.bancairediensten.nl/psd2/snsbank/v1/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 "*AIS*".
state	String	Y	Attribute contains the unique identification of the request issued by the AISP.
consentId	UUID	Y	Attribute contains the unique identification of the consent.
redirect_uri	url	Y	Attribute filled with the value where the service redirects the user-agent to after granting the authorization code. No wildcards can be used in the callback URL. De Volksbank validates the exact callback URL.
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	Attribute invariably filled with the value "*application/x-www-form-urlencoded*".

4.2.5 Request body

The authorize endpoint does not have a request body.

4.2.6 Example authorize request

The authorize request is illustrated below:

```
GET
https://psd.bancairediensten.nl/psd2/snsbank/v1/authorize?response_type=code&scope=AIS&state=111111&consentId=05873005-99c2-42ed-810e-99e6a91ce335&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: 1. The URL leading to the login page of the ASPSP; 2. Session data stored in a JWT object (JWT stands for *Json WebToken*).
Content-Type	String	Y	Attribute invariably filled with the value "*text/plain*".

4.2.9 Response body

The authorize endpoint does not have a response body.

4.2.10 Example authorize response

The authorize response is illustrated below:

```
HTTP/1.x 302

Location:
https://diensten.snsbank.nl/online/toegangderden/#/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 **state** in the **Authorize** 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 Get consent status request

With the get consent status endpoint, an AISP can request information about the status of a consent.

4.4.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/consents/{consent-id}/status	Get consent status endpoint as defined by the Berlin Group in the implementation guide version 1.3.

4.4.2 Path parameters

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

4.4.3 Query parameters

The get consent status endpoint does not have any query parameters.

4.4.4 Request header

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

4.4.5 Request body

The get consent status endpoint does not have a request body.

4.4.6 Example get consent status request

The get consent status request is illustrated below:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1/consents/05873005-
99c2-42ed-810e-99e6a91ce335/status

Content-Type:        application/json

X-Request-ID:        fdb9757d-8f27-4f9e-9be0-0eadacc89012

Authorization:       132b095e702f5952e881373c746532dafe
```

4.4.7 Response code

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*".
X-Request-ID	UUID	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the AISP).

4.4.9 Response body

Attribute	Type	Mandatory	Description
consentStatus	String	Y	Attribute filled with the status of the consent. Values are conform the Berlin Group Consent Status list. Enumeration: 1. received; 2. rejected; 3. partiallyAuthorized; 4. valid; 5. revokedByPsu; 6. expired; 7. terminatedByTpp. De Volksbank does not support the status partiallyAuthorized.

Note: when the status of the response is:

- *received*, the consent has been received and is technically correct. The consent is not authorized yet. The AISP can issue an authorization request as long as the consent is not expired (refer to 4.2) or start with creating a new consent ID (refer to 4.1.);
- *rejected,* the PSU has cancelled the consent during the approval process (refer to 4.3) e.g. no successful authorization has taken place;
- *valid,* the consent is approved by the PSU and the AISP should have received an authorization code from the PSU (refer to 4.3) and must exchange this code for an access token and refresh token (refer to 4.5). After these operations the consent is valid for GET account information service calls (refer to chapter 5);
- *revokedByPsu,* the consent has been revoked by the PSU towards the ASPSP (consent revoked by the PSU in his online banking environment);
- *expired,* the consent is automatically expired. If applicable, a new consent ID should be created (refer to 4.1);
- *terminatedByTpp,* the AISP has terminated the consent by applying the DELETE method to the consent resource (see also paragraph 4.8).

4.4.10 Example get consent status response

The get consent status response is illustrated below:

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

4.5 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.

4.5.1 Method and URL

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

4.5.2 Path parameters

The token endpoint does not have any path parameters.

4.5.3 Query parameters

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

4.5.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute invariably filled with the value "*application/x-www-form-urlencoded*".
X-Request-ID	UUID	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 *client_id* and *client_secret* separated by a colon (**:**) in a **base64** encoded string. – Format: Basic base64 (<client_id>:<client_secret>); – client_id: Identification of the 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=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>)
```

4.5.7 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

4.5.8 Response header

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

4.5.9 Response body

Attribute	Type	Mandatory	Description
access_token	String	Y	Attribute filled with the access token needed to call the PSD2 interface, in this case 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".*

4.5.10 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"
    }
```

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.

4.6 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. The validity of the access and refresh tokens is independent of the SCA duration of the consent.

4.6.1 Method and URL

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

4.6.2 Path parameters

The token endpoint does not have any path parameters.

4.6.3 Query parameters

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

4.6.4 Request header

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

4.6.5 Request body

The token endpoint does not have a request body.

4.6.6 Example token request

The token request is illustrated below:

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

4.6.7 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

4.6.8 Response header

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

4.6.9 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	Attribute filled with the new refresh token. 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 “*AIS*”.

4.6.10 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.

4.7 Get consent

With the get consent endpoint, an AISP can request additional information about a consent given by the PSU. This information consists of the current status of the consent and characteristic fields pertaining to the consent.

4.7.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/consents/{consent-id}	Get consent endpoint as defined by the Berlin Group in the implementation guide version 1.3.

4.7.2 Path parameters

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

4.7.3 Query parameters

The get consent endpoint does not have any query parameters.

4.7.4 Request header

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

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

4.7.5 Request body

The get consent endpoint does not have a request body.

4.7.6 Example Get Consent request

The get consent request is illustrated below:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1/consents/05873005-
99c2-42ed-810e-99e6a91ce335
Content-Type:       application/json
X-Request-ID:       fdb9757d-8f27-4f9e-9be0-0eadacc89012
Authorization:      Bearer <ACCESS-TOKEN>
```

4.7.7 Response code

Code	Description
200	OK

4.7.8 Response header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute is invariably filled with the value "*application/json*".
X-Request-ID	UUID	Y	ID of the request obtained from the request header.

4.7.9 Response body

Attribute	Type	Mandatory	Description
access accounts balances transactions	Account Access object array of Account Reference	Y	This attribute is part of the object Account Access and refers to the requested access services. accounts, balances and transactions are arrays filled with Account Reference, which contains an IBAN (String, format: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}).
recurringIndicator	Boolean	Y	If the value of the attribute *recurringIndicator* is set to *true*, the consent is for a recurring access to the account data. If the value of the attribute *recurringIndicator* is set to *false*, the consent is for a one-off access to the account data.
validUntil	Date	Y	The attribute *validUntil* contains the date until when the consent is valid.

			The attribute has the ISO 8601 Date format (YYYY-MM-DD). N.B.: Each consent granted by a PSU to an AISP is valid for a maximum of 180 days in accordance with the PSD2 RTS requirements on strong customer authentication (see also section 2.1). If the initial validUntil value that the TPP submitted is below the 180 days then that value will be returned, otherwise the date 180 days after initiation will be returned.
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".
lastActionDate	String	Y	This field contains the date of the last action on the consent object having an impact on the status. The attribute has the ISO 8601 Date format (YYYY-MM-DD).
consentStatus	String	Y	Attribute filled with the status of the consent. Values are conform the Berlin Group Consent Status list. Enumeration: 1. received; 2. rejected; 3. partiallyAuthorized; 4. valid; 5. revokedByPsu; 6. expired; 7. terminatedByTpp. De Volksbank does not support the status partiallyAuthorized.
commercialNameAssetUser	String	N	When this attribute has been used in the Consent request, it will be returned here. This attribute is the name of the asset user which uses the services of the AISP.

4.7.10 Example get consent response

The get consent response is illustrated below:

```
HTTP/1.x 200
Content-Type: application/json
   { "access":
         {"accounts":
            [{"iban": "NL64SNSB0948305280"}],
         },
         {"balances":
            [{"iban": "NL64SNSB0948305280"}],
         },
         {"transactions":
            [{"iban": "NL64SNSB0948305280"}],
         },
      "recurringIndicator": true,
      "validUntil": "2019-07-05",
      "frequencyPerDay": "4",
      "lastActionDate": "2019-06-18",
      "consentStatus": "valid"
   }
```

4.8 Delete consent request

With the delete consent endpoint, an AISP can delete a consent given by the PSU.

4.8.1 Method and URL

Method	URL	Description
DELETE	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/consents/{consent-id}	Delete consent endpoint as defined by the Berlin Group in the implementation guide version 1.3.

4.8.2 Path parameters

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

4.8.3 Query parameters

The delete consent endpoint does not have any query parameters.

4.8.4 Request header

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

4.8.5 Request body

The delete consent endpoint does not have a request body.

4.8.6 Example delete consent request

The delete consent request is illustrated below:

```
DELETE https://psd.bancairediensten.nl/psd2/snsbank/v1/consents/05873005-
99c2-42ed-810e-99e6a91ce335
Content-Type:       application/json
X-Request-ID:       fdb9757d-8f27-4f9e-9be0-0eadacc89012
Authorization:      Bearer <ACCESS-TOKEN>
```

4.8.7 Response code

Code	Description
204	No Content

4.8.8 Response header

Attribute	Type	Mandatory	Description
X-Request-ID	UUID	Y	ID of the request obtained from the request header.

4.8.9 Response body

The delete consent endpoint does not have a response body.

4.8.10 Example delete consent response

The delete consent response is illustrated below:

```
HTTP/1.x 204 No Content
X-Request-ID:   fdb9757d-8f27-4f9e-9be0-0eadacc89012
```

4.9 Renew consent

When the SCA expires but the consent's validUntil date has not expired, the consent can be renewed. To renew the consent the following conditions must be true:

- Consent status is valid, expired or revokedByPsu
- ValidUntil date has not yet expired
- Consent request has been approved by a customer at least once
- The consent is recurring (recurringIndicator = true)

If the above holds true, the consent can be renewed by using the Authorize Request (see 4.2). This will return a new URL to be used by the PSU to authorize the consent. The PSU will be unable to change the selected account for the consent.

After the consent has been authorized by the PSU the consent's scaExpirationDate will be set to 180 days from the moment of approval, or to the validUntil date if it is less than 180 days from the moment of authorization. It can then be used again with the same consentId and accountId until the new scaExpirationDate.

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

4.10 Read Account List v1.1

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 attributes as described in 5.1.9.

Please note: when a consent has been renewed the resourceId (accountId) will also be changed. Therefore it is needed to use the read account to get the new resourceId.

4.10.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1.1/accounts {query parameters}	Account information endpoint as defined by the Berlin Group in the implementation guide version 1.3.

4.10.2 Path parameters

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

4.10.3 Query parameters

Attribute	Type	Mandatory	Description
withBalance	Boolean	N	The Berlin Group Implementation guide version 1.3 states the following about the attribute *withBalance*: *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.

4.10.4 Request header

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

4.10.5 Request body

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

4.10.6 Example Read Account List request

The Read Account List request is illustrated below:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1.1/accounts
Content-Type:        application/json
X-Request-ID:        fdb9757d-8f27-4f9e-9be0-0eadacc89012
Consent-ID:          05873005-99c2-42ed-810e-99e6a91ce335
Authorization:       Bearer <ACCESS-TOKEN>
```

4.10.7 Response code

Code	Description
200	Ok

4.10.8 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	UUID	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the AISP).

4.10.9 Response body

Attribute		Type	Mandatory	Description
accounts		Account Details array	Y	
	resourceId	UUID	Y	A universally unique identifier (UUID), a 128-bit number used to identify the account. This identifier is determined by the ASPSP. This identifier is also known as account-id.
	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
	ownerName	String	N	Name of the account holder(s). If an account has a joint account holder, the name of the account holder and joint account holder are separated with ' CJ '.
	product	String	N	Product name of the Bank for this account, proprietary definition.
	customerBic	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}
	usage	String	N	Specifies the usage of the account: - PRIV: Private personal account - ORGA: professional account - NPRV: Not provided

4.10.10 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",
        "ownerName": "Z H van der Zee CJ Z Bottema",
        "product": "Plus Betalen",
        "customerBic": "RBRBNL21"
      }
    ]
}
```

4.11 Read Balance v1.1

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.

4.11.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1.1/accounts/{account-id}/balances	Balance information endpoint as defined by the Berlin Group in the implementation guide version 1.3.

4.11.2 Path parameters

Attribute	Type	Mandatory	Description
account-id	UUID	Y	The UUID identifying the account as returned by the service *Read Account List*.

4.11.3 Query parameters

The Read Balance endpoint does not have any query parameters.

4.11.4 Request header

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

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

4.11.5 Request body

The Read Balance endpoint does not have a request body.

4.11.6 Example Read Balance request

The Read Balance request is illustrated below:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1.1/accounts/3dc3d5b3-
7023-4848-9853-f5400a64e80f/balances

Content-Type:        application/json

X-Request-ID:        fdb9757d-8f27-4f9e-9be0-0eadacc89012

Consent-ID:        05873005-99c2-42ed-810e-99e6a91ce335

Authorization:     Bearer <ACCESS-TOKEN>
```

4.11.7 Response code

Code	Description
200	Ok

4.11.8 Response header

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

4.11.9 Response body

Attribute	Type	Mandatory	Description
account iban	Account Reference object String	N	iban: Attribute is part of the *Account Reference* object as defined by the Berlin Group. This attribute is optional and de Volksbank does not return it.
Balances balanceType	Balance object String	Y Y	 balanceType: De Volksbank only supports the balance type *interimAvailable*

Attribute	Type	Mandatory	Description
balanceAmount	Amount object	Y	
currency	String	Y	currency: Attribute is part of the array *Amount* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code
amount	String	Y	amount: 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	lastChangeDateTime: Required format is ISODateTime Last time the balanceAmount has changed

4.11.10 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"
    } ]
}
```

4.12 Read Transaction List v1.1

The Account Information Service **Read Transaction List** provides transaction detail information about a PSU’s account uniquely identified by an IBAN. The transaction information as described in 5.3.9 is shown.

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

4.12.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank/v1.1/accounts/{account-id}/transactions {query-parameters}	Transaction information endpoint as defined by the Berlin Group in the implementation guide version 1.3.

4.12.2 Path parameters

Attribute	Type	Mandatory	Description
account-id	UUID	Y	The UUID identifying the account as returned by the service *Read Account List*.

4.12.3 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). Cannot be used in combination with an entryReferenceFrom.
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). Cannot be used in combination with an entryReferenceFrom.
entryReferenceFrom	String	N	The attribute *entryReferenceFrom* is a concatenation of a journal date and a sequence number. The format is YYYYMMDD-XXXXXXXXXXXX. The journal date has the format YYYYMMDD. The sequence number is a numerical string with a maximum of 12 digits without leading zeros. Cannot be used in combination with a dateFrom and/or dateTo.

Attribute	Type	Mandatory	Description
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**". Please note that de Volksbank in her direct online banking 'account statement' to PSUs doesn't show a "pending" status of a booking, only "booked" is shown.
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. When your search yields more results than the limit, the results will be presented in the form of a 'page' (result set) with the most recent results (where the amount of results is equal to the limit) and a link to the next page, where the remainder of the results will be present (unless these are again more results than the limit, in which case another full page will be presented with another next link, and so on).

The results will be presented in descending order; the most recent transaction in the result set will be the first in the list.

4.12.4 Request header

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

4.12.5 Request body

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

4.12.6 Example Read Transaction List request

The Read Transaction List request is illustrated below:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1.1/accounts/04d1402b-
979d-4e6d-b38b-aacff0b3a993/transactions
?entryReferenceFrom=201823999&bookingStatus=booked&limit=1000

Content-Type:  application/json

X-Request-ID:  fdb9757d-8f27-4f9e-9be0-0eadacc89012

Consent-ID:  05873005-99c2-42ed-810e-99e6a91ce335

Authorization: Bearer <ACCESS-TOKEN>
```

4.12.7 Response code

Code	Description
200	Ok

4.12.8 Response header

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

4.12.9 Response body

Attribute	Type	Mandatory	Description
account	Account Reference object	N	iban: ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}
iban	String	N	currency:
currency	String	N	ISO 4217 Alpha 3 currency code
transactions	Account Report object	N	JSON based account report.
booked	Array of Transaction objects	N	
entryReference	String	N	entryReference: 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 is a numerical string with a maximum of 8 digits without leading zeros.
endToEndId	String	N	endToEndId: Unique identification as provided by a third party or entered by the PSU.

Attribute	Type	Mandatory	Description
			The ISO 20022 length of the attribute is Max35Text.
mandateId	String	N	mandateId: 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	creditorId: EPC rulebook attribute AT-02 for SEPA Direct Debits: Identifier of the Creditor. Max35Text
bookingDate	String	N	bookingDate: The date when an entry is posted to an account on the ASPSPs books. Format is YYYYMMDD
valueDate	String	N	valueDate: The date when interest on the account is calculated. Besides cost/interest postings and certain incoming (credit) international payments, the valueDate equals the bookingDate. Format is YYYYMMDD
transactionAmount:	Amount object	Y	
currency	String	Y	currency: Attribute *currency* is part of the array *Amount* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code
amount	String	N	amount: 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	creditorName: Counterparty to which an amount of money is due. Max70Text
creditorAccount	String	N	iban: ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}

Attribute	Type	Mandatory	Description
iban or bban	Account Reference object String	N	bban: Local account number in case of international payments where country does not support IBAN.
ultimateCreditor	String	N	ultimateCreditor: Name of the ultimate creditor.
debtorName	String	N	debtorName: Counterparty that owes an amount of money to the (ultimate) creditor. Max70Text
debtorAccount	Account Reference object	N	iban: ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}
iban or bban	String	N	bban: Local account number in case of international payments where country does not support IBAN.
ultimateDebtor	String	N	ultimateDebtor: Name of the ultimate debtor.
remittanceInformationUnstructured	String	N	remittanceInformationUnstructured: Max140Text. Please note: In case of international payments (non-SEPA) and card based transactions, this attribute is filled with extended booking information.
remittanceInformationStructured	String	N	reference: Creditor reference.
reference	String	N	referenceIssuer:
referenceIssuer	String	N	Reference to the issuer of the structured remittance information, e.g. ‘iso’ of ‘cur’.
purposeCode	String	N	purposeCode: Filled with a value belonging to purpose code (ISO 20022 ExternalPurpose1Code set) or category purpose code (ISO 20022 ExternalCategoryPurpose1Code). When both values are available, purpose code will be used as output.
bankTransactionCode	String	N	bankTransactionCode: Note: De Volksbank will fill in a numerical code, as de Volksbank does not use the ISO 20022 codes. See also Appendix A of this document.

Attribute	Type	Mandatory	Description
proprietaryBankTransactionCode	String	N	proprietaryBankTransactionCode: The proprietary transaction code used by de Volksbank. See also Appendix A of this document. Max35Text
batchIndicator	boolean	N	batchIndicator: If this indicator equals true, then the related entry is a batch entry.
batchNumberOfTransactions	integer	N	batchNumberOfTransactions: Shows the number of transactions in a batch entry. Only used when the value of batchIndicator equals true.
paymentInformationIdentification	String	N	paymentInformationIdentification: Reference assigned by a sending party in order to unambiguously identify the batch payment.
instructionIdentification	String	N	instructionIdentification: A unique reference assigned by the initiator to unambiguously identify the transaction.
transactionIdentification	String	N	transactionIdentification: TransactionIdentification is the identification of the initiating party. If de Volksbank initiates a transaction on behalf of her customer then this identification is a Volksbank indentification. If de Volksbank receives a transaction from an initiating party then the identification of this initiating party is used.
returnInformationCode	String	N	returnInformationCode: A 4-digit code indicating why a SEPA payment is returned (ISO 20022 ExternalReturn Reason1Code) or SCT instant reversed due to negative conformation (AB05, AB06, AB09).

Attribute	Type	Mandatory	Description
_links	Links object	N	A list of hyperlinks to be recognised by the TPP.
account	Href type	N	href:
href	String	Y	No specific length defined by the Berlin Group.
next	Href type	N	When your search yields more results than the limit, the results will be presented in the form of a 'page' (result set) with the most recent results (where the amount of results is equal to the limit) and this link to the next page, where the remainder of the results will be present (unless these are again more than the limit, in which case another full page will be presented with another next link, and so on). The next link contains no search filters, only the original account-id, the bookingStatus BOOKED (de Volksbank only acknowledges this status, also in her direct online banking channels) and a next page key, which is build based on your original search filters plus a cursor pointing to the next transactions of the result set.
href	String	Y	

A note on the fields transactionAmount, creditorAccount, creditorName, debtorAccount, debtorName, and returnInformationCode: depending on the type of transaction, amount will be positive or negative, and the counterparty will be either the creditor or the debtor.

- A normal debit payment will show up as a negative amount, and the fields creditorName and creditorAccount (= counterparty) will be returned.
- A normal credit payment is shown as a positive amount, and returns debtorName and debtorAccount (= counterparty).
- When a debit payment transaction is returned/reversed (containing a returnInformationCode) this results in a positive return amount on the customer account, and the fields creditorName and creditorAccount are presented in the response (= the original counterparty).
- A returned/reversed credit transaction results in a negative return amount and the debtor fields (= the original counterparty) are returned.
- Counterparty data is not presented for interest/costs/charges transactions, nor for cards-based transactions.

4.12.10 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":"0193507",
      "creditorId":"KLM08642LAX",
      "bookingDate":"2017-10-25",
      "valueDate":"2017-10-25",
      "transactionAmount":{"currency":"EUR","amount":"-256.67"},
      "creditorName":"I.N.G. von Ginieus",
      "creditorAccount":{"iban":"NL64ASNB0123456789"},
      "remittanceInformationUnstructured":"Uw toelage",
      "purposeCode":"SALA",
      "bankTransactionCode":"3723",
      "proprietaryBankTransactionCode":"FNGI"}
    ],
    "_links":{
       "account":{
"href":"https://psd.bancairediensten.nl/psd2/snsbank/v1.1/accounts/3fdb89
46-52ee-4a6d-8a0c-c7ba6f4a45ed"
         },
       "next":{
          "href":"
https://psd.bancairediensten.nl/psd2/snsbank/v1.1/accounts/3fdb8946-52ee-
4a6d-8a0c-
c7ba6f4a45ed/transactions?bookingStatus=BOOKED&nextPageKey=abcdef123"
       }
    }
  }
}
```

4.12.11 Example Read Transaction List response with filtering

The Read Transaction List response below is applying a filter to only return the transactions without creditorName, creditorAccount and remittanceInformationUnstructured.

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1.1/accounts/04d1402b-
979d-4e6d-b38b-
aacff0b3a993/transactions?fields=(transactions(booked!(creditorName,credi
torAccount,remittanceInformationUnstructured)))
HTTP/1.x 200 Ok
Content-Type:  application/json
X-Request-ID: fdb9757d-8f27-4f9e-9be0-0eadacc89012
{
  "transactions":{
   "booked":[
      {
      "entryReference":"20190101-33263746",
      "endToEndId":"12345678901234567890123456789012345",
      "mandateId":"0193507",
      "creditorId":"KLM08642LAX",
      "bookingDate":"2017-10-25",
      "valueDate":"2017-10-25",
      "transactionAmount":{"currency":"EUR","amount":"-256.67"},
      "purposeCode":"SALA",
      "bankTransactionCode":"3723",
      "proprietaryBankTransactionCode":"FNGI"}
    ]
  }
}
```

4.13 Error handling

4.13.1 HTTP error codes

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

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

4.13.2 Additional error information

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

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

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

HTTP status	Category	Code	Text
400	ERROR	FORMAT_ERROR	The format of the input is not valid. Note: This set of errors can have a variety of text messages, each one indicating which specific input error was found, e.g. “validUntil doesn't match date format yyyy-MM-dd”.
400	ERROR	CONSENT_FAILED	Consent call failed.
401	ERROR	CONSENT_INVALID	The mandate could not be found.
401	ERROR	CONSENT_INVALID	The mandate is revoked.
401	ERROR	CONSENT_INVALID	The mandate has an invalid status.
401	ERROR	CONSENT_INVALID	The consent gives no access to this information.
401	ERROR	CONSENT_EXPIRED	The expiration date of the mandate has been expired.
401	ERROR	CONSENT_EXPIRED	The consent should be executed once within 10 minutes.
401	ERROR	SERVICE_BLOCKED	Access to this account has been revoked.
403	ERROR	SERVICE_BLOCKED	This account's master switch is switched off.
403	ERROR	CONSENT_INVALID	Recurring operations are not allowed for this consent.
403	ERROR	CONSENT_INVALID	The mandate has been deleted by the TPP.
403	ERROR	CONSENT_INVALID	No available accounts.
403	ERROR	RESOURCE_UNKNOWN	The consentId and account combination is invalid.
403	ERROR	RESOURCE_UNKNOWN	The consentId and resourceId combination is invalid.
500	ERROR	INTERNAL_SERVER_ERROR	An internal server error occurred.

4.13.3 Redirect error codes

The possible redirect errors that are returned to the third party’s with the possible error description and error code.

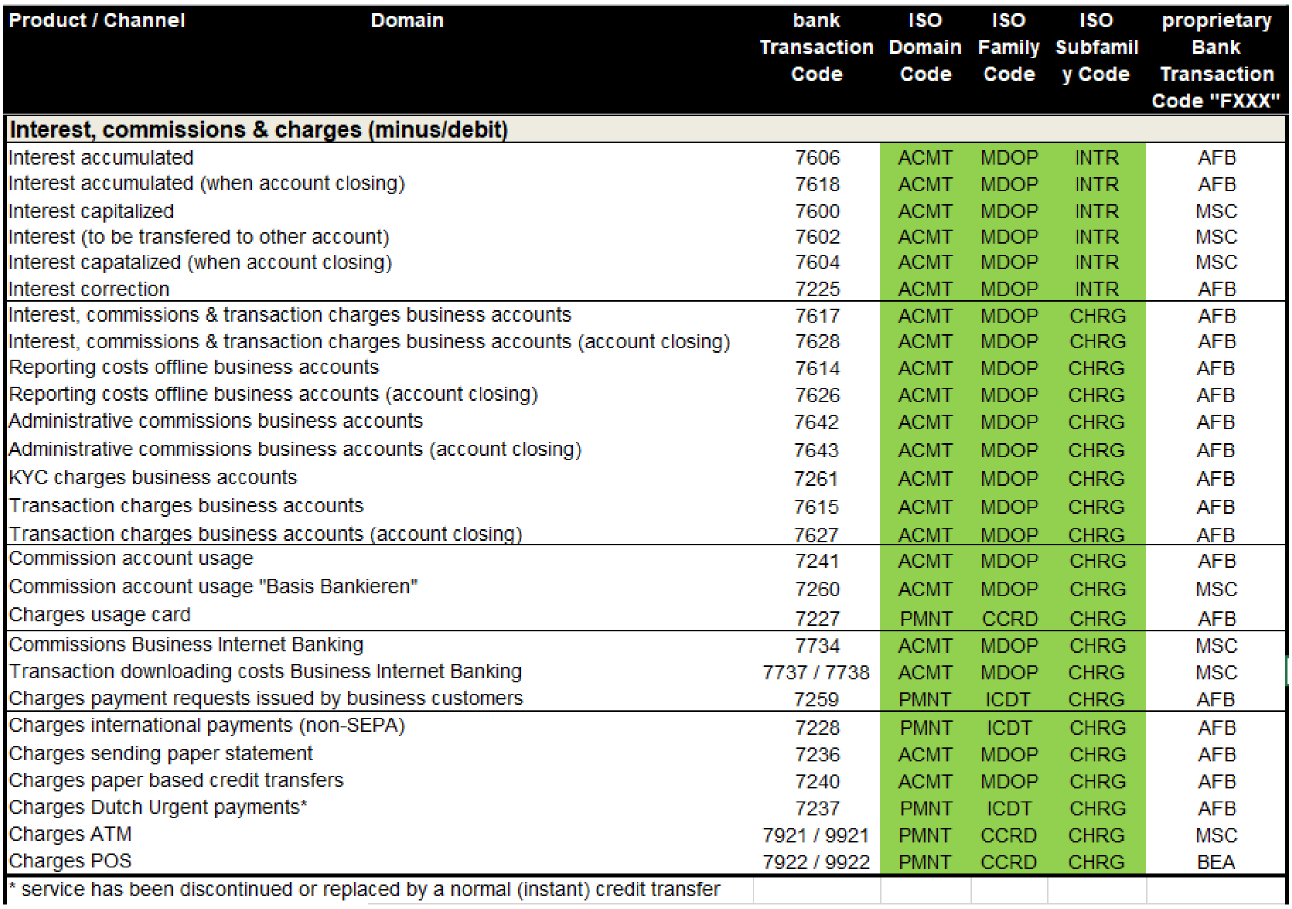
Category	Error code	Error description
ERROR	DS24	Waiting time expired due to incomplete order
ERROR	DS02	An authorized user has cancelled the order
ERROR	AM04	Insufficient funds or account blocked
ERROR	TKVE	Token found with value limit rule violation
ERROR	MS03	Miscellaneous reason
ERROR	AG03	Services not supported/authorized on any account
ERROR	AC01	Account number is invalid or missing
ERROR	AG01	Transaction forbidden on this type of account
ERROR	DU01	Message Identification is not unique for this user
ERROR	AM14	Transaction amount exceeds limits agreed between bank and client

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

Debit entries

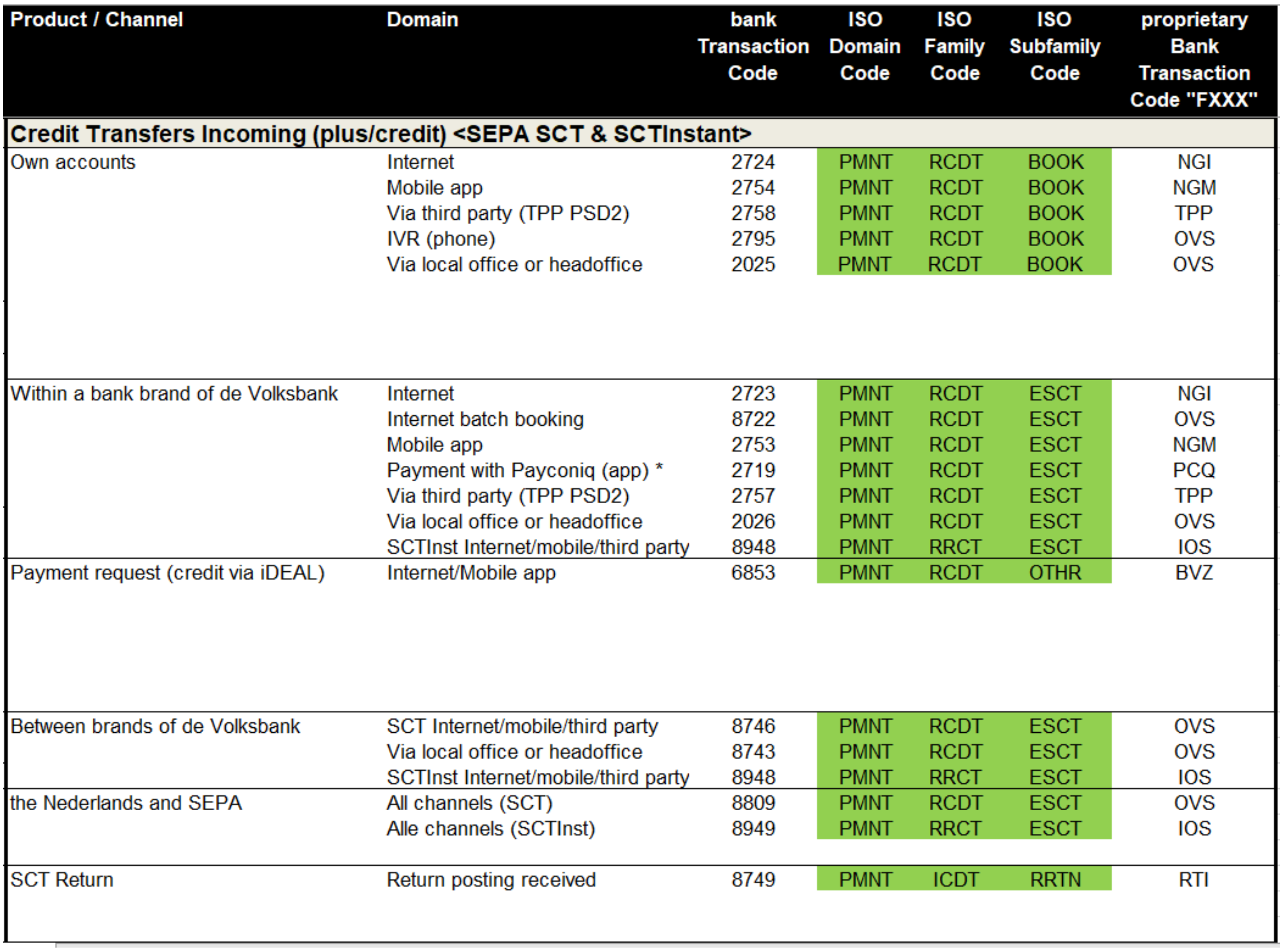
Product / Channel	Domain	bank Transaction Code	ISO Domain Code	ISO Family Code	ISO Subfamily Code	proprietary Bank Transaction Code "FXXX"
Credit Transfers outgoing (minus/debit) <SEPA SCT & SCTInstant>						
Internet	Own accounts	3724	PMNT	ICDT	BOOK	NGI
	SCT within a bank brand	3723	PMNT	ICDT	ESCT	NGI
	SCTinst within a bank brand, the bank & NL	9930	PMNT	IRCT	ESCT	IOI
	SCT NL+SEPA & TIPS (instant within EU)	9720	PMNT	ICDT	ESCT	NGI
	SCTinst within the Netherlands*	9933	PMNT	IRCT	ESCT	IOI
	SCT SEPA (excl. NL)*	9747	PMNT	ICDT	ESCT	OVS
Corporate Internet Banking batch booking	Own accounts, within the bank, the Nettherlands, SEPA	9722	PMNT	ICDT	ESCT	OVS
Mobile app	Own accounts	3754	PMNT	ICDT	BOOK	NGM
	SCT within a bank brand	3753	PMNT	ICDT	ESCT	NGM
	SCTinst within a bank brand, the bank & NL	9932	PMNT	IRCT	ESCT	IOM
	SCT NL+SEPA & TIPS (instant within EU)	9755	PMNT	ICDT	ESCT	NGM
	SCTinst within the Netherlands*	9935	PMNT	IRCT	ESCT	IOM
	SCT SEPA (excl. NL)*	9747	PMNT	ICDT	ESCT	OVS
Payment with Payconiq (app) *	SCT within a bank brand	3719	PMNT	ICDT	ESCT	PCQ
	SCT within the Netherlands / SEPA	9719	PMNT	ICDT	ESCT	PCQ
Via third party (TPP PSD2)	Own accounts	3758	PMNT	ICDT	BOOK	TPP
	SCT within a bank brand	3757	PMNT	ICDT	ESCT	TPP
	SCTinst within a bank brand, the bank & NL	9931	PMNT	IRCT	ESCT	ITP
	SCT NL+SEPA & TIPS (instant within EU)	9759	PMNT	ICDT	ESCT	TPP
	SCTinst within the Netherlands*	9934	PMNT	IRCT	ESCT	ITP
	SCT SEPA (excl. NL)*	9747	PMNT	ICDT	ESCT	OVS
Paper based payment	Within the bank / the Netherlands	9846	PMNT	ICDT	ESCT	OVS
(Optical readable form)	SCT SEPA (excl. NL)	9747	PMNT	ICDT	ESCT	OVS
Via IVR (phone)	Own accounts	3795	PMNT	ICDT	BOOK	OVS
Via local office or headoffice	Own accounts	3025	PMNT	ICDT	BOOK	OVS
	SCT within a bank brand	3026	PMNT	ICDT	ESCT	OVS
	SCT within the Netherlands / SEPA	9801	PMNT	ICDT	ESCT	OVS
Recall SCT	SCT: within the bank and the Netherlands	9718	PMNT	RCDT	RRTN	RTI
	SCTinst: within the bank (on us)	9948	PMNT	RCDT	RRTN	IOS
	SCTinst: not on us	9949	PMNT	RCDT	RRTN	IOS
Acceptgiro Outgoing (minus/debit) <SEPA SCT, Local instrument = ACCEPT>						
Internet *	SCT within the Netherlands	9721	PMNT	ICDT	ESCT	AGI
Mobile app *	SCT within the Netherlands	9756	PMNT	ICDT	ESCT	AGM
Paper based payment (optical readable)	SCT within the Netherlands	9844	PMNT	ICDT	ESCT	ACC
iDEAL outgoing (minus/debit) <SEPA SCT, Local instrument = IDEAL>						
Internet	SCT within the Netherlands / SEPA	9806	PMNT	ICDT	ESCT	IDE
Mobile appl	SCT within the Netherlands / SEPA	9856	PMNT	ICDT	ESCT	IDM
Dutch Urgent payments / TNS outgoing (minus/debit) *						
Internet	the Netherlands	9729	PMNT	ICDT	PRCT	OVS
Local office with charges	the Netherlands	9772	PMNT	ICDT	PRCT	OVS
Local office without charges	the Netherlands	9773	PMNT	ICDT	PRCT	OVS
Foreign payments (NON SEPA) outgoing (minus/debit)						
Internet	World	7727	PMNT	ICDT	XBCT	OVS
	Target cross border	7767	PMNT	ICDT	XBCT	OVS
Local office	Wereld	7761	PMNT	ICDT	XBCT	OVS
	Target cross border	7768	PMNT	ICDT	XBCT	OVS

Product / Channel	Domain	bank Transaction Code	ISO Domain Code	ISO Family Code	ISO Subfamily Code	proprietary Bank Transaction Code "FXXX"
SEPA Direct Debets (minus/debit)						
CORE SDD	the Netherlands and SEPA	9714	PMNT	RDDT	ESDD	EIC
B2B SDD	the Netherlands and SEPA	9827	PMNT	RDDT	BBDD	EIC
Overheidsvordering (Govermental debit)	the Netherlands	9885	PMNT	RDDT	PMDD	MSC
SDD Return	the Netherlands and SEPA	9715	PMNT	IDDT	UPDD	RTI
SDD Refund	the Netherlands and SEPA	9716	PMNT	IDDT	UPDD	RTI
SDD Reversal	the Netherlands and SEPA	9717	PMNT	IDDT	PRDD	RTI
SDD Reject	by creditor bank	9842	PMNT	IDDT	RCDD	RTI
Automated credit transfers outgoing (minus/debit)						
Automated deposits (internet)	Own accounts, fixed amount	3700	PMNT	ICDT	AUTT	POV
	Own accounts, cash pooling	3701	CAMT	ACCB	SWEP	POV
Standing orders (internet, mobile app, local office)	Bank/Nederland/SEPA	9802	PMNT	ICDT	STDO	POV
Cash withdrawel (minus/debit)						
Local office	RegioBank	1002	PMNT	CNTR	BCWD	KAS
ATM SNS	SNS	1003 / 7008	PMNT	CCRD	CWDL	GEA
ATM NL (Meastro)	the Netherlands	7900 / 9900	PMNT	CCRD	CWDL	GEA
ATM NL (VPay)	the Netherlands	7910 / 9910	PMNT	CCRD	CWDL	GEA
ATM EU (Meastro)	Europe	7901 / 9901	PMNT	CCRD	XBCW	GEA
ATM EU (VPay)	Europe	7911 / 9911	PMNT	CCRD	XBCW	GEA
ATM World (Meastro)	World	7902 / 9902	PMNT	CCRD	XBCW	GEA
ATM World (VPay)	World	7912 / 9912	PMNT	CCRD	XBCW	GEA
POS Card payments (minus/debit)						
POS NL (Meastro)	the Netherlands	7903 / 9903	PMNT	CCRD	POSD	BEA
POS NL (VPay)	the Netherlands	7913 / 9913	PMNT	CCRD	POSD	BEA
POS EU (Meastro)	Europe	7904 / 9904	PMNT	CCRD	POSD	BEA
POS EU (VPay)	Europe	7914 / 9914	PMNT	CCRD	POSD	BEA
POS World (Meastro)	World	7905 / 9905	PMNT	CCRD	POSD	BEA
POS World (VPay)	World	7915 / 9915	PMNT	CCRD	POSD	BEA
POS Card Refund (minus/debit)						
POS (Maestro), debit correction		7909 / 9909	PMNT	CCRD	RIMB	RTI
POS (Vpay), debit correction		7920 / 9920	PMNT	CCRD	RIMB	RTI
Mobile payments / NFC (minus/debit)						
NFC NL (Meastro)	the Netherlands	7906 / 9906	PMNT	CCRD	POSD	BEA
NFC NL (VPay)	the Netherlands	7916 / 9916	PMNT	CCRD	POSD	BEA
NFC EU (Meastro)	Europe	7907 / 9907	PMNT	CCRD	POSD	BEA
NFC EU (VPay)	Europe	7917 / 9917	PMNT	CCRD	POSD	BEA
NFC World (Meastro)	World	7908 / 9908	PMNT	CCRD	POSD	BEA
NFC World (VPay)	World	7918 / 9918	PMNT	CCRD	POSD	BEA
Card not present payments (minus/debit) (available in due course)						
NL (Mastercard)	the Netherlands	7923 / 9923	PMNT	CCRD	POSD	OVS
NL (VISA)	the Netherlands	7926 / 9926	PMNT	CCRD	POSD	OVS
EU (Mastercard)	Europe	7924 / 9924	PMNT	CCRD	POSD	OVS
EU (VISA)	Europe	7927 / 9927	PMNT	CCRD	POSD	OVS
World (Mastercard)	World	7925 / 9925	PMNT	CCRD	POSD	OVS
World (VISA)	World	7928 / 9928	PMNT	CCRD	POSD	OVS



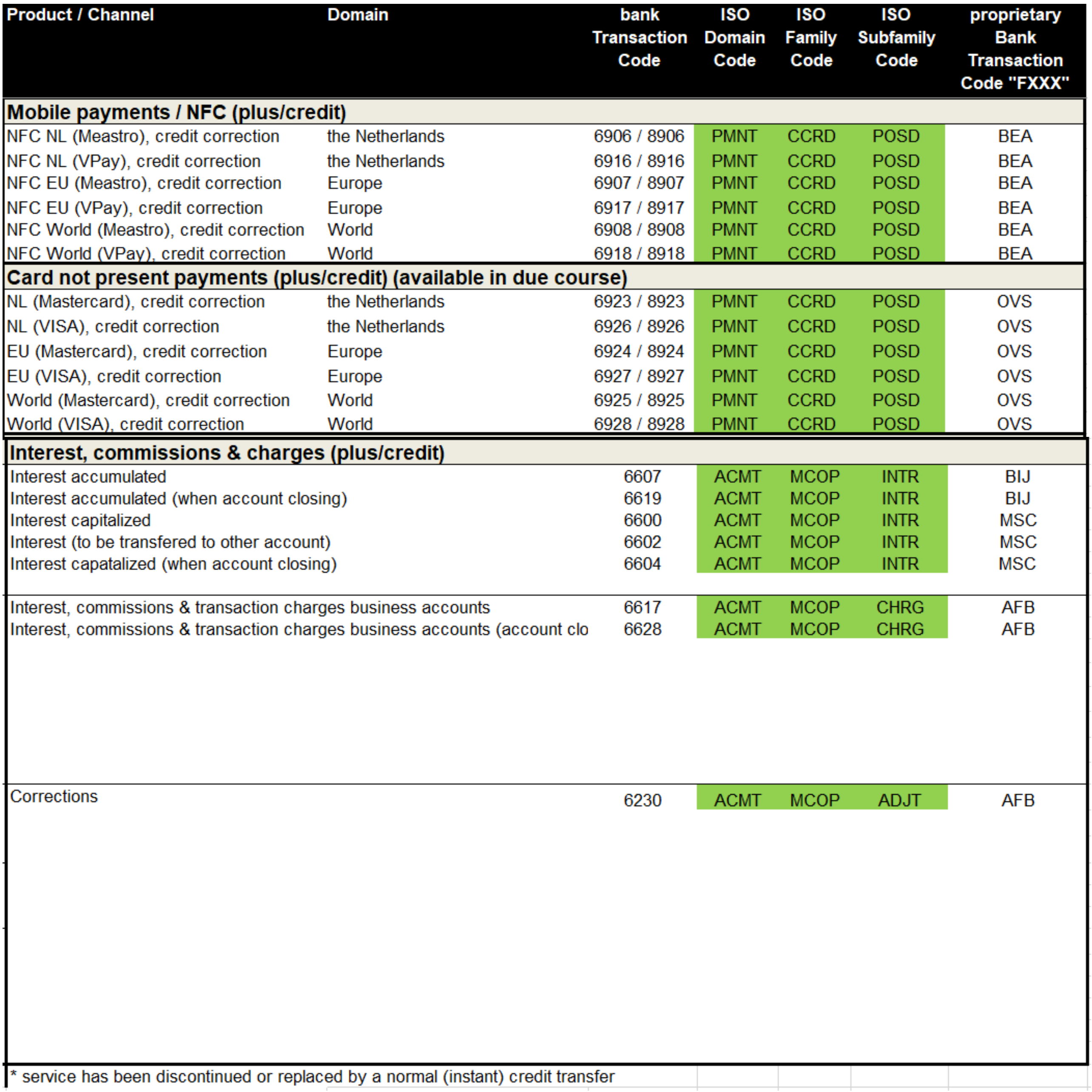
Product / Channel	Domain	bank Transaction Code	ISO Domain Code	ISO Family Code	ISO Subfamily Code	proprietary Bank Transaction Code "FXXX"
Interest, commissions & charges (minus/debit)						
Interest accumulated		7606	ACMT	MDOP	INTR	AFB
Interest accumulated (when account closing)		7618	ACMT	MDOP	INTR	AFB
Interest capitalized		7600	ACMT	MDOP	INTR	MSC
Interest (to be transfered to other account)		7602	ACMT	MDOP	INTR	MSC
Interest capatalized (when account closing)		7604	ACMT	MDOP	INTR	MSC
Interest correction		7225	ACMT	MDOP	INTR	AFB
Interest, commissions & transaction charges business accounts		7617	ACMT	MDOP	CHRG	AFB
Interest, commissions & transaction charges business accounts (account closing)		7628	ACMT	MDOP	CHRG	AFB
Reporting costs offline business accounts		7614	ACMT	MDOP	CHRG	AFB
Reporting costs offline business accounts (account closing)		7626	ACMT	MDOP	CHRG	AFB
Administrative commissions business accounts		7642	ACMT	MDOP	CHRG	AFB
Administrative commissions business accounts (account closing)		7643	ACMT	MDOP	CHRG	AFB
KYC charges business accounts		7261	ACMT	MDOP	CHRG	AFB
Transaction charges business accounts		7615	ACMT	MDOP	CHRG	AFB
Transaction charges business accounts (account closing)		7627	ACMT	MDOP	CHRG	AFB
Commission account usage		7241	ACMT	MDOP	CHRG	AFB
Commission account usage "Basis Bankieren"		7260	ACMT	MDOP	CHRG	MSC
Charges usage card		7227	PMNT	CCRD	CHRG	AFB
Commissions Business Internet Banking		7734	ACMT	MDOP	CHRG	MSC
Transaction downloading costs Business Internet Banking		7737 / 7738	ACMT	MDOP	CHRG	MSC
Charges payment requests issued by business customers		7259	PMNT	ICDT	CHRG	AFB
Charges international payments (non-SEPA)		7228	PMNT	ICDT	CHRG	AFB
Charges sending paper statement		7236	ACMT	MDOP	CHRG	AFB
Charges paper based credit transfers		7240	ACMT	MDOP	CHRG	AFB
Charges Dutch Urgent payments*		7237	PMNT	ICDT	CHRG	AFB
Charges ATM		7921 / 9921	PMNT	CCRD	CHRG	MSC
Charges POS		7922 / 9922	PMNT	CCRD	CHRG	BEA
* service has been discontinued or replaced by a normal (instant) credit transfer						

Credit entries



Product / Channel	Domain	bank Transaction Code	ISO Domain Code	ISO Family Code	ISO Subfamily Code	proprietary Bank Transaction Code "FXXX"
Credit Transfers Incoming (plus/credit) <SEPA SCT & SCTInstant>						
Own accounts	Internet	2724	PMNT	RCDT	BOOK	NGI
	Mobile app	2754	PMNT	RCDT	BOOK	NGM
	Via third party (TPP PSD2)	2758	PMNT	RCDT	BOOK	TPP
	IVR (phone)	2795	PMNT	RCDT	BOOK	OVS
	Via local office or headoffice	2025	PMNT	RCDT	BOOK	OVS
Within a bank brand of de Volksbank	Internet	2723	PMNT	RCDT	ESCT	NGI
	Internet batch booking	8722	PMNT	RCDT	ESCT	OVS
	Mobile app	2753	PMNT	RCDT	ESCT	NGM
	Payment with Payconiq (app) *	2719	PMNT	RCDT	ESCT	PCQ
	Via third party (TPP PSD2)	2757	PMNT	RCDT	ESCT	TPP
	Via local office or headoffice	2026	PMNT	RCDT	ESCT	OVS
	SCTInst Internet/mobile/third party	8948	PMNT	RRCT	ESCT	IOS
Payment request (credit via iDEAL)	Internet/Mobile app	6853	PMNT	RCDT	OTHR	BVZ
Between brands of de Volksbank	SCT Internet/mobile/third party	8746	PMNT	RCDT	ESCT	OVS
	Via local office or headoffice	8743	PMNT	RCDT	ESCT	OVS
	SCTInst Internet/mobile/third party	8948	PMNT	RRCT	ESCT	IOS
the Nederlands and SEPA	All channels (SCT)	8809	PMNT	RCDT	ESCT	OVS
	Alle channels (SCTInst)	8949	PMNT	RRCT	ESCT	IOS
SCT Return	Return posting received	8749	PMNT	ICDT	RRTN	RTI

Product / Channel	Domain	bank Transaction Code	ISO Domain Code	ISO Family Code	ISO Subfamily Code	proprietary Bank Transaction Code "FXXX"
Acceptgiro incoming (plus/credit) <SEPA SCT, local instrument = ACCEPT>						
the Nederlands	All channels (SCT)	8845	PMNT	RCDT	ESCT	ACC
iDEAL incoming (plus/credit) <SEPA SCT, Local instrument = IDEAL>						
Netherlands/SEPA	Internet/Mobile	8806	PMNT	RCDT	ESCT	IDE
Netherlands/SEPA	Internet/Mobile (within the bank / brands	8877	PMNT	RCDT	ESCT	IDE
Netherlands/SEPA batch booking	Internet/Mobile	2806	PMNT	RCDT	ESCT	IDE
Dutch Urgent Payments / TNS incoming (plus/credit) *						
Between brands of de Volksbank	All channels	8783	PMNT	RCDT	PRCT	OVS
the Netherlands	All channels	8872	PMNT	RCDT	PRCT	OVS
Foreign payments (NON SEPA) incoming (plus/credit)						
World	All channels	6761	PMNT	RCDT	XBCT	OVS
Target cross border	All channels	6768	PMNT	RCDT	XBCT	OVS
SEPA Direct Debets (plus/credit)						
SDD Return	by debtor bank	8715	PMNT	RDDT	UPDD	RTI
SDD Refund	Internet/mobile app/local office	8716	PMNT	RDDT	UPDD	RTI
SDD Reversal		8717	PMNT	RDDT	PRDD	RTI
SDD Core recurring	Corporate internet banking	8820	PMNT	IDDT	ESDD	EIC
SDD Core one-off	Corporate internet banking	8821	PMNT	IDDT	OODD	EIC
SDD Reject	by creditor bank	8842	PMNT	IDDT	RCDD	RTI
Automated credit transfers incoming (plus/credit)						
Own accounts, fixed amount	Internet	2700	PMNT	RCDT	AUTT	POV
Own accounts, cash pooling	Internet	2701	CAMT	ACCB	TOPG	POV
Standing order within a bank brand of de Volksbank	Internet/Mobile app/ Local office	8706	PMNT	RCDT	STDO	POV
Standing order between brands of de Volksbank	Internet/Mobile app/ Local office	8746	PMNT	RCDT	STDO	POV
Cash deposit (plus/credit)						
Local office	RegioBank	0001	PMNT	CNTR	BCDP	KAS
ATM NL (Meastro), credit correction	the Netherlands	6900 / 8900	PMNT	CCRD	CWDL	GEA
ATM NL (VPay), credit correction	the Netherlands	6910 / 8910	PMNT	CCRD	CWDL	GEA
ATM EU (Meastro), credit correction	Europe	6901 / 8901	PMNT	CCRD	XBCW	GEA
ATM EU (VPay), credit correction	Europe	6911 / 8911	PMNT	CCRD	XBCW	GEA
ATM World (Meastro), credit correction	World	6902 / 8902	PMNT	CCRD	XBCW	GEA
ATM World (VPay), credit correction	World	6912 / 8912	PMNT	CCRD	XBCW	GEA
POS Card payment (plus/credit)						
POS NL (Meastro), credit correction	the Netherlands	6903 / 8903	PMNT	CCRD	POSD	BEA
POS NL (VPay), credit correction	the Netherlands	6913 / 8913	PMNT	CCRD	POSD	BEA
POS EU (Meastro), credit correction	Europe	6904 / 8904	PMNT	CCRD	POSD	BEA
POS EU (VPay), credit correction	Europe	6914 / 8914	PMNT	CCRD	POSD	BEA
POS World (Meastro), credit correction	World	6905 / 8905	PMNT	CCRD	POSD	BEA
POS World (VPay), credit correction	World	6915 / 8915	PMNT	CCRD	POSD	BEA
POS Card Refund (plus/credit)						
POS (Maestro)		6909 / 8909	PMNT	CCRD	RIMB	RTI
POS (Vpay)		6920 / 8920	PMNT	CCRD	RIMB	RTI



Product / Channel	Domain	bank Transaction Code	ISO Domain Code	ISO Family Code	ISO Subfamily Code	proprietary Bank Transaction Code "FXXX"
Mobile payments / NFC (plus/credit)						
NFC NL (Meastro), credit correction	the Netherlands	6906 / 8906	PMNT	CCRD	POSD	BEA
NFC NL (VPay), credit correction	the Netherlands	6916 / 8916	PMNT	CCRD	POSD	BEA
NFC EU (Meastro), credit correction	Europe	6907 / 8907	PMNT	CCRD	POSD	BEA
NFC EU (VPay), credit correction	Europe	6917 / 8917	PMNT	CCRD	POSD	BEA
NFC World (Meastro), credit correction	World	6908 / 8908	PMNT	CCRD	POSD	BEA
NFC World (VPay), credit correction	World	6918 / 8918	PMNT	CCRD	POSD	BEA
Card not present payments (plus/credit) (available in due course)						
NL (Mastercard), credit correction	the Netherlands	6923 / 8923	PMNT	CCRD	POSD	OVS
NL (VISA), credit correction	the Netherlands	6926 / 8926	PMNT	CCRD	POSD	OVS
EU (Mastercard), credit correction	Europe	6924 / 8924	PMNT	CCRD	POSD	OVS
EU (VISA), credit correction	Europe	6927 / 8927	PMNT	CCRD	POSD	OVS
World (Mastercard), credit correction	World	6925 / 8925	PMNT	CCRD	POSD	OVS
World (VISA), credit correction	World	6928 / 8928	PMNT	CCRD	POSD	OVS
Interest, commissions & charges (plus/credit)						
Interest accumulated		6607	ACMT	MCOP	INTR	BIJ
Interest accumulated (when account closing)		6619	ACMT	MCOP	INTR	BIJ
Interest capitalized		6600	ACMT	MCOP	INTR	MSC
Interest (to be transfered to other account)		6602	ACMT	MCOP	INTR	MSC
Interest capatalized (when account closing)		6604	ACMT	MCOP	INTR	MSC
Interest, commissions & transaction charges business accounts		6617	ACMT	MCOP	CHRG	AFB
Interest, commissions & transaction charges business accounts (account clo		6628	ACMT	MCOP	CHRG	AFB
Corrections		6230	ACMT	MCOP	ADJT	AFB
* service has been discontinued or replaced by a normal (instant) credit transfer						