asn bank

AIS API

PSD2 interface AIS ASN Bank

Version 1.25
July 1 2025

Colophon

Label	Data
Owner	Service Centre KBS ASN Bank NV
Authors	ITC VO KWB Open Banking
Status	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.
1.22	2025-01-08	- Added endpoints for the AIS Consent API v2: initiate account access consent, get account access consent, get account access consent status, and delete account access consent. - Updated Appendix A, list of bank transaction codes. Updates are marked in red.
1.23	2025-04-24	- Removed Appendix A (is now a separate file on our documentation website). - Updated format of tables and added Appendix 1 Data Dictionary as reference.
1.24	2025-05-22	- Updated information on notifications. - Fixed error regarding data type of field bankTransactionCode.
1.25	2025-07-01	- Rebranded de Volksbank NV to ASN Bank NV. - Removed documentation for deprecated v1 consent endpoints.

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	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 ASN Bank 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) for the AIS endpoints (readAccountList, readBalance, and readTransactionList);
- follows the Berlin Group openFinance API Framework Implementation Guidelines (Consent API for V2.x) for the consent endpoints.

The remainder of this document will be organized as follows:

- Chapter 2 describes the conditions ASN Bank applies to the use of its account initiation services, the character set used for the account information to be exchanged between the AISPs and ASN Bank 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 ASN Bank;
- 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 ASN Bank

2.1 Conditions on the use of ASN Bank'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, ASN Bank 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 ASN Bank NV 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

ASN Bank 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, ASN Bank 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 ASN Bank. 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 ASN Bank 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 ASN Bank 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

ASN Bank 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

ASN Bank 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 consent endpoints (endpoints 1, 4, 7 and 8) are also known as the account access consent endpoints. This follows the consent categories defined by the Berlin Group openFinance API Framework. Account access consents are consents for AIS access to addressed accounts.

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 ASN Bank offers, we will point out which of these elements they have and explain them in depth.

4.1 Account access consent initiation request

By issuing an account access 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.

Account access consents can be valid for multiple (current/payment) accounts at once. The AISP can provide one or more accounts in the request body, or the PSU can select one or more accounts when authorizing the account access consent.

[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).

4.1.1 Method and URL

Method	URL	Description
POST	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v2/consents/account-access	Account access consent request endpoint as defined by the Berlin Group in the openFinance API Framework Implementation Guidelines Consent API for V2.x version 2.0.

4.1.2 Path parameters

The account access consent request endpoint does not have any path parameters.

4.1.3 Query parameters

The account access 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 a client_id*:* identification of the AISP as registered with ASN Bank.
PSU-IP-Address	String	Y	Attribute filled with the IP-address of the PSU as recorded in the HTTP request from the PSU to the PISP. If the PSU has not sent its IP-address to the PISP, the PISP has to send its own IP-address.
TPP-Redirect-URI	String	Y	URI of the TPP, where the transaction flow shall be redirected to after a Redirect.
Client-Notification-URI	String	N	Use this header when you want to receive notifications. The URI of the Client API where notifications about the consent status will be sent towards. The URI should match with the common name or one of the domains of the QWAC certificate.

Attribute	Type	Mandatory	Description
Client-Notification-Content-Preferred	String	N	Use this header when you want to receive notifications. The string has the form 'status=X1, …, Xn'. Xi is one of SCA, PROCESS, or LAST, and the constants are not repeated. Only SCA is supported by ASN Bank. We support one event: 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	AccountAccess*	Y	This attribute refers to the requested access services. The choice of consentType (see next attribute) influences what this attribute is allowed to contain.
consentType	String	Y	The technical consent type. The choice of this type has an effect on the allowed rights in the access attribute. Values are conform the Berlin Group Consent Type Code list. ASN Bank only supports consents with consentType "global" or "detailed".

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 AISP will have ten minutes, starting from the moment of the first Read Transaction List call, for requesting the transaction data.
validTo	Date	Y	The attribute validTo 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. SCA expiration date: 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 validTo value is less than 180 days in the future then that value will be used as SCA expiration date, 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.

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.

*For a data dictionary, see appendix 1.

4.1.6 Example request

Example global consent:

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v2/consents/account-access
Content-Type:       application/json
X-Request-ID:       99391c7e-ad88-49ec-a2ad-99ddcb1f7756
Authorization:      l71bc95e703f6042e881384c746532dcfe
PSU-IP-Adress:      192.168.8.78
TPP-Redirect-URI:   https://www.redirect-to-me.com
   { "access": {
         "payments": [
            {
               "rights": [
                  "ais", "ownerName"
               ]
            }
         ]
      },
      "consentType": "global",
      "recurringIndicator": true,
      "validTo": "2025-07-05",
```

```
      "frequencyPerDay": 4
   }
```

Example detailed consent without account information:

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v2/consents/account-access
Content-Type:       application/json
X-Request-ID:       99391c7e-ad88-49ec-a2ad-99ddcb1f7756
Authorization:      l71bc95e703f6042e881384c746532dcfe
PSU-IP-Adress:      192.168.8.78
TPP-Redirect-URI:   https://www.redirect-to-me.com
{ "access": {
         "payments": [
            {
               "rights": [
                  "accountList", "transactions", "ownerName"
               ]
            }
         ]
      },
      "consentType": "detailed",
      "recurringIndicator": true,
      "validTo": "2025-07-05",
      "frequencyPerDay": 4
   }
```

Example detailed consent with account information, for access to two accounts:

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v2/consents/account-access
Content-Type:       application/json
X-Request-ID:       99391c7e-ad88-49ec-a2ad-99ddcb1f7756
Authorization:      l71bc95e703f6042e881384c746532dcfe
PSU-IP-Adress:      192.168.8.78
TPP-Redirect-URI:   https://www.redirect-to-me.com
{ "access": {
         "payments": [
            {
               "account": {
                  "iban": "NL64SNSB0948305280"
```

```
            },
            "rights": [
               "accountList", "transactions", "ownerName"
            ]
         },
         {
            "account": {
               "iban": "NL64SNSB0948305281"
            },
            "rights": [
               "accountList", "transactions", "ownerName"
            ]
         }
      ]
   },
   "consentType": "detailed",
   "recurringIndicator": true,
   "validTo": "2025-07-05",
   "frequencyPerDay": 4
}
```

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”.
ASPSP-Notification-Support	Boolean	N	Only returned when the request contained notification headers. When returned, always contains “true” since ASN Bank supports resource push notifications for account access consents.

Attribute	Type	Mandatory	Description
ASPSP-Notification-Content	String	N	Only returned when the request contained notification headers. When returned, always contains "status=SCA" since only SCA is supported by ASN Bank.

4.1.9 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. In case of a successful consent request (HTTP status code 201), only the status "received", as defined by the Berlin Group, 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 response

```
HTTP/1.x 201 Created

Content-Type:       application/json

Location:
https://psd.bancairediensten.nl/psd2/snsbank/v2/consents/account-
access/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

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 ASN Bank.

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. ASN Bank 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 request

```
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 response

```
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

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 ASN Bank, 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 response

```
HTTP/1.x 302

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

4.4 Get account access consent status request

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

4.4.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v2/consents/account-access/{consent-id}/status	Get account access consent status request endpoint as defined by the Berlin Group in the openFinance API Framework Implementation Guidelines Consent API for V2.x version 2.0.

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 account access consent status endpoint does not have any query parameters.

4.4.4 Request header

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 consists of client_id: identification of the AISP as registered with ASN Bank.

4.4.5 Request body

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

4.4.6 Example request

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v2/consents/account-access/05873005-99c2-42ed-810e-99e6a91ce335/status
X-Request-ID:       fdb9757d-8f27-4f9e-9be0-0eadacc89012
Authorization:      l32b095e702f5952e881373c746532dafe
```

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; 8. replacedByTpp. ASN Bank 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 section 4.2) or start with creating a new consent ID (refer to section 4.1.);
- *rejected,* the PSU has cancelled the consent during the approval process (refer to section 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 section 4.3) and must exchange this code for an access token and refresh token (refer to section 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 section 4.1);
- *terminatedByTpp,* the AISP has terminated the consent by applying the DELETE method to the consent resource (see also section 4.8).
- *replacedByTpp,* the AISP has terminated the consent implicitly by submitting a new (recurring) consent for the same PSU/Corporate.

4.4.10 Example response

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

4.5 Access token request

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 ASN Bank.

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. ASN Bank 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 ASN Bank; – client_secret: secret agreed between the AISP and ASN Bank.

4.5.5 Request body

The token endpoint does not have a request body.

4.5.6 Example request

```
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 response

```
HTTP/1.x 200 Ok
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

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 ASN Bank.

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. ASN Bank 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 ASN Bank; – client_secret: secret agreed between the AISP and ASN Bank.

4.6.5 Request body

The token endpoint does not have a request body.

4.6.6 Example request

```
POST
https://psd.bancairediensten.nl/psd2/snsbank/v1/token?grant_type=
refresh_token&refresh_token=<REFRESH_TOKEN>&redirect_uri=https://thirdpar
ty.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 response

```
HTTP/1.x 200 Ok
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 account access consent request

With the get account access consent endpoint, an AISP can request additional information about an account access 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]/v2/consents/account-access/{consent-id}	Get account access consent endpoint as defined by the Berlin Group in the openFinance API Framework Implementation Guidelines Consent API for V2.x version 2.0.

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 account access consent endpoint does not have any query parameters.

4.7.4 Request header

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 account access consent endpoint does not have a request body.

4.7.6 Example request

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

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	AccountAccess*	Y	This attribute refers to the requested access services. It contains an array of Account Access Rights in the payments field.
consentType	String	Y	The technical consent type as submitted by the AISP in the initiation request.
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.
validTo	Date	Y	The attribute validTo contains the date until when the consent is valid. The attribute has the ISO 8601 Date format (YYYY-MM-DD). SCA expiration date: 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 validTo value that the AISP submitted is less than 180 days in the future then that value will be used as SCA expiration date, 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".
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; 8. replacedByTpp. ASN Bank 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.

*For a data dictionary, see appendix 1.

4.7.10 Example response

Example global consent:

```
HTTP/1.x 200 Ok
X-Request-ID: fdb9757d-8f27-4f9e-9be0-0eadacc89012
Content-Type: application/json
   { "access": {
         "payments": [
            {
               "account": {
                  "iban": "NL64SNSB0948305280"
               },
               "rights": [
                  "ais", "ownerName"
               ]
            }
         ]
      },
      "consentType": "global",
      "recurringIndicator": true,
      "validTo": "2025-07-05",
      "frequencyPerDay": 4,
      "consentStatus": "valid"
   }
```

Example detailed consent for two accounts:

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

```
                "iban": "NL64SNSB0948305280"
            },
            "rights": [
                "accountList", "transactions", "ownerName"
            ]
        },
        {
            "account": {
                "iban": "NL64SNSB0948305281"
            },
            "rights": [
                "accountList", "transactions", "ownerName"
            ]
        }
    ]
  },
  "consentType": "detailed",
  "recurringIndicator": true,
  "validTo": "2025-07-05",
  "frequencyPerDay": 4,
  "consentStatus": "valid"
}
```


4.8 Delete account access consent request

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

4.8.1 Method and URL

Method	URL	Description
DELETE	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v2/consents/account-access/{consent-id}	Delete account access consent endpoint as defined by the Berlin Group in the openFinance API Framework Implementation Guidelines Consent API for V2.x version 2.0.

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 account access consent endpoint does not have any query parameters.

4.8.4 Request header

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.

4.8.5 Request body

The delete account access consent endpoint does not have a request body.

4.8.6 Example request

```
DELETE https://psd.bancairediensten.nl/psd2/snsbank/v2/consents/account-access/05873005-99c2-42ed-810e-99e6a91ce335
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 account access consent endpoint does not have a response body.

4.8.10 Example response

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

4.9 Renewing a consent

When the SCA expires but the consent's validTo 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;
- ValidTo 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 section 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(s) 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.

5 ASN Bank Account Information Services

The Account Information Services (AIS) ASN Bank 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.

ASN Bank 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.

5.1 Read Account List request

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, ASN Bank 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.

5.1.1 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.

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	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 ASN Bank. It should be left out.

5.1.4 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.

5.1.5 Request body

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

5.1.6 Example request

```
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>
```

5.1.7 Response code

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*".
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).

5.1.9 Response body

Attribute	Type	Mandatory	Description
accounts	Array of AccountDetails*	Y	Contains the requested details of the account.

*For a data dictionary, see appendix 1.

5.1.10 Example response

```
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"
      }
    ]
}
```

5.2 Read Balance request

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]/v1.1/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	UUID	Y	The UUID identifying the account as returned by the service *Read Account List*.

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 "*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.

5.2.5 Request body

The Read Balance endpoint does not have a request body.

5.2.6 Example request

```
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>
```

5.2.7 Response code

Code	Description
200	Ok

5.2.8 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).

5.2.9 Response body

Attribute	Type	Mandatory	Description
account	AccountReference*	N	This attribute is optional and ASN Bank does not return it.
balances	Array of Balance*	Y	Balance information of the account.

*For a data dictionary, see appendix 1.

5.2.10 Example response

```
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 request

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.

5.3.1 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.

5.3.2 Path parameters

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

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). 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.* ASN Bank accepts the values "**booked**" and "**both**", but ASN Bank will only return transactions with the status "**booked**". Please note that ASN Bank 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. ASN Bank has set the **maximum** limit to **2000** transactions. ASN Bank 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.

5.3.4 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.

5.3.5 Request body

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

5.3.6 Example request

```
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>
```

5.3.7 Response code

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*".
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).

5.3.9 Response body

Attribute	Type	Mandatory	Description
account	AccountReference *	N	Attribute filled with details of the account.
transactions	AccountReport*	N	JSON based account report. This account report contains transactions resulting from the query parameters.

*For a data dictionary, see appendix 1.

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.

5.3.10 Example response

```
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/3fdb8946-52ee-4a6d-8a0c-c7ba6f4a45ed"
         },
       "next":{
          "href":"
https://psd.bancairediensten.nl/psd2/snsbank/v1.1/accounts/3fdb8946-52ee-4a6d-8a0c-
c7ba6f4a45ed/transactions?bookingStatus=BOOKED&nextPageKey=abcdef123"
```

```
        }
    }
  }
}
```

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,creditorAccount,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"}
    ]
  }
}
```

6 Error handling

6.1.1 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.

6.1.2 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.

6.1.3 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 1: Data Dictionary

AccountAccess

Attribute	Type	Mandatory	Description
payments	Array of AccountAccessRights	Y	This field presents the required access rights to current/payment accounts. It contains an account reference and a list of access right codes.

AccountAccessRights

Attribute	Type	Mandatory	Description
account	AccountReference	N	Account Reference contains an IBAN (String, format: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}).
rights	List of AccessRightsCodes	Y	This field contains the access rights. Supported by ASN Bank: ais, accountList, balances, transactions, ownerName. The right ais gives access to accountList, balances, and transactions. A balances or transactions access right implicitly also gives access to accountList. Without the right ownerName, the field ownerName will not be returned in the readAccountList response. The choice of consentType influences what the access attribute is allowed to contain. For a global consent, the following rights are allowed: ais and ownerName. The right ais is mandatory for a global consent. It is not allowed to include one or more account references during initiation. For a detailed consent, the following rights are allowed: accountList, balances, transactions and ownerName. The AISP can provide one or more account references in the access attribute. When providing multiple accounts, the rights for each account should be the same. When one or more accounts are provided, the PSU does not have the option to select other or additional accounts when authorizing the consent.

AccountDetails

Attribute	Type	Mandatory	Description
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

AccountReference

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

AccountReport

Attribute	Type	Mandatory	Description
booked	Array of Transactions	N	Array of Transactions objects.
_links	Links	Y	A list of hyperlinks to be recognised by the AISP. 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 (ASN Bank 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.

Amount

Attribute	Type	Mandatory	Description
currency	String	Y	Attribute is part of the array *Amount* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code.
amount	String	Y	Attribute is part of the array *Amount* as defined by the Berlin Group. The amount given with fractional digits, if needed. The decimal separator is a dot. The number of fractional digits (or minor unit of currency) must comply with ISO 4217. totalDigits: 18 fractionDigits: 5.

Balance

Attribute	Type	Mandatory	Description
balanceType	String	Y	ASN Bank only supports the balance type *interimAvailable*
balanceAmount	Amount	Y	Amount.

Attribute	Type	Mandatory	Description
lastChangeDateTime	String	N	Last time the balanceAmount has changed. Format is ISODateTime.

Href

Attribute	Type	Mandatory	Description
href	String	Y	No specific length defined by the Berlin Group.

Links

Attribute	Type	Mandatory	Description
account	Href	N	A link to the resource providing the details of one Account.
next	Href	N	Navigation link for paginated account reports.

RemittanceInformationStructured

Attribute	Type	Mandatory	Description
reference	String	N	Creditor reference.
referenceIssuer	String	N	Reference to the issuer of the structured remittance information, e.g. 'iso' of 'cur'.

Transactions

Attribute	Type	Mandatory	Description
entryReference	String	N	The attribute *entryReference* is a concatenation of journaldate and a sequence number. The format is YYYYMMDD-XXXXXXXX. The journal date has the format is YYYYMMDD. The sequence number is a numerical string with a maximum of 8 digits without leading zeros.
endToEndId	String	N	Unique identification as provided by a third party or entered by the PSU. The ISO 20022 length of the attribute is Max35Text.
mandateId	String	N	The attribute *mandateId* contains the unique identification, as assigned by the creditor, to unambiguously identify the mandate belonging to a direct debit agreement. The ISO 20022 length of the mandateId value is Max35Text.

Attribute	Type	Mandatory	Description
creditorId	String	N	EPC rulebook attribute AT-02 for SEPA Direct Debits: Identifier of the Creditor. Max35Text
bookingDate	String	N	The date when an entry is posted to an account on the ASPSPs books. Format is YYYYMMDD
valueDate	String	N	The date 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	Y	Amount of the transaction.
creditorName	String	N	Counterparty to which an amount of money is due. Max70Text
creditorAccount	AccountReference	N	Details of the creditor account.
ultimateCreditor	String	N	Name of the ultimate creditor.
debtorName	String	N	Counterparty that owes an amount of money to the (ultimate) creditor. Max70Text
debtorAccount	AccountReference	N	Details of the debtor account.
ultimateDebtor	String	N	Name of the ultimate debtor.
remittanceInformationUnstructured	String	N	Max140Text. Please note: In case of international payments (non-SEPA) and card based transactions, this attribute is filled with extended booking information.
remittanceInformationStructured	RemittanceInformationStructured	N	Structured remittance information.
purposeCode	String	N	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	Integer	N	Note: ASN Bank will fill in a numerical code, as ASN Bank does not use the ISO 20022 codes. See also 'Transaction Codeset ASN Bank for AIS' on our documentation website.

Attribute	Type	Mandatory	Description
proprietaryBankTransactionCode	String	N	The proprietary transaction code used by ASN Bank. See also 'Transaction Codeset ASN Bank for AIS' on our documentation website.
batchIndicator	Boolean	N	If this indicator equals true, then the related entry is a batch entry.
batchNumberOfTransactions	Integer	N	Shows the number of transactions in a batch entry. Only used when the value of batchIndicator equals true.
paymentInformationIdentification	String	N	Reference assigned by a sending party in order to unambiguously identify the batch payment.
instructionIdentification	String	N	A unique reference assigned by the initiator to unambiguously identify the transaction.
transactionIdentification	String	N	TransactionIdentification is the identification of the initiating party. If ASN Bank initiates a transaction on behalf of her customer then this identification is an ASN Bank identification. If ASN Bank receives a transaction from an initiating party then the identification of this initiating party is used.
returnInformationCode	String	N	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).