PIS API

PSD2 interface PIS de Volksbank

September 28 2023

Colophon

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

Version and change log

Version	Date	Changes
1.0	2019-04-04	Final version
1.1	2019-07-05	- Added the *Get Transaction Status Request* endpoint; - Updated request and response objects and headers (4).
1.2	2019-08-02	- Added error information.
1.3	2019-09-12	- Added information about Android problem in 2.4; - Updated path parameters for refresh token call.
1.4	2019-11-21	- Added information about agended payments; - Added information about the *Cancel Payments* endpoint; - Updated response headers payment initiation call.
1.5	2020-01-27	- Changed authorization for the *Get Payment Status* endpoint and added information about the meaning of several payment statuses.
1.6	2020-04-29	- Updated certificates paragraph.
1.7	2020-07-14	- Added the *Get Payment* endpoint; - Added *Initiate Payment* validations; - Added missing error messages; - Removed unnecessary redirect uri paragraph; - Changed redirect uri in example response to new redirect uri.
1.8	2020-07-14	- Added the *periodic payment* payment service; - Added the *Get Payment* endpoint for periodic payment.
1.9	2021-06-08	- Added v1.1 of the *Get Payment Status* endpoints for one-time direct, one-time agended and deferred payments.
1.10	2021-10-20	- Added *Initiate Bulk Payment* and *Get Bulk Status* endpoints; - Combined descriptions of *Get Payment Status v1.1* into one paragraph; - Updated error information.
1.11	2022-01-20	- Added *Get Recurring Payment Status* v1.1.
1.12	2022-02-28	- Added *Cancel Bulk Payment.*
1.13	2022-03-30	- Deleted v1.0 of the *Get Payment Status* endpoints for one-time direct, one-time agended, deferred and recurring payments. - Updated support of bulk payments with debit postings for each individual payment within a batch (i.e. ‘batch booking parameter = false’). - Added withdrawal of future dated batches by the PSU.
1.14	2022-05-05	- Add error code for unknown payment id.

1.15	2023-04-20	- Add endToEndIdentification and remittanceInformationUnstructured to getPayment response body. - Update datatypes for X-Request-ID.
1.16	2023-09-28	- Added SEPA Direct Debit services.

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 PIS (Payment Initiation Service) interface offered by de Volksbank under PSD2. It explains the process of the consent a PSU (Payment Service User) must give to allow a TPP (Third Party Provider), in its role of PISP (Payment Initiation Service Provider), to submit a payment debiting the PSU's account or, in case of a SEPA Direct Debit, to submit a payment crediting the PSU's business account.

It should be noted that this interface:

- complies with Berlin Group standards (NextGenPSD2 XS2A Framework Implementation Guidelines V1.3);
- supports the initiation of a single SEPA Credit Transfer (SCT) as well as the upload of bulk SCT payments and SEPA Direct Debits.

The remainder of this document will be organized as follows:

- Chapter 2 describes the conditions de Volksbank applies to the use of its payment initiation services, the character set used for the payment information to be exchanged between the PISP and de Volksbank in its role of ASPSP, the datatypes defined for the individual pieces of information and the URLs to be used by the PISPs for the different brands of de Volksbank.
- Chapter 3 sheds some light on the requirements PISPs must meet to access the systems controlled by de Volksbank.
- Chapter 4 not only lays out the fine details of the Berlin Group payment initiation flow, but also describes some payment initiation services specific to de Volksbank.

2 Payment Initiation Services offered by de Volksbank

2.1 Conditions on the use of de Volksbank's payment initiation services

De Volksbank offers seven payment services:

1. One-time direct payments. This payment service is referred to as *payments* by the Berlin Group (POST /v1/payments/{payment-product});
2. One-time agended payments. This payment service is referred to as *future dated payments* by the Berlin Group;
3. Deferred payments. In contrast to the Berlin Group requirements, the scheduling of deferred payments lies with the PISPs. With respect to the data structure and most of the process steps, the deferred payment of de Volksbank complies with the Berlin Group standard;
4. Recurring payments. In contrast to the Berlin Group requirements, the scheduling of recurring payments lies with the PISPs. With respect to the data structure and most of the process steps, the recurring payment of de Volksbank complies with the Berlin Group standard.
5. Periodic payments. This payment service is referred to as *periodic payments* by the Berlin Group also.
6. Bulk SCT payments. This payment type is known as *bulk payments* by the Berlin Group.
7. SEPA Direct Debits. This is a de Volksbank implementation and not described by the Berlin Group.

The following conditions apply to the usage of all of these payment initiation 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 **90** days.

These services also have their own specific requirements which must be met by the PISP. They are listed below per specific payment service:

One-time direct payments

1. A one-time direct payment cannot be cancelled by neither the PISP nor the PSU.
2. A one-time direct payment never has an *endDate* in the request body.
3. A one-time direct payment cannot be re-submitted by the PISP with the same paymentId, even if the payment request cannot be processed by the ASPSP for technical reasons or because of insufficient balance.

One-time agended payments

1. A one-time agended payment can be cancelled by the PISP using the cancel payment endpoint.
2. A one-time agended payment never has an *endDate* in the request body; endDate is only used for deferred and recurring payments.

3. A one-time agended payment must have a *requestedExecutionDate* in the request body.
4. The ASPSP is responsible for the execution of the payment on the indicated date.
5. The PSU (customer) can withdraw the permission for the execution of the payment up to the date as recorded in the attribute *requestedExecutionDate* in the original payment request.
6. Withdrawal of the permission by the PSU can only be done in the online banking environment of the ASPSP.

Deferred payments

1. The execution date for a deferred payment as recorded in the mandatory attribute *endDate* cannot be after 13 months counted from and including the month where the payment request was received by the ASPSP and replied to with the status *RCVD* (RCVD means *received*).
2. The PISP (not the ASPSP) is responsible for the submission of a deferred payment for execution;
3. The PSU (customer) can withdraw the permission for the execution of a deferred payment up to and including the date as recorded in the attribute *endDate* in the original payment request.
4. Withdrawal of the permission by the PSU can only be done in the online banking environment of the ASPSP.
5. The permission to execute a deferred payment expires automatically after the date as recorded in the attribute *endDate*.
6. The PISP can offer a deferred payment for execution before the date as recorded in the *endDate* in the original payment request.
7. A deferred payment can only be submitted once by the PISP with the same paymentId, even if the payment request cannot be processed by the ASPSP for technical reasons or because of insufficient balance.

Recurring payments

1. A recurring payment can be delivered with the attribute *endDate* filled with a date, or without the attribute *endDate*. In the latter case we are dealing with an *infinite* or *perpetual* recurring payment.
2. In a series of recurring payments, the PISP (not the ASPSP) is responsible for submitting every individual payment for execution by the ASPSP.
3. A PISP can only submit one recurring payment for execution by the ASPSP per week, provided that the execution of the payment is successful.
4. If submission or execution of an individual payment in a series of recurring payments fails, the PISP is allowed to re-submit the payment for a period of 7 calendar days with a maximum of one attempt per calendar day.
5. The PSU is entitled to withdraw the permission for a series of recurring payments up to and including the date as recorded in the attribute *endDate* delivered in the original payment request.
6. The PSU is entitled to withdraw the permission for a series of recurring payments lacking an *endDate* at any moment.
7. Withdrawal of a permission can only be done in the online banking environment of the ASPSP.

8. The permission for the execution of a series of recurring payments expires automatically on the date as recorded in the attribute *endDate* delivered in the original payment request.
9. A PSU is allowed to view individual payments in a series of recurring payments, even if the permission has been withdrawn.

Periodic payments

1. A periodic payment can be delivered with the attribute *endDate* filled with a date, or without the attribute *endDate*. In the latter case we are dealing with an *infinite* or *perpetual* periodic payment.
2. Withdrawal of a permission can only be done in the online banking environment of the ASPSP;
3. A periodic payment must have a frequency in the request body.
4. The permission for the execution of a series of periodic payments expires automatically on the date as recorded in the attribute *endDate* delivered in the original payment request.
5. The ASPSP is responsible for the execution of the periodic payments.
6. The PSU is entitled to withdraw the permission for a series of periodic payments up to and including the date as recorded in the attribute *endDate* delivered in the original payment request.
7. The PSU is entitled to withdraw the permission for a series of periodic payments lacking an *endDate* at any moment.

Bulk payments

1. *Bulk/batch payments is only supported for SNS and RegioBank business customers. This is also the case in our direct online channels and conform our account product conditions.*
2. A bulk payment request must follow the XML pain.001.001.03 file format. We check against the XSD of EPC, 2021 version: https://www.europeanpaymentscouncil.eu/document-library/implementation-guidelines/sepa-credit-transfer-scheme-customer-psp-implementation.
3. Multiple batches (with a requested execution date) in one XML file is supported.
4. Both batch posting (compressed debit entry by batch) and bulk payment processing with debit entries for each individual payment within a batch (i.e. ‘batch posting parameter = false’) are supported.
5. SCA redirect conditions:
   a. Digipass or Mobile Banking app as SCA token are supported;
   b. We check against the agreed business client’s account signing limits. Multiple SCA signing (signing of batches by more than 1 person) is currently not supported;
   c. Single SCA is supported as long as all batches in the file are signed/approved by our business customer. If one or more batches in a file are not signed/approved we request the customer to do a new and as such a second SCA signing;
   d. All unsigned batches will automatically be cancelled. Please note, the customer is warned about this in our redirect screens.
6. A bulk payment can be cancelled by the PISP using the cancel payment endpoint.

The PSU is entitled to withdraw a batch with an execution date in the future. Withdrawal can be done in the online banking environment of the ASPSP.

SEPA Direct Debits

1. *The SEPA Direct Debit (SDD) initiation service is only supported for SNS and RegioBank business customers. This is also the case in our direct online channels and conform our account product conditions.*
   Please note that:
   - De Volksbank only supports Core SDD and not B2B SDD initiation services;
   - For SDD initiation services the PSU (business customer) needs to have a separate SDD Core contract with SNS Bank or RegioBank. The terms and conditions ('voorwaarden') mentioned in this contract also apply for this API service. This contract describes agreements like:
     - The applicable Creditor account (IBAN), Creditor Name and Creditor Scheme ID. These have to be used in the pain.008 file !
     - Limits: the maximum number of batches in a predefined period, maximum amount of a batch, maximum number of direct debits within a batch and maximum amount of a direct debit.
     - The way the pain.008 has to be delivered. In this case it must always be 'via the bank' (Mijn SNS Zakelijk or RegioBank Zakelijk Internetbankieren) and the terms and conditions (like ultimate delivery timelines) mentioned in the SDD Core contract also apply for this way of delivery.

   If a SDD file is initiated and it contains not SDD Core or the business customer has for his credit creditor account (IBAN) no contract the file is rejected with reason code AC01.
2. A SEPA Direct Debit request must follow the XML pain.008.001.02 file format. We check against the XSD of ISO 20022, 2009 version (pain.008.001.02) and according to EPC planning from the 19th of November 2023 onwards also the 2019 version (pain.008.001.08). These can be found in the ISO 20022 Message Archive: https://www.iso20022.org/catalogue-messages/iso-20022-messages-archive.
3. Multiple SEPA Direct Debit batches in one XML file is supported.
4. SCA redirect conditions:
   a. Digipass or Mobile Banking app as SCA token are supported;
   b. Once uploaded, the XML file cannot be altered. All SEPA Direct Debit batches present in the XML will be submitted.
5. A SEPA Direct Debit cannot be cancelled by the PISP. If a business customer want to cancel/revoke a SDD batch (before settlement) of reverse/recall a SDD batch (after settlement) the customer has to contact his bank as mentioned in the terms and conditions in his SDD Core contract.
6. Early delivery of SDD batches is supported (till 99 days before the requested SDD collection due date). Also late delivery until 4 calendar days after the requested SDD collection is due is supported.

In that case the requested SDD collection due date is adjusted by the bank to 1 target day before the day of delivery.

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

Most APIs as defined by de Volksbank 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.

Note that the bulk payment initiation call expects a pain.001 XML structure, and the SEPA Direct Debit a pain.008 XML structure.

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 to start the PSU's SCA and approval process:
  - for TPPs in the role of PISP to start the approval 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 PISP to redeem a one-off authorization code or a recurring refresh token 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

Attention:

Known Android problem

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

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

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

3 Access

The PISP can only use the PSD2 APIs as authorized by de Volksbank. The PISP must be registered with the Competent Authority with a license to perform payment initiation services (refer to payment service 7 as described in Annex of the Payment Services Directive (2015/2366),
PISPs 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 payment initiation request, the subsequent authorization request and token exchange request to the appropriate address of the PISP.

3.1 Certificates

The connections between the TPP and de Volksbank endpoints are secured by a mutual TLS authentication, as required by 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 can subsequently be used in each PSD2 API service, but only once.

4 The APIs for submitting a payment request on behalf of a PSU

The PISPs must[1] use the following APIs for initiating and executing a payment request:

1. Payment initiation request with JSON encoding, or XML for bulk payments and SEPA Direct Debits;

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

4. Access token request: access token and refresh token based on an authorization code;
5. New access token request: new access and refresh tokens based on a refresh token;
6. Get transaction status request v1.1 for **one-time direct**, **one-time agended, deferred, recurring** and **bulk payments**, and for **SEPA Direct Debits**;
7. Payment execution request for **deferred** and **recurring payments**;
8. Get payment request to retrieve the payment details for all authorized payment types, including the debtor account and the name of the holder(s) of this account;
9. Cancel payment request for **one-time agended payments** and **bulk payments**;
10. Get payment status report for **SEPA Direct Debits**.

Please note that endpoints 7 (payment execution request for deferred/recurring payments) and 8 (get payment details for all payment types) are published on our Developer Portal as one API Swagger file, named "<Brand name> Manage Payments Services". The SEPA Direct Debit endpoints are published on our Developer Portal as separate APIs (one for initiating and retrieving the status, and one for retrieving the payment status report).

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.

[1] The APIs 6, 8, 9 and 10 are optional: a PISP can use these APIs to get information about the status of an executed payment, payment details or to cancel a payment.

4.1 Payment initiation request

By issuing a payment initiation request, the PISP seeks permission from an ASPSP to submit a payment debiting the account a PSU is holding with the addressed ASPSP on behalf of that PSU.

In the sub-sections to come, we will discuss at length the parts which make up the payment initiation endpoint.

4.1.1 Method and URL

Method	URL	Description
POST	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/payments/{payment-product}	Payment initiation endpoint for **one-time direct payments** and **one-time agended payments** as defined by the Berlin Group in the implementation guide version 1.3.
POST	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/deferred-payments/{payment-product}	Volksbank-specific payment initiation endpoint for **deferred payments** with a make-up conform to the structure as laid down by the Berlin Group in the implementation guide version 1.3.
POST	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/recurring-payments/{payment-product}	Volksbank-specific payment initiation endpoint for **recurring payments** with a make-up conform to the structure as laid down by the Berlin Group in the implementation guide version 1.3.
POST	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/periodic-payments /{payment-product}	Payment initiation endpoint for **periodic payments** as defined by the Berlin Group in the implementation guide version 1.3.
POST	https://psd.bancairediensten.nl/psd2/[snsbank|regiobank]/v1/bulk-payments/{payment-product}	Payment initiation endpoint for **bulk payments** and **SEPA Direct Debits** as defined by the Berlin Group in the implementation guide version 1.3.

4.1.2 Path parameters

Attribute	Type	Mandatory	Description
payment-product	String	Y	The attribute refers to the payment product associated with the credit transfer payment method. The Berlin Group distinguishes the following payment products for JSON-based calls: 1. sepa-credit-transfers; 2. instant-sepa-credit-transfers; 3. target-2-payments; 4. cross-border-credit-transfers. It is up to the ASPSP to decide which of these payment products it supports. At the moment, de Volksbank only supports the following product: 1. sepa-credit-transfers.[2] For bulk payments, de Volksbank supports the product pain.001-sepa-credit-transfers. For SEPA Direct Debits, use the product pain.008-sepa-direct-debits

4.1.3 Query parameters

The payment initiation endpoint does not have any query parameters.

4.1.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute invariably filled with the value "*application/json*", except for bulk payments. For **bulk payments** and **SEPA Direct Debits** this attribute should be filled with the value “*application/xml*”.
X-Request-ID	UUID	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the PISP).
Authorization	String	Y	Attribute consists of *client_id:* identification of the PISP as registered with de Volksbank.
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.

[2] De Volksbank processes sepa-credit-transfers instantly, provided that the bank of the creditor is reachable for instant payments. So, there is no difference in the settlement of these payments with the processing via our PSU interfaces.

4.1.5 Request body

Below attributes are for all payment types except bulk payments and SEPA Direct Debits. For bulk payments the request body is a pain.001 structure corresponding to the SCT schema urn:iso:std:iso:20022:tech:xsd:pain.001.001.03. For SEPA Direct Debits the request body is a pain.008 structure corresponding to the SDD schema urn:iso:std:iso:20022:tech:xsd:pain.008.001.02.

Attribute	Type	Mandatory	Description
endToEndIdentification	String	N	Attribute filled with the unique identification of the payment request as provided by the PISP. Max35Text The attribute *endToEndIdentification* is not allowed for **periodic payments.**
debtorAccount iban currency	Account Reference Object String String	N N N	iban: Attribute *iban* is part of the object *Account Reference* as defined by the Berlin Group. ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}. currency: Attribute *currency* is part of the object *Account Reference* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code. Should be EUR.
instructedAmount currency amount	Amount Object String String	Y Y Y	currency: Attribute *currency* is part of the object *Amount* as defined by the Berlin Group. Should be EUR. ISO 4217 Alpha 3 currency code. amount: Attribute *amount* is part of the object *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.
creditorAccount iban currency	Account Reference Object String String	Y Y N	iban: Attribute *iban* is part of the object *Account Reference* as defined by the Berlin Group. ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}. currency: Attribute *currency* is part of the object *Account Reference* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code.
creditorAgent	String	N	Attribute filled with a BIC. ISO 20022 definition BIC: [A-Z]{6,6}[A-Z2-9][A-NP-Z0-9]([A-Z0-9]{3,3}){0,1}.
creditorName	String	Y	Party to which an amount of money is due. Max70Text.

Attribute	Type	Mandatory	Description
ultimateCreditor	String	N	Ultimate party to which an amount of money is due. Max70Text. The attribute *ultimateCreditor* is not allowed for **periodic payments.** This attribute is optional. Nevertheless it is highly recommended to provide this information in case the TPP is acting as Collecting Service Provider. The TPP is temporarily in the possession of the collected funds (after the initiated payment is executed and settled) and transfers the collected funds from his "escrow" creditor account to the ultimate receiver/creditor account.
ultimateCreditorId	String	N	The attribute *ultimateCreditorId* is de Volksbank-specific attribute *ultimate_receiver_id*. The attribute *ultimateCreditorId* is not on the list of attributes as defined by the Berlin Group. Max35Text. The attribute *ultimateCreditorId* is not allowed for **periodic payments.** This attribute is optional. Nevertheless it is highly recommended to provide this information in case the TPP is acting as Collecting Service Provider.
remittanceInformationUnstructured	String	N	Max140Text. remittanceInformationUnstructured and remittanceInformationStructured attributes are mutually exclusive in accordance with the EPC rule stating that "*Either 'Structured' or 'Unstructured' may be present".*
remittanceInformationStructured	String	N	Remittance information according to the list of Currence ("CUR") or ISO-20022 ("ISO"). Max35Text. remittanceInformationUnstructured and remittanceInformationStructured attributes are mutually exclusive in accordance with the EPC rule stating that "*Either 'Structured' or 'Unstructured' may be present".*

Attribute	Type	Mandatory	Description
issuerSRI	String	N	The attribute *issuerSRI* is a Volksbank-specific attribute required whenever the attribute *remittanceInformationStructured* is used. The attribute *issuerSRI* is not on the list of attributes as defined by the Berlin Group. It can, for instance, have the following values: • CUR; • ISO. Max35Text.
endDate	String	N	The attribute *endDate* is not allowed with payments of the payment service **one-time direct** and **one-time agended payments**. The attribute *endDate* is mandatory for payments of the payment service **deferred payments**. The *endDate* marks the ultimate date on which the PISP can submit a payment for execution by the ASPSP. For deferred payments, the endDate should not be more than 13 months in the future. The attribute *endDate* is optional for payments of the payment service **recurring payments** and **periodic payments**, because de Volksbank also allows for recurring and periodic payments with no end date, the so-called infinite or perpetual recurring or periodic payments. If the *endDate* is filled, it is the last date where the PISP can submit a payment in a series of payments for execution by the ASPSP. Attribute *endDate* has the ISO 8601 Date format (YYYY-MM-DD).

Attribute	Type	Mandatory	Description
requestedExecutionDate	String	N	The attribute *requestedExecutionDate* is not allowed with payments of the payment service **deferred**, **recurring and periodic payments**. The attribute *requestedEndDate* is mandatory for **one-time agended payments**. Attribute *requestedEndDate* has the ISO 8601 Date format (YYYY-MM-DD). The date cannot be in the past or more than 10 years in the future. If the date is today's date, the payment will be executed as a **one-time direct payment**; for a date in the future the ASPSP will execute the payment on that date.
startDate	String	N	The attribute *startDate* is only allowed for **periodic payments**. The attribute *startDate* is mandatory for **periodic payments.** Attribute *startDate* has the ISO 8601 Date format (YYYY-MM-DD). The date cannot be today, in the past or more than one year from now.
executionRule	String	N	The attribute *executionRule* is only allowed for **periodic payments.** De Volksbank only supports the value following.
frequency	String	Y	The attribute *frequency* is only allowed for **periodic payments**. The attribute *frequency* is mandatory for **periodic payments.** The following codes from the EventFrequency7Code of ISO 20022 are supported: Weekly, EveryFourWeeks, Monthly, Quarterly, SemiAnnual, Annual
dayOfExecution	String	N	The format is following the regular expression \d{1,2}. Example: the first day is addressed by "1". The date is referring to the timezone of the ASPSP. The attribute *dayOfExecution* is not used.

4.1.6 Examples payment initiation request

The payment initiation request is illustrated below. We give two examples: one for a JSON-based payment initiation and one for a pain.001 XML-based payment initiation.

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v1/deferred-payments/sepa-credit-transfers

Content-Type: application/json

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Authorization: l72b095e702f4042e881384c746532defe

PSU-IP-Address: 192.168.8.78

{

   "endToEndIdentification": "ID234567",

   "debtorAccount": {"iban": "NL64MAART0948305290", "currency": "EUR"},

   "instructedAmount": {"currency": "EUR", "amount": "123.50"},

   "creditorAccount": {"iban": "NL55WIND0000012345", "currency": "EUR"},

   "creditorAgent": "WINDNL2A",

   "creditorName": "Adyen",

   "ultimateCreditor": "Krentebol dot com",

   "ultimateCreditorId": "1234",

   "remittanceInformationStructured": "1234 5678 9012 3456",

   "issuerSRI": "CUR",

   "endDate": "2099-01-01"

 }


POST https://psd.bancairediensten.nl/psd2/snsbank/v1/bulk-payments/pain.001-sepa-credit-transfers

Content-Type: application/xml

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Authorization: l72b095e702f4042e881384c746532defe

PSU-IP-Address: 192.168.8.78

<?xml version="1.0" encoding="utf-8"?>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pain.001.001.03"
xsi:schemaLocation="urn:iso:std:iso:20022:tech:xsd:pain.001.001.03
schema.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <CstmrCdtTrfInitn>
        <GrpHdr>
            <MsgId>msgid</MsgId>
            <CreDtTm>2002-07-06T06:34:11.85</CreDtTm>
            <NbOfTxs>1</NbOfTxs>
            <CtrlSum>3.00</CtrlSum>
            <InitgPty />
        </GrpHdr>
        <PmtInf>
            <PmtInfId>batchId1</PmtInfId>
            <PmtMtd>TRF</PmtMtd>
            <NbOfTxs>1</NbOfTxs>
            <CtrlSum>3.00</CtrlSum>
            <ReqdExctnDt>1973-08-09</ReqdExctnDt>
            <Dbtr>
                <Nm>SNS klant</Nm>
            </Dbtr>
            <DbtrAcct>
                <Id>
                    <IBAN>NL19SNSB0123426270</IBAN>
                </Id>
            </DbtrAcct>
            <DbtrAgt>
                <FinInstnId />
            </DbtrAgt>
            <CdtTrfTxInf>
                <PmtId>
                    <EndToEndId>eteid1</EndToEndId>
                </PmtId>
                <Amt>
                    <InstdAmt Ccy="IZR">3.00</InstdAmt>
                </Amt>
                <Cdtr>
                    <Nm>Anton</Nm>
                </Cdtr>
                <CdtrAcct>
                    <Id>
                        <IBAN>NL15ASNB0706723484</IBAN>
                    </Id>
                </CdtrAcct>
                <RmtInf>
                    <Strd>
                        <CdtrRefInf>
                            <Tp>
                                <CdOrPrtry>
                                    <Cd>SCOR</Cd>
                                </CdOrPrtry>
                                <Issr>CUR</Issr>
                            </Tp>
                            <Ref>9000007960551590</Ref>
                        </CdtrRefInf>
                    </Strd>
                </RmtInf>
            </CdtTrfTxInf>
        </PmtInf>
    </CstmrCdtTrfInitn>
</Document>
```

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 PISP).
ASPSP-SCA-Approach	String	Y	Attribute invariably filled with the value "*REDIRECT*".

4.1.9 Response body

Attribute	Type	Mandatory	Description
transactionStatus	String	Y	Value of the attribute is conform with the ISO 20022 **ExternalPaymentTransactionStatus1Code** list. Enumeration: RCVD (*RCVD* means received).
paymentId	String	Y	Max16Text. **N.B.**: ▪ relationship paymentId - one time direct or agended payment is 1:1; ▪ relationship paymentId - deferred payment is 1:1; ▪ relationship paymentId – recurring payment is 1:n; ▪ relationship paymentId – periodic payment is 1:n. This means that the paymentId cannot be used as correlation ID for individual transactions in a series of payments of the type recurring and periodic payments.
_links	Links	Y	**Remark:** 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. "**status**": the link to retrieve the transaction status of the payment initiation.

Note: if a bulk payment file (pain.001) or SEPA Direct Debit file (pain.008) is rejected it is possible that you receive additional error information. Please refer to paragraph 4.11.2.

4.1.10 Example payment initiation response

The payment initiation response is illustrated below:

```
HTTP/1.x 201 Created
Content-Type:       application/json
Location:
https://psd.bancairediensten.nl/psd2/snsbank/v1/payments/SNS0123456789012
```

```
X-Request-ID:       99391c7e-ad88-49ec-a2ad-99ddcb1f7756
ASPSP-SCA-Approach: REDIRECT
{
   "transactionStatus": "RCVD",
   "paymentId": "SNS0123456789012",
   "_links": {
      "scaOAuth": {"href": "
https://psd.bancairediensten.nl/psd2/snsbank/v1/authorize
"},
      "status": {"href": "/v1.1/payments/sepa-credit-
transfers/SNS0123456789012/status"}
   }
}
```

4.2 Authorize request

The PISP 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 execute the payment submitted by the PISP.

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 "*PIS*".
state	String	Y	Attribute contains the unique identification of the request issued by the PISP. The Berlin Group calls this attribute *X-Request-ID*.

Attribute	Type	Mandatory	Description
paymentId	String	Y	Attribute hosts the unique identification assigned by the ASPSP to the payment, when the initiation request was sent in by the PISP.
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*".
Authorization	String	Y	Attribute consists of *client_id:* identification of the PISP as registered with de Volksbank.

4.2.5 Request body

The authorize endpoint does not have a request body.

4.2.6 Example authorize request

The authorize request is illustrated below:

```
GET
https://psd.bancairediensten.nl/psd2/snsbank/v1/authorize?response_type=c
ode&scope=PIS&state=111111&paymentId=SNS0000123456789redirect_uri=https:/
/thirdparty.com/callback&client_id=<client_id>

Content-Type: application/x-www-form-urlencoded

Authorization: l72b095e702f4042e881384c746532defe
```

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 payment 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 PISP's request to execute the payment. In case of success, the service returns an authorization code and redirects the user-agent to the application defined by the 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, that 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	Attribute filled with the value which the PISP has delivered in the attribute **state** in the Authorize request.

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

4.3.3 Example authorization response

The authorization response is illustrated below:

```
HTTP/1.x 302
```

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

4.4 Access token request

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

4.4.1 Method and URL

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

4.4.2 Path parameters

The token endpoint does not have any path parameters.

4.4.3 Query parameters

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

4.4.4 Request header

Attribute	Type	Mandatory	Description
Content-Type	String	Y	Attribute invariably filled with the value "*application/x-www-form-urlencoded*".
X-Request-ID	UUID	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the PISP).
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 PISP as registered with de Volksbank; – client_secret: secret agreed between the PISP and de Volksbank.

4.4.5 Request body

The token endpoint does not have a request body.

4.4.6 Example token request

The token request is illustrated below:

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

4.4.7 Response code

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

Code	Description
200	Ok

4.4.8 Response header

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

4.4.9 Response body

Attribute	Type	Mandatory	Description
access_token	String	Y	Attribute filled with the access token needed to call the PSD2 interface, in this case PIS.
token_type	String	Y	Attribute invariably 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 “*PIS*”.

4.4.10 Example token response

The token response is illustrated below:

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

At this point, the PISP has been authorized. It is allowed to use the token until the token expires or is revoked. A refresh token may be used to request new access tokens, if the original token has expired.

4.5 New access token request

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

4.5.1 Method and URL

Method	URL	Description
POST	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/token?	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 fixed value “*refresh_code*”; defines the OAuth2 flow.
refresh_token	String	Y	Refresh token 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 PISP).

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 PISP as registered with de Volksbank; – client_secret: secret agreed between the PISP and de Volksbank.

4.5.5 Request body

The token endpoint does not have a request body.

4.5.6 Example token request

The token request is illustrated below:

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

4.5.7 Response code

If the authorization is valid, the ASPSP will return a response containing the access token (and optionally, 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 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 PSD2 interface, in this case PIS.
token_type	String	Y	Attribute invariably filled with the fixed value “*Bearer*”.
expires_in	Number	Y	Attribute filled with the lifetime in seconds of the access token.
refresh_token	String	Y	Value of the attribute can be used to obtain a new access token using the same authorization grant in the situation where the current token has expired.

scope	String	Y	Attribute filled the scope of the access token. In this context “*PIS*”.

4.5.10 Example token response

The token response is illustrated below:

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

Now, the PISP has been authorized again.

4.6 Get transaction status request v1.1

This section describes the endpoint for retrieving the transaction status of a one-time direct, one-time agended, deferred, recurring and bulk payment as well as the status of a SEPA Direct Debit.

After the PSU’s approval of the payment, the PISP can retrieve its most recent status by submitting a transaction status request.

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

4.6.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1.1/payments/sepa-credit-transfers/{payment-id}/status	Transaction status request endpoint for the payment services **one-time direct payments** and **one-time agended payments** as defined by the Berlin Group in the implementation guide version 1.3.
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1.1/deferred-payments/sepa-credit-transfers/{payment-id}/status	Transaction status request endpoint for the de Volksbank-specific payment service **deferred payments**.
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1.1/recurring-payments/sepa-credit-transfers/{payment-id}/status	Transaction status request endpoint for the de Volksbank-specific payment service **recurring payments**.

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/ [snsbank|regiobank]/v1.1/bulk-payments/pain.001-sepa-credit-transfers/{payment-id}/status	Transaction status request endpoint for the payment service **bulk payments** as defined by the Berlin Group in the implementation guide version 1.3.
GET	https://psd.bancairediensten.nl/psd2/ [snsbank| regiobank]/v1/bulk-payments/pain.008-sepa-direct-debits /{payment-id}/status	Transaction status request endpoint for the SEPA Direct Debit service, following the status request format as defined by the Berlin Group in the implementation guide version 1.3.

4.6.2 Path Parameters

Attribute	Type	Mandatory	Description
payment-id	String	Y	Attribute hosts the unique identification assigned by the ASPSP to the payment, when the initiation request was sent in by the PISP.

4.6.3 Query Parameters

The transaction status request endpoint does not have any query parameters.

4.6.4 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 PISP).
Authorization	String	Y	Attribute consists of *client_id*: identification of the PISP as registered with de Volksbank.

4.6.5 Request body

The transaction status request endpoint does not have a request body.

4.6.6 Example transaction status request

The transaction status request is illustrated below:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1.1/payments/sepa-credit-transfers/SNS0123456789012/status

Content-Type: application/json

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Authorization: l72b095e702f4042e881384c746532defe
```

4.6.7 Response code

Code	Description
200	Ok

4.6.8 Response 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 PISP).

4.6.9 Response body

Below you can find the response body in case of JSON-based payment initiation calls (all types except bulk payments and SEPA Direct Debits), followed by the response body in case of XML-based payment initiation calls (bulk payments and SEPA Direct Debits).

Note: for recurring payments, several payments can be executed by the PISP. This endpoint returns the status of the **latest** executed payment, or the status of the payment mandate when no executions have taken place yet.

Attribute	Type	Mandatory	Description
transactionStatus	String	Y	Value of the attribute is conform to the ISO 20022 **ExternalPaymentTransactionStatus1Code** list. Enumeration: - ACSC (accepted settlement completed, Settlement on the debtor's account has been completed) This status holds for the **non-instant** execution of a one-time direct, one-time agended, deferred or recurring payment. - ACCC (accepted settlement completed, Settlement on the creditor's account has been completed) This status holds for the **instant** execution of a one-time direct, one-time agended, deferred or recurring payment. - RCVD (received) Payment has been initiated but not signed. This status indicates that one of the following situations has occurred: - The payment initiation is received and the redirect SCA Authorization call is not yet issued/requested by the TPP; - During the SCA redirect the PSU closed the browser; - During the SCA redirect it appeared that the selected debtor account is not an online payment account or the PSU is not authorized to use this account for payment initiation; - The SCA daily token limit is exceeded. - RJCT (rejected) The execution of the payment is rejected by the bank (payment account is blocked, insufficient

Attribute	Type	Mandatory	Description
			funds, fraud detection), or is timed out during the redirect SCA Authorization call. Or, in case of a **deferred or recurring payment**, the payment may be expired (endDate has gone by before the payment was executed by the TPP). - ACSP (accepted settlement in process) All preceding checks such as technical validation and customer profile were successful and therefore the payment initiation has been accepted for execution. This status holds for a **one-time agended payment** of which the requestedExecutionDate is in the future (the payment has been scheduled but not executed yet), and for an approved **deferred payment** that has not been executed yet. - ACCP (accepted customer profile) Payment is accepted/completely signed and ready for the settlement process. This status is returned when a **recurring payment** has been signed and approved, but the PISP has not yet executed a payment under the payment mandate. If a payment has been executed then the status of the latest executed payment will be returned. - CANC (cancelled) The payment has been cancelled. This status indicates that one of the following situations has occurred: - A **one-time agended** payment has been cancelled by the PISP with a Cancel Payment request (see section 4.9); - The PSU cancelled the **one-time direct**, **one-time agended, deferred or recurring payment** during redirect SCA; - A **one-time agended, deferred or recurring** payment has been cancelled by the PSU in his/her online banking application of one of the brands of de Volksbank. Note for **recurring**: when a payment has already been executed before the PSU cancelled the payment mandate, the status of the latest executed payment will be returned.

Response body in case of an XML-based payment initiation request (for bulk payments and SEPA Direct Debits):

Attribute	Type	Mandatory	Description
originalMessageIdentification	String	Y	Point to point reference, as assigned by the original initiating party, to unambiguously identify the original mandate request message.

Attribute	Type	Mandatory	Description
groupStatus	String	N	Value of the attribute is conform to the ISO 20022 standard. **ExternalPaymentTransaction Status1Code** list. Enumeration: - RCVD - ACTC - ACCP - ACSP - ACSC - RJCT - CANC - PART[3]

[3] PART is used when a pain file has more batches and these batches have different end statuses. Or in case of 'batch booking parameter = false' the individual payment transactions in a batch have different end statuses.

statusReasonInformation	String	N	Additional reason information for a specific status conform ISO20022 standard. Enumeration: - AC01 - AC02 - AC03 - AC04 - AC06 - AG01 (transaction forbidden on this type of account) - AG02 (incorrect operation code / SDD sequence type) - AM02 - AM04 - AM05 - AM16 - AM17 - AM19 - AM20 - CH03 - CH04 - CNOR (SCT Creditor bank not reachable) - DNOR (SDD Debor bank not reachable) - DS0H - DU01 - DU02 - FF01 - MD01 (SDD Core no mandate) - MD02 - MD07 - MS02 (SDD refusal by debtor) - MS03 - RC01 (invalid BIC) - RR01 (missing debtor account) - RR02 (missing debtor name or address) - RR03 (missing creditor name or address) - RR04 (general regulatory reason) - SL01 (SDD black-/whitelisting) Proprietary SDD reject reason codes: - EQ01: Maximum number of rejected transactions exceeded. - EQ04: The creditor scheme ID is not registered for customer. - EQ05: The creditor scheme ID is not registered for account of customer.

Attribute	Type	Mandatory	Description
downloadPain002Urls	Array of Strings	N	Relative URL to where the pain002 can be downloaded with more details on the status (when one or more pain.002 files are present). Only for **SEPA Direct Debits**. See also section 4.10. Relative URL follows format: "/v1/bulk-payments/pain.008-sepa-direct-debits/{payment-id}/payment-status-reports/{payment-status-report-id} "

Attribute	Type	Mandatory	Description
originalPaymentsInformationAndStatus Array contains:	Array	Y	A list of original payments including payment information.
originalPaymentInformationIdentification	String	Y	Unique identification, as assigned by the original sending party, to unambiguously identify the original payment information group i.e. Batch id.
paymentInformationStatus	String	N	Value of the attribute is conform to the ISO 20022 standard. See for possible values 'Groupstatus' earlier in this table.
statusReasonInformation	String	N	Additional reason information for a specific status conform ISO20022 standard. See for possible values 'statusReasonInformation' earlier in this table.
transactionsInformationAndStatus Array contains:	Array	N	List of transactions including detailed information.
originalInstructionIdentification	String	N	Unique identification, as assigned by the original instructing party for the original instructed party, to unambiguously identify the original instruction.
originalEndToEndIdentification	String	N	Unique identification, as assigned by the original initiating party, to unambiguously identify the original transaction.
transactionStatus	String	N	Value of the attribute is conform to the ISO 20022 standard. See for possible values 'Groupstatus' earlier in this table.
statusReasonInformation	String	N	Additional reason information for a specific status conform ISO20022 standard. See for possible value 'statusReasonInformation' earlier in this table

4.6.10 Example transaction status response

The transaction status response is illustrated below. We give two examples: one for a JSON-based initiated payment and one for a pain.001 XML-based initiated payment.

```
HTTP/1.x 200 OK

Content-Type:       application/json
X-Request-ID:       99391c7e-ad88-49ec-a2ad-99ddcb1f7721

{

   "transactionStatus": "ACSC"

}


HTTP/1.x 200 OK

Content-Type:       application/json
X-Request-ID:       99391c7e-ad88-49ec-a2ad-99ddcb1f7721

{
  "originalMessageIdentification": "MIPI-123456789RI-123456789",
  "groupStatus": "RJCT",
  "statusReasonInformation": "AM04",
  "originalPaymentsInformationAndStatus": [
    {
      "originalPaymentInformationIdentification": "BIPI-123456789RI-
123456789",
      "paymentInformationStatus": "RJCT",
      "statusReasonInformation": "AM04",
      "transactionsInformationAndStatus": [
        {
          "originalInstructionIdentification":
"INNDNL2U20101004000042800000011",
          "originalEndToEndIdentification": "RCUR-0-40239498-369-2018-12-
03",
          "transactionStatus": "RJCT",
          "statusReasonInformation": "AM04"
        }
      ]
    }
  ]
}
```

4.7 Payment execution request

The approval of payments of the type deferred payments and recurring payments and the subsequent execution of these payments is a disjunct process in the sense that the execution is done in a separate service call. By issuing a payment execution request, the PISP explicitly requests the ASPSP to process the submitted credit transfer payment for which the PSU has given approval.

In the sub-sections to come, we will discuss at length the parts which make up the payment execution endpoint.

4.7.1 Method and URL

Method	URL	Description
POST	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/{payment-service}/{payment-product}/{payment-id}	Payment execution endpoint for de Volksbank specific payment services **deferred payments** and **recurring payments**.

4.7.2 Path parameters

Attribute	Type	Mandatory	Description
payment-service	String	Y	Attribute refers to the type of payment service. For this particular endpoint, de Volksbank only supports the proprietary payments services **deferred payments** and **recurring payments**. Therefore, the enumeration is: 1. deferred-payments; 2. recurring-payments.
payment-product	String	Y	The attribute refers to the payment product associated with the credit transfer payment method. The Berlin Group distinguishes the following payment products: 1. sepa-credit-transfers; 2. instant-sepa-credit-transfers; 3. target-2-payments; 4. cross-border-credit-transfers. It is up the ASPSP to indicate which of these payment products it supports. At the moment, de Volksbank only supports the following product: 1. sepa-credit-transfers.[4]
payment-id	String	Y	Attribute hosts the unique identification assigned by the ASPSP to the payment, when the initiation request was sent in by the PISP.

[4] De Volksbank processes sepa-credit-transfers instantly, provided that the bank of the creditor is reachable for instant payments. So, there is no difference in the settlement of these payments with the processing via our PSU interfaces.

4.7.3 Query parameters

The payment execution request 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*".
X-Request-ID	UUID	Y	Attribute filled with the ID of the request, unique to the call, as determined by the initiating party (the PISP).
Authorization	String	Y	Attribute contains the access token acquired by the PISP as a result of calling the token endpoint.

4.7.5 Request body

Attribute	Type	Mandatory	Description
endToEndIdentification	String	N	Unique identification as provided by the PISP. Max35Text.
remittanceInformationUnstructured	String	N	Max140Text.
remittanceInformationStructured	String	N	Max35Text.
issuerSRI	String	N	The attribute *issuerSRI* is a Volksbank-specific attribute required whenever the attribute *remittanceInformationStructured* is used. The attribute *issuerSRI* is not on the list of attributes as defined by the Berlin Group. Max35Text.

4.7.6 Examples payment execution request

The payment execution request is illustrated below. We give two examples: one with a filled attribute *remittanceInformation**Structured*** and one with a filled attribute *remittanceInformation**Unstructured***. Both attributes are mutually exclusive in accordance with the EPC rule stating that "*Either 'Structured' or 'Unstructured' may be present*"

```
POST https://psd.bancairediensten.nl/psd2/snsbank/v1/recurring-
payments/sepa-credit-transfers/SNS0123456789012
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Authorization: Bearer "<ACCESS_TOKEN>"
{
   "endToEndIdentification": "ID234567",
   "remittance Information Structured": "1234 5678 9012 3456",
   "issuerSRI": "CUR"
 }


POST https://psd.bancairediensten.nl/psd2/snsbank/v1/recurring-
payments/sepa-credit-transfers/SNS0123456789012
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Authorization: Bearer "<ACCESS_TOKEN>"
{
   "endToEndIdentification": "ID234567",
   "remittanceInformationUnstructured": "payment for oodles of buns"
}
```

4.7.7 Response code

Code	Description
201	Created

4.7.8 Response 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 PISP).

4.7.9 Response body

Attribute	Type	Mandatory	Description
transactionStatus	String	Y	Value of the attribute is conform with the ISO 20022 **ExternalPaymentTransactionStatus1Code** list.
paymentId	String	Y	Max16Text. N.B.: ▪ relationship paymentId - one time or agended direct payment is 1:1; ▪ relationship paymentId - deferred payment is 1:1; ▪ relationship paymentId – recurring payment is 1:n. This means that the paymentId cannot be used as correlation id for individual transactions in a series of payments of the type recurring-payments.
resourceId	String	Y	Unique identification as assigned by the ASPSP to uniquely identify the payment execution resource.

4.7.10 Example payment execution response

The payment execution response is illustrated below:

```
HTTP/1.x 201 Created
Content-Type:    application/json
X-Request-ID:    99391c7e-ad88-49ec-a2ad-99ddcb1f7756
{
   "transactionStatus": "ACCC",
   "paymentId": "SNS0123456789012",
   "resourceId": "XYZ",
}
```

4.8 Get payment request

With the get payment endpoint, a PISP can request the payment details of an authorized payment.

4.8.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/payments/{payment-product}/{payment-id}	Get payment endpoint for **one-time direct payments** and **one-time agended payments** as defined by the Berlin Group in the implementation guide version 1.3.
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/deferred-payments/{payment-product}/{payment-id}	Volksbank-specific get payment endpoint for **deferred payments**.
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/recurring-payments/{payment-product}/{payment-id}	Volksbank-specific get payment endpoint for **recurring payments**.
GET	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/periodic-payments/{payment-product}/{payment-id}	Volksbank-specific get payment endpoint for **periodic payments**.

4.8.2 Path parameters

Attribute	Type	Mandatory	Description
payment-product	String	Y	The attribute refers to the payment product associated with the credit transfer payment method. The Berlin Group distinguishes the following payment products: 1. sepa-credit-transfers; 2. instant-sepa-credit-transfers; 3. target-2-payments; 4. cross-border-credit-transfers. It is up to the ASPSP to decide which of these payment products it supports. At the moment, de Volksbank only supports the following product: sepa-credit-transfers.[5]
payment-id	String	Y	Attribute contains the unique identification of the payment.

4.8.3 Query parameters

The get payment 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 PISP).
Authorization	String	Y	Attribute filled with the access-token as obtained in the token request call.

4.8.5 Request body

The get payment endpoint does not have a request body.

4.8.6 Example get payment request

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1/payments/sepa-credit-
transfers/SNS0289089808735

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

Authorization:      Bearer <ACCESS-TOKEN>
```

4.8.7 Response code

Code	Description
200	OK

[5] De Volksbank processes sepa-credit-transfers instantly, provided that the bank of the creditor is reachable for instant payments. So, there is no difference in the settlement of these payments with the processing via our PSU interfaces.

4.8.8 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.

4.8.9 Response body

Attribute	Type	Mandatory	Description
debtorAccount iban currency	Account Reference Object String String	Y Y N	iban: Attribute *iban* is part of the object *Account Reference* as defined by the Berlin Group. ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}. currency: Attribute *currency* is part of the object *Account Reference* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code.
debtorName	String	N	Attribute contains the name of the debtor(s). If an account has a joint account holder, the name of the account holder and joint account holder are separated with ' CJ '. Max144Text.
instructedAmount currency amount	Amount Object String String	Y Y Y	currency: Attribute *currency* is part of the object *Amount* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code. amount: Attribute *amount* is part of the object *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.
creditorAccount iban currency	Account Reference Object String String	Y Y N	iban: Attribute *iban* is part of the object *Account Reference* as defined by the Berlin Group. ISO 20022 pattern: [A-Z]{2,2}[0-9]{2,2}[a-zA-Z0-9]{1,30}. currency: Attribute *currency* is part of the object *Account Reference* as defined by the Berlin Group. ISO 4217 Alpha 3 currency code.
creditorAgent	String	N	Attribute filled with a BIC. ISO 20022 definition BIC: [A-Z]{6,6}[A-Z2-9][A-NP-Z0-9]([A-Z0-9]{3,3}){0,1}.
creditorName	String	Y	Party to which an amount of money is due. Max70Text.

Attribute	Type	Mandatory	Description
ultimateCreditor	String	N	Ultimate party to which an amount of money is due. Max70Text.
ultimateCreditorId	String	N	Max35Text.
endDate	String	N	The attribute *endDate* can be provided for **deferred payments, recurring payments and periodic payments**. Note that de Volksbank also allows for recurring and periodic payments with no end date, the so-called infinite or perpetual recurring payments. If the *endDate* is filled, it is the last date where the PISP can submit a deferred payment or a payment in a series of recurring payments for execution by the ASPSP. Attribute *endDate* has the ISO 8601 Date format (YYYY-MM-DD).
requestedExecutionDate	String	N	The attribute *requestedExecutionDate* is provided for **one-time agended payments**. Attribute *requestedExecutionDate* has the ISO 8601 Date format (YYYY-MM-DD).
startDate	String	N	The attribute *startDate* is provided for **periodic payments**. Attribute *startDate* has the ISO 8601 Date format (YYYY-MM-DD).
frequency	String	N	The attribute *frequency* is provided for **periodic payements**. Enumeration: 1. Weekly 2. EveryFourWeeks 3. Monthly 4. Quarterly 5. SemiAnnual 6. Annual
remittanceInformationUnstructured	String	N	The unstructured remittance information provided by the calling party during initiation or execution.
endToEndIdentification	String	N	Identification key provided by the calling party during initiation or execution.

4.8.10 Example get payment response

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

```
{
   "debtorAccount": {"iban": "NL64MAART0948305290", "currency": "EUR"},
   "debtorName": "Z H van der Zee CJ Z Bottema",
   "instructedAmount": {"currency": "EUR", "amount": "123.50"},
   "creditorAccount": {"iban": "NL55WIND0000012345", "currency": "EUR"},
   "creditorName": "Adyen",
   "ultimateCreditor": "Krentebol dot com"
 }
```

4.9 Cancel payment request

With the cancel payment endpoint, a PISP can cancel a payment approved by the PSU. Only a one-time agended or a bulk payment can be cancelled. A one-time direct payment is executed immediately after authorization is given and can therefore not be cancelled. This cancel endpoint also cannot be used by a PISP to cancel deferred or recurring payment(s) since the PISP, not the ASPSP, is responsible for the submission of the execution of a deferred or recurring payment.

4.9.1 Method and URL

Method	URL	Description
DELETE	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/payments/sepa-credit-transfer/{payment-id}	Cancel payment endpoint as defined by the Berlin Group in the implementation guide version 1.3 for the payment service **one-time agended payments**.
DELETE	https://psd.bancairediensten.nl/psd2/[snsbank|asnbank|regiobank]/v1/bulk-payments/pain.001-sepa-credit-transfer/{payment-id}	Cancel payment endpoint as defined by the Berlin Group in the implementation guide version 1.3 for the payment service **bulk payments**.

4.9.2 Path parameters

Attribute	Type	Mandatory	Description
payment-id	String	Y	Attribute hosts the unique identification assigned by the ASPSP to the payment, when the initiation request was sent in by the PISP.

4.9.3 Query parameters

The cancel payment endpoint does not have any query parameters.

4.9.4 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 PISP).

Attribute	Type	Mandatory	Description
Authorization	String	Y	Attribute filled with the *client_id*: identification of the PISP as registered with de Volksbank.

4.9.5 Request body

The cancel payment endpoint does not have a request body.

4.9.6 Example cancel payment request

The cancel payment request is illustrated below:

```
DELETE https://psd.bancairediensten.nl/psd2/snsbank/v1/payments/sepa-
credit-transfer/SNS5678901234567

Content-Type:       application/json

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

Authorization:      172b095e702f4042e881384c746532defe
```

4.9.7 Response code

Code	Description
200	OK (for one-time agended)
204	No Content (for bulk)

4.9.8 Response header

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

4.9.9 Response body

Only the response of a one-time agended payment cancellation call contains a body:

Attribute	Type	Mandatory	Description
transactionStatus	String	Y	Value of the attribute is conform with the ISO 20022 **ExternalPaymentTransactionStatus1Code** list. Enumeration: CANC (*CANC* means cancelled).

4.9.10 Example cancel payment response

The cancel payment response is illustrated below. For one-time agended:

```
HTTP/1.x 200 OK

Content-Type:   application/json

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

{

   "transactionStatus": "CANC"

}
```

For bulk:

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

4.10 Get payment status report request

When a SEPA Direct Debit is rejected, a pain.002 rejection file is generated. With this endpoint, the pain.002 file can be retrieved by the TPP.

4.10.1 Method and URL

Method	URL	Description
GET	https://psd.bancairediensten.nl/psd2/[snsbank|regiobank]/v1/bulk-payments/pain.008-sepa-direct-debits/{payment-id}/payment-status-reports/{payment-status-report-id}	Endpoint for retrieving the pain.002 XML rejection file for the service **SEPA Direct Debits**.

4.10.2 Path parameters

Attribute	Type	Mandatory	Description
payment-id	UUID	Y	Attribute hosts the unique identification assigned by the ASPSP to the payment, when the initiation request was sent in by the PISP.
payment-status-report-id	UUID	Y	Attribute filled with the ID of the payment status report/pain.002 XML rejection file, as returned in the response of a transaction status call of a SEPA Direct Debit (only returned if present – see also section 4.6).

4.10.3 Query parameters

The payment status report endpoint does not have any query parameters.

4.10.4 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 PISP).
Authorization	String	Y	Attribute filled with the access-token as obtained in the token request call.

4.10.5 Request body

The payment status report endpoint does not have a request body.

4.10.6 Example payment status report request

The payment status report request is illustrated below:

```
GET https://psd.bancairediensten.nl/psd2/snsbank/v1/bulk-
payments/pain.008-sepa-direct-debits/1bba72b6-0b44-47c1-bfa5-
32ae6bd53520/payment-status-reports/7d9601f8-1a59-4649-9542-a1d6742f4d0f

X-Request-ID:       fdb9757d-8f27-4f9e-9be0-0eadacc89017

Authorization:      Bearer <ACCESS-TOKEN>
```

4.10.7 Response code

Code	Description
200	OK

4.10.8 Response header

Attribute	Type	Mandatory	Description
Content-Disposition	String	Y	Header indicating that the file should be downloaded with a suggested filename.
Content-Type	String	Y	Attribute invariably filled with the value "*application/xml*".
X-Request-ID	UUID	Y	ID of the request obtained from the request header.

4.10.9 Response body

The response of a payment status report call contains an XML (not JSON) of the full pain.002 as received from Worldline.

4.10.10 Example get payment status report response

The cancel payment response is illustrated below.

```
HTTP/1.x 200 OK

Content-Disposition:   attachment;
filename="PAIN.002.001.03.4bddb96167104433999597ecfcb8074e.2023-05-01"

Content-Type: application/xml

X-Request-ID:   fdb9757d-8f27-4f9e-9be0-0eadacc89017


<?xml version="1.0" encoding="UTF-8"?>

<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pain.002.001.03">

    <CstmrPmtStsRpt>

        <GrpHdr>

            <MsgId>12345</MsgId>

            <CreDtTm>2022-09-25T16:07:00Z</CreDtTm>

        </GrpHdr>

        <OrgnlGrpInfAndSts>

            <OrgnlMsgId>54321</OrgnlMsgId>

            <OrgnlMsgNmId>pain.008.001.02</OrgnlMsgNmId>

            <OrgnlNbOfTxs>10</OrgnlNbOfTxs>
            <OrgnlCtrlSum>100</OrgnlCtrlSum>
        </OrgnlGrpInfAndSts>
        <OrgnlPmtInfAndSts>
            <OrgnlPmtInfId>13040576.500272</OrgnlPmtInfId>
            <OrgnlNbOfTxs>10</OrgnlNbOfTxs>
            <OrgnlCtrlSum>100</OrgnlCtrlSum>
            <PmtInfSts>RJCT</PmtInfSts>
            <StsRsnInf>
                <Orgtr>
                    <Id>
                        <OrgId>
                            <BICOrBEI>INNDNL2U</BICOrBEI>
                        </OrgId>
                    </Id>
                </Orgtr>
                <Rsn>
                    <Cd>EQ04</Cd>
                </Rsn>
            </StsRsnInf>
        </OrgnlPmtInfAndSts>
    </CstmrPmtStsRpt>
</Document>
```

4.11 Error handling

4.11.1 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.

Code	Description
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.

4.11.2 Additional error information

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

Attribute	Type	Mandatory	Description
category	String	Y	Error category. Always filled with “*ERROR*”.
code	String	Y	Error code. See table below for possible codes.
text	String	Y	Details of the error. See table below for possible text values.
additionalErrors	Array	N	A list for additional error information.
Array contains:			
code	String		Error code.
text	String		Extra information regarding the error.

Examples:

```
[
  {
    "category": "ERROR",
    "code": " FORMAT_ERROR",
    "text": " The format of input is not valid."
  }
]



[
  {
    "category" : "ERROR",
    "code" : "FORMAT_ERROR",
    "text" : "Validation failed, see additionalErrors property for more
details."
    "additionalErrors": {
      "code" : "AM16"
      "text" : "InvalidGroupControlSum in msgid.batchId2"
     }
  }
]
```

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.
400	ERROR	FORMAT_ERROR	One or more input fields are invalid.
400	ERROR	FORMAT_ERROR	Content-invalid
400	ERROR	FORMAT_ERROR	endToEndIdentification should be between 1 and 35 characters
400	ERROR	FORMAT_ERROR	debtorAccount IBAN is not valid
400	ERROR	FORMAT_ERROR	invalid country code in IBAN
400	ERROR	FORMAT_ERROR	IBAN is non-SEPA; payment cannot be processed as a SEPA Credit Transfer
400	ERROR	FORMAT_ERROR	debtorAccount currency should be EUR
400	ERROR	FORMAT_ERROR	instructedAmount should not be null
400	ERROR	FORMAT_ERROR	The format of the input is not valid.
400	ERROR	FORMAT_ERROR	amount should have no more than two decimals
400	ERROR	FORMAT_ERROR	instructedAmount currency should be EUR
400	ERROR	FORMAT_ERROR	creditorAccount should not be null
400	ERROR	FORMAT_ERROR	creditorAccount IBAN is not valid
400	ERROR	FORMAT_ERROR	IBAN is non-SEPA; payment cannot be processed as a SEPA Credit Transfer
400	ERROR	FORMAT_ERROR	creditorAgent doesn't match ISO 20022 definition of BIC
400	ERROR	FORMAT_ERROR	creditorName should be between 1 and 70 characters
400	ERROR	FORMAT_ERROR	ultimateCreditor should be between 1 and 70 characters
400	ERROR	FORMAT_ERROR	remittanceInformationUnstructured should be between 1 and 140 characters
400	ERROR	FORMAT_ERROR	remittanceInformationStructured should be between 1 and 35 characters
400	ERROR	FORMAT_ERROR	issuerSRI should be ISO or CUR
400	ERROR	FORMAT_ERROR	endDate should not be null
400	ERROR	FORMAT_ERROR	endDate doesn't match date format yyyy-MM-dd
400	ERROR	FORMAT_ERROR	deferred payment endDate should not be more than 13 months in the future
400	ERROR	FORMAT_ERROR	endDate cannot be in the past
400	ERROR	FORMAT_ERROR	requestedExecutionDate doesn't match date format yyyy-MM-dd
400	ERROR	FORMAT_ERROR	requestedExecutionDate cannot be in the past
400	ERROR	FORMAT_ERROR	requestedExecutionDate cannot be more than 10 years in the future
400	ERROR	FORMAT_ERROR	paymentId should be 16 characters
400	ERROR	FORMAT_ERROR	id should be a UUID

HTTP status	Category	Code	Text
400	ERROR	INVALID_ACCOUNT_ NUMBER_FORMAT	The format of the account number is not valid.
400	ERROR	INVALID_INPUT	The parameter is not supported.
400	ERROR	INVALID_INPUT	Retrieving the payment status has failed.
400	ERROR	PAYMENT_FAILED	The payment execution has failed.
400	ERROR	PAYMENT_FAILED	The payment initiation has failed.
400	ERROR	PAYMENT_FAILED	The payment has failed.
400	ERROR	PAYMENT_FAILED	Processing the payment has failed.
400	ERROR	PAYMENT_FAILED	The payment is rejected.
400	ERROR	PAYMENT_FAILED	The payment amount is invalid.
400	ERROR	PAYMENT_FAILED	(Various messages, originating from XSD validations of XML initiation files)
401	ERROR	INVALID_JWT_TOKEN	JWT token is invalid.
401	ERROR	CONSENT_INVALID	The mandate could not be found.
401	ERROR	CONSENT_INVALID	The mandate is revoked.
401	ERROR	CONSENT_INVALID	The mandate has an invalid status.
401	ERROR	CONSENT_INVALID	The entered digipass credentials are invalid.
401	ERROR	CONSENT_INVALID	The selected digipass token is invalid.
401	ERROR	CONSENT_INVALID	The account is not within the contract.
401	ERROR	CONSENT_INVALID	The mandate could not be granted.
401	ERROR	CONSENT_INVALID	The age is not allowed.
401	ERROR	CONSENT_EXPIRED	The expiration date of the mandate has been expired.
401	ERROR	CONSENT_EXPIRED	The consent should be executed once within 10 minutes.
403	ERROR	SERVICE_BLOCKED	This account's master switch is switched off.
403	ERROR	SERVICE_BLOCKED	The requested service is not allowed for this account.
403	ERROR	RESOURCE_UNKNOWN	The payment could not be found.
403	ERROR	RESOURCE_UNKNOWN	The paymentId and resourceId combination is invalid.
403	ERROR	RESOURCE_UNKNOWN	The paymentId is invalid.
404	ERROR	RESOURCE_UNKNOWN	The requested resource could not be found.
500	ERROR	INTERNAL_SERVER_ERROR	An internal server error occurred.

Bulk payments: Additional error ISO20022 reject reason codes after initiation of an XML pain.001 file.

AM02 NotAllowedAmount
AM16 InvalidGroupControlSum
AM19 InvalidGroupNumberOfTransactions
AM17 InvalidPaymentInfoControlSum
AM20 InvalidPaymentInfoNumberOfTransactions
AC02 InvalidDebtorAccountNumber
CH03 RequestedExecutionDateOrRequestedCollectionDateTooFarInFuture
DU02 DuplicatePaymentInformationID:

- Payment Information Block is not unique within a file
AC03 InvalidCreditorAccountNumber
CNOR CreditorBankIsNotRegistered
RR09 InvalidStructuredCreditorReference - Unstructured Remittance is also used - Issuer and Creditor reference should both have a value - Issuer code is invalid - Credit reference must be numeric if Issuer code = ‘CUR’ - Credit reference must start with RF and must be alphanumeric if Issuer code = ‘ISO’ - Credit reference lengthcode is incorrect (in case Issuer code = ‘CUR’) - Credit reference length is incorrect - Credit reference checksum digit is incorrect

SEPA Direct Debits: Additional error ISO20022 reject reason codes after initiation of an XML pain.008 file.

AC02 InvalidDebtorAccountNumber
AC03 InvalidCreditorAccountNumber
AM02 NotAllowedAmount
AM16 InvalidGroupControlSum
AM17 InvalidPaymentInfoControlSum
AM19 InvalidGroupNumberOfTransactions
AM20 InvalidPaymentInfoNumberOfTransactions
CH03 RequestedExecutionDateOrRequestedCollectionDateTooFarInFuture
CH04 RequestedExecutionDateOrRequestedCollectionDateTooFarInPast
DU01 DuplicateMessageId
DU02 DuplicatePaymentInformationId
DS0H NotAllowedAccount
MS03 NotSpecifiedReasonAgentGenerated