

**Skandiabanken
Technical documentation Open Banking**

1	Introduction	4
1.1	Background	4
1.2	Status	4
1.3	Contact us and channels for communication	4
2	Document history	5
3	Test environment and sandbox	6
3.1	General information	6
3.2	Onboarding of TPP in Test Environment	6
3.3	Guidelines for the Test Environment	6
4	Onboarding of TPP in Production Environment	7
4.1	Process overview	7
4.2	Create an account in the portal	7
4.3	Adding a colleague to your consumer organization	7
4.4	How to setup your apps and subscriptions	7
4.5	Update eIDAS-certificate	10
5	General information about API invocation	12
5.1	Gateway	12
5.2	General error messages	12
5.3	Overview of available accounts and customers	12
6	 AIS - Security and authentication of TPP including SCA of PSU	13
6.1	OAuth2	13
6.2	Request Access code and ultimately Access token	13
7	 AIS 2.0.0 – operations	17
7.1	Introduction	17
7.2	Get Account List	17
7.3	Get Account Details	21
7.4	Get Balance List	24
7.5	Get transaction list of an account	27
7.6	Get Transaction details	31
8	 PIS 3.0.0 - operations	35
8.1	Introduction	35
8.2	Payment Initiation flow	35
8.3	Post Payment initiation request	36
8.4	Start the authorization process for a payment	41
8.5	Get Payment information	43
8.6	Payment Cancellation Request	46

8.7	<i>Get Payment status request</i>	49
8.8	<i>Create Signing Basket</i>	50
8.9	<i>Rules and different statuses for Payments</i>	51
9	Fallback Solution	53

1 Introduction

Welcome to Skandiabanken Open Banking solutions!

1.1 Background

This document and our information-site are created to provide the information needed to access our API's. If you have questions or suggestions, you are welcome to contact us. Contact information can be found in section 1.3 Contact us and channels for communication.

Info site: www.skandia.se/openbanking

Portal: <https://developer.skandia.se/open-banking/core-bank/>

Test-Portal: <https://developer.test.skandia.se/open-banking/core-bank/>

A glossary of abbreviations and acronyms can be found on the information site.

1.2 Status

This section will clarify what we have in place and the status of the functionality. Please read the rest of this documentation for further information and details.

Functionality	Available	Comments
SCA	Yes	A redirect solution using Swedish BankID. We are investigating embedded/decoupled solutions.
TPP-identification (eIDAS)	Yes	We support eIDAS/QWAC. QSealC is currently not required but we are investigating it.
Relevant standards	Yes	Berlin Group NextGenPSD2 Framework version 1.3.6 OAuth2 including OpenID Connect TLS 1.2
AIS	Yes	Payment account information for private customers over 18 years. We have no business customers with payment accounts.
PIS	Yes	Domestic transfer and bill payments. International payments and signing basket will be available in a later release.

During the timespan 04:00-04:30 each day our service provider restarts services and servers, which has impact on performance on all our channels (Online, App and Open Banking). For you to get the best experience, and in the end our common end customers, we recommend that during that time not to schedule batch calls. Response times will be much longer, and error rate will be higher. We apologize for this but we want to give you as much insight as possible to obtain the best possible service.

1.3 Contact us and channels for communication

If you have questions, feedback or general problems you are welcome to contact us via mail openbanking@skandia.se. This mailbox is mainly monitored during business hours. Please use this for technical questions or business inquiries.

If you have very urgent issues outside business hours, please contact our customer and TPP support:

<https://www.skandia.se/kontakta-skandia/kontakta-oss/>.

Mainly use phone: +46771555500

Open hours 07-23 Monday through Friday, 08-22 Saturday and Sunday, year around.

2 Document history

Version	Date	Description
1.29	2024-05-03	<ul style="list-style-type: none"> - New chapter added regarding PIS v3. Chapters regarding PIS v2 and PIIS was removed.
1.28	2024-02-13	<ul style="list-style-type: none"> - Instruction on how to change certificate.
1.27	2023-10-10	<ul style="list-style-type: none"> - Updates regarding HTTP 403.
1.26	2023-07-11	<ul style="list-style-type: none"> - Updated section 8.3.4 and 8.3.6 regarding debtor account.
1.25	2023-06-27	<ul style="list-style-type: none"> - Updated information regarding change from 90 to 180 days consent for PSUs. - Corrected section 8.3.1 regarding Payment initiation – Request description. Removing unsupported headers TPP-Redirect-URI and TPP-Nok-Redirect-URI - Corrected section 8.3.3 regarding Payment initiation - Domestic credit transfer request. Removing unsupported field DebtorAccount.Iban
1.24	2023-06-08	<ul style="list-style-type: none"> - Corrected section 8.11.2 regarding payment status. - Addition of examples for Giro payments, section 8.3.3.
1.23	2023-03-15	<ul style="list-style-type: none"> - Clarification of parameter “requestedExecutionDate” - Body description single payment initiation - GiroDomesticCreditTransfer as well as 08.9.1 Execution rules for payments. - Section 6.3 General error messages is reworked and more detailed error messages are added - Section 7.3.5 HTTP 404 Resource unknown added
1.22	2022-10-24	<ul style="list-style-type: none"> - Move section version history to top of document. - Rework and added clarifications in section 5 Security and authentication of TPP including SCA of PSU - Addition of response examples in sections 5.2.1, 5.2.2 and 5.2.4 - Correction of section 6.2.4 Refresh token. - More example responses under section 7.2 Get Account List. - Clarification of responses on sections about AIS and PIS, sections 7 AIS 2.0.0 – operations and 8 PIS 3.0.0 - operations. - Fixing spelling and grammatical errors. - New section about expired token upon authorization of a payment in section 0 { <pre> "scaStatus": "Started" </pre> <pre> "transactionStatus": "ACSP", "_links": { "scaRedirect": { "href": "/pis/v3/payments/domestic-transfer/915003010004026/authorisations" }, "self": { "href": "/pis/v3/payments/domestic-transfer/915003010004026" }, "status": { "href": "/pis/v3/payments/domestic-transfer/915003010004026/status" } } </pre>
1.21		Added information regarding changes in app switch from BankID
1.20		Removed information regarding a bug which is no longer relevant
1.19		Added information regarding rules and statuses for Payments
1.18		Added information regarding known bug in payment flow.
1.17		Added chapter regarding PIS v2, CrossborderCreditTransfers
1.15		Improved response examples. Description of “Get transaction list of an account”

1.14		Adding information regarding Signing Basket and Periodic payments in PIS v2.
1.12		Adding chapter regarding PIS v2 and some information regarding handling of consent, remove chapter regarding AIS v1 and PIS v1.
1.11		Adding chapter regarding Get Transaction List and Get Transaction Details in AIS v2.
1.10		Adding chapter about AIS v2 and information regarding scope
1.09		Adding chapter about Confirmation Of Funds
1.08		Information about fallback solution and test environment.
1.07		Adding Payment cancellation and information about refresh token
1.06		Spelling mistakes
1.05		Miscellaneous clarifications to PIS.
1.04		Updated to include PIS - domestic transfers with same date. AIS updated.
1.03		Clarifications and examples. Mainly regarding OAuth2 flows.
1.02		Updates for production portal registration and APIs
1.01		Updates for testing with mocked data

3 Test environment and sandbox

3.1 General information

We currently support testing of the same services as we have in production:

- AIS
- PIS, both transfers and payments

To be able to use the test environment you need:

- Test or production eIDAS-certificate. If you use a test-certificate:
 - The certificate must be issued by a publicly trusted CA. No self-signed certificates will be accepted.
 - The certificate must contain a correct Organization Identifier (2.5.4.9.7 = PSDXX-YYYY-ZZZZZZZZ)
 - The certificate must contain a QC Statement with the PSD2 roles that you intend to use.
- A test BankID. (Swedish BankID is currently the only supported SCA).
 - The BankID client must be configured as a test BankID client. More info about how this is done is available at demo.bankid.com

3.2 Onboarding of TPP in Test Environment

The process of onboarding in the Test Portal is the same as onboarding in the Production Environment but with a few exceptions.

1. You reach the test portal at <https://developer.test.skandia.se/open-banking/core-bank/>
 - a. You will have to create separate users for the Test and Production Portals.
 - b. Since there are separate users you will receive different Client-Ids in Test and Production.
2. You only need a test eIDAS-certificate and not a production certificate.
 - a. You can use your production certificate, but it is not necessary.

Except for the above differences you can follow the instruction in 4 Onboarding of TPP in Production Environment when onboarding in the Test Environment.

3.3 Guidelines for the Test Environment

There is a limited number of test PSU's in the environment, please contact openbanking@skandia.se after onboarding to receive specific test PSU to run test on.

The account numbers used in testing must follow the logic of real accounts. You can therefore not test transfers to made up accounts. Notice that other TPPs also can see the test PSUs transactions history. Any account numbers used in testing can therefore be seen by other TPPs.

4 Onboarding of TPP in Production Environment

4.1 Process overview

This section provides a process overview how a TPP can gain access to our production environment including portal and API gateway.

1. Get an approval from a local NCA (Finansinspektionen in Sweden) as an AISP or PISP. If you are a bank you already have an approval.
2. Obtain a production eIDAS-certificate from a QTSP. QWAC is required.
 - a. Note 1: you cannot use a CA root certificate
 - b. Note 2: you cannot use a test certificate
3. Register in our portal and create apps and subscriptions. You will need the public key of your production eIDAS QWAC certificate in this process.
4. When you add a subscription to an app there will be a manual step for us to grant your app access. You will receive an e-mail when your app is granted access.
5. You can access the APIs (AIS and/or PIS) your certificate allows you to invoke

Business partners have a similar process which is not covered in this documentation.

4.2 Create an account in the portal

Browse to the portal (<https://developer.skandia.se/open-banking/core-bank>). We strongly recommend that you use Firefox or Chrome as a browser when using the portal.

Step by step to register an account

1. Navigate to the portal. Click the "CREATE ACCOUNT" button (top right corner).
2. Enter the fields:
 - a. user name (please make a note of the selected user name, it is required for login)
 - b. email address (will be used for communication with your organization)
 - c. first name
 - d. last name
 - e. phone (optional but recommended)
 - f. consumer organization (defines the name of the collective under which client applications will be created)
 - g. password and confirm password and captchaPress the "Sign up" button
3. Open the email received from the portal and follow the activation link. This will activate the user account.
4. Login using the username and password selected by you

4.3 Adding a colleague to your consumer organization

It is possible to invite additional users to your consumer organization. This can be done while logged in as the consumer organization owner/creator or if you possess the administrator role of that specific consumer organization.

The new user is invited using an e-mail address. An e-mail containing a registration link is sent to the provided e-mail address. If the e-mail is registered to an existing user account, following the link will add that user to the specific consumer organization. If the e-mail is previously unused, following the link will require the user to step through the process for creating an account except that no new consumer organization needs to be created.

4.4 How to setup your apps and subscriptions

Product

The API Products view provides an overview of the products available in the portal. A product acts as a collection of APIs. To enable invocation of an API, you must subscribe with an app to a product's plan containing the desired API.

API

An API is a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service. The API can be protected by various security mechanism, including, but not limited to, Client-Id identification, MTLS and OAuth.

We expose a set of APIs which makes it possible for third parties to create applications using payment account information and payment initiation.

Plan

A plan represents a collection of APIs from a specific product. Subscribing to a plan allows the consuming app to invoke the APIs included in the plan given the correct security protocols are satisfied. A plan can contain terms of the usage of its APIs, including invocation rate limits and debit.

Apps

Apps are the components that are used to invoke the APIs. An app has its own set of security credentials, Client-Id and client secret. To create an app, navigate to the apps page and click the “Create new app” button.

To create an app, the following fields are required:

Field	Comment
Title	The name of the app (only visible to you and us)
QWAC Certificate	<p>Paste the content of the public part of your eIDAS QWAC x509 Certificate in PEM format with base 64 encoding. Please provide PEM encapsulation (BEGIN CERTIFICATE, END CERTIFICATE) on separate lines with the base 64 encoded certificate on a single line between the encapsulations. This certificate will be used for both MTLS and to determine your TPP accessibility.</p> <p>The certificate should contain the whole certificate chain.</p>
QSEAL Certificate (optional)	<p>Paste the content of the public part of your eIDAS QSEAL x509 Certificate in PEM format with base 64 encoding.</p> <p>We currently do not validate QSEAL but will do later, by entering this field the process will be easier for you when we require QSEAL.</p> <p>The certificate should contain the whole certificate chain.</p>
Application OAuth Redirect URL(s)	<p>A list of redirect urls to be used in the OAuth Authorization code flow. These addresses will be used to receive the authorization code required when claiming the access token for the API invocation.</p> <p>The url:</p> <ul style="list-style-type: none"> • Must follow the format (?=\w+:\V?*\w+) • Cannot contain intermediate white spaces <p>There is a timeout for how long an authorization code is valid, and that’s 60 seconds. If it takes longer than that to replace it with an access token, you will get the error message authorization code is invalid or expired.</p>
Sign Redirect Url (optional)	Does not need to be included here since this information is not used. The redirect url that the PISP wants to use must instead be included in the call.

```
-----BEGIN CERTIFICATE-----CR LF
MIIHoDCCBoigAwIBAgIKBllY7rSIPwDBDANBgkqhkiG9w.....CR LF
-----END CERTIFICATE-----CR LF
```

Above: example of a correctly PEM-formatted public part of a QWAC Certificate

After creating an app, Client-id and client secret will be provided. Take note, this is the only time the client secret will be shown for you. It is possible to reset the client secret by navigating to apps, select an app, click subscriptions, select the menu present in the top right corner of the credentials window and click reset client secret.

Step by step to invite a user to your Consumer Organization

1. While logged in, view the “Organization” label on the right side of the top menu.
2. Ensure that the selected consumer organization is the one that you wish to invite a new member to by observing the name displayed under the organization label.
3. Click the “Organization” label on the right side of the top menu.
4. Click “My Organization” from the drop-down-menu.
5. Ensure that you are in the correct consumer organization by viewing the name displayed in the top left corner.
6. Click the green “Invite” button on the right side of the screen.
7. Provide the e-mail address of the member you wish to invite (existing or new user).
8. Assign a role that the new member should possess.
 - a. Administrator – Manage members, apps and subscriptions of this consumer organization.
 - b. Developer – Manage apps and subscriptions of this consumer organization.
 - c. Viewer – View apps and subscriptions of this consumer organization.
9. Click “Submit”
10. Once the e-mail is received by the new member, the activation link should be followed to activate the invitation.

Step by step to create an App

1. While logged in, click the “APPS” label from the top menu
2. Click the “Create new app” button
3. Enter mandatory fields title, QWAC-certificate¹, application OAuth redirect URL(s) (minimum 1) and click the ‘Submit’ button
4. Take note of the API Key (Client-Id) and Secret and click the “Continue” button

Step by step to update an App

1. While logged in, click the “APPS” label from the top menu
2. Select and click the App to edit
3. Click the three vertical dots in the top right corner and select “Edit” from the drop-down menu
4. Change any of the available fields, including title, application OAuth Redirect URL(s) and Sign Redirect URL.
5. Click the ‘Submit’ button

Step by step to reset client secret

1. While logged in, click the “APPS” label from the top menu
2. Select and click the app to which you would like to reset client secret
3. Click the “Subscription” link located below the app name
4. Click the three vertical dots located in the top right corner of the credentials window and select “Reset Client Secret” from the drop-down menu
5. Click the “Reset” button
6. Check the ‘Show’ checkbox at to the top of the page
7. Take note of the new client secret

Step by step to delete an App

1. While logged in, click the “APPS” label from the top menu
2. Select and click the app to be deleted
3. Click the three vertical dots in the top right corner and select “Delete” from the drop-down menu
4. Click the “Delete” button

Subscription

¹ The eIDAS certificate holds authorization/the role you have and regulates if you can access AIS and/or PIS. If you as an ASIP create an app/subscription for PIS, the subscription will be denied.

A subscription defines a connection between a plan and an app. The plan defines the how and what of the subscription, including what APIs and how the APIs are accessible. The app defines the which of the subscriptions and hence details what credentials that are to be used against the gateway when attempting to invoke any of the APIs. Without a valid subscription, an app can never invoke a published API in the production environment.

To subscribe to a plan, go to the product overview page, select a product, click the plan you desire to subscribe to. Choose the App to which the subscription should be created for and confirm the subscription.

The act of requesting a new subscription will require a manual approval from us before the client app is enabled to invoke the API. It is possible to track the approval status by navigating to the app's subscriptions overview. If you know in advance that you need to get a fast approval, please contact us via mail and let us know a business day ahead.

Step by step to create a subscription

1. While logged in, click "API PRODUCTS" from the top menu
2. Select and click the product that the subscription should regard
3. Select and click the 'Subscribe' button of the desired Plan
4. Select and click the 'Select App' button of the desired app
5. Overview the subscription details and press the "Next" button
6. Click the "Done" button

Step by step to view Subscription status

1. While logged in, click the "APPS" label from the top menu
2. Select and click the app to which the subscription belongs to
3. Click the 'Subscription' link located below the app name
4. View the status of subscriptions in the subscriptions window

Step by step to remove a Subscription

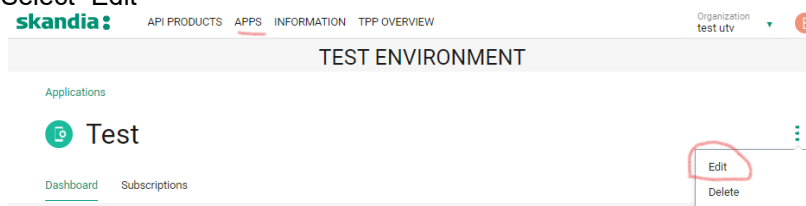
1. While logged in, click the "APPS" label from the top menu
2. Select and click the app to which the subscription belongs to
3. Click the "Subscription" link located below the app name
4. Click the three vertical dots located to the right of the specific subscription located in the Subscriptions window
5. Select "Unsubscribe" from the drop-down menu
6. Click the "Unsubscribe" button

4.5 Update eIDAS-certificate

An eIDAS-certificate has an expiration date and must be changed/updated before that date, otherwise the subscription will stop working. Here is an instruction how you can do that. This can only be done if the roles and issuer in the new and old certificate are the same, otherwise a new application must be created.

Step by step to update QWAC/Certificate

1. While logged in, click the "APPS" label from the top menu
2. Select and click the app to update
3. Click the three vertical dots
4. Select "Edit"



5. Paste the new QWAC/Certificate into the box "New QWAC Certificate" PEM, base-64
6. Click "Submit"

If checks are ok the new certificate will be update and will immediately start to be used going forward.
The old certificate will no longer be used and will automatically be removed when expiration date is expired.

If checks are not ok, read the message.

5 General information about API invocation

5.1 Gateway

Invoking the APIs requires three security measures:

1. Header "Client-Id" containing the client id of your App created in the developer portal. The app holds a valid subscription containing the specific API.
2. MTLS with the eIDAS QWAC certificate provided when creating the App.
3. For AIS: An Authorization header containing a bearer access token of type reference containing the scope demanded by the API definition.

5.2 General error messages

The APIs return errors that are common for all the available products as well as ones that are specific for the API product or method.

5.2.1 HTTP 401 Unauthorized

These are common 401 Unauthorized response messages and their implication:

- **Invalid client id or secret:** You are attempting to invoke the API using a Client-Id that is not valid for the specific API.
- **Client certificates for mutual TLS in the API request doesn't match the registered certificate:** The provided Client-Id is correct, but you are using a certificate that is not related to that Client-Id.
- **Cannot find valid subscription for the incoming API request:** The provided Client-Id is valid, but you are not authorized to invoke this API as that Client-Id (App) does not possess an approved subscription.
- **Cannot pass the security checks that are required by the target API or operation, enable debug headers for more details:** Could be one of the following three reasons.
 - Access token is not a valid reference token.
 - Access token has expired.
 - Access token does not contain the scope required by the API

5.2.2 HTTP 503 Service Unavailable

The service is unavailable. This can be caused by for example high load on the server or other unplanned issues. This error should be temporary and it is recommended to try again later.

```
{
  "tppMessages": [
    {
      "category": "ERROR",
      "code": "SERVICE_UNAVAILABLE",
      "text": "Service unavailable"
    }
  ]
}
```

5.3 Overview of available accounts and customers

The API:s give access to payment accounts owned by private consumers over the age of 18.

Summary of available accounts:

- "Allt i Ett-konto". Transaction account, typically used for everyday transactions and bill payments
- "Sparkonto". Typically, a savings account. Only domestic transfers possible, no bill payments etc.
- No fixed rate accounts are available
- The consumer must own the account
 - We have no co-owned accounts

6 AIS - Security and authentication of TPP including SCA of PSU

6.1 OAuth2

We use OAuth 2.0 for authentication and authorization. Our APIs are protected by the OAuth Authorization Code Grant type which is depicted in detail at <https://oauth.net/2/>.

6.2 Request Access code and ultimately Access token

To be granted access to the PSU's accounts, the PSU needs to be authenticated by us. This is performed using a redirect approach. We are however investigating supporting other approaches such as decoupled and embedded. Swedish BankID is currently the only supported SCA.

This section provides information how to perform SCA with the redirect solution.

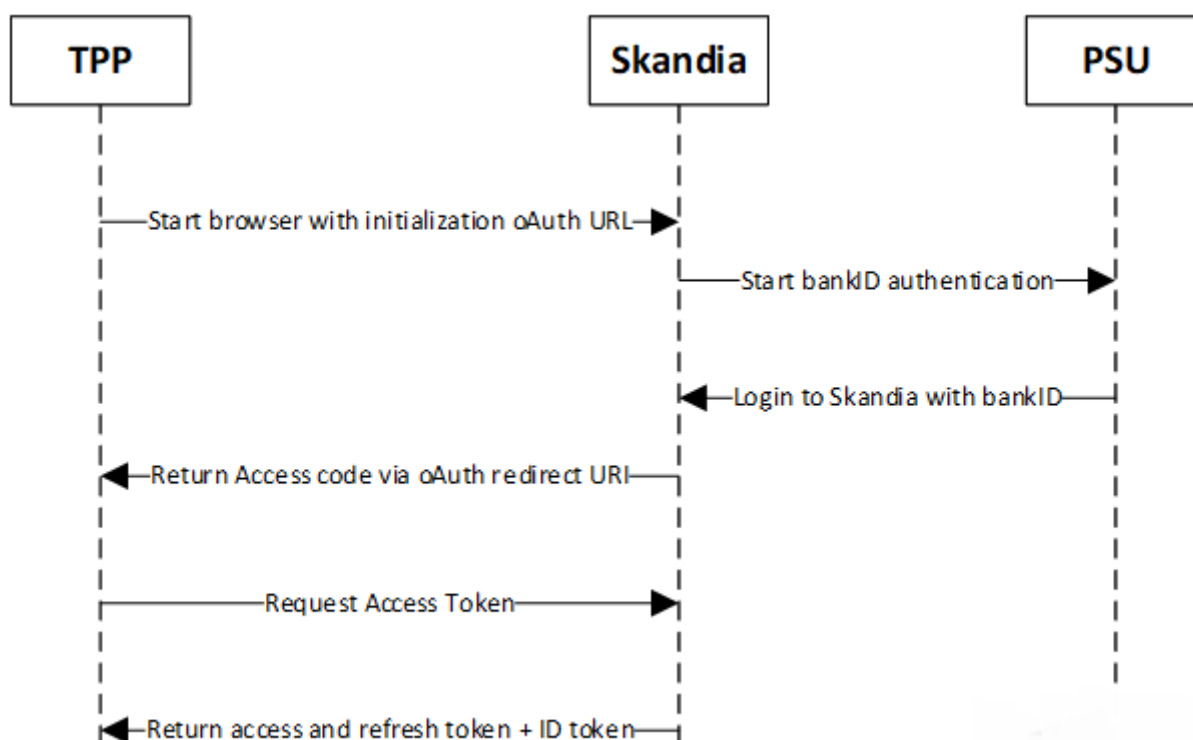


Figure 1 Overview of the authentication flow.

1. You, the TPP, makes a request to Skandia for the authentication of the PSU. In the request, your Client Id, a redirect URI and requested scopes must be provided.
2. The PSU identifies themselves using Swedish BankID
3. If BankID sign is successful, we return an access code to the redirect URI provided by you.
4. TPP can now request access token using the access code and client secret.

6.2.1 Request for authorization

Use the `client_id` (denoted “Key” in Figure 2) and `client_secret` (denoted “Secret” in Figure 2) received when you created the app in the developer portal along with the redirect URI’s that you provided for that specific app.

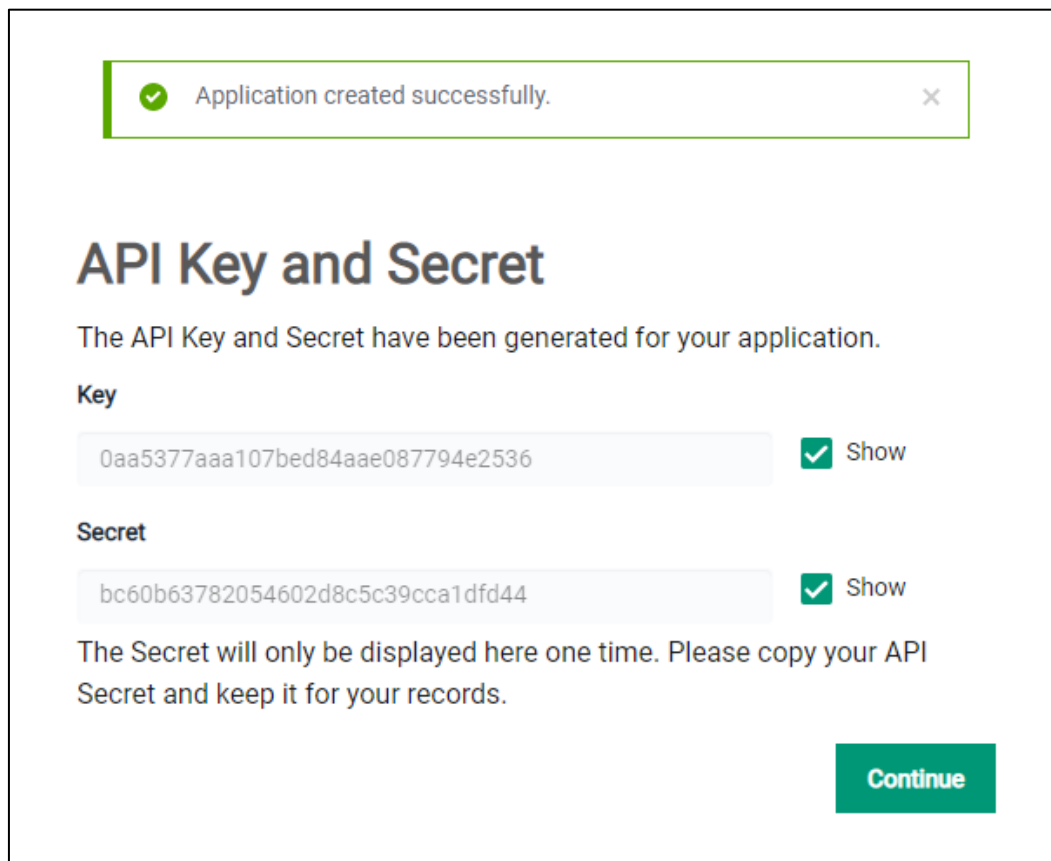


Figure 2: Example of view when an application has been created and the Key and Secret are shown.

The authorization request² should contain the following query parameters:

- **response_type:** code
- **client_id:** The `client_id` of your App in the developer portal
- **redirect_uri:** A redirect URI that you have provided for the app in the portal. You cannot have a '/' as the last character in the URL, because it will be removed by the system. It must be URL encoded.
- **scope:** Should at least contain the API specific scope, i.e. `psd2.aisp` for AIS or `psd2.pisp` for PIS, and the openid scope. You must call on the format "`scope=openid+psd2.aisp+psd2.pisp`". The '+' sign can be substituted with '%20'.
- **state:** A random string that should be validated to be identical in the redirect return after the user authorizes the app.

² For production environment use: `fsts.skandia.se`
For test environment use: `fsts.ctx.skandia.se`

Example Authorization Request:

```
GET https://fst.s.skandia.se/as/authorization.oauth2?
response_type=code
&client_id=0aa5377aaa107bed84aae087794e2536
&redirect_uri=https%3A%2F%2Flocalhost/
&scope=psd2.aisp%20openid
&state=ca17f9d039024a789493641d8cdbba14
```

The PSU is directed to Skandia's authentication server and prompted to identify themselves with BankID. After identification has been completed successfully, a code and state are returned to the redirect location. In this example, the PSU will be redirected to the below URL:

```
https://localhost/
?code=Im6_IkPhrd67m2gFw9upLilm9h32PmM51gUAAAAC
&state=ca17f9d039024a789493641d8cdbba14
```

6.2.2 Request for access token

The code received in the redirect is used when requesting the access token.

Body Parameters:

- **grant_type:** authorization_code
- **code:** Access code received in the redirect from the authorization request.
- **redirect_uri:** Same redirect URI that was used in the authorization request.
- **client_id:** The ID of your App created in the developer portal, denoted Key in the image above.
- **client_secret:** Is received when creating the App, denoted Secret in the image above.

Example Access Token Request:

```
POST https://fst.s.skandia.se/as/token.oauth2
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code
&code=661e9996602e47f7b23039a441c91061
&redirect_uri=https%3A%2F%2Flocalhost/
&client_id=0aa5377aaa107bed84aae087794e2536
&client_secret=bc60b63782054602d8c5c39cca1dfd44
```

Response

```
HTTP/1.1 200 OK

{
  "access_token": "000dbQSzY6Q0JXKS8FNBC5w5gS4c",
  "refresh_token": "RU76PJdqG0CjOvybmr1Y5Z6VzgmGji692hvXQgzTvY",
  "id_token": "XXXXXX",
  "token_type": "Bearer",
  "expires_in": 7199
}
```

6.2.3 Token types and its uses

To access the APIs, you need to provide a valid access token in the Authorization header. The access token is a short-lived token, valid only for 15 minutes. After 15 minutes you will get HTTP 401 Unauthorized. When the access token has expired, you can use the refresh token to get a new access token.

The refresh token is only valid for one time use. When a refresh token is used to issue a new access token, the response will contain the new access token and a new refresh token. The access token can be refreshed for a maximum time of 180 day from the initial time of authentication. After 180 days the PSU needs to be authenticated again as previously described.

The [ID token \(of type OpenID Connect\)](#) is a representation of the identity (SSN, “*personnummer*”) of the authenticated PSU. This enables you as a TPP to validate that the PSU using your services corresponds to the PSU authenticated by us.

6.2.4 Refresh token

Refreshing a token is possible by using the refresh_token provided in the response to the access token request. The request should contain the following body parameters:

- **grant_type**: refresh_token
- **refresh_token**: The refresh token received from the previous access token request.
- **client_id**: The client_id of your created app in the portal.
- **client_secret**: The client_secret received when creating the app.

Example Refresh Token Request:

```
POST https://fsts.skandia.se/as/token.oauth2
Content-Type: application/x-www-form-urlencoded

grant_type=refresh_token
&refresh_token=661e9996602e47f7b23039a441c91061
&client_id=0aa5377aaa107bed84aae087794e2536
&client_secret=bc60b63782054602d8c5c39cca1dfd44
```

Response

```
HTTP/1.1 200 OK

{
  "access_token": "000dPpNS21W4DiCdAmqCPym6yCpt",
  "refresh_token": "Qfc2u0ayWwN9w3zrItK4hCgZQtEsHcXZ5cbmMdQ3iz",
  "token_type": "Bearer",
  "expires_in": 7200
}
```

6.2.5 AIS consent

You as a TPP are responsible of handling the consent that the customer gives you and act according to it. We do not.

After authentication by the PSU you have access to account information for 180 days without a renewed authentication. You will have access to the accounts present at the time of the SCA and any new payment accounts the PSU creates.

If the PSU is authenticated again within the 180 days, you will receive a new token valid for another 180 days. If you for some reason, for example due to some agreement with the PSU, do not want access for another 180 days, you simply throw away the new token and continue using the old one.

7 AIS 2.0.0 – operations

7.1 Introduction

The Account Information Services API is used to get account information, such as transactions and balances, about customers payment accounts.

Prerequisites:

1. Have registered a user account in the portal (see section 4.2 Create an account in the portal)
2. Have an app setup in the portal with an eIDAS-certificate of QWAC-type telling us you are an AISP (see section 4.4 How to setup your apps and subscriptions)

Flow for first time access for a given customer:

1. The PSU agrees with you to use your services to retrieve account information from us
2. OAuth2/SCA – customer is informed about giving information to the you
 - a. The OAuth token will contain the ID of the customer
3. AISP invokes the AIS-operation of choice and receives a response with the requested information

Please view the swagger file for more information.

7.2 Get Account List

The operation will return a list of all payment accounts for a given PSU. Only the accounts which is owned by the PSU will be listed.

We do not support the query parameter “withBalance” at the moment. Request balances with the separate call.

GET/v2/accounts

7.2.1 Request description

Name	Type	Information
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: he forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia

		Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-IP-Address	String	In: header Required: recommended by Skandia Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Referer	String	In: header Required: recommended by Skandia Description: "Referer" header field sent by the PSU terminal when connecting to the TPP
PSU-TimeStamp	String	In: header Required: recommended by Skandia Description: Timestamp of the most relevant PSU's terminal request to the TTP
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available

7.2.2 Response description

Name	Type	Description
AccountList	list	The list of accounts for the given customer
Parameters of accountList		
accountsDetails		
resourceId	string	Id of an account (used to call other AIS operations)
bban	string	Bban identifier (clearing + number)
bic	string	BIC code of Skandiabanken: SKIASSESS
cashAccountType	string	Always "CACC"
currency	string	The currency code of the account ISO 4217

DisplayName	string	Currently not supported
iban	string	Iban of an account
name	string	Our product name of the account type Example: <ul style="list-style-type: none">• “Allt i Ett-konto” (transaction account)• “Sparkonto” (savings account)
OwnerName	string	Currently not supported
usage	string	Always “PRIV” (private personal account, natural person)
_links		linked resources
_links		
self	string	link to get account details
balances	string	link to get balances
transactions	string	link to get transactions

7.2.3 HTTP 200 Response

When the PSU has accounts that are available in the channel, the response body will be formatted as below, with one item in the accounts array per available account.

```
{
  "accounts": [
    {
      "resourceId": "957054871102373",
      "bban": "91598570120",
      "bic": "SKIASESS",
      "cashAccountType": "CACC",
      "currency": "SEK",
      "displayName": "",
      "iban": "SE079150000091598570120",
      "name": "Allt i Ett-konto",
      "ownerName": "",
      "usage": "PRIV",
      "_links": {
        "self": {
          "href": "/v2/accounts/957054871102373"
        }
      },
      "balances": {
        "href": "/v2/accounts/957054871102373/balances"
      },
      "transactions": {
        "href": "/v2/accounts/957054871102373/transactions"
      }
    }
  ]
}
```

7.2.4 HTTP 200 Response - no accounts available in the channel

When the PSU has no payment accounts that are available for viewing in the Open Banking channel, the response will be HTTP 200 and the body will be an empty array³.

```
{ "accounts": [] }
```

7.2.5 HTTP 404 Resource unknown

When no accounts at all are found for the PSU, the response will be the following:

```
{
  "tppMessages": [
    {
      "category": "ERROR",
      "code": "RESOURCE_UNKNOWN",
      "text": "No available payment accounts"
    }
  ]
}
```

³ This behavior was introduced on September 13th 2022. Before this date, the behavior was to response with HTTP 404 Not Found.

7.3 Get Account Details

The operation will return detailed information for the account addressed by account-Id.

GET /v2/accounts/{account-Id}

7.3.1 Request description

Name	Type	Information
Account-Id	String	In: path Required: true Description: This identification is denoting the addressed account. The account-Id is retrieved by using a "Get Account List" call, using information from ResourceId.
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: he forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-IP-Address	String	In: header

		Required: recommended by Skandia Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available
PSU-Referer	String	In: header Required: recommended by Skandia Description: "Referer" header field sent by the PSU terminal when connecting to the TPP
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Referer	String	In: header Required: recommended by Skandia Description: "Referer" header field sent by the PSU terminal when connecting to the TPP
PSU-TimeStamp	String	In: header Required: recommended by Skandia Description: Timestamp of the most relevant PSU's terminal request to the TPP
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available

7.3.2 Response description

Name	Type	Description
Parameters of accountList		
resourceId	string	Id of an account (used to call other AIS operations)
bban	string	Bban identifier (clearing + number)
bic	string	BIC code of Skandiabanken: SKIASSESS
cashAccountType	string	Always "CACC"
currency	string	The currency code of the account ISO 4217
DisplayName	string	Currently not supported
iban	string	Iban of an account
name	string	Our product name of the account type. Example: <ul style="list-style-type: none">• "Allt i Ett-konto" (transaction account)• "Sparkonto" (savings account)
OwnerName	string	Currently not supported
usage	string	Always "PRIV" (private personal account, natural person)
_links		
self	string	Link to get account details
balances	string	Link to get balances
transactions	string	Link to get transactions

7.3.3 Response example Body:

```
{
  "accounts": [
    {
      "resourceId": "957054871102373",
      "bban": "91598570120",
      "bic": "SKIASSESS",
      "cashAccountType": "CACC",
      "currency": "SEK",
      "displayName": "",
      "iban": "SE079150000091598570120",
      "name": "Allt i Ett-konto",
      "ownerName": "",
      "usage": "PRIV",
      "_links": {
        "self": {
          "href": "/v2/accounts/957054871102373"
        },
        "balances": {
          "href": "/v2/accounts/957054871102373/balances"
        },
        "transactions": {
          "href": "/v2/accounts/957054871102373/transactions"
        }
      }
    }
  ]
}
```

7.4 Get Balance List

The Operation will return the balances for the account addressed by account-Id.

GET /v2/accounts/{account-Id}/balances

7.4.1 Request description

Name	Type	Information
Account-Id	String	In: path Required: true Description: This identification is denoting the addressed account. The account-id is retrieved by using a "Read Account List" call, using information from ResourceId.
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: he forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-IP-Address	String	In: header Required: recommended by Skandia

		Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Referer	String	In: header Required: recommended by Skandia Description: "Referer" header field sent by the PSU terminal when connecting to the TPP
PSU-TimeStamp	String	In: header Required: recommended by Skandia Description: Timestamp of the most relevant PSU's terminal request to the TPP
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available

7.4.2 Response description

Name	Type	Description
account		
bban	string	bban of an account
iban	String	iban of an account
currency	String	the currency code of the account ISO 4217
balances		list of balances
balanceType "closingBooked"	List	booked transactions
balanceAmount		
amount		Balance amount of booked credit and debit transactions when the request was initiated
currency	String	The currency of the amount
balances		
balanceType "interimAvailable"	List	booked transactions
balanceAmount		
amount		Balance amount of booked credit and debit transactions when the request was initiated. Including reserved transactions.
currency	String	The currency of the amount
creditLimitIncluded	Boolean	Always "true". This does not say if an account has a credit or not. It only states that; if the account has a credit, it is included in the amount.
referenceDate	Date	Now

7.4.3 Response body example

```
{
  "account": {
    "bban": "91598570120",
    "iban": "SE079150000091598570120",
    "currency": "SEK"
  },
  "balances": [
    {
      "balanceAmount": {
        "amount": "-1333.26",
        "currency": "SEK"
      },
      "balanceType": "closingBooked",
      "creditLimitIncluded": true,
      "referenceDate": "2019-02-22T00:00:00+01:00"
    },
    {
      "balanceAmount": {
        "amount": "8566.74",
        "currency": "SEK"
      },
      "balanceType": "InterimAvailable",
      "creditLimitIncluded": true,
      "referenceDate": "2019-02-22T00:00:00"
    }
  ]
}
```

7.5 Get transaction list of an account

The Operation will return the transactions for the account addressed by account-id. Transactions list reports depending on the parameter "booking-status" together with balances. For a given account, additional parameters are e.g. the attributes "date-from" and "date-to".

When calling to get a list of transactions you will receive a maximum of 50 transactions. If the chosen timespan has more than 50 transactions, a Next link will be shown that returns the following 50 transactions, and so on. See response example 6.6.3.

Note that there is no automatic switch back from mobile BankID to the TPP:s interface when signing the payment when using iOS devices. The PSU needs to manually switch from BankID the TPP:s interface.

GET /v2/accounts/{account-id}/transactions

7.5.1 Request description

Name	Type	Information
booking-status	String	In: query Required: true Description: Permitted codes are * "booked", * "pending". To get both booked and pending transactions you will need to call the operation twice. We are investigating supporting "both"-option.
date-from	string (date-time)	In: query Required: false Description: Starting date (including the date date-from) of the transaction list. For pending transactions, you cannot choose a past date since there are no pending transactions on earlier dates. If there is no date-to or date-from, the last 30 days of transactions are displayed from the current date if you are calling for booked transaction. We recommend always using both date-to and date-from to avoid confusion.
date-to	string (date-time)	In: query Required: false Description: End date (including the data date-to) of the transaction list. For booked transaction you cannot choose a future date since there are no booked transactions after the current date. If date-to is on a weekend the next weekday will also be shown in the response. This is because in our systems payments made on week-ends are not visible as booked, until the next banking day, even if funds are drawn from the account.
entry-reference-from	string	In: query Required: false Description: This data attribute is indicating that the AISP is in favour to get all transactions after the transaction with identification entry-reference-from alternatively to the above defined period. Transaction list response that exceeds the maximum number of results will contain a next link that should be used to request the next batch of data. The pagination token found in the query parameter entry-reference-from will be unique

		for each pagination window. If this data element is contained the entries date-from and date-to are ignored.
account-id	String	In: path Required: true Description: This identification is denoting the addressed account. The account-id is retrieved by using a "Read Account List" call.
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: he forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-IP-Address	String	In: header Required: recommended by Skandia Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU
PSU-IP-Port	String	In: header Required: recommended by Skandia

		Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Referer	String	In: header Required: recommended by Skandia Description: "Referer" header field sent by the PSU terminal when connecting to the TPP
PSU-TimeStamp	String	In: header Required: recommended by Skandia Description: Timestamp of the most relevant PSU's terminal request to the TTP
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available

7.5.2 Response description

Information for each transaction will differ depending on payment type.

Name	Type	Description
transactions	list	list of transactions for the given account
Account		
bban	String	Bban of the account
iban	string	Iban of the account
currency	string	Currency code of the account
Transactions		
booked	list	List of booked transactions (based on input parameter)
pending	list	List of pending transactions (based on input parameter)
Information	list	Information regarding recurring payments
transactions-id	string	The Id of the payment initiation request
entryReference	string	A reference based on execution date and time
endToEndId	string	The Id of the payment initiation request
TransactionAmount		
amount	string	
currency	string	
remittanceInformation Unstructured	string	Remittance information regarding the transaction
AdditionalInformationStructured		
startDate	String	The first applicable day of execution
frequency	String	monthly
endDate	String	The last applicable day of execution
executionRule	String	This data attribute defines the behaviour when recurring payment dates falls on a weekend or bank holiday.
Parameters of pending and booked list		
bookingDate	string	Date when entry was posted to the account
valueDate	string	Date when assets become available (credit)
Cross-border Payments		
creditorAgent	string	BIC code
debtorAgent	string	BIC code
debtorAgentProprietary	string	Bank code

7.5.3 Response body example

```
{
  "account": {
    "bban": "91598570120",
    "iban": "SE0791500000091598570120",
    "currency": "SEK"
  },
  "transactions": {
    "booked": [
      {
        "transactionId": "915088937100081@YGCB0169@2021-02-04@2021-02-04-19.27.40.805936",
        "entryReference": "2021-02-04-19.27.40.805936",
        "bookingDate": "2021-02-04T00:00:00+01:00",
        "valueDate": "2021-02-04T00:00:00+01:00",
        "transactionAmount": {
          "amount": "-200",
          "currency": "SEK"
        },
        "_links": {
          "transactionDetails": {
            "href":
"/ais/v2/accounts/915088937100081/transactions/915088937100081@YGCB0169@2021-02-04@2021-02-04-19.27.40.805936"
          }
        },
        "remittanceInformationUnstructuredArray": ["Överfört"]
      }
    ],
    "_links": {
      "account": {
        "href": "/ais/v2/accounts/915088937100081"
      },
      "next": {
        "href": "/ais/v2/accounts/915088937100081/transactions?booking-status=booked&entry-reference-from=SlCoJaCDV-qjwFhi98h_3Q.7VZEj6ysPjYtFV3p4Ido-V3hVyjC1nbTU9gvhwbgfIvsLENGjzvCdZRSBEedrWcwrKPegHalotbs-jXEuf5DDOnT30U1xgGcwc8fRLNgzvIaeCG1zuFuFdg3xw51mf1KWwxbmCw1ca4AnqTdM2vpsAke-q8-wpAw1pdAPMRtSZRUJ512erm08tZrQgLdqQ-wBXIU4fmRrJOjrNC9DG-ocQTa9XQ17uWTECctyWUcBoU"
      }
    }
  }
}
```

7.6 Get Transaction details

GET /v2/accounts/{account-id}/transactions/{transaction-id}/

7.6.1 Request description

Name	Type	Information
account-id	String	In: path Required: true Description: This identification is denoting the addressed account. The account-id is retrieved by using a "Read Account List" call.
transaction-id	String	In: path Required: true Description: This identification is given by the attribute transaction-id of the corresponding entry of a transaction list.
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: he forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE

PSU-IP-Address	String	In: header Required: recommended by Skandia Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Referer	String	In: header Required: recommended by Skandia Description: "Referer" header field sent by the PSU terminal when connecting to the TPP
PSU-TimeStamp	String	In: header Required: recommended by Skandia Description: Timestamp of the most relevant PSU's terminal request to the TPP
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available

7.6.2 Response description

Information for each transaction will differ depending on payment type.

Name	Type	Description
TransactionDetails		
transactionId	string	This identification is given by the attribute transaction-id of the corresponding entry of a transaction list.
entryReference	string	A reference based on execution date and time
endToEndId	string	The Id of the payment initiation request
Parameters of pending and booked transaction		
bookingDate	string	Date when entry was posted to the account
valueDate	string	Date when assets become available (credit)
TransactionAmount		
amount	string	
currency	string	
remittanceInformation Unstructured	string	Remittance information regarding the transaction
remittanceInformationStructuredArray		
reference	string	Remittance information regarding the transaction
AdditionalinformationStuctured -> StandingOrderDetails		
startDate	String	The first applicable day of execution
frequency	String	monthly
endDate	String	The last applicable day of execution
executionRule	String	This data attribute defines the behaviour when recurring payment dates falls on a weekend or bank holiday.
Cross-border Payments		
creditorAgent	string	BIC code
debtorAgent	string	BIC code
debtorAgentProprietary	string	Bank code
interbankSettlementDate	string	Execution date
regulatoryReportingCode	string	Payment tax code
AmountDetails		instructedAmount and transactionAmount
instructedAmount	string	
amount	string	
sourceCurrency	string	
targetCurrency	string	
exchangeRate	string	

7.6.3 Response example – pending transfer

```
{
  "transactionId": "957054871102373",
  "entryReference": "2021-02-04-19.27.40.805936",
  "bookingDate": "2030-02-02T00:00:00+01:00",
  "endToEndId": "0EAD3F14-35FB-4634-87F7-C48F26DCE42",
  "transactionAmount": {
    "amount": "7.07",
    "currency": "SEK"
  },
  "_links": {
    "transactionDetails": {
      "href": "/ais/v2/accounts/915088937100081/transactions/957054871102373"
    }
  },
  "remittanceInformationStructuredArray": [
    {
      "reference": "To Account Text"
    }
  ],
  "remittanceInformationUnstructuredArray": ["Message"]
}
```

8 PIS 3.0.0 - operations

8.1 Introduction

The PIS API is available for you to initiate payments.

Pre-requisites:

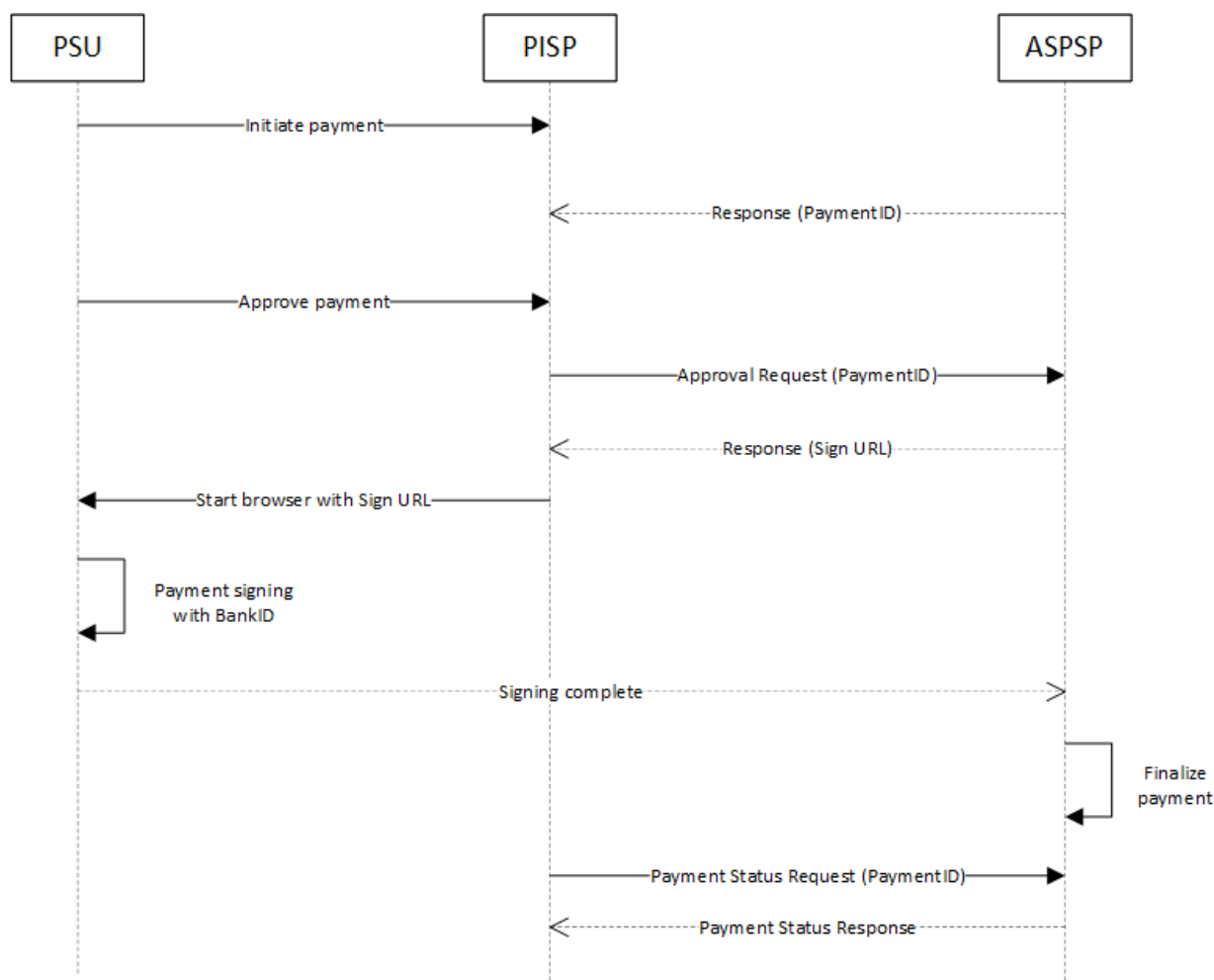
1. Have registered a user account in the portal
2. Have an app setup in the portal with an eIDAS-certificate of QWAC-type telling us you are an PISP

Please view the swagger file for more information.

8.2 Payment Initiation flow

Skandiabanken is using a two-step Payment flow. The first step is for the TPP to Initiate the payment. The TPP can then approve and confirm the payment directly or in a later stage. (But no later than 24 hours after initiating the payment. In that case a new payment must be initiated.)

It is a single sign SCA approach, which means the customers does not need to be identified by the bank before initiating the payment. Instead, identification occurs the same time as the signing of the payment.



8.3 Post Payment initiation request

The operation to initiate a payment is depending on the payment product in the path. We support request media type: application/json.

POST /{payment-service}/{payment-product}

8.3.1 Request description

Name	Type	Description
payment-service	String	In: path Required: true Description: Supported values for Payment Service is 'payments'
payment-product	String	In: path Required: true Description: Supported values for Payment Product is 'domestic transfer', 'giro payment'
Client-Id	String	In: header Required: true Description: The Client Id of the calling client
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-IP-Address	String	In: header Required: true Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP.
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia

		Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available

8.3.2 Body description, initiation of Domestic Transfer

Please view swagger file for details regarding formats.

Name	Type	Description
CreditorAccount		
Bban	String	Only supports Bban, not Iban. Clearing number 4-5 characters and account number 7-10 characters. When using Swedbank account, take away the fifth number in the clearingnr, the "9".
DebtorAccount		
Bban	String	You cannot have "-" in the number.
EndToEndIdentification	String	The Id of the payment initiation request, maximum of 35 characters
InstructedAmount		
Amount	Number	Minimum 1 SEK. Max 6 integers and 2 decimals. Example: "123.50"
Currency	String	ISO 4217 code for the currency. Supported values: "SEK"
RemittanceInformationStructuredArray		
reference	String	Max 12 characters can be used.
referenceType		Supports "PDTX" and "DPDT". PDTX is for reference to creditor account. DPDT is for reference to debtor account.
requestedExecutionDate	String	Required.

Example Body – Domestic Transfer

```
{
  "creditorAccount": {
    "bban": "91500053920"
  },
  "debtorAccount": {
    "bban": "91500053904"
  },
  "endToEndIdentification": "<Your text(maxlength 35)>",
  "instructedAmount": {
    "amount": "10.5",
    "currency": "SEK"
  },
  "remittanceInformationStructuredArray": [
    {
      "reference": "<PSU text(maxlength 12)>",
      "referenceType": "PDTX"
    }
  ],
  "requestedExecutionDate": "2024-06-15"
}
```

8.3.3 Body description, initiation of Giro Payment

Please view swagger file for details regarding formats.

Name	Type	Description
CreditorAccount		
giroNumber	String	Account number Identification represented by a GIRO number, only used in the creditor part.
giroType	String	Plusgiro or Bankgiro
DebtorAccount		
Bban	String	Either 'Bban' or 'Iban' must be provided. Not both You cannot have "-“in the number.
Iban	String	
EndToEndIdentification	String	The Id of the payment initiation request, maximum of 35 characters
InstructedAmount		
Amount	Number	Minimum 1 SEK. Max 6 integers and 2 decimals. Example: "123.50"
Currency	String	ISO 4217 code for the currency. Supported values: "SEK"
RemittanceInformationStructuredArray		
reference	String	OCR number: 3-25 characters
referenceType		SCOR; Payment reference to Creditor in GIRO OCR.
RemittanceInformationUnstructuredArray	String	Text to merchant: 1-25 characters
requestedExecutionDate	String	Required. If after 09:00, must be a future date.

Example Body – Giro Payment with message

```
{
  "creditorAccount": {
    "giroNumber": "235-9750",
    "giroType": "Bankgiro"
  },
  "debtorAccount": {
    "bban": "91598570120"
  },
  "endToEndIdentification": "<Your text (maxlength 35)>",
  "instructedAmount": {
    "amount": "10.5",
    "currency": "SEK"
  },
  "remittanceInformationUnstructuredArray": [
    "<Text to merchant, 25 characters>"
  ],
  "requestedExecutionDate": "2024-05-03"
}
```

Example Body – Giro Payment with OCR

```
{
  "creditorAccount": {
    "giroNumber": "901950-6",
    "giroType": "Plusgiro"
  },
  "debtorAccount": {
    "bban": "91598570120"
  },
  "endToEndIdentification": "<Your text (maxlength 35)>",
  "instructedAmount": {
    "amount": "10.5",
    "currency": "SEK"
  },
  "remittanceInformationStructuredArray": [
    {
      "reference": "<OCR number>",
      "referenceType": "Scor"
    }
  ],
  "requestedExecutionDate": "2024-05-03"
}
```

8.3.4 Body description, initiation of CrossBorderTransfers

Has not been released in this version yet.

8.3.5 Body description, initiation of Periodic Payments

Has not been released in this version yet.

8.4 Start the authorization process for a payment

POST /{payment-service}/{payment-product}/{payment-id}/authorisations

3.1.1 Request description

Name	Type	Description
PaymentService	String	In: path Required: true Description: Supported values for Payment Service is 'payments'
PaymentProduct	String	In: path Required: true Description: Supported values for Payment Product is Swedish 'domestic-transfer' or 'giro-payment'
paymentId	String	In: path Required: true Description: The id of the created transaction
Client-Id	String	In: header Required: true Description: The Client Id of the calling client
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-IP-Address	String	In: header Required: true Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia

		Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available
TPP-Nok-Redirect-URI	String	In: header Required: true Format: uri. Description: If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method.
TPP-Redirect-URI	String	In: header Required: true Format: uri. Description: URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Remark for Future: This field might be changed to mandatory in the next version of the specification
TPP-Redirect-Preferred	boolean	In: header Description: You must choose Redirect or Decoupled, but only redirect is the available choice at the moment. Decoupled will be available in the future.
TPP-Decoupled-Preferred	boolean	Not available at the moment.

8.4.1 Response example

```

{
  "scaStatus": "Started",
  "transactionStatus": "ACSP",
  "_links": {
    "scaRedirect": {
      "href": "/pis/v3/payments/domestic-transfer/915003010004026/authorisations"
    },
    "self": {
      "href": "/pis/v3/payments/domestic-transfer/915003010004026"
    },
    "status": {
      "href": "/pis/v3/payments/domestic-transfer/915003010004026/status"
    }
  }
}

```

8.5 Get Payment information

Returns the content of a payment initiation.

GET /{payment-service}/{payment-product}/{payment-id}

8.5.1 Request description

Name	Type	Description
PaymentService	String	In: path Required: true Description: Supported values for Payment Service is 'payments'
PaymentProduct	String	In: path Required: true Description: Supported values for Payment Product is Swedish 'domestic-transfer' or 'giro-payment'
paymentId	String	In: path Required: true Description: The id of the created transaction
Client-Id	String	In: Header Required: true Description: The Client Id of the calling client
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-IP-Address	String	In: header Required: true Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP.
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Accept	String	In: header

		Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU? TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available

8.5.2 Response description

Information about a payment.

Name	Type	Description
EndToEndIdentification	String	The Id of the payment initiation request
DebtorAccount		
Bban	String	
CreditorAccount		
Bban	String	
InstructedAmount		
Amount	Number	
Currency	String	ISO 4217 code for the currency. Supported values: "SEK"
RemittanceInformation Unstructured	String	Remittance information regarding the transaction
remittanceInformation Structured	String	Remittance information regarding the transaction
requestedExecutionDate	String	The date when the amount is requested to be drawn from the debtor account
transactionStatus	String	The status of the payment. Can be RCVD, ACSP, ACSC, PDNG, CANC or RJCT.

8.5.3 Response example

```
{
  "creditorAccount": {
    "bban": "91598616325"
  },
  "debtorAccount": {
    "bban": "91598570120"
  },
  "endToEndIdentification": "<Your text(maxlength 35)>",
  "instructedAmount": {
    "amount": "10.5",
    "currency": "SEK"
  },
  "remittanceInformationStructuredArray": [
    {
      "reference": "<PSU text(maxlength 12)>",
      "referenceType": "Pdtx"
    }
  ],
  "requestedExecutionDate": "2024-05-02",
  "transactionStatus": "RCVD"
}
```

8.6 Payment Cancellation Request

This method initiates the cancellation of a payment addressed by paymentId.

DELETE /{payment-service}/{payment-product}/{payment-id}

8.6.1 Request description

Name	Type	Description
PaymentService	String	In: path Required: true Description: Supported values for Payment Service is 'payments'
PaymentProduct	String	In: path Required: true Description: Supported values for Payment Product is Swedish 'domestic-transfer' or 'giro-payments'
paymentId	String	In: path Required: true Description: The id of the created transaction
Client-Id	String	In: Header Required: true Description: The Client Id of the calling client
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-IP-Address	String	In: header Required: true Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia

		Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available
TPP-Nok-Redirect-URI	String	In: header Required: true Format: uri. Description: If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method.
TPP-Redirect-URI	String	In: header Required: true Format: uri. Description: URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Remark for Future: This field might be changed to mandatory in the next version of the specification
TPP-Redirect-Preferred	boolean	In: header Description: You must choose Redirect or Decoupled, but only redirect is the available choice at the moment. Decoupled will be available in the future.
TPP-Decoupled-Preferred	boolean	Not available at the moment.

8.6.2 Response description

Status information about a cancellation payment initiation.

Name	Type	Description
TransactionsStatus	String	Status of the transaction. Which ever status the transaction has at the moment. Status does not change by initiating cancellation, only by signing cancellation.
_links		
scaRedirect.href	String	The SCA link
self.href	String	Link to get the transaction details
status.href	String	Link to get the status of the payment

8.6.3 Response example

```
{
  "scaStatus": "Started",
  "transactionStatus": "RCVD",
  "_links": {
    "scaRedirect": {
      "href": "/pis/v3/payments/domestic-transfer/915003010004026/authorisations"
    },
    "self": {
      "href": "/pis/v3/payments/domestic-transfer/915003010004026"
    },
    "status": {
      "href": "/pis/v3/payments/domestic-transfer/915003010004026/status"
    }
  }
}
```


8.7 Get Payment status request

Check the transaction status of a payment.

GET /{payment-service}/{payment-product}/{payment-id}/status

3.1.1 Request description

Name	Type	Description
PaymentService	String	In: path Required: true Description: Supported values for Payment Service is 'payments'
PaymentProduct	String	In: path Required: true Description: Supported values for Payment Product is Swedish 'domestic-transfer' or 'giro-payment'
paymentId	String	In: path Required: true Description: The id of the created transaction
Client-Id	String	In: Header Required: true Description: The Client Id of the calling client
X-Request-ID	string	In: header Required: true Format: uuid Description: ID of the request, unique to the call, as determined by the initiating party.
PSU-IP-Address	String	In: header Required: true Description: The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU
PSU-IP-Port	String	In: header Required: recommended by Skandia Description: The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available
PSU-Accept	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Charset	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Encoding	String	In: header Required: recommended by Skandia

		Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Accept-Language	String	In: header Required: recommended by Skandia Description: The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available
PSU-Device-ID	String	In: header Required: recommended by Skandia Description: UUID for a device, which is used by the PSU
PSU-Geo-Location	String	In: header Required: recommended by Skandia Description: The forwarded Geo Location of the corresponding http request between PSU and TPP
PSU-Http-Method	String	In: header Required: recommended by Skandia Description: HTTP method used at the PSU TPP interface, if available. Valid values are: * GET * POST * PUT * PATCH * DELETE
PSU-User-Agent	String	In: header Required: recommended by Skandia Description: The forwarded Agent header field of the HTTP request between PSU and TPP, if available

8.7.1 Response description

Status information about a payment initiation.

Name	Type	Description
fundsAvailable	boolean	
TransactionsStatus	String	Status of the transaction. Possible values [RCVD, ACSP, ACSC, PDNG, CANC, RJCT]

8.7.2 Response body example

```
{
  "fundsAvailable": true,
  "transactionStatus": "RCVD"
}
```

8.8 Create Signing Basket

Has not been released in this version yet.

8.9 Rules and different statuses for Payments

This section will contain information that is necessary for TPPs to create a good user experience around payments. Here are answers about when payments can be made and when those payments are booked and what status a payment gets in different situations.

8.9.1 Execution rules for payments

Product	Initiation Time	Execution Time
RequestedExecutionDate as current day on a business day		
Domestic-Transfer	Before 13:45	Same day (These transfers can not be cancelled.)
	After 13:45	Next business day. (These transfers can not be cancelled.)
Domestic-Transfer within Skandiabanken	Same day (regardless if business day or not). (These transfers can not be cancelled.)	
Giro-Payment	You can only choose same day as RequestedExecutionDay before 09:00. After that you must choose a later date. These transactions can be cancelled by PSU in other channels.	
Cross-border-transfers	1-2 days to EU/EES in Euros, 2-3 days to EU/EES in other currencies, 3-5 for other countries.	
RequestedExecutionDate on a non-business day		
Domestic -Transfer	As current date on a non-business day	Next business day. (These transfers cannot be cancelled.)
	On a business day	First business day after RequestedExecutionDate. (Transfers can be cancelled.)
Giro-Payment	Giro cannot be initiated with a RequestedExecutionDay that is on a non-business day	
Cross-border -transfers	Same as for business days.	

* If the recipient bank is located outside the EU / EEA, the bank cannot provide any guarantees regarding execution times for payment transactions.

8.9.2 Examples of status codes during different stages of PIS operation.

Operation	Day of initiation	Requested Execution Day	Status after Initiate	Status after approve & sign	Status booked transaction
Domestic -Transfer (same day)	Monday	Monday	RCVD	ACSC	ACSC
Domestic -Transfer (weekend)	Saturday	Saturday	RCVD	ACSC	ACSC. Funds transferred on Monday.
Domestic -Transfer (future)	Monday	Wednesday	RCVD	ACSP	ACSC
Domestic -Transfer (future weekend)	Monday	Saturday	RCVD	ACSP	ACSC. Funds transferred on Monday.

Giro-Payment (before 09:00 same day)	Monday	Monday	RCVD	ACSC	ACSC
Giro-Payment (weekend)	-	-	-	-	-
Giro-Payment (future)	Monday	Wednesday	RCVD	ACSP	ACSC
Payment cancellation	-----	-----	Current status	CANC	-----

Meaning of different statuses

- RCVD - Received - Payment initiation has been received by the receiving agent.
- ACSP -AcceptedSettlementInProgress - All preceding checks such as technical validation and customer profile were successful and therefore the payment initiation has been accepted for execution.
- ACSC - AcceptedSettlementCompleted - Settlement on the debtor's account has been completed.
- CANC – Cancelled – Payment has been cancelled and will not be executed.
- PNDG – Pending – A future payment did not have enough funds on the account on Requested Execution Day and a new try will be made.

9 Fallback Solution

Skandia allows TPPs to make use of the fallback solution (online bank) when the special interface does not meet all the requirements or if functions are temporarily out of order or have slow response times. You do not have to wait for information from us about incidents or deficiencies, you can use the backup solution when deficiencies occur. As a TPP, you are asked to report your use of the backup solution to us. Send an e-mail to openbanking@skandia.se. The backup solution consists of the bank's customer interface via so-called screen scraping or overlay.

The fallback solution will let you continue to provide services for account information and payment initiation to customers without any interruption. You can identify yourself in the fallback solution by the usage of signed headers, using the "Signing HTTP messages"-standard that is defined in "draft-cavage-http-signatures-10" by the HTTP Networking Group (<https://tools.ietf.org/html/draft-cavage-http-signatures-10>).

The solution requires you to provide an extra set of http headers to the first request towards login.skandia.se. The headers include:

- **TPP-Signature-Certificate**, your eIDAS QSEAL certificate that is to be used for signing the message. The certificate should be Base64-encoded in DER format (PEM format without the encapsulations BEGIN CERTIFICATE and END CERTIFICATE).
- **Signature**, a signature of the request as described in "draft-cavage-http-signatures-10".
 - *keyId* is always assumed to be the certificate provided in header *Tpp-Signature-Certificate*.
 - *algorithm* is used to specify the digital signature algorithm that was used when generating the signature. Allowed algorithms include SHA-256 and SHA-512.
 - *headers* should include at least '(request-target)', 'host' and 'date'.
 - *signature* contains the actual signature in base64 encoding.

Example:

```
GET
/?client_id=i_web_individual_short&redirect_uri=https%3A%2F%2Fsecure.skandia.se%2Foverview%2Fsigni
n-Skandia&response_type=... HTTP/1.1
Host: login.skandia.se
Date: Sat, 14 Sep 2019 00:00:00 GMT
Tpp-Signature-Certificate: MIIHoDCCBoigAwIBAgIKBilyT7rSIPwDBDANBgkqhkiG9w0BAQ...
Signature: keyId="tpp-signature-certificate",algorithm="rsa-sha256",headers="(request-target) host date",
signature="Base64(RSA-SHA256(signing_string))"
```

where **signing_string** is (\n is the ASCII-value for newline):

```
(request-target): get
/?client_id=i_web_individual_short&redirect_uri=https%3A%2F%2Fsecure.skandia.se%2Foverview%2Fsigni
n-Skandia&response_type=...\n
host: login.skandia.se\n
date: Sat, 14 Sep 2019 00:00:00 GMT
```

If you have questions about this don't hesitate to contact us at openbanking@skandia.se.