Frequently Asked Questions

General FAQs

1. Which markets are covered by the PSD2 APIs?

The APIs cover all European markets that N26 is present in.

2. Do the PSD2 APIs differ for retail and business accounts?

The same API implementation is used for retail and business accounts, and the APIs work the same for both.

3. Which type of certificate is needed to access the PSD2 APIs?

The PSD2 APIs can be accessed with a valid eIDAS QWAC certificate.

4. How can TPPs renew their certificates?

TPPs can renew their certificates by making a normal API call with the new certificate, in which the certificate will be onboarded automatically. Both the new and old certificate will be supported concurrently, and both can be used, until the old certificate expires.

Please note that if key TPP data (e.g. legal name, TPP number) will be different in the new certificate, TPPs will need to re-obtain authorisation tokens from PSUs for the new certificate.

5. How long is consent valid for?

For AIS requests, consent is valid for a maximum of 90 days, unless a shorter period is specified using the “validUntil“ parameter. Please note that a PSU has up to 5 minutes to confirm consent in the N26 app.

For PIS requests, access is only valid for 15 minutes and for one transaction. Please note that a PSU has up to 5 minutes to certify the payment in the N26 app.

6. Do the PSD2 APIs support one-time consents?

The PSD2 APIs support both one-time ("recurringIndicator": false) and recurring ("recurringIndicator": true) consents.

7. What is the maximum amount of transaction data that can be retrieved through the API?

Generally, transactions requests are limited to a period of 90 days from the time the request is made. The only exception to this limitation, applies during the first 15 minutes of an AIS consent lifecycle. In this time period, any transactions request made will not be limited. Moreover, requests made without specifying dateFrom and dateTo will return all transactions made since the account was created. After this time period, the above limitation will apply, and any requests trying to retrieve transactions older than 90 days will be rejected.

Please note our services use UTC timing, and keep this in mind when setting dateFrom and dateTo parameters.

8. Which currencies are supported for payments?

The Euro.

9. Are there minimum or maximum limits for payments?

Transaction limits are set by the customer.

10. What happens when an account is closed?

Response should be a 404 error, which indicates that the account could not be found (either because it has been closed, or because it does not exist).

Technical FAQs

1. I’m trying to connect to your APIs, but I receive a 401 “Unauthorized“ error

This could happen for a few reasons, such as:

- Incorrect certificate used (as our APIs can only be accessed with a valid eIDAS QWAC certificate)
- No certificated included in the authorization call (our oAuth/authorize end point includes certificate validation)
- client_id parameter does not match the organizationId field in your certificate

If you continue to face this error, and it is not caused by any of the above reasons, please reach out to us.

2. I received a 401 “Invalid token error“

This could indicate that the access token used in the call has been invalidated, which could be due to multiple refresh token calls, as each refresh token call invalidates the previous access token. Please be sure you are using the newest generated access token. If this is not the cause of your error, please reach out to us.

3. I received a 401 “Refresh token not found“ error

This indicates that the refresh token has been invalidated, which could happen for one of the following reasons:

- It expired after 90 days
- The PSU made a change to their core data (e.g. password, email, phone number)
- The PSU’s KYC status was reset

In this scenario, the PSU is required to re-log in. If this is something you would like us to look into, please reach out to us with the following information:

- Confirmation of how many PSUs are affected by the issue
- Confirmation of whether you received direct complaints from affected PSUs
- Any information you might have on whether the affected PSUs made any changes to their account
- If possible, request IDs of both failed attempts to refresh the access token (with this error) and previous successful attempts for the same affected PSU

4. I received a 429 “Too many requests“ error

It is likely that you have exceeded our rate limiting rules. While we do not publish our rate limiting policy, we have limits and quotas on our APIs, and rate limit according to user IP address, external IP address or certificate. Any changes to the rules **may only be considered** if we are confident that the activity does not negatively impact N26 or our customers. If this negatively affects your integration with us, please reach out to us and share more details on your needs, such as:

- External IPs used
- Requests per application per second or per hour etc