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).

11. What type of accounts are accessible through the API?

N26 customers have a main account and, depending on their membership, up to 10 additional sub-accounts which are called Spaces. Furthermore, N26 customers can enable a unique IBAN number for each sub-account, which is different to the IBAN number of the main account.

Please note that the main account and sub-accounts each have their own individual balances. More specifically, the main account balance **does not include** the balance(s) of the sub-account(s).

There is currently, unfortunately, no way to retrieve a customer's single total account balance through our API. To achieve this, we recommend retrieving the balance of the main account and each sub-account individually, and then aggregating them. The balance of Space(s) will be returned even in cases where N26 customers have chosen to "lock" a Space or "hide" the Space's balance in the N26 app.

12. Are AIS and PIS certificates interchangeable?

Please note that the end points that can accessed are dependent on the role stated in the QWAC certificate. A PIS certificate is required to access the PIS endpoints, and an AIS certificate is required to access AIS endpoints. This is true for all our interfaces; whether you wish to access the dedicated, fallback or sandbox interface. TPPs can possess an AIS certificate, a PIS certificate or both. Access and refresh tokens are also different depending on whether the call to the API is AISP or PISP.

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

5. I've noticed a transaction is "missing"

In some cases you may notice that a transaction is present in our response up to a certain date, after which it is "missing". This usually pertains to card transactions, and it is likely that the transaction has been hidden and replaced by another one. Please note that this takes place within the N26 app, and is not unique to our Open Banking implementation.

When a card purchase is made, typically:

1. The funds are initially reserved *authorisation* transaction (bank code: `PMNT-MCRD-UPCT`)
    a. Balance is impacted, although the funds have not yet left the customer's account
2. The merchant settles the claim and collects the funds *authorisation* transaction is hidden, and replaced by *presentment* transaction (bank code: `PMNT-CCRD-POSD`)
    a. Merchant has up to ~12 days to settle the claim
    b. No further balance impact

In some cases:

- The *authorisation* is cancelled by the merchant or it expires *authorisation reversal* or *authorisation expiry* transaction (bank code: `PMNT-MCRD-DAJT` for both)
    - Balance is impacted, and it appears as a "refund" in the transaction list

- The *authorisation* is higher than the actual purchase amount *authorisation reversal* transaction for the excess amount

Below are some examples with numbers:

Example 1: Customer purchases 12€ book from book store, and merchant settles claim			
What takes place	1. Funds are reserved		2. Merchant settles claim
Transaction list impact	-12€ *authorisation* transaction		~~-12€ *authorisation* transaction~~ *(hidden)* -12€ *presentment* transaction
Balance impact	-12€		0€
Example 2: Customer purchases 12€ book from book store, but merchant does NOT settle claim			
What takes place	1. Funds are reserved	2. *Authorisation* is reversed	
Transaction list impact	-12€ *authorisation* transaction	+12€ *authorisation reversal/expiry* transaction	
Balance impact	-12€	+12€	
Example 3: Customer rents electric scooter for 12€, but in the end the cost is only 8€			
What takes place	1. Funds are reserved	2. *Authorisation* is partially reversed (the excess)	3. Merchant settles claim (the actual cost)
Transaction list impact	-12€ *authorisation* transaction	+4€ *authorisation reversal* transaction	~~-12€ *authorisation* transaction~~ *(hidden)* ~~+4€ *authorisation reversal* transaction~~ *(hidden)* -8€ *presentment* transaction
Balance impact	-12€	+4€	0€

6. I've noticed duplicate transactions with different details

Since our change to bookingStatus made on 14 March 2022, you may notice duplicate transactions with different transactionIDs, booking and value dates. This usually pertains to card transactions.

As described in **technical FAQ #5**, when a card purchase is made, the first transaction is an *authorisation* transaction (e.g. which took place on 1st March 2022). This is then hidden and replaced by a *presentment* transaction which takes place at a later date (e.g. 3rd March 2022). These are treated as two separate transactions, and thus have different transactionIDs as well as bookingDate and valueDates. Thus, if you are seeing duplicate transactions with different details, you are most likely seeing both the *authorisation* and *presentment*.

Please note that once the *authorisation* transaction is hidden, it is no longer included in our API response and only the *presentment* transaction is shared.

7. I've noticed the date of a transaction provided in the response, is different to the date of the same transaction in the N26 app

In some cases you may notice that the date of a particular transaction in our response, appears different to the date of the same transaction in the N26 app. This usually pertains to card transactions.

As described in **technical FAQ #5**, when a card purchase is made, the first transaction is an *authorisation* transaction (e.g. which took place on 1st March 2022). This is then hidden and replaced by a *presentment* transaction which takes place at a later date (e.g. 3rd March 2022). Although, from 3rd March 2022, the transaction the customer sees in their transaction list is the *presentment* transaction, the associated date of the transaction does not change from 1st March 2022 to 3rd March 2022. This is to avoid confusing the customer, who is most likely more interested in the date the purchase was made, rather than the date the merchant settled the claim.

Please note that once the *authorisation* transaction is hidden, it is no longer included in our API response and only the *presentment* transaction is shared. Therefore, the transaction you observe in the response our APIs provide, with a different date, is most likely the *presentment* transaction - this can be confirmed by checking the transaction's bank code. Additionally, as our implementation provides transaction data as it is stored, our APIs will always return the accurate date of the transaction.