AUSTRIAN RAIFFEISEN BANKING GROUP

PSD2 API Portal

Portal information, API overview and technical integration guide

REGULATORY FRAMEWORK

Information for the use of the Internet Portal established by the Austrian Raiffeisen Banking Group according to Art 30 (5) Commission Delegated Regulation (EU) 2018/389.

INSIDE THIS DOCUMENT

01 **Summary and Conditions**
Portal use, testing environment and responsibilities

02 **Available APIs**
Account information, payment initiation and confirmation of funds

03 **How to call our APIs**
Certificate validation, OAuth token and API requests

04 **FAQs**
Certificate renewal, company changes and client IDs

01 TERMS OF USE

Summary and Conditions

The following conditions apply to registration for and use of the Portal and its Testing Environment.

01 On behalf of the banks being member of the Austrian Raiffeisen Banking Group (altogether: "RBG") Raiffeisen e-force GmbH, Friedrich-Wilhelm-Raiffeisen-Platz 1, 1020 Wien ("Portal Operator") operates the Portal for the purposes of Art 30 Commission Delegated Regulation (EU) 2018/389 ("Regulation").

02 Full documentation of the technical specification ("Specification") of all interfaces operated by RBG for the purposes of Art 30 of the Regulation (altogether: "RBG Interface") is made available upon request and free of charge to payment initiation service providers, account information service providers, payment service providers issuing card-based payment instruments and payment service providers that have applied to their competent authorities for the relevant authorization after their registration in the Portal (altogether: "registered TPP"). A summary of the Specification is available.

03 Registered TPP may use the testing environment provided in the Portal ("Testing Environment") for testing the connectivity and functionality of their software and applications towards RBG Interface to the extent required by Art 30 (5) of the Regulation. Such testing activities shall neither include direct nor indirect personal data nor any data of real transactions or accounts.

04 Except for emergency situations registered TPP will be informed about any change to the Specification and in the Testing Environment in advance as soon as possible and not less than 3 months before the change is implemented. In emergency situations this information will be provided as soon as feasible prior to or after implementation of the change.

05 Access to the Portal and usage of the Testing Environment may be restricted for the time needed for maintenance work. If possible, such restriction will be made known to registered TPP in advance through an announcement in the Portal.

06 The Portal Operator may terminate a registered TPP access to the Portal if its activities in the Portal and the Testing Environment seriously endangers security and continuity of services provided in the Portal or availability of these services for other registered TPP.

07 To the extent permitted by law, the Portal Operator is not responsible for damage suffered by a registered TPP on the occasion of the access to the Portal or due to the use of the testing environment.

08 The identification credentials assigned to a registered TPP during its registration for access to the Portal must be kept secret and must not be disclosed to any unauthorized third party.

09 Information provided by the registered TPP for its registration will be processed by the Portal Operator for verifying the registered TPP registration and permission to use the Portal, tracking the use of the Portal to ensure the security and continuity of services provided therein and contacting the registered TPP with the information about the Portal and available services (eg. new services, customer experience and satisfaction, or planned availability restrictions). Additional information on data protection issues are available.

02 API CATALOGUE

Available APIs

Three interfaces are available to eligible third-party providers under the Berlin-Group NextGenPSD2 Framework.

01 Account information

This API allows approved Account Information Service Providers (AISPs) to request access to Payment Accounts from a PSU.

KEY FEATURES

- Create an "account information consent" resource for a list of accounts and request an SCA from the PSU.
- Account information consents are valid up to 90 days
- Consent is requested from the customer via Redirect and SCA
- Get access to account details, balances and transactions
- This API is developed according to specifications of the Berlin-Group NextGenPSD2 Framework

LIVE API ACCESS To Access the Live API an eIDAS QWAC certificate according to PSD2-Regulation with the roles AISP or ASPSP is required.

02 Payment initiation

Allows approved payment initiation service providers (PISPs) to initiate a transaction and request an authorization from the PSU.

KEY FEATURES

- Supported Payment Formats: SEPA credit transfer, Instant Payments and others
- Supported Payments: Recurring Payments and Future Dated Payments
- Let the customer sign the payment with Strong Customer Authentication
- This API is developed according to specifications of the Berlin-Group NextGenPSD2 Framework

LIVE API ACCESS To Access the Live API an eIDAS QWAC certificate according to PSD2-Regulation with the roles PISP or ASPSP is required

03 Confirmation of funds

This API allows approved Card Based Payment Instrument Issuers (CBPIIs) to securely check if funds are available in a specific account.

KEY FEATURES

- Create a "funds confirmation consent" resource for a specific account and request an SCA from the PSU.
- Make requests to confirm if funds are available in the account
- Funds Confirmation consents do not have any limitation on the validity period.
- This API is developed according to Specifications of the Berlin-Group NextGenPSD2 Framework

LIVE API ACCESS To Access the Live API an eIDAS QWAC certificate according to PSD2-Regulation with the roles CBPII, PISP or ASPSP is required

03 TECHNICAL INTEGRATION

How to call our APIs

According to the Berlin Group´s NextGenPSD2-Standard, Third Party Providers (TPPs) are attributed the OAuth-role "client". As set out from the Internet Engineering Task Force, the "Client Credentials Grant" is used to generate an access token.

01 Certificate & Client-ID	**02** OAuth access token	**03** API call

Step 1 | Validate the eIDAS QWAC certificate

You will have to call the first-contact endpoint once to receive a Client-ID. This step also ensures that your eIDAS certificate is valid. You can send this request multiple times - as long as your certificate's subject DN does not change, you will receive the same Client-ID.

Certificate requirement: Please note that our APIs only support certificates with a maximum key length of 2048 bits.

EXAMPLE CURL REQUEST

```
curl -X POST "https://psd2.raiffeisen.at/api/psd2-xs2a/first-contact/" \
  -H "Content-Type: application/json" \
  -H "Cache-Control: no-cache" \
  --cert "/path/to/cert.pem" \
  --key "/path/to/key.key"
```

EXAMPLE RESPONSE

```
{
  "clientId": "API-7d6f204b-3219-4b63-b66e-5f7a0be1d067"
}
```

Step 2 | Obtain an OAuth access token

Once you have obtained a Client-ID you can retrieve an access token.

EXAMPLE CURL REQUEST

```
curl -X POST "https://sso-psd2.raiffeisen.at/as/token.oauth2" \
  -H "Content-Type: application/x-www-form-urlencoded" \
  -H "Cache-Control: no-cache" \
  --cert "/path/to/cert.pem" \
  --key "/path/to/key.key" \
  -d "grant_type=client_credentials&client_id=API-7d6f204b-3219-4b63-b66e-5f7a0be1d067&scope=apic-psd2"
```

EXAMPLE RESPONSE

```
{
  "access_token": "kUNrj52ZqpXpYstVfmPU9Iv9Igiz",
  "token_type": "Bearer",
  "expires_in": 599
}
```

03 TECHNICAL INTEGRATION / CONTINUED

Step 3 | Make authenticated API requests

For all subsequent calls to our APIs you have to transmit the generated Access Token in the "Authorization: Bearer" header field. In the example below a request to the accounts endpoint is made.

EXAMPLE CURL REQUEST

```
curl -X GET "https://psd2.raiffeisen.at/api/psd2-xs2a/rest/v1/accounts" \
  -H "Authorization: Bearer kUNrj52ZqpXpYstVfmPU9Iv9Igiz" \
  -H "X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721" \
  -H "Consent-ID: e6151d43-dca8-4fe1-b139-3a89bfeb57a2" \
  -H "Cache-Control: no-cache" \
  --cert "/path/to/cert.pem" \
  --key "/path/to/key.key"
```

04 SUPPORT INFORMATION

Frequently asked questions

Q01 Our certificate will expire soon, do we need to inform Raiffeisen about the new certificate?

If only the key is renewed and thus the validity is extended you can use the new certificate without any additional steps and without informing us. It is a good idea to call the first-contact Endpoint again, which should result in the same client-id for the new certificate. If the fields in the certificate are different the first-contact will result in a new client-id.

Q02 Our company has a new name or has merged with another company, do we need to inform Raiffeisen about this?

If your company has changed its name, then most likely the "subject" field will be different for any new certificates. If the fields in the certificate change you will need to call the first-contact Endpoint again to get a new client-id. With a new client-id all old consents will have to be renewed. We cannot check if the old and new company are the same legal entity, so customers will need to give their consent again to access their accounts.

Q03 In case the first-contact returns a new client-id are services going to be disrupted or are both the old and new client-id going to be working?

Both client-ids will continue to work as long as the corresponding certificates are valid. Please be aware, that consent's are always tied to a client-id and thus consents from the old client-id are not available on the new client-id. With a new client-id all old consents will have to be renewed.