

Consent authorization using Postman

1. Execute “POST /resource/v1/api/consents” endpoint. You will get a consent object in JSON format as a response.

Params:

- SwaggerClient = Application Key;
- X-Request-ID = ID of the request, unique to the call, as determined by the initiating party;
- PSU-IP-Address = The forwarded IP Address header field consists of the corresponding http request IP Address field between PSU and TPP.

Body:

```
{
  "access": {
    "accounts": [],
    "balances": [],
    "transactions": []
  },
  "recurringIndicator": "true",
  "validUntil": "",
  "frequencyPerDay": "",
  "combinedServiceIndicator": "false"
}
```

2. As a next step, created consent need to be authorized.

To start authorization process, PSU must be redirected to URL formatted according to OAUTH2 specification:

https://<URL>/auth/oauth2/authorize?response_type=code&client_id=<TPP_KEY>&redirect_uri=<REDIRECT_URI>&scope=AISP%3A<CONSENT_ID>&state=<RANDOM_NUMBER>

Params:

- response_type = code;
- <TPP_KEY> = Application key;
- <REDIRECT_URI> = Application redirect URL;
- <CONSENT_ID> = Consent id received in previous step;
- <RANDOM_NUMBER> = random number (request ID).

Example:

https://{host}/auth/oauth2/authorize?response_type=code&client_id=9304aae0-8b50-477a-afff-e9f6697a7b47&redirect_uri=http://test1748.lv&scope=AISP%3A8f1d0343-7866-4e36-824d-334dcf31ddd0&state=587454

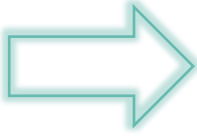
3. Go through Internetbank authorization process:

Welcome to internetbank

User ID (any 6 digits)

Password (123456)

Login >



Welcome to internetbank

Mobile Digipass

Authorization code (123456)

Login >

4. Select client accounts, enter authorization code and press “Send”.

Izvēlēties visus

Kontu informācija:

- LV16MULT000000000000005
- LV27MULT000000000000001
- LV43MULT000000000000004
- LV70MULT000000000000003
- LV70MULT000000000000003
- LV97MULT000000000000002

Atlikumi:

- LV16MULT000000000000005
- LV27MULT000000000000001
- LV43MULT000000000000004
- LV70MULT000000000000003
- LV70MULT000000000000003
- LV97MULT000000000000002

Transakcijas:

- LV16MULT000000000000005
- LV27MULT000000000000001
- LV43MULT000000000000004
- LV70MULT000000000000003
- LV70MULT000000000000003
- LV97MULT000000000000002

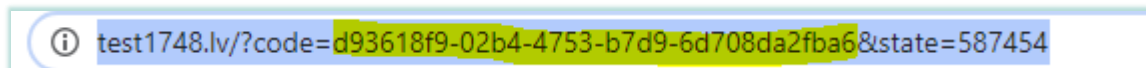
Autorizācijas kods (123456)

Autorizācijas rīka numurs *

FDM1802654

Nosūtīt >

5. After account selection you will be redirected to the redirect URL with code. This code will be used to get token.



6. To get token must be called "POST <https://{host}/auth/oauth2/token>" endpoint.

Params:

- grant_type = authorization_code;
- redirect_uri = Application redirect URL;

- code = code received in previous step;
- client_id = Application key;
- client_secret = Application secret.

Response example:

```

1  {
2    "scope": "AISP:8f1d0343-7866-4e36-824d-334dcf31ddd0",
3    "access_token": "a0ff1824-683d-4037-bd97-945bc11cf82e",
4    "token_type": "bearer",
5    "expires_in": 7776000
6  }

```

7. Now we can use received token to get information about accounts, balances etc.

Authorization type OAuth 2.0.

Params ● Authorization ● Headers (12) Body Pre-request Script Tests Settings

TYPE
OAuth 2.0

The authorization data will be automatically generated when you send the request. [Learn more about authorization](#)

Add authorization data to
Request Headers

Preview Request

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about](#)

Access Token
a0ff1824-683d-4037-bd97-945bc11cf82e
Get New Access Token

Params:

- Access Token = token received in the previous step.

GET https:// {host} /resource/v1/api/accounts?withBalance=true

Params ● Authorization ● Headers (12) Body Pre-request Script Tests Settings

▼ Headers (3)

KEY	VALUE
<input checked="" type="checkbox"/> X-Request-ID	{{ \$guid }}
<input checked="" type="checkbox"/> Consent-ID	8f1d0343-7866-4e36-824d-334dcf31ddd0
<input checked="" type="checkbox"/> SwaggerClient	9304aae0-8b50-477a-aff-e9f6697a7b47
Key	Value

► Temporary Headers (9) ⓘ

Params:

- SwaggerClient = Application Key;
- X-Request-ID = ID of the request, unique to the call, as determined by the initiating party;
- Consent-ID = Consent ID received in 1. step.