API AUTHENTICATION

1. Introduction

To access private API:s at the Riksbank, you (the reporting agent) must provide a valid access token in your requests.

Example:

```
curl -X POST https://api-gw-test.riksbank.se/demo-api \
-H "Authorization: Bearer $access_token" \
```

To retrieve a valid bearer token, this must be configured.

- If you are using Entra, see section 3.
- For any other OIDC Discovery compatible IdP, see section 4.

Disclaimer: The api-test_scope given under “references” is subject to change in later versions of this document.

2. References

- test_login_url=”https://login.microsoftonline.com/ e4f5c9c2-409e-4eb2-be12-d4659315aee0/oauth2/v2.0/token
- `api-test_scope=”api://a1aa0827-a7a1-481a-9aa0-a60583065aa5/.default”`

3. Using Microsoft Entra

The client (reporting agent) must do an “App registration” in Azure Entra and provide the Riksbank with the application (client) Id of the registered app.

Specify https://localhost as redirect URI for your app (you can have other redirect URI:s specified for your own usage).

For help creating an app registration:
How to register an app in Microsoft Entra ID - Microsoft identity platform | Microsoft Learn

When you have provided information about application (client) Id to the Riksbank, we will register your app as eligible to use resources in our environment. When this is done, you can retrieve valid tokens from Entra, e.g:

```
token_response=$(curl -X POST $test_login_url \
-H "Content-Type: application/x-www-form-urlencoded" \
-d "client_id=$client_id" \
-d "client_secret=$client_secret" \
-d "scope=$api-test_scope" \
-d "grant_type=client_credentials")

access_token=$(echo "$token_response" | jq -r '.access_token')
```

In the above example, `client_id` is the application id of your registered app and `client_secret` is your own created secret for this app (if this method is used on the client end). The `test_login_url` and `api-test_scope` are found above under “references”.

4. Using Workload Identity Federation

1) Inform the Riksbank about your Issuer’s OIDC Discovery-endpoint URI (.well-known endpoint) and the subject (sub claim) that will be used in your issued tokens.
2) The Riksbank will then provide you with a client_id for which you should be able to exchange your issued tokens for valid tokens to authenticate to our API.

Token exchange example:

```
curl -X POST \
  -H "Content-Type: application/x-www-form-urlencoded" \
  -d "scope=$api-test_scope" \
  -d "client_id=$client_id" \
  -d "client_assertion_type=urn:ietf:params:oauth:client-assertion-
type:jwt-bearer" \
  -d "client_assertion=$access_token" \
  -d "grant_type=client_credentials" \
  $test_login_url
```

In the above example, `access_token` is the token issued by your IdP. This token must contain the audience `(aud)` claim “`api://AzureADTokenExchange`” and the issuer `(iss)` and subject `(sub)` claims provided to the Riksbank in step 1. The `test_login_url` and `api-test_scope` are found above under “references”.