**Playing with APIM policies (30’)**

In this exercise, you will play with APIM policies.

Follow the the below steps:

* Create an API using your firstname
* Use your trigram as API suffix (ie: for me sey)
* Create an operation called “test”
* Create an operation called “healthz”
* Both operations must return an empty response with 200 result code.

Test already that both operations work at this stage.

Now, using Fiddler or Postman or whatever you want, grab a token using the following HTTP payload:

POST https://login.windows.net/ceaabb16-9554-4ac1-98bb-0e2fa69a9425/oauth2/token

resource=api://711fccca-69f5-4ece-a7a3-32521be46f45

&client\_id=711fccca-69f5-4ece-a7a3-32521be46f45

&grant\_type=client\_credentials

&client\_secret=X-08Q~7MCaN-ROsI498fhB4xrMhm9BDKfNm5BcCV

To complete the exercise:

* Analyze the token to figure out the next steps
* Add an **API-level** JWT validation policy, which validates the following:
  + That the token has not expired
  + The issuer
  + The audience

Because the healthz operation is called by load balancers that have no way to grab a token, make sure to make it available using the subscription key only through the query string and that it should not require the token.

Because the target API will be consumed by multiple client systems, make sure that a given client cannot make more than 10 calls per minute.

To test your API works correctly, grab another token with the following payload:

POST https://login.windows.net/ceaabb16-9554-4ac1-98bb-0e2fa69a9425/oauth2/token

resource=api://711fccca-69f5-4ece-a7a3-32521be46f45

&client\_id=d17fe98b-c493-4b76-a270-592a8884fb9b

&grant\_type=client\_credentials

&client\_secret=hj88Q~SKVpn1H5moeN5IMm90GIuHURvGJl12yaKs

If your setup is correct, one token could not be used more than 10 times per minute, while the other token should still be usable.

Tips:

* You’ll have to grab the well known OIDC endpoint of my tenant
* You’ll have to break policy inheritance
* You’ll have to make use of the following 3 policies:
  + return-response
  + validate-jwt
  + rate-limit-by-key