Google Cloud

Edge Microgateway

Security

Agenda

- Edge Microgateway Security
  - OAuth 2.0
    - API Key Validation
    - JWT Access Token Validation - Client Credentials grant

OAuth 2.0

- OAuth 2.0 is delegated authorization framework that allows a third-party application to access a user's data.
- There are four grant types:
  - Resource Owner Password Credentials
  - Client Credentials
  - Implicit
  - Authorization Code

Which grant types does Edge Microgateway support?

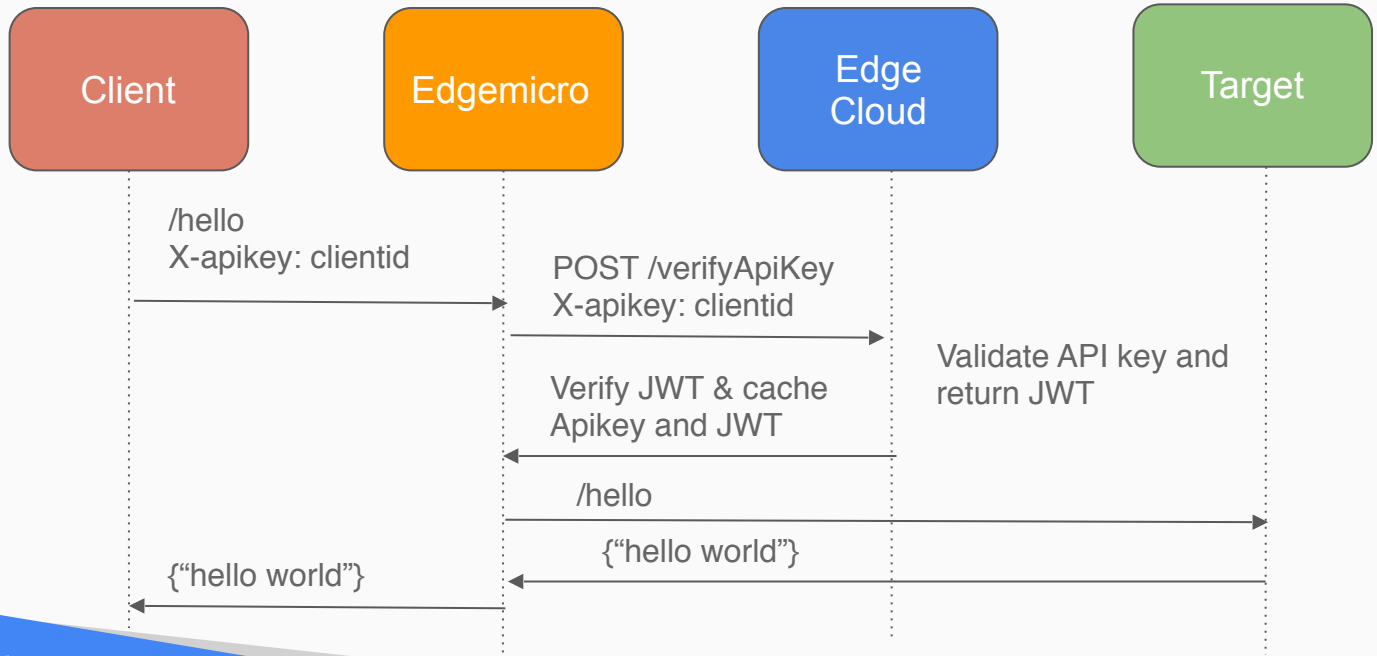
- API Key Validation - enabled OOTB
- Client Credentials - enabled OOTB
- Password Grant is also supported, but user has to implement it within the edgemicro-auth proxy

How is the JWT generated?

- Edgemicro configure command generates public/private key which are stored in Apigee Edge
- edgemicro-auth proxy generates the JWT and signs it with the private key stored in Apigee Edge
- JWT is not encrypted so anyone that obtains the JWT can read the contents
- JWT expires in 15 minutes, but this value can be changed in the edgemicro-auth proxy

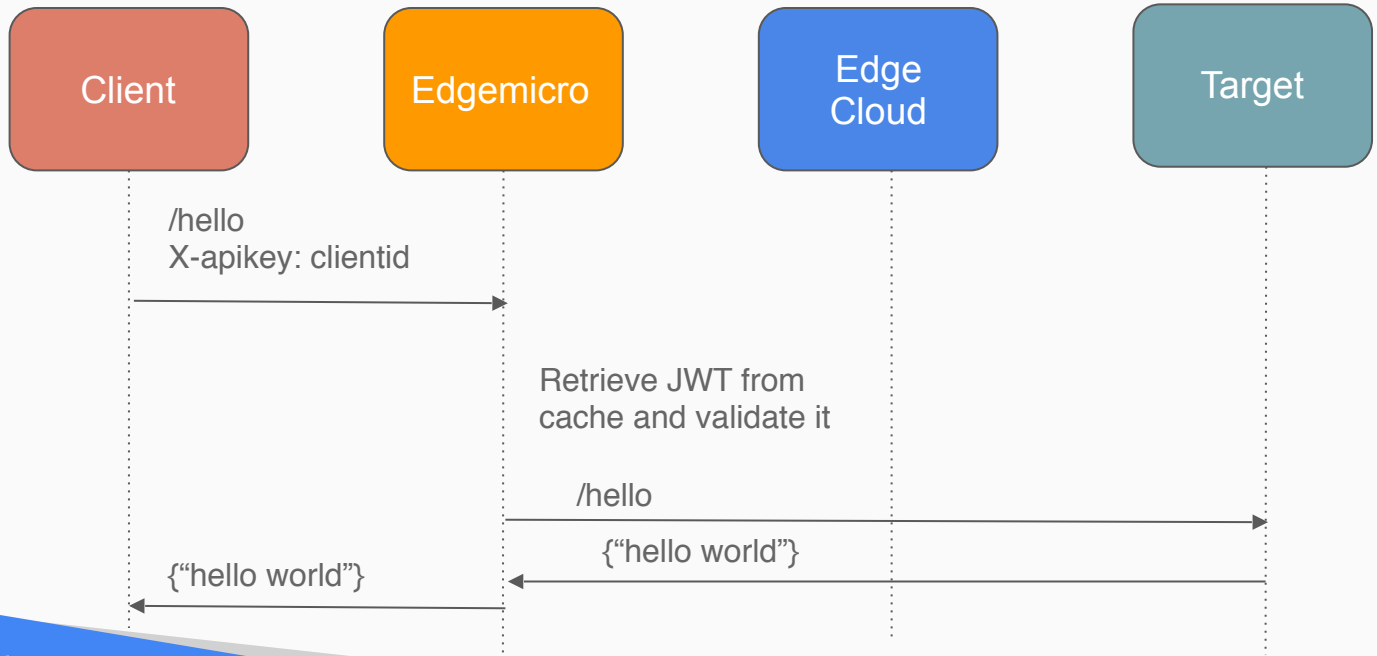
API Key Validation - Initial Request

- API Key Validation
  - Submit requests with just the API key (client ID)
  - Edgemicro exchanges the API key for a JWT

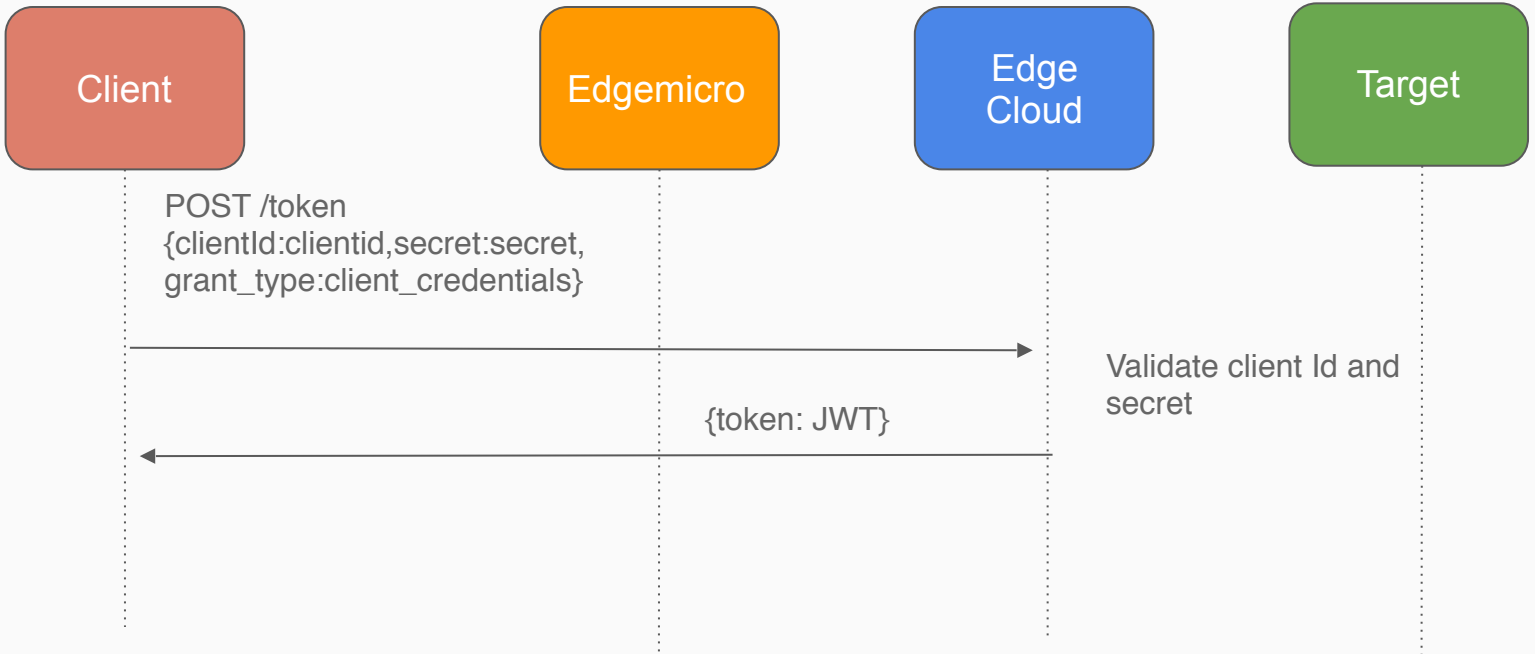


API Key Validation - Subsequent Requests

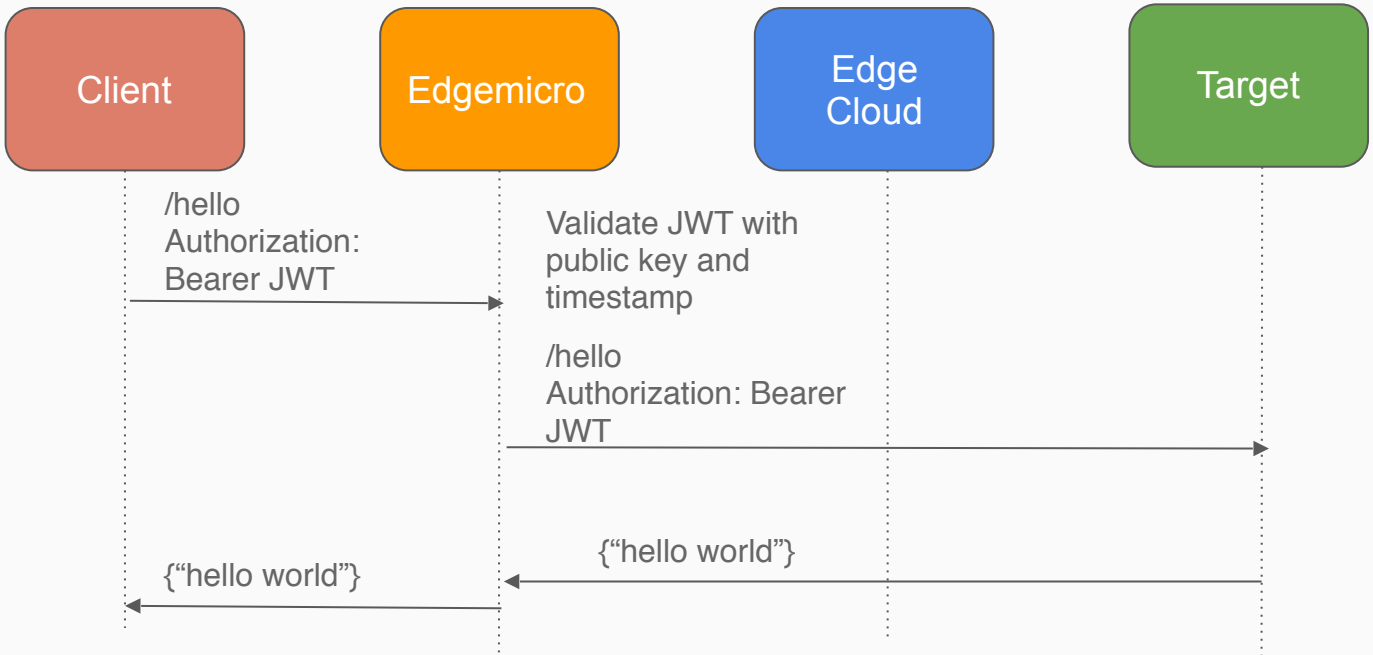
Subsequent requests are validated from the cached access token



Client Credentials - Token Request



Client Credentials - Subsequent Requests



THANK YOU

Target Server Setup

- If the target server is running on same VM as Edge Microgateway
  - Configure firewall to prevent access to target server port
  - Sample Github Repo

- If the target server is running on separate VM
  - Configure firewall to only allow access to target via Microgateway IP/port
  - Sample Github Repo