Creating a microservice app with Shuttle

… well, how to guard access with JWTs

About me

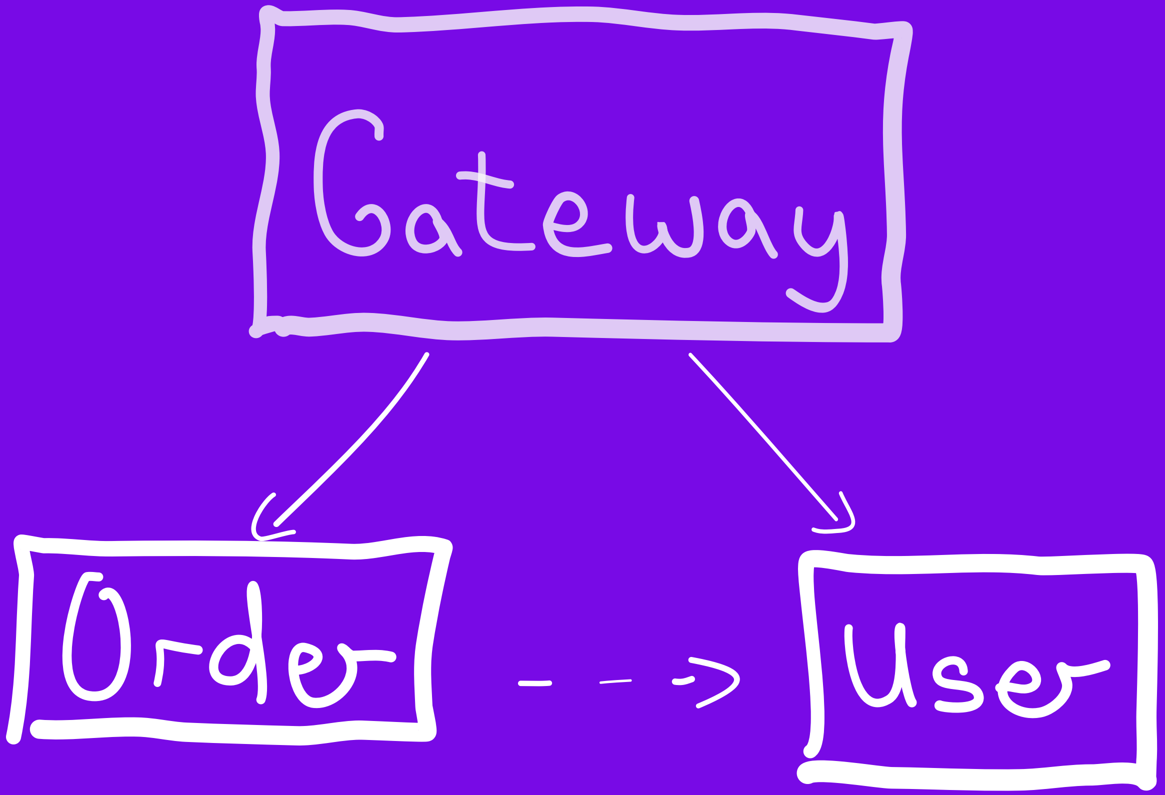
- Pieter Engelbrecht
- But known as **chesedo** on online forums
- Tech lead at **Shuttle**

Layout

Interactive tutorial

Interleave theory

Ask questions at any time



- Gateway
  - /order -> Order service
  - /user -> User service

What is a JWT anyway?

Is used for authorization

JSON Web Token is made up of 3 parts:

1. Header
2. Payload
3. Signature (base64(header) . base64(payload))

Header

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

Payload

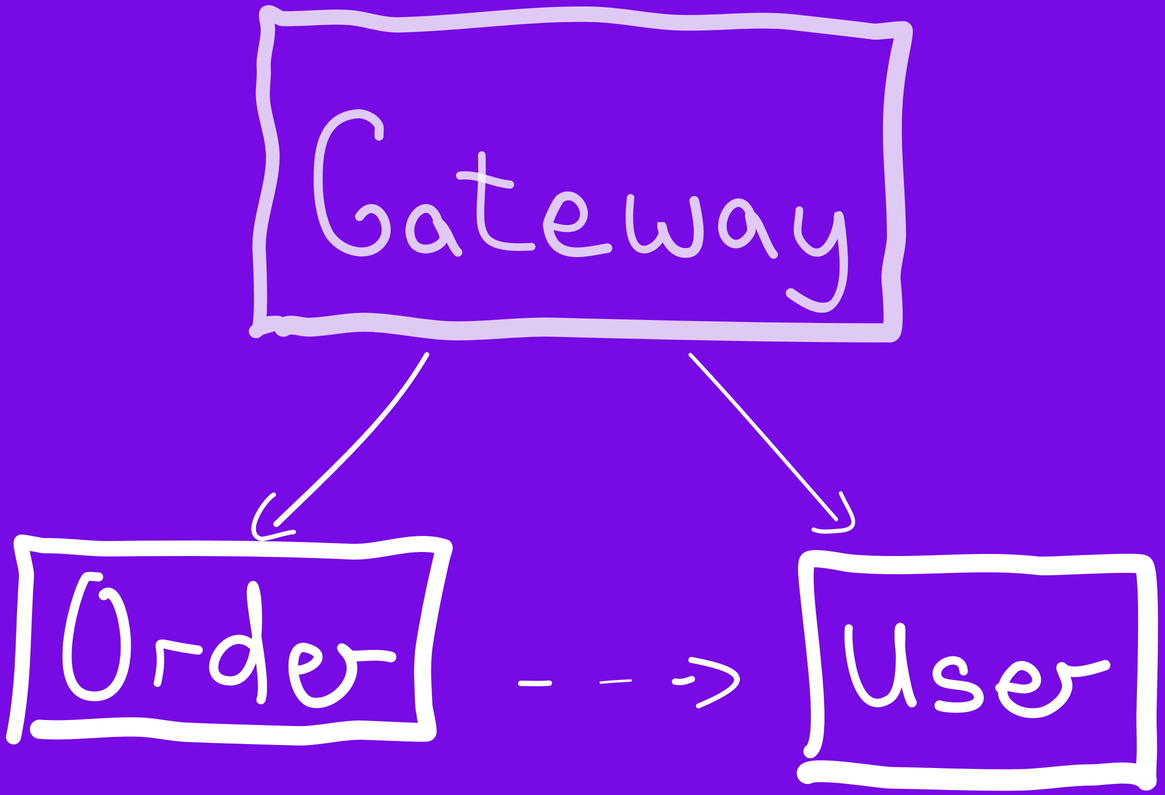
```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

Signature

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwib
mFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ =>
XbPfbIHMI6arZ3Y922BhjWgQzWXcXNrz0ogtVhfEd2o

Payload fields

- Registered (RFC 7519)
  - iss = Issuer
  - sub = Subject
  - aud = Audience
  - exp = Expiration Time
  - nbf = Not Before
  - iat = Issued At
  - jti = JWT ID
- Public
- Private



- Gateway
  - /order -> Order service
  - /user -> User service

Best practices

Keep the payload compact

Short expiry

Don't have sensitive information in the payload

Don't send the token in the request params

Not ideal for session management

Questions?