Open ID Connect

KAROL BULER

Zielona Góra, 26.04.2017

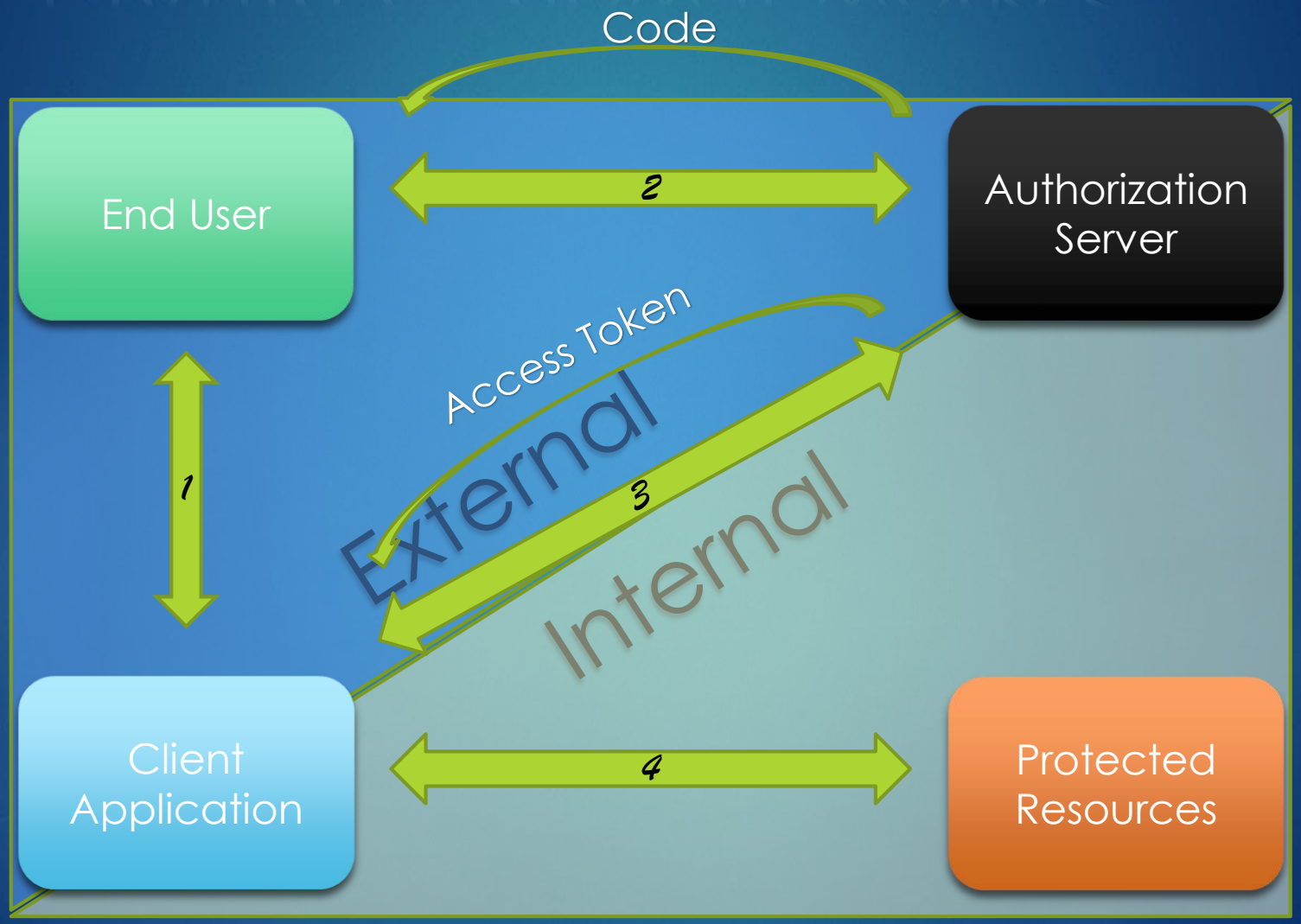
Agenda

- OAuth 2
- Differences between OAuth2 and Open ID Connect
- Authorization flows
- Good known implementations in Java
- Keycloak + live demo
- You are probably use it
- Advantages and disadvantages

OAuth2 – what it is?

- A simple open standard for secure authorization
- Easy to implement security in different types of applications
- Easy to understand by the users
- Developers don't need to handle authorization
- Username and password are not needed

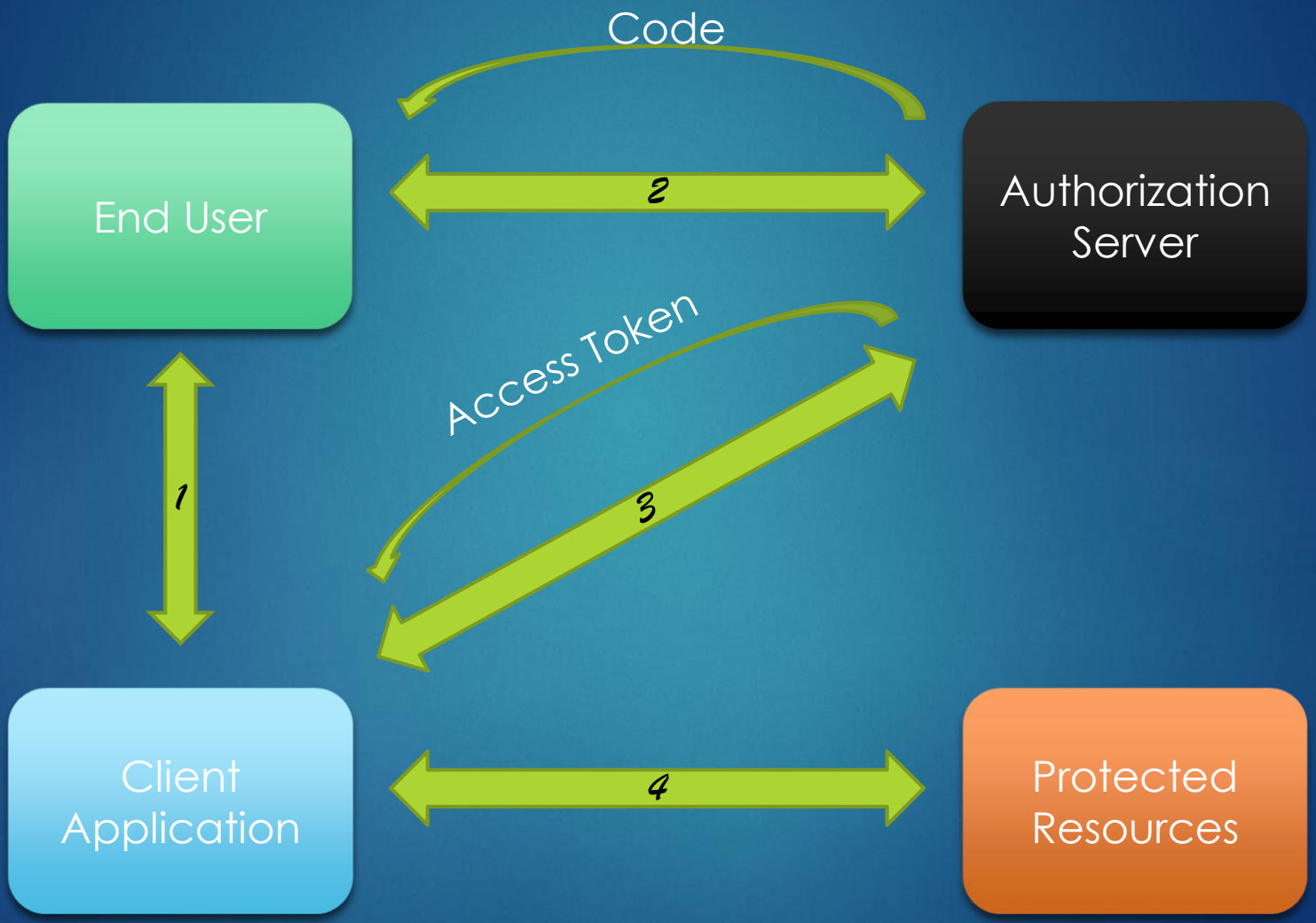
OAuth2 – how it works?



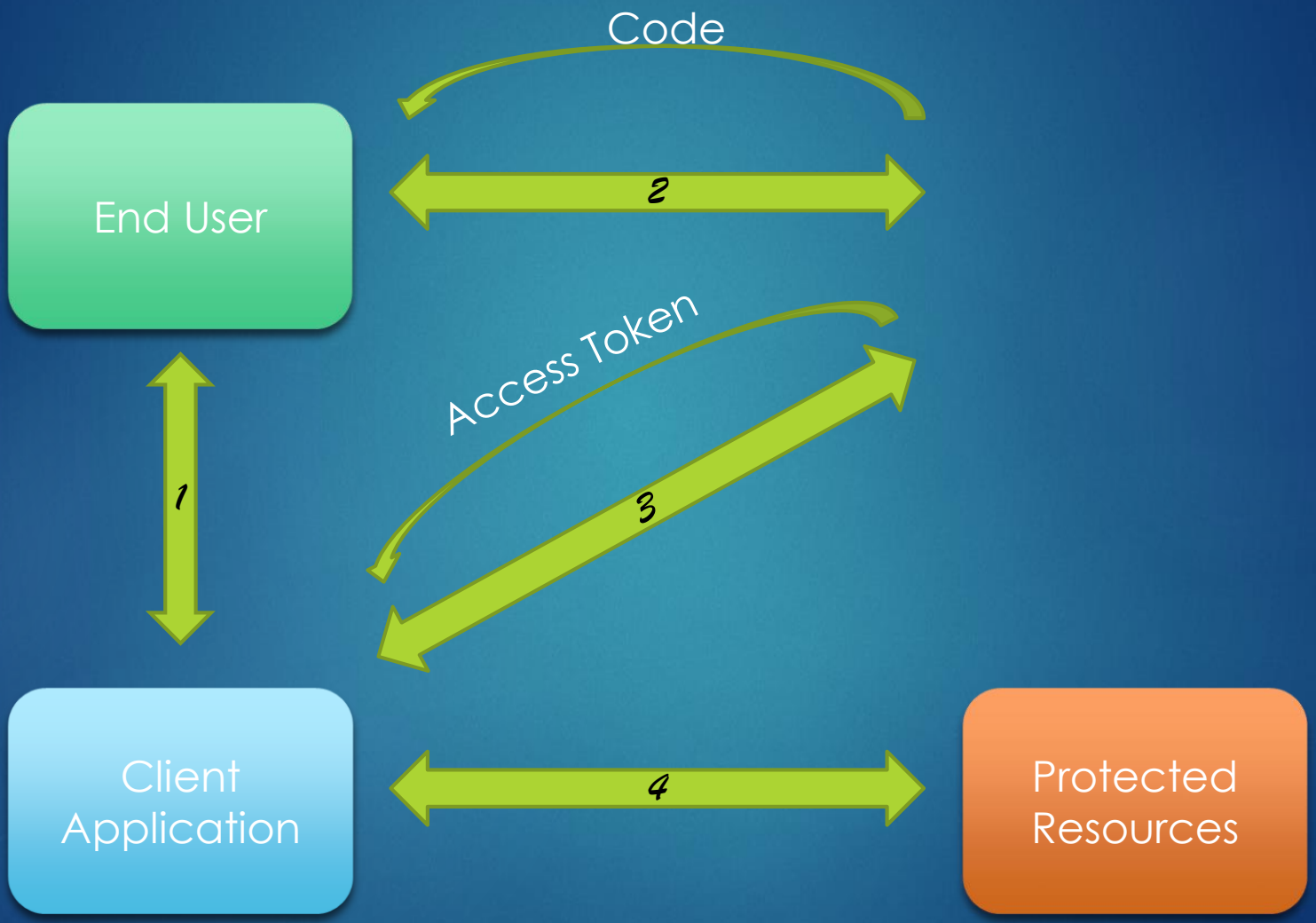
What OAuth does not tell you

- Who the user is
- If the user is still there

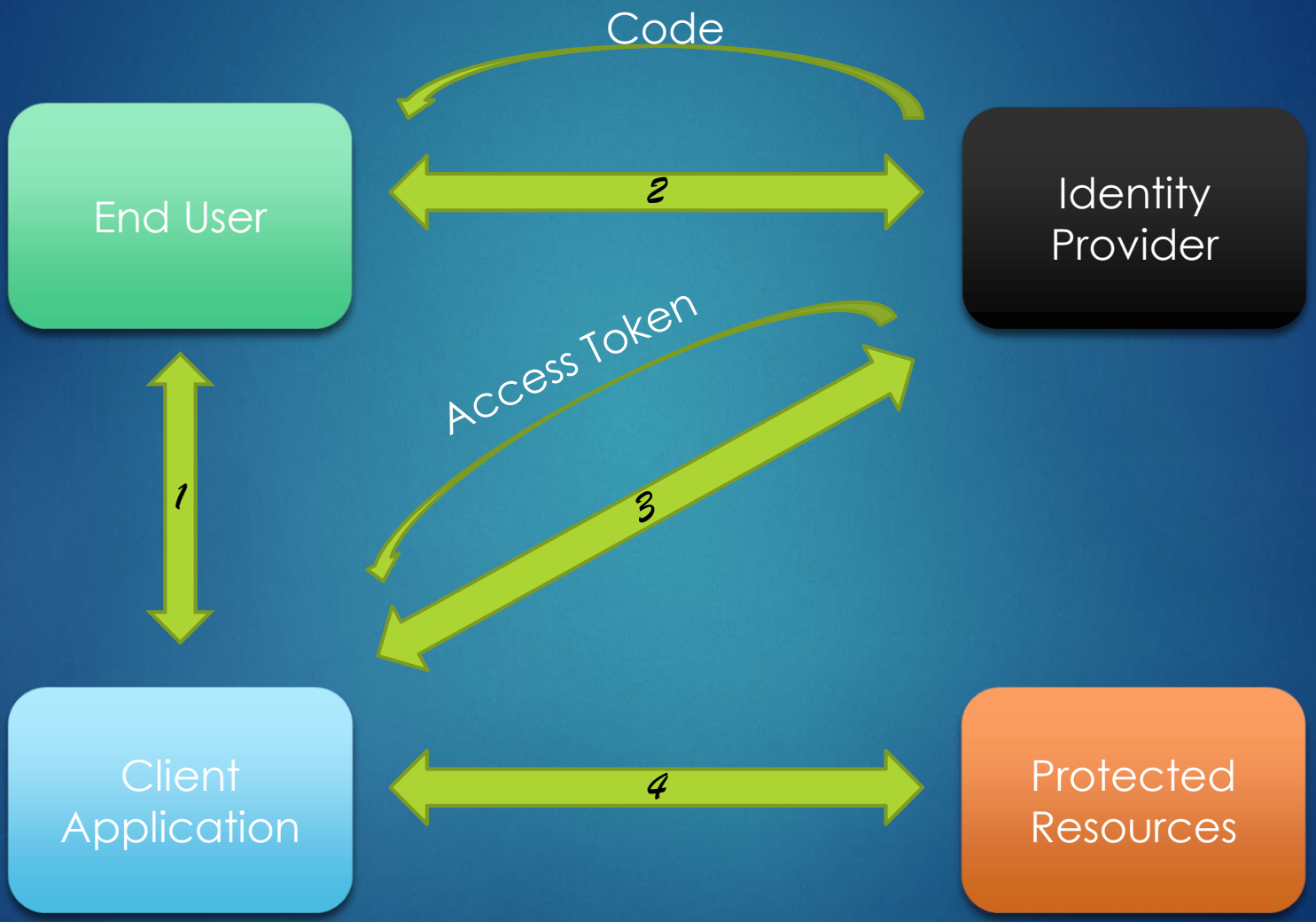
OAuth2 > Open ID Connect



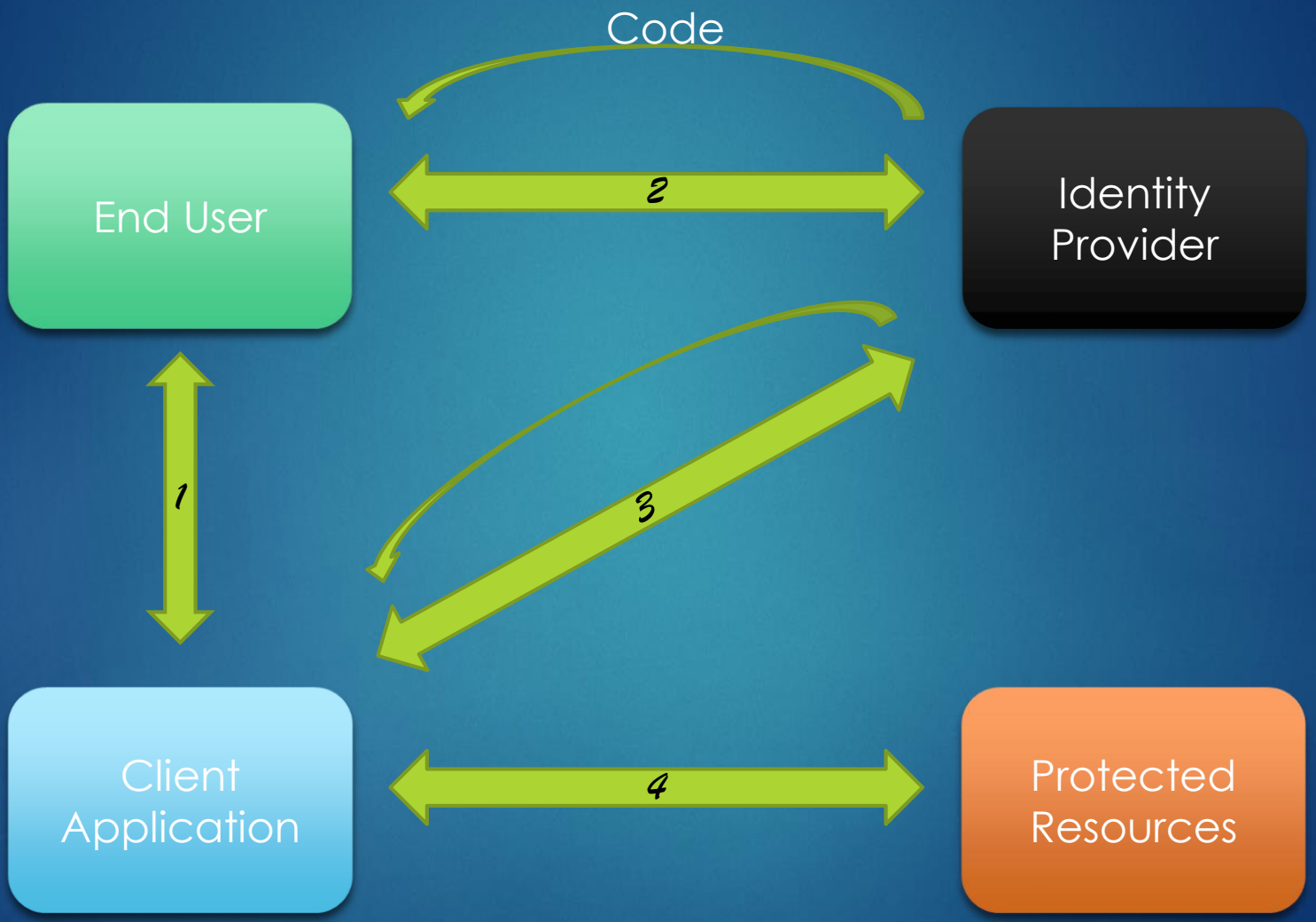
OAuth2 > Open ID Connect



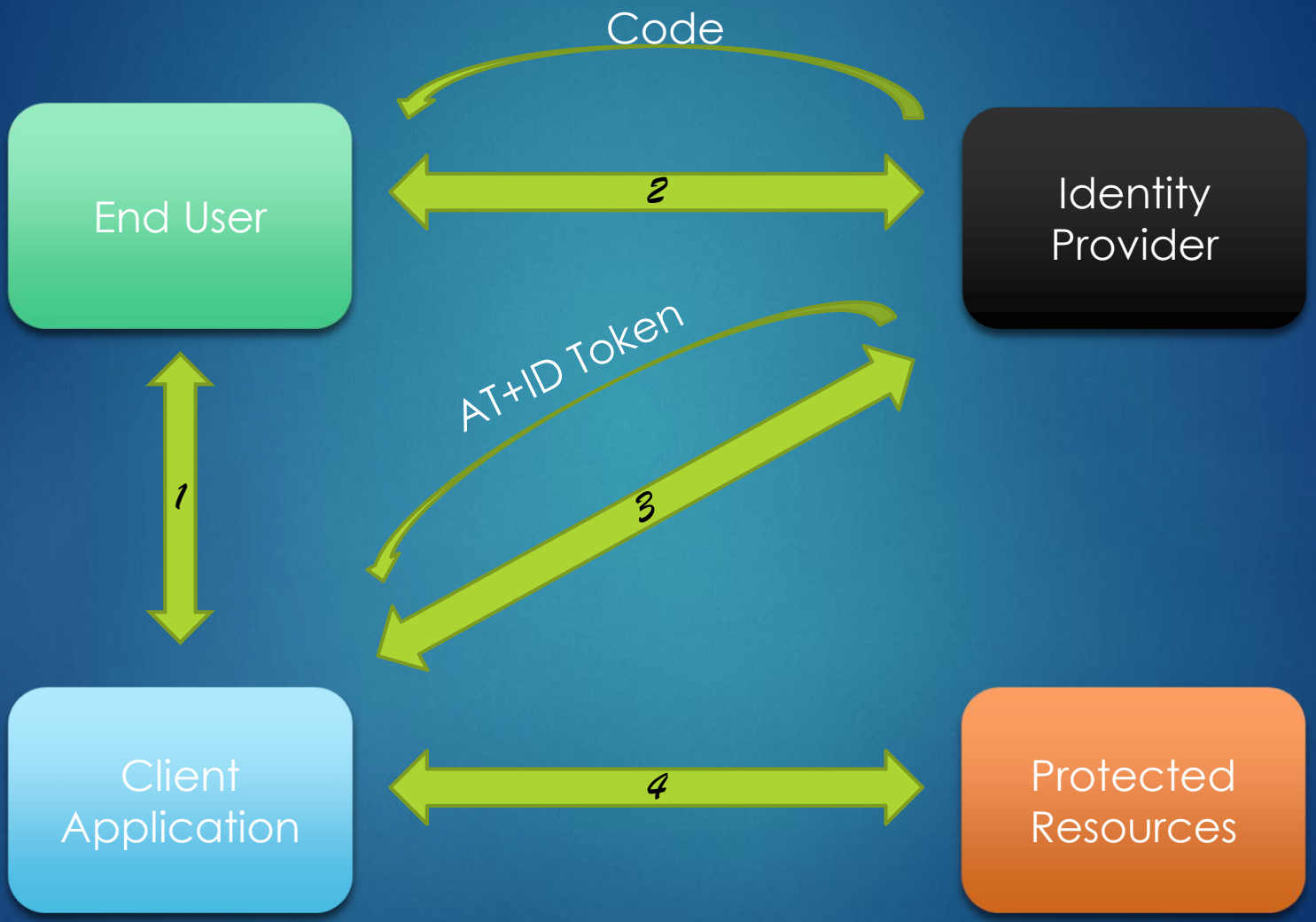
OAuth2 > Open ID Connect



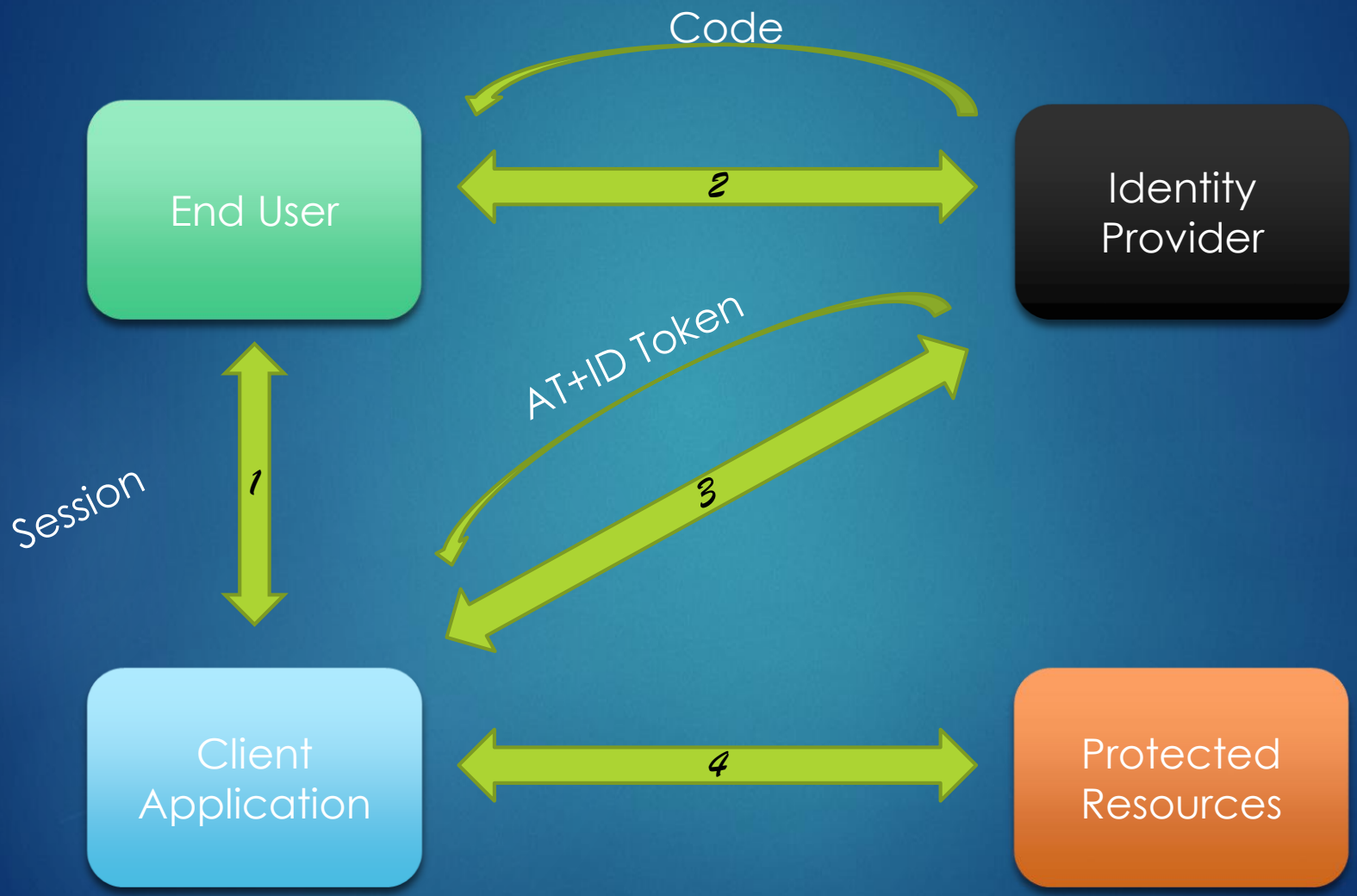
OAuth2 > Open ID Connect



OAuth2 > Open ID Connect



OAuth2 > Open ID Connect



JSON Web Token (JWT)

Encoded

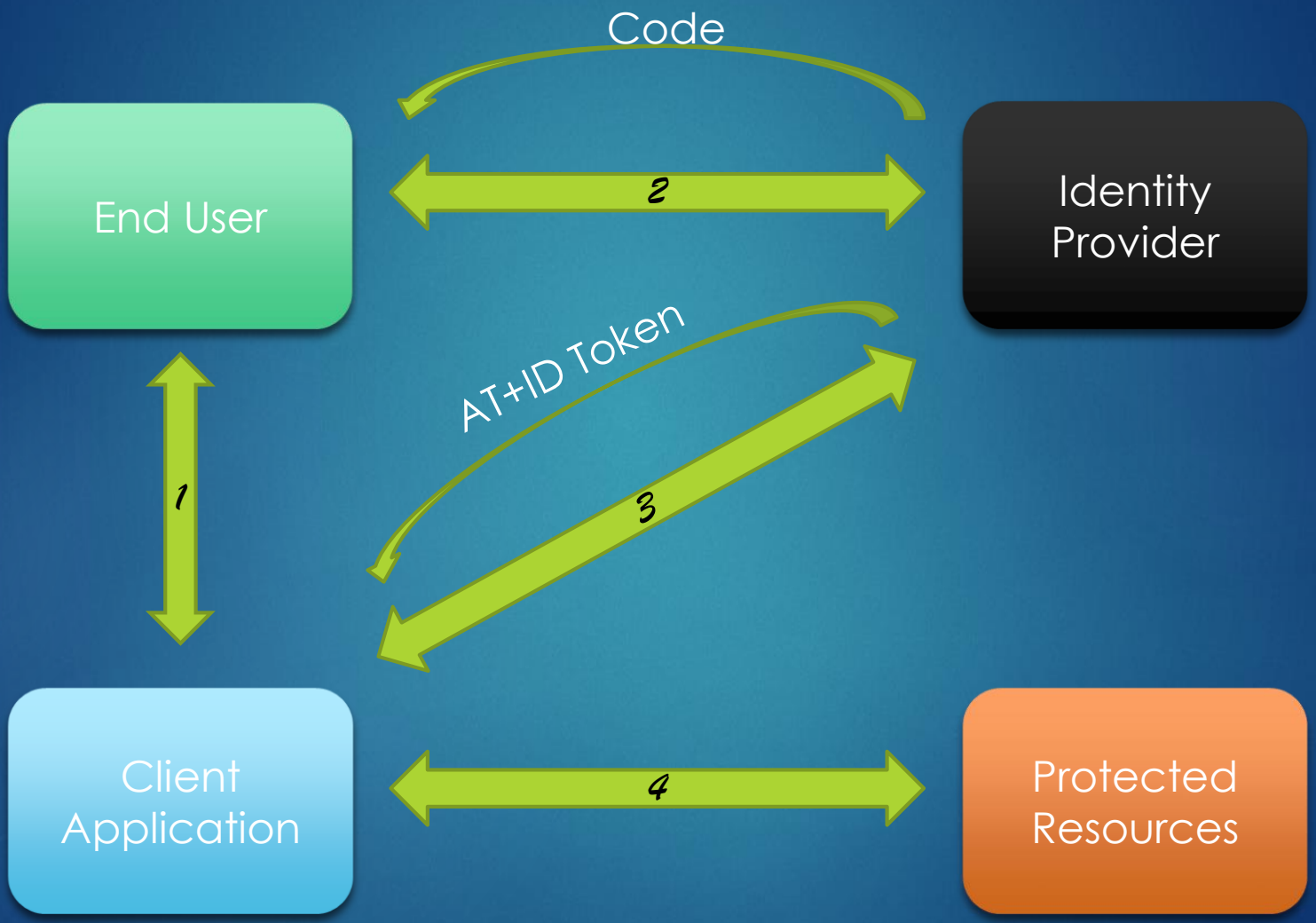
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ

Decoded

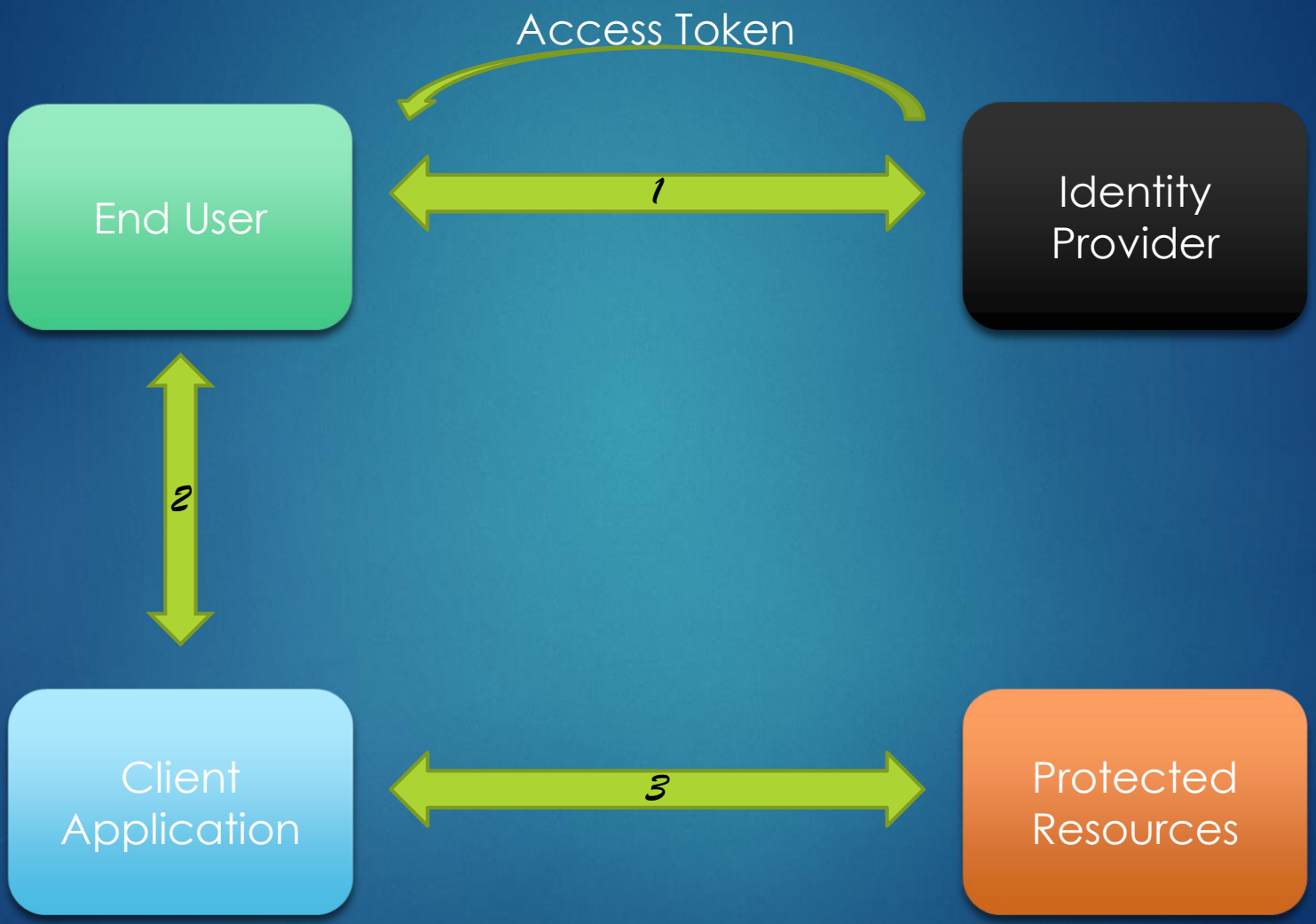
Header {
  "alg": "HS256",
  "typ": "JWT"
}
Payload {
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
Verify Signature
HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
secret) secret base64 encoded

From https://jwt.io

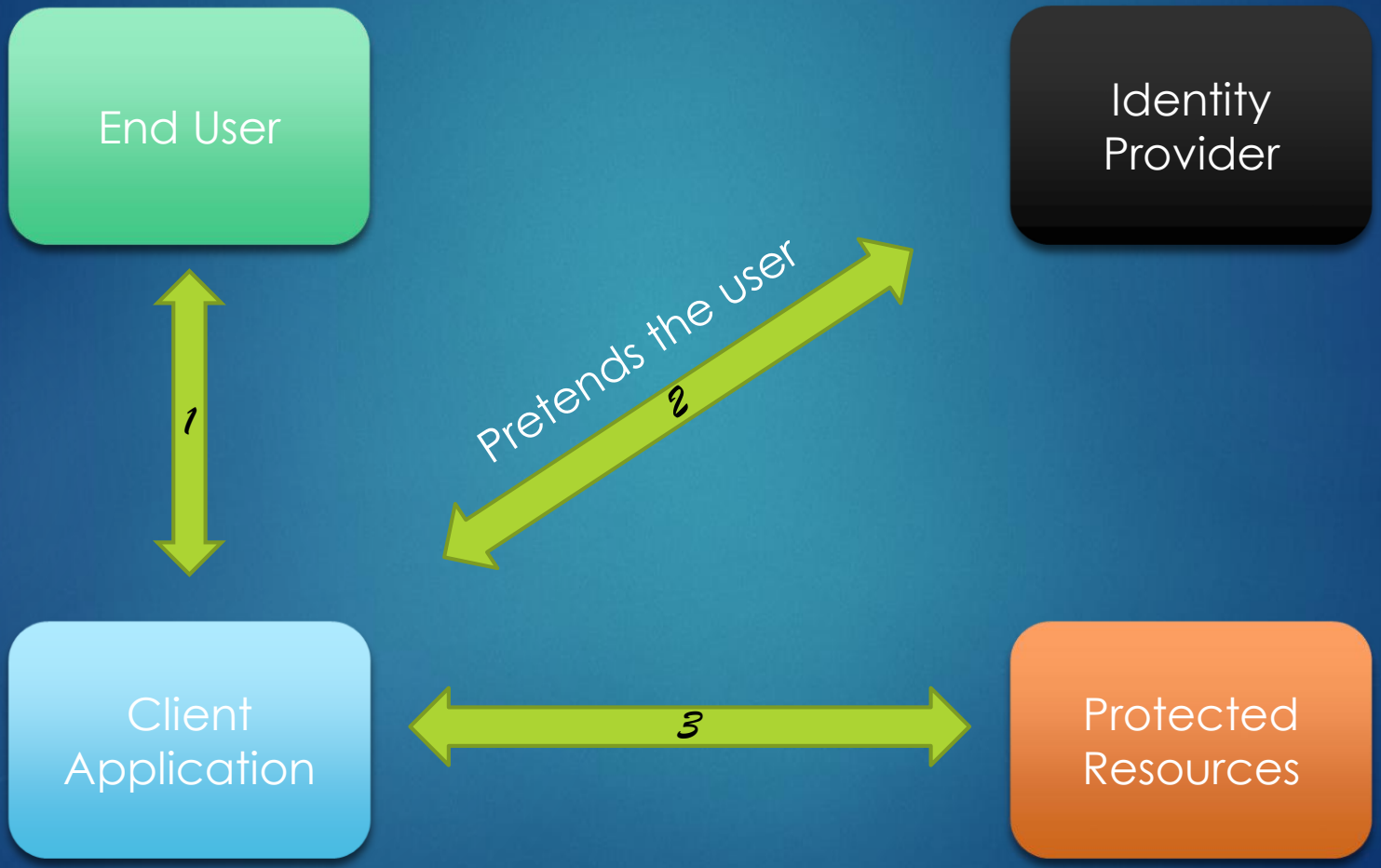
Code Flow


Code
End User
2
Identity Provider
AT+ID Token
1
3
Client Application
4
Protected Resources

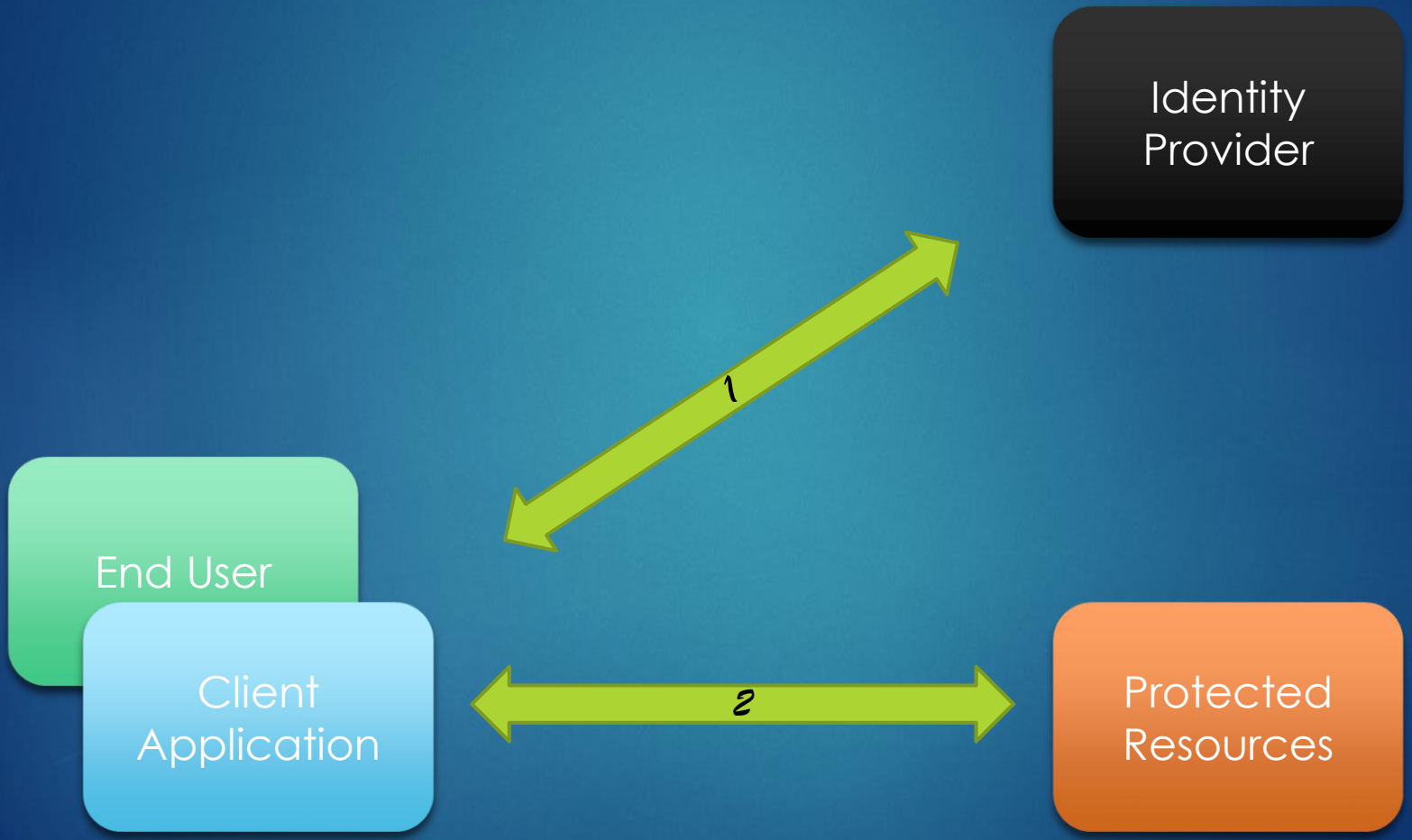
Implicit Flow



Password Flow



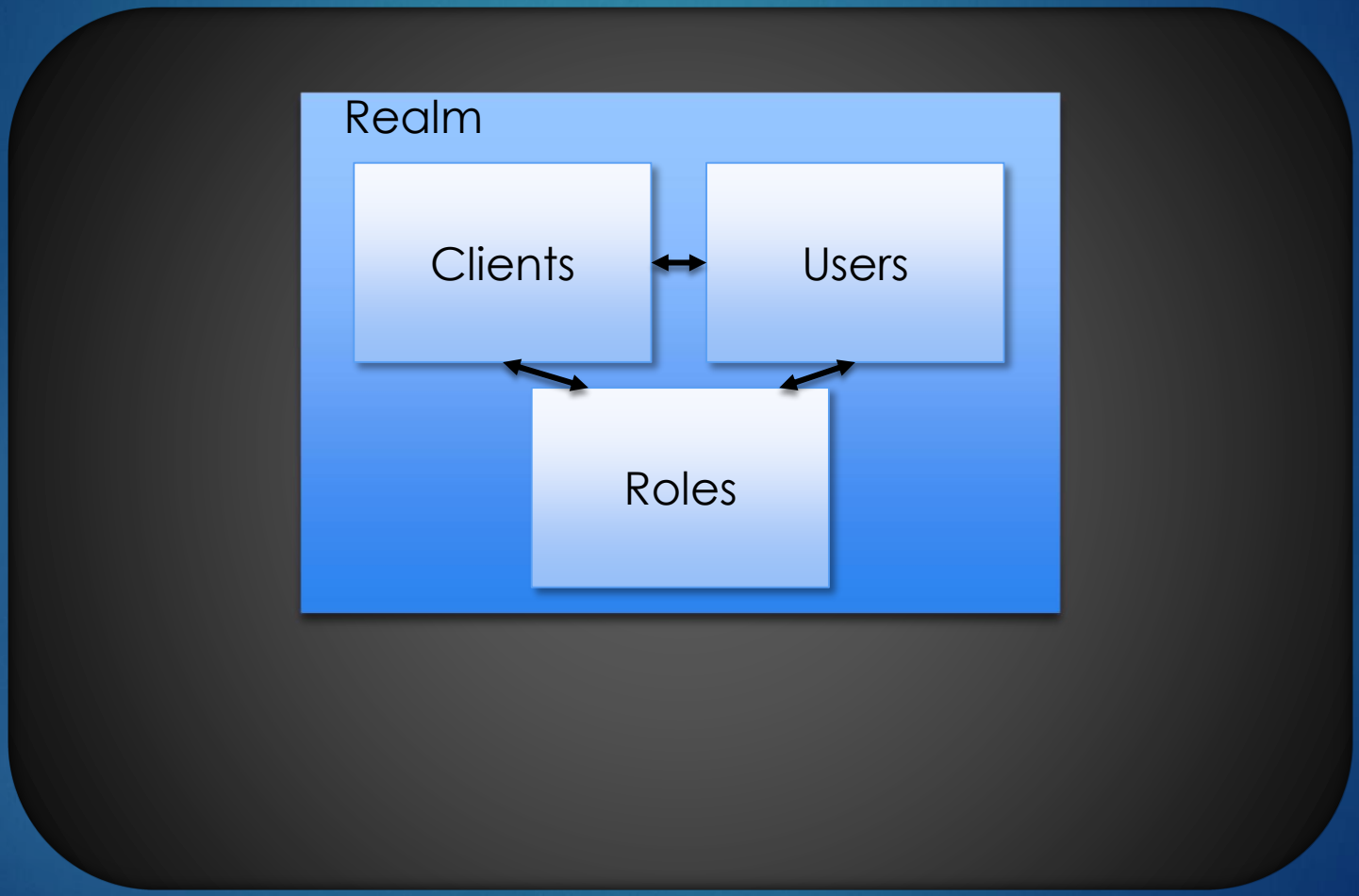
Client Credentials Flow



Good known implementation in Java

- Keycloak – **red**hat (very intensively developed)
- MitreID – Massachusetts Institute of Technology
- Gluu Server – Gluu, Inc.

Keycloak inside



Keycloak demo

You probably use it

- Facebook (GraphAPI)
- Google+ (Google Identity Platform)
- Twitter (Sign in with Twitter)

Advantages

- High level of security
- Do not need to handle authorization and authentication
- Do not need to keep user's credential
- There are many ready-to-use solutions
- People knows the Open ID flow (Facebook, Google, etc.)

Disadvantages

- Requests to resources may be longer (depends on token's hashing algorithm e.g. in Keycloak implementation, there is "pbkdf2" by default, which iterates the passwords 20 000 times)
- A lot of work if you decide to implement Open ID on your own