OAUTH
2
OAUTH

Table of content

- What is Oauth2

- Differences Oauth1 and Oauth2

- Oauth2 Roles

- Protocol types

- Protocol flows

- JSON Web token

- Workshop Registration

- Workshop Client

Differences Oauth1 and Oauth2

- Security
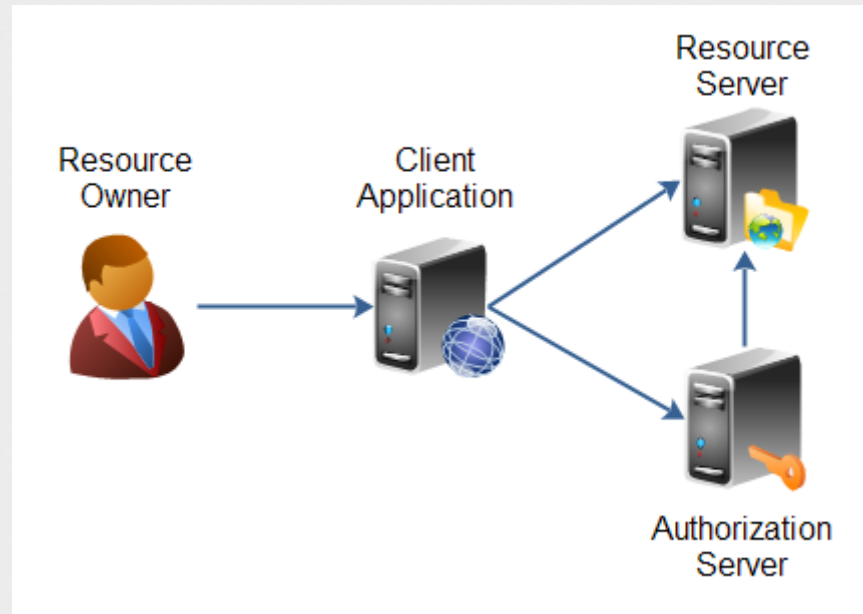
- Token life span

- Flows

- Roles

What is Oauth2

- Protocol

- Recources

Oauth2 roles

- Resource owner
- Resource server
- Client Application
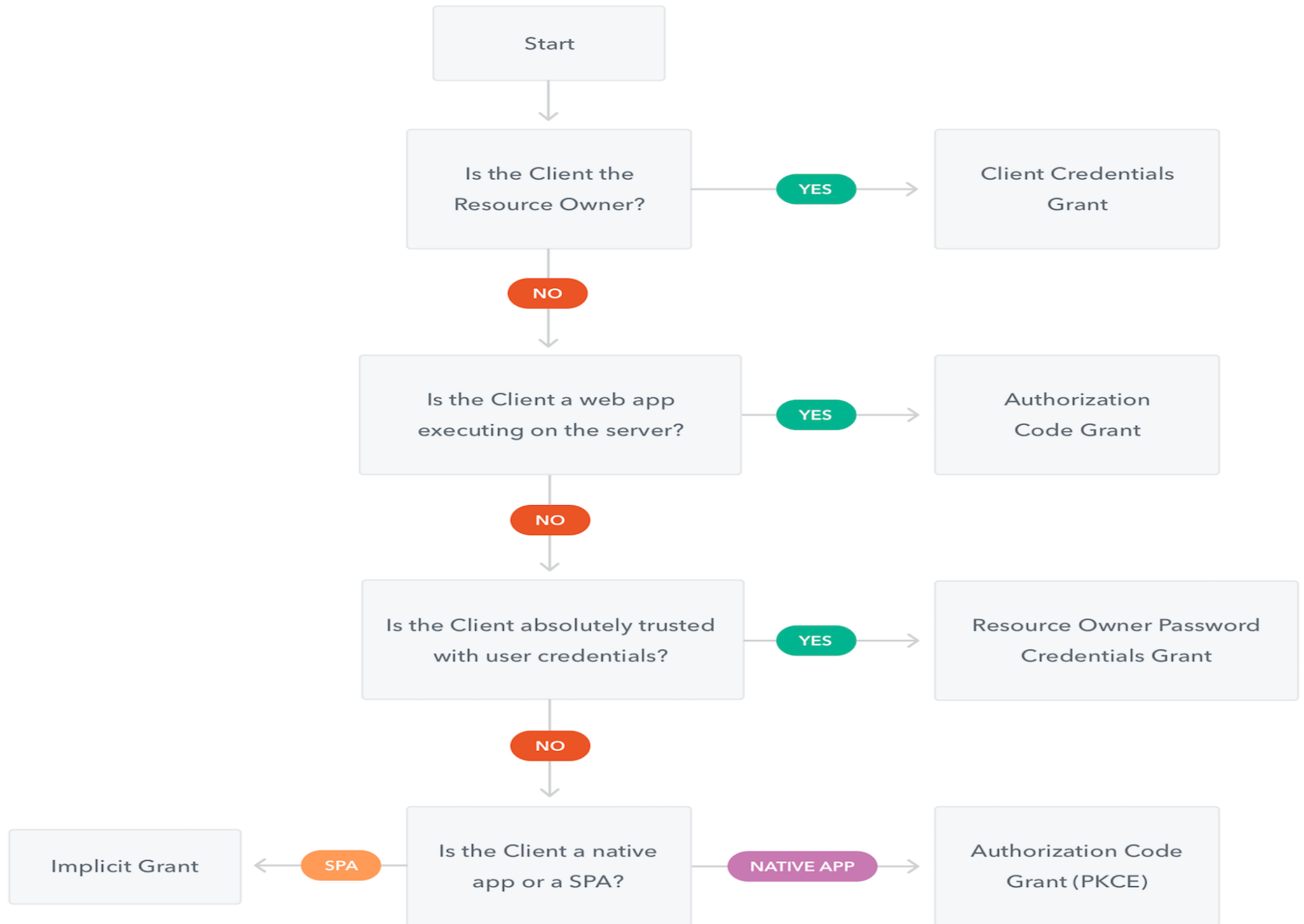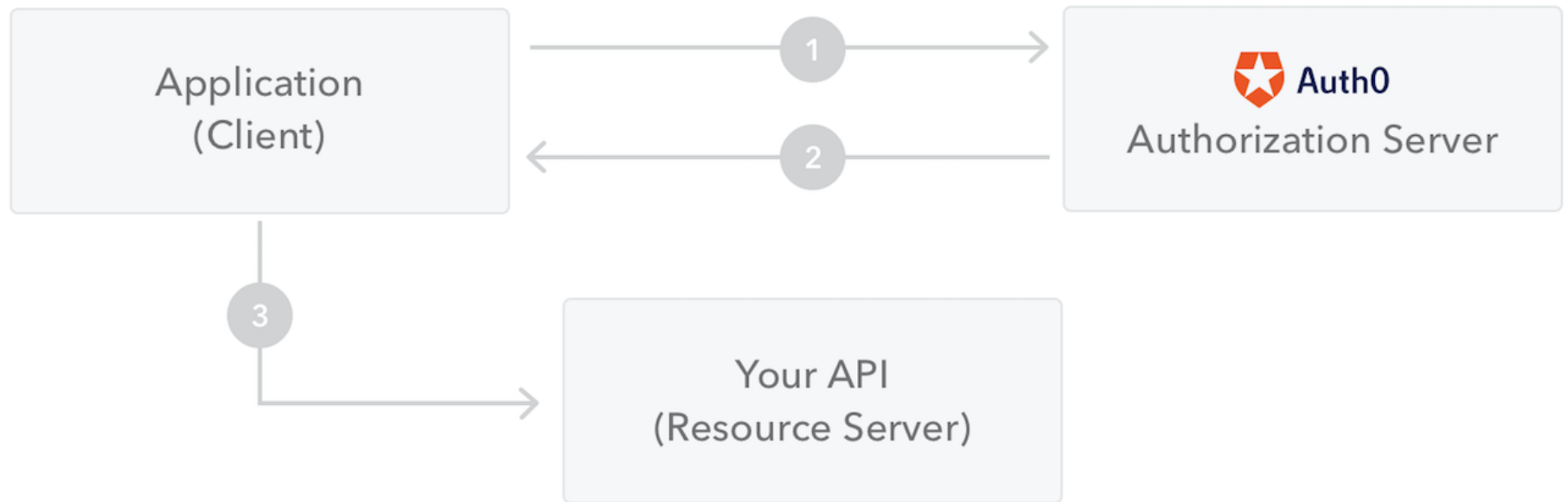- Authorization Server
- User Agent

Oauth2 Roles

Grant types

- Authorization code grant
- Implicit grant
- Resource owner credentials grant
- Client credentials grant
- Refresh token grant

Protocol flows

- Client Credential Grant
- Authorization Code Grant
- Implicit Grant
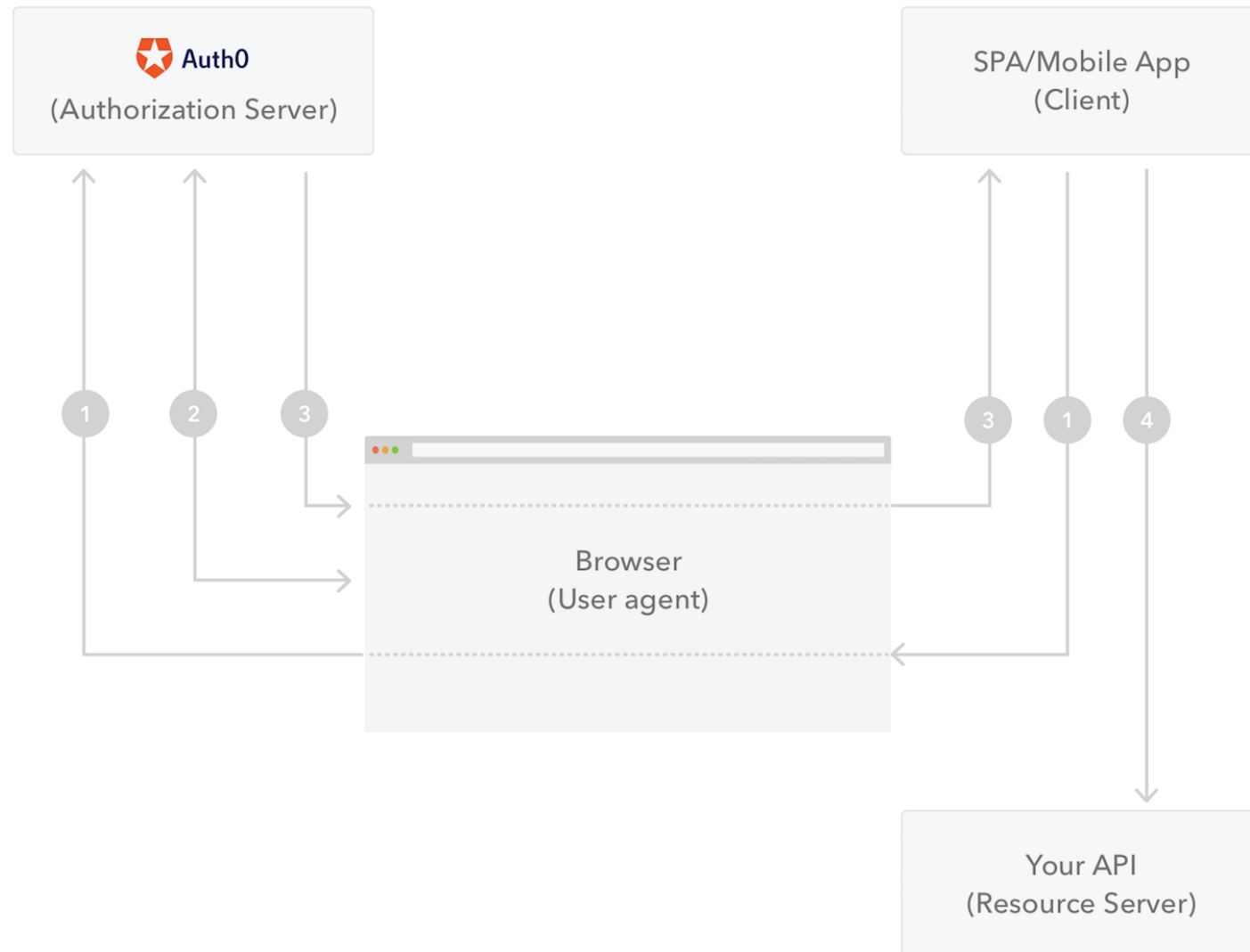- Authorization Code Grant (PKCE)

```
                          ┌──────────┐
                          │  Start   │
                          └────┬─────┘
                               │
                               ▼
        ┌──────────────────────────┐              ┌──────────────────────┐
        │    Is the Client the     │───[YES]────▶ │  Client Credentials  │
        │     Resource Owner?      │              │        Grant         │
        └────────────┬─────────────┘              └──────────────────────┘
                   [NO]
                     │
                     ▼
        ┌──────────────────────────┐              ┌──────────────────────┐
        │  Is the Client a web app │───[YES]────▶ │    Authorization     │
        │  executing on the server?│              │     Code Grant       │
        └────────────┬─────────────┘              └──────────────────────┘
                   [NO]
                     │
                     ▼
        ┌──────────────────────────┐              ┌──────────────────────────┐
        │ Is the Client absolutely │───[YES]────▶ │  Resource Owner Password │
        │  trusted with user       │              │    Credentials Grant     │
        │  credentials?            │              └──────────────────────────┘
        └────────────┬─────────────┘
                   [NO]
                     │
                     ▼
┌────────────┐   ┌──────────────────────────┐   ┌──────────────────────┐
│  Implicit  │◀──[SPA]─ │ Is the Client a native │──[NATIVE APP]──▶│ Authorization Code │
│   Grant    │         │    app or a SPA?       │               │   Grant (PKCE)     │
└────────────┘   └──────────────────────────┘   └──────────────────────┘
```
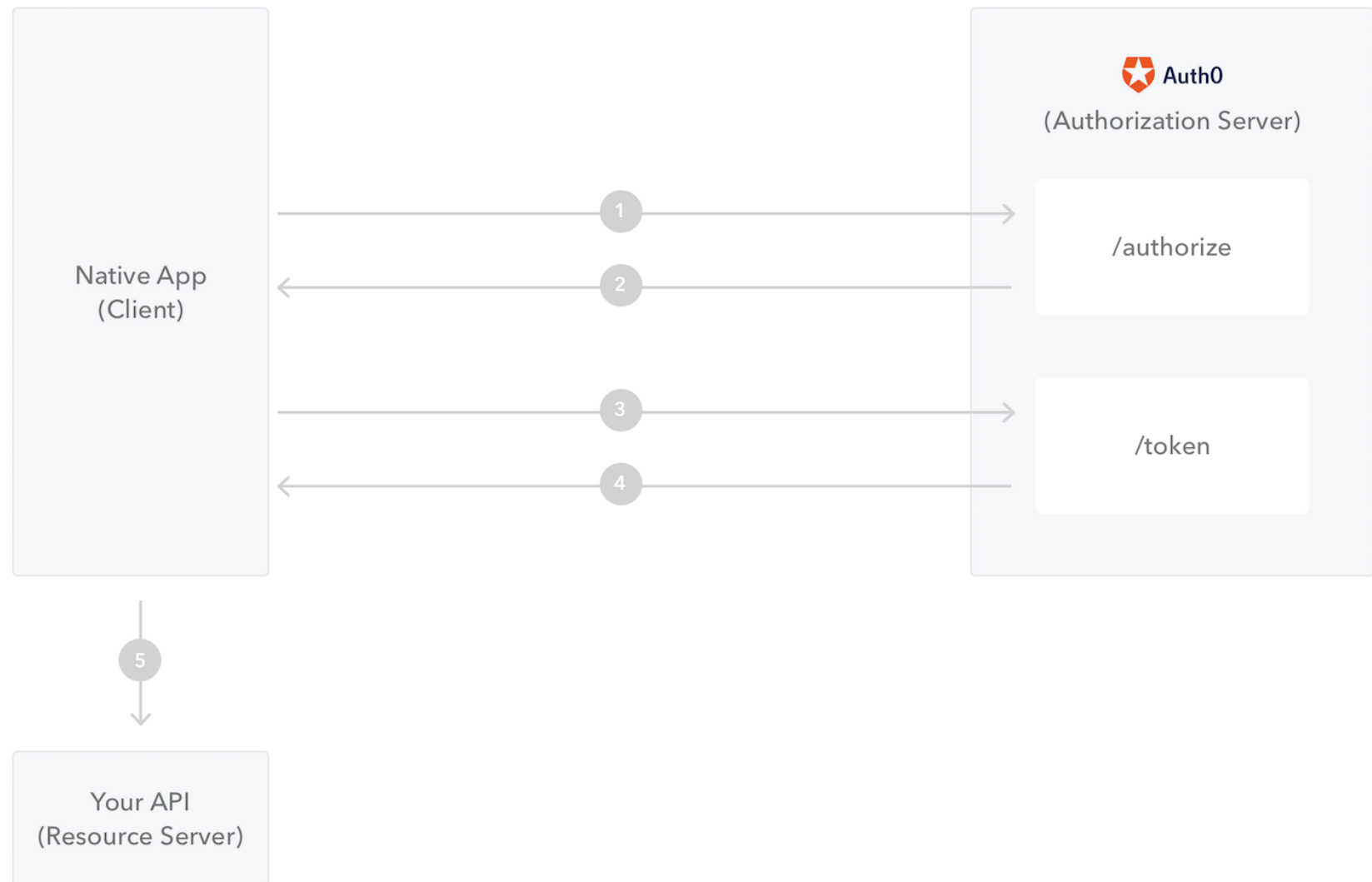
Client Credentials Grant

Authorization Code Grant
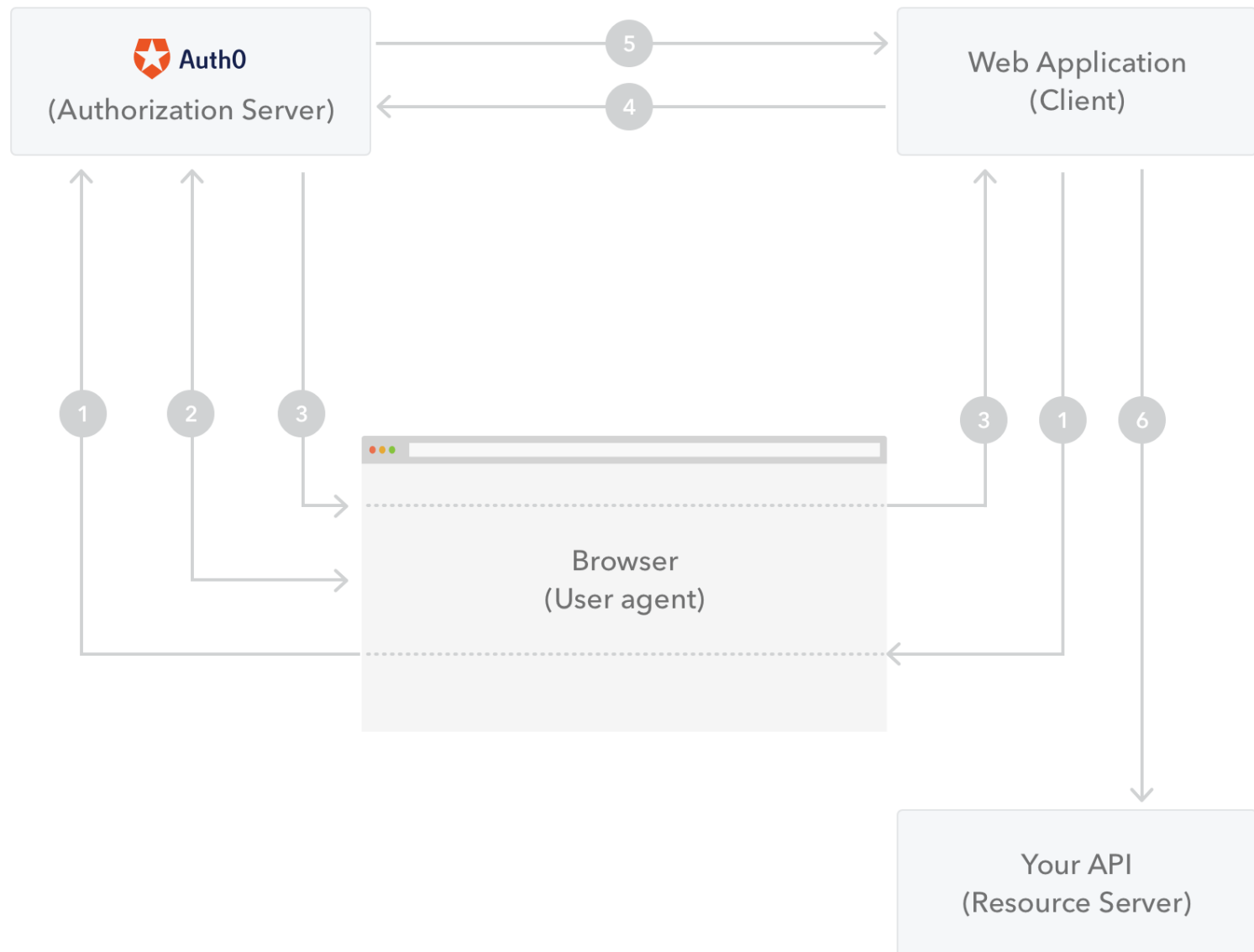
Implicit grant

Authorization Code Grant (PKCE)

JWT

- Header
- Claims
- Signature

Workshop registration

Workshop client

Workshop Client

```yaml
facebook:
  client:
    clientId: 233668646673605
    clientSecret: 33b17e044ee6a4fa383f46ec6e28ea1d
    accessTokenUri: https://graph.facebook.com/oauth/access_token
    userAuthorizationUri: https://www.facebook.com/dialog/oauth
    tokenName: oauth_token
    authenticationScheme: query
    clientAuthenticationScheme: form
  resource:
    userInfoUri: https://graph.facebook.com/me
```

Workshop client

```yaml
facebook:
  client:
    clientId: 233668646673605
    clientSecret: 33b17e044ee6a4fa383f46ec6e28ea1d
    accessTokenUri: https://graph.facebook.com/oauth/access_token
    userAuthorizationUri: https://www.facebook.com/dialog/oauth
    tokenName: oauth_token
    authenticationScheme: query
    clientAuthenticationScheme: form
    scope: email
  resource:
    userInfoUri: https://graph.facebook.com/me?fields=id,name,email
```