

Skillbox

# Security

OAuth 2.0

OpenID connect

JWT

SSO

**Чернухин Максим**

Software Architect АО Альфа-Банк

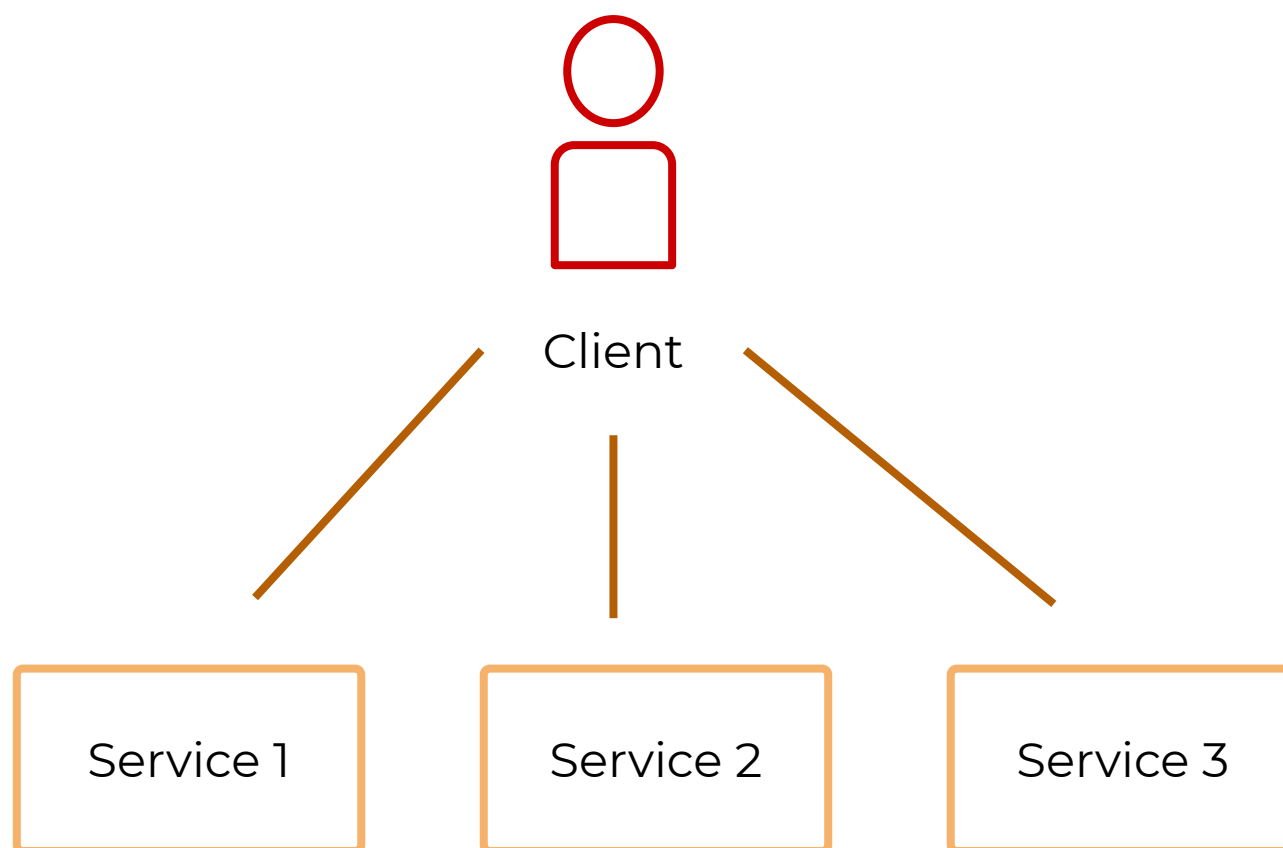
# На этом уроке мы узнаем

- Что такое OAuth 2.0
- Чем он отличается от OpenID connect
- Зачем нужен JWT
- Как использовать SSO

# Управление ключами

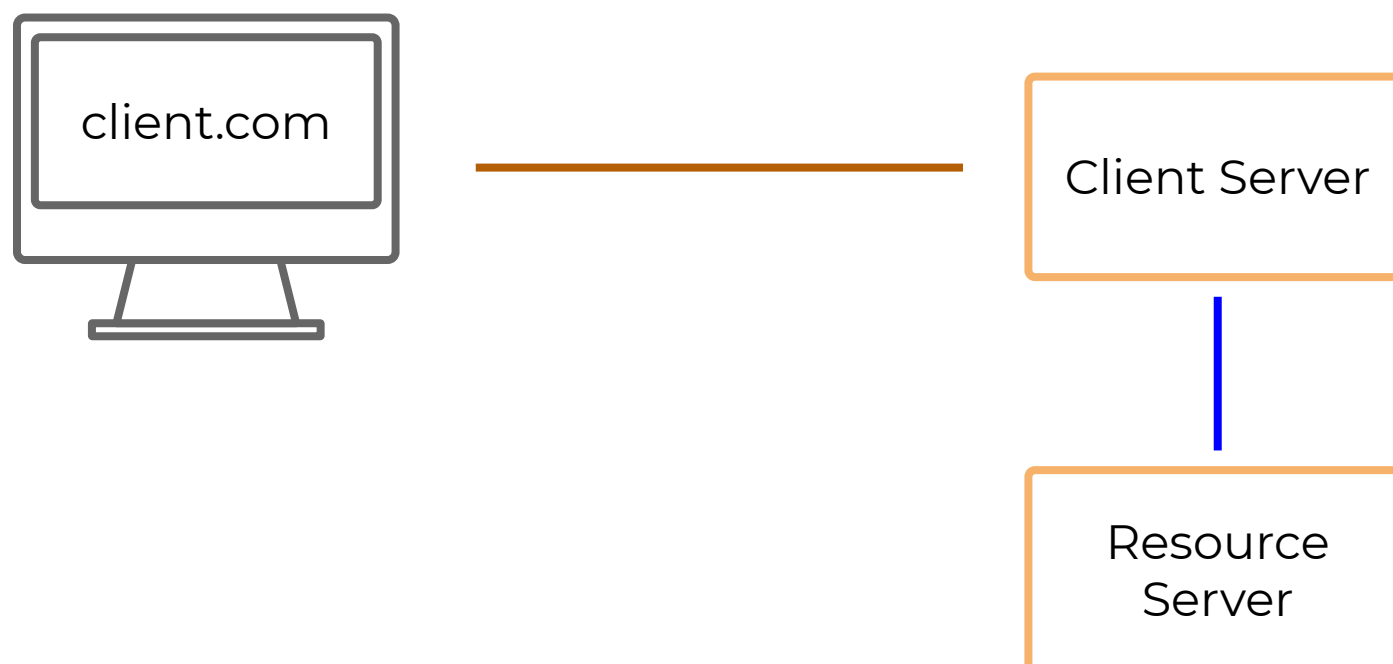


# Аутентификация

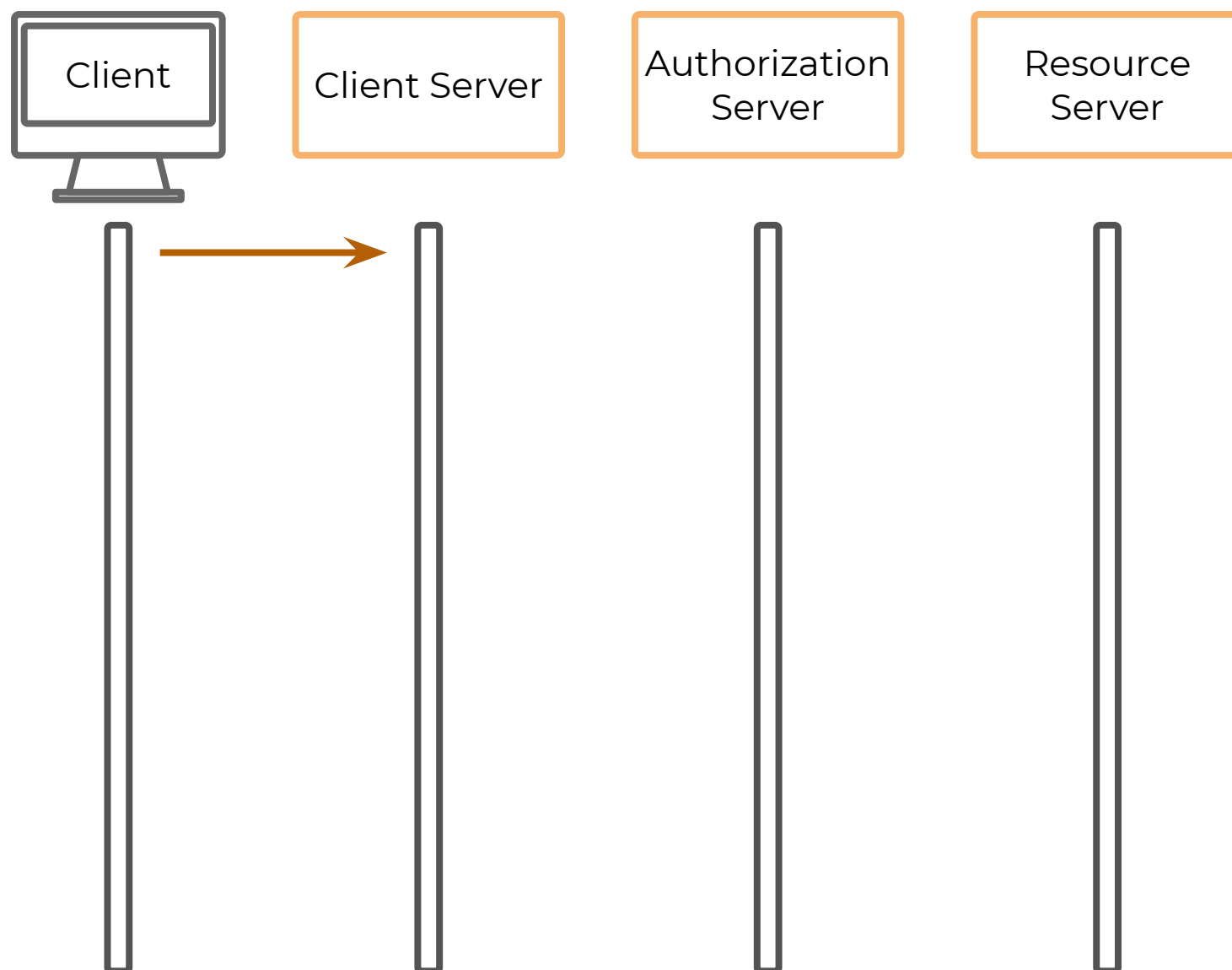


# OAuth 2.0

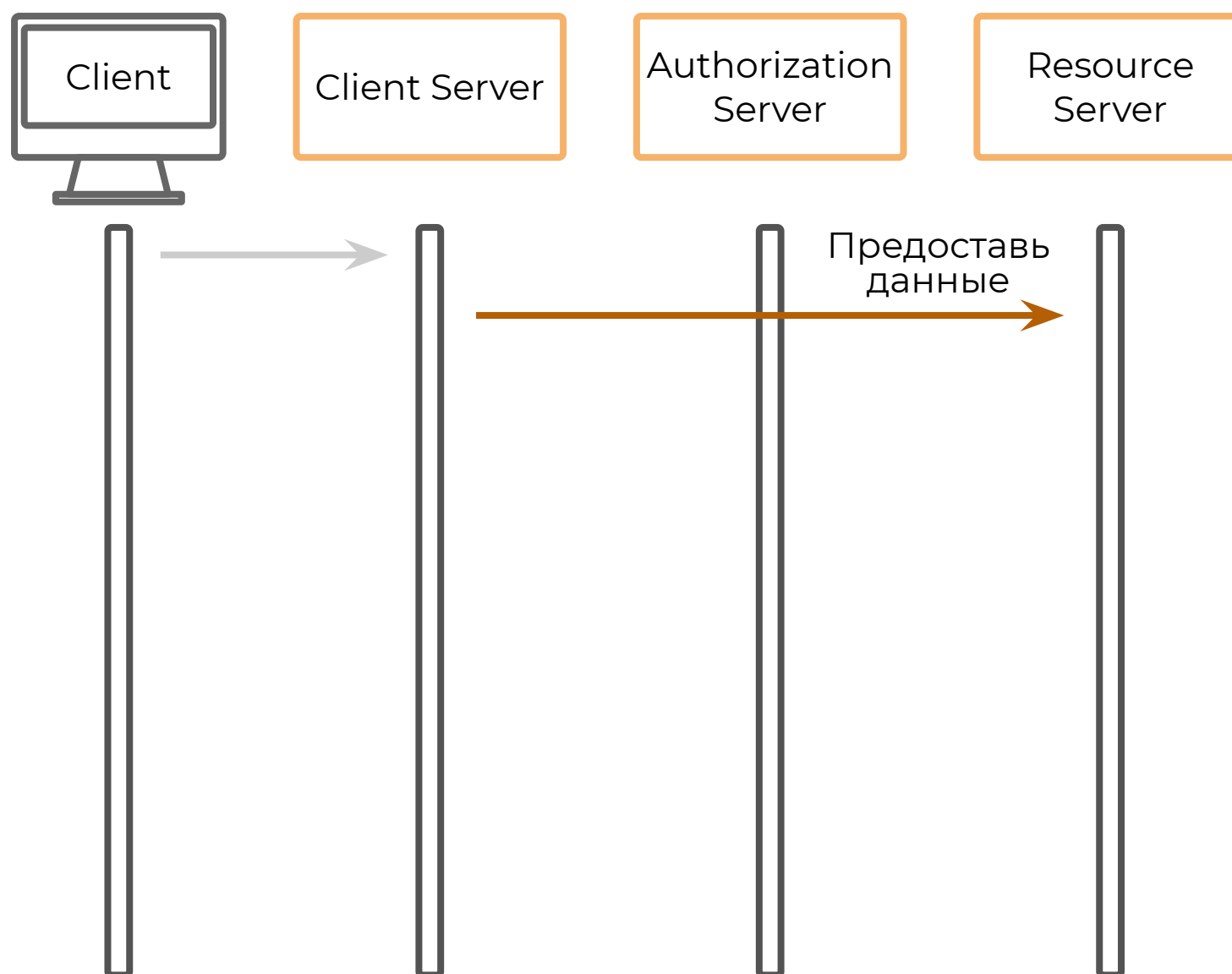
- RFC 6749 2012
- Позволяет легко и безопасно предоставлять данные другим системам



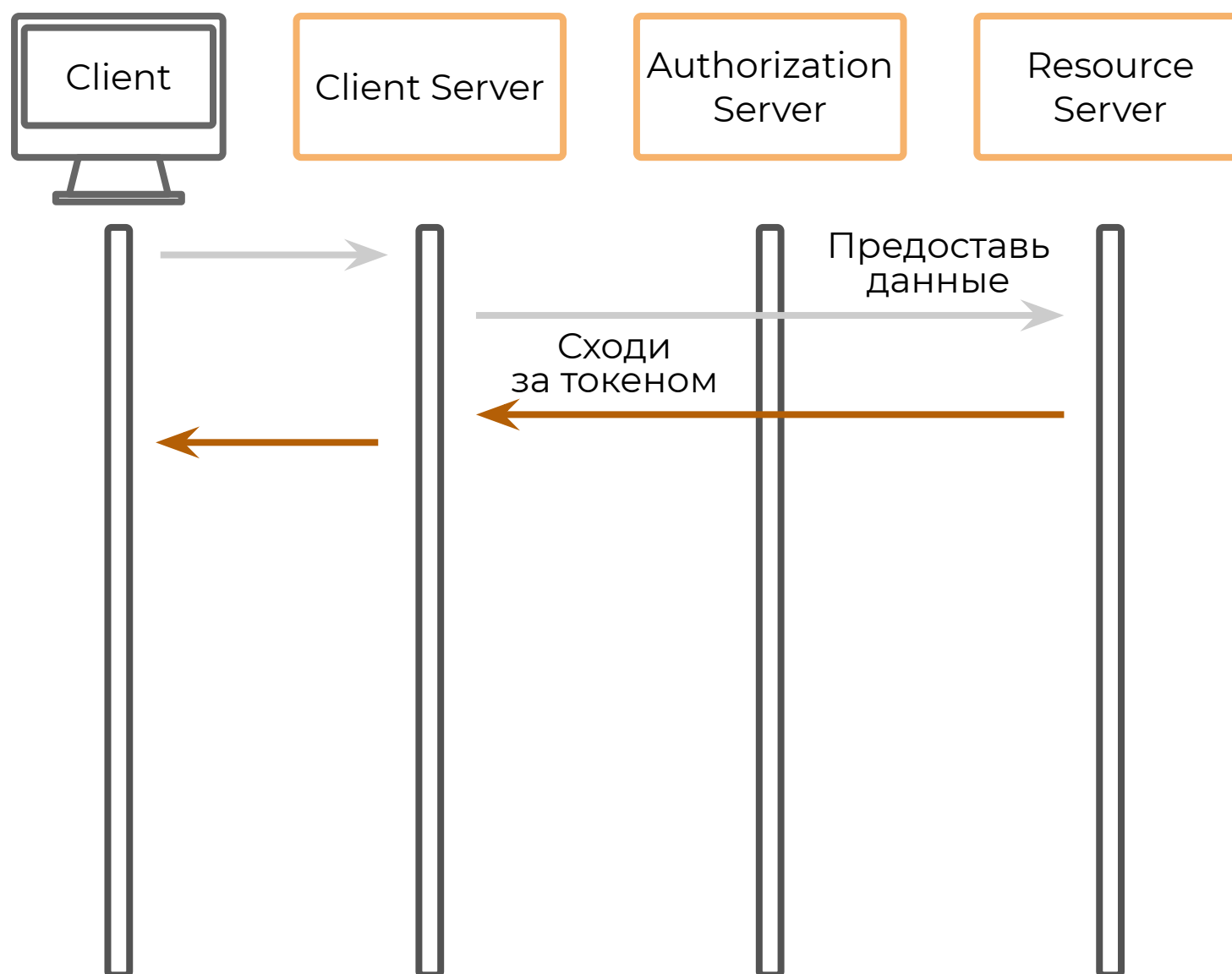
# OAuth 2.0



# OAuth 2.0

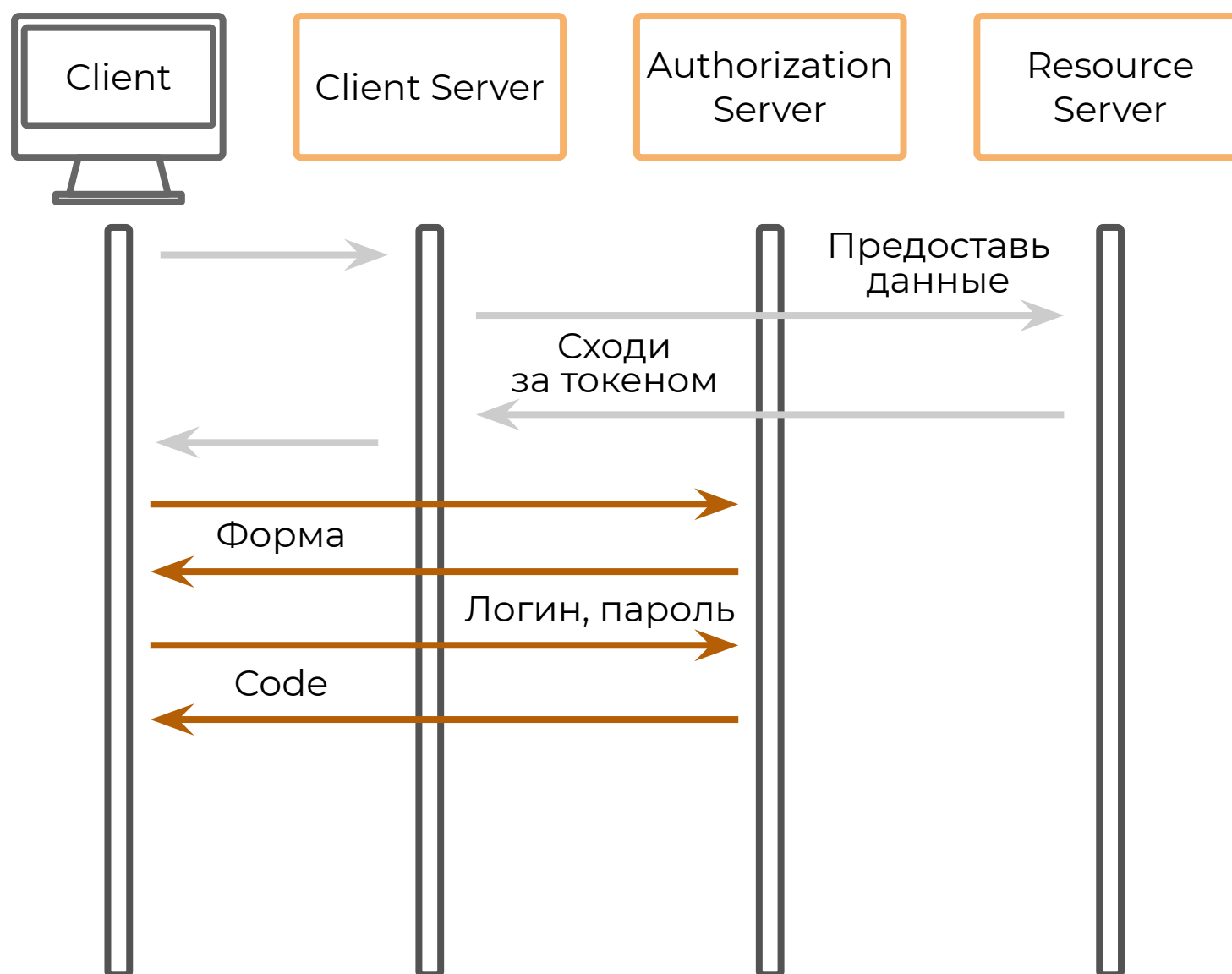


# OAuth 2.0

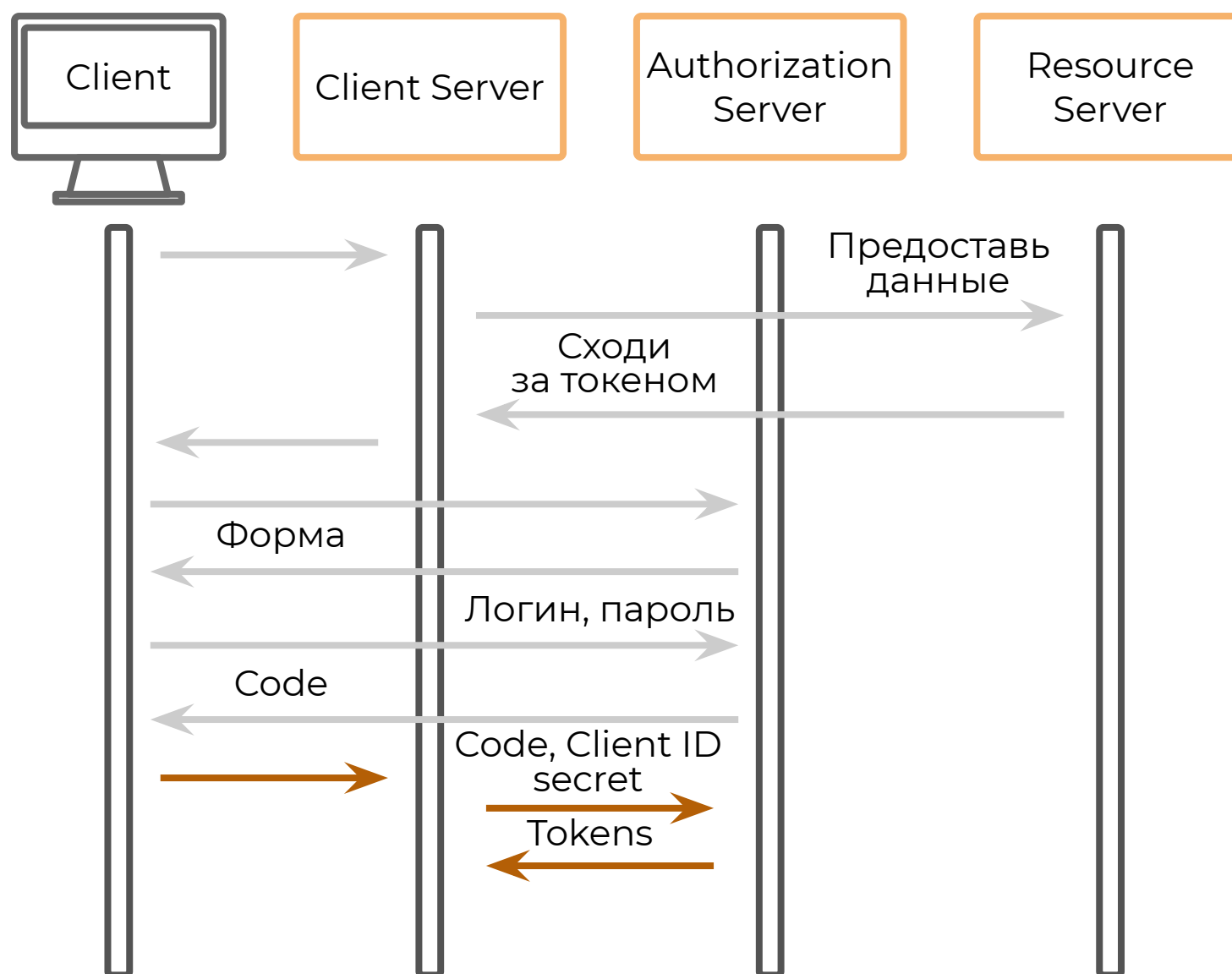




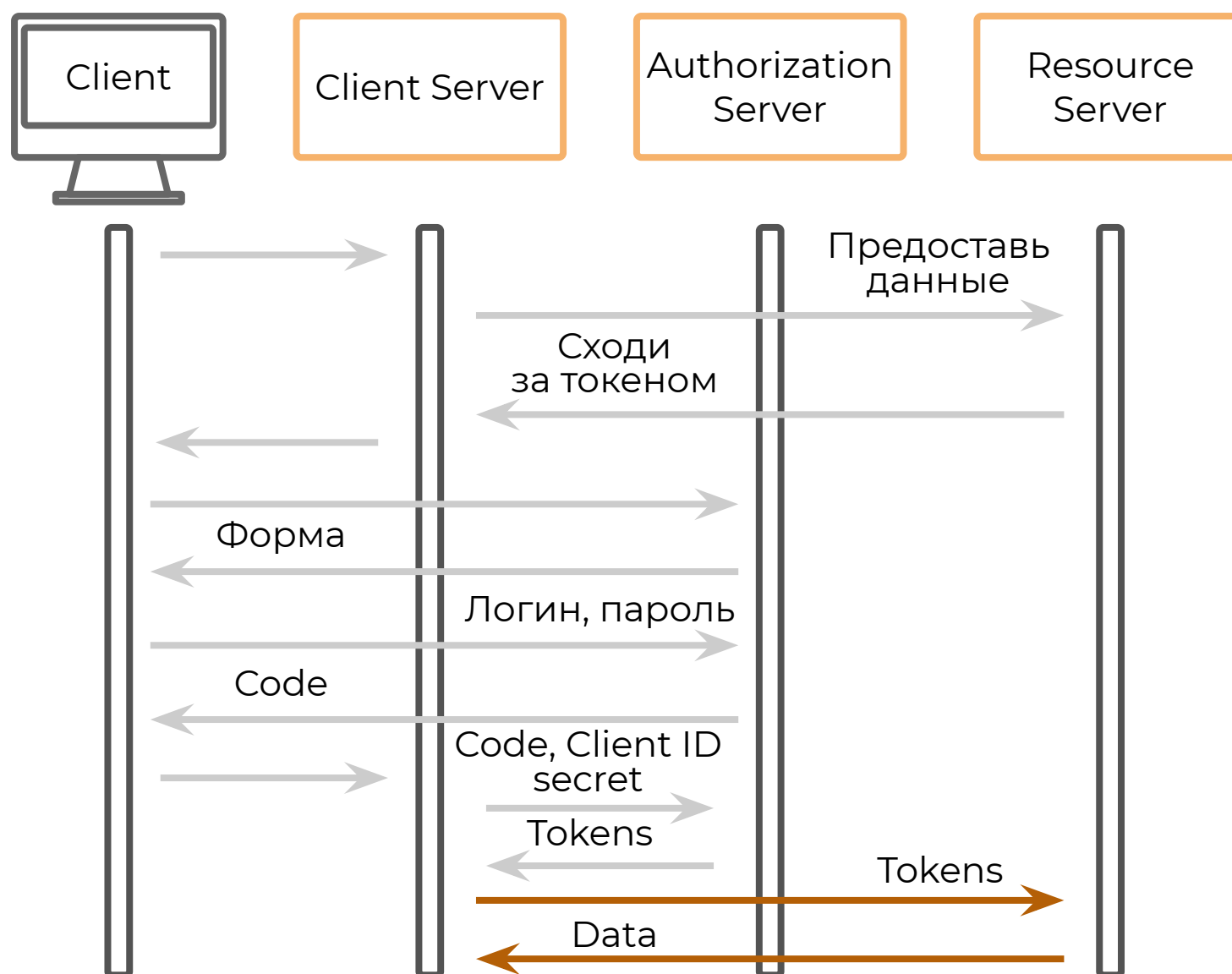
# OAuth 2.0



# OAuth 2.0



# OAuth 2.0



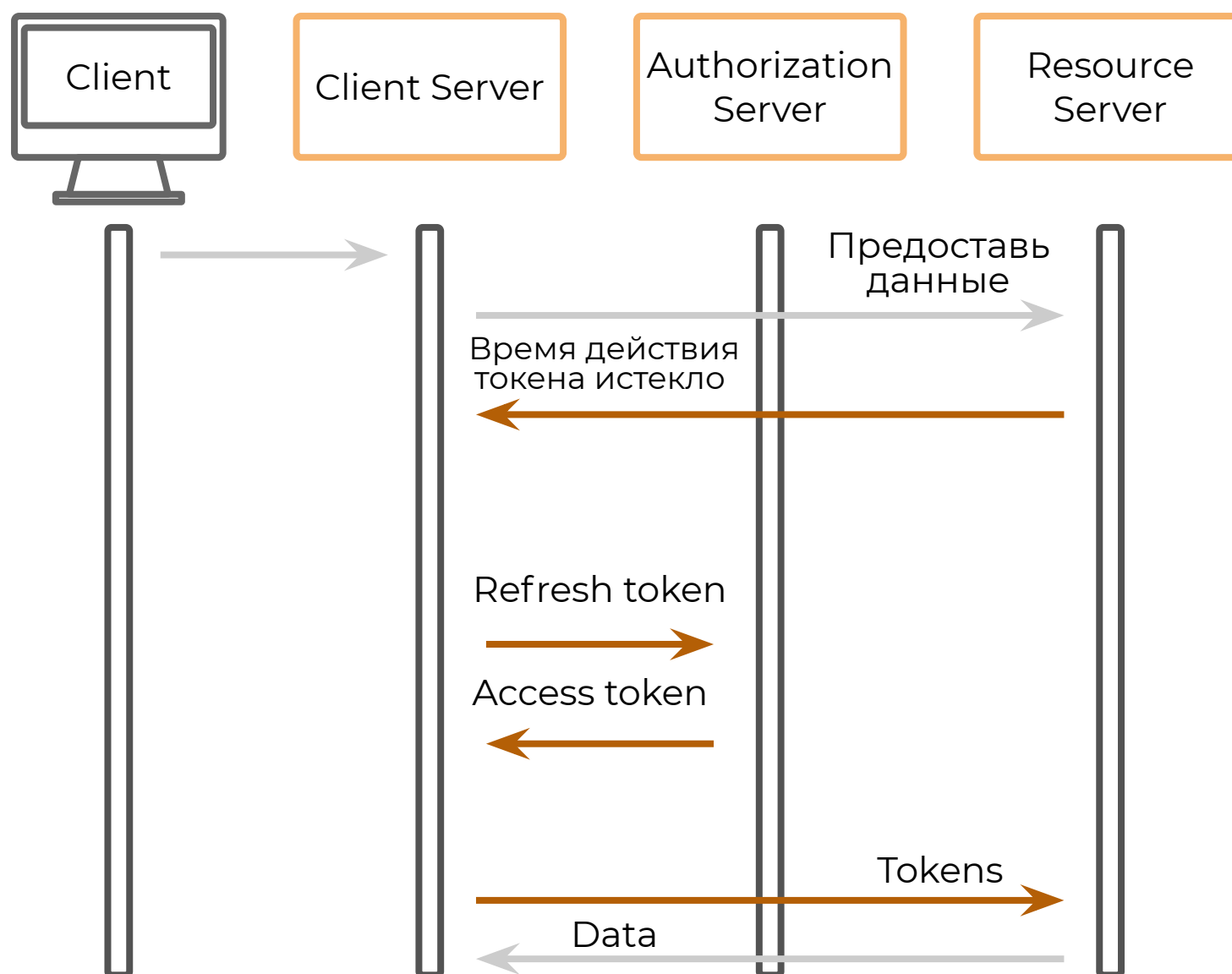
Skillbox

# OAuth 2.0

Сервис авторизации возвращает два токена:

- Access token
- Refresh token

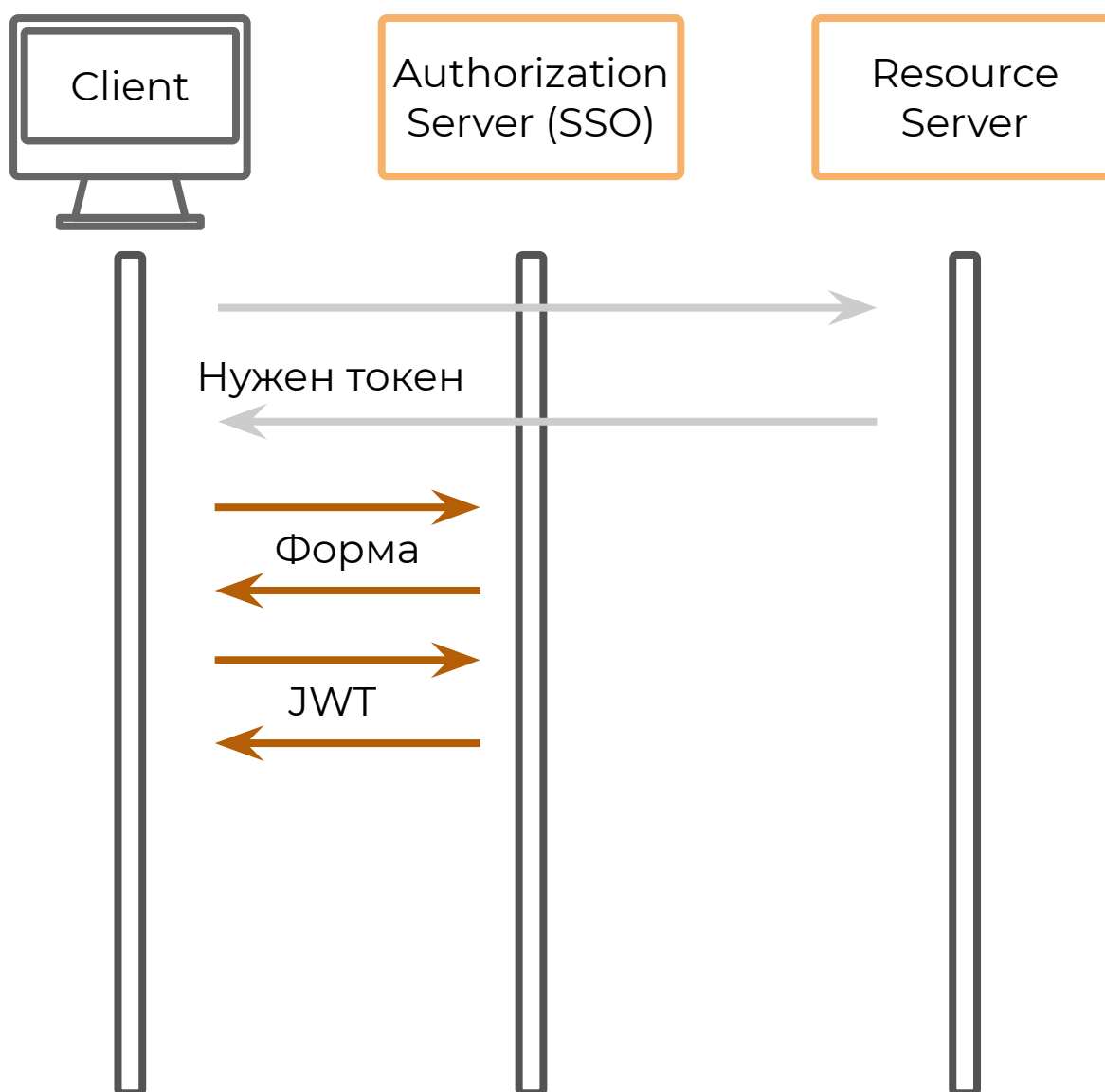
# OAuth 2.0



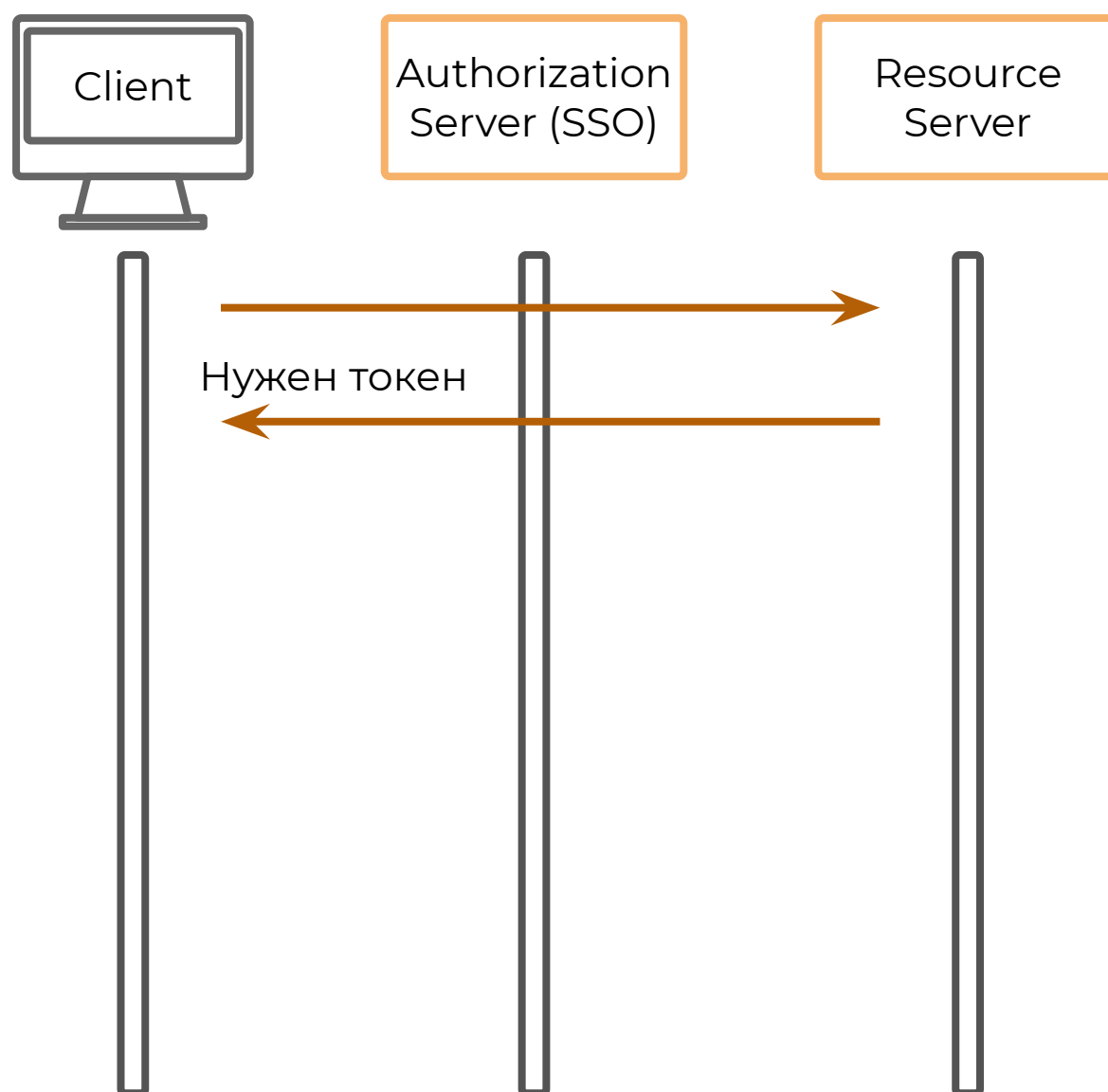
# OpenID Connect

- Настройка над OAuth 2.0
- Добавляет возможность идентификации
- Single Sign-on
- Сервис авторизации возвращает:
  - Identity token
  - Access token
  - Refresh token

# OpenID Connect

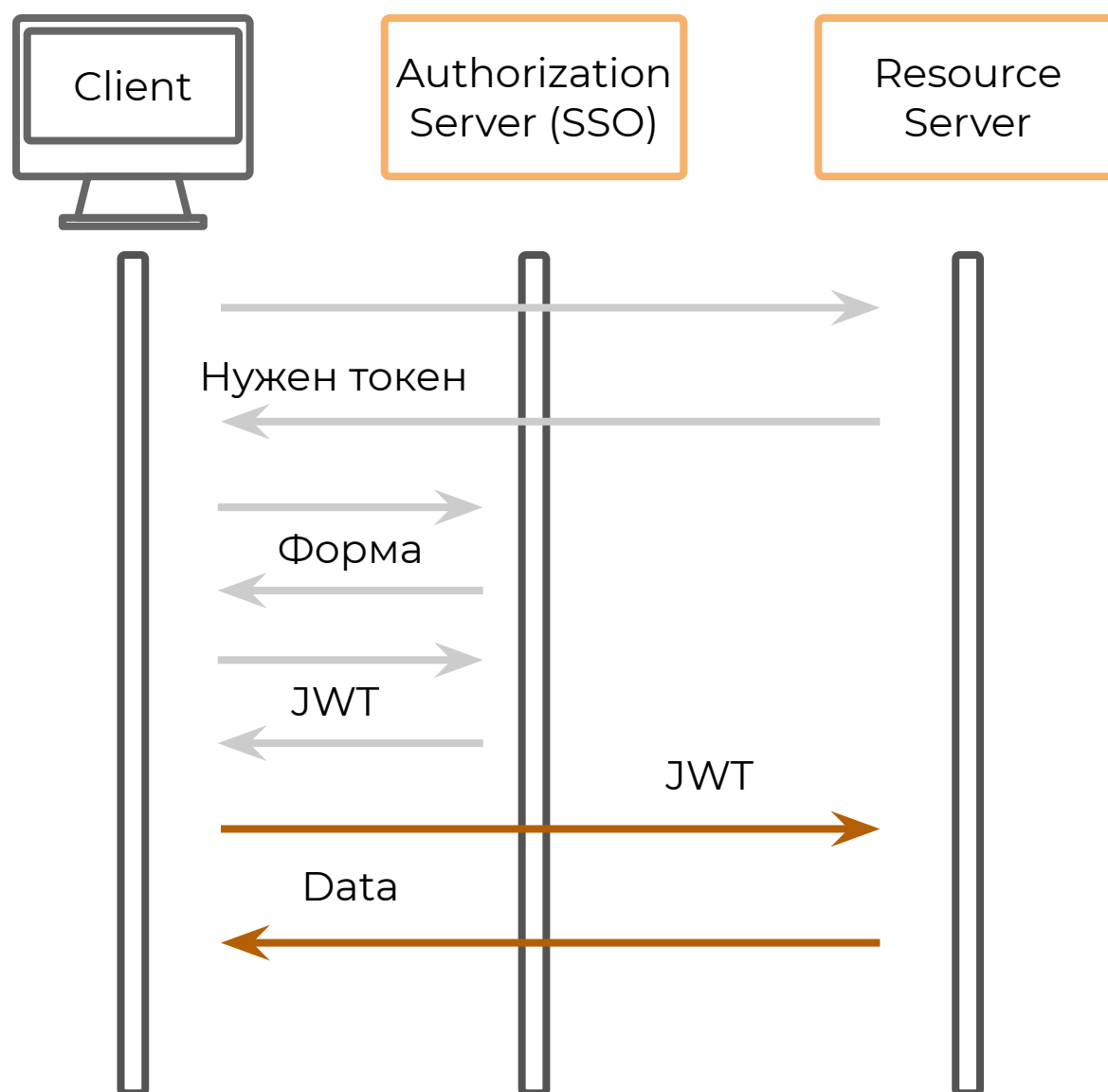


# OpenID Connect

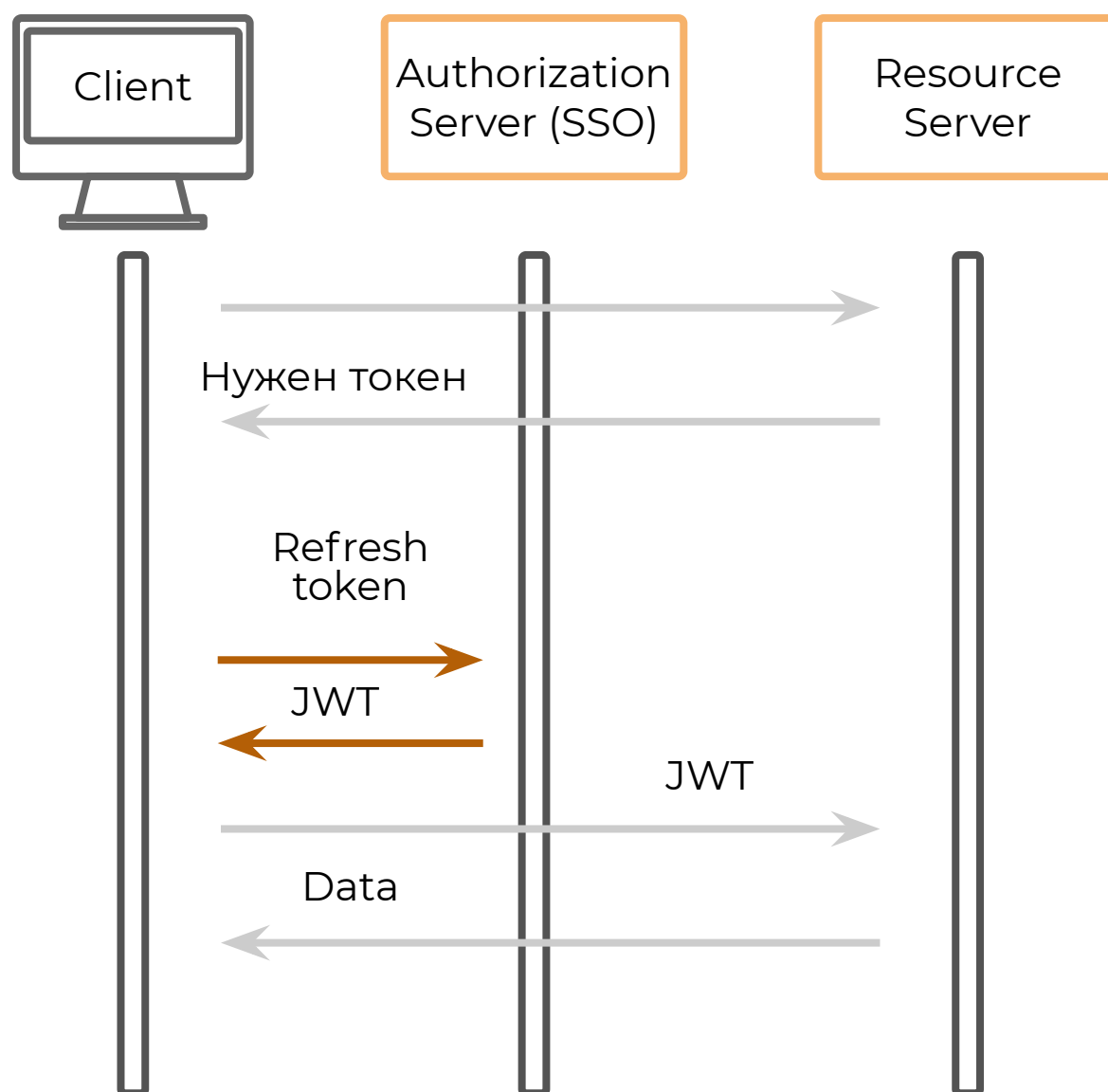




# OpenID Connect

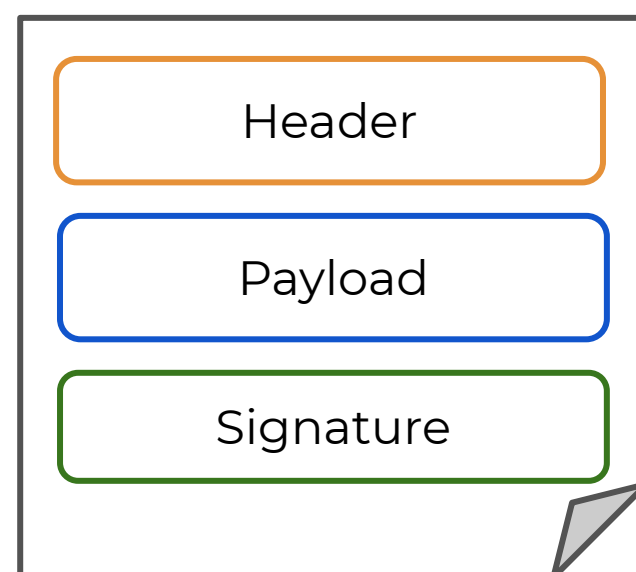


# OpenID Connect



# JWT token

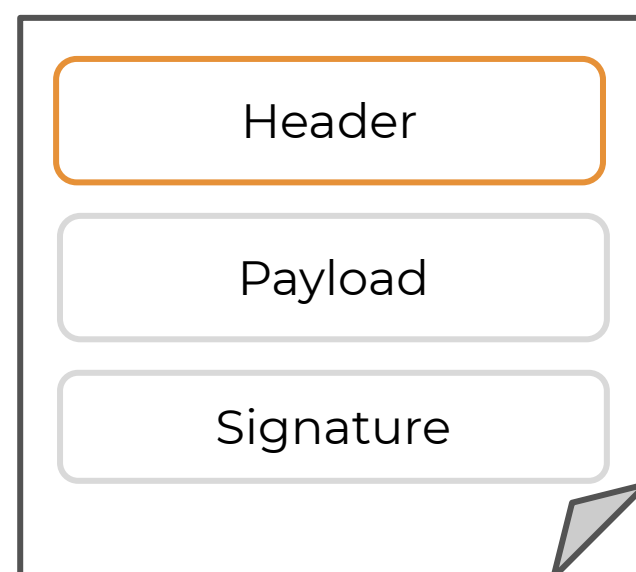
**JSON Web Token (JWT)** — это открытый стандарт (RFC 7519) для создания токенов доступа, основанный на формате JSON.



# JWT Header

- **Header** — для хранения информации о токене, о том, как его прочитать
- JSON в Base64-URL

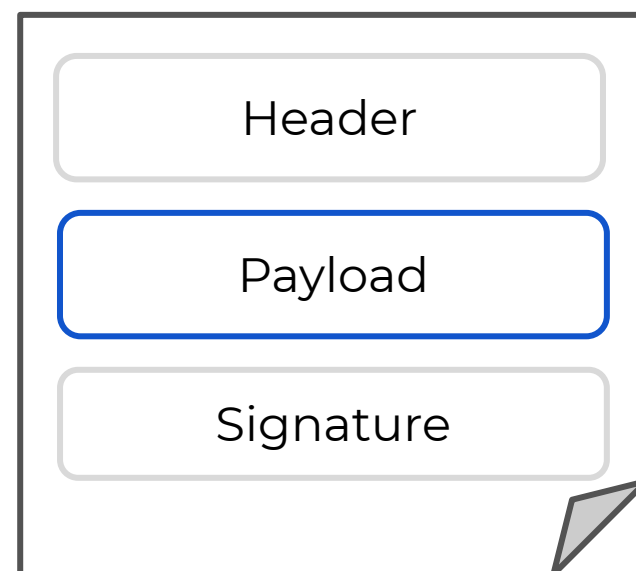
Например: {"alg":"HS256","typ":"JWT"}



# JWT Payload

- **Payload data** — полезная информация
- JSON в Base64-URL
- iss — имя приложения
- user\_id — идентификатор клиента

Например: {"sub": "1234567890",  
"name": "John Doe",  
"admin": true }

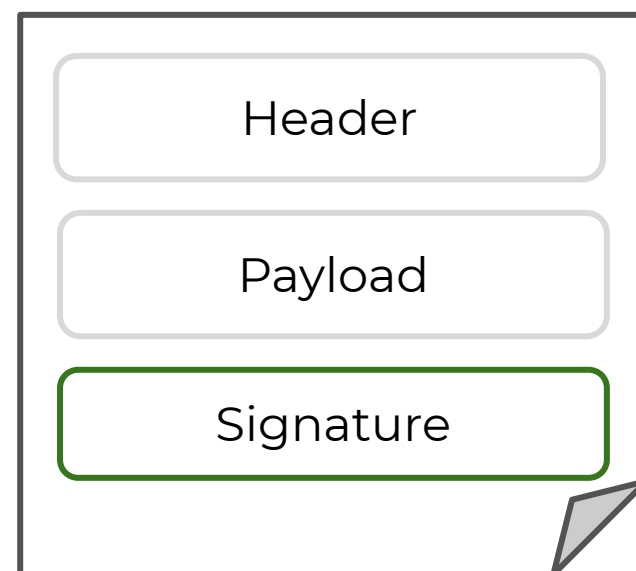


# JWT Signature

- **Signature** — цифровая подпись
- Подпись Base64-URL

Например:

```
HMACSHA256(  
base64UrlEncode(header) + "." +  
base64UrlEncode(payload) )
```



# Итоги

- Познакомились с OAuth 2.0
- Узнали, что OpenID Connect — это надстройка над OAuth 2.0
- Изучили SSO (KeyCloak)
- Выяснили, из чего состоят JWT-токены

# В следующем модуле

- Узнаем, что такое API Gateway
- Как его лучше применять
- Какие решения есть на рынке
- В рамках каких паттернов работает



Skillbox

**Спасибо  
за внимание!**