


# OAuth 2.0

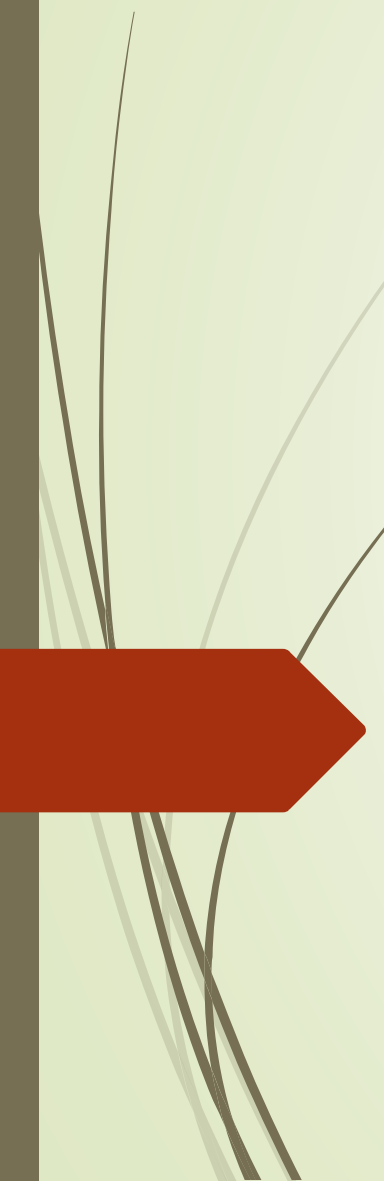
На примере доступа в *Office 365 Sharepoint API*  
с мобильного приложения

A large, solid red arrow pointing horizontally to the right, positioned below the text.



# Содержание

- Терминология
- Windows Azure OAuth 2.0
- Демо

- 
- *Область применения:* любой клиент поддерживающий HTTP протокол
  - *Требование безопасности:* все запросы следует делать по HTTPS
  - *Это фреймворк:* многое относится к деталям конкретной реализации. Например, подпись token-ов.
  - *Идентификатор клиента:* данные позволяющие службе авторизации различать клиентские приложения
  - *Область доступа:* каждое приложение должно сообщить службе авторизации о планируемых действиях.
  - *Максимальная гибкость:* возможность добавление своих claims в тело маркера доступа(*access\_token* )

# Схема взаимодействия

## Роли:

- Владелец ресурса
- Клиент
- Служба авторизации
- Сервер ресурса

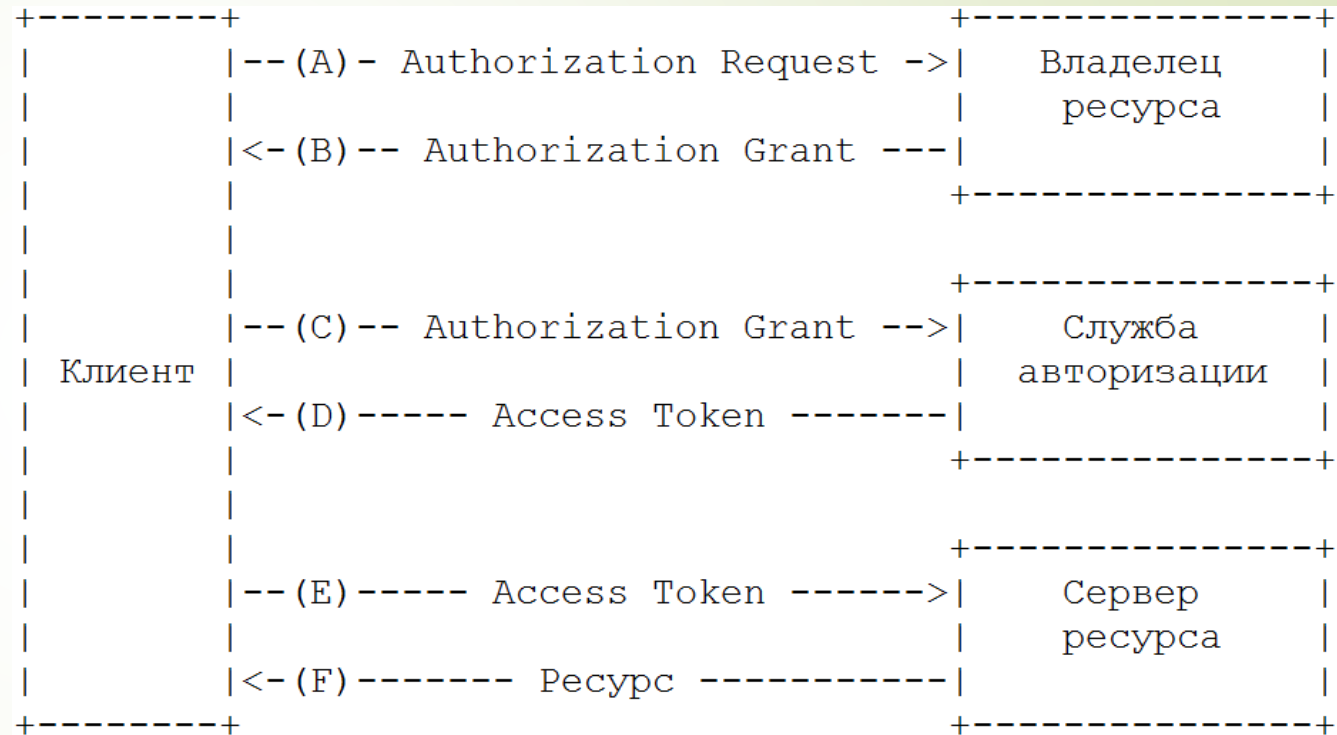
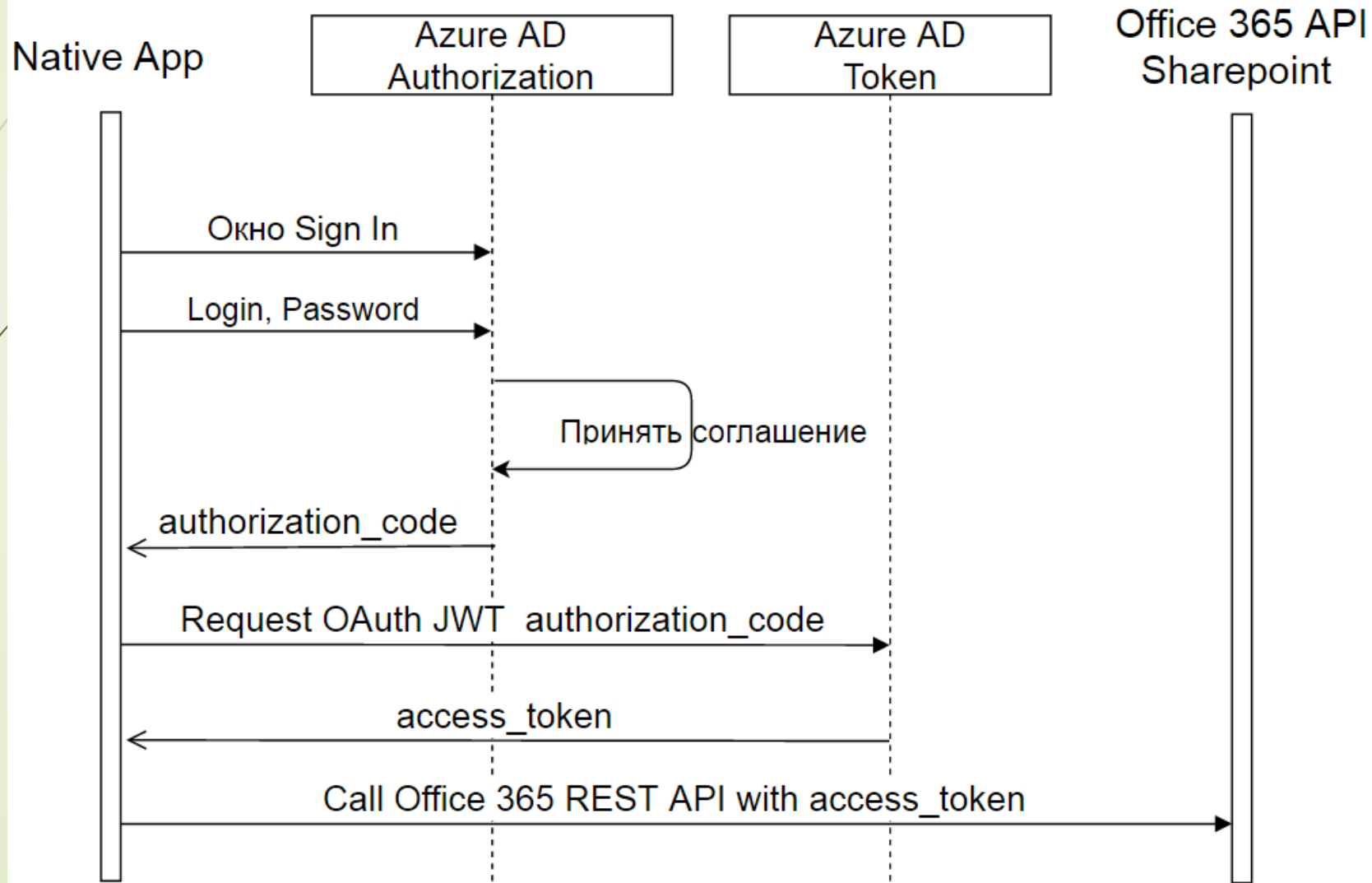


Рисунок 1: Общее взаимодействие по OAuth 2.0

# Azure AD Authorization Flow

## OAuth 2.0 Endpoints

<https://login.windows.net/<tenant>.onmicrosoft.com>



# OAuth 2.0 JWT access token

HEADER:

```
{  
  "typ": "JWT",  
  "alg": "RS256",  
  "x5t": "MnC_VZcATfM5pOYiJHMba9goEKY",  
  "kid": "MnC_VZcATfM5pOYiJHMba9goEKY"  
}
```

PAYLOAD:

```
{  
  "aud": "https://azhuravlev.sharepoint.com/",  
  "iss": "https://sts.windows.net/b12e8362-  
874e-4b18-a89e-8d4d2b9fab13/",  
  "iat": 1469251551,  
  "nbf": 1469251551,  
  "exp": 1469255451,  
  "acr": "1",  
  "altsecid": "1:live.com:0006BFFDF3BADA8E",  
  "amr": [  
    "pwd"  
  ],  
  "appid": "511f8f39-95e9-4fe4-b7b9-
```



# Демо



# References

- OAuth 2.0 specification <https://tools.ietf.org/html/rfc6749>
- JSON Web Token (JWT) <http://self-issued.info/docs/draft-ietf-oauth-json-web-token.html>
- Вячеслав Михайлов, «Безопасность в микросервисных приложениях» [https://www.youtube.com/watch?v=ifOgWMfoW\\_I](https://www.youtube.com/watch?v=ifOgWMfoW_I)
- "Getting Started with OAuth 2.0", Ryan Boyd, Publisher: O'Reilly Media
- OAuth 2.0 Threat Model and Security Considerations <https://tools.ietf.org/html/rfc6819>

## Критика OAuth 2.0

- OAuth 2.0 and the Road to Hell <https://hueniverse.com/2012/07/26/oauth-2-0-and-the-road-to-hell/>





Контактный e-mail

➤ [artem.zhur@hotmail.com](mailto:artem.zhur@hotmail.com)

Спасибо за внимание

