Пять видов аутентификации и где они обитают

skyeng

Намиг Нурмамедов

Backend Developer
in mobile team

n.nurmamedov@skyeng.ru
t.me/namig_nurmamedov

skyeng

🖖

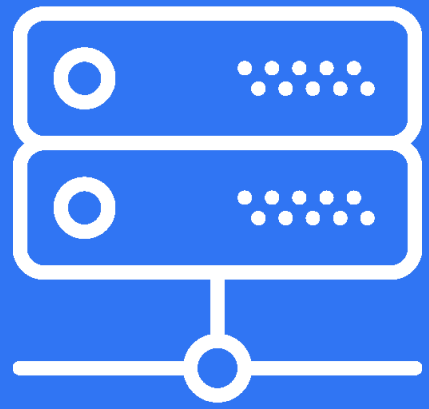
Экосистема Skyeng

- Обучающая платформа Vimbox
- Мобильное приложение для изучения слов
- Skyeng TV с субтитрами
- Расширение для браузера
- И многое другое

skyeng

Аутентификация бывает:

Клиентская



Межсерверная

skyeng

Виды аутентификации

- Session
- JWT
- OAuth 2.0
- Query Token
- Basic Http

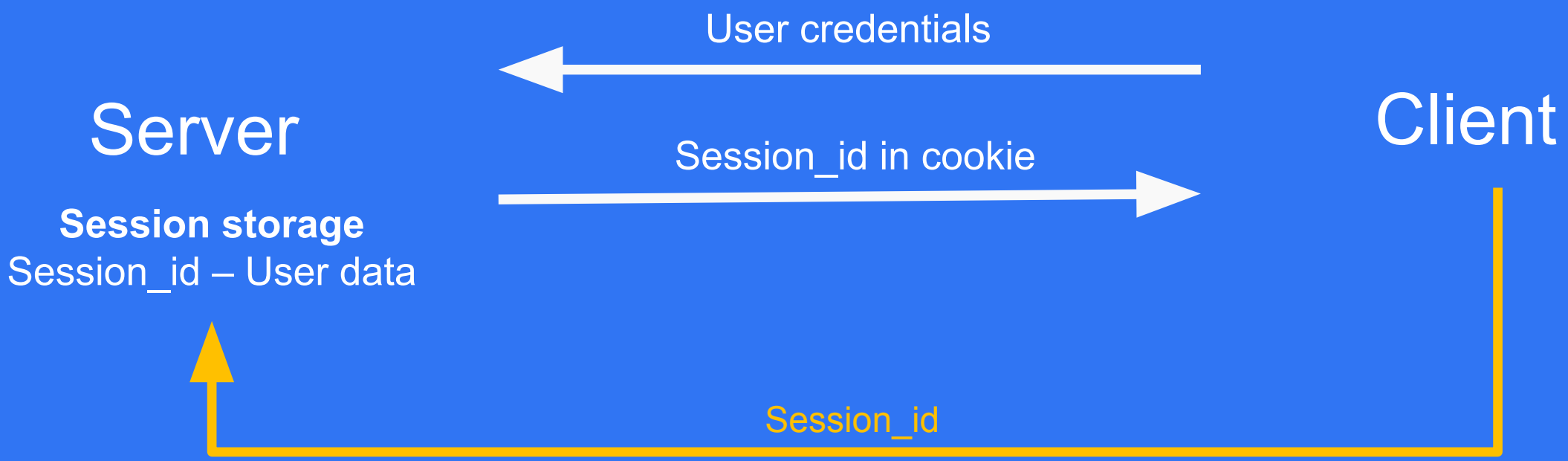
skyeng

Аутентификация в монолитных приложениях

- Исторически, аутентификация была **stateful** сервисом.
- Аутентификация встроена в сервер монолитного приложения.

skyeng

Сессия



skyeng

Использование сессии в skyeng

Open

words.skyeng.ru

Redirec
t

id.skyeng.ru
?redirect=words.skyeng.ru

- User log in
- Set browser cookie session_id=123 for domain *.skyeng.ru

Redirect back

Send session_id=123

GET id.skyeng.ru/session
?session_id=123

Return user data

- Check user roles
- Show homepage

skyeng

Аутентификация и микросервисы

- **Аутентификация** — предоставление доказательств, что вы на самом деле есть тот, кем идентифицировались.
- **Авторизация** — проверка, что вам разрешен доступ к запрашиваемому ресурсу.

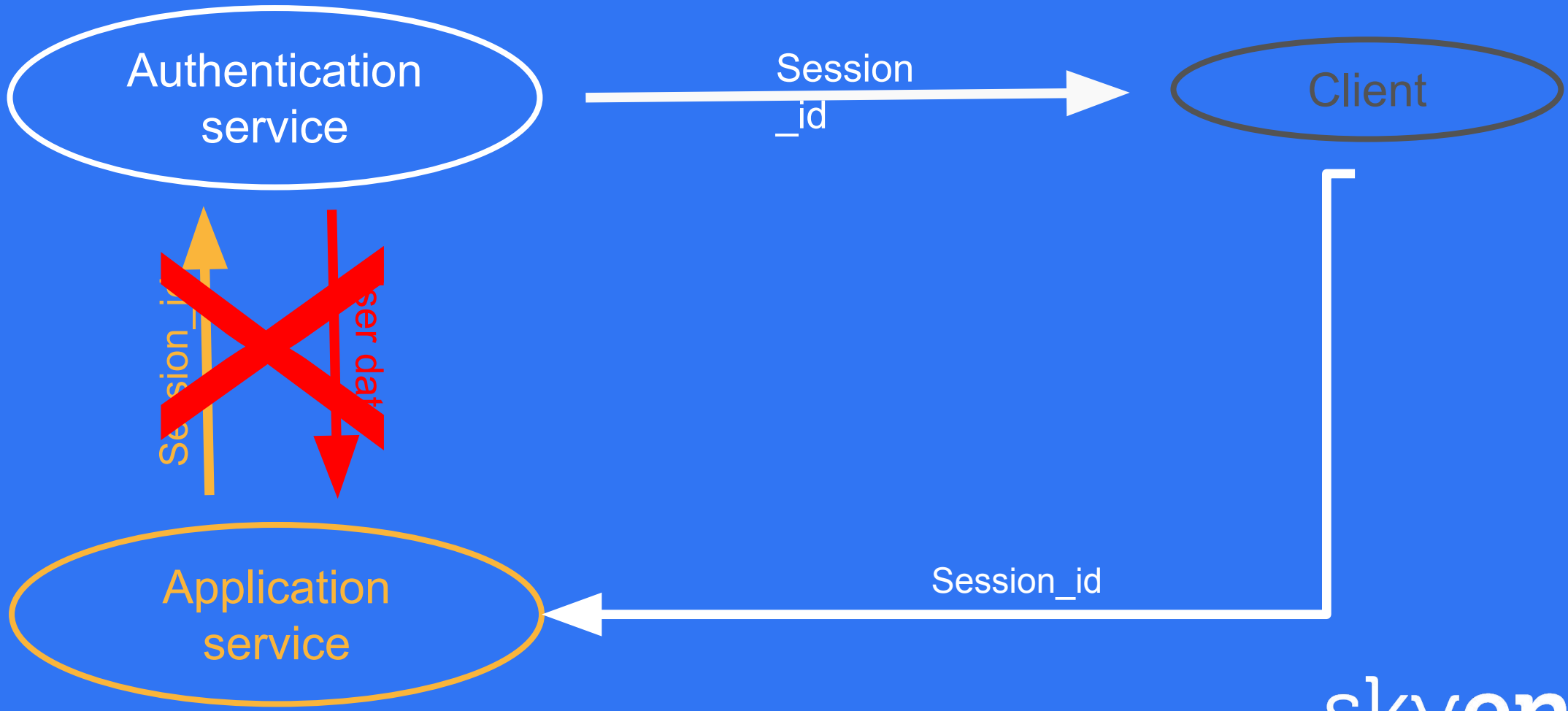
skyeng

В контексте микросервисов

- **Аутентификация** представляет из себя сервис.
- **Авторизация** - общая для всех сервисов функциональность.

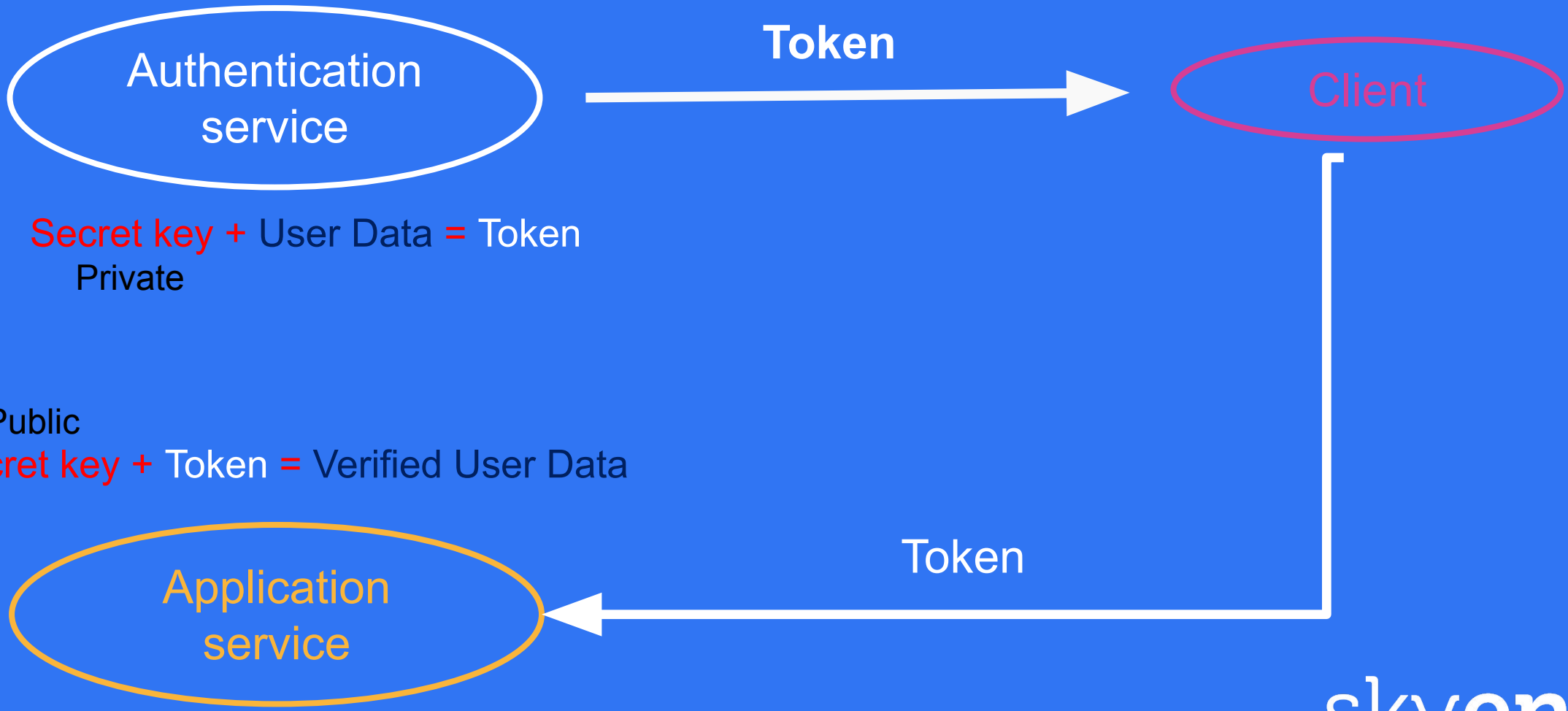
skyeng

В контексте микросервисов



skyeng

В контексте микросервисов



skyeng

Json Web Token - JWT

skyeng

JWT.IO

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

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

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) secret base64 encoded
```

Signature Verified

SHARE JWT

skyeng

JWT.IO

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ewogICJzdWIiOiAiMTIzNDU2Nzg5MCIsCiAgIm5hbWUiOiAiQWRtaW4iLAogICJpYXQiOiAxNTE2MjM5MDIyCn0.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "Admin",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

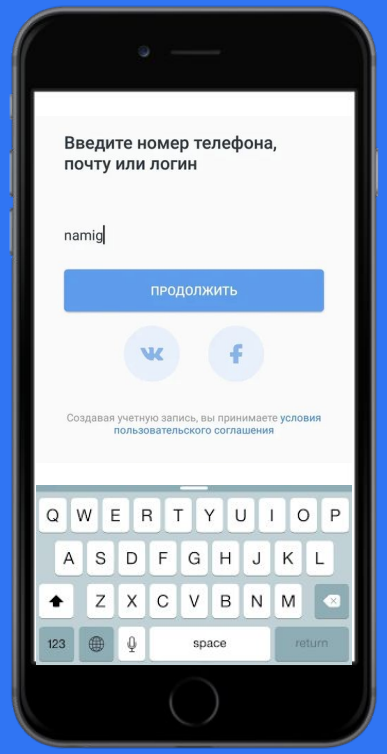
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) secret base64 encoded
```

⊗ Invalid Signature

SHARE JWT

skyeng

Использование JWT



Приложение для изучения слов

Login / password

JWT / user_id

Сервис Words

Login / password

JWT

Сервис Auth

skyeng

Почему мы не генерируем JWT в сервисе Words?

- Это ответственность сервиса Auth
- Токен созданный в нашем проекте не сможет использоваться в других

skyeng

Какие инструменты использует мобильный бэкенд?

- Symfony Guard Authentication System
- LexikJWTAuthenticationBundle

skyeng

Как работаем с JWT локально и в тестах?

- Моки пользователей с разными ролям
- В качестве токена используется логин пользователя

skyeng

OAuth 2.0

OAuth 2.0 — протокол авторизации, позволяющий выдать одному сервису (приложению) права на доступ к ресурсам пользователя на другом сервисе.

skyeng

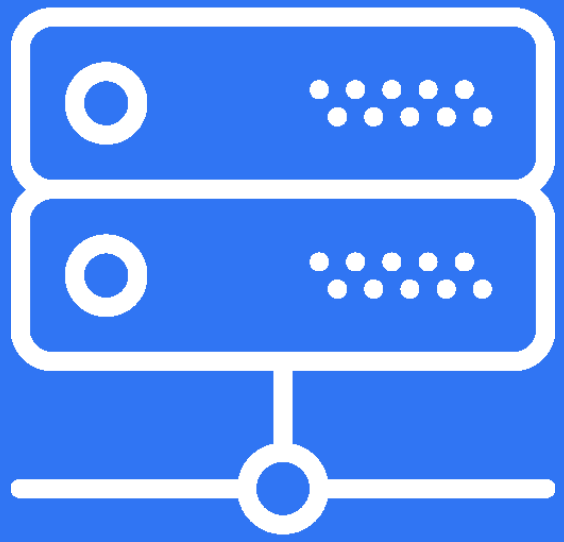
OAuth 2.0: роли

Владелец ресурса

Пользователь, данные которого мы будем шарить

skyeng

OAuth 2.0: роли



Сервер ресурсов

Приложение, которое содержит защищенные ресурсы

skyeng

OAuth 2.0: роли

Сервер авторизации

Приложение, которое подтверждает подлинность пользователей

skyeng

OAuth 2.0: роли

Клиент

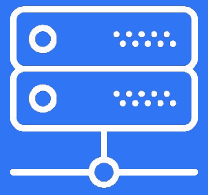
Приложение, которое делает запросы к серверу ресурсов от имени владельца ресурса

skyeng

OAuth 2.0 в Skyeng

Ученик школы

Браузерное расширение



Сервис Words

Сервис Auth

skyeng

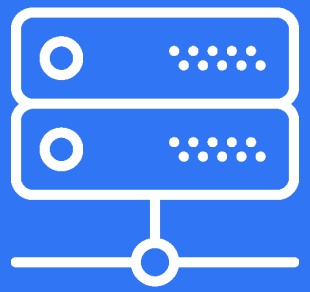
OAuth 2.0

Привет, браузерное расширение.
Я хочу посмотреть список своих слов на изучении

Сервис Words, можешь дать мне список слов пользователя?

Привет, сервис Auth. Могу я получить access_token?
Сервис Words спрашивает его. Ну пожалуйста)

Извини, друг, это защищенный ресурс.
Тебе нужно передать мне access_token.



OAuth 2.0

Ноу проблем, сир. Мой логин **n.nurmamedov@skyeng.ru** и пароль **secret**.

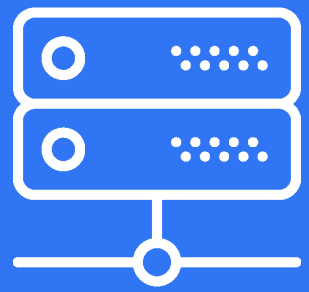
Привет, друг. Можешь предоставить мне свои доступы? Мне нужно тебя идентифицировать.

Ноу проблем, сир. Мой логин **n.nurmamedov@skyeng.ru** и пароль **secret**.

Привет, друг. Можешь предоставить мне свои доступы? Мне нужно тебя идентифицировать.

Чуши, дорогой. Мне нужно спросить несколько вопросов у пользователя.

Вот access_token: aKJkqKw1qk5yeuTokn2Jlq



OAuth 2.0

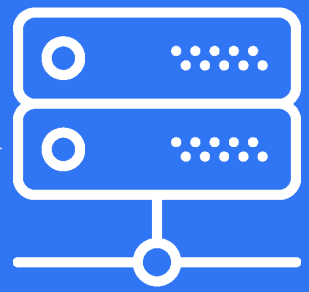
Вот твой список слов. Учи на здоровье!

Сервис Words, вот access_token:
qKJkqkw1qk5yeuTolkpKn2Jlq

Все в порядке. Получай список слов.

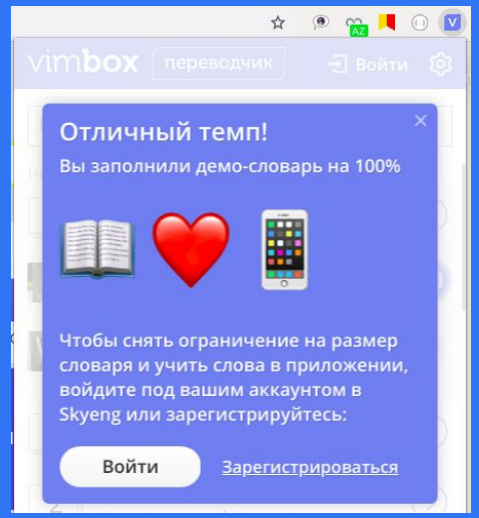
Привет, мне дали qKJkqkw1qk5yeuTolkpKn2Jlq
Можешь сказать, кому он принадлежит?

Да, конечно, этот токен валиден и принадлежит
n.nurmamedov@skyeng.ru

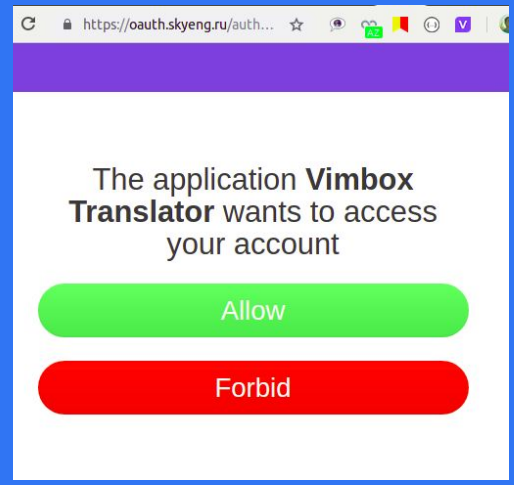


Использование OAuth 2.0

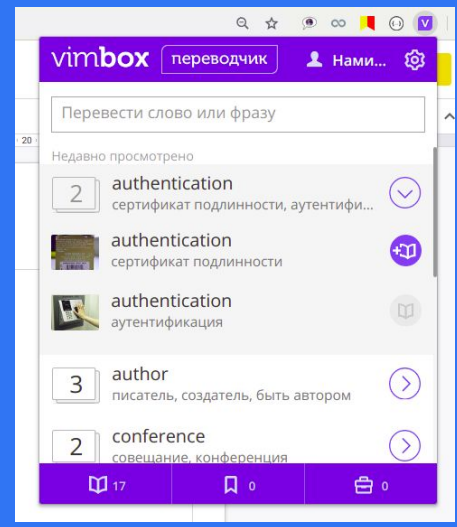
Шаг 1: Аутентификация в браузерном расширении



client_id
redirect_uri
response_type=code



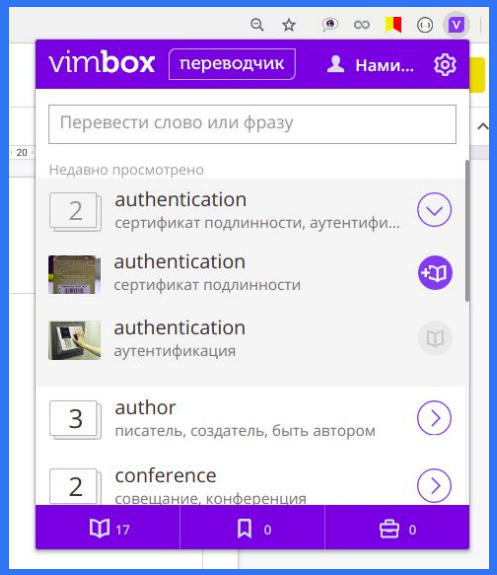
access_token

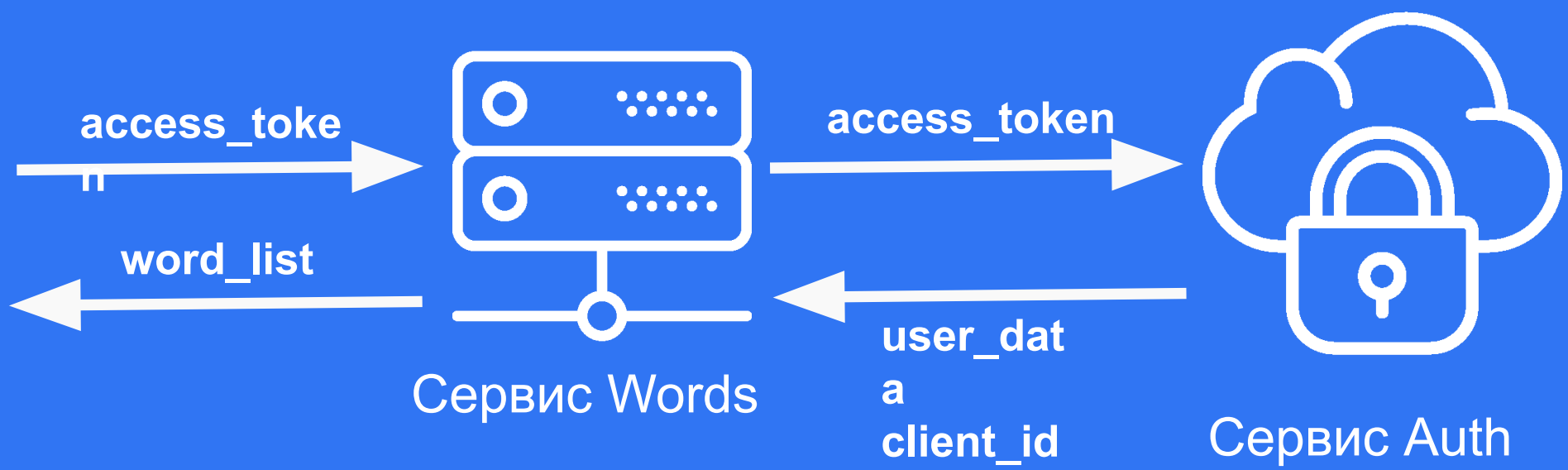


skyeng

Использование OAuth 2.0

Шаг 2: Получение списка слов на изучении





skyeng

Query Token

- Токен передается в строке запроса вместе с email пользователя.
- Используется в публичном API для пользователей.
- Токен отправляется пользователю на email по запросу.

skyeng

Query Token

GET api.words.ru/api/public/words
?email=n.nurmamedov@skyeng.ru
&token=bcfaa

skyeng

Query Token

- Токен генерируется на основе хэш-функции по email + secret key.
- Токены не хранятся на сервере.

skyeng

Basic Http

- Для аутентификации между внутренними сервисами Skyeng

skyeng

Вывод

Существуют разные виды аутентификации и каждый из них имеет свою область применения

skyeng

ВОПРОСЫ?

skyeng