.NET 9
Pushed authorization request

Никитин Валерий

О чем доклад?

- авторизация и аутентификация;
- OAuth;
- OpenID, OIDC;
- PAR, RAR;
- PAR в .NET 9;

Аутентификация

Процесс проверки подлинности пользователя, письма, ресурса:

- вход в операционную систему;
- разблокировка мобильного устройства;

OpenID, OIDC

- единый стандарт аутентификации, через третий провайдер аутентификации;
- часто работает в связке с OAuth2;

Авторизация

Процесс подтверждения прав доступа к каталогу, базе данных, веб-сайту

- при выполнении SQL-запроса;
- при открытии папки;
- при входе в раздел сайта;

OAuth

- процесс авторизации, предоставляющий доступ третьей стороне, к ресурсам пользователя, без раскрытия логина-пароля пользователя;

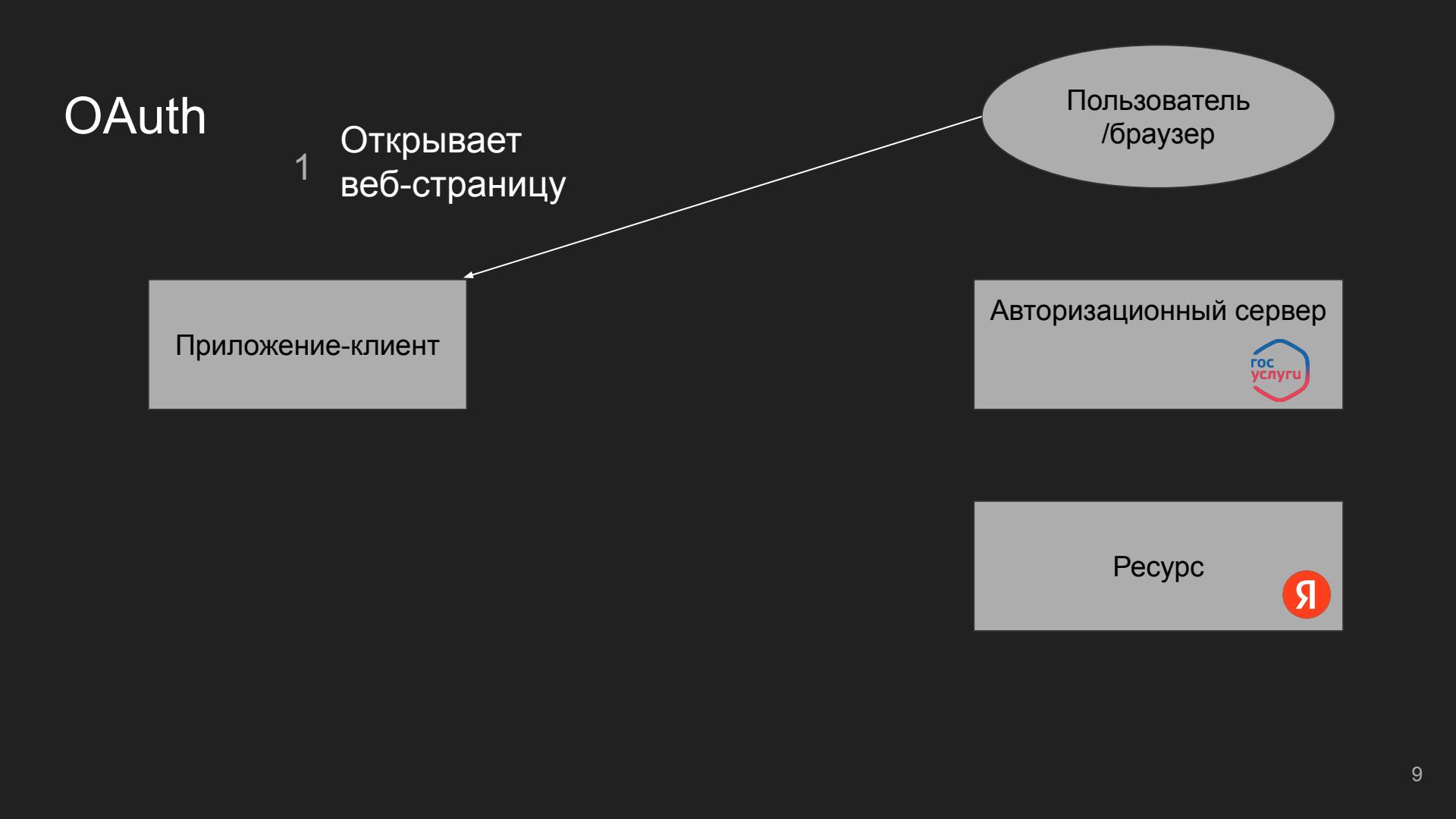
Как работает OAuth

OAuth, кто есть кто

- пользователь (владелец ресурса API);
- приложение-клиент;
- ресурс API;
- авторизационный сервер;

OAuth

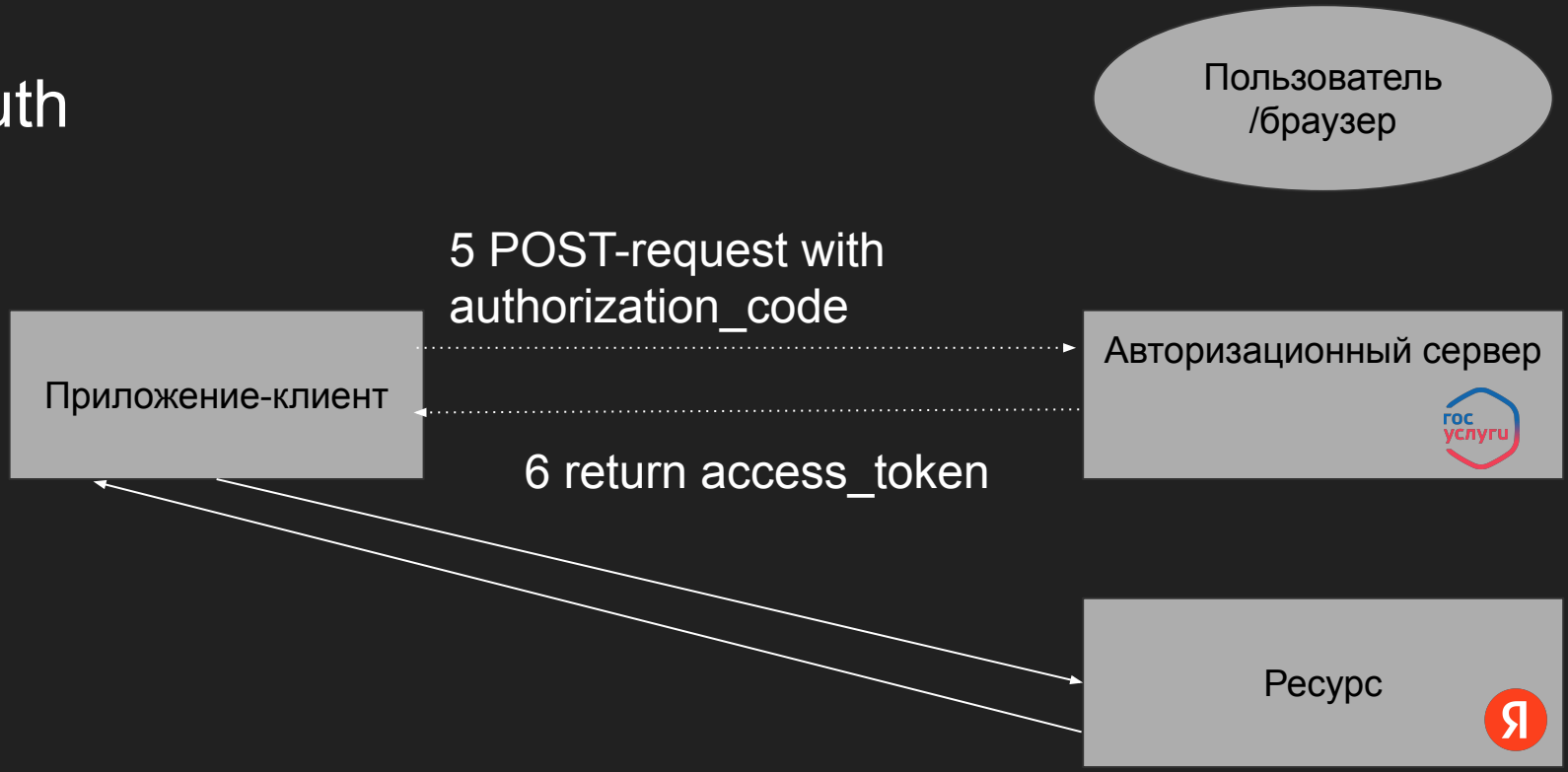
1 Открывает веб-страницу



OAuth

Мне нужны твои (сапоги) контакты

OAuth


Пользователь
/браузер
5 POST-request with
authorization_code
Приложение-клиент
Авторизационный сервер
гос
услуги
6 return access_token
Ресурс
Я

Rich Authorization Request

- обычный OAuth2 с обычным набором scope;

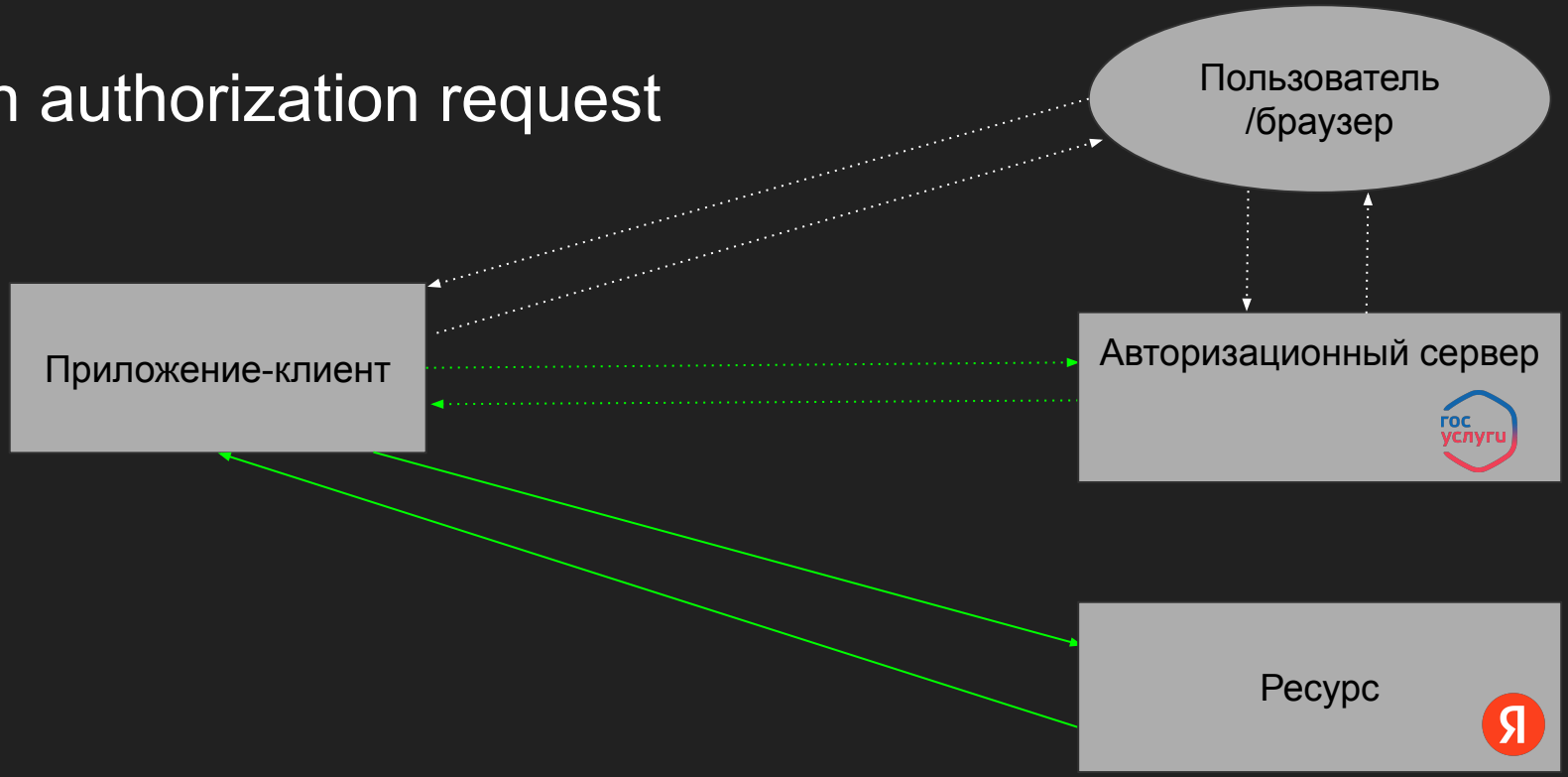
```
https://authorization-server.com/oauth/authorize?
response_type=code
&client_id=YOUR_CLIENT_ID
&redirect_uri=YOUR_REDIRECT_URI
&scope=read write
&state=RANDOM_STRING
```

Rich Authorization Request

- примеры scope для RAR;
- в query запроса добавляем, большой authorization_details, с перечислением конкретных действий;

```
https://authorization-server.com/oauth/authorize?
response_type=code
&client_id=YOUR_CLIENT_ID
&redirect_uri=YOUR_REDIRECT_URI
&scope=openid
&state=RANDOM_STRING
&authorization_details=[{
    "type": "payment_initiation",
    "locations": ["https://api.bank.com/payments"],
    "instructedAmount": {
        "currency": "EUR",
        "amount": "100.00"
    },
    "creditorAccount": {
        "iban": "DE02100100109307118603"
    }
}]
```

Rich authorization request



Недостатки

- участвует третья сторона в виде браузера;
- данные могут утечь злоумышленникам;
- могут залогироваться в промежуточных системах;
- избыточность запроса;

Push authorization request

- запрос на авторизацию отправляется с бэкенда, без участия клиента;
- клиент проходит авторизацию на доступ по request_id;

Push authorization request

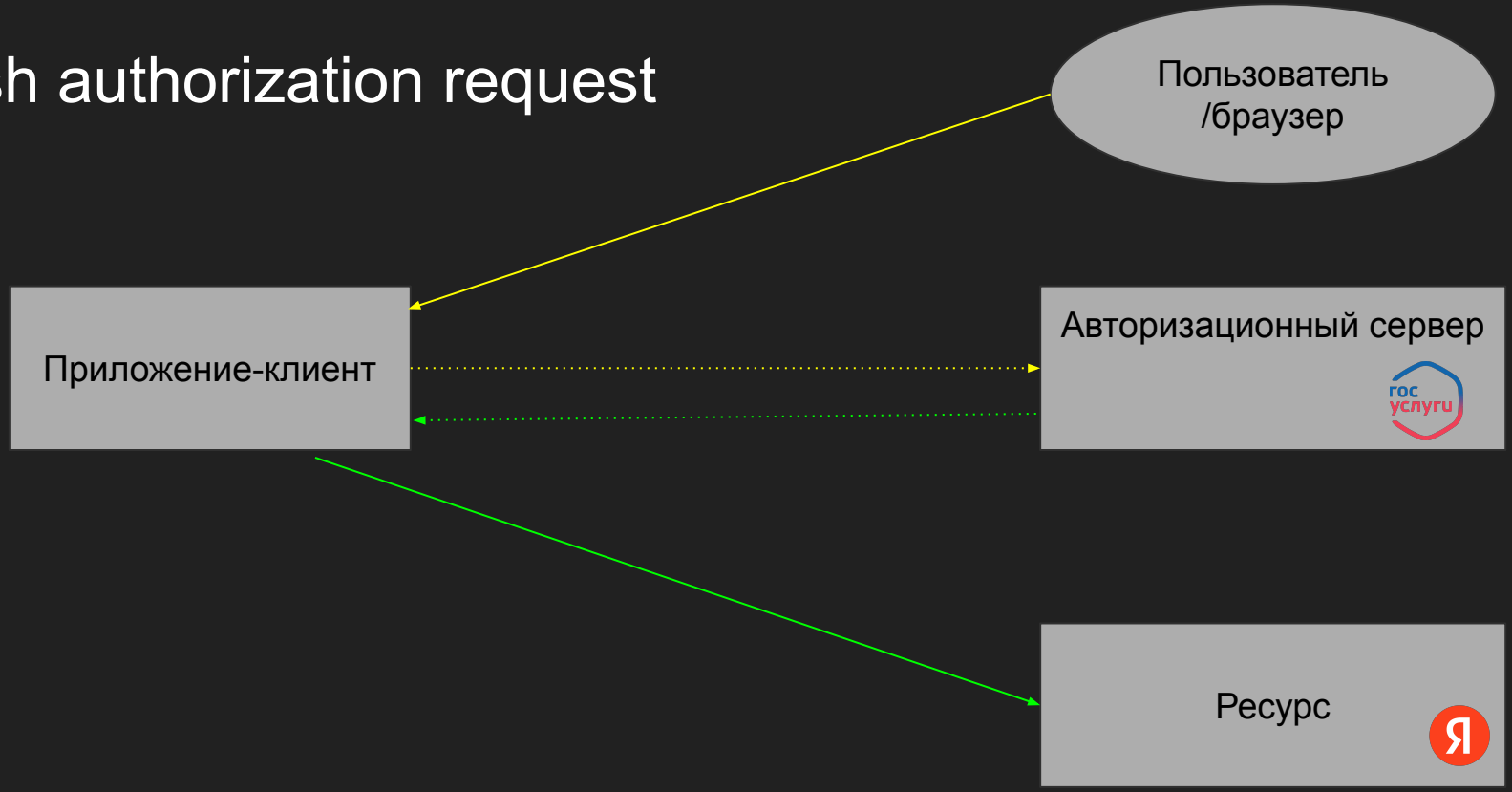
POST-запрос к авторизационному серверу с набором параметров и возвращение id запроса на авторизацию

Push authorization request

запрос на получение access_token с
id заявки

Ресурс

Push authorization request



запрос к ресурсу с access_token

Таблица сравнений

	RAR	PAR
Чувствительная информация	Передается в query GET-запроса	Передается в body POST-запроса
Тип http запроса	GET	POST

Push authorization request в .NET 9

- включен по-умолчанию;
- добавлен enum PushAuthorizationBehaivor;

```
public enum PushedAuthorizationBehavior
 {
    UseIfAvailable,//DEFAULT
    Disable,
    Require
 }
```

Как это работает в целом?

- как начать работать с PAR?
  - /.well-known/oauth-authorization-server:
    - используем flow который рассказали ранее;
  - если не поддерживается:
    - то используем flow обычного Oauth, либо выдаем exception;

Push authorization request в .NET 9 в клиенте

```
.AddOpenIdConnect("oidc", oidcOptions =>
    {
        oidcOptions.PushedAuthorizationBehavior = PushedAuthorizationBehavior.Disable;
    });
```

OpenConnectIdEvents

- можем конфигурировать поведение при авторизации, нужным нам образом;

Вывод:

- делает процесс авторизации более безопасным;
- автоматически включено в .NET 9;
- можно конфигурировать и влиять на поведение авторизации;

Список литературы: