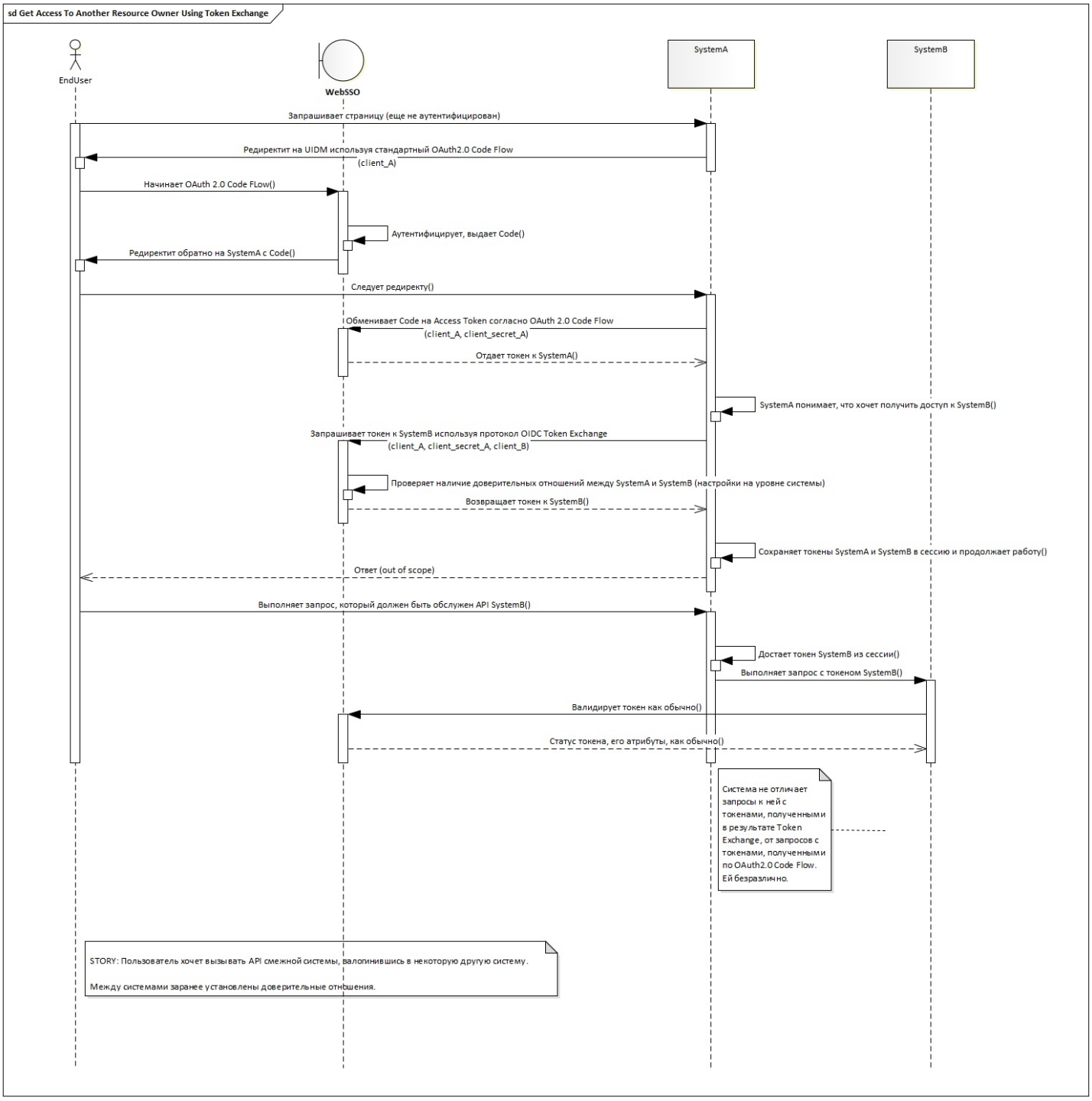
OpenID Connect Token Exchange - получение токена по другому токену

Оглавление

Конечная точка
Получение токена для стороннего сервиса - новый вариант согласно спецификации
Поддержка старого протокола получения обмена токенов
Конфигурация
Особенности и ограничения
Ссылки на внешнюю документацию

После успешной аутентификации пользователя сервис, выполняющий аутентификацию, получает токен доступа, привязанный **к своему сервису.**

Если пользователь хочет вызывать API другого сервиса, находящегося так же под прикрытием UIDM, следует получить новый токен доступа, который будет привязан к целевому сервису.



Конечная точка

```
GET https://{sso_host}/sso/oauth2/access_token
```

- Референсная спецификация: OpenID Connect Discovery 1.0
- Предоставляется сервисом: `sso-server`

Получение токена для стороннего сервиса - новый вариант согласно спецификации

Запрос

```
POST /sso/oauth2/access_token
Host: {sso_host}
Accept: application/json
Content-Type: application/x-www-form-urlencoded

client_id=<client_id>& (1)
client_secret=<client_secret>& (2)
grant_type=urn:ietf:params:oauth:grant-type:token-exchange& (3)
urn:vnd-roox:params:oauth:realm=/customer& (4)
subject_token=<access_token>& (5)
audience=<aud>& (6)
```

1. Идентификатор текущего сервиса
2. Секрет текущего сервиса
3. Выбор протокола Token Exchange стандартным для этого OIDC параметром - grant_type
4. Реалм пользователя
5. Access token пользователя в текущем сервисе
6. Идентификатор сервиса, токен для которого получаем

Успешный ответ

```
HTTP/1.1 200 OK
Content-Type: application/json
```

```
{
  "cn": "9263752235",
  "realm": "/customer",
  "token_type": "Bearer",
  "access_token": "960a5a04-2e02-4af6-913d-c599faa1faef", (1)
  "expires_in": 28 (2)
}
```

1. Выданный токен доступа к запрошенному сервису
2. Время жизни выданного токена

Неуспешный ответ

```
HTTP/1.1 401 Not Authorized (1)
```

```
{
  "error": "invalid_grant", (2)
  "error_description": "" (3)
}
```

1. Любой 4xx код трактовать как ошибочный и non-retryable. Любые 5xx коды трактовать как ошибочный и retryable
2. Код ошибки, см. таблицу ниже
3. Описание ошибки для разработчика/техподдержки, выводить в лог

Таблица 1. Коды ошибок `error`

Код	Причина	Что делать
invalid_request	Запрос сформирован некорректно	Разработчикам свериться с документацией
invalid_client	Идентификатор, секрет системы или реалм неверен	Техподдержке проверить креденшелы системы, вместе с техподдержкой WebSSO убедиться, что система не заблокирована
invalid_grant	Переданный токен невалиден	Получить новый токен и повторить запрос с ним
unauthorized_client	Система не имеет права использовать token exchange	Обратиться к техподдержке WebSSO
unsupported_grant_type	Token exchange не включен на данном инстансе WebSSO	Обратиться к техподдержке WebSSO

Поддержка старого протокола получения обмена токенов

В настоящий момент поддерживается и старая схема (получение токена через обращение на /sso/authentication/).

Схема будет выведена из эксплуатации, поэтому рекомендуется перейти на новую схему в ближайшее время.

Конфигурация

- В настройках OAuth2 клиента, которому будет разрешено использовать Token Exchange, установить свойство `audience`. Значение - идентификаторы OAuth2 клиентов, для которых будут выпускаться новые токены.

Параметр является массивом, следует использовать особый синтаксис.

Пример файла конфигурации клиента

```
clientName=onlinebank_web

audience[0]=esb
audience[1]=sms_gateway
```

Данный пример конфигурации разрешает клиенту onlinebank_web обменивать свой токен доступа на токен доступа к клиентам esb, sms_gateway.

Особенности и ограничения

1. Token Exchange позволяет за одно обращение обменять токен только для одного целевого сервиса. Для получения токенов для обращения к разным сервисам, выполняйте несколько запросов.

Ссылки на внешнюю документацию

OIDC Token Exchange https://tools.ietf.org/html/draft-ietf-oauth-token-exchange-16 OAuth Errors https://tools.ietf.org/html/rfc6749#section-5.2