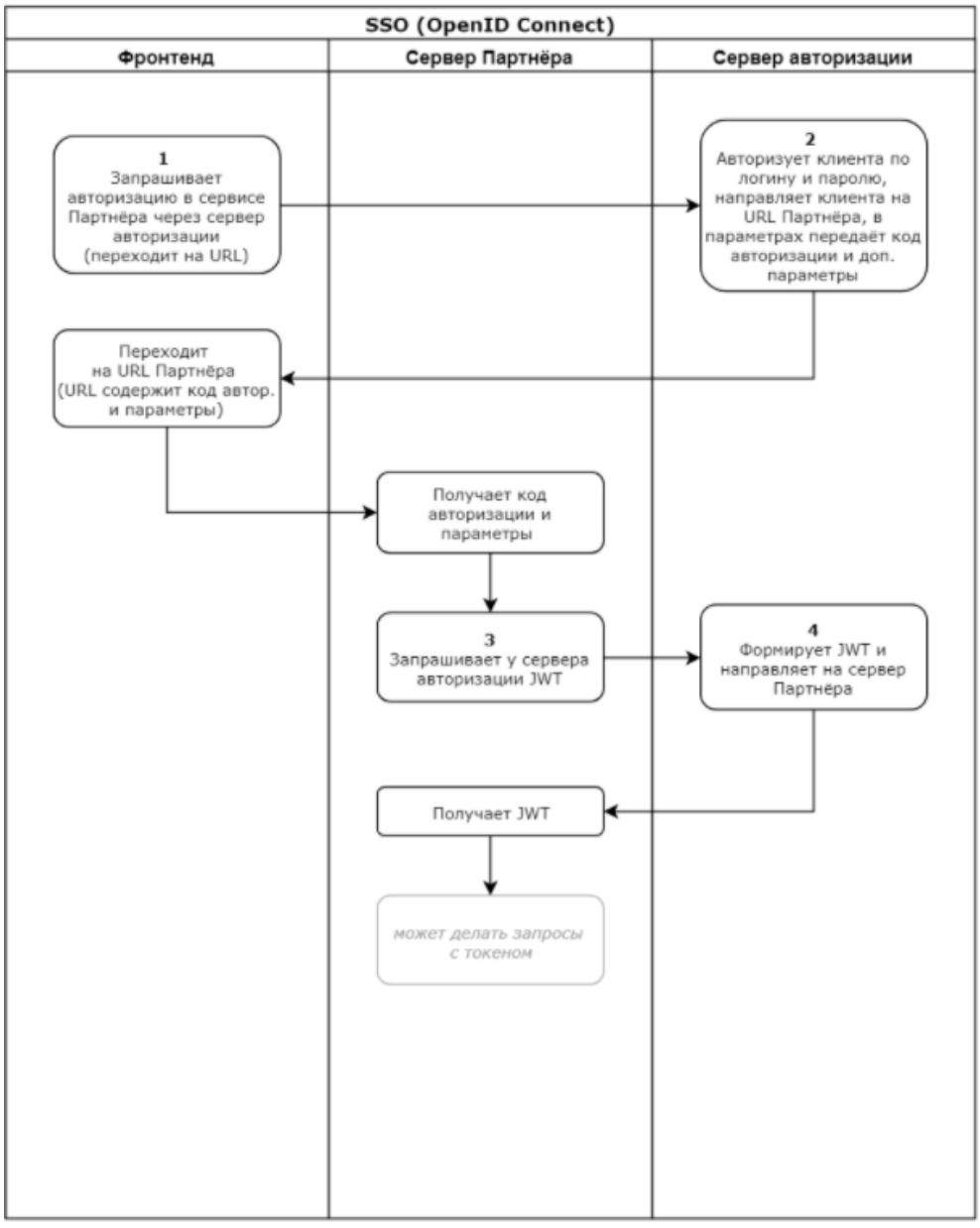
Функциональные характеристики и информация необходимая для установки, эксплуатации модуля «Identity Server»

Продукт предназначен для контроля и управления доступом сервисов друг к другу, без необходимости ввода логина и пароля пользователя в каждом конкретном сервисе, где он уже зарегистрирован. Должен представлять собой серверный компонент для реализации технологии единого входа в рамках внутренних и внешних функциональных систем.

Общее описание концепции авторизации.

Авторизация происходит с помощью Identity Server на стороне любого стороннего сервиса (например, Маркетплейса) по стандарту OpenID Connect.



1. Запрос для открытия окна ввода логина/пароля и предоставления разрешений

GET https://auth.artsofte.ru/connect/authorize?scope=openid offline_access profile legal_info&response_type=code&client_id=test&redirect_uri=http://localhost:5002/signin-oidc

Реквизиты Партнёра (логин/пароль):

- test / test Secret

Пользователи в нашей тестовой системе (логин/пароль):

- user1/pass
- user2/pass
- user 3/ pass (не заполнены ИНН и КПП)

Параметры запроса:

1. scope - набор тех прав и возможностей, которые нужно получить от имени пользователя Заказчика
    - openid - обязательно для использования
    - offline_access - передавать, если требуется refresh_token
    - profile - минимальная инфо о пользователе: Id, логин
    - legal_info - юр. данные пользователя для идентификации (ИНН и КПП)
2. response_type - обязательное поле, передать значение code
3. client_id - «логин» сервера Партнёра, выданный ему (test)
4. redirect_uri - адрес на стороне Партнёра, куда будет отправлен Код для получения JWT (в примере указан http :// localhost :5002/ signin - oidc)

2. Авторизация клиента и направление на URL Партнёра

Первый вариант, если пользователь согласился предоставить права → скриншот .

GET http://localhost:5002/signin-oidc?code=425f9b52a414b7843b2ba0bd25f025039fc937fd2fececa7be0000d4f38be083&scope=openid%20profile%20legal_info%20offline_access&session_state=DF4xnu0fchKOTIwkDWxsP7c3dzn_PX_L09XhCaCJOTY.bbd282e5fae27c92f0ad694a29bfdaa8

Код авторизации передаётся в поле code .

Второй вариант, когда пользователь отказался предоставить права → скриншот .

GET http://localhost:5002/signin-oidc?error=access_denied#_=_

Партнёр понимает, что по какой-то причине, указанной в error, Код ему не передан.

3. Запрос на получение JWT

POST https://auth.artsofte.ru/connect/token

- Используется Basic-аутентификация с логином/паролем от Партнёра (test / test Secret).

Http-заголовки:

- Authorization:Basic edSbW9Vsbzb2VkZWxvU2VfSkTh0
- Content-Type:application/x-www-form-urlencoded

Тело POST- запроса

- grant_type:authorization_code
- code:52e52b78cbe98b5ee548d56a61d3f6778303c4544c58ec6c224a074099c434eb
- redirect_uri:http://localhost:5002/signin-oidc

4. Отправка JWT

Пример ответа


```
{
   "id_token":
"eyJhbGciOiJSUzI1NiIsImtpZCI6IjFERkIzODk1MDMwRTc1M0E4NTQ2Njg2OTAyMkQzQzc5N
0U5MkM1Q0EiLCJ0eXAiOiJKV1QiLCJ4NXQiOiJIZnM0bFFNT2RUcUZSbWhwQWkwOGVYNlN
4Y28ifQ.eyJuYmYiOjE1MjIyMTc0NDQsImV4cCI6MTUyMjIxNzc0NCwiaXNzIjoiaHR0cDovL2F
1dGguYXJ0c29mdGUucnUiLCJhdWQiOiJtb2VkZWxvI3NDQ0LCJhdF9oYXNoIjoiUGZzbHNYdV
RfLVRxUVBFVEx3alpiZyIsInNpZCI6ImQwZTBkMTY1NzNiZWFjMjgyMDZlODY1MmJmZDk4N
TA0Iiwic3ViIjoiMTkiLCJhdXRoX3RpbWUiOjE1MjIyMTczOTAsImlkcCI6ImxvY2FsIiwiYW1yIjpb
InB3ZCJdfQ.d4Tf47vm8iNCLw2t54xF_jRWLivLomNaaWLnhUnSpaK0javgMc9uBudKVf7l1op
FGKFUDH9QdL2y-jOlV6_jTiMkCJofPD7SgeGGnJUJ2jllX_GKw6b-
XXYbja05hrK6sNxa9NCTj54OKyVnq2pwn4xnR5A9JN4PAsMiF7N9BIh4fKbse7_HAu_t_4cl3
MaRKBxHihzVcMHG_3sDfBiovSxn4HzqTFBoZy64hiVIlzK6M_B4bG0XJWS-
YWJffEuFodmWl76uNwP4-
KTb3OWkymbPXNkkWSGK6wO6Yqe9M4u8X_mEx1PgJZcCptNK3Ayi6LN8znyvKwxPbVAHxx
PMBg",
   "access_token":
"eyJhbGciOiJSUzI1NiIsImtpZCI6IjFERkIzODk1MDMwRTc1M0E4NTQ2Njg2OTAyMkQzQzc5N
0U5MkM1Q0EiLCJ0eXAiOiJKV1QiLCJ4NXQiOiJIZnM0bFFNT2RUcUZSbWhwQWkwOGVYNlN
4Y28ifQ.eyJuYmYiOjE1MjIyMTc0NDQsImV4cCI6MTUyMjI1MzQ0NCwiaXNzIjoiaHR0cDovL2
F1dGguYXJ0c29mdGUucnUiLCJhdWQiOlsiaHR0cDovL2F1dGguYXJ0c29mdGUucnUvcmVzb3
VyY2VzIiwiQXBpUmVzb3VyY2VfTEsiLCJBcGlSZXNvdXJjZV9NYXJrZXRQbGFjZSJdLCJjbGllbnRf
aWQiOiJtb2VkZWxvIiwic3ViIjoiMTkiLCJhdXRoX3RpbWUiOjE1MjIyMTczOTAsImlkcCI6ImxvY
2FsIiwibmFtZSI6InVzZXIxIiwiZW1haWwiOiJ1c2VyMTFAZ21haWwuY29tIiwiSpUmVzb3VyY2
VfTEsiLCJBcGlSZXNvdXJjZV9NYXJrZXRQbGFjZSIsIm9mZmxpbmVfYWNjZXNzIl0sImFtciI6WyJ
wd2QiXX0.nS8Ol3MXJp8xnZJ_lgxUsJyCY6Z2xMsURXj0VnvPu4RyZSRR0PG2KnCdfubQavMy
T0Zg1WWPsumTuNBJJKePRt9iIQ_untyJaF4BTncJdI39QlEgsSoAPF_xmu3yUl8XonFsXMGrjo
AI88S2IzN6f9m_4o-
VtPJP11W6p9f0_oNcIIwfSqDPuFfhsAhTpiLRSVk2bGjd8c3t8GRrXACHAP9If-
sj3QTwjHDVs5DkC1CjfvsunetM0_tA6BvMV9l8_pZ9eFQXZX1f-
gmNliwI3BGWKDJOHw6hV0YwF-Xi3CPJRNE9lnVuMavpuP5bkYc79QUdq3pap-
kLJOTwS5Wx3Q",
   "expires_in": 36000,
   "token_type": "Bearer",
   "refresh_token": "0ba4cafba0f749645aa4asf449dc48ed503df7a3451241161f59f2f5c"
}
```


В ответ на запрос придёт JWT .

Дополнительно

Енд-поинт для получения информации о пользователе, с использованием JWT .

```
GET https://auth.artsofte.ru/connect/userinfo
```

Http-заголов о к:

- Authorization:Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6IjdhZWVkOWE0YTNiNzJmZTM3Y2Q3MDdlMjM2MmExZDFkIiwidHlwIjoiSldUIn0

— в заголовке использовать полученный access _ token .

Используем JWT , в котором уже содержится ключевая информация о клиенте, про которого нужна информация с сервера интернет-Заказчика. Сама ключевая информация уже есть в JWT , если его распарсить.
В этой ключевой информации есть поле `sub` — это уникальный идентификатор пользователя в базе IdentityServer. Если у Партнёра есть своя база пользователей, Партнёр должен сохранять в этой базе для своих пользователей значение поля `sub` - таким образом Вендор сможет сопоставить пользователя IdentityServer из JWT с пользователем в своей базе.

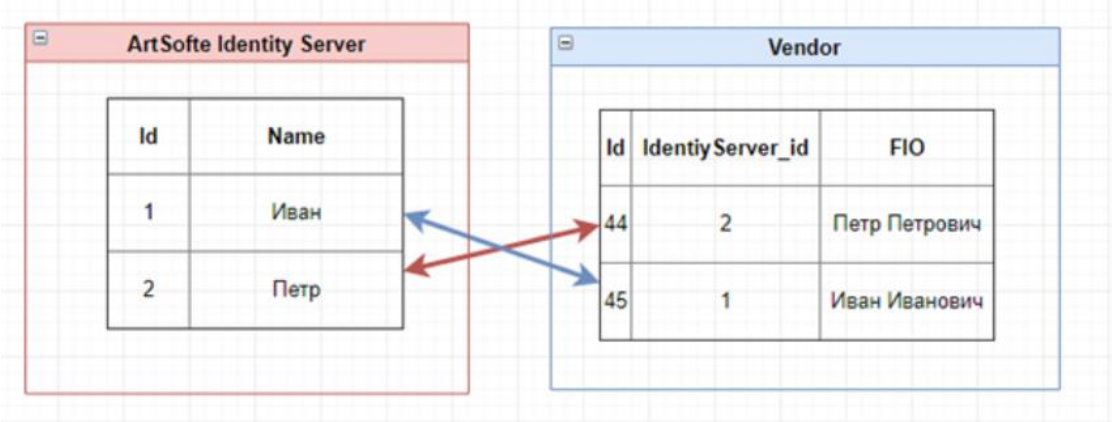
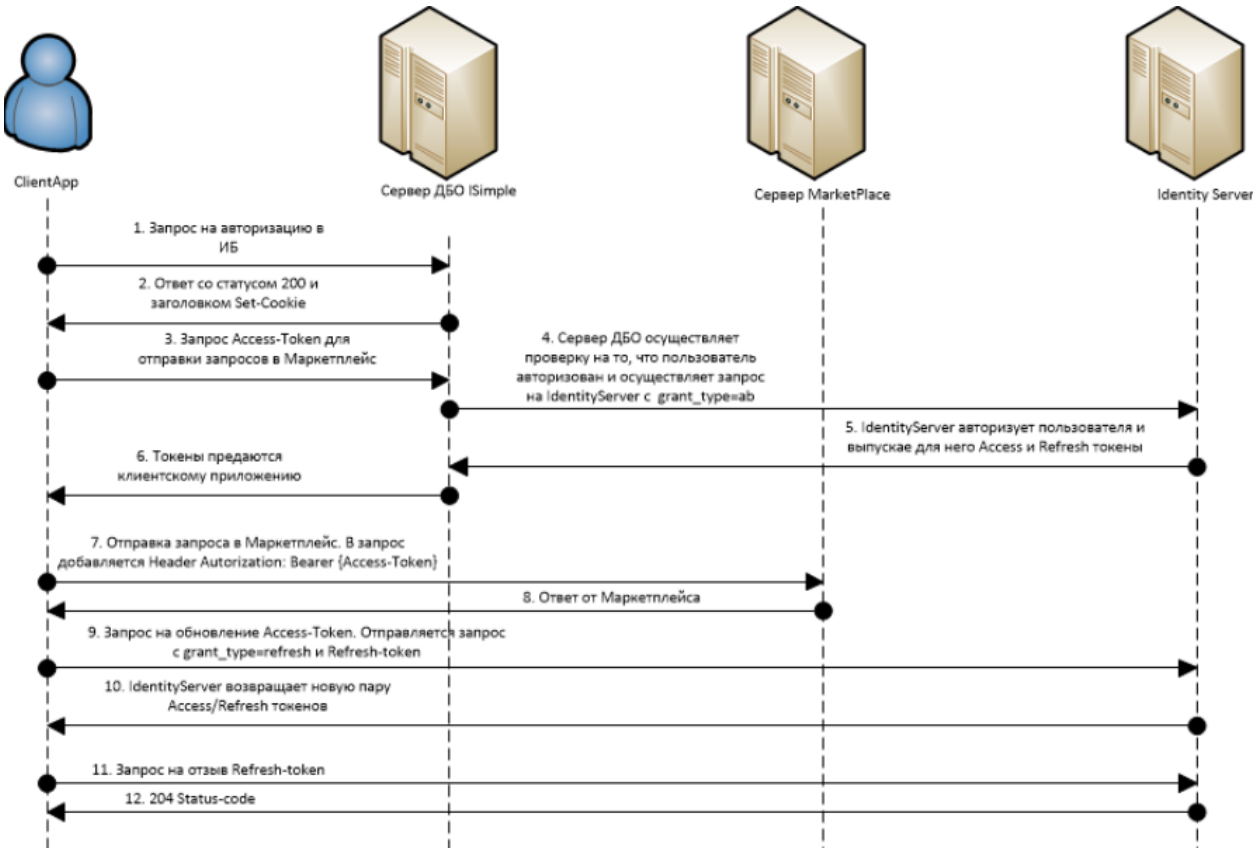
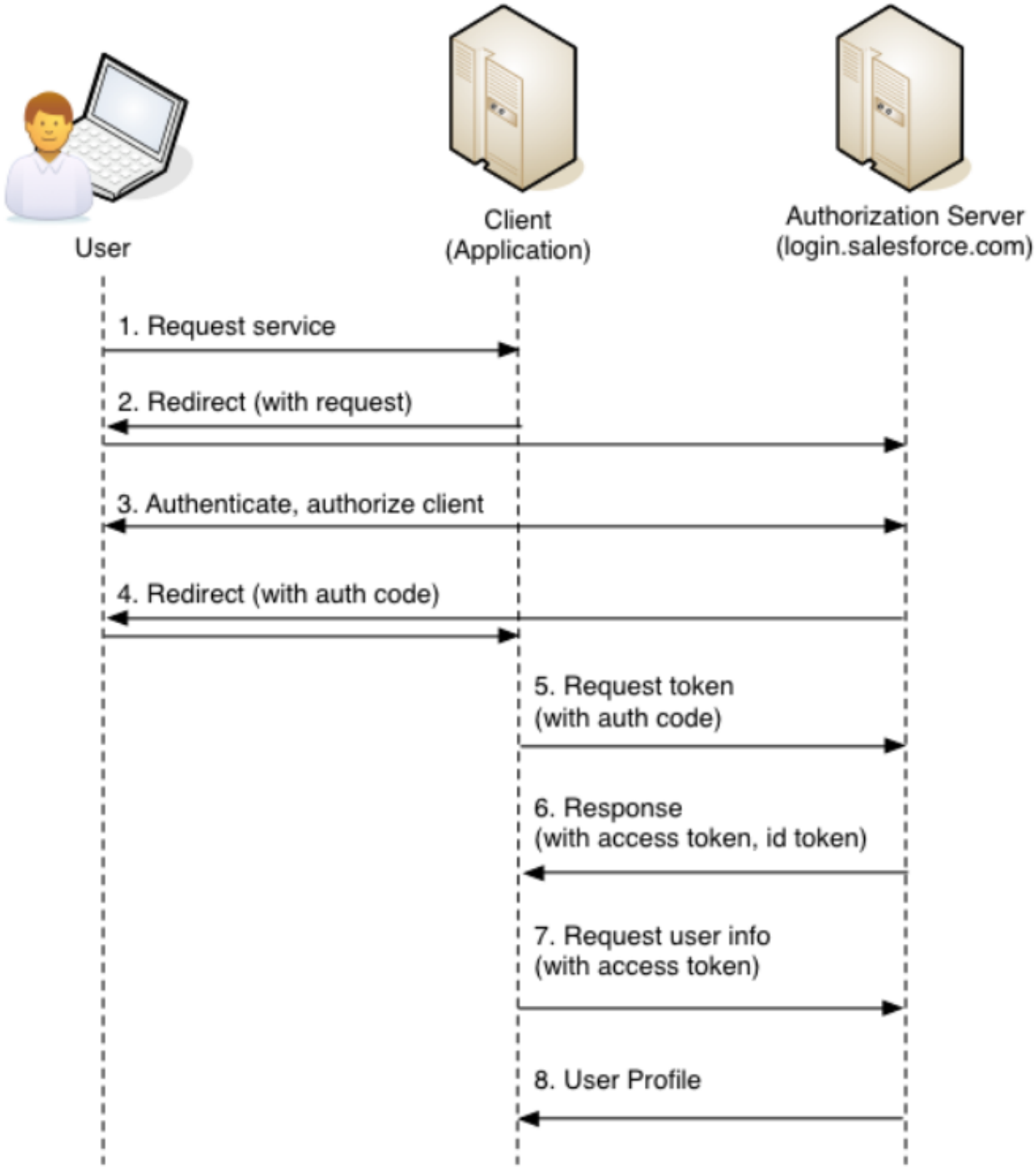


Рис. Сопоставление пол ьзователей
Авторизация через Identityserver.





Стек технологий: .net core, PostgreSQL

Функциональные требования:

1. Настроить Имя хоста апи ДБО, в которое будет обращаться сервер авторизации нет
2. Настроить Запрашиваемые права у сервера ДБО, для сценария рефреша ключа read строка
3. Настроить client_id для сценария рефреша ключа
4. Настроить client_secret, для сценария рефреша ключа нет строка
5. Настроить Время жизни сессии
6. Настроить Сообщение, выводимое, когда пользователь не найден
7. Настроить Сообщение, выводимое, когда был введён неверный пароль
8. Настроить Шаблон, которому должен соответствовать новый логин

9. Включать/отключать проверку на время жизни пароля
10. Настроить Время жизни временного пароля в минутах
11. Настроить Время жизни постоянного пароля в днях
12. Настроить Сообщение, если пароль просрочен "Пароль пользователя просрочен"
13. Настроить наличие в пароле пользователя цифр
14. Настроить наличие в пароле пользователя цифр
15. Настроить наличие в пароле пользователя букв в нижнем регистре
16. Настроить наличие в пароле пользователя букв в нижнем регистре
17. Настроить наличие в пароле пользователя букв в верхнем регистре
18. Настроить минимальную длину пароля пользователя
19. Настроить количество не удачных попыток для авторизации
20. Настроить время в минутах, на которое пользователь блокируется

Настроить ссылку, которую возвращает сервер в ответ на запрос /api/user/generateonetimelink подробнее запрос описан в SWAGGER , по ней пользователь может перейти в авторизованную зону и сразу быть авторизованным