Введение

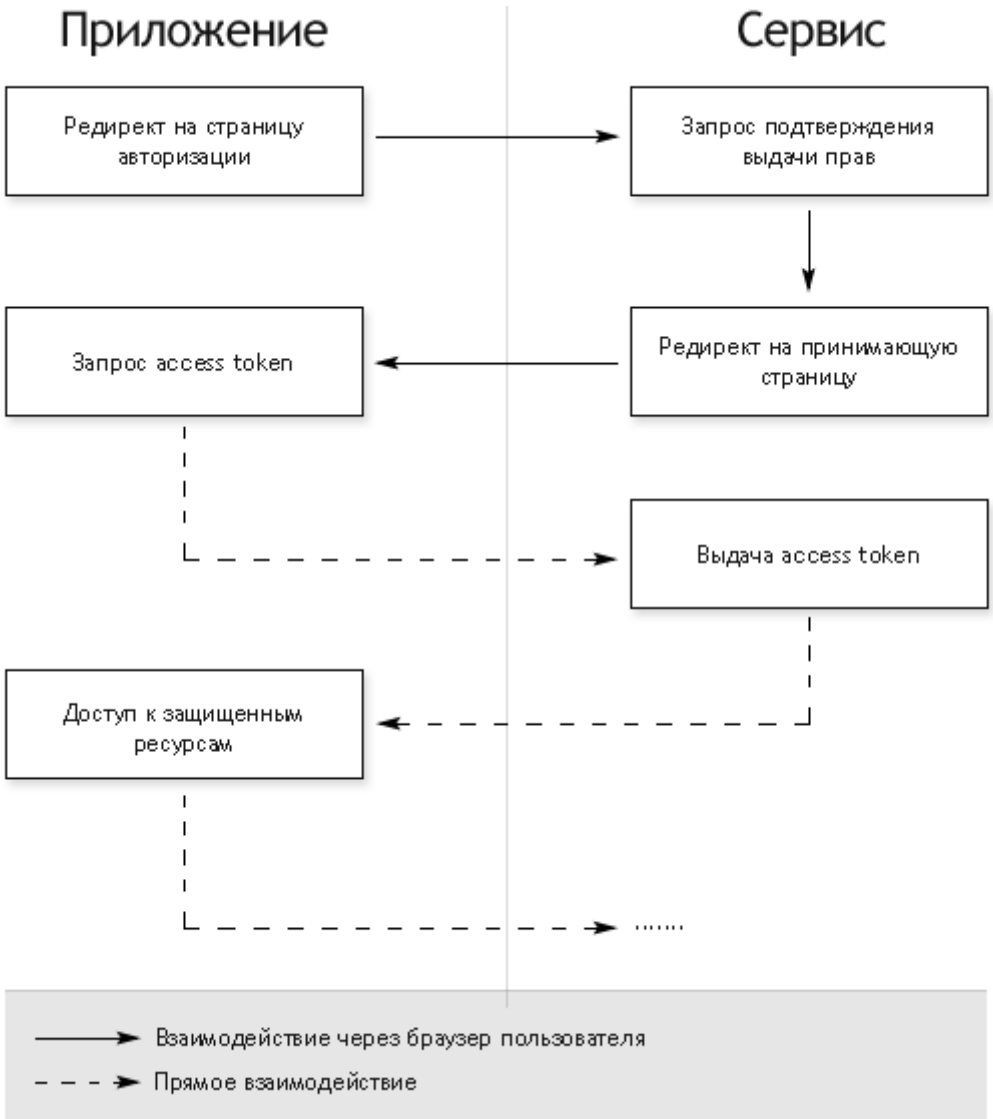
Данный сервис позволяет провести авторизацию пользователей ТПУ в приложении, сохранив при этом учетные данные пользователей.

Адрес сервиса в сети интернет: https://oauth.tpu.ru

Описание сервиса

Данный сервис авторизации, позволяющий выдать одному сервису (приложению) права на доступ к ресурсам пользователя на другом сервисе. Протокол избавляет от необходимости доверять приложению логин и пароль, а также позволяет выдавать ограниченный набор прав, а не все сразу.

Авторизация для приложений, имеющих серверную часть

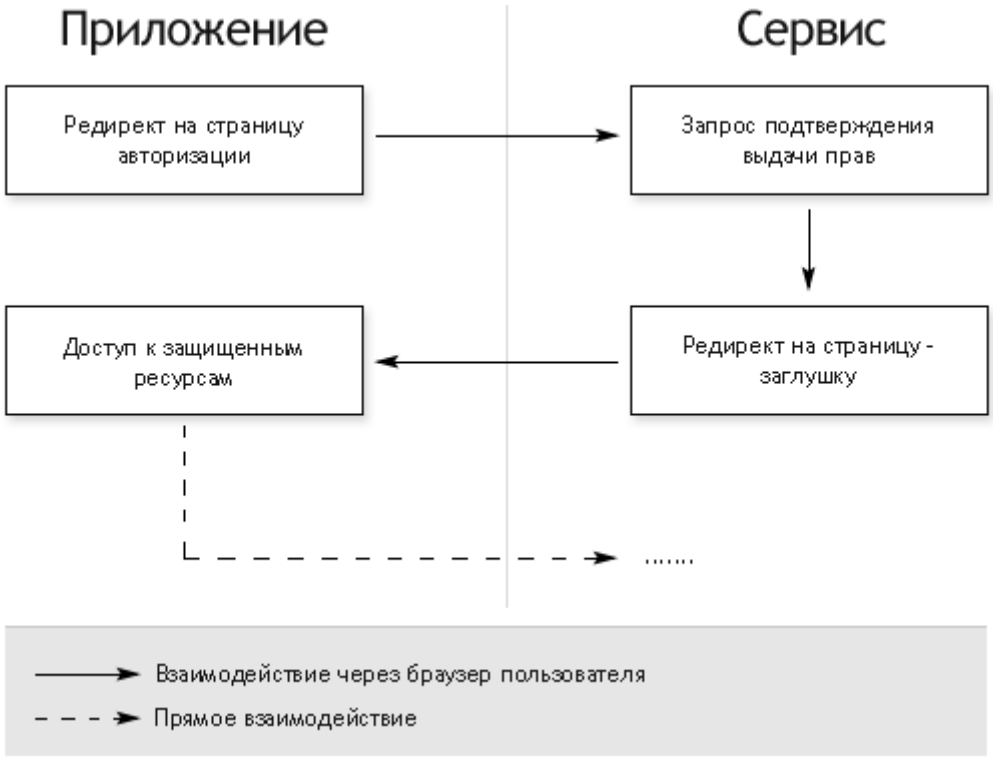


1. Редирект на страницу авторизации

2. На странице авторизации у пользователя запрашивается подтверждение выдачи прав
3. В случае согласия пользователя, браузер редиректится на URL, указанный при открытии страницы авторизации, с добавлением в GET-параметры специального ключа — *authorization code*
4. Сервер приложения выполняет POST-запрос с полученным *authorization code* в качестве параметра. В результате этого запроса возвращается *access token*

Это самый сложный вариант авторизации, но только он позволяет сервису однозначно установить приложение, обращающееся за авторизацией (это происходит при коммуникации между серверами на последнем шаге). Во всех остальных вариантах авторизация происходит полностью на клиенте и по понятным причинам возможна маскировка одного приложения под другое. Это стоит учитывать при внедрении OAuth-аутентификации в API сервисов.

Авторизация полностью клиентских приложений



1. Открытие встроенного браузера со страницей авторизации
2. У пользователя запрашивается подтверждение выдачи прав
3. В случае согласия пользователя, браузер редиректится на страницу-заглушку во фрагменте (после #) URL которой добавляется *access token*
4. Приложение перехватывает редирект и получает *access token* из адреса страницы

Этот вариант требует поднятия в приложении окна браузера, но не требует серверной части и дополнительного вызова сервер-сервер для обмена authorization code на access token.

Восстановление предыдущей авторизации

Access token имеет ограниченный срок годности (30 минут), так как он передается по открытым каналам. Чтобы не заставлять пользователя проходить авторизацию после истечения срока действия ***access token***'а, в дополнение к ***access token***'у возвращается еще ***refresh token***. По нему можно получить ***access token*** с помощью HTTP-запроса.

Описание процесса **восстановление авторизации**

OpenID Connect

OpenID Connect (*OIDC*) — это безопасный механизм, позволяющий приложению связаться со службой идентификации, чтобы получить необходимые данные о пользователе и вернуть их обратно в приложение, обеспечив полную защиту данных.

Термины и понятия

Используемые сокращения при работе с сервером авторизации

Параметр	Описание
client_id	Идентификатор приложения
client_secret	Защищенный ключ приложения
redirect_uri	Адрес, на который будет передан code (домен указанного адреса должен соответствовать основному домену в настройках приложения и перечисленным значениям в списке доверенных redirect uri — адреса сравниваются до корневого домена).
response_type	Тип ответа, по умолчанию значение ***code***.
state	Произвольная строка, которая будет возвращена вместе с результатом авторизации.
grant_type	Способ авторизации