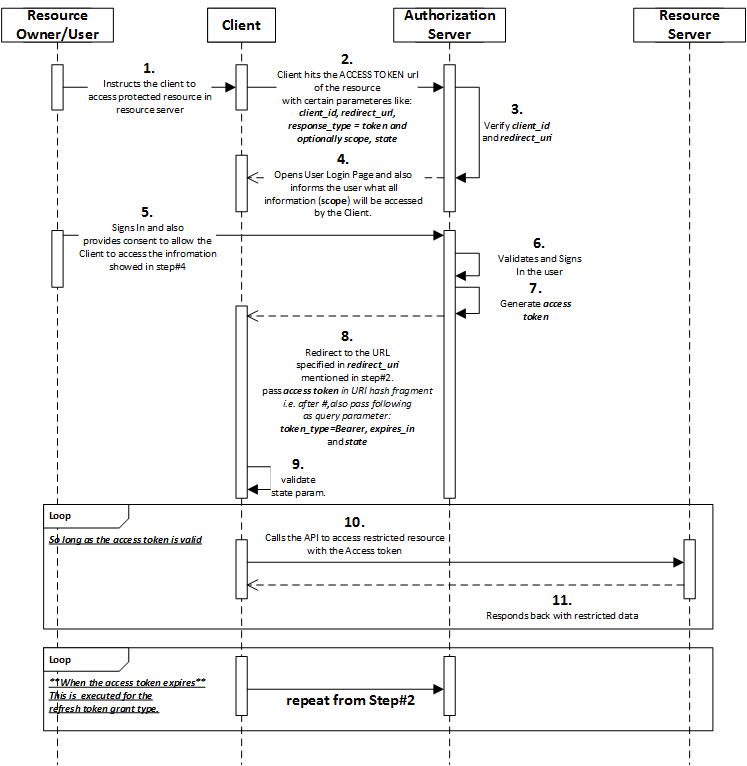
Grand Type: Implicit

oAuth2-implicit-grant-flow-diagram



1. Resource Owner/ Користувач дає вказівку Клієнту отримати доступ до його захищеного ресурсу на сервері ресурсів.
2. Отримавши запит на доступ Клієнт надсилає Access Token url до Authorization server з наступними параметрами :client\_id, redirect\_uri,state ,scope,response\_type
3. Authorization server Перевіряє client\_id і redirect\_url
4. Після цього відкривається веб-сторінка/діалогове вікно входу, а також вказується, до якої інформації (області) матиме доступ Клієнт.
5. Користувач або власник ресурсу входить і надає згоду на те, що клієнт може отримати доступ до даних вказаних в кроці 4.
6. Підтвердження Входу: Якщо надані облікові дані правильні, користувач увійшов у систему, а згоди записалися. Якщо користувач не надає згоду, весь процес зупиняється.
7. Якщо вхід успішний генерується access token
8. Перенаправлення до Url визначеному в redirect\_uri вказаному в кроці 2 . Передача access token в URI хеш фрагменті.
9. Перевіряється параметр state Клієнтом
10. Клієнт використовується access token, щоб перейти до URL-адреси захищеного ресурсу та отримати доступ до захищених даних.
11. Сервер відповів з захищеними даними
12. Коли термін дії access token закінчиться потрібно почати з кроку 2.