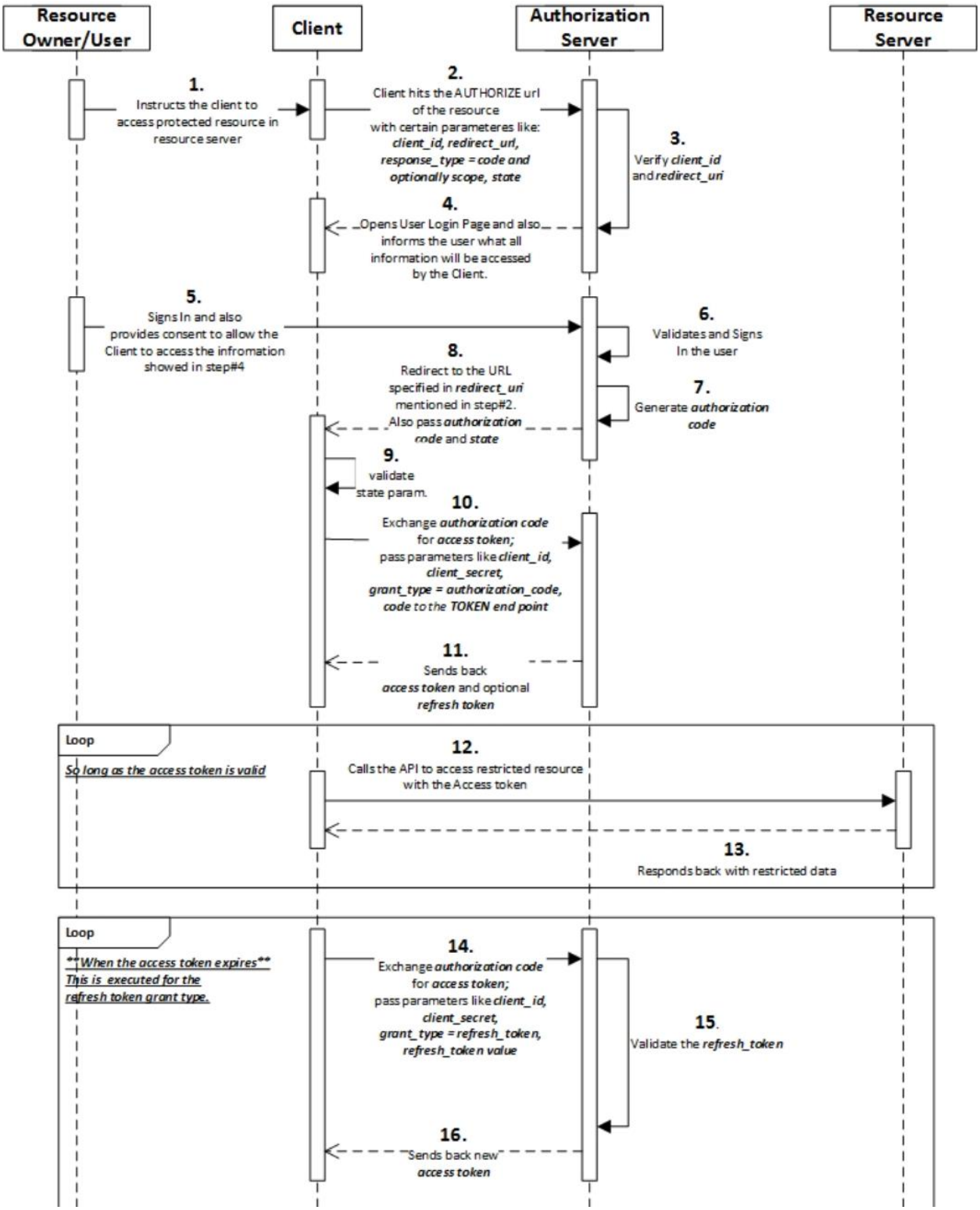
OAuth-authorization with refresh token OAuth grant type



Крок 1

- На діаграмі згори виконання починається з моменту , коли *Resource Owner/User* просить клієнта *Client* отримати доступ до захищених даних в *Resource Server*.

Крок 2

- Отримавши виклик користувача щодо доступу до захищених даних, *Client* клієнт відправляє запит до ендпоінту Authorization з наступними параметрами:

  1) *client_id* – унікальне число ідентифікації клієнта;
  2) *redirect_uri* – це URL, де Authorization сервер надішле response назад з кодом авторизації;
  3) *state* – в цьому параметрі *Client* надсилає request до Authorization ендпоінту з певним значенням. Коли Authorization сервер надсилає response назад до *redirect_uri,* він надсилає назад значення *state*. Потім *Client* перевіряє це значення, щоб переконатися, що це справді зворотний виклик для того самого запиту, який він надіслав Authorization сервер;
  4) *scope* – наприклад, профіль, електронна пошта, місцезнаходження тощо;
  5) *response_type* – Це означає, що запит спрямований на отримання Authorization Code.

Крок 3

- Ендпоінт AUTH перевіряє *client_id*.

Крок 4

- Потім відкривається sign-in сторінка/діалогове вікно, де відображається інформація (*scope*), яка буде надана *Client*.

Крок 5

- *User* або *Resource Owner* надає облікові дані і згоду на те, щоб *Client* міг отримати доступ до *scope*.

Крок 6

- Якщо надані облікові дані правильні, користувач погодився й увійшов у систему.
- Якщо користувач не надає згоди, весь процес зупиняється.

Крок 7

- Після успішного входу та згоди користувача AUTH сервер створює authorization code.

Крок 8

- Перенаправлення користувача на URL, що вказаний в *redirect_uri*. AUTH сервер передає *state* разом з authorization code.

Крок 9

- *Client* порівнює значення стану, щоб переконатися, що це те саме значення, яке було надіслано в кроці 2. Це запобігає атакам CSRF.

Крок 10

- Потім *Client* змінює authorization code на *access token*. Щоб це виконати *Client* викликає TOKEN ендпоінт з інформацією:
    1) *client_id* – унікальна строка, що ідентифікує клієнта;
    2) *client_secret* – секретна строка від клієнта;

3) *grant_type*;
4) *code* – authorization code.

Крок 11

- AUTH сервер відсилає назад *access token* і *refresh token*;

Крок 12 - 13

- *Client* потім використовує *access token*, щоб перейти до URL захищеного ресурсу і отримати захищені дані;

Крок 14 -15

- У випадку, якщо *access token* закінчується, *Client* викликає TOKEN ендпоінт знов, однак зі значенням *grant_type* на кшталт *refresh token.*
- AUTH сервер перевіряє *refresh token* і повертається з оновленим *access token* для подальшого використання.