AUTHLETE

OAuth 2.0

Refresh token

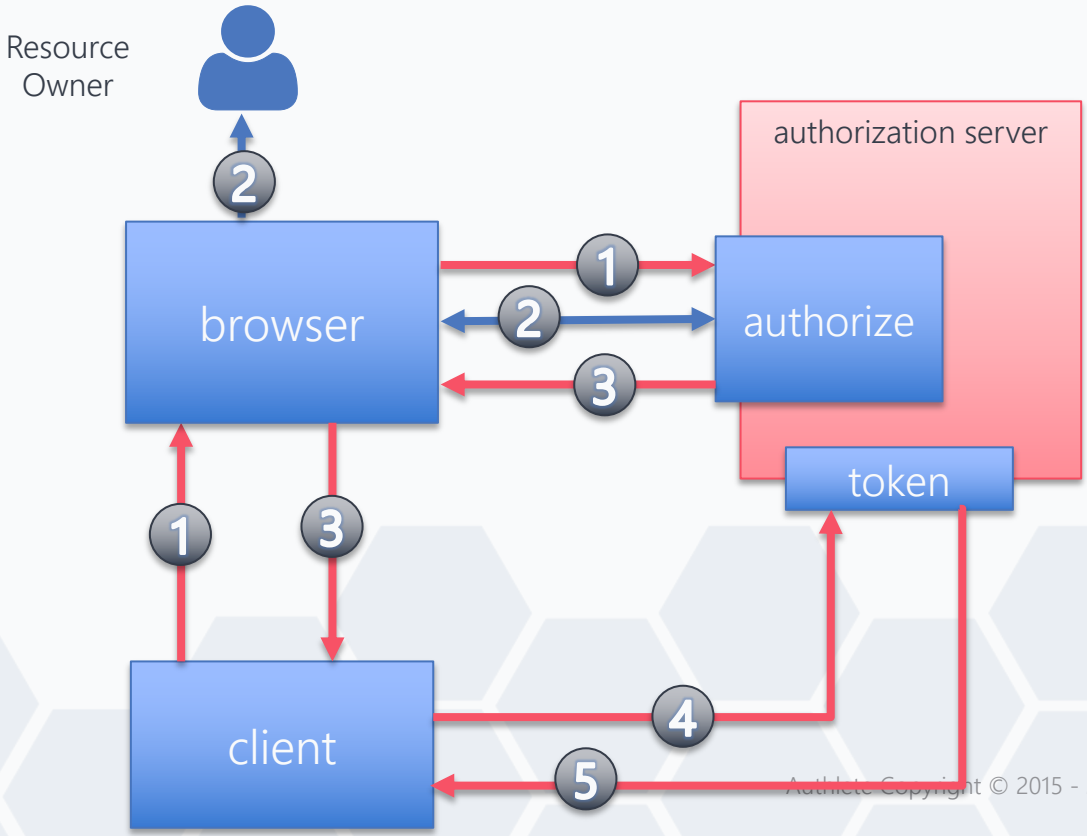
Recap - Authorization Server Endpoints

- Authorization
  - Allow the resource owner interact with the authorization server in order to grant permissions to client
- Token
  - Used by the client to retrieve access tokens using grants from authorization or refresh tokens

Recap

Authorization code is one of the grant types that can be used by clients and AS

Authorization code flow



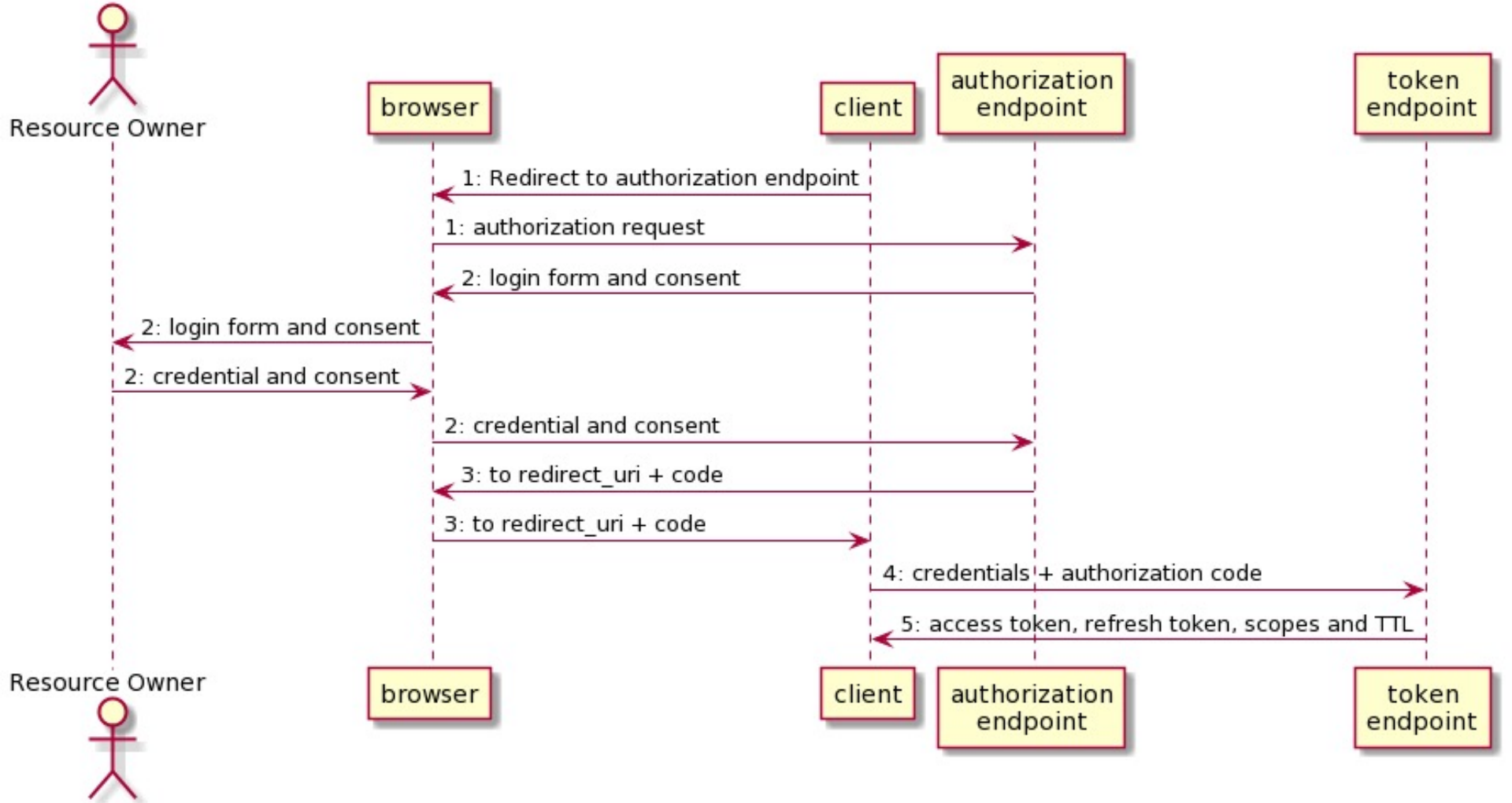
1 – Redirect to authorize endpoint with response_type=code

2 – The user login and grant the permission

3 – redirect to client with the authorization code

4 – client send the authorization code to token with credentials

5 – AS returns the access token, refresh token, granted scopes and time to live of the token



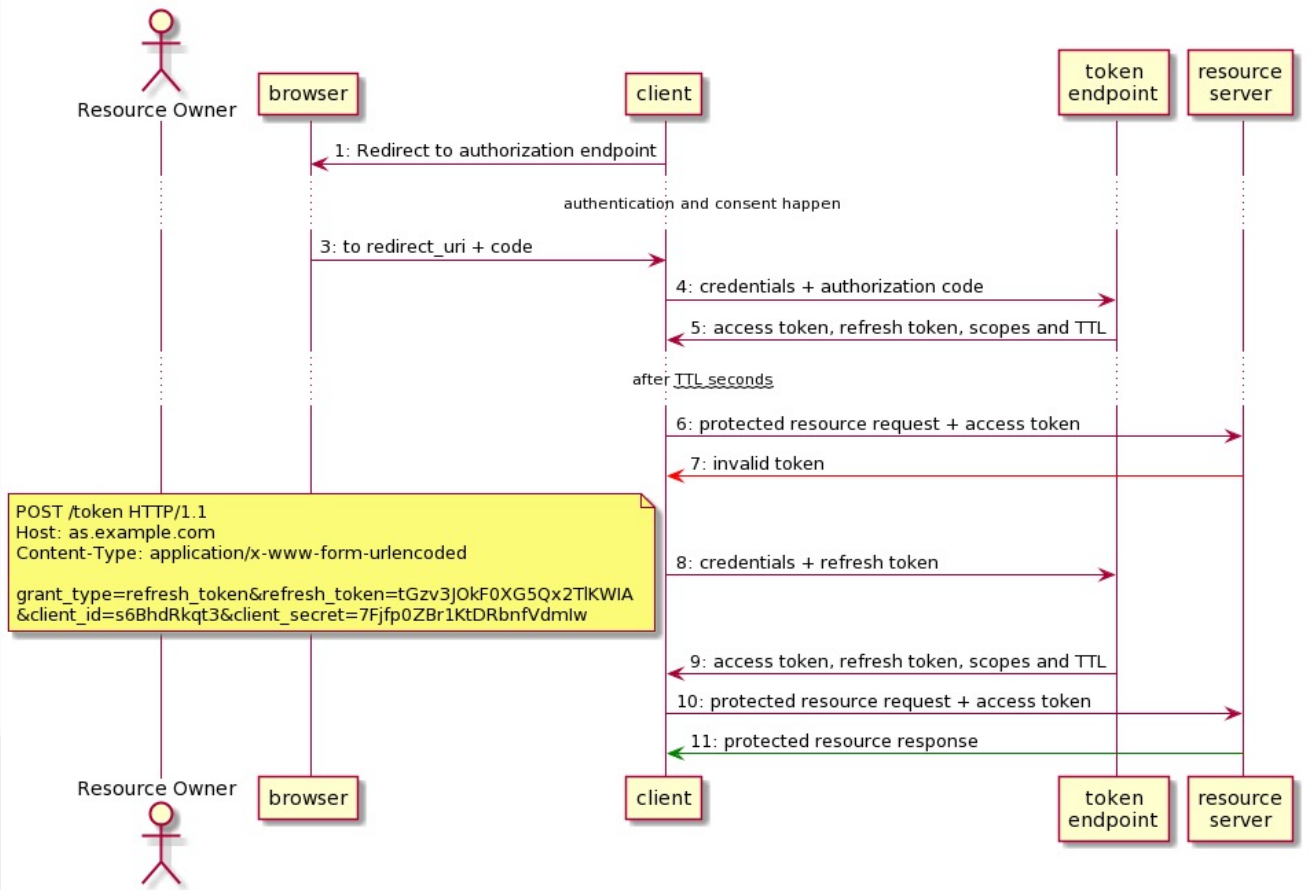
Refresh token

It materializes the authorization granted by the resource owner.

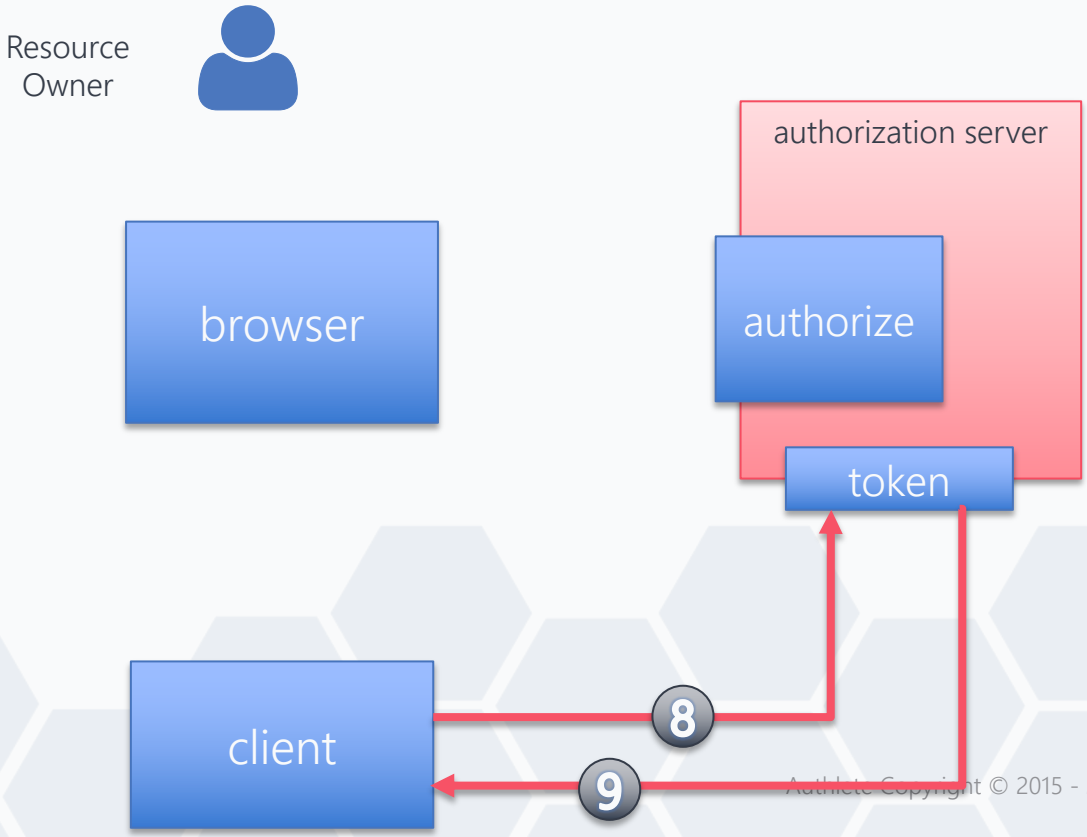
Refresh token as authorization grant

a grant that can be used by client on token endpoint to issue another access token

Refresh token sequence



Refresh token sequence



1 – Redirect to authorize endpoint with response_type=code

…

5 – AS returns the access token, refresh token, granted scopes and time to live of the token

…

8 – client send the refresh token with credentials

9- AS issues a new access token, and optionally a new refresh token

As the time goes by...

it is expected that the permissions gets narrowed or can be not extendable

Refresh token as authorization grant

Access token issued using a refresh token might not have the same set of scopes

Mapping the concepts

- Access token -> permission to access the API

- Refresh token -> permission to extend the session

Refresh token

It makes sense only for the interaction of client and authorization server

Deployment

The usage is dependent on the clients, so the volume of calls and workload created needs to be monitored per client based

Deployment Tradeoff

Refresh token rotation prevents access to protected resources for longer periods to be granted but AS needs to offer a mechanism to prevent too many refresh tokens to be living

AUTHLETE

www.authlete.com

AUTHLETE

OAuth 2.0

Refresh token