An ID token is a JSON Web Token (JWT) that contains information about the authenticated user. It is sent to the client application (typically a Single-Page Application or SPA) after a user successfully authenticates. The ID token contains claims about the identity of the authenticated user, such as their name, email address, and other identifying information. The ID token is typically used at the front end of the application to display the user’s name and other information or to make authorization decisions.

An access token, on the other hand, is a JWT that contains information about the user’s authorization to access a protected resource, such as a backend API. The access token is sent to the backend API in the Authorization header of an HTTP request, along with the Bearer keyword. The backend API uses the access token to determine if the user is authorized to access the requested resource. Access tokens typically have a short lifetime and need to be renewed or refreshed.

ID tokens and access tokens are different in terms of the information they contain and the purpose they serve. The ID token is used to identify the user and the access token is used to authorize the user. They are issued by the authorization server and can be obtained by the client application after successful authentication.

npm install @azure/msal-browser @azure/msal-angular

ng g environments