**ID token vs Access Token**

ID tokens and access tokens are both used in OAuth 2.0 and OpenID Connect to authenticate users and authorize them to access protected resources. However, they have different purposes and are used in different ways.

* ID tokens are used to verify the identity of a user. They contain information about the user, such as their name, email address, and unique identifier. ID tokens are typically used by the client application to display the user's information to the user, or to make claims about the user to other services.
* Access tokens are used to authorize the user to access protected resources. They contain information about the resources that the user is authorized to access, and the scope of their access. Access tokens are typically used by the client application to make requests to protected resources.

1-ID Token:

* **Purpose**: The ID token is primarily used for authentication and user identification. It contains information about the authenticated user, such as their identity and basic profile information.
* **Content**: The ID token typically contains claims like user ID, name, email, and potentially other user-related information. It provides a way for the application to verify the user's identity.
* **Usage**: The ID token is often sent to the client application after successful authentication via an OpenID Connect flow. It helps the client application know who the user is without having to make additional requests to the identity provider.
* **Scope**: The ID token is requested with the openid scope.

**2-Access Token:**

* **Purpose**: The access token is used to authorize access to specific resources on behalf of a user. It represents the user's permissions to access protected resources.
* **Content**: The access token carries information about the user's granted permissions, scopes, and potentially other metadata that the resource server uses to determine whether the user has the necessary privileges to access a particular resource.
* **Usage**: The access token is sent by the client application to the resource server when making API requests. The resource server validates the token and allows or denies access based on the permissions encoded in the token.
* **Scope**: The access token is requested with scopes that define the level of access the application needs.

In summary, the ID token is primarily used for authentication and user identification, allowing the client application to know who the user is without making additional requests to the identity provider. On the other hand, the access token is used for authorization, granting the client application permission to access specific resources on behalf of the user.

It's important to note that while these tokens have distinct purposes, in some authentication flows, such as OpenID Connect, both ID tokens and access tokens can be issued together to provide a comprehensive solution for both authentication and authorization.

**Reference:**

https://auth0.com/blog/id-token-access-token-what-is-the-difference/