Module 4 Vocabulary

**Identity Token:** <https://www.techopedia.com/definition/24834/identity-token>

Identity Tokens are portable pieces of hardware a user carries to use for access to a network. These tokens aid in proving a user’s identity as well as authenticating that user for use of a service. Identity tokens are also sometimes referred to as Security Tokens and Authentication Tokens.

**Access Token:** <https://auth0.com/docs/tokens/access-tokens>

Access Tokens are part of token-based authentication to allow access to an API for an application. To do this, the application receives an access token after a user gains authentication and authorization, then the access token is passed as a credential when it calls an API. After that the API is informed by the passed token what the bearer of said token is authorized to access, as well as what actions specified by scopes granted during authorization.

**Refresh Token:** <https://auth0.com/learn/refresh-tokens/>

Refresh Tokens are used when an application is using access tokens that have a limited lifetime. These refresh tokens can be used to keep access granted to a user even when their access token expires. This is done by allowing the application to gather a new access token *without* prompting the user. To do this, when a new access token is needed, the application makes a request to the token endpoint using a refresh token to gain a new ID token.

**RBAC:** <https://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC>

RBAC, which stands for Role-based Action Control, is a method for restricting access to a network based on roles of individual users. These roles can be based on many things. For employees, you can see roles used based on authorization level, their responsibilities, or even job competency. However, these roles can also be used for things like customers, and can restrict access generally off things like if the customer pays for the service or not, and how much they pay for the service.

**ABAC:** <https://www.axiomatics.com/attribute-based-access-control/>

ABAC, which stands for Action-based Action Control, uses attribute building blocks in structured language to define access control rules as well as describe access requests. Attributes are sets of labels/properties that can describe all entities being considered for authorization purposes. These attributes all have key-value pairs, for example… Role=Manager. Unlike RBAC roles, attributes can be used for multiple things. This allows for cleaner setup, since you don’t need to make a new role for every new access limitation.