In Azure, a security principal is an identity used to authenticate and authorize access to resources. It represents a user, application, or service that can access Azure resources.

There are four main types of security principals:

1. User:

A real human being with a username and password. They log in via Azure Active Directory (Azure AD).

2. Group:

A collection of users. You can assign permissions to a group instead of individual users for easier management.

3. Service Principal:

An identity used by applications or services to access Azure resources. It's like a “user identity” for non-humans.

4. Managed Identity:

A special type of service principal managed by Azure. It simplifies the authentication of Azure services without the need to manage credentials (like passwords or secrets).

Example use case:

If you have an app running in Azure App Service that needs to read from Azure Key Vault, you can assign it a managed identity. Azure uses that identity to authorize access without storing credentials in your code.