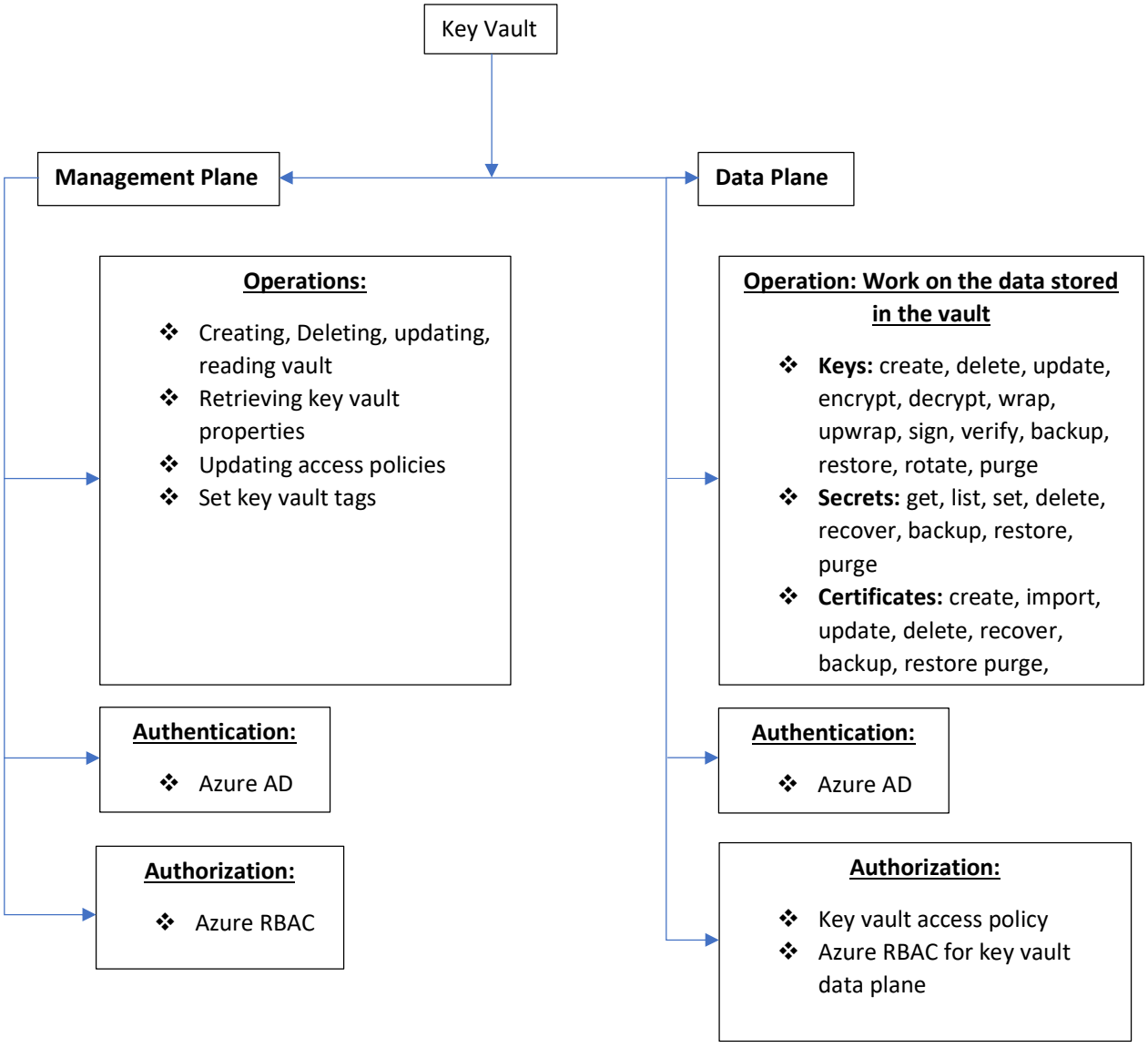
Azure Key Vault

Key Vault: Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.

Information about the Management and Data Plane of the key vault is shared below:



Authentication: Authentication establishes the identity of the caller.

Authorization: Authorization determines which operations the caller can execute.

In all types of access, the application authenticates with Azure AD. The application uses any supported authentication method based on the application type. The application acquires a token for a resource in the plane to grant access. The resource is an endpoint in the management or data plane, based on the Azure environment. The application uses the token and sends a REST API request to Key Vault.

When using the Access Policy permission model, if a user has Contributor permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy.

Flow chart – Azure Key Vault – Reference: Microsoft Docs