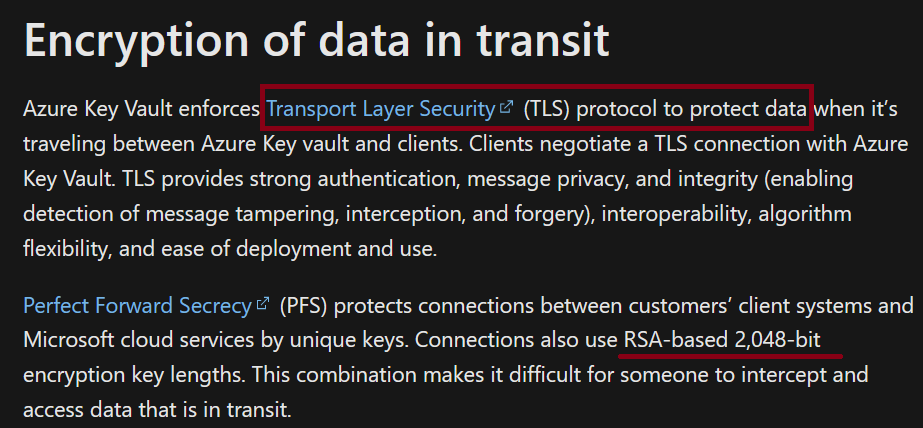
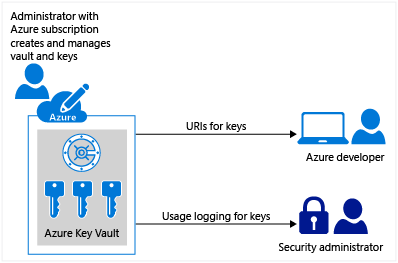
Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.

Encryption: Azure Key Vault uses AES 256-bit encryption to protect your secrets and keys, ensuring they remain private and safe.



Concept:

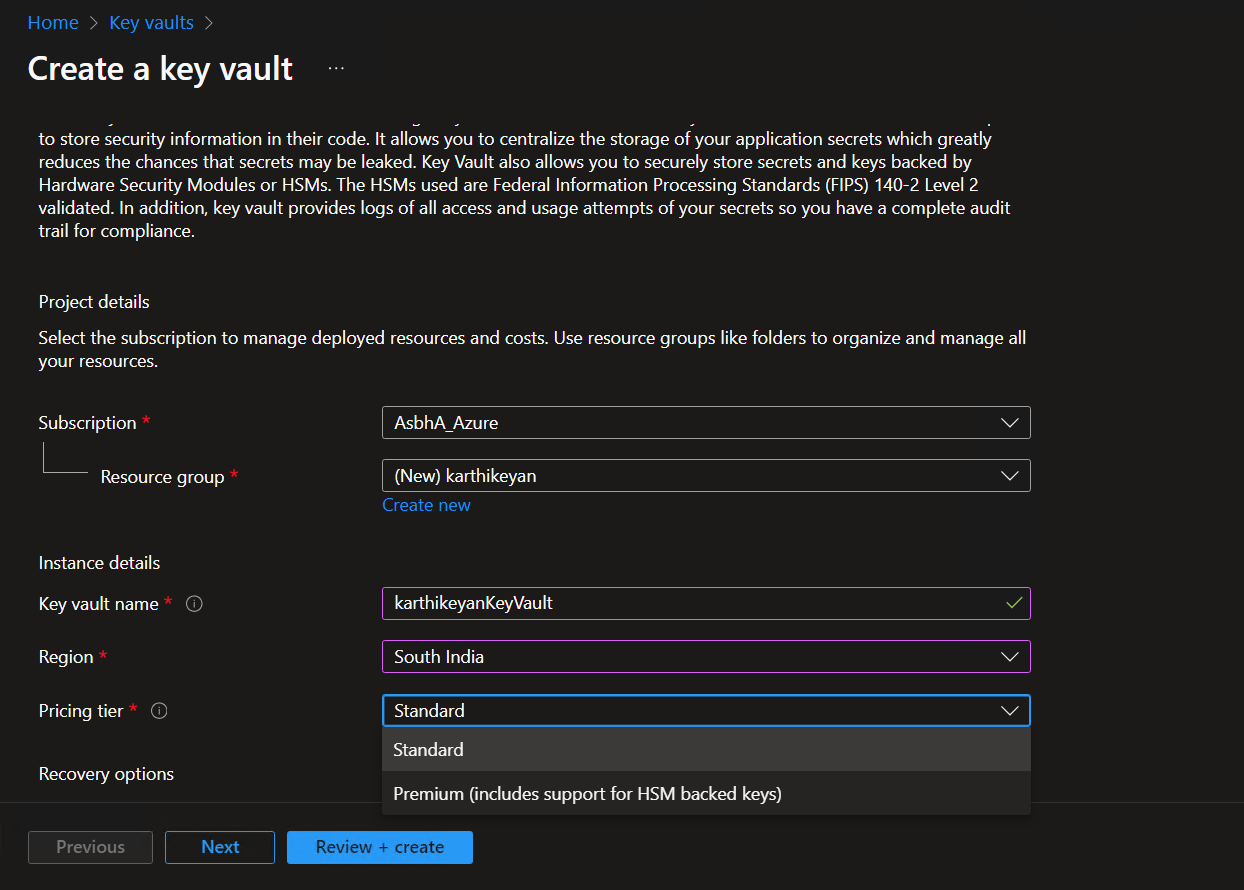


Ref - <https://learn.microsoft.com/en-us/azure/key-vault/general/basic-concepts>

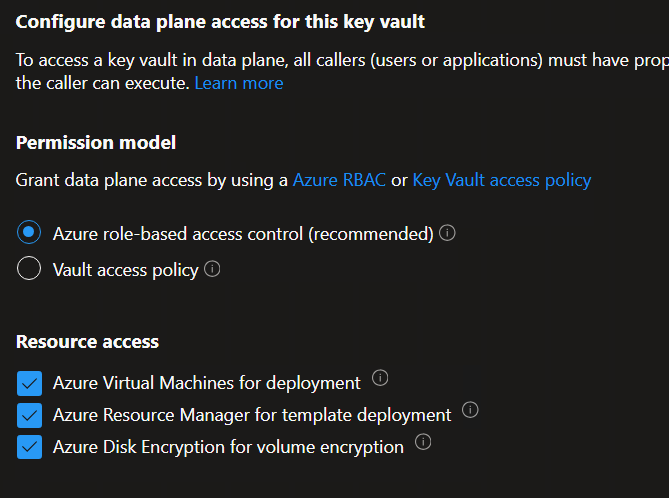
LAB:

Creation of key vault

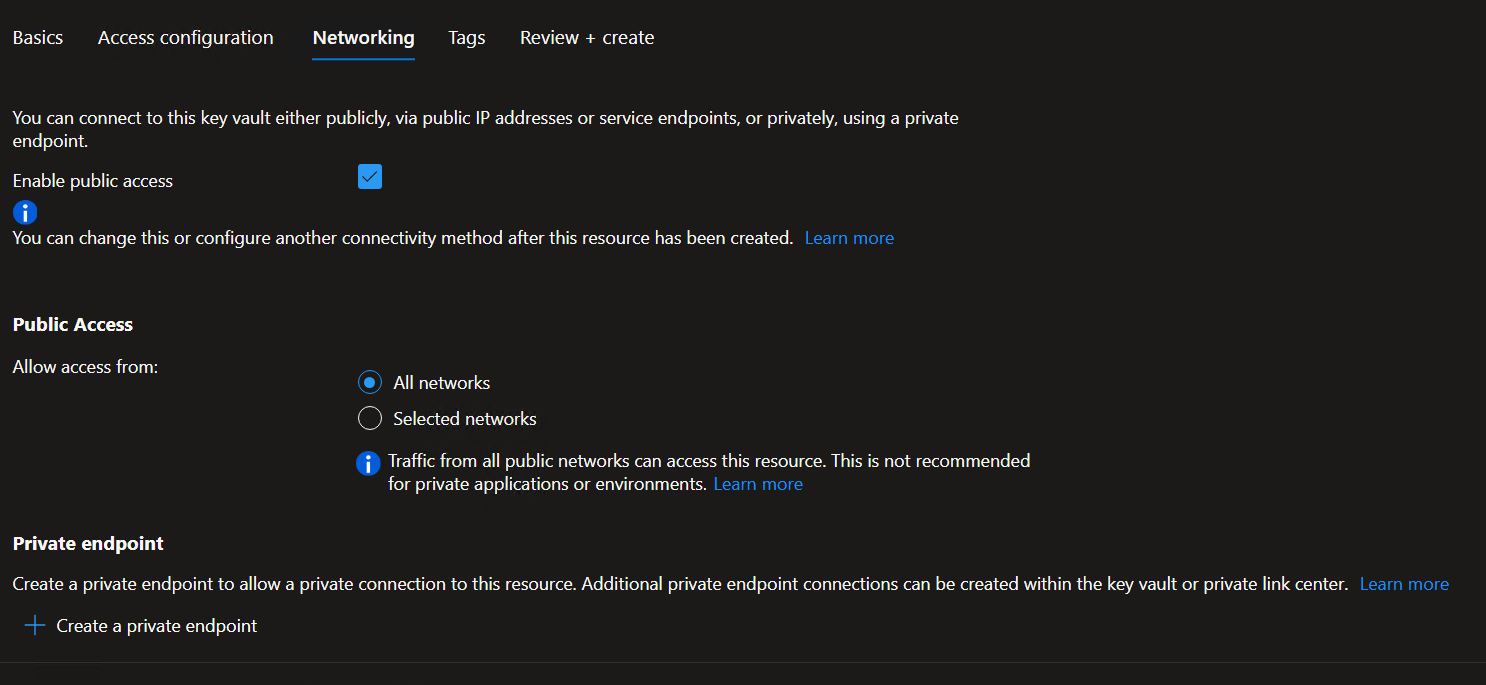
SKU – Standard, Premier



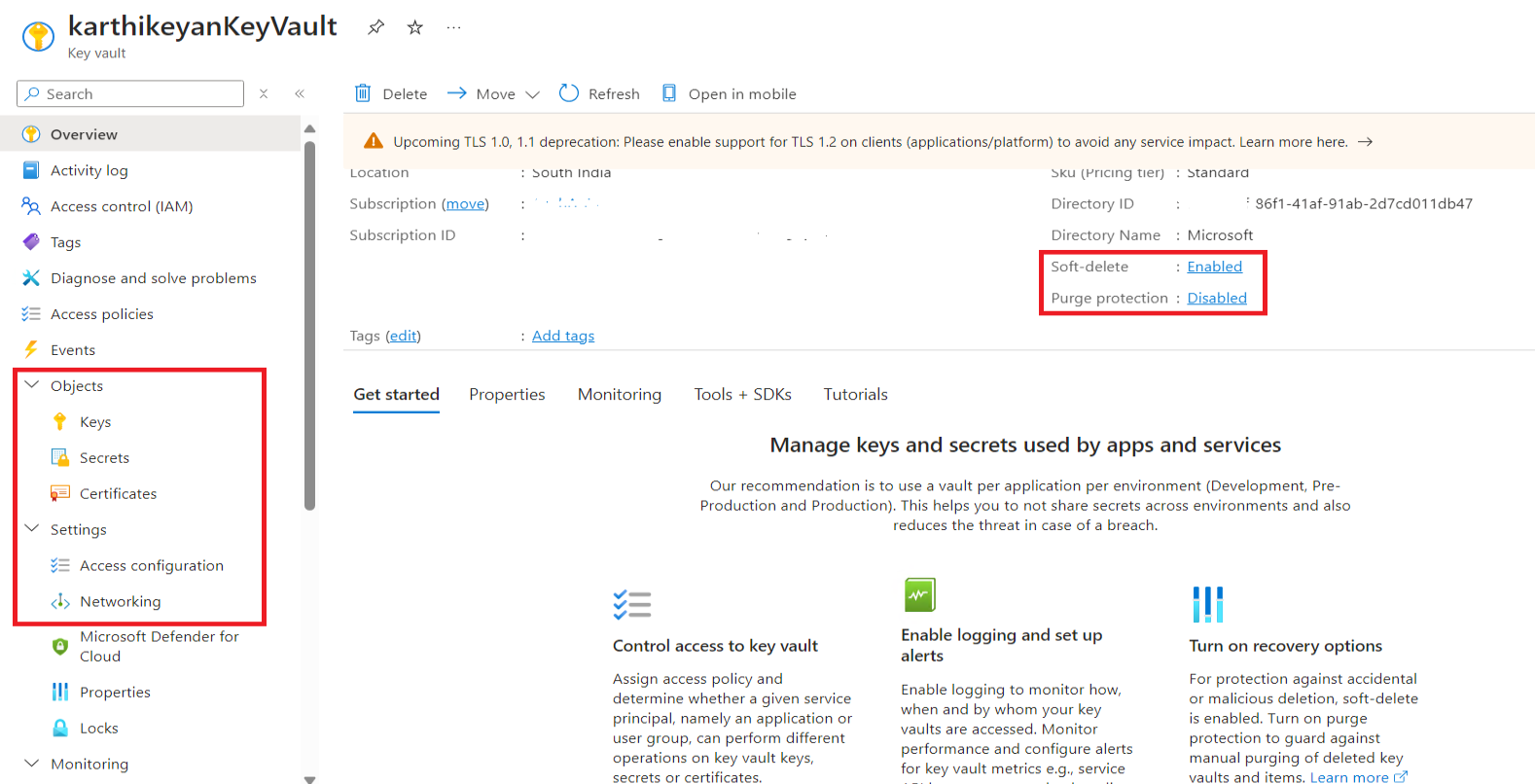
Here there is different types of Permission mode



In networking tab we can customize the virtual network as per our need and also use private endpoint



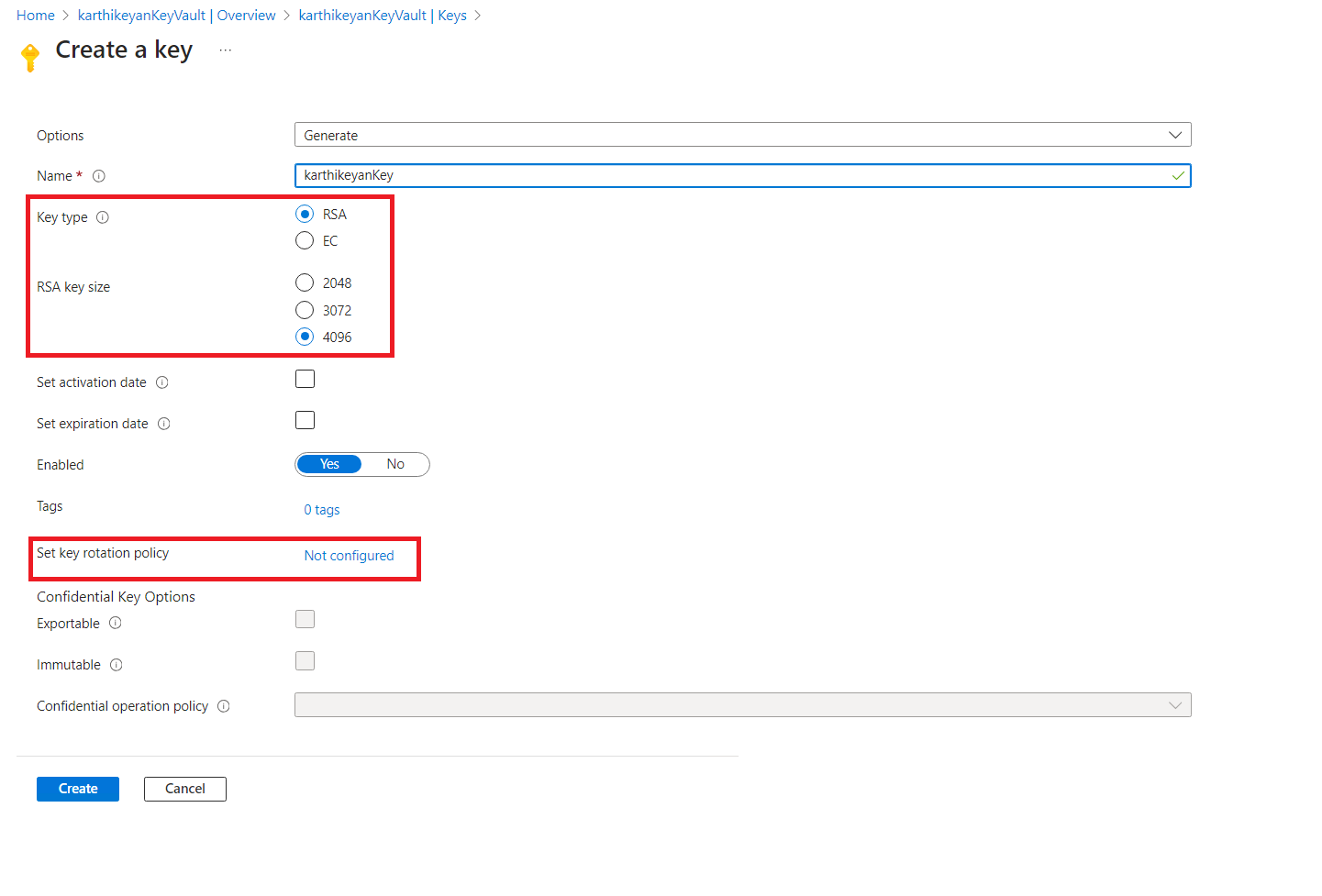
Azure Keyvault



Now let’s generate a Key

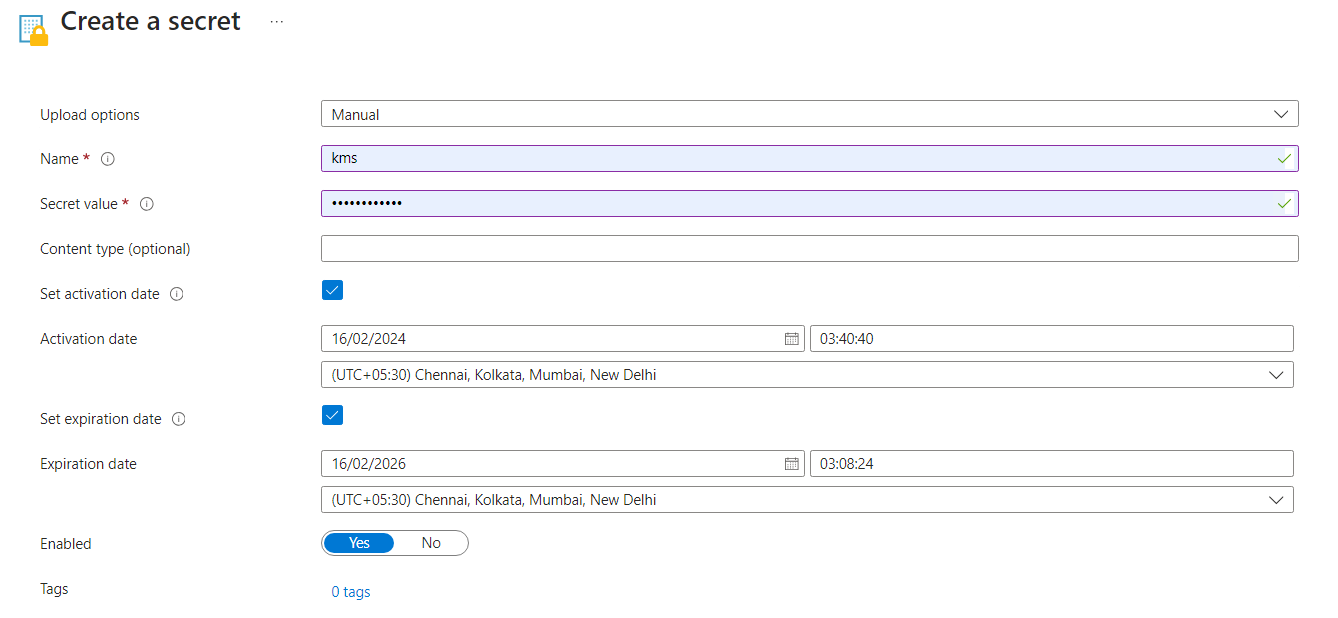
Here there is 2 key types (RSA, EC)

RSA key size (max) 4096 [interview que]

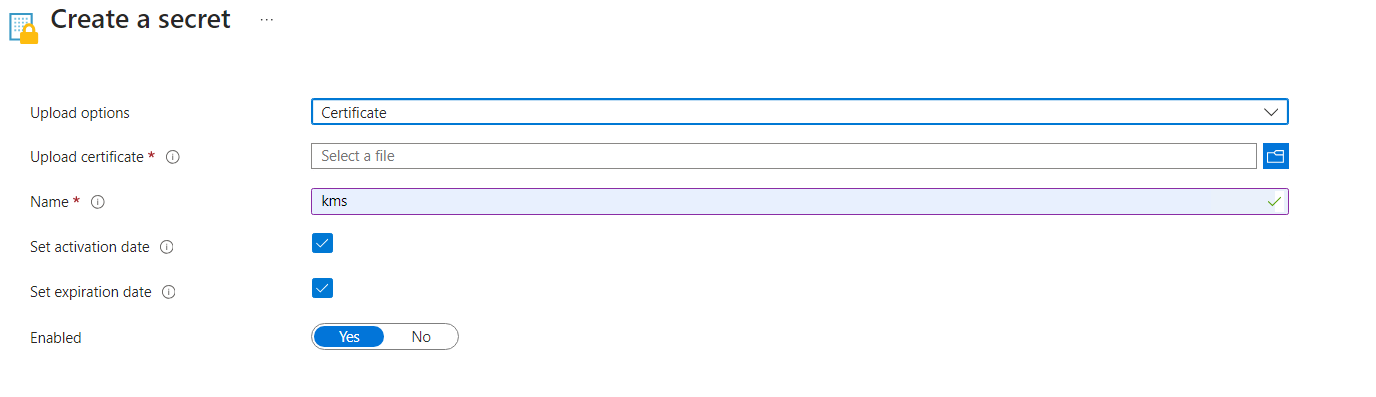


The storage capacity of an Azure Key Vault is limited by the total size of all the secrets, certificates, and keys stored within it. The maximum size of a single Key Vault is 25 KB (25,600 bytes) for standard vaults and 50 KB (51,200 bytes) for premium vaults

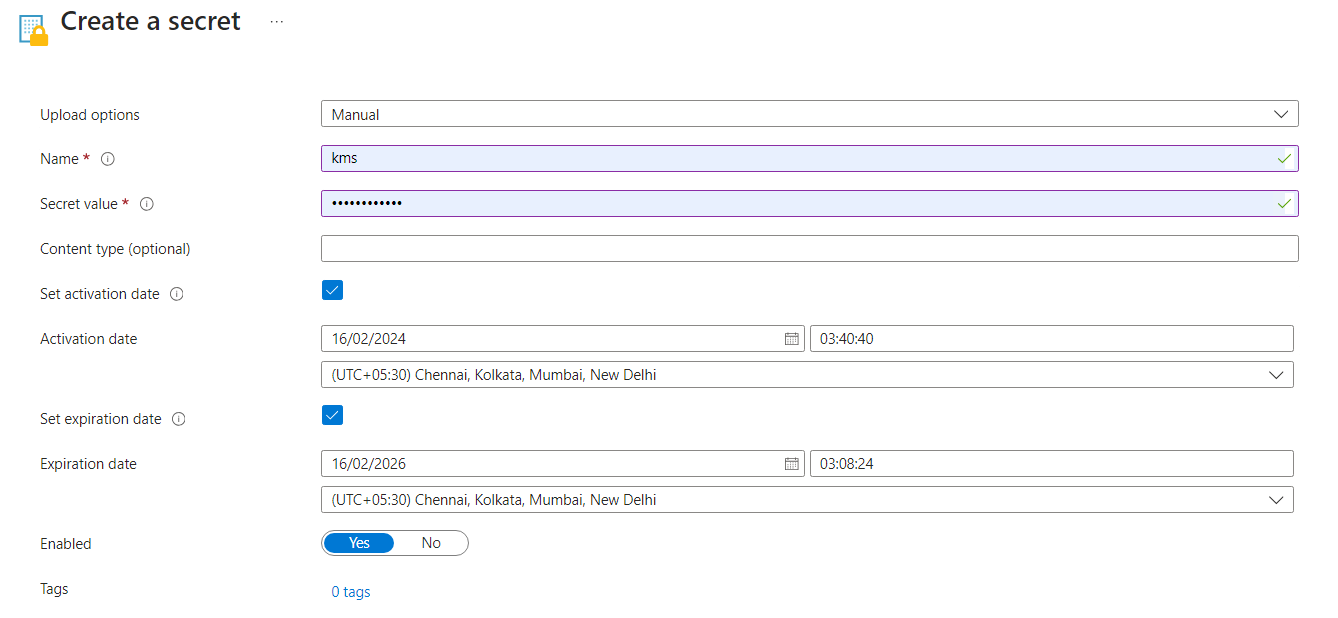
Creating secret – Manual



Creating secret – Certificate



Creating certificate



Networking setting

Like storage account we have Firewall & Virtual network / Private endpoint

