**Azure Key vault - Password management and Password Rotation**

Paper submitted by: Santanu Kumar Sinha, [Santanu.kumar@cognizant.com](mailto:Santanu.kumar@cognizant.com), Microsoft Business Group, Security

Submitted to: Mr. Meera Saheb Shaik, [meerasaheb.shaik@cognizant.com](mailto:meerasaheb.shaik@cognizant.com)

Practice Lead Infra Architect, Microsoft Business Group, Security

Table of Contents

[Azure Key Vault Description 2](#_Toc150636377)

[Azure AD Workload Identities Management 2](#_Toc150636378)

[Best practices for service credentials management in Azure 2](#_Toc150636379)

[Azure Key Vault – Creation and Password Management 3](#_Toc150636380)

[Pre-requisites 3](#_Toc150636381)

[Key Vault creation 3](#_Toc150636382)

[Generate Password 3](#_Toc150636383)

[Show Password using CLI 3](#_Toc150636384)

[Azure Key Vault – Password Rotation Using Key, Secret and Certificate 4](#_Toc150636385)

[Key Vault creation 4](#_Toc150636386)

[Enable Password Rotation with ‘Key’ 5](#_Toc150636387)

[Pre-requisites 5](#_Toc150636388)

[Configuration 5](#_Toc150636389)

[Validation 5](#_Toc150636390)

[Azure AD App ‘Client Secret’ Rotation 5](#_Toc150636391)

[Pre-requisites 5](#_Toc150636392)

[Generate Secret 5](#_Toc150636393)

[Install Function with Template for AAD App Client Secret 5](#_Toc150636394)

[Add permissions using Graph API to Azure Function to generate client secrets in AAD App 6](#_Toc150636395)

[Validation 6](#_Toc150636396)

[Auto Renewal of Certification 6](#_Toc150636397)

[Pre-requisites 6](#_Toc150636398)

[Generate Secret 6](#_Toc150636399)

[Automatic Renewal 7](#_Toc150636400)

[Validation 7](#_Toc150636401)

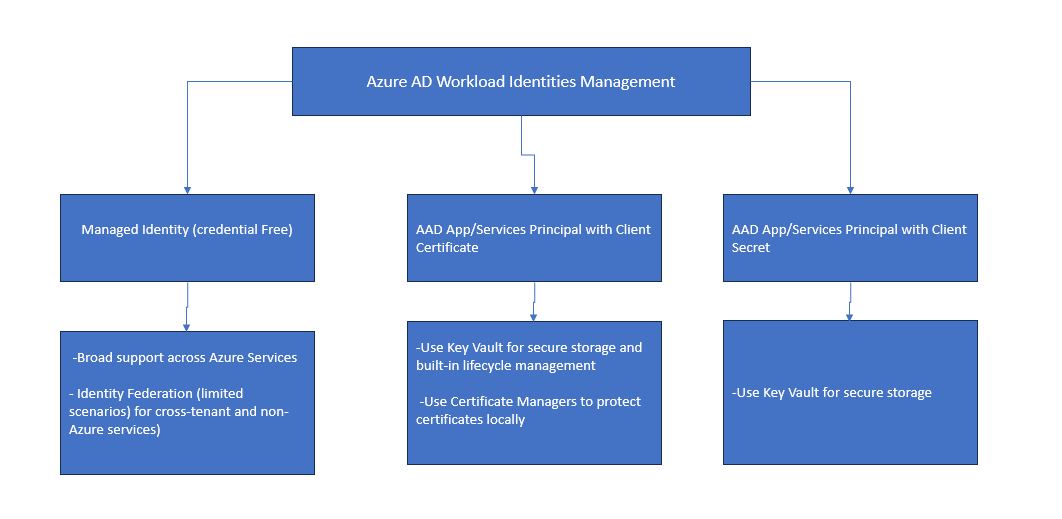
# 

# Azure Key Vault Description

Microsoft Azure Key Vault is a cloud-based security service offered by Microsoft as part of its Azure platform. It provides a secure and centralized storage solution for cryptographic keys and secrets, such as passwords, certificates and keys used for encryption.

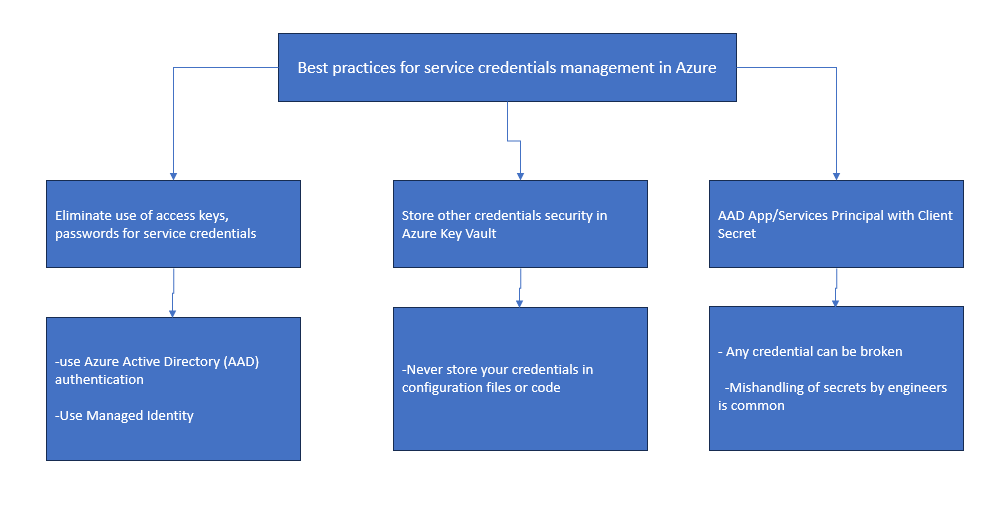
# Azure AD Workload Identities Management

Kindly see below diagram which represent usage of key vault using client certificate, secret and managed identity.



# Best practices for service credentials management in Azure

Kindly see below diagram which represent good practices for managing service credentials.



# Azure Key Vault – Creation and Password Management

## Pre-requisites

* Azure AD subscription with security administrator role.
* Azure AD resource group.
* Azure AD key vault.

## Key Vault creation

<https://portal.azure.com> > Azure services > create a resource > search box, type key vault > create

**Basics:**

* Subscription: select the appropriate subscription.
* Resource Group (RG): Create or select resource group.
* Key vault name: Enter the key vault name.
* Region: Select the region like East US.
* Pricing tier: Standard.
* Soft delete: enabled.
* Days to retain deleted vault: 90 (default)
* Purge protection: select “Disable purge protection (allow key vault and objects to be purged during retention period)” or “Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)”.

**Access configuration**: Azure role-based access control (recommended)

[What is Azure role-based access control (Azure RBAC)? | Microsoft Learn](https://learn.microsoft.com/en-us/azure/role-based-access-control/overview?WT.mc_id=Portal-Microsoft_Azure_KeyVault)

[Assign an Azure Key Vault access policy (CLI) | Microsoft Learn](https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?WT.mc_id=Portal-Microsoft_Azure_KeyVault&tabs=azure-portal)

**Networking**: Public endpoint (all networks).

Review + Create > **Create.**

## Generate Password

* Go to resources after successfully deployment of key vault.
* Click ‘Secrets’ > Generate/import
* Upload option: manual
* Name: enter name like ‘CTS password’
* Value: enter password.
* Enabled: yes.
* Create.
* Click ‘Secrets’ -> open ‘CTS password’ > Show secret value.

## Show Password using CLI

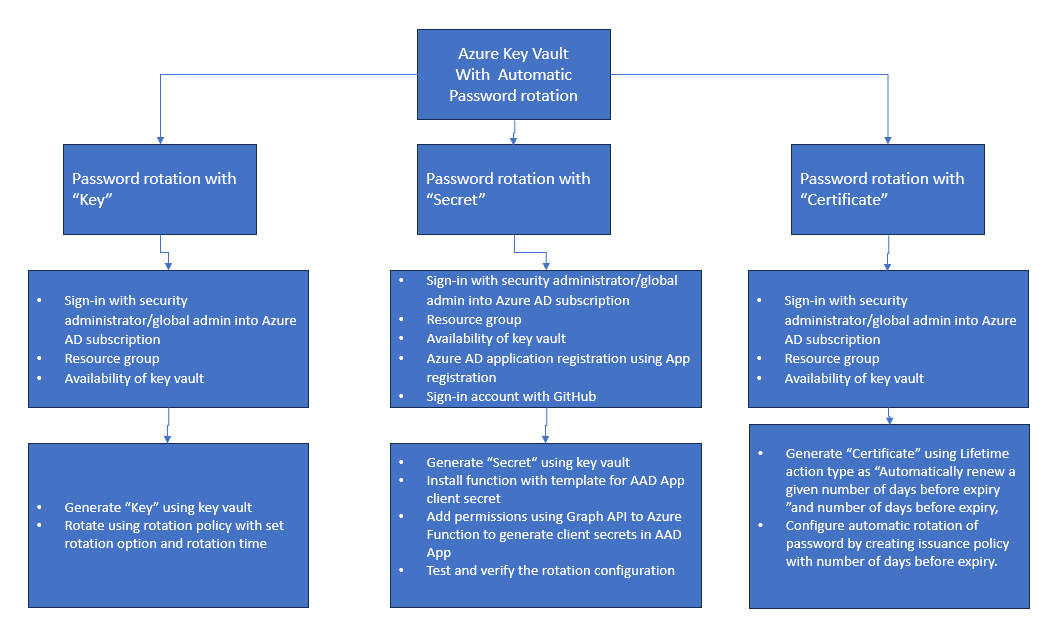
* Open Azure CLI > type the following below.

az keyvault secret show -- name ‘CTS password’ --vault-name ‘key vault name’ -- query value --output tsv

* This will show secret value.

# Azure Key Vault – Password Rotation Using Key, Secret and Certificate

The following below diagram represent the automatic password rotation using key vault.



## Key Vault creation

<https://portal.azure.com> > Azure services > create a resource > search box, type key vault > create

**Basics:**

* Subscription: select the appropriate subscription.
* Resource Group (RG): Create or select resource group.
* Key vault name: Enter the key vault name.
* Region: Select the region like East US.
* Pricing tier: Standard.
* Soft delete: enabled.
* Days to retain deleted vault: 90 (default)
* Purge protection: select “Disable purge protection (allow key vault and objects to be purged during retention period)” or “Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)”.

**Access configuration**: Azure role-based access control (recommended)

[What is Azure role-based access control (Azure RBAC)? | Microsoft Learn](https://learn.microsoft.com/en-us/azure/role-based-access-control/overview?WT.mc_id=Portal-Microsoft_Azure_KeyVault)

[Assign an Azure Key Vault access policy (CLI) | Microsoft Learn](https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?WT.mc_id=Portal-Microsoft_Azure_KeyVault&tabs=azure-portal)

**Networking**: Public endpoint (all networks).

Review + Create > **Create.**

## Enable Password Rotation with ‘Key’

### Pre-requisites

* Azure AD subscription with security administrator role.
* Azure AD resource group.
* Azure AD key vault.

### Configuration

- Open Key vault > keys > Generate/import > Create a key > name (name of the key) > remaining values can be same > create.

- Key is created > Open Key vault > keys > refresh > Select the appropriate key > click to open > Click on ‘rotation policy’ from the menu bar > rotate now > yes.

- Click on Rotation policy >

- Every time: fill the time like 40 days.

- Rotation option: select "Automatically renew at a given number of days before expiry".

- Rotation time: 7 days <save>.

### Validation

- Open Key vault > keys > refresh > Select the appropriate key > click to open > new version of the key will be created along with old version(s). So, current version of the key is the latest key.

## Azure AD App ‘Client Secret’ Rotation

### Pre-requisites

* Azure AD subscription with security administrator role.
* Azure AD resource group.
* Azure AD key vault.
* Azure App registration.
* Sign-in account with GitHub.

### Generate Secret

* Open Key vault > secrets > Generate/import >
* upload option: manual
* name: fill the name
* value: put any value
* content type > text/plain > Create.

### Install Function with Template for AAD App Client Secret

* Browse on <https://github.com/azure/keyvault-secrets-rotation-aadapp-powershell> > go to “Installation” section.
* Click on “Secrets rotation Azure Function and configuration deployment template “ (https://github.com/Azure/KeyVault-Secrets-Rotation-AADApp-PowerShell/blob/main/ARM-Templates/Readme.md) > Click "Deploy to Azure" > Fill "Resource Group", "Key vault name", AD app object ID ( App registration > select and open the app and copy App ID), Secret id and secret value (App registration > select and open the APP > Certificates and secrets > New client secret, copy the secret ID and secret value), secret expiration date Unix time (search Unix timestamp converter in google) > review + create >create.

### Add permissions using Graph API to Azure Function to generate client secrets in AAD App

* Copy the script from the attached test file and replace the “Tenant ID” (go to app registration > select and open the app and get tenant ID) in the script. Also, replace the “Function Identity ObjectID” (Open resource group > select function > click Identity and copy) in the script,
* Copy the attached script and open Cloud shell and execute the script.

### Validation

Azure services > create a resource > search box, type key vault

* Key vault > select appropriate key vault > click to open > Secrets > select the "Secret" > click to open and see the current version of secret does exist.
* Go to Expiration Date: Change the expiration date to one month.
* Go back to “Secret” and refresh.
* Current version and old version secrets will be shown.
* Application registration > select application > Certificates and secrets > click on Client secrets
* new secret will be generated successfully.

## Auto Renewal of Certification

* Provision, manage and deploy digital certificates by Azure Key Vault.
* The certificates can be public, private SSL, TLS certificates signed by a certificate authority or a self-signed certificate.

### Pre-requisites

* Azure AD subscription with security administrator role.
* Azure AD resource group.
* Azure AD key vault.

### Generate Secret

* Go to resources > Open Key vault > certificates > Generate/import >
* method of certificate creation: generate
* Certificate name:
* Type of certificate: Self-signed certificate/certificate issued by an integrated CA/certificate issued by a non-integrated CA
* Subject: CN=xyz.com, for SAN, select DNS names.
* Verify period: 3 months (default 12)
* Content type: PKCS#12
* Lifetime action type:

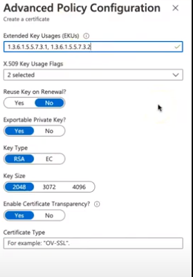
Automatic renew at a given percentage lifetime

Automatically renew a given number of days before expiry (**selected**)

E-mail contacts at a given percentage lifetime

Email all contacts at a given number of days before expiry.

* Number of days before expiry: 30 days (can be changed).
* For advanced configuration: no change.



* Create.

### Automatic Renewal

* Go to resources > Open Key vault > certificates > Refresh, Certificate is available.
* Open the certificate > Click on the correct version of the certificate to validate.
* For automatic renewal, go to resources > Open Key vault > certificates > select certificate > click to open the certificate > issuance policy > number of days before expiry: like 40 days <save>.

### Validation

Open Key vault > certificates > select certificate > click to open the certificate > current version along with old version of certificate will be created with the latest date/time.