



Azure Key Vault

Solve problems

Secrets Management

- Securely store and control access to Tokens, Passwords, Certificates, API keys and Other secrets

Key Management

- Create and control the encryption keys used to encrypt your data

Certificate Management

- Provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates

Why use Azure Key Vault?

Centralize application secrets

Securely store secrets and keys

Monitor access and use

Simplified administration of application secrets

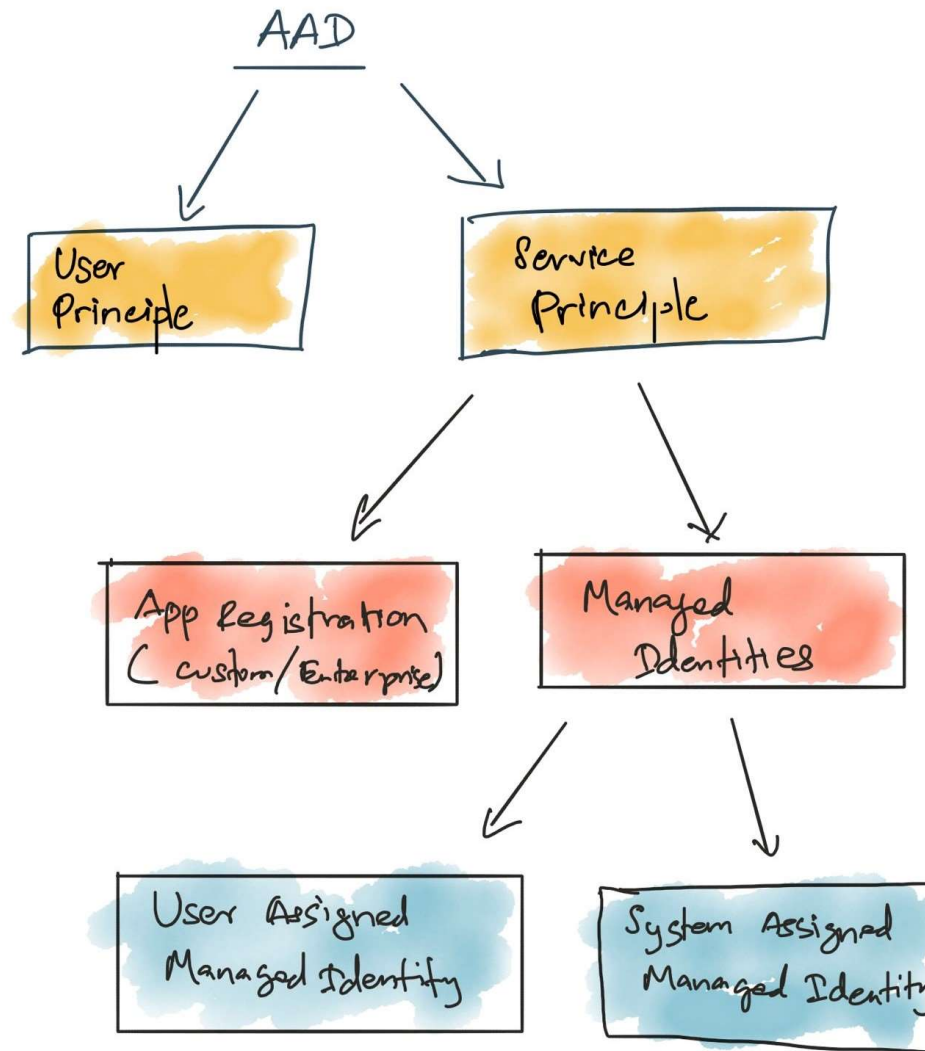
Keys vs Secrets

- Key
 - A Cryptographic key represented as JWK (JSON Web Key).
 - Example: store A .pfx certificate file that contains a pair of public & private keys
- Secret
 - Key Vault accepts any value and stores it as a binary.
 - Example: A password or API key

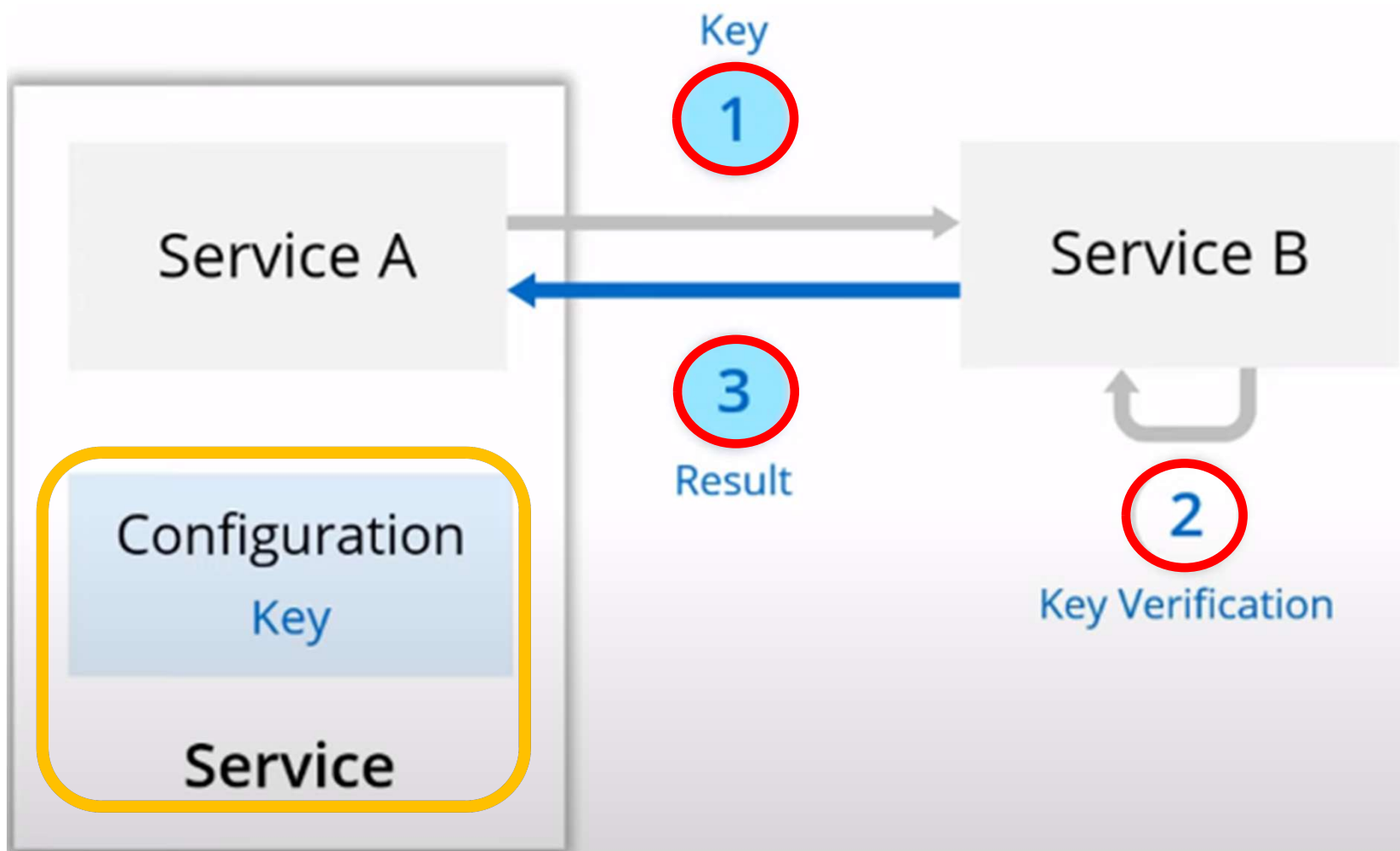
Hands-On: Key Vault

Managed Identity

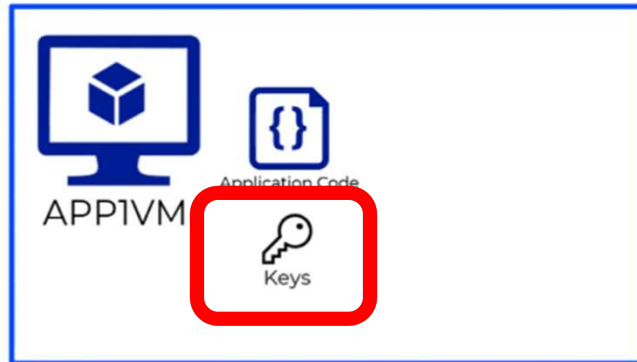
AAD Principle



The Problem



The Problem

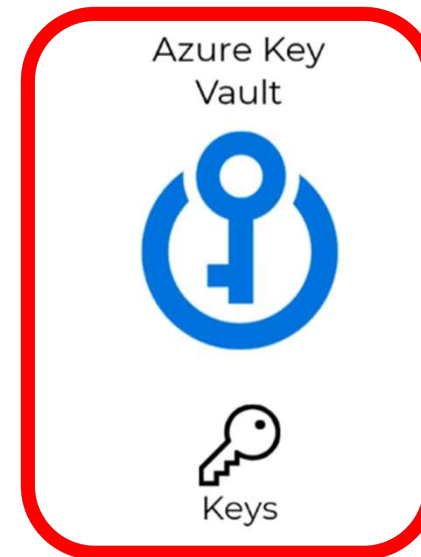
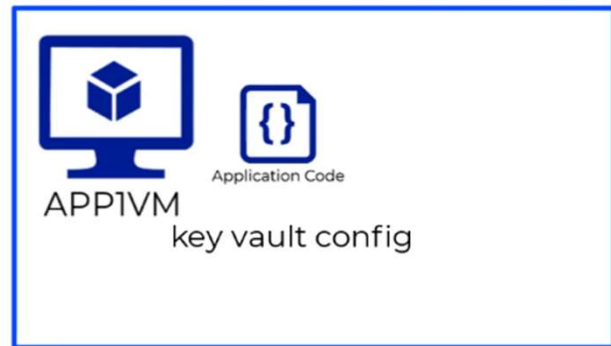


Azure SQL
Database



Keys, Secrets in Code
and Config ?? No WAY !





Azure SQL Database



Can we have ZERO secrets or keys in code please ??

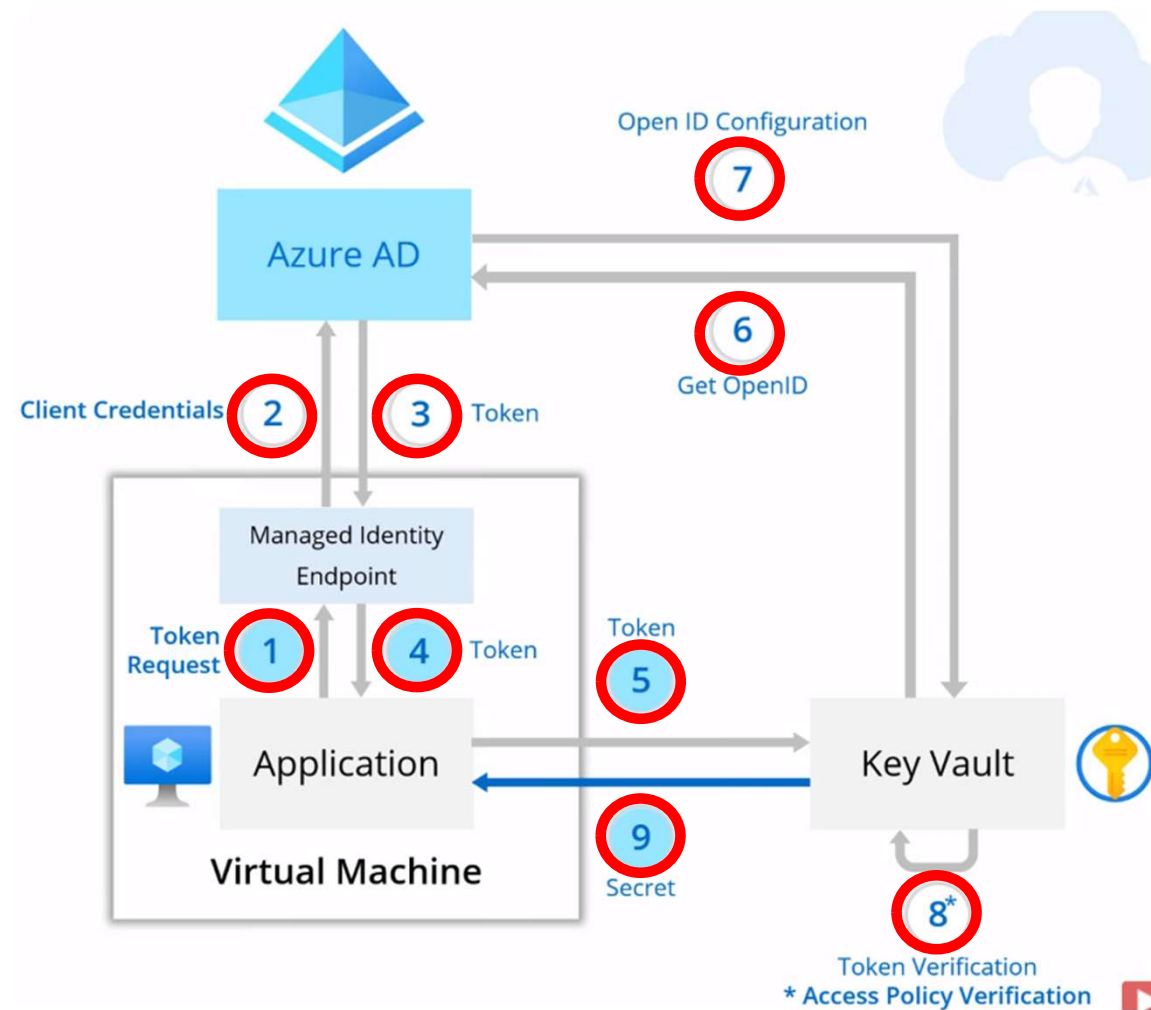


Solution: Managed Identities

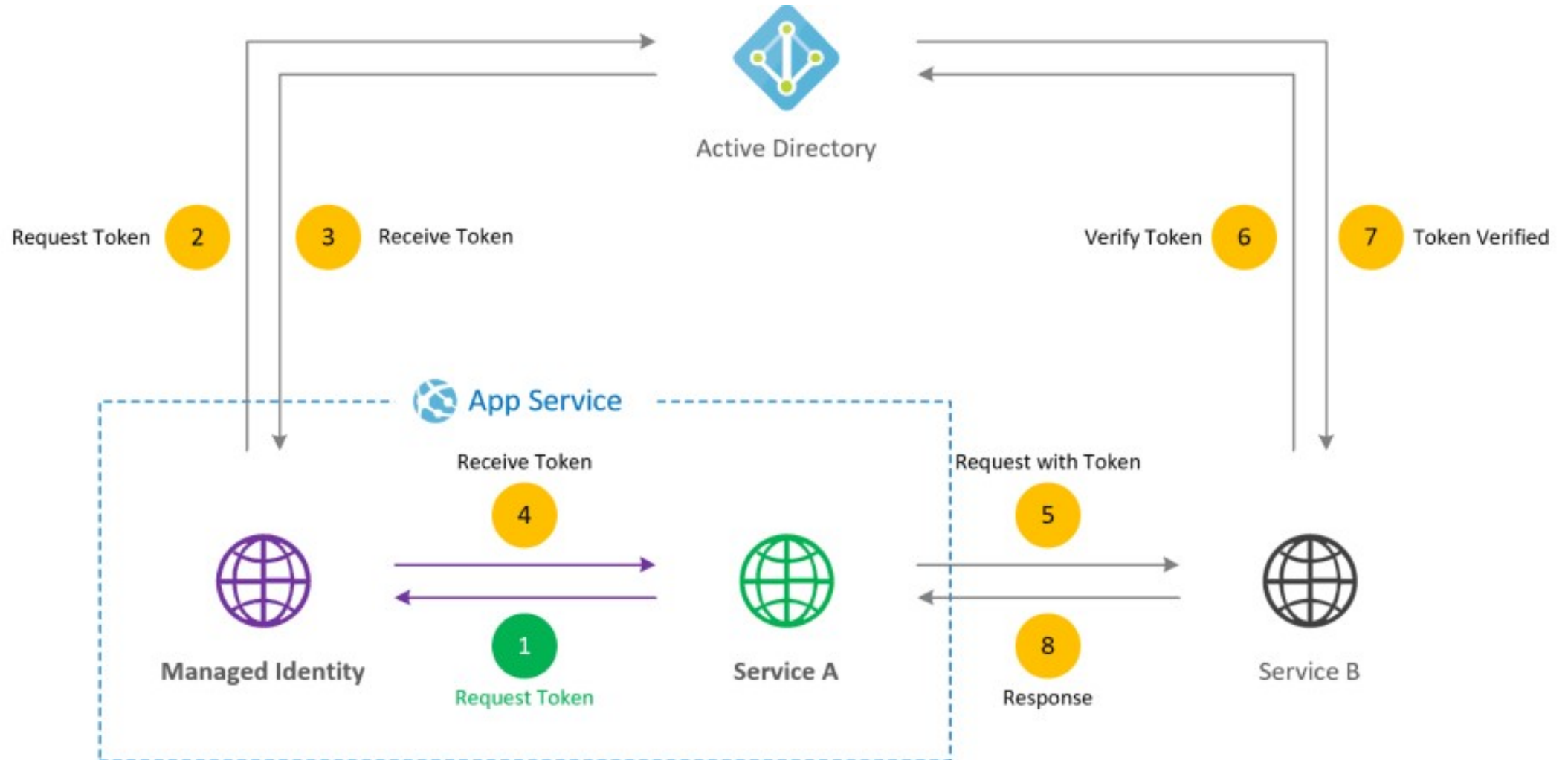
- Characteristics
 - Credentials are moved out of application code
 - Identity created and tied with resource lifecycle
 - Managed Identities are Service Principals of special type
 - Auditable
 - Can be assigned and revoked from individual resources

Managed Identities – Solving Challenges

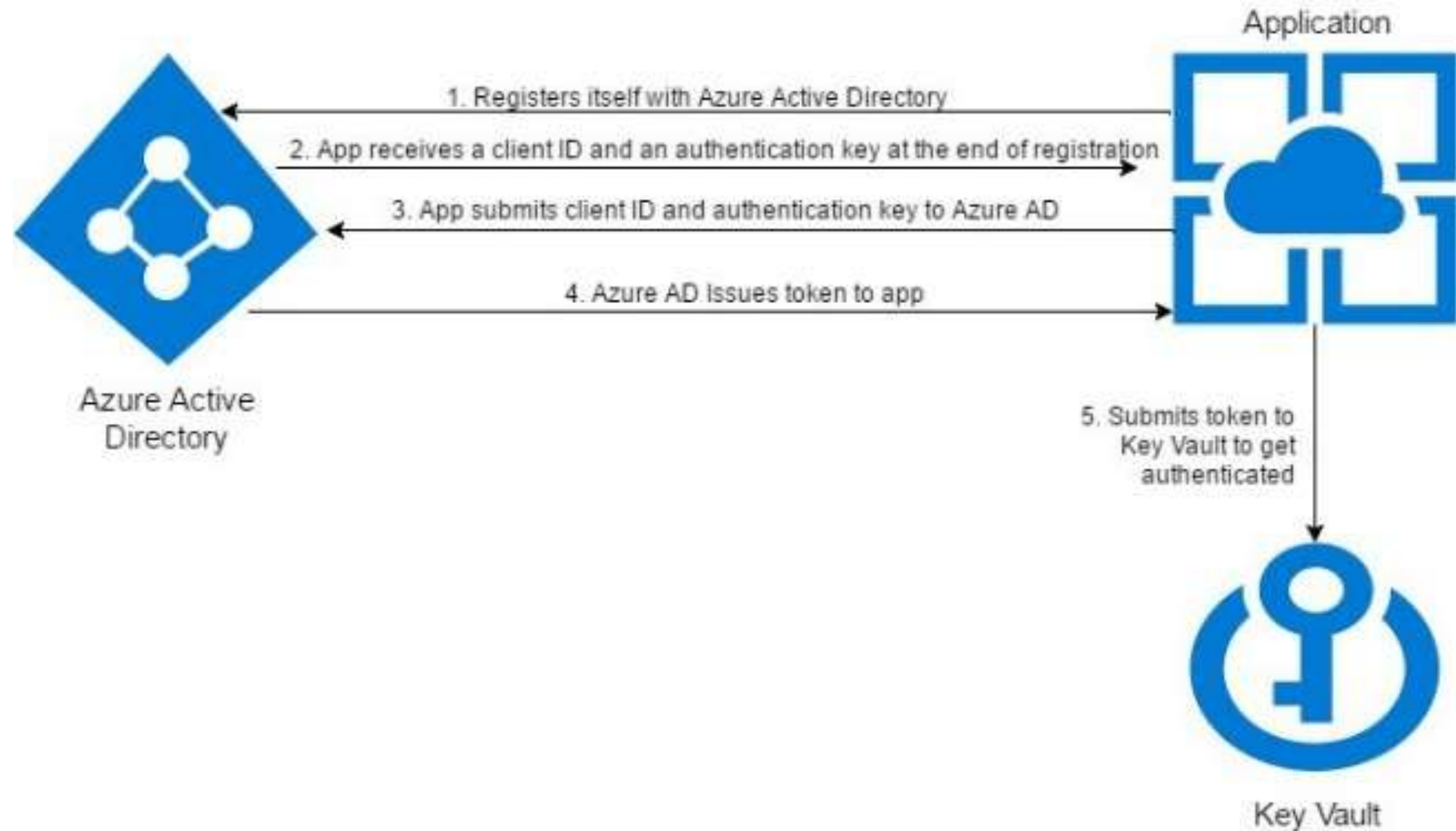
- Internal Endpoint
- No Credentials in the code
- Identity name is the same as resource name
- Identity lifecycle is tied to resource



Managed Identities – Solving Challenges



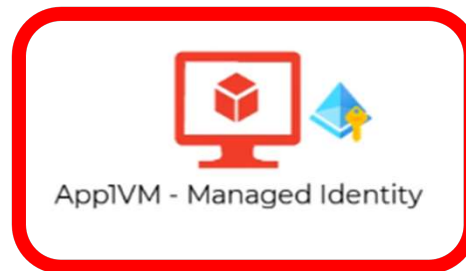
Managed Identities – Solving Challenges



Managed Identities Enabled



Azure Active Directory

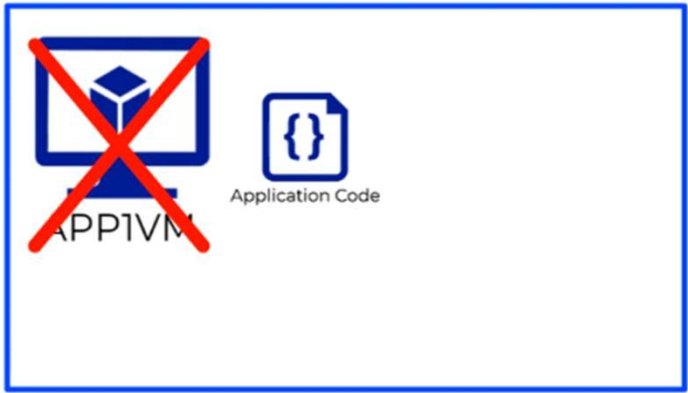


Azure SQL Database



Identity and Access Management

Auto Deleted if VM is Deleted



Azure Active Directory



Azure SQL Database



Contributor-->



Hands-On: System Assigned Managed Identity

- Step 1: Create Data Factory
 - Managed Identity for Data Factory is auto created
- Step 2: Grant Access to the Identity
 - Open Target Resource (SQL Server) which is to be access securely
 - Open IAM
 - Grant Permission to Managed Identity
 - Role: Reader
- Now data factory can access SQL Server

Add role assignment

Role Contributor

Assign access to Virtual Machine

Subscription * Anand MS Internal

Select Search by name

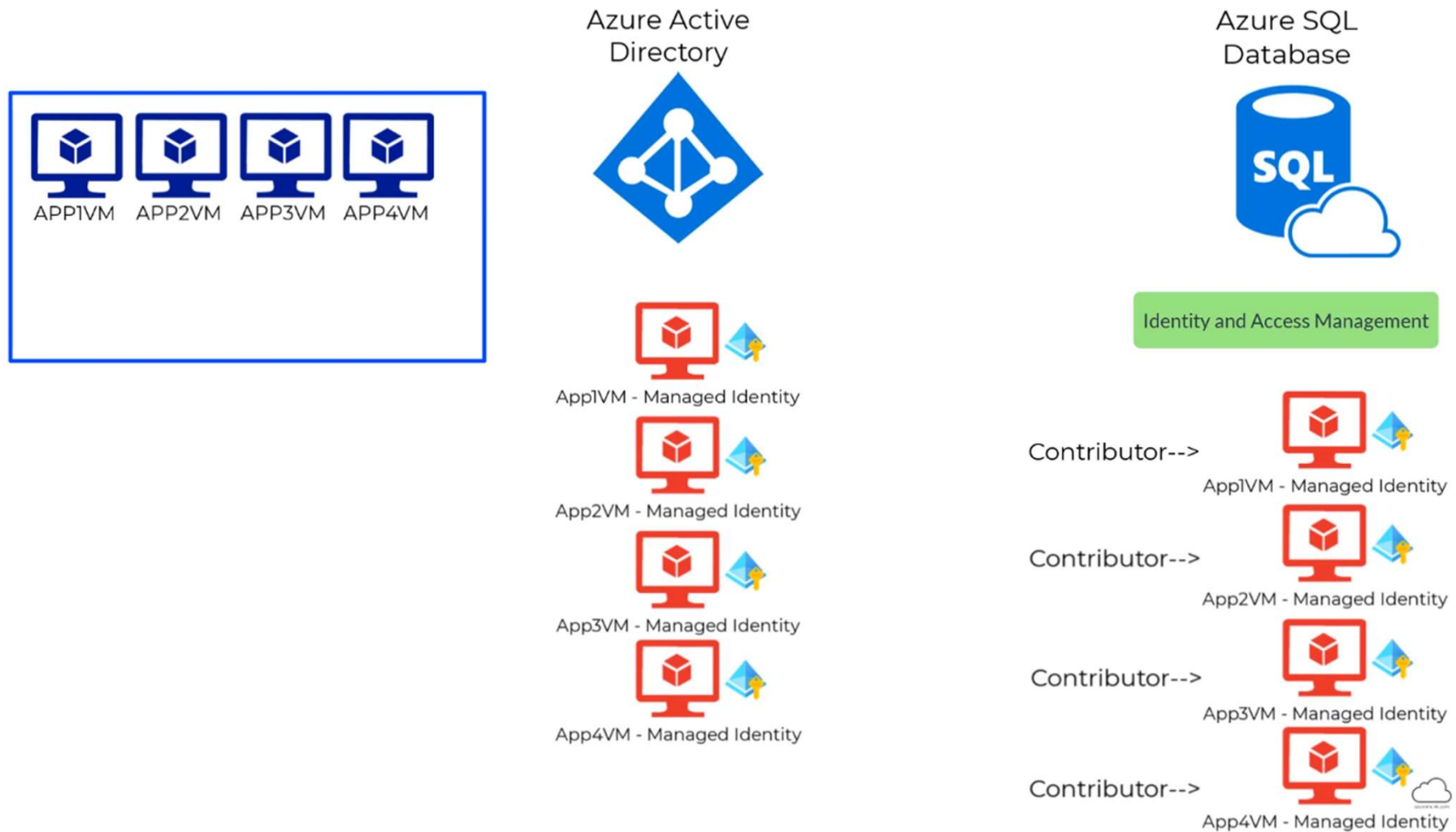
No results to display.

Selected members:

App1VM /subscriptions/25dfeaff-87e5-44fc-9a... [Remove](#)

[Save](#) [Discard](#)

Becomes unmanageable if VMs increases



Azure Key Vault Security and Best Practices

Control Access to your vault

- Lock down access to your subscription, resource group and Key Vaults (RBAC)
- Create Access policies for every vault
- Use least privilege access principal to grant access
- Turn on Firewall and VNET Service Endpoints

Use separate Key Vault

- Use a vault per application per environment

Backup

Use Logging from Monitoring Section

Turn on recovery options

- Turn on Soft Delete.
- Turn on purge protection

Thanks