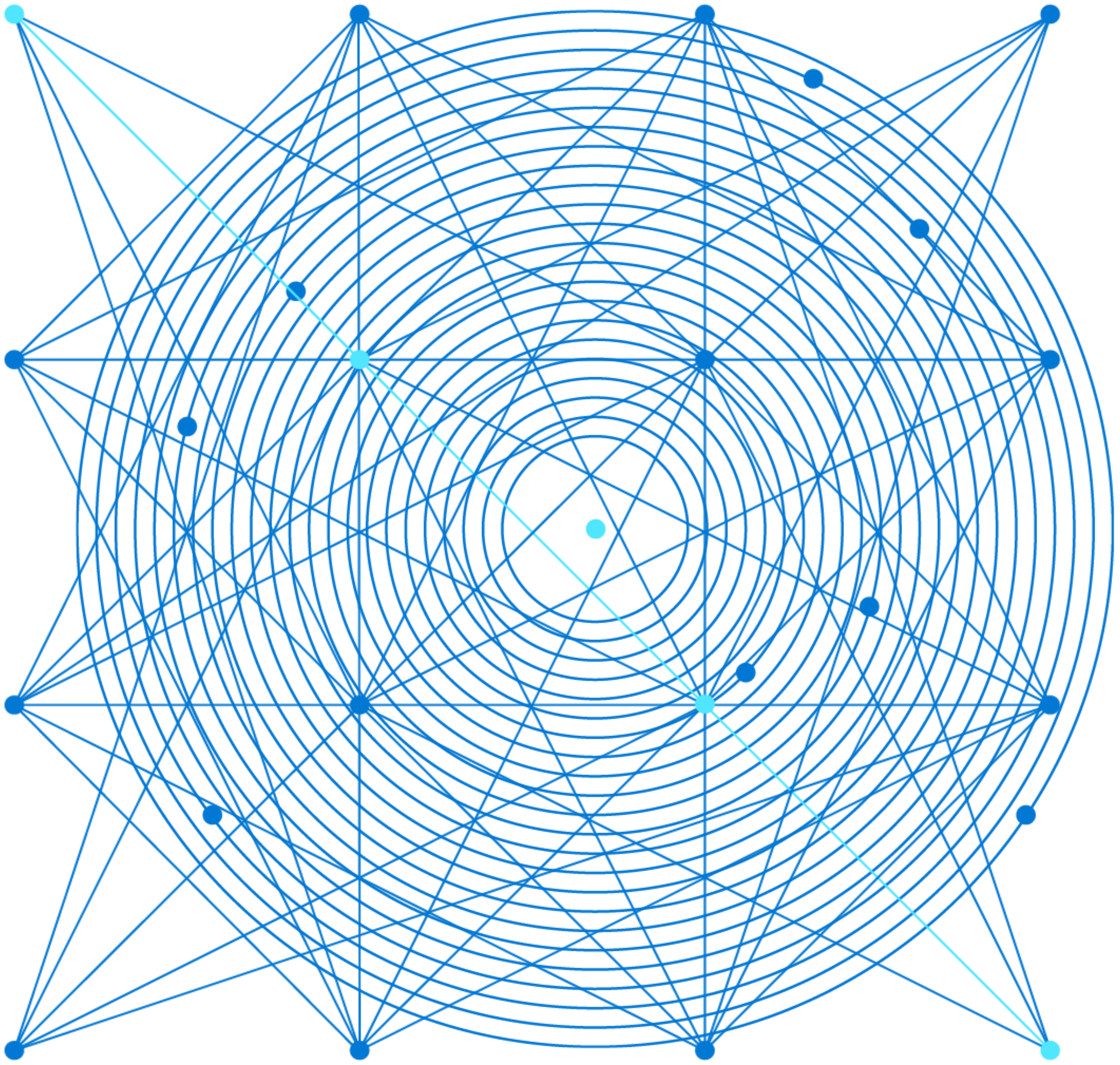
AZ-303: Microsoft Azure Architect Technologies



Module 11: Manage Security for Applications

Azure Key Vault and Managed Identities

Learning Objectives

You will learn the following concepts:

Azure Managed Identity

- Authentication with Azure managed identities
- Using managed identities with Azure resources

Azure Key Vault

- Azure Security Center
- Key Vault users

Azure Managed Identity

Authentication with Azure Managed Identities

A managed identity:

- combines Azure AD authentication and Azure RBAC
- eliminates the need for rotating credentials or certificates

The concept of managed identities involves the use of:

- Client ID
- Object ID
- Azure Instance Metadata Service

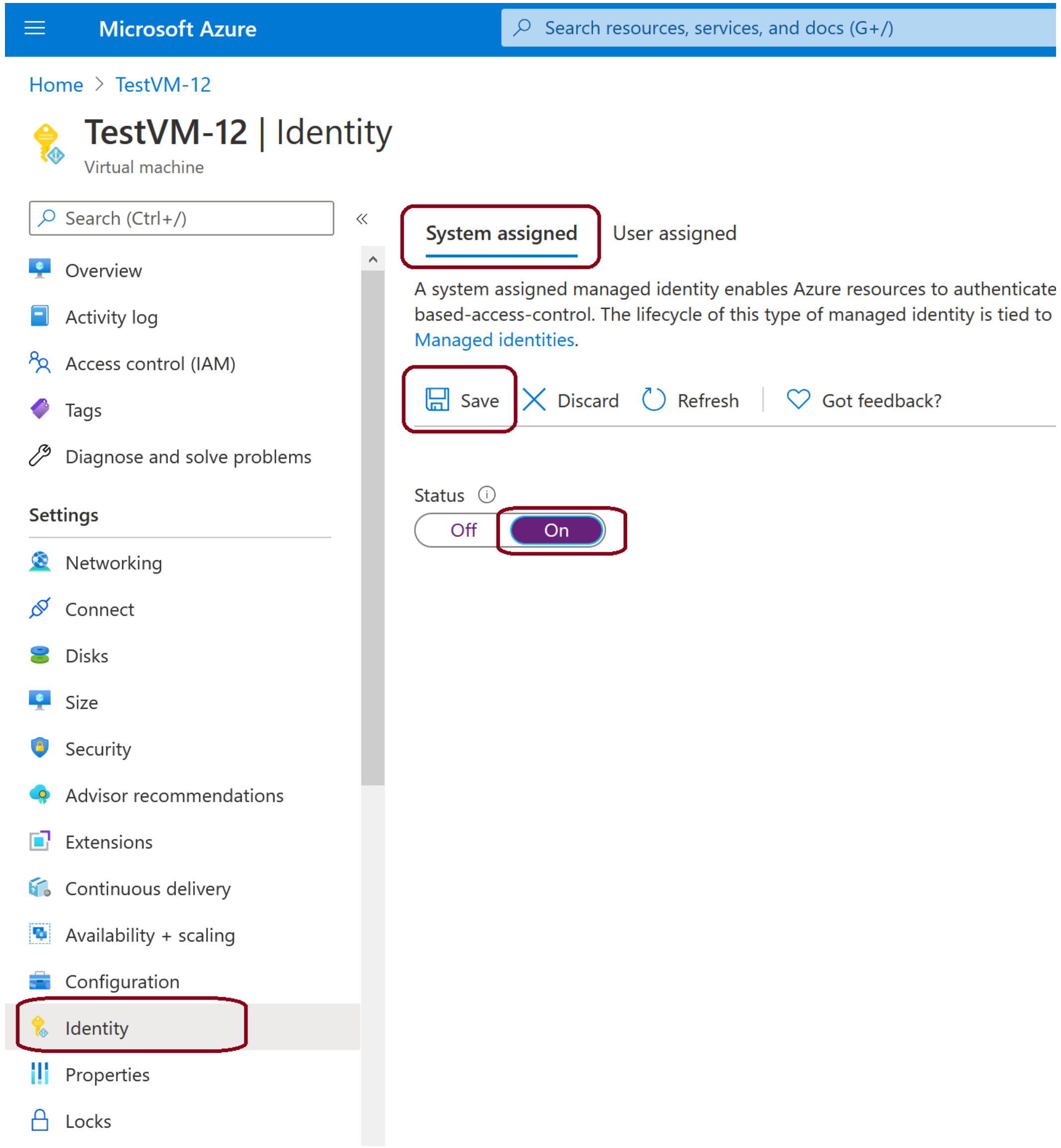
There are two types of managed identities:

- System-assigned managed identity
- User-assigned managed identity

Using Managed Identities with Azure Resources

To set up a managed identity:

1. In the Azure portal, go to the VM that hosts the app you want to authenticate
2. On the overview page, under **Settings**, select **Identity**
3. Choose a system-assigned or user-assigned identity
4. Save your changes



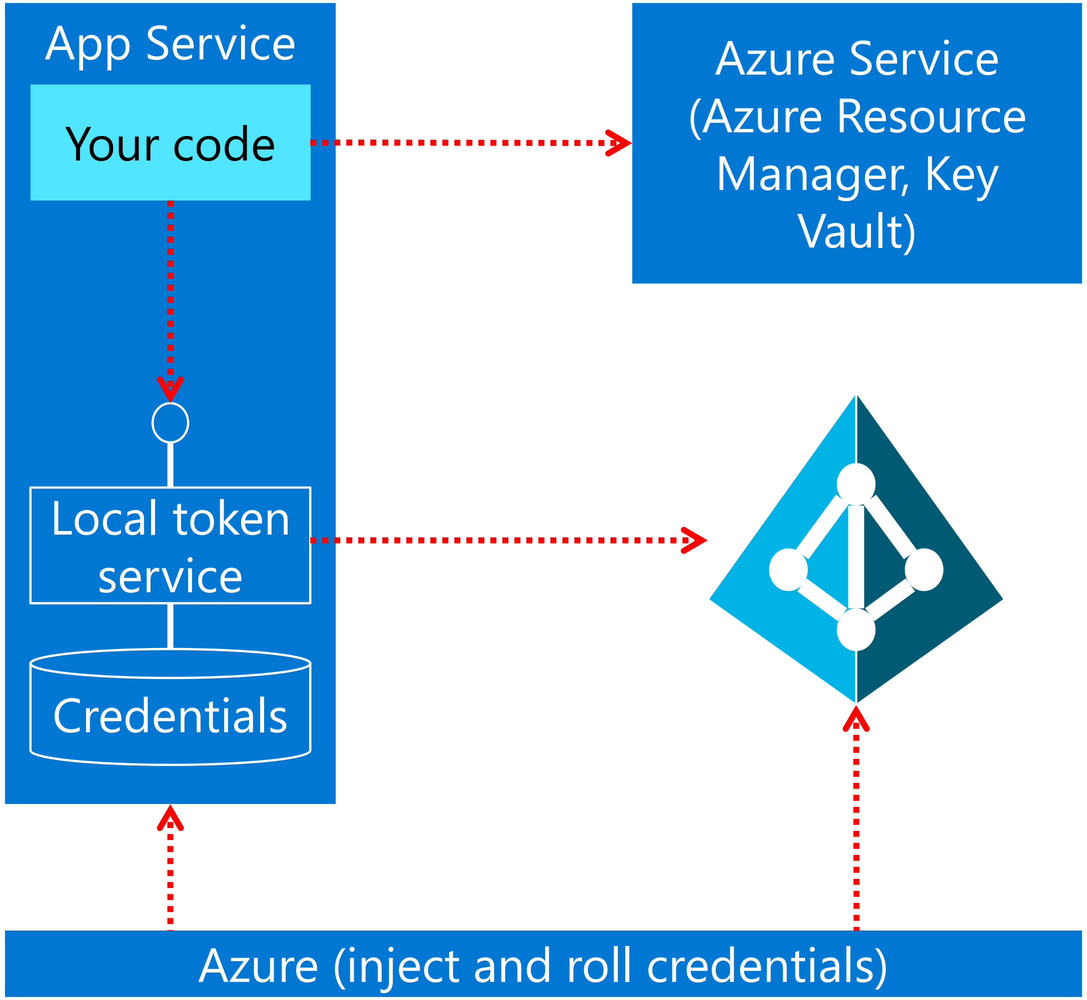
A system assigned managed identity enables Azure resources to authenticate based-access-control. The lifecycle of this type of managed identity is tied to Managed identities.

Status: Off [✓ On]

Managed Identities for Azure Resources in Azure AD

Help you manage the credentials for authenticating to cloud services, when building cloud applications:

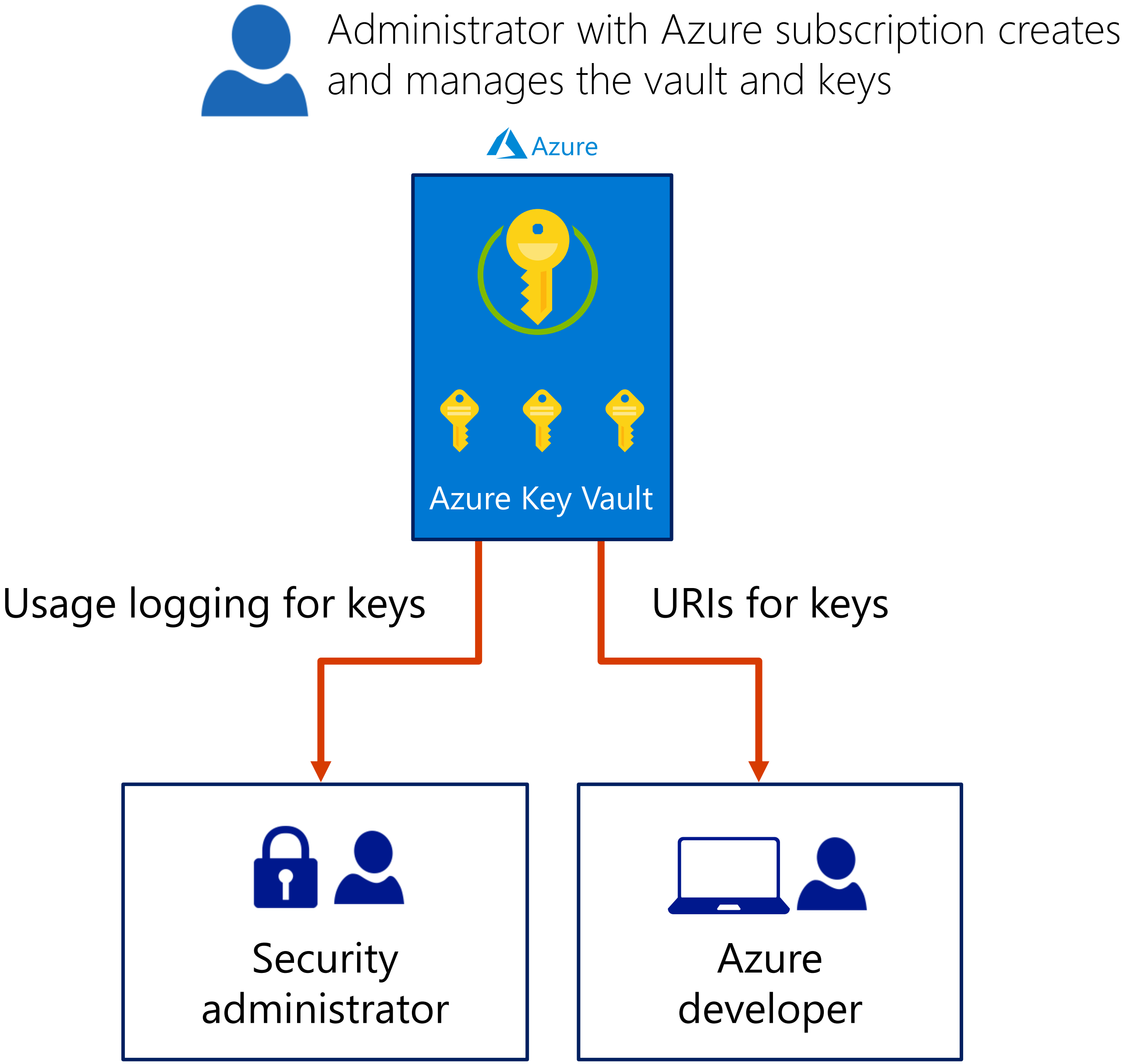
- Keeps credentials out of code
- Identity automatically managed in Azure AD for Azure resources
- Uses a local MSI endpoint to get access tokens from Azure AD
- Direct authentication with services or retrieve credentials from Azure Key Vault


App Service
Your code
Local token service
Credentials
Azure Service (Azure Resource Manager, Key Vault)
Azure (inject and roll credentials)

Azure Key Vault

Azure Key Vault Overview

- Secrets management
- Key management
- Certificate management
- Storing secrets



Azure Key Vault

Azure Key Vault is a service that facilitates storage and management of:

- Secrets
- Keys
- Certificates

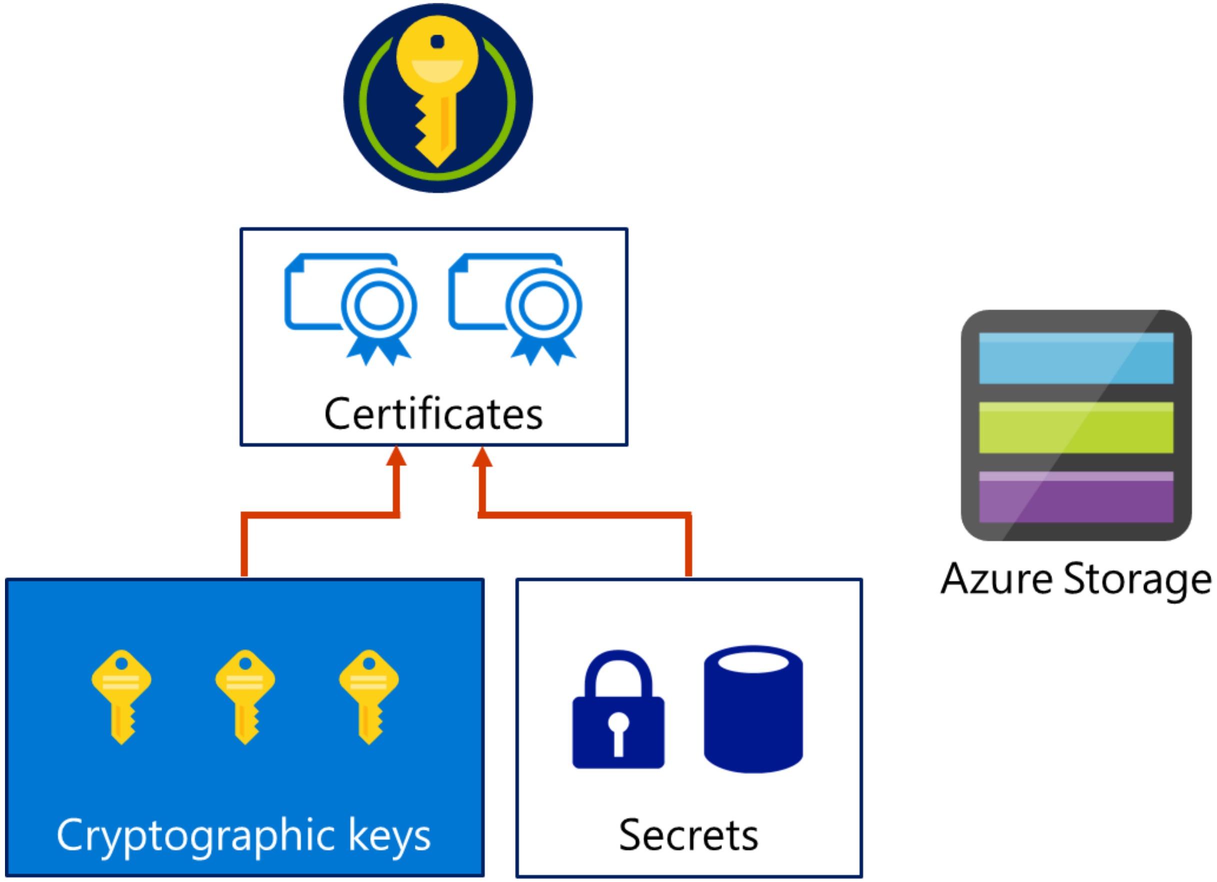
Keys

- hardware-protected by using HSMs that provide a hardened, tamper-resistant environment for cryptographic processing and key generation
- software-protected by using software-based RSA and ECC algorithms

Secrets

- Small (less than 10K) data blobs protected by a HSM-generated key

Key Vault Secret Types



Key Vault Terminology

Vault owner

Vault consumer

Service principal

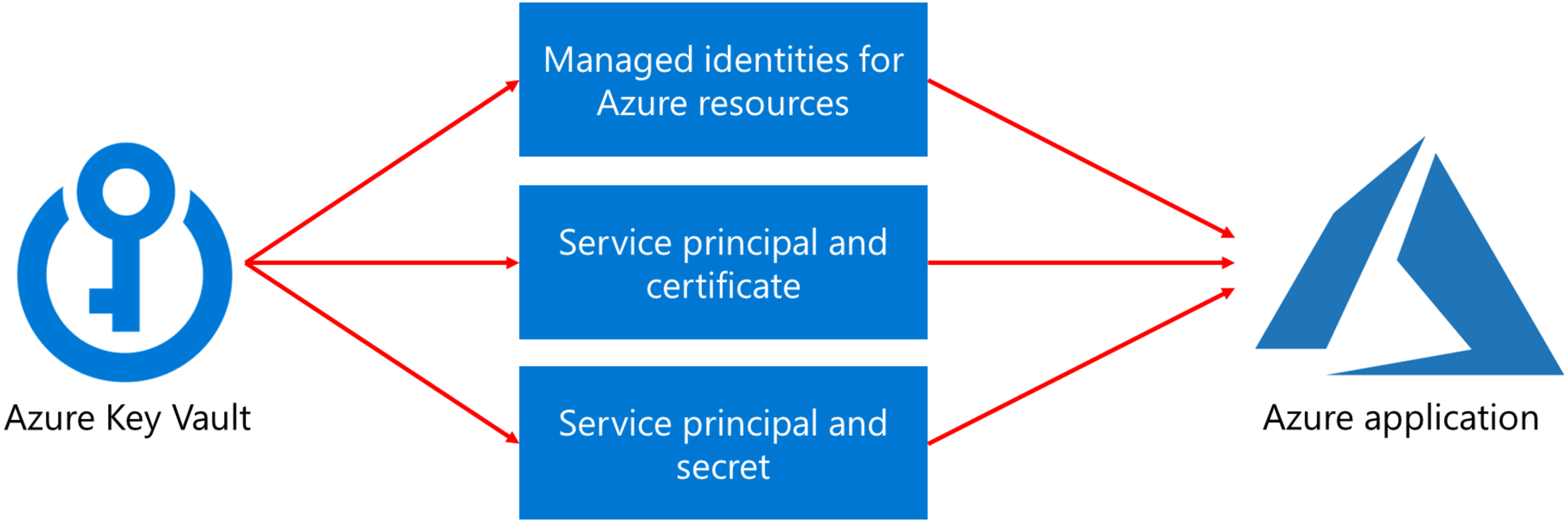
Azure Active Directory

Azure tenant ID

Managed identities

Authentication

Ways to authenticate to Key Vault:



Managed identities for Azure resources
Service principal and certificate
Service principal and secret
Azure Key Vault
Azure application

Key Vault Users

Azure Key Vault helps manage the following tasks:

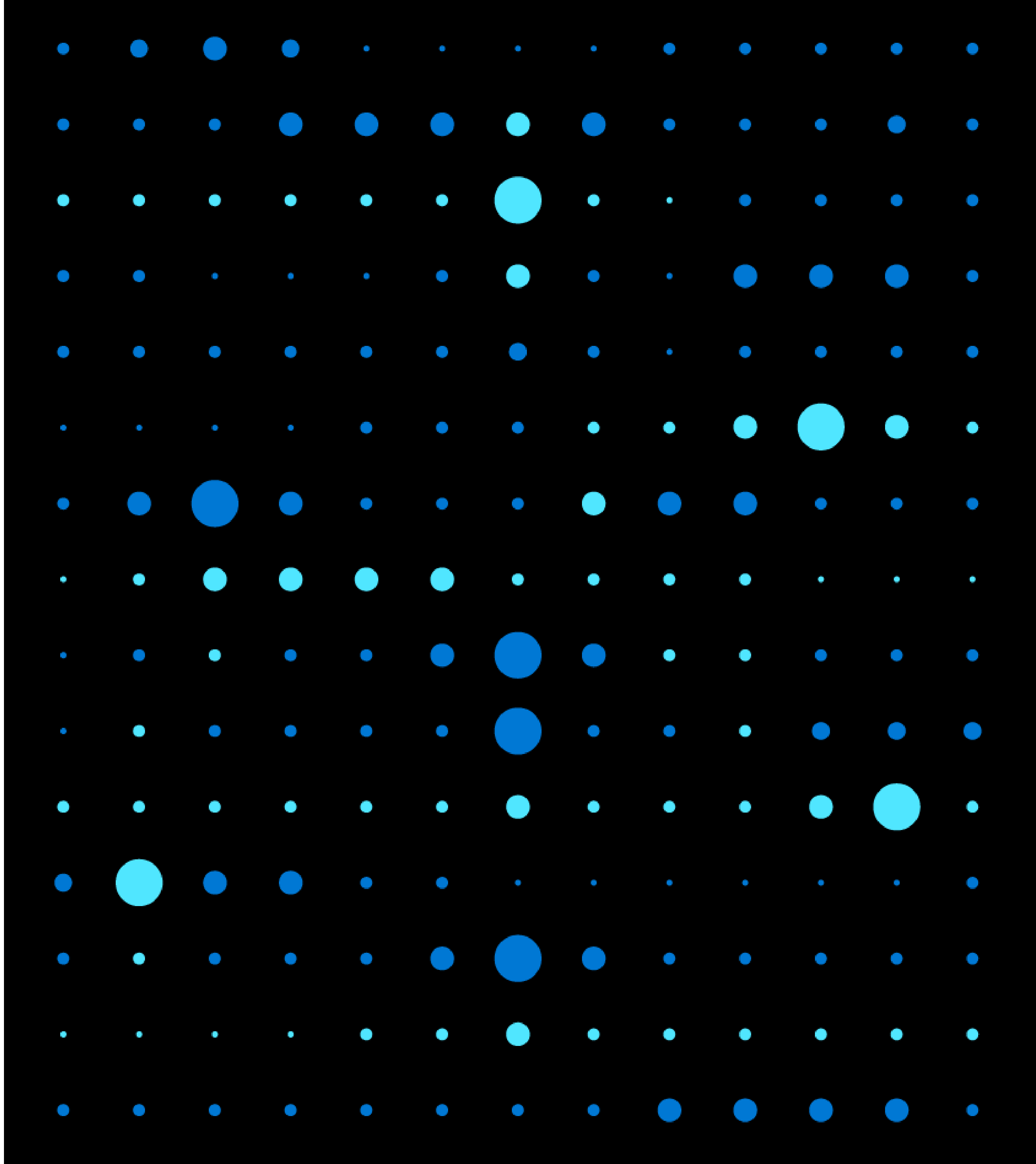
- Secrets management
- Key management
- Certificate management

Best practices:

- Grant access at a specific scope
- Control what users have access to
- Store certificates in the key vault
- Ensures that you can recover a deleted key vault or key vault objects

Demonstration: Configure Certificate Auto-Rotation in Key Vault

- Manage a certificate by using the Azure portal.
- Add a CA provider account.
- Update the certificate's validity period.
- Update the certificate's auto-rotation frequency.
- Update the certificate's attributes by using Azure PowerShell.



Module 11 Review Questions

Microsoft Azure

Online Role-based training resources:

Microsoft Learn

https://docs.microsoft.com/en-us/learn/

Microsoft Azure

Thank you.