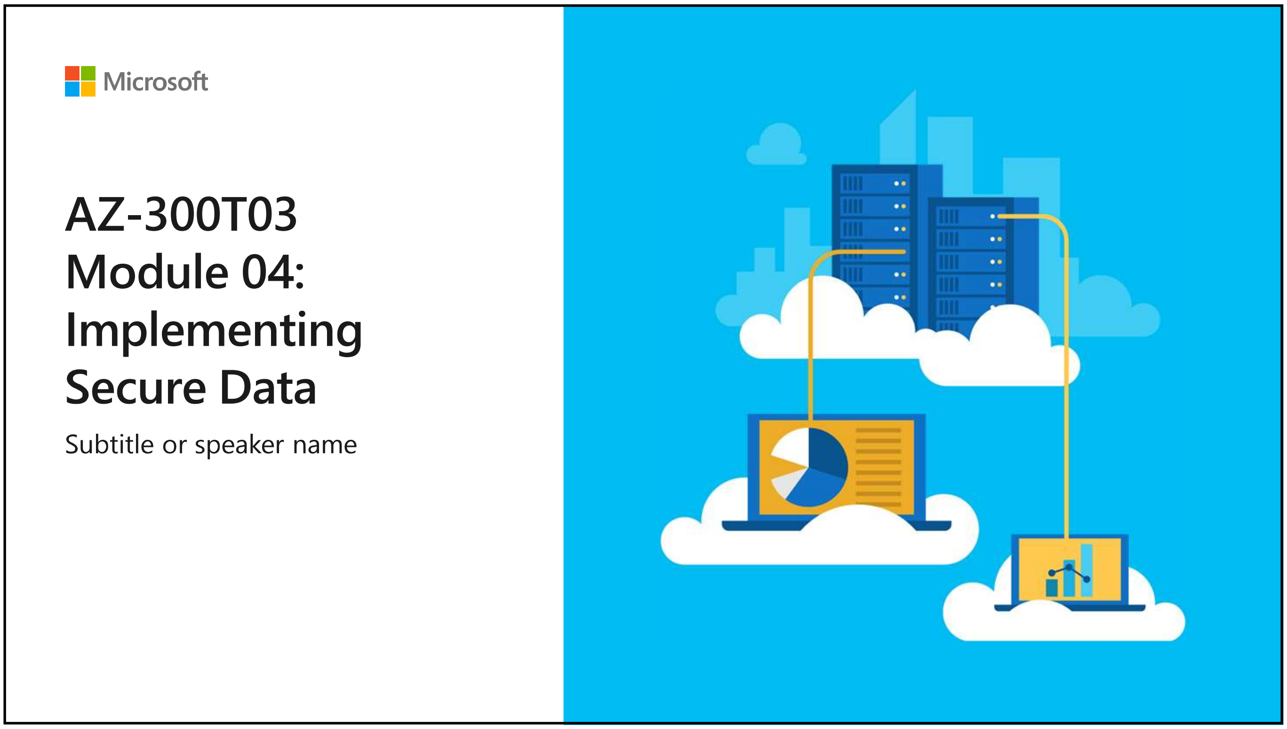


Microsoft

AZ-300T03 Module 04: Implementing Secure Data

Subtitle or speaker name

1

Module 05: Implementing Secure Data

Lesson 01: Encryption Options

2

Encryption

The process of translating plain text into ciphertext.

Uses an encryption algorithm and one or two keys:

- **The objective of the algorithm is to make it as difficult as possible to decrypt the ciphertext without using the key(s)**
- **In symmetric encryption:**
  - **The same key is used for encryption and decryption**
  - **Intended for encryption of large amounts of data**
- **In asymmetric encryption:**
  - **Different key for encryption (public) and decryption (private)**
  - **Intended for small amounts of data or for encryption of a symmetric key**

3

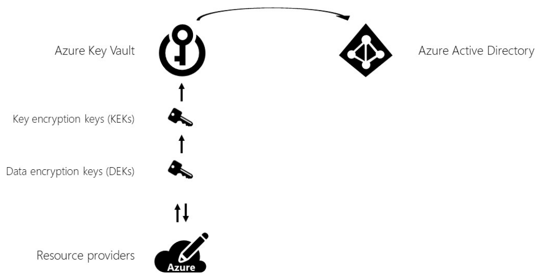
Encryption at rest

Encryption of data when it is persisted:

- **Protects against attempts to obtain physical access to the hardware on which the data is stored and to then compromise the contained data**
- **Is mandatory in many scenarios due to compliance and security requirements**

Encryption at rest in Azure:

- **Dynamically encrypts/decrypts during writes/reads**
- **Uses symmetric encryption keys**
- **Uses different keys across partitions**
- **Stores keys in a secure location**
- **Includes:**
  - **Azure Storage encryption**
  - **Azure SQL Database encryption**
  - **Azure Cosmos DB encryption**



4

Module 05: Implementing Secure Data

Lesson 02: End-to-end Encryption

5

Encrypt data with Always Encrypted

Encryption technology in Azure SQL Database and SQL Server:

- **helps ensure that sensitive data never appears as plaintext inside the database system.**
- **allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the database engine (SQL Database or SQL Server).**
- **helps protect sensitive data:**
  - **at rest on the server**
  - **during movement between client and server**
  - **while the data is in use**
- **provides a separation between:**
  - **those who own the data (and can view it)**
  - **those who manage the data (but should have no access).**
- **requires a specialized driver installed on client computers to automatically encrypt and decrypt sensitive data in the client application:**
  - **For many applications, this does require some code changes.**

6

Module 05: Implementing Secure Data

Lesson 03: Manage Cryptographic Keys in Azure Key Vault

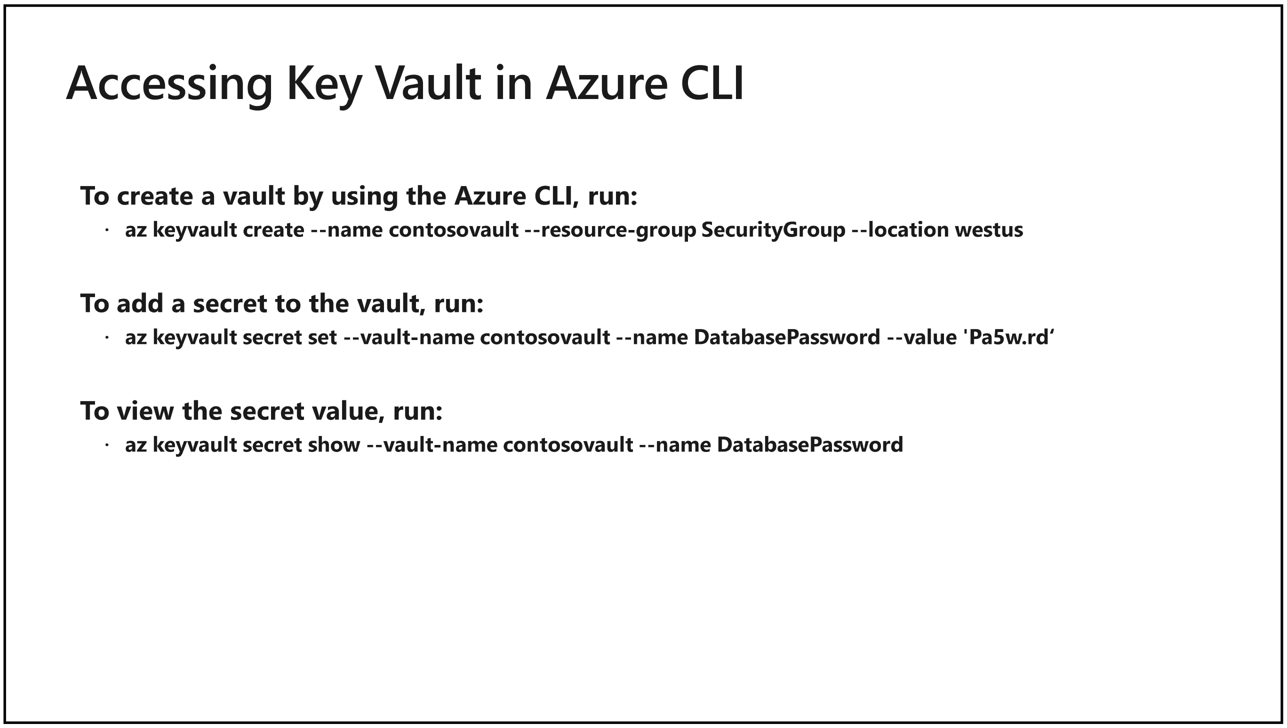
7

Azure key vault

A cloud service that works as a security-enhanced secrets store:

- **Allows you to create multiple security-enhanced containers, called vaults**
- **Main vault characteristics:**
  - **Support for secrets, such as a password, keys, and certificate.**
  - **The use of hardware security modules (HSMs) for key storage and cryptographic operations**
  - **The ability to request and renew TLS certificates**
  - **Logging of all operations.**

8



Accessing Key Vault in Azure CLI

To create a vault by using the Azure CLI, run:

- **az keyvault create --name contosovault --resource-group SecurityGroup --location westus**

To add a secret to the vault, run:

- **az keyvault secret set --vault-name contosovault --name DatabasePassword --value 'Pa5w.rd’**

To view the secret value, run:

- **az keyvault secret show --vault-name contosovault --name DatabasePassword**

9

Microsoft

10