

Encrypting and Decrypting Data at Rest



Reza Salehi

MCT, MCSA(CLOUD PLATFORM), MCPD

@zaalion [linkedin.com/in/rezasalehi2008](https://www.linkedin.com/in/rezasalehi2008)



Overview



Understanding Azure Storage Service Encryption for data at rest

Configuring customer-managed keys (BYOK) for storage account

Demo: Configuring customer-managed keys (BYOK) for *MyAddressBook+*

Azure Disk Encryption for IaaS Virtual Machines

Demo: Azure Disk Encryption

Summary



Azure Storage Service Encryption for Data at Rest



Data in Transit vs. Data at Rest

Data in transit

When data is being transferred between components, locations, or programs, such as over the network, across a service bus

Data at rest

Inactive data that is stored physically in any digital form (e.g. databases, files, data warehouses)



Attacks against data at rest
include attempts to obtain
physical access to the
hardware on which
the data is stored



“Encryption at Rest” is the encoding (encryption) of data when it is persisted



Azure Storage Service Encryption for Data at Rest

Organizational security

Your security strategy requires
all data at rest to be
encrypted at all times

Compliance commitments

Your organization is required
by customers, partners, or
government regulations to
encrypt data at rest



“Azure Storage Service Encryption (SSE) for data at rest helps you protect your data to meet your organizational security and compliance commitments.”

Microsoft



Azure Storage Supported Types



Azure Blob storage



Azure Table storage



Azure Files



Azure Queue storage



Azure Managed Disks



Azure Storage Service Encryption for Data at Rest



Storage Service Encryption (SSE) is enabled for all new and existing storage accounts and cannot be disabled



Your data is secured by default, you don't need to modify your code or applications to take advantage of Storage Service Encryption



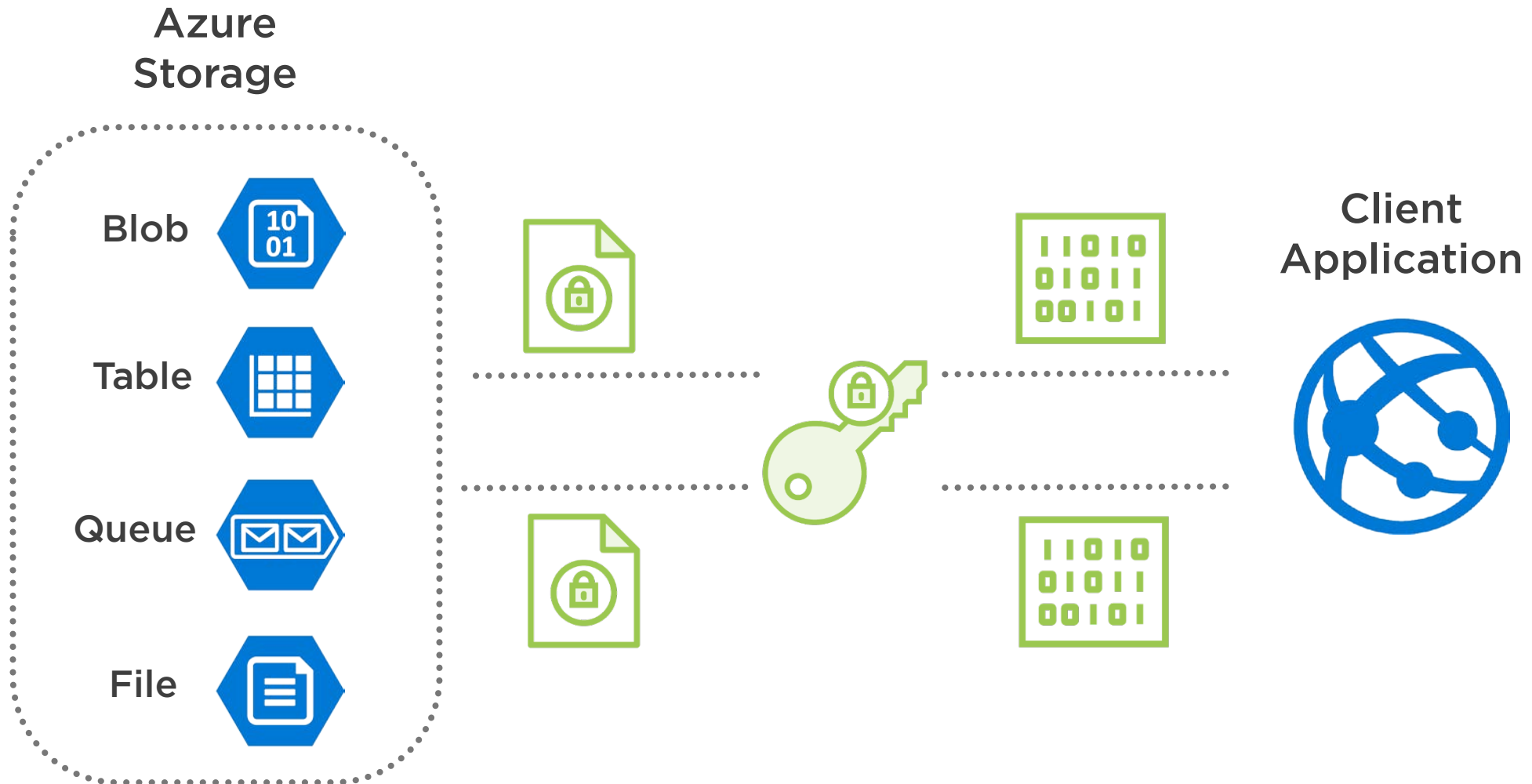
SSE automatically encrypts data in all performance tiers (Standard and Premium), all deployment models (Azure Resource Manager and Classic)



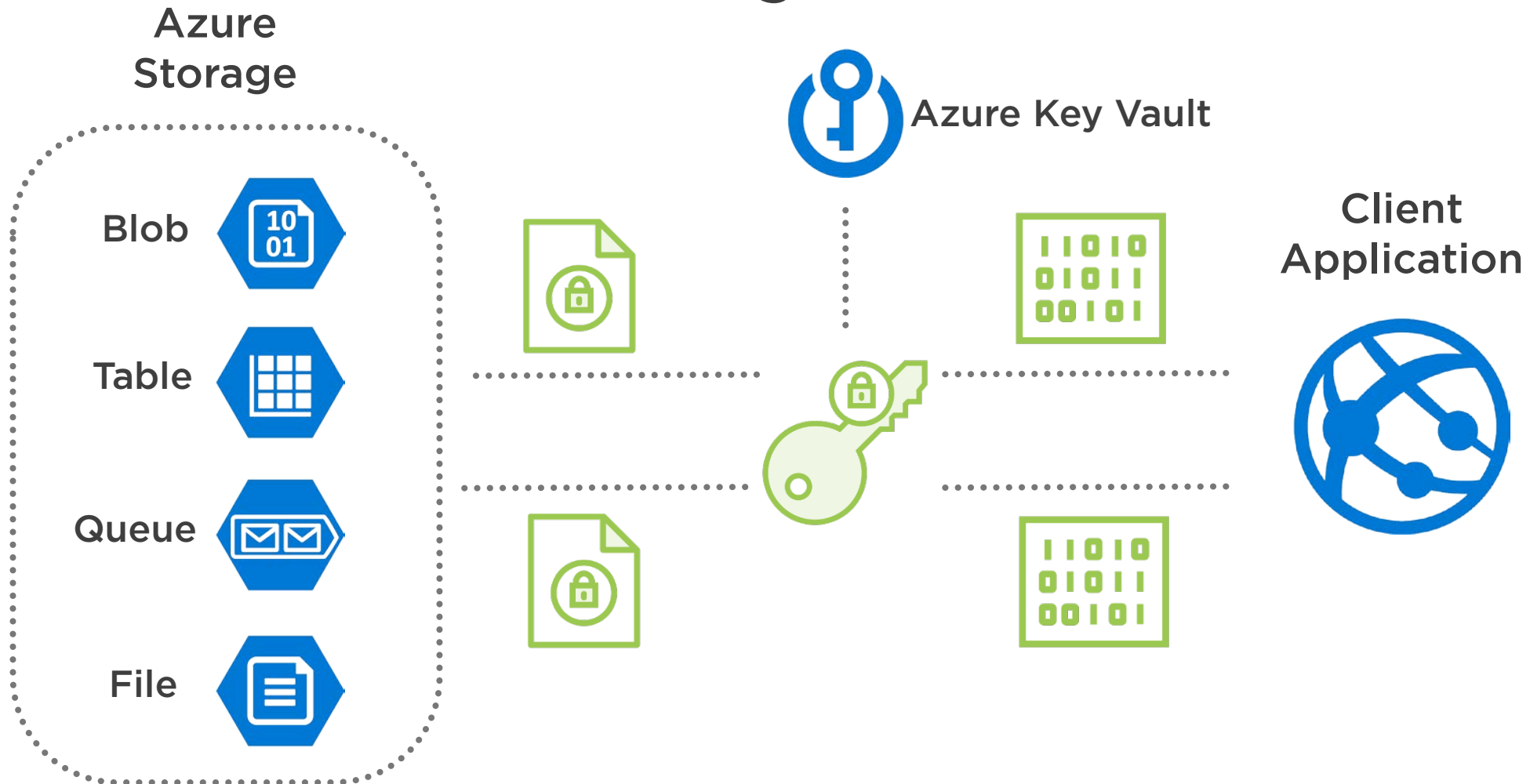
Azure storage platform is encrypted through *256-bit AES encryption*, one of the strongest block ciphers available



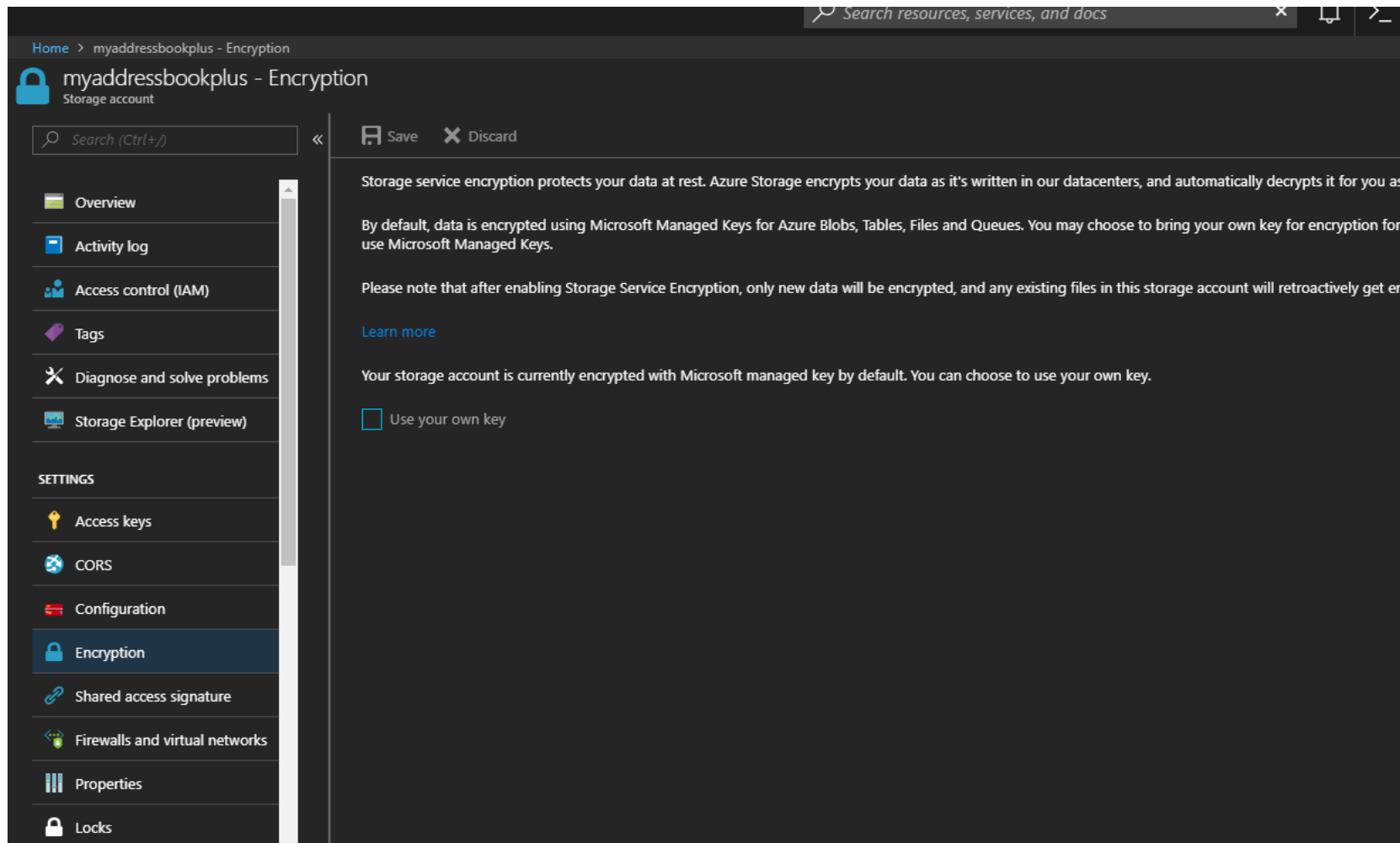
How Does Encryption for Data at Rest Work?



Customer-managed Keys (BYOK) for Storage Account



Customer-managed Keys (BYOK) for Storage Account



Customer-managed Keys (BYOK) for Storage Account

The screenshot shows the 'Encryption' settings page for a storage account named 'myaddressbookplus'. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Storage Explorer (preview), SETTINGS (Access keys, CORS, Configuration, Encryption, Shared access signature, Firewalls and virtual networks, Properties, Locks), and a search bar. The main content area has a 'Save' button and a 'Discard' button. It explains that Storage service encryption protects data at rest and that by default, data is encrypted using Microsoft Managed Keys. It notes that enabling Storage Service Encryption will retroactively encrypt existing files. The 'Use your own key' option is selected. Below this, there are two sections: 'Encryption key' with options 'Enter key URI' and 'Select from Key Vault' (selected), and 'Key Vault' with a link to 'Configure required settings'. A final note states that the storage account will be granted access to the selected key vault, with soft delete and purge protection enabled.

Home > myaddressbookplus - Encryption

myaddressbookplus - Encryption
Storage account

Search (Ctrl+/) << Save Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Encryption key

☐ Enter key URI

☒ Select from Key Vault

* Key Vault
[Configure required settings](#)

* Encryption key
[Configure required settings](#)

i The storage account named 'myaddressbookplus' will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and



Using Customer Managed Keys with SSE



The storage account and the key vault must be in the same region



Two key protection features, *Soft Delete* and *Do Not Purge*, must also be enabled. These settings ensure the keys cannot be accidentally or intentionally deleted



SSE is available for Azure Managed Disks with Microsoft-managed keys, but not with customer managed keys. In lieu of Managed Disks supporting SSE with customer-managed keys, *Microsoft* recommends Azure Disk Encryption



Demo



Configuring *MyAddressBook+* storage account to use customer-managed keys for encryption at rest




```
Set-AzureRmStorageAccount -ResourceGroupName  
$storageAccount.ResourceGroupName -AccountName  
$storageAccount.StorageAccountName -KeyvaultEncryption  
-KeyName $key.Name -KeyVersion $key.Version -KeyVaultUri  
$keyVault.VaultUri
```

Associate a Key with an Existing Storage



Azure Disk Encryption for Windows and Linux IaaS VMs



You Are Already Using Disk Encryption!

Windows

BitLocker Drive Encryption is a data protection feature that addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers

Linux

“dm-crypt is a transparent disk encryption subsystem in Linux kernel versions 2.6 and later.”

Wikipedia



“Azure Disk Encryption (ADE) is a capability that helps you encrypt your Windows and Linux IaaS virtual machine disks.”

Microsoft



Azure Disk Encryption for IaaS VMs

Defense in depth

Multiple layers of security defense

Not enabled by default

Should specifically get enabled

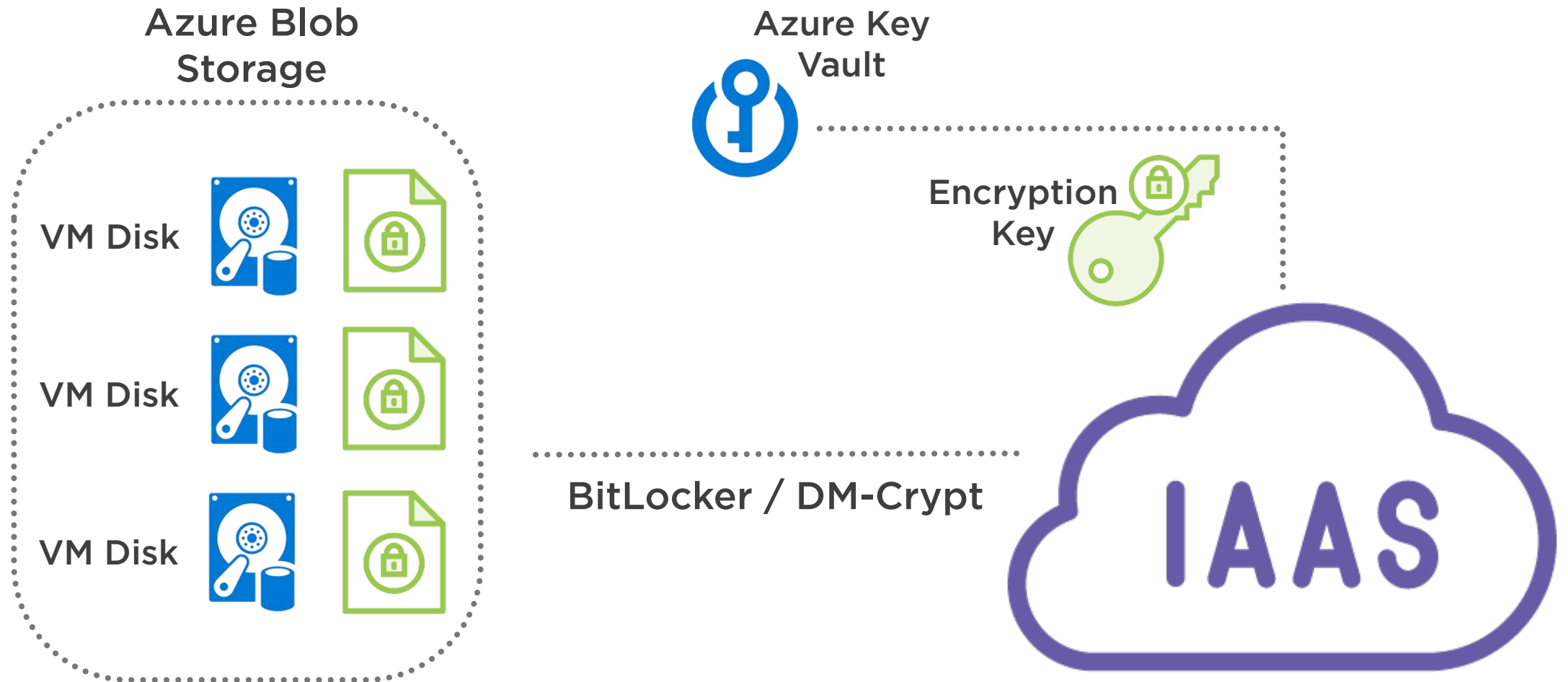
Azure Disk Encryption (ADE) helps you encrypt your IaaS virtual machine disks

ADE leverages *BitLocker* of Windows and the *DM-Crypt* of Linux

Is integrated with Azure Key Vault to help you manage the disk-encryption keys



How Does Azure Disk Encryption Work?



Demo



Create a new Windows VM

Configure Azure Disk Encryption for the VM

- Create an Azure Key Vault
- Store an encryption key in the vault
- Set the correct access to the key
- Enable encryption option on the VM using Azure PowerShell
- Verify that Disk Encryption is enabled

Disable the encryption



Encrypt a Running VM Using a Client Secret

```
Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName  
'MySecureGroupName' -VMName $vmName -AadClientID  
$aadClientID -AadClientSecret $aadClientSecret -  
DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -  
DiskEncryptionKeyVaultId $keyVaultResourceId;
```



Verify the Disks Are Encrypted

```
Get-AzureRmVmDiskEncryptionStatus -ResourceGroupName  
'MySecureGroupName' -VMName 'MySecureVMName'
```



Summary



Why Using Azure Storage Service Encryption for data at rest?

Customer-managed keys (BYOK) for Storage Account

Demo: Customer-managed keys (BYOK)

Azure Disk Encryption for IaaS Virtual Machines

Demo: Azure Disk Encryption

