Encrypting and Decrypting Data at Rest

Reza Salehi
MCT, MCSA(CLOUD PLATFORM), MCPD

@zaalion 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

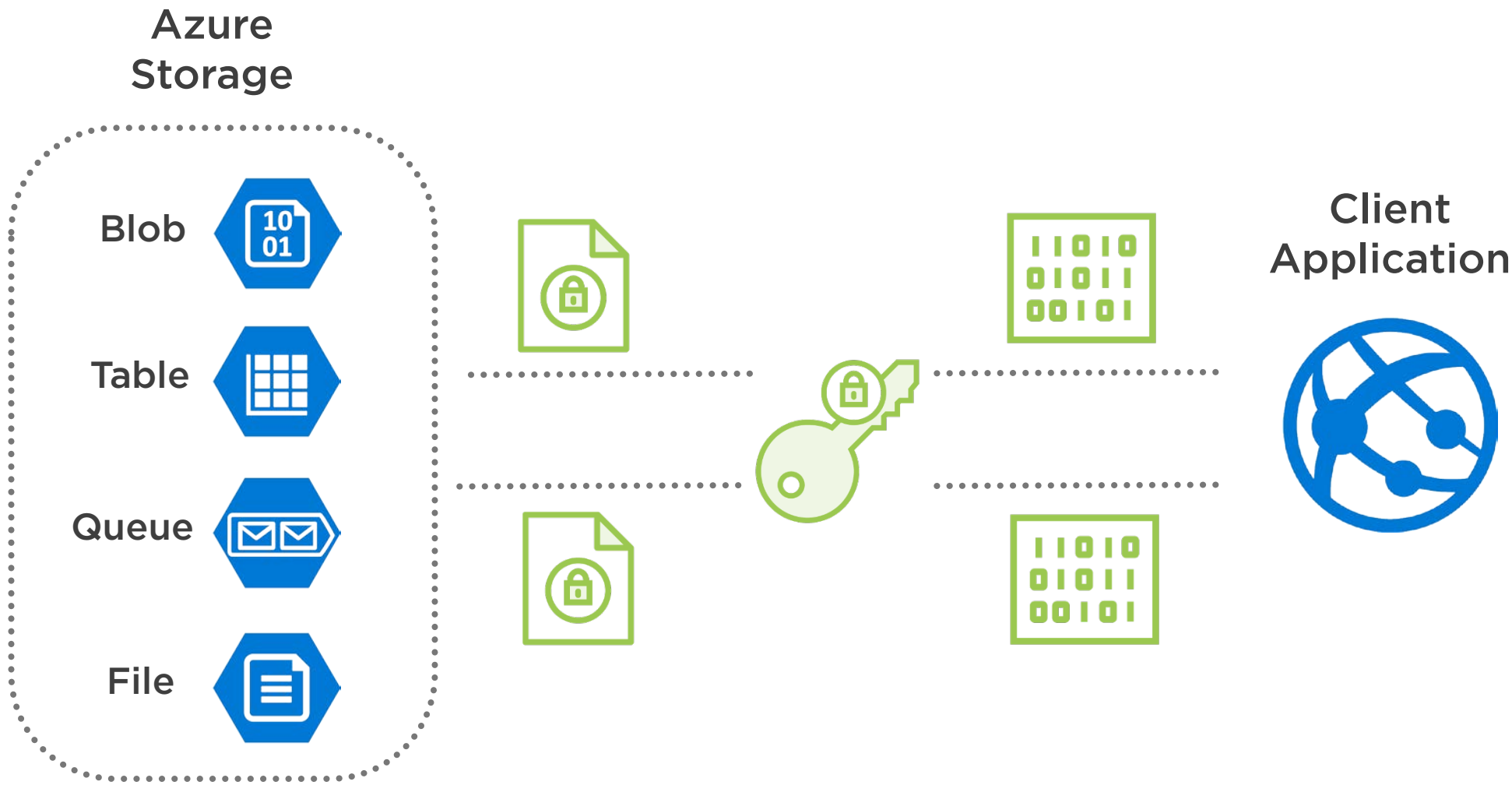
Storage Service Encryption (SSE) is enabled for all new and existing storage accounts and cannot be disabled

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

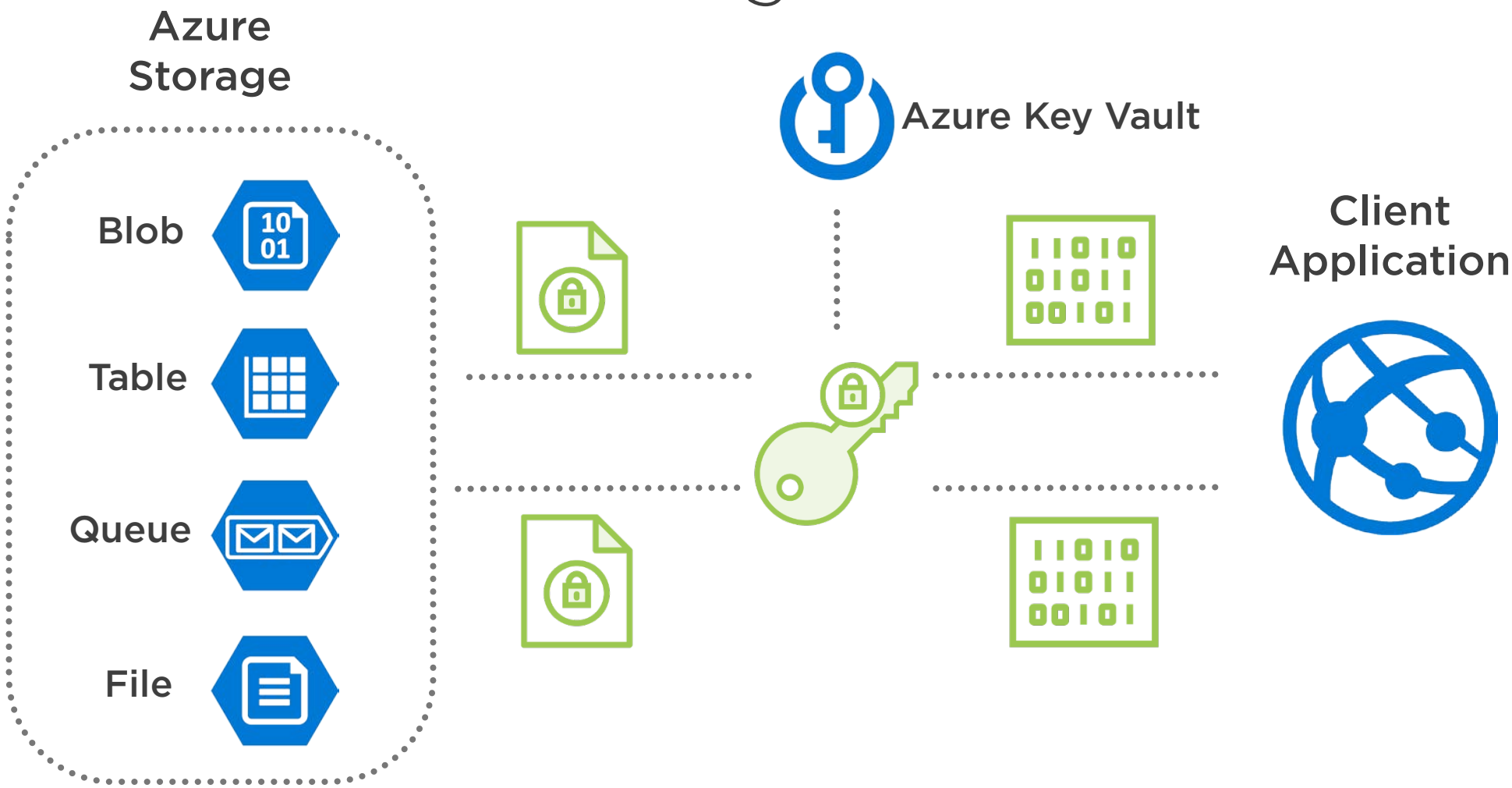
SSE automatically encrypts data in all performance tiers (Standard and Premium), all deployment models (Azure Resource Manager and Classic)

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

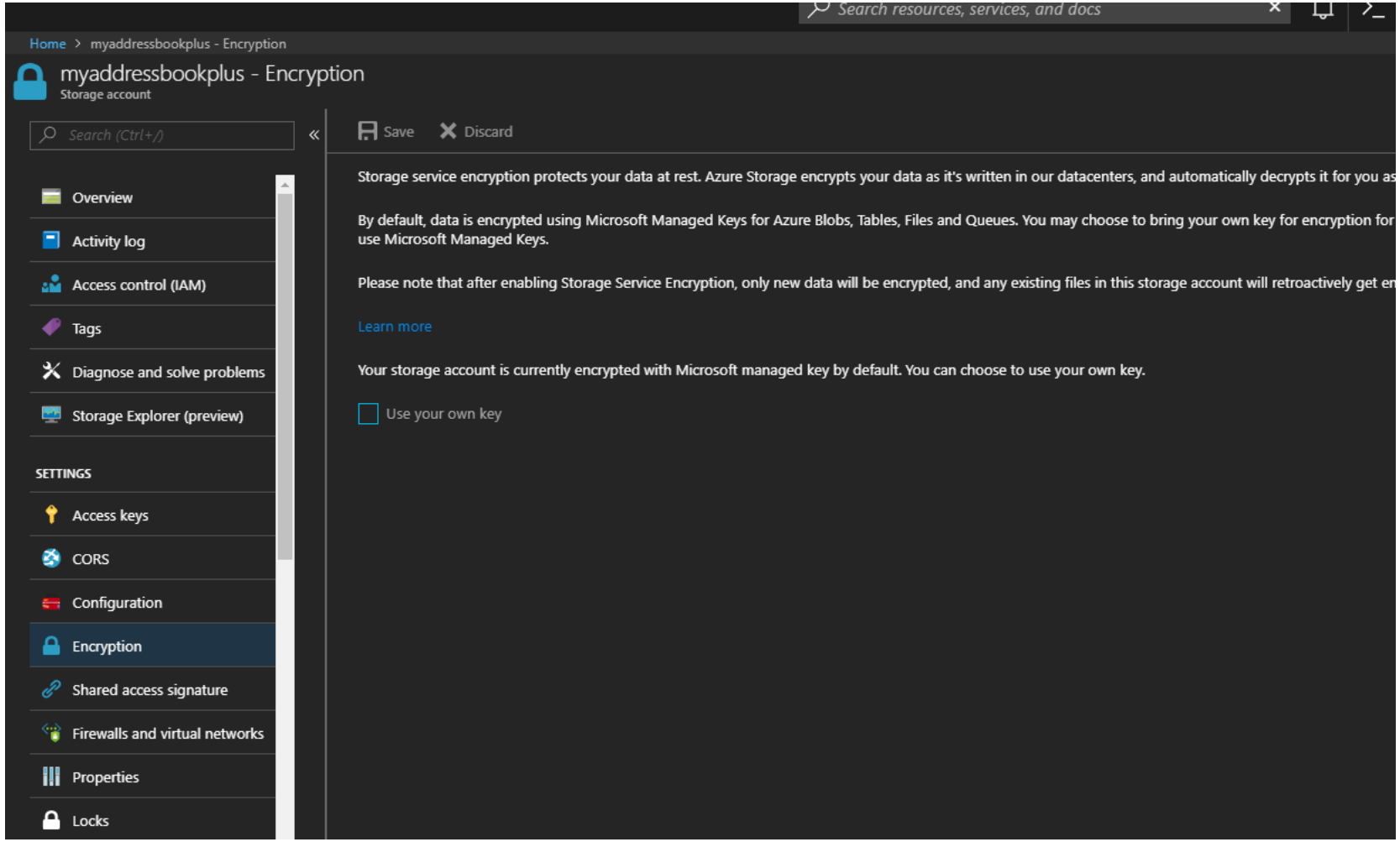
How Does Encryption for Data at Rest Work?



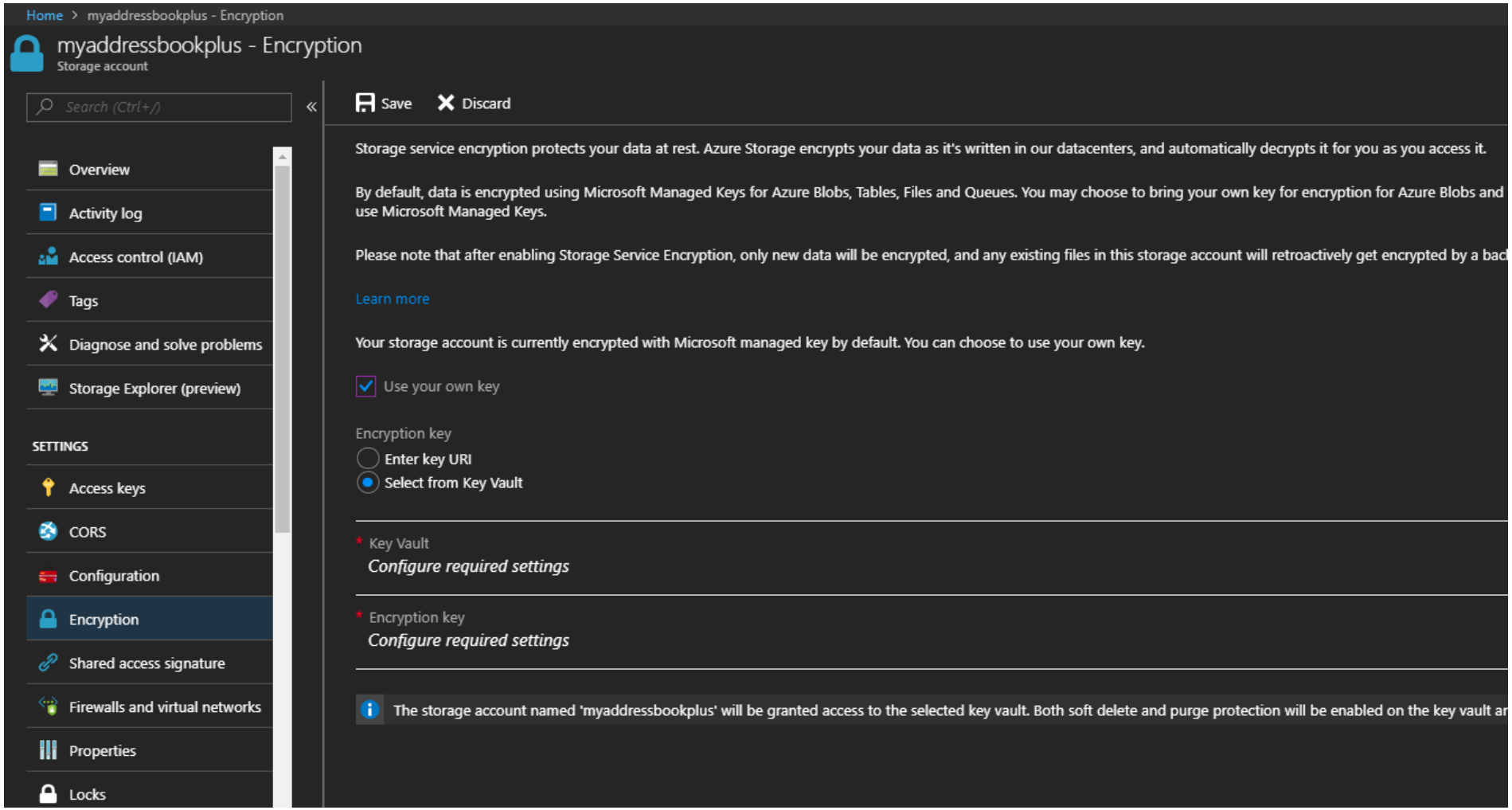
Customer-managed Keys (BYOK) for Storage Account



Customer-managed Keys (BYOK) for Storage Account



Customer-managed Keys (BYOK) for Storage Account



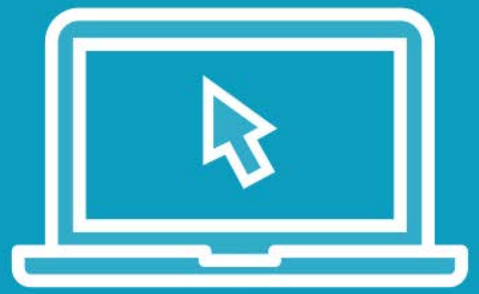
Using Customer Managed Keys with SSE

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

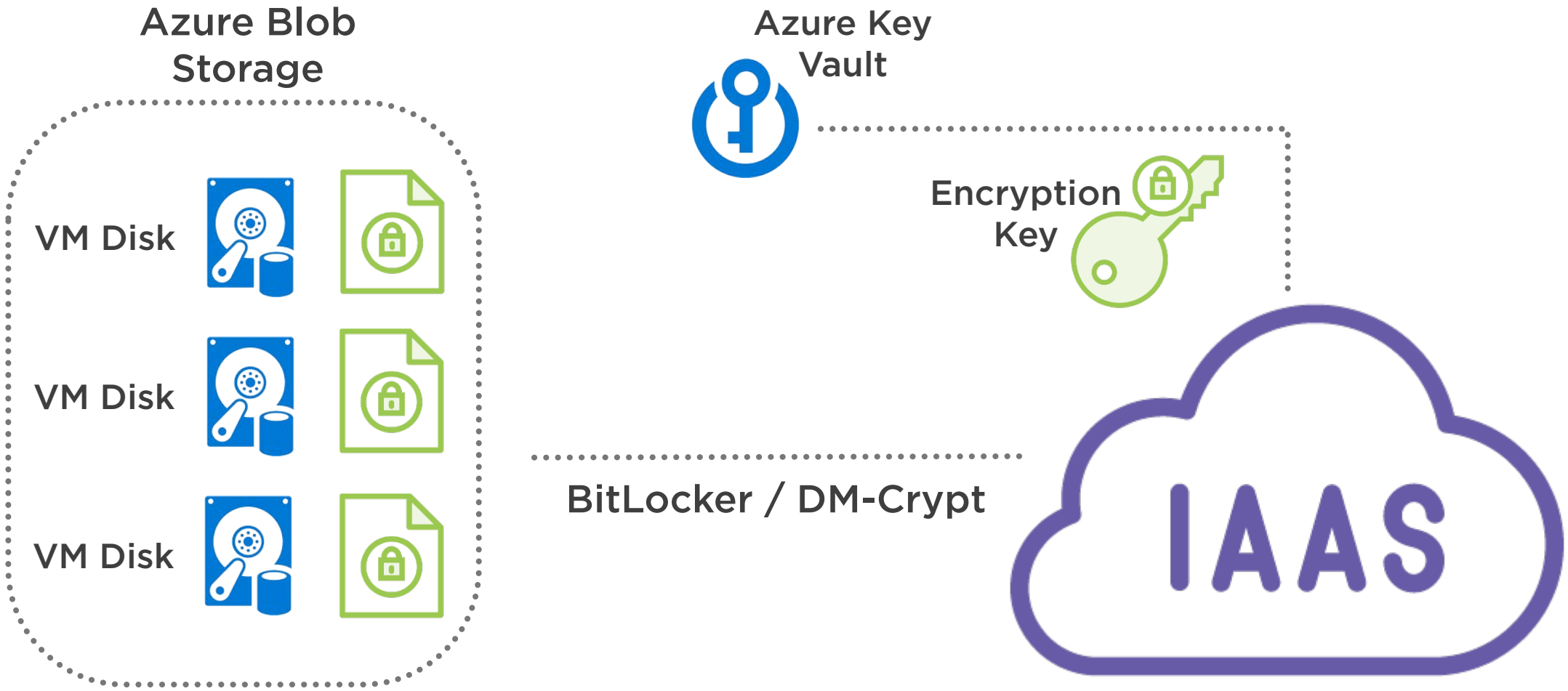
Should specifically get enabled

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

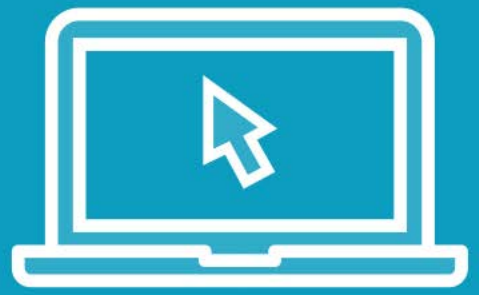
ADE leverages *BitLocker* of Windows and the *DM-Crypt* of Linux

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