Windows PowerShell Get-Help on Cmdlet 'Invoke-AzKeyVaultKeyOperation'

PS:\>Get-HELP Invoke-AzKeyVaultKeyOperation -Full

NAME

Invoke-AzKeyVaultKeyOperation

SYNOPSIS

Performs operation like "Encrypt", "Decrypt", "Wrap" or "Unwrap" using a specified key stored in a key vault or managed hsm.

SYNTAX

Invoke-AzKeyVaultKeyOperation [-HsmName] <System.String> [-Name] <System.String> -Algorithm <System.String> [-ByteArrayValue <System.Byte[]>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Operation <System.String> [-Version <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Invoke-AzKeyVaultKeyOperation [-InputObject] <Microsoft.Azure.Commands.KeyVault.Models.PSKeyVaultKeyIdentityItem> -Algorithm <System.String> [-ByteArrayValue <System.Byte[]>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Operation <System.String> [-Version

<System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Invoke-AzKeyVaultKeyOperation [-VaultName] <System.String> [-Name] <System.String> -Algorithm <System.String> [-ByteArrayValue <System.Byte[]>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Operation <System.String> [-Version <System.String>] [-Confirm] [-WhatIf]
[<CommonParameters>]

DESCRIPTION

Invoke-AzKeyVaultKeyOperation cmdlet supports 1. Encrypting an arbitrary sequence of bytes using an encryption key. 2. Decrypting a single block of encrypted data. 3.
Wrapping a symmetric key using a specified key. 4. Unwrapping a symmetric key using the specified key that was initially used for wrapping that key.

PARAMETERS

-Algorithm <System.String>

Algorithm identifier

Required? true
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-ByteArrayValue <System.Byte[]>

The value to be operated in byte array format.

Required? false
Position? named
Default value None
Accept pipeline input? False

Accept wildcard characters? false

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-HsmName <System.String>

HSM name.

Required? true

Position? 0

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.KeyVault.Models.PSKeyVaultKeyIdentityItem>

Key object

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Name <System.String>

Key name.

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Operation <System.String>

Algorithm identifier

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-VaultName <System.String>

Vault name.

Required? true

Position? 0

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Version <System.String>

Key version.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false
Position? named
Default value False
Accept pipeline input? False
Accept wildcard characters? false

-WhatIf <System.Management.Automation.SwitchParameter>
Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false
Position? named
Default value False
Accept pipeline input? False
Accept wildcard characters? false

<CommonParameters>
This cmdlet supports the common parameters: Verbose, Debug,
ErrorAction, ErrorVariable, WarningAction, WarningVariable,
OutBuffer, PipelineVariable, and OutVariable. For more information, see
about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

Microsoft.Azure.Commands.KeyVault.Models.PSKeyVaultKeyIdentityItem

OUTPUTS

Microsoft.Azure.Commands.KeyVault.Models.PSKeyOperationResult

NOTES

---- Example 1: Encrypts byte array using an encryption key ----

$byteArray = [Byte[]]@(58, 219)

$encryptedData = Invoke-AzKeyVaultKeyOperation -Operation Encrypt -Algorithm RSA1_5 -VaultName test-kv -Name test-key -ByteArrayValue $byteArray

$encryptedData

KeyId : https://bez-kv.vault.azure.net/keys/bez-key/c96ce0fb18de446c9f4b911b686988af

RawResult : {21, 39, 82, 56.}

Algorithm : RSA1_5

Encrypts `$byteArray` using test-key stored in test-kv.

---- Example 2: Decrypts byte array using an encryption key ----

$decryptedData = Invoke-AzKeyVaultKeyOperation -Operation Decrypt -Algorithm RSA1_5 -VaultName test-kv -Name test-key -ByteArrayValue $encryptedData.RawResult

$decryptedData

KeyId : https://bez-kv.vault.azure.net/keys/bez-key/c96ce0fb18de446c9f4b911b686988af

RawResult : {58, 219}

Algorithm : RSA1_5

Decrypts `$encryptedData.RawResult` using test-key stored in test-kv. The `$decryptedData.RawResult` is same with `$byteArray`, which is original data.

---- Example 3: Encrypts plain text using an encryption key ----

```
$plainText = "test"
$byteArray = [system.Text.Encoding]::UTF8.GetBytes($plainText)
 $encryptedData = Invoke-AzKeyVaultKeyOperation -Operation Encrypt -Algorithm RSA1_5 -VaultName test-kv -Name test-key -ByteArrayValue $byteArray
$encryptedData
```

```
KeyId     : https://test-kv.vault.azure.net/keys/test-key/bd8b77352a2443d4983bd70e9f660bc6
RawResult : {58, 219, 6, 236.}
Algorithm : RSA1_5
```

Encrypts string "test" using test-key stored in test-kv. The `RawResult` is the encrypted result in byte array format.

------- Example 4: Decrypt encrypted data to plain text -------

```
 $decryptedData = Invoke-AzKeyVaultKeyOperation -Operation Decrypt -Algorithm RSA1_5 -VaultName test-kv -Name test-key -ByteArrayValue $encryptedData.RawResult
$plainText = [system.Text.Encoding]::UTF8.GetString($decryptedData.RawResult)
$plainText
```

```
test
```

Decrypts encrypted data that is encrypted using test-key stored in test-kv. The `RawResult` is the decrypted result in byte array format.

---- Example 5: Wraps a symmetric key using a specified key ----

```
$key = "ovQIlbB0DgWhZA7sgkPxbg9H-Ly-VlNGPSgGrrZvlIo"
$byteArray = [system.Text.Encoding]::UTF8.GetBytes($key)
 $wrappedResult = Invoke-AzKeyVaultKeyOperation -Operation Wrap -Algorithm RSA1_5 -VaultName test-kv -Name
```

test-key -ByteArrayValue $byteArray

$wrappedResult | Format-List

KeyId : https://test-kv.vault.azure.net/keys/test-key/375cdf20252043b79c8ca0c57b6c7679

RawResult : {58, 219, 6, 236.}

Algorithm : RSA1_5

Wraps a symmetric key using key named test-key stored in test-kv. The `RawResult` is wrapped result in byte array format.

--- Example 6: Unwraps a symmetric key using a specified key ---

$unwrappedResult = Invoke-AzKeyVaultKeyOperation -Operation Unwrap -Algorithm RSA1_5 -VaultName test-kv -Name test-key -ByteArrayValue $wrappedResult.RawResult

$key = [system.Text.Encoding]::UTF8.GetString($unwrappedResult.RawResult)

$key

ovQIlbB0DgWhZA7sgkPxbg9H-Ly-VlNGPSgGrrZvlIo

Unwraps a symmetric key using a specified key test-key stored in test-kv. The `RawResult` is unwrapped result in byte array format.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.keyvault/invoke-azkeyvaultkeyoperation