Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Format-SecureBootUEFI'

PS C:\Users\wahid> Get-Help Format-SecureBootUEFI

NAME

Format-SecureBootUEFI

SYNOPSIS

Formats certificates or hashes into a content object that is returned and creates a file that is ready to be signed.

SYNTAX

Format-SecureBootUEFI -Algorithm {sha1 | sha256 | sha384 | sha512} [-AppendWrite] [-ContentFilePath <String>] -Hash <String[]> -Name {PK | KEK | db | dbx} [-SignableFilePath <String>] -SignatureOwner <Guid> [-Time <String>] [<CommonParameters>]

Format-SecureBootUEFI [-AppendWrite] -CertificateFilePath <String[]> [-ContentFilePath <String>] [-FormatWithCert] -Name {PK | KEK | db | dbx} [-SignableFilePath <String>] -SignatureOwner <Guid> [-Time <String>] [<CommonParameters>]

Format-SecureBootUEFI -Delete -Name {PK | KEK | db | dbx} [-SignableFilePath <String>] [-Time <String>] [<CommonParameters>]

DESCRIPTION

The Format-SecureBootUEFI cmdlet receives certificates or hashes as input and formats the input into a content object that is returned. The Set-SecureBootUEFI cmdlet uses this object to update the variable. If you specify a signable file, this cmdlet creates a file that has the specified name that has to be signed.

This cmdlet runs on both UEFI and BIOS (non-UEFI) computers.

PARAMETERS

-Algorithm <String>

Specifies which algorithm to use if this cmdlet is formatting hashes. The acceptable values for this parameter are: SHA1, SHA256, SHA384, and SHA512.

-AppendWrite [<SwitchParameter>]

Indicates that the contents of the current variable are appended instead of overwritten.

-CertificateFilePath <String[]>

Specifies one or more files that each contain a certificate that is used to generate the content object.

If you specify only the name, the file must be in the current working directory. Otherwise, specify the full path of the file.

-ContentFilePath <String>

Specifies the name of the file that is created and contains the information for the content object that is generated by this cmdlet.

-Delete [<SwitchParameter>]

Indicates that this cmdlet creates a content object and the appropriate sign-able file that deletes the variable.

-FormatWithCert [<SwitchParameter>]

Indicates whether the certificate will be stored or just the public key. If this parameter is set, the whole certificate is stored in the content object.

-Hash <String[]>

Specifies an array of hashes that are used to generate the content.

-Name <String>

Specifies the name of the UEFI environment variable. The acceptable values for this parameter are: PK, KEK, DB, and DBX.

-SignableFilePath <String>

Specifies the file that contains the contents of the data that is ready to be signed.

If only the name is specified, the file must be in the current working directory. Otherwise, specify the full path of the file.

-SignatureOwner <Guid>

Specifies the GUID of the signature owner.

-Time <String>

Specifies the timestamp that is used in the signature. Format this value as follows so that it is accepted as a DateTime object:

`"2011-11-01T13:30:00Z"`

<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).

---------- Example 1: Format a private key ----------

```
PS C:\> Format-SecureBootUefi -Name PK -SignatureOwner
12345678-1234-1234-1234-123456789abc -CertificateFilePath PK.cer
-SignableFilePath GeneratedFileToSign.bin -Time 2011-11-01T13:30:00Z |
Format-List
Name        : PK
Time        : 2011-11-01T13:30:00Z
AppendWrite : False
Content     : {232, 102, 87, 60...}
```

This command formats the private key in PK.cer that is later piped to the
Set-SecureBootUEFI cmdlet.

---------- Example 2: Format a hash ----------

```
PS C:\> Format-SecureBootUEFI -Name DBX -SignatureOwner
12345678-1234-1234-1234-123456789abc -Algorithm SHA256 -Hash
00112233445566778899001122334455667788990011223344556677889900 11
-SignableFilePath GeneratedFileToSign.bin -Time 2011-11-01T13:30:00Z
-AppendWrite | Format-List
Name        : dbx
Time        : 2011-11-01T13:30:00Z
AppendWrite : True
Content     : {18, 165, 108, 130...}
```

This command formats the hash to beg appended to the DBX UEFI variable when
the result is piped to the Set-SecureBootUEFI cmdlet.

-------- Example 3: Format for a variable to be deleted --------

PS C:\> Format-SecureBootUEFI -Name KEK -Delete -SignableFilePath

GeneratedFileToSign.bin -Time 2011-11-01T13:30:00Z | Format-List

Name : KEK

Time : 2011-11-01T13:30:00Z

AppendWrite : False

Content :

This command formats the KEK UEFI variable being deleted when the result is

piped into the Set-SecureBootUEFI cmdlet.

REMARKS

To see the examples, type: "get-help Format-SecureBootUEFI -examples".

For more information, type: "get-help Format-SecureBootUEFI -detailed".

For technical information, type: "get-help Format-SecureBootUEFI -full".

For online help, type: "get-help Format-SecureBootUEFI -online"