



Rocky Enterprise Linux 9.2 Manual Pages on command 'sbvarsign.1'

C:\>man sbvarsign.1

SBVARSIGN(1) User Commands SBVARSIGN(1)

NAME

sbvarsign - UEFI authenticated variable signing tool

SYNOPSIS

sbvarsign [options] --key <keyfile> --cert <certfile> <var-name> <var-data-file>

DESCRIPTION

Sign a blob of data for use in SetVariable().

OPTIONS

--engine <eng>

use the specified engine to load the key

--key <keyfile>

signing key (PEM-encoded RSA private key)

--cert <certfile>

certificate (x509 certificate)

--include-attrs

include attrs at beginning of output file

--guid <GUID>

EFI GUID for the variable. If omitted, EFI_IMAGE_SECURITY_DATABASE or EFI_GLOBAL_VARIABLE (depending on <var-name>) will be used.

--attr <attrs>

variable attributes. One or more of: NON_VOLATILE BOOTSERVICE_ACCESS RUN? TIME_ACCESS TIME_BASED_AUTHENTICATED_WRITE_ACCESS APPEND_WRITE

Separate multiple attrs with a comma,

default is all attributes, TIME_BASED_AUTH... is always included.

--output <file>

write signed data to <file> (default <var-data-file>.signed)

sbvarsign 0.9.2

March 2022

SBVARSIGN(1)