

NAME

efi-updatevar - tool for updating secure variables

SYNOPSIS

efi-updatevar: [-a] [-e] [-d <list>[-<entry>]] [-k <key>] [-g <guid>] [-b <file>|-f <file>|-c <file>] <var>

DESCRIPTION

Takes a variety of input files and adds them to one of the UEFI secure boot signature or key databases.

Note that the efivarfs filesystem must be mounted somewhere on the box and efi-updatevars must have the ability to write to the files (this usually means it must run as root).

Manipulate the UEFI key database via the efivarfs filesystem

OPTIONS

- a** append a value to the variable instead of replacing it
- e** use EFI Signature List instead of signed update (only works in Setup Mode)
- b** <binfile>
 Add hash of <binfile> to the signature list
- f** <file>
 Add or Replace the key file (.esl or .auth) to the <var>
- c** <file>
 Add or Replace the x509 certificate to the <var> (with <guid> if provided)
- g** <guid>
 Optional <guid> for the X509 Certificate
- k** <key>
 Secret key file for authorising User Mode updates
- d** <list>[-<entry>]
 Delete the signature list <list> (or just a single <entry> within the list)
- engine** <eng>
 Use engine <eng> for private key

EXAMPLES

Assuming you own your own platform key and have the PK.auth and noPK.auth files which go with it, you can programmatically move the system out of User Mode by doing

```
efi-updatevar -f noPK.auth PK
```

and put it back again with

```
efi-updatevar -f PK.auth PK
```

To add the hash of an efi binary bin.efi to db in Setup Mode do

```
efi-updatevar -b bin.efi db
```

And to append an EFI signature list append.esl to db in Setup Mode do

```
efi-updatevar -a -e append.esl db
```

To add your key (KEK.crt) to the Key Exchange Key in User Mode, assuming the private part of the platform key is in PK.key, do

```
efi-updatevar -a -c KEK.crt -k PK.key KEK
```

To add certificate DB.crt to db in User Mode assuming the private part of the Key Exchange Key (KEK) is in KEK.key do

```
efi-updatevar -a -c DB.crt -k KEK.key db
```

To replace the old platform key (PK) with a new one in newPK.crt in User Mode assuming the private part of the old platform key is in PK.key, do

```
efi-updatevar -c newPK.crt -k PK.key db
```

To delete the private key, tipping the platform from User Mode to Setup Mode, do

```
efi-updatevar -d 0 -k PK.key PK
```

And to put the private key back again (in Setup Mode) do

```
efi-updatevar -c PK.crt -k PK.key PK
```