NAME

efisecdb − utility for managing UEFI signature lists

SYNOPSIS

efisecdb [**−s** *SORT*] [**−i** *file* [**−i** *file*] ...]
[**−g** *guid* ⟨**−a** | **−r**⟩ ⟨[**−t** *hash-type*] **−h** *hash* | **−c** *file*⟩
[**−g** *guid* ⟨**−a** | **−r**⟩ ⟨[**−t** *hash-type*] **−h** *hash* | **−c** *file*⟩] ...] ⟨**−d** [**−A**] | **−o** *file* | **−L**⟩

DESCRIPTION

efisecdb is a command line utility for management of UEFI signature lists in detached files. That is, it's for command line generation and management of files in the format of KEK, DB, and DBX.

Operation occurs in three phases:

1. Loading of security databases specified with **−−input**
2. Left-to-right processing of other options, using **−−hash-type, −−owner-guid, −−add,** and **−−remove** as state to build selectors to add or remove hashes and certificates specified by **−−hash** and **−−certificate**.
3. Generation of output

The accumulated state is persistent; once an Owner GUID, Add or Delete operation, or hash type are specified, they need only be present again to change the operations that follow. Operations are added to the list to process when **−h** *hash* or **−c** *cert* are specified, and are processed in the order they appear. Additionally, at least one **−g** argument and either **−−add** or **−−remove** must appear before the first use of **−h** *hash* or **−c** *cert*.

OPTIONS

⟨**−s** | **−−sort**⟩ ⟨*all* | *data* | *none* | *type*⟩
Sort by data after sorting and grouping entry types, entry data, no sorting, or by entry type

⟨**−s** | **−−sort**⟩ ⟨*ascending* | *descending*⟩
Sort in ascending or descending order

−i *file* | **−−infile** *file*
Read EFI Security Database from *file*

−g *guid* | **−−owner-guid** *guid*
Use the specified GUID or symbolic refrence (i.e. {empty}) for forthcoming addition and removal operations

−a | **−−add** | **−r** | **−−remove**
Select *add* or *remove* for forthcoming operations

−t *hash-type* | **−−hash-type** *hash-type*
Select *hash-type* for forthcoming addition and removal operations (default *sha256*)

Use hash-type *help* to list supported hash types.

−h *hash* | **−−hash** *hash*
Add or remove the specified hash

−c *file* | **−−certificate** *file*
Add or remove the specified certificate

−d | **−−dump**
Produce a hex dump of the output

−A | **−−annotate**
Annotate the hex dump produced by **−−dump**

−o *file* | **−−outfile** *file*
Write EFI Security Database to *file*

−L | **−−list-guids**
List the well known guids

The output is tab delimited: GUID short_name desription

EXAMPLES

Dumping the current system's *DBX* database with annotations

```
host:~$ efisecdb -d -A -i /sys/firmware/efi/efivars/dbx-d719b2cb-3d3a-4596-a3bc-dad00e67656f
00000000  26 16 c4 c1 4c 50 92 40  ac a9 41 f9 36 93 43 28  |&...LP.@..A.6.C(|  esl[0].signature_type = {sha256}
00000010  60 00 00 00                                       |....|              esl[0].signature_list_size = 96
00000014              00 00 00 00                           |....|              esl[0].signature_header_size = 0
00000018                          30 00 00 00               |0...|              esl[0].signature_size = 48
0000001c                                                                       esl[0].signature_header (end:0x0000001c)
0000001c                                    bd 9a fa 77     |...w|  esl[0].signature[0].owner = {microsoft}
00000020  59 03 32 4d bd 60 28 f4  e7 8f 78 4b              |Y.2M.‘(...xK|
0000002c                                    fe cf b2 32     |...2|  esl[0].signature[0].data (end:0x0000004c)
00000030  d1 2e 99 4b 6d 48 5d 2c  71 67 72 8a a5 52 59 84  |...KmH],qgr..RY.|
00000040  ad 5c a6 1e 75 16 22 1f  07 9a 14 36              |...u."....6|
0000004c                                    bd 9a fa 77     |...w|  esl[0].signature[1].owner = {microsoft}
00000050  59 03 32 4d bd 60 28 f4  e7 8f 78 4b              |Y.2M.‘(...xK|
0000005c                                    fe 63 a8 4f     |.c.O|  esl[0].signature[1].data (end:0x0000007c)
00000060  78 2c c9 d3 fc f2 cc f9  fc 11 fb d0 37 60 87 87  |x,.........7‘..|
00000070  58 d2 62 85 ed 12 66 9b  dc 6e 6d 01              |X.b...f..nm.|
0000007c
```

Building a new EFI Security Database for use as *KEK*, replacing one certificate.

```
# Figure out the original cert... the easy way
host:~$ strings KEK-* | grep microsoft.*crt
Dhttp://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt0

# Find it, because --export isn't implemented yet
host:~$ wget \
    --user-agent='Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko' \
    http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt
--2020-06-04 20:41:27--  http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt
Resolving www.microsoft.com (www.microsoft.com)... 2600:141b:800:287::356e, 2600:141b:800:2a0::356e, 23.43.254.254
Connecting to www.microsoft.com (www.microsoft.com)|2600:141b:800:287::356e|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1539 (1.5K) [application/octet-stream]
Saving to: ‘MicCorThiParMarRoo_2010-10-05.crt’

MicCorThiParMarRoo_ 100%[===================>]   1.50K  --.-KB/s    in 0s

2020-06-04 20:41:27 (177 MB/s) - ‘MicCorThiParMarRoo_2010-10-05.crt’ saved [1539/1539]

# Pick a GUID-like object, any GUID-like object...
host:~$ uuidgen
aab3960c-501e-485e-ac59-62805970a3dd

# Remove the old KEK entry and add a different one
host:~$ efisecdb -i KEK-8be4df61-93ca-11d2-aa0d-00e098032b8c \
    -g {microsoft} -r -c MicCorThiParMarRoo_2010-10-05.crt \
    -g aab3960c-501e-485e-ac59-62805970a3dd -a -c pjkek.cer \
    -o newkek.bin
```

Searching

the list of well-known GUIDs

host:~$ **efisecdb -L | grep shim**

{605dab50-e046-4300-abb6-3dd810dd8b23} {shim} shim

STANDARDS

UEFI Specification Working Group, *Unified Extensible Firmware Interface (UEFI) Specification Version 2.8, Unified Extensible Firmware Interface Forum*, https://uefi.org/specifications , March 2019.

SEE ALSO

authvar(1), efikeygen(1), pesign(1)

AUTHORS

Peter Jones

BUGS

efisecdb is currently lacking several useful features:

- positional exporting of certificates
- **−−dump** and **−−annotate** do not adjust the output width for the terminal
- certificates can’t be specified for removal by their *ToBeSigned* hash