NAME

cert-to-efi-hash-list - tool for converting openssl certificates to EFI signature hash revocation lists

SYNOPSIS

cert-to-efi-hash-list [*-g <guid>*][*-t <timestamp>*][*-s <hash>*] *<crt file> <efi sig list file>*

DESCRIPTION

Take an input X509 certificate (in PEM format) and convert it to an EFI signature hash list file containing only that single certificate

OPTIONS

−g <guid>

Use <guid> as the owner of the signature. If this is not supplied, an all zero guid will be used

−s <hash>

Use SHA<hash> hash algorithm (256, 384, 512)

−t <timestamp>

Time of Revocation for hash signature

Set to 0 if not specified meaning revoke for all time.

NOTE

Signature revocation hashes are only implemented in UEFI 2.4 and up

EXAMPLES

To take a standard X509 certificate in PEM format and produce an output EFI signature list file, simply do

cert-to-efi-hash-list PK.crt PK.esl

Note that the format of EFI signature list files is such that they can simply be concatenated to produce a file with multiple signatures:

cat PK1.esl PK2.esl > PK.esl

If your platform has a setup mode key manipulation ability, the keys will often only be displayed by GUID, so using the -g option to give your keys recognisable GUIDs will be useful if you plan to manage lots of keys.

SEE ALSO

sign-efi-sig-list(1) for details on how to create an authenticated update to EFI secure variables when the EFI system is in user mode.