UEFI SECURE BOOT - WINDOWS 11 UND MONTEREY (DUALBOOT MIT OPENCORE) TEIL 2

Beitrag von „talkinghead“ vom 8. Oktober 2021, 18:14

Hier gehts zu Teil1 SECURE BOOT - WINDOWS 11 UND Monterey (DUALBOOT MIT OPENCORE) Teil 1

Variante2: Eigenes Zertifikat erstellen, im Bios einspielen und Bootloader damit signieren.

*****Achtung*** an dieser Stelle im Bios liegen voreingespielte Herstellerzertifikate. Ich übernehme keine Verantwortung dafür falls durch die folgenden Schritte Information gelöscht werden oder andere Betriebssysteme nicht mehr starten.**

Für diese Variante habe ich Informationen aus diesen Quellen verwendet

http://www.rodsbooks.com/efi-bootloaders/controlling-sb.html

https://github.com/dortania/Op…ecurity/uefisecureboot.md

In dieser Variante erstelle ich mir ein Zertifikat mit einer Laufzeit von 3650 Tagen.

openssl req -new -x509 -newkey rsa:2048 -subj "/CN=Your Secure Boot key set DB/" -keyout DB.key -out DB.crt -days 3650 -nodes -sha256

Wir erhalten zwei Dateien DB.key (privater Schlüssel) und DB.crt (öffentlicher Schlüssel)

Das Bios erwartet den öffentlichen Schlüssel im DER-Format, daher konvertieren wir die crt-Datei zusätzlich noch in eine der-Datei.

openssl x509 -outform der -in DB.crt -out DB.der

Jetzt haben wir drei Dateien: DB.key, DB.crt und DB.der

Der öffentliche Schlüssel im der-Format (der-datei) wird später im Bios in die Authorized Signature Database (db) eingespielt. Damit kann im Secure Boot Prozess überprüft werden, ob unsere selbssignierten Bootfiles mit unserem privaten Schlüssel (key-File) signiert wurde. Dazu kopieren wir die DER-Datei auf einen FAT-Formatieren USB Stick, den wir später für den Key-import in das Bios benötigen.

Signieren der OC-Dateien:

Für das Signieren der OC-Dateien orientiere ich mich am Inhalt von uefisecureboot.md (s.o.)

Legt euch einen leeren Ordner “secureboot”

In den Ordner secureboot kopiert ihr folgende Dateien:

- DB.key
- DB.crt
- BOOTx64.efi(aus EFI/BOOT/)
- OpenCore.efi(aus EFI/OC/)
- OpenRuntime.efi(aus EFI/OC/Drivers/)
- HfsPlus.efi (aus EFI/OC/Drivers/) wobei ich nicht sicher bin ob HfsPlus.efi signiert werden muss
- signed (Legt hier noch den Ordner “signed” an)

In der CLI wechselt in den Ordner secureboot und führt folgende Commands aus (sbsign solltet ihr irgendwo im Pfad halten)

sbsign --key DB.key --cert DB.crt --output signed/BOOTx64.efi BOOTx64.efi

sbsign --key DB.key --cert DB.crt --output signed/OpenCore.efi OpenCore.efi

sbsign --key DB.key --cert DB.crt --output signed/OpenRuntime.efi OpenRuntime.efi

sbsign --key DB.key --cert DB.crt --output signed/HfsPlus.efi.efi HfsPlus.efi

Anschließend solltet ihr im Ordner “signed” die 4 signierten EFIs finden.

Info: das sbsign-Tool wirft bei mir warnings aus. Prinzipiell besteht die Möglichkeit, dass die

Binaries einen Schaden haben. Ich habe aber bisher nichts negatives feststellen können. Mit den warnings werde ich mich später noch befassen.

Nachdem ihr die 4 OC Dateien signiert habt, solltet ihr ein Backup des EFI-Ordners anlegen und dann die signierten efi-Files an ihren Platz im EFI Ordner über die unsignierten Versionen kopieren.

Den Signiervorgang müsst ihr immer dann wiederholen, wenn ihr neue Binaries einspielt. Denkt auch an eure USB-EFI Boot Sticks (wobei man hier temporär Secure Boot deaktivieren kann).

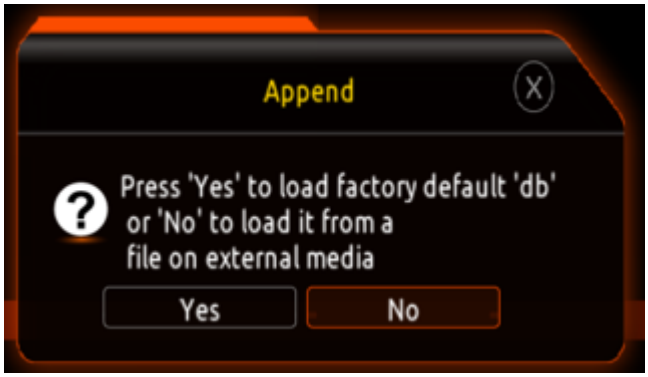
Falls ihr auch reFind benutzt, dann könnt ihr den auch mit sbsign signieren und in die reFind-EFI-Partition einspielen.

Nachdem nun die Binaries alle signiert sind, muss noch der öffentliche Schlüssel ins Bios rein.

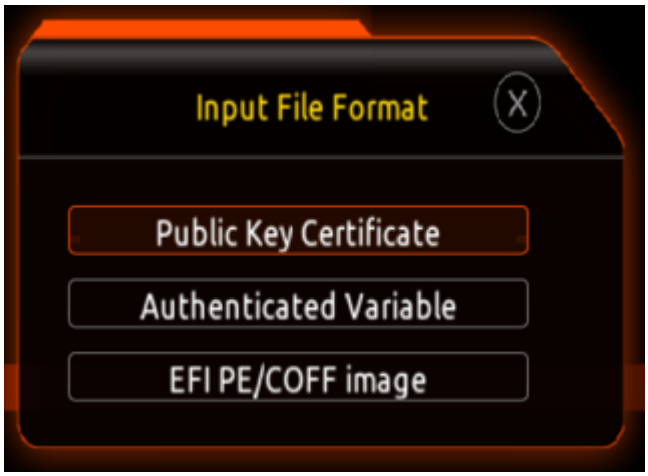
Einspielen von DER-Datei ins Bios:

Ins Bios gehen und USB Stick anstecken.

Im Bios -> *Boot -> Secure Boot -> Key Management -> Authorized Signatures -> Append -> "No" load it from a file -> DB.der -> Public Key Certificate -> Yes -> OK (Success).*


Append
Press 'Yes' to load factory default 'db'
or 'No' to load it from a
file on external media
Yes
No


Select File
<.Spotlight-V100>
<.fseventsd>
<.Trashes>
211008142116.BMP
211008142105.BMP
211008142054.BMP
DB.der
DB.pem
DB.key
DB.cer
DB.pfx
DB.crt


Input File Format
Public Key Certificate
Authenticated Variable
EFI PE/COFF image


Append
Confirm update of 'db' with content from the file DB.der
Yes
No

(Der Eintrag #3 ist mein oben erstellter Public Key)

Anschließend könnt ihr nochmals in Authorized Signatures gehen und über Details den Inhalt anzeigen. Ihr solltet nun zusätzlich euer Zertifikat sehen.

Info: Ich hatte durch das EFI Enrollment bereits zusätzliche Einträge in Authorized Keys und ein “Append” der DER-Datei war nicht auf Anhieb möglich. Ich musste dort erst alle meine hinzugefügten Hashes löschen, bevor “Append” möglich war.

Bevor ihr das Bios verlasst, schaltet Secure Boot ein und speichert beim Verlassen.

Wenn alles geklappt hat, könnt ihr OC booten und anschließend den Start von Windows testen.

Troubleshooting:

In meinen Tests lief alles rund. Es kann aber dennoch sein dass ich in der Doku oder ihr beim Durcharbeiten was übersehen habt.

- Prüft ob Secure Boot aktiviert ist
- Prüft ob ihr ohne Secure Boot booten könnt.
- Prüft ob im authorized Signatures euer Zertifikat drin ist
- Prüft ob ihr mit Enroll EFI Image und Secure Boot = on booten könnt
- Prüft, ob ihr die Binaries korrekt signiert habt.

(Bilder folgen)