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).

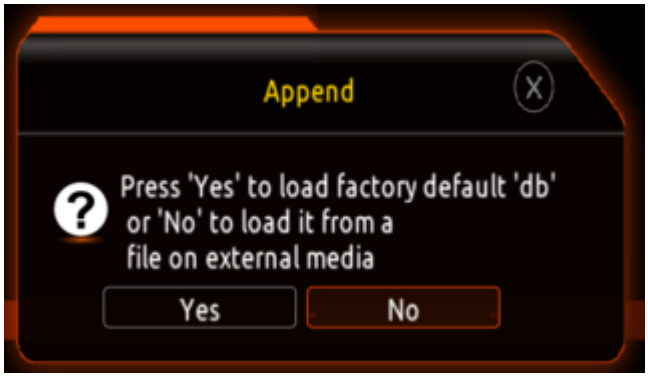
Falls ihr auch reFind benutzt, dann könnt ihr den auch mit sbsign signieren und in die reFind-EFI-Partition einspielen.

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

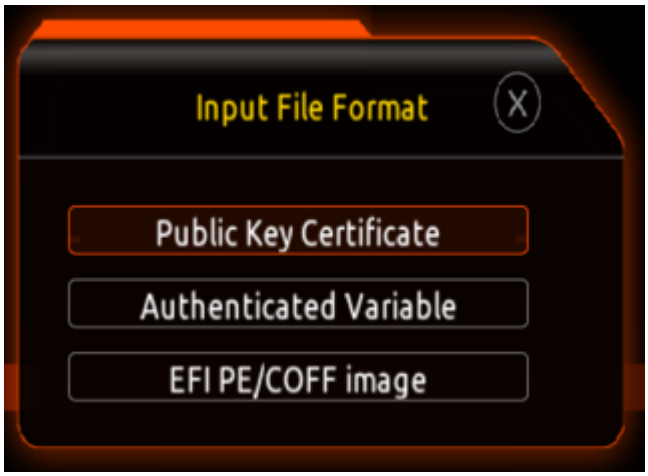
Einspielen von DER-Datei ins Bios:

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

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

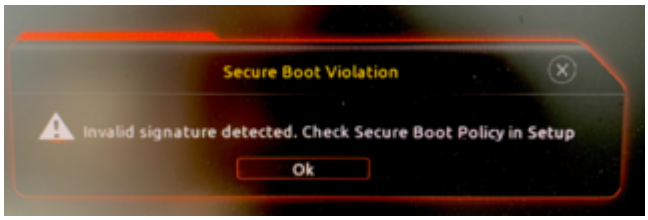
Anschließend könnt ihr nochmals in Authorized Signatures gehen und über Details den Inhalt anzeigen. Ihr solltet nun zusätzlich euer Zertifikat sehen.

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)

Beitrag von „PSI69“ vom 25. Oktober 2021, 13:01

@talkinghead

Mahlzeit! Liest sich gut - nur, wie / woher hast du die *sbsigntools/efitiools unter OS X zum Laufen bekommen / bezogen? Ich habe das hier <sbsigntools.git> gefunden, bekomme es aber nicht kompiliert...*

Danke Peter

Beitrag von „karacho“ vom 25. Oktober 2021, 13:55

PSI69 Mit Linux. Entweder auf einem Live-Linux vom USB Stick oder einem Linux in einer VM.

Beitrag von „PSI69“ vom 25. Oktober 2021, 14:12

karacho

Das wollte ich ja vermeiden. Ich habe jetzt hier etwas gefunden. Ist unter 11.6 benutzbar und erstellt geänderte/signierte Files. Ob die dann booten, werde ich sehen. Erst steht noch ein Firmware Update vom Board an, danach Secure Boot ein / Cert einspielen und dann schauen wir mal...

Gruß Peter

Beitrag von „talkinghead“ vom 25. Oktober 2021, 14:50

> Zitat von PSI69
>
> Mahlzeit! Liest sich gut - nur, wie / woher hast du die *sbsigntools/efitiools unter OS X zum Laufen bekommen / bezogen? Ich habe das hier <sbsigntools.git> gefunden, bekomme es aber nicht kompiliert...*
>
> *Danke Peter*

moment ..... Github Repo "sbsigingtools" kompilerbar unter macOS

Beitrag von „PSI69“ vom 25. Oktober 2021, 14:57

talkinghead

... 0.9.4 ist neuer als 0.6; ok. Danke,

Peter

Beitrag von „karacho“ vom 26. Oktober 2021, 08:10

talkinghead Dein Repo lässt sich hier leider nicht kompilieren. Bricht damit ab, dass libcrypto (aus openssl) nicht gefunden wird. Ist jedoch installiert, allerdings mit brew und nicht mit MacPorts.

Beitrag von „talkinghead“ vom 26. Oktober 2021, 09:01

Hmm...

bricht es bei ./configure ab?

configure versucht über pkg-config die benötigen Header/Libs zu finden.

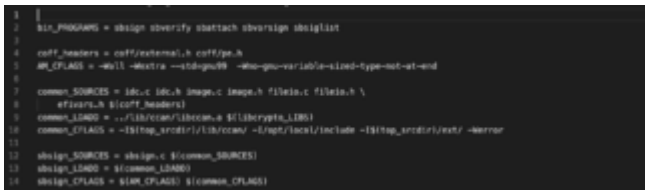
Gibt das mal ein... und prüfe den Output.

Code

1. sbsigntools-macOS % pkg-config --cflags libcrypto
2. -I/opt/local/libexec/openssl11/include
3.
4. sbsigntools-macOS % pkg-config --libs libcrypto
5. -L/opt/local/libexec/openssl11/lib -lcrypto

Falls du openssl-dev installiert hast, könntest du versuchen in src/Makefile.am -I/pfad_zu_openssl_Header rein bauen

In Zeile 10



Beitrag von „SchmockLord“ vom 26. Oktober 2021, 10:33

talkinghead Ich weiss nicht ob du das mitbekommen hast. Ich hab zum Thema SecureBoot mit OC neulich auch ein Video gemacht: https://youtu.be/c8JcuIQu9XY

Beitrag von „talkinghead“ vom 26. Oktober 2021, 10:37

SchmockLord : Danke für die Info. Sind in den 15.x min ein paar Worte zu sbsign bzw zum Kompilieren von sbsign mit drin? Den Rest bzgl Bios und Enrollment hab ich bereits verstanden.

Beitrag von „SchmockLord“ vom 26. Oktober 2021, 10:45

Ne, Fokus ist config.plist für SecureBoot einstellen. Enroll EFIs und BIOS Einstellungen. ApecID ermitteln.

Beitrag von „karacho“ vom 26. Oktober 2021, 13:06

> Zitat von talkinghead
>
> /opt/local/libexec/openssl11/

Und genau da liegt bei mir der Hund begraben. Das Paket 'openssl' wird von Homebrew nach /usr/local/Cellar/openssl installiert und ist 'keg-only'. D.h., dieses openssl wird jetzt Standardmäßig nur noch nach /usr/local/opt verlinkt und von dort aber nicht mehr weiter zu /usr/local/lib und /usr/local/include, weil Homebrew das LibreSSL von macOS den vorzug gibt und da nix ändert. Ein `> brew link openssl` wird daher nur mit einer Fehlermeldung quittiert.

Die nacheinander eingegebenen Befehle `export LDFLAGS="-L/usr/local/opt/openssl@3/lib"` , `export CPPFLAGS="-I/usr/local/opt/openssl@3/include"` und `export PKG_CONFIG_PATH="/usr/local/opt/openssl@3/lib/pkgconfig"` vor deinem ./configure Befehl brachte auch nix. ./configure lief zwar durch, aber make hat irgenwann wieder gemeckert und abgebrochen. Nun, lange Rede kurzer Sinn...hatte keinen Bock mehr der Ursache auf den Grund zu gehen und hab jetzt deine precompiled Binaries genommen

---

Beitrag von „juemue54“ vom 30. April 2022, 13:51

Hallo zusammen,

ich habe ein Thinkpad T450S und muste die Keys über das KeyTool ins UEFI einfügen. Das hat auch alles soweit funktioniert.

Sobald ich aber mit aktivierten SecureBoot booten will komme ich nichtmal in den Picker von OpenCore. Er bricht ab mit

Code

1. OC: Driver OpenRuntime.efi at 0 cannot be loaded - Invalid Parameter! Halting on critical error

Wenn ich die Reihenfolge der Treiber in der config.plist anpasse, bleibt es immer schon beim ersten hängen.

Sobald ich im UEFI SecureBoot wieder ausschalte, bootet er problemlos mit der identischen config.plist.

Habt ihr eine Idee?

Beitrag von „Michael1965“ vom 30. April 2023, 07:14

Hallo SchmockLord,

leider weiß ich nicht wie ich das anstellen soll mit meinem Asus Rog Strix Z490 e -Gaming Board.
Ich bekomme es einfach nicht hin.
Deine Anleitungen sind super, die mir auch schon geholfen haben, aber das mit dem Secure Boot und Key ist mir zu hoch.
Kannst du mir dabei helfen?

Gruß
Michael

Beitrag von „SchmockLord“ vom 30. April 2023, 10:25

Hallo Michael1965

Ich hab neulich noch ein Video gemacht, für ein Asus Board mit 13600k.

Am Ende siehst du die Einstellungen, die ich für Secure Boot vornehme.

FAST AND BEAUTIFUL. My newest Hackintosh Build. Asus AP201. 13600k. 6900XTH. - YouTube

Ich versuche es mal mit einfachen Worten zu erklären.

Secure Boot soll sicherstellen, dass dein Rechner nur von (dir) authorisierte Bootmanager/Betriebssysteme starten kann. Damit dir keiner ein Fremd-OS unterjubeln kann um dich z.B. auszuspionieren.

Das Key Management ist Teil von Secure Boot, quasi der Spicher der authorisierten Signaturen. Die Signaturen sind Checksummen von den Dateien, die du mit deiner persönlichen Signatur authorisiert hast.

Deswegen muss das auch jedes Mal neugemacht werden, wenn du OpenCore updatest und die .efi Dateien austauscht.

Du musst im Key Management jetzt die ganzen .efi Dateien bekanntmachen und whitelisten, die zu OpenCore gehören.

Im Asus BIOS:

Unter Boot in das SecureBoot Untermenü.

OS Type: Windows UEFI Mode

Secure Boot Mode: Custom

Dann ins Key Management.

Dort auf DB Management. Dann Append Key.

Bei der Frage ob es vom externen Medien importieren willst "No" (auch wenn sich das erstmal falsch anhört).

Dann kriegst du eine ganze Latte von Medien angezeigt. Hier musst du rausfinden, welcher davon dein Open Core Stick ist.

Dann musst du eine .efi nach der anderen mit Enter auswählen. Zwei Mal Enter drücken, dann sollte Success kommen.

Immer wenn Success kommt, hat er eine zusätzlich Signatur/Checksumme von der Datei in seinen Speicher der autorisierten Signaturen/Checksummen aufgenommen.

Das machst du mit jeder .efi Datei, die du in deinem OpenCore Stick hast und lädst.

Bei mir sind das:

Boot/Bootx64.efi

OC/OpenCore.efi

OC/Drivers/OpenRumtime.efi

OC/Drivers/OpenCanopy.efi

OC/Drivers/HFSPlus.efi

OC/Drivers/ResetNVRAM.efi

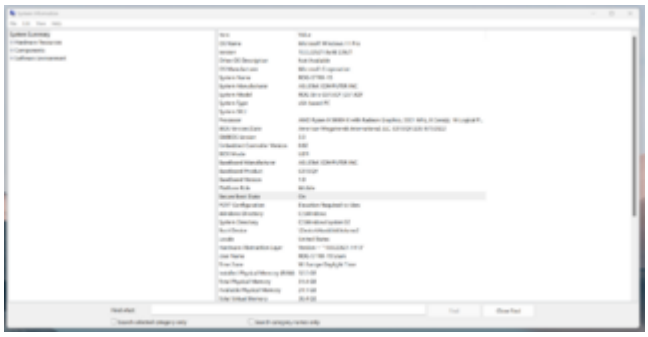
Danach speichern und BIOS verlassen. Und ab jetzt nur noch vom OC Stick booten. Windows und Mac. Ansonsten kommt Windows durcheinander.

Am besten den Windows Boot Manager auf Disabled setzen.

Prüfen kannst du das ganze, indem du in Windows, vom OC Stick gestartet, in die System Informationen gehst. Dort muss bei SecureBootState "on" stehen.

Und darauf gucken mittlerweile auch neue Spiele wahrscheinlich auch Fifa 23.

Manchmal braucht es auch erstmal 2-3 Neustarts bis das kommt.



Gruß,

Chris

Beitrag von „Michael1965“ vom 1. Mai 2023, 08:52

Guten Morgen @SchmockLord

ok ich verstehe. also kann ich nicht von der Festplatte aus Booten nur vom USB Stick.

Ich werde es ausprobieren.

Es funktioniert. Danke. Hatte auch dein Video angeschaut, hatte es auch so gemacht, nur wusste ich nicht das man alle EFIś so machen muss.

Ich muss mit vollem Respekt sagen, deine Videos sind echt super. Habe da einiges gelernt.

Gruß Michael

Beitrag von „SchmockLord“ vom 1. Mai 2023, 11:22

Super das freut mich. Auch für das Feedback zu den Videos!

Prinzipiell funktioniert das auch, wenn OpenCore auf der Festplatte liegt.

Aber ich rate den Leuten immer, OC auf einem Stick zu lassen. Wenn irgendwas ist und ihr kommt nicht mehr auf euer System, ist das blöd und macht die Sache unnötig komplizierter. So einen Stick kann man schnell mal abziehen, an einen anderen Rechner hängen und die OC config anpassen, bis es wieder funktioniert. Und es spielt bei der Dauer des Bootvorgangs auch keine Rolle, dass der Stick langsamer ist als interne SSDs.

Beitrag von „Michael1965“ vom 2. Mai 2023, 18:32

Hi Chris,

ich werde es auch von der interne Festplatte mal ausprobieren. Laut deine Aussage oben könnte es ja Probleme mit dem Windows Bootloader geben.

Wenn mal nichts funktioniert kann man ja den Key löschen neu installieren und nur Windows starten. Das geht, habe ich schon ausprobiert.

Ich habe mir mein Hackintosh Festplatte kopiert 1:1 für Reserve. Wenn die andere nicht mehr funktioniert sollte. Da ist nur das OS X drauf sonst nix.
Denn Rest kann ich immer noch nach installieren. Wenigstens weiß ich jetzt wie das funktioniert.

Nochmals vielen Dank

Gruß
Michael

Beitrag von „SchmockLord“ vom 3. Mai 2023, 10:00

Hallo Michael1965 ,

ich glaube du hast das mit den Keys noch nicht verstanden.

Du musst da keinen löschen um Windows neuzuinstallieren. Wenn du es so gemacht hast, wie ich gesagt habe, dann erweiterst du die Datenbank der authorisierten EFIs nur um die von OpenCore. Die von Windows werden weiter und immer authorisiert.

Und das mit dem Stick meine ich so: Meistens merken die Leute, dass sie mal wieder eine neue OC Version brauchen, wenn das nächste macOS Update nicht durchläuft. Und dann hast du den Salat. Kommst nicht mehr an die alte EFI ran um sie zu bearbeiten. Klar kannst du eine neue auf nen Stick packen. Aber viele checken dass dann nicht, von welcher jetzt eigentlich gebooted wird. Dann hast im schlimmsten Fall ein MIschmasch, dass das macOS Update mit der neuen config vom Stick startet und nach dem nächsten Restart wieder mit der alten internen.

Ich kanns nur raten. Aber ich seh in meinen Patreon Sessions und auch hier, wie viele Leute dadurch in Probleme kommen über die sie sich nie einen Kopf gemacht haben.

Nur weil jeder denkt es wäre nicht richtig, OC auf dem Stick zu lassen und der Bootvorgang wäre dadurch langsamer o.ä.

Und wenn du mich direkt anschreibst, pack mal ein SchmockLord davor. Sonst merk ich das nicht.

Gruß

Chris

Beitrag von „KungfuMarek“ vom 3. Mai 2023, 12:11

SchmockLord

Habe mal deinen Guide auf meinem Gigabyte Z690 Gaming X angewandt, ist an manchen Stellen etwas anders. Ist etwas komfortabeler gelöst. Habe das Prinzip aber verstanden und die .EFI Dateien gewhitelisted.

Klappte dann sofort mit dem Secureboot.

Danke für das super Video!

Beitrag von „Michael1965“ vom 3. Mai 2023, 18:29

Hallo @SchmockLord

ich habe es verstanden.

Was ich meine ist, wenn es Probleme geben sollte kann man das alles neu machen.

Aber eine andere frage.

Wenn ich Windows starte dann kommt die richtige Uhrzeit. Starte ich Mac OS dann auch.

Wenn ich dann wieder Windows starte ist die Uhrzeit 2 Stunden zurück.

Habe mehrere Zeit Server benutzt auch die Fritzbox.

Es passiert immer das gleiche. Wenn ich Mac OS starte ist alles ok, wenn ich Windows starte ist die Uhrzeit 2 Stunde zurück.

Habe im Bios nachgeschaut. Jedes mal nach dem Mac Os gelaufen ist, ist auch im Bios die Uhrzeit um 2 Stunden zurück.

Wie kann das passieren?

Gruß
Michael

Beitrag von „Nightflyer“ vom 3. Mai 2023, 18:39

Zum Uhrzeit Problem gibt es einen Wiki Eintrag

Uhrzeit Synchronisieren mit Windows und macOS

Beitrag von „Michael1965“ vom 6. Mai 2023, 05:20

Hallo @Nightflyer,

danke das hat geholfen.

Vielen Dank.

Gruß Michael