UEFI SECURE BOOT - WINDOWS 11 UND Monterey (DUALBOOT MIT OPENCORE) Teil 1

Beitrag von „talkinghead“ vom 8. Oktober 2021, 18:12

Danke a1k0n für den Hinweis bzgl der (UEFI) Secure Boot Thematik. Die Behebung hat mich dann doch sehr interessiert und es ist ein längerer Guide herausgekommen.

Ich hab den Text offline geschrieben und paste den hier einfach mal rein. Screenshots habe ich griffbereit und die werde ich nach und nach einpflegen.

Die Screenshots und die Anleitung fürs Bios basieren auf meinem Gigabyte Z390 Aorus Pro; BiosVer F12l.

UEFI Secure Boot und Dual Boot OC-macOS/Windows 10/11

Worum geht es _nicht_ in dem Guide:

In diesem Guide geht es nicht um die wirksame Absicherung des Bootvorgangs mittels UEFI Secure Boot. Eine umfängliche Betrachtung sprengt den Rahmen dieses Guides.

Worum geht es in dem Guide:

In diesem Guide geht es darum, eine Mindestanforderungen “(UEFI) Secure Boot” für Windows 11 zu aktivieren und die dadurch entstehenden Auswirkungen, dass anschließend nicht-signierte EFIs nicht mehr gestartet werden können, zu beheben.

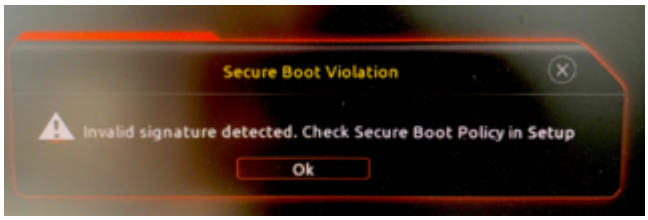
Ich selbst habe noch kein Windows 11, sondern bin in der Vorbereitung in Bezug auf die aktuellen Win11 Mindestvoraussetzungen (TPM, Secure Boot).

Es gibt unterschiedliche Meinungen dazu, ob für den Betrieb von Win11, Features wie TPM oder Secure Boot nur vorhanden oder auch (dauerhaft) aktiviert sein müssen.

Ich stütze mich hier ausschließlich auf meine Beobachtungen auf meiner Plattform und die sind, dass Windows Update erst _nach_ der Aktivierung von TPM und Secure Boot meldet, dass

meine Plattform die Mindestvoraussetzungen für Win11 erfüllt, während der Windows 11 Kompatibiltätschecker bereits ohne Aktivierung von Secure Boot die Readyness bestätigte.

Meine Beobachtung ist auch, dass auf meiner Plattform ein im Bios aktiviertes (UEFI) Secure Boot dazu führt, dass unsignierte oder einer vom Bios nicht per Public Key überprüfbaren Signatur versehenen Bootloader mit folgender Meldung (erwartungsgemäß) blockiert werden:



Um also Windows 11 via Windows Update bekommen zu können, fehlte mir zuletzt noch die Aktivierung von Secure Boot im Bios, jedoch mit dem Seiteneffekt dass dann reFind und OC und somit macOS nicht mehr startbar waren.

Warum kann trotz aktivem Secure Boot Win10/11 starten und warum startet reFind bzw OC nicht?

Weil Microsoft den Windows Bootloader digital signiert und mein Mainboardhersteller den passenden Public Key zur Validierung auf meinem Board im Bios hinterlegt hat.

Mein reFind und OC Bootloader ist aktuell nicht digital signiert. Daher schlägt Secure Boot wegen fehlender digitaler Signatur fehl.

Das Ziel des Lösungswegs ist somit klar: die unsignierten Bootloader benötigen eine digitale Signatur und diese digitale Signatur muss über die im Bios hinterlegten Public Keys validiert werden können.

Ich möchte hier 2 Wege vorstellen:

1. Enroll EFI Image
   Vorteil: Das geht ad-hoc aus dem Bios
   Nachteil: geänderte EFIs (OC-Update) müssen jedesmal neu Enrollt werden. Es sammeln sich ggfs alte Enrollments im Bios
2. Signieren mit eigenem Zertifikat
   Vorteil: Man kann während des OC Updateprozesses die relevanten EFIs per sbsign signieren und muss das nicht im Bios nachpflegen.

Nachteil: Man benötigt extra Tools wie sbsign und openssl. Man muss die Zertifikate erstellen und sicher verwahren.

Beide Verfahren können auch kombiniert werden. Sollte man bei einem Update das signieren per sbsign vergessen haben, kann man über Enroll EFI Image das temporär nachholen und später wieder herauslöschen.

Die zwei Verfahren habe ich selbst ausprobiert und unten dokumentiert.

Variante1: Enroll EFI Image über das Gigabyte Bios

Zuerst habe habe mich für den am einfachsten zu realisierenden Lösungsweg entschieden, in dem ich die im Gigabyte Bios eingebaute Funktion zur Validierung von EFIs nutze.

Das Bios meines Gigabyte Z390 Aorus Pro Boards hat eine Funktion eingebaut, mit der man ad-hoc EFIs für Secure Boot validieren kann.

Grob funktioniert das so, dass über das Bios in einem Dialog mountbare (FAT) Partitionen angezeigt werden. Durch diese kann man zur einer EFI navigieren und diese dann für die Validierung auswählen. Die für die Validierung nötigen Informationen werden dabei im Bios hinterlegt. Anschließend lässt sich ein so validiertes EFI auch mit Secure Boot starten.

Da ich keine Veränderung an den validierten EFIs via shasum feststellen konnte, gehe ich davon aus, dass der Validierungsprozess einen digitalen Fingerabdruck des EFIs erstellt und diesen im Bios hinzufügt. Tatsächlich wird sha256 als Signaturtyp benutzt und im Gigabyte Bios unter Authorized Signatures eingetragen.

Das Hinzufügen individueller digitaler Fingerabdrücke ins Bios führt mich direkt zur Frage, wie viele kann man da hinterlegen, kann man Alte löschen? Hierauf habe ich für mich noch keine konkrete Antwort, ausser dass das Gigabyte Bios eine Funktion bietet, den Validierungsstore zu resetten bzw einzelne oder alle Authorized Signatures zu löschen. Das habe ich aber noch nicht ausprobiert und kann noch keine Aussage zu den Auswirkungen treffen.

Vorbereitung:

Im Bios werden die Disks in einer Reihenfolge auflistet, die wahrscheinlich den SATA Ports entspricht.

Um auf Nummer Sicher zu gehen, könnte man vorab die EFI-Partitionen mit einem Dummy-Ordner “SignME” kennzeichnen.

WIchtig:

Macht euch Screenshots vom Bios im Bereich Secure Boot. Im Gigabyte Bios kann man das mit F12 machen. Steckt dazu einen Fat-formatierten USB Stick ein drückt F12. Der Screenshot landet auf dem USB Stick.

Macht euch Screenshots von den Inhalten der einzelnen Secure Boot Variablen Platform Key(PK), Key Exchange Keys und Authorized Signatures - jeweils reingehen und auf Details klicken und dann Screenshot, damit ihr Anhaltspunkte habt das vorher drin war und was ihr hinzugefügt habt.

Schritt 1:

Ins Bios gehen und Secure Boot aktivieren und Bios Änderungen Speichern. Achtet darauf dass "Secure Boot Mode" auf Custom steht, damit KeyManagement zugänglich ist.

Optional: das Bios an dieser Stelle nach dem Speichern verlassen und ersten Test durchführen: Windows sollte weiterhin booten können. OC-macOS jedoch nicht.

Schritt 2: OC Validieren

Damit OC Secure Boot klappt müsst ihr mind diese .efi validieren:

BOOT/Bootx64.efi

OC/OpenCore.efi

OC/Drivers/OpenRuntime.efi

(Die anderen EFIs in Drives habe ich nicht validiert. Falls ich diese punktuell brauche , werde ich temporär Secure Boot ausschalten.)

-> Im Bios zu Key Management gehen und dort Enroll EFI Image auswählen

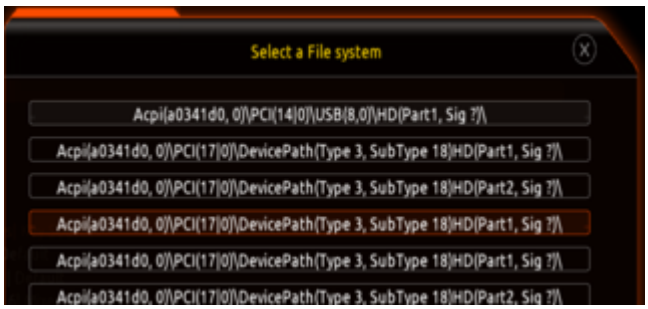
-> In der Liste der Filesystems eure Disk und Partition mit OC auswählen und nacheinander die Dateien

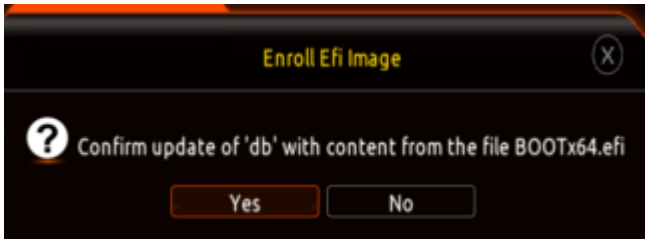
BOOT/Bootx64.efi

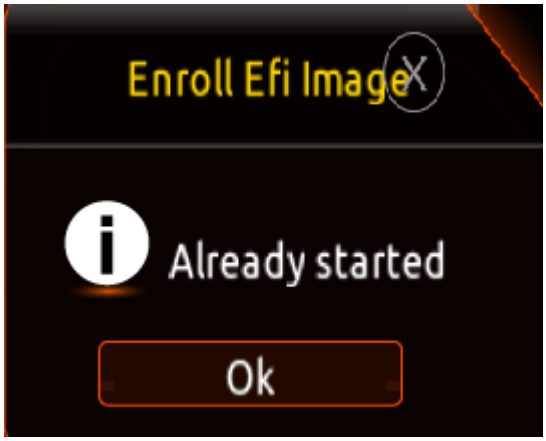
OC/OpenCore.efi

OC/Drivers/OpenRuntime.efi

validieren







(Hier steht normalerweise "! Success". Bei mir steht "Already started", weil ich den Loader erneut Enrollt hab und bereits ein Eintrag in der DB ist)

Schritt 3: Bios Änderungen Speichern, verlassen und neu starten

Jetzt solltet ihr Windows on OC-macOS booten können.

Optionale Schritte: Löschen von alten Signaturen

In Authorized Signatures kann man über "Delete -> No" einzelne Signaturen wieder löschen.

Achtet bei Delete und andern Aktivitäten immer genau auf den Text im Yes - No Dialog.

Troubleshooting:

Solltet ihr o.g. Meldung erhalten, solltet ihr prüfen, ob ihr das korrekte EFI Enrollt habt.

Bei OC müsst ihr daran denken, dass da mehrere EFIs enrollt werden müssen.

Alternativ könnt ihr UEFI Secure Boot im Bios erst mal wieder deaktivieren.

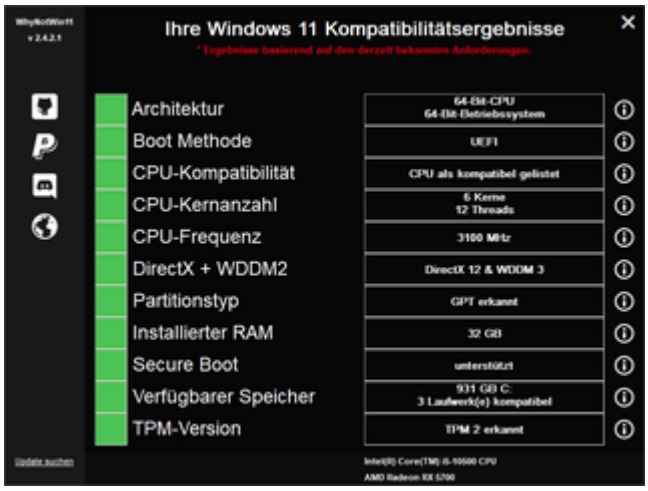
Teil 2 folgt hier SECURE BOOT - WINDOWS 11 UND MONTEREY (DUALBOOT MIT OPENCORE) TEIL 2

Beitrag von „julian91“ vom 8. Oktober 2021, 18:41

Coole Anleitung,

allerdings muss ich sagen das ich Secureboot und TPM 2.0 anhabe , keine EFI signiert habe und trotzdem sauber booten kann inkl Windows 11 (von dem ich grade schreibe) also irgendwas ist hier dann doch faul oder ?

selbst whynotwin11 sagt das alles aktiv ist O.o



Beitrag von „greecedrummer“ vom 8. Oktober 2021, 18:50

Bestätige dass ich auf meinem Z590 Vision G mit Bios F5 ohne gewurschtel, auch SecureBootMode enabled und TPM 2.0 aktive auf WIN11, macOS 11/12 ohne Probleme switchen kann!

Benutze OpenCore 0.7.5 nightly.

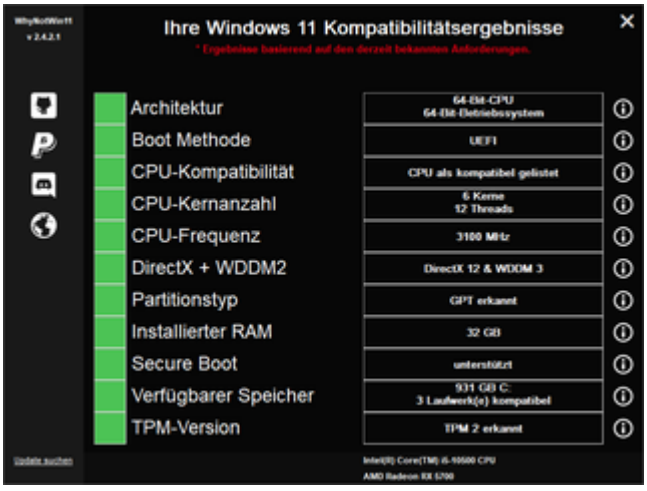
Versuchsweise auch Linux, klappt alles super

Beitrag von „a1k0n“ vom 8. Oktober 2021, 22:31

Beim 2. Lösungsweg würde ich noch anmerken das OpenCore.efi und Bootx64.efi erst signiert werden müssen mit den eignen Zertifikaten bevor man sie nochmal signiert mit sig.command im Falle man nutzt zusätzlich Apple Secure Boot mit Vault -> Secure in der config.plist. Ansonsten lässt es sich nicht booten weil OpenCore Fehler ausspuckt. Ansonsten super Anleitung

---

Beitrag von „talkinghead“ vom 9. Oktober 2021, 10:19

> Zitat von julian91
>
> Coole Anleitung,
>
> allerdings muss ich sagen das ich Secureboot und TPM 2.0 anhabe , keine EFI signiert habe und trotzdem sauber booten kann inkl Windows 11 (von dem ich grade schreibe) also irgendwas ist hier dann doch faul oder ?
>
> selbst whynotwin11 sagt das alles aktiv ist O.o
>
> 
>
>
> Alles anzeigen

Vielleicht reden wir von 2 verschiedenen "Secure Boot":

Es gibt "UEFI Secure Boot" und es gibt "Apple Secure Boot".

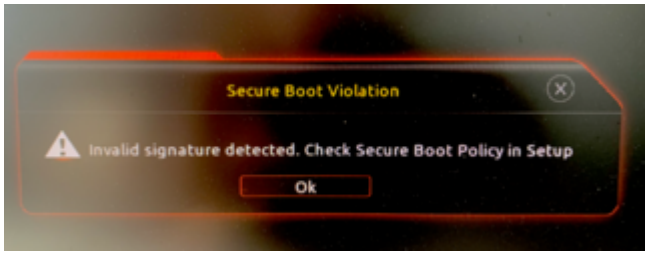
Ich beziehe mich auf UEFI Secure Boot.

Meinen Beobachtungen nach, verhält sich UEFI Secure Boot bei mir genau so wie ich es erwarte:

Ist UEFI Secure Boot im Bios aktiviert, kann ich nur diejenigen Bootloader starten die signiert oder Enrollt sind.

Mein OC und reFind sind jetzt mit einem eigenen Zertifikat signiert.

Wenn UEFI Secure Boot an ist und ich den öffentlichen Schlüssel meines Zertifikat aus dem DB-Store im Bios entferne, erscheint eine BIOS-Meldung "Invalid signature detected. Check Secure Boot Policy in Setup". Das ist genau das was ich auch erwarte, dass UEFI Secure Boot -wenn an- unerlaubte EFIs blockiert.



Wenn ich dann _meinen_ Public Key wieder in den Bios DB Store einfüge, kann ich die vorher blockierten EFIs starten. Genau so wie es zu erwarten ist.

Wie schon erwähnt: das hat nichts mit Apple Secure Boot und OC/config.plist zu tun. Das ist _vor_ dem Laden von OC.

Beitrag von „julian91“ vom 9. Oktober 2021, 16:01

Ich rede auch von UEFI Secure Boot.

sonst würde das W11 tool auch nicht grün ausschlagen das secureboot aktiv wäre

---

Beitrag von „xrabit“ vom 9. Oktober 2021, 16:19

whynotwin11 sagt bei dir nicht, dass secure boot aktiviert ist. Es wird nur geprüft, ob die Hardware secure boot unterstützt. Ich hab mein System auch ohne aktiviertes secure boot von 10 auf 11 upgraden können und bei dem Check wurde mir das auch grün angezeigt. Habe das gerade testweise auch noch mal bei whynotwin11 gemacht (mit deaktiviertem secure boot) und da ist auch alles grün bei mir. Ich denke deswegen kam die Frage auf, ob wirklich secure boot aktiv ist, weil das das Tool eben nicht anzeigt.

Beitrag von „julian91“ vom 9. Oktober 2021, 16:41

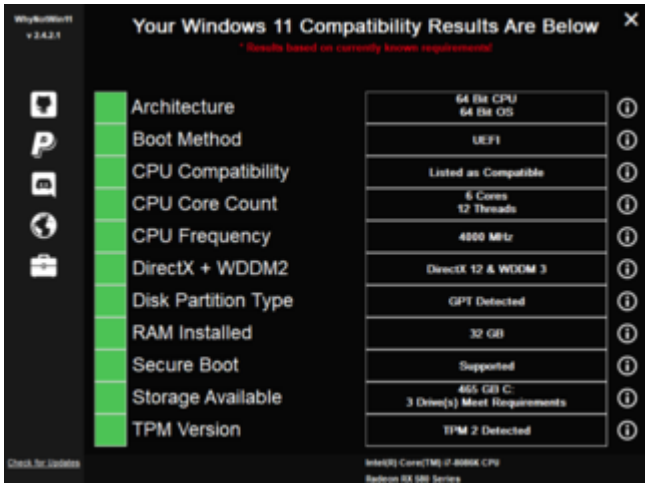
xrabit

komisch bei mir zeigt whynotw11 rot an wenn secureboot aus ist.

und auf nem technik DC wo ich aktiv bin haben wir viele fälle wo secureboot aus ist und das toll auch rot wirft.

Beitrag von „xrabit“ vom 9. Oktober 2021, 16:44

Okay dann ist das echt seltsam, so sieht das bei mir nämlich mit deaktiviertem Secure Boot aus



Beitrag von „julian91“ vom 9. Oktober 2021, 16:48

Ich bin grade maximal verwirrt ... ich bin 100% sicher das SB eingeschaltet war !

grade extra ins bios geschaut und es war wieder aus ... eingeschaltet und bekomme das signatur problem

---

Beitrag von „talkinghead“ vom 9. Oktober 2021, 16:49

julian91 : Wenn UEFI Secure Boot bei dir an ist und dennoch unlinierte Bootloader durchlässt, dann hast du glücklicherweise keinen Handlungsbedarf. Passt ja. Es muss ja UEFI Secure Boot nicht auf jedem Board richtig funktionieren und unsignierte Loader blocken. Hauptsache die Betriebssysteme starten.

Beitrag von „MPC561“ vom 9. Oktober 2021, 16:52

Auf meinem B460M DS3H auch von Gigabyte verhält es sich wie bei talkinghead wenn ich Secure Boot und TPM aktiviere.

Aktiviere ich es nicht zeigt mir der Win11 Update Checker an das ich TPM nicht aktiviert habe und nicht updaten kann, aktiviere ich es ist der Win11 Update Checker grün aber ich komm nicht mehr in den OC Bootmanager.

Am besten klingt es aktuell das im Bios zu "enrollen". Da ich mich mit dem Thema Sec Boot/TPM/Signieren noch nicht intensiv beschäftigt habe noch ein paar Fragen:

- Wenn ich OC im Bios "enrolle" sagtest du ich muss die irgendwie auswählen. Das bedeutet ich muss meinen Rettungsstick auch da reinbekommen?

- Was ist das Kriterium das ich einen neuen Enroll brauche? Eine geänderte bootx64.efi oder schon die änderung der confif.plist oder eine kextupdate?

Gruss,

Joerg

Beitrag von „julian91“ vom 9. Oktober 2021, 16:58

talkinghead

xrabit

So , nachdem ich SB eingeschaltet hatte war sense ...

allerdings bietet auch ASRock im Bios die Möglichkeit zu signieren ...

allerdings musste ich hier ALLE .efi files signieren damit er sauber OC Bootet , war in meinem Fall die Boot64 , opencore.efi , hfsplus.efi und openruntime.efi...

aber jetzt ist secureboot an und ich kann per OC booten, nice 

Die Anleitung hat mir jedenfalls den weg in die richtige richtung in meinem bios gegeben

---

Beitrag von „talkinghead“ vom 9. Oktober 2021, 16:58

MPC561 :

Bzgl. Rettungsstick: Theoretisch müsste es so klappen, dass Du die *.efis auf der Bootpartition enrollst und dann genau diese *.efis auf den Rettungsstick kopierst, weil dann diese *.efis die identische Hash (sha256) haben, wie die auf der Platte. Das müsste gehen. Vielleicht kannst du das ausprobieren und hier posten.

Neu enrollen musst du nur dann, wenn einer der entrollten Binaries sich ändert. Config etc zählt nicht mit.

Beitrag von „julian91“ vom 9. Oktober 2021, 17:04

und hier auch der "beweiß" das es aktiv ist

Beitrag von „xrabit“ vom 9. Oktober 2021, 17:10

Hauptsache es funktioniert werde das morgen auch mal nach der Anleitung hier machen. Da ich auch ein ASRock Board wie julian91 habe, sollte ich die Option mit dem Enroll ja hoffentlich auch haben

---

Beitrag von „karacho“ vom 9. Oktober 2021, 18:46

Ein Freund von mir, daniel14513 hier im Board , dem ich heute Nachmittag per WhatsApp Video geholfen habe das UEFI SecureBoot einzurichten, hat auch ein Z370er MB von ASUS. Diese haben wohl diesen Menüpunkt 'Enroll EFI' im Bios, was das ganze sehr vereinfacht. Mein MB, bzw. das Bios, hat diese Auswahl leider nicht. Daher bleibt denen die es nicht im Bios haben nur der Weg, die *.efi Boot Dateien per sbsign unter Linux zu signieren. ALLE Startdateien, die in der config.plist unter UEFI->Drivers eingetragen sind (und dito die BOOTx64.efi in /EFI/BOOT und die OpenCore.efi in /EFI/OC), müssen signiert werden, sonst stockt OC beim starten. Das hatten wir heute, weil wir vergaßen die HfsPlus.efi zu signieren. Erst danach startete OC durch.

Beitrag von „a1k0n“ vom 9. Oktober 2021, 18:57

Wer Enroll EFI im Bios hat brauch natürlich nichts signieren und kann sich glücklich schätzen. Auf dem Laptop würde da zusätzlich ein Biospasswort sinn machen. (zwecks verloren gehen)

Beitrag von „karacho“ vom 9. Oktober 2021, 19:20

> Zitat von a1k0n
>
> (zwecks verloren gehen)

Oder abhanden ~~gekommen~~ geworden 

Beitrag von „Gordon-1979“ vom 14. März 2022, 19:00

@talkinghead

habe es getestet und funktioniert.

Dabei habe ich herausgefunden, das Schritt 1:

> Zitat
>
> **Schritt 1:**
>
> Ins Bios gehen und Secure Boot aktivieren und Bios Änderungen Speichern. Achtet darauf dass "Secure Boot Mode" auf Custom steht, damit KeyManagement zugänglich ist.

Nicht verändert werden darf auf Default, dann funktioniert es nicht mehr.

Danke für die Anleitung. Genial!!!!!! 

Beitrag von „CilentCipha“ vom 11. August 2022, 10:53

Hallo,

ich habe auch das Gigabyte z390 Pro und gerade auf Win 11 upgegradet. Secure Boot ist noch deaktiviert ich müsste es aber für eine Kundensoftware aktivieren. Verstehe ich es richtig, dass man dann bei jedem OC Update immer alles neu signieren muss?

Das ist mir ehrlich gesagt zu heikel. Das System läuft seit Jahren 100% zuverlässig und das klingt nach einer potentiellen Fehlerquelle. Dann organisiere ich mir lieber einen zusätzlichen Win11 Laptop.

Oder ist meine Sorge da unbegründet?

Danke für eure Einschätzung

Beitrag von „julian91“ vom 11. August 2022, 11:07

ja musst du da sich die EFI files ändern.
hab damit aber bisher noch keine probleme gehabt. läuft sauber und stabil

---

Beitrag von „CilentCipha“ vom 11. August 2022, 15:24

Danke, ich hab es mal riskiert und hat direlt funktioniert. Danke für die tolle Anleitung!

Beitrag von „shane52“ vom 21. November 2022, 20:30

Hallo Leute

Ich bekomme die Methode 1 mit dem eingeben im **Enroll EFI nicht hin (siehe Anhang)**

Ich habe ein Gigabyte Z590 Aorus Pro Ax mit Bios Version F9A und möchte Ventura

installieren.

Habe das BIOS schon neu Geflasht aber keine Änderung.

Könnt ihr vielleicht schritt für schritt zeigen was man wo eingeben muss.

Ich bekomme kein oc Bootmenü mehr habe Warscheinlich was falsch eingegben oder gelöscht.

Bin in Enroll EFI in EFI / OC / Drivers / OpenRuntime.efi und enter (siehe Bilder)

aber das ist bestimmt falsch ☹

Beitrag von „a1k0n“ vom 22. November 2022, 10:45

In deiner config.plist wurde HfsPlus.efi angegeben in deinem Drivers Ordner liegt aber die OpenHfsPlus.efi

Das ist das Problem 🙂

Beitrag von „shane52“ vom 23. November 2022, 10:30

Oh ja Du hast recht Danke für den Tipp.

Ich hatte die Treiber mit dem Oc Configurator eingetragen und nicht mehr kontrolliert.

Dann kann ich jetzt die Eintragung in Enroll EFI so eintragen wie auf meinen Bildern oder werden die von Hand eingetragen?

Beitrag von „kuko“ vom 23. November 2022, 13:33

Frage: Bei mir funktioniert das "Enroll EFI Image" im BIOS nicht - findet nichts. Gibt es weitere Voraussetzungen dafür? Z.B. Name der EFI Partition? Habe diese auf meinen Festplatten umbenannt, um sie besser auseinander halten zu können (-> also nicht "EFI").

Habe: Mainboard MSI MAG Z590 Torpedo mit neusten BIOS v7D08vA8

Beitrag von „talkinghead“ vom 23. November 2022, 17:06

Wenn du EFI umbenannt hast, könnte das der Grund sein, warum du die Partition nicht findest.

Beitrag von „a1k0n“ vom 23. November 2022, 18:38

shane52

Je nach dem. Die config.plist Angabe muss mit der Datei in Drivers übereinstimmen. Ob du HFSPlus.efi oder OpenHFSPlus.efi nimmst ist dabei Jacke wie Hose. OpenCore.efi nicht vergessen mit anzugeben im Bios.

Beitrag von „Erdenwind Inc.“ vom 23. November 2022, 20:11

Warum so umständlich? Efi Ordner auf OSX Platte und im Bios drauf booten und fertig

---

Beitrag von „a1k0n“ vom 23. November 2022, 22:04

Bei aktivierten Secure Boot kommt man nicht weit mit EFI Ordner einfach auf OSX Platte kopieren.

Beitrag von „iPhoneTruth“ vom 25. Januar 2023, 17:34

> Zitat von talkinghead
>
> Ich möchte hier 2 Wege vorstellen:
>
> 1. Enroll EFI Image
> …
> 2. Signieren mit eigenem Zertifikat

Sehe ich das richtig, daß die Anleitung zum zweiten Weg, dem Signieren mit eigenem Zertifikat, noch fehlt und auch im anderen verlinkten Beitrag "

SECURE BOOT - WINDOWS 11 UND BIG SUR (DUALBOOT MIT OPENCORE)" nicht zu finden ist? Kommt das noch oder kann jemand dafür auch einen Guide schreiben für diejenigen, bei denen der erste Weg nicht geht?

Beitrag von „talkinghead“ vom 25. Januar 2023, 18:53

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

Beitrag von „G.com“ vom 22. August 2023, 00:04

Moin,

ich hoffe ich darf mich hier mal anhängen. Bei mir funktioniert das Enroll nicht. Es kommt immer die Nachricht fail.

Ist das ein bekannter Fehler? Was mache ich da falsch?

Danke für Eure Tips.

Gruß

g.com

Beitrag von „byebye123“ vom 28. Dezember 2023, 21:14

Für MSI Board User aber auch generell ist ganz einfach:

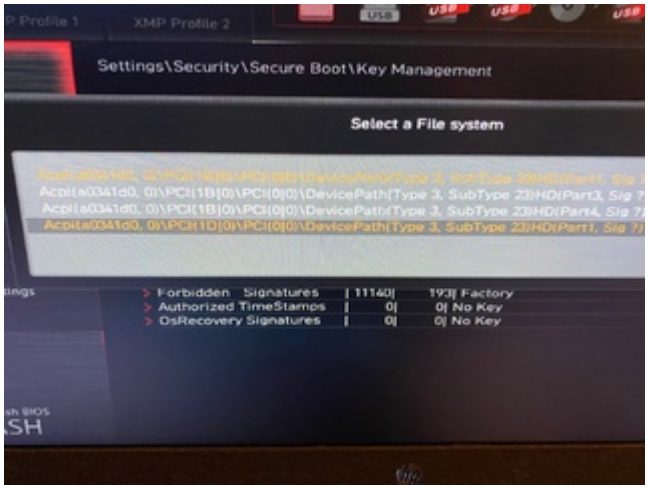
Settings->Security->Secure Boot:

Secure Boot Mode<Custom>

Zunächst Enroll all Factory default Keys.

Dann unter Key Management->Enroll EFI Image

Select Path:



Und unter EFI die Dateien:

Boot/Bootx64.efi

OC/OpenCore.efi

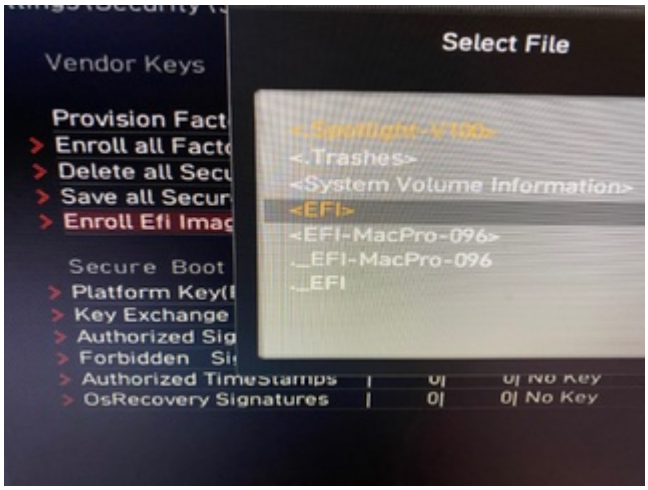
OC/Drivers/OpenRumtime.efi

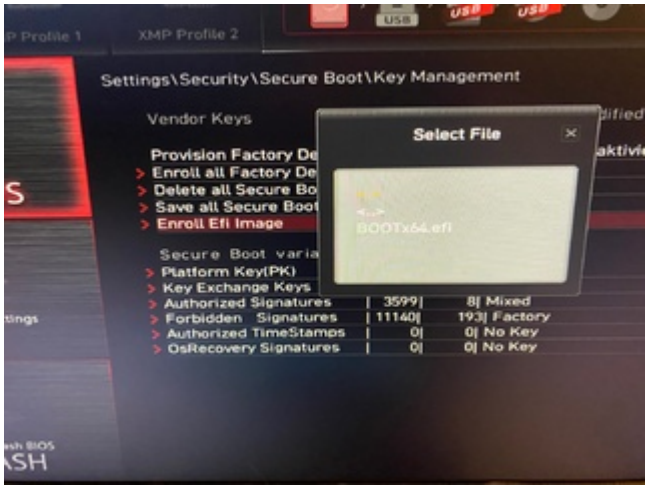
OC/Drivers/OpenCanopy.efi

OC/Drivers/HFSPlus.efi

OC/Drivers/ResetNVRAM.efi

am besten alles im Ordner Driver das ihr nutzt.....





Nacheinander Enrollen.....

Feddich.

Da alles direkt aus dem Bios machbar ist, auch einfach nach Update eben neu Enrollen für OpenCore oder Secure Boot ausschalten.....