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

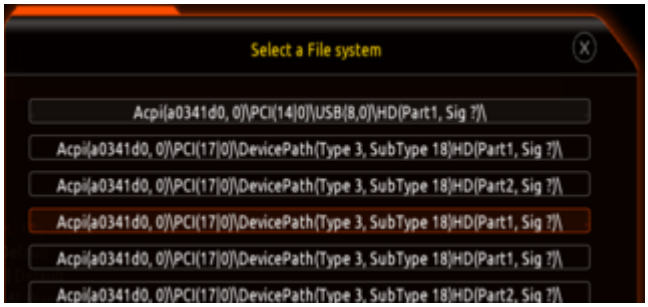
-> In der Liste der Filesystems eure Disk und Partition mit OC auswählen und nacheinander die Dateien

BOOT/Bootx64.efi

OC/OpenCore.efi

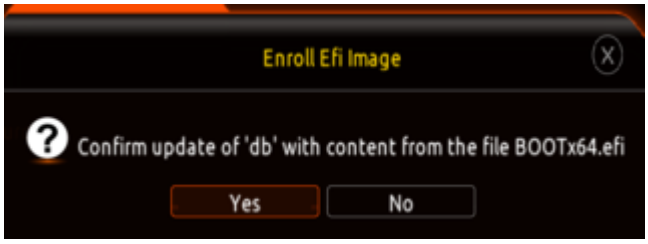
OC/Drivers/OpenRuntime.efi

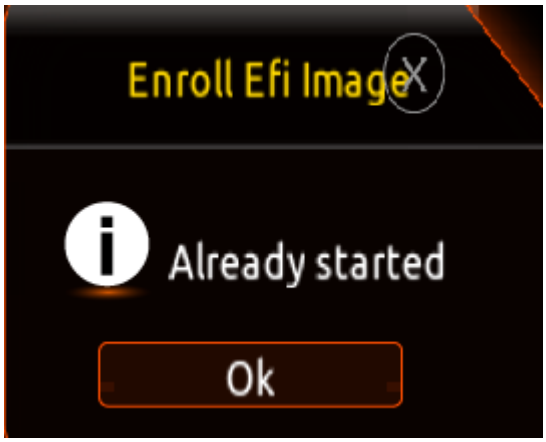
validieren


Select a File system
Acpi(a0341d0, 0)\PCI(14|0)\USB(8,0)\HD(Part1, Sig ?)\
Acpi(a0341d0, 0)\PCI(17|0)\DevicePath(Type 3, SubType 18)HD(Part1, Sig ?)\
Acpi(a0341d0, 0)\PCI(17|0)\DevicePath(Type 3, SubType 18)HD(Part2, Sig ?)\
Acpi(a0341d0, 0)\PCI(17|0)\DevicePath(Type 3, SubType 18)HD(Part1, Sig ?)\
Acpi(a0341d0, 0)\PCI(17|0)\DevicePath(Type 3, SubType 18)HD(Part1, Sig ?)\


Select File
<.>
<..>
<BOOT>
<OC>
<APPLE>


Select File
<.>
<..>
._BOOTx64.efi
BOOTx64.efi





(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