ECOS SecureBootStick®

Wie Sie bei HP-Laptops 3rd-Party-CA-Zertifikate erlauben

Anleitung

Version: 1.0

Datum: 02/2024

IT-Security Solutions

Made in Germany

ECOS TECHNOLOGY GMBH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel: +49 6133 939-0 | Fax: +49 6133 939-333

Einführung

Secure Boot ist eine wichtige Sicherheitsfunktion des UEFI-Standards, mit der sichergestellt wird, dass nach Initialisierung der Firmware nur signierte UEFI-Binärdateien ausgeführt werden können und Kernkomponenten wie Bootloader oder Kernel nicht manipuliert wurden.

Mit der Secured-Core-PC-Initiative hat Microsoft außerdem einen Standard etabliert, bei dem Secure Boot standardmäßig aktiviert und so konfiguriert ist, dass der UEFI-CA-Signatur eines Drittanbieters nicht automatisch vertraut wird.

Bei Secured-Core-PCs ist daher ein zusätzlicher Schritt notwendig, um die Verwendung von CA-Zertifikaten von Drittanbietern beim Secure Boot zu erlauben und den Linux-basierten ECOS **SecureBootStick®** (SBS) starten zu können.

Des Weiteren kommt bei neueren Computern der Marke Hewlett Packard (HP) hinzu, dass diese per HP Sure Start geschützt werden. Dabei handelt es sich um eine Sicherheitsfunktion des UEFI. Es schützt und erkennt Schäden oder Angriffe auf das UEFI. Es stoppt die Angriffe und kann das BIOS wiederherstellen.

Diese Schritt-für-Schritt-Anleitung beschreibt exemplarisch, wie Sie den HP Sure Start deaktivieren und die 3rd-Party-CA-Zertifikate erlauben.

Weitere Informationen zum HP Sure Start finden Sie im Infoblatt. Bei weiteren Fragen hierzu wenden Sie sich bitte direkt an den HP Kundensupport.

HP Sure Start deaktivieren

Um die 3rd-Party-CA-Zertifikate erlauben zu können, müssen Sie einmalig den HP Sure Start deaktivieren.

1

Schalten Sie Ihren Computer aus und trennen Sie den SBS von Ihrem Gerät.

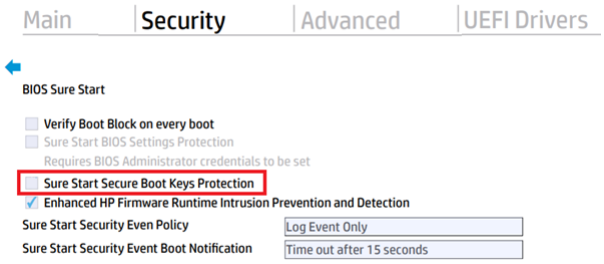
2

Starten Sie Ihren Computer und drücken Sie F10, um den Startvorgang zu unterbrechen und das BIOS-Setup zu öffnen.

3

Navigieren Sie zum Reiter **Security** (Sicherheit).

Unter dem Punkt **BIOS Sure Start** deaktivieren Sie die Option **Sure Start Secure Boot Keys Protection**.



4

Speichern Sie die Einstellungen mit F10 und bestätigen Sie die Änderung mit **Yes** (ja).

Ihr Gerät startet neu und es erscheint eine Aufforderung zur Eingabe eines Zahlencodes.

Geben Sie den auf Ihrem Bildschirm angezeigten **4-stelligen Zahlencode** ein und bestätigen Sie mit ENTER.

Hinweis: Der Zahlencode ändert sich jedes Mal. Der rechts abgebildete Code ist nur ein Beispiel.

Hinweis: Die Eingabe erfolgt i.d.R. ohne visuelle Bestätigung Ihrer Eingabe.

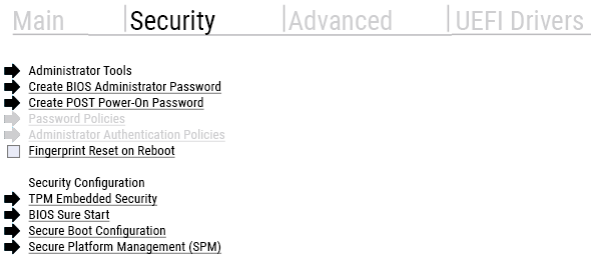
3rd-Party-CA-Zertifikate erlauben

Um den Secure Boot Stick (SBS) an Ihrem Gerät zu booten, müssen Sie die Verwendung der 3rd-Party-CA-Zertifikate erlauben.

1

Wiederholen Sie die Schritte ❶ + ❷, wenn Sie nicht mehr im BIOS Ihres Geräts sind.

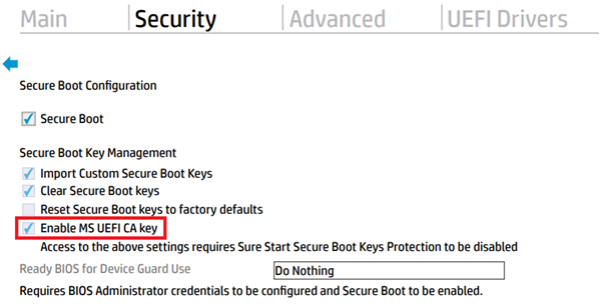
Andernfalls navigieren Sie zum Reiter **Security** (Sicherheit).



2

Unter dem Punkt **Secure Boot Configuration** aktivieren Sie die Option **Enable MS UEFI CA key**.

Hinweis: Je nach Modell kann diese Option auch *Allow Microsoft & 3rd Party UEFI CA* heißen.



3

Speichern Sie die Einstellungen mit F10 und bestätigen Sie die Änderung mit **Yes** (ja).

Ihr Gerät startet neu.

Je nach Sicherheitsvorgaben können Sie den **HP Sure Start** wie oben beschrieben wieder aktivieren. Die vorgenommenen Änderungen an der **Secure Boot Configuration** bleiben unberührt.