ECOS SecureBootStick®

Wie Sie 3rd-Party-CA-Zertifikate für UEFI Secure Boot erlauben

Anleitung

Version: 1.1

Datum: 01/2025

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.

Diese Schritt-für-Schritt-Anleitung beschreibt exemplarisch, wie Sie die Verwendung von 3rd-Party-CA-Zertifikaten in den UEFI-Einstellungen folgender Secured-Core-PCs aktivieren:

- Microsoft Surface
- Lenovo Thinkpad

Die hier beschriebene Vorgehensweise ist auch für andere Secured-Core-PCs anwendbar.

Eine Liste der gängigsten Tastenkombinationen zum Aufruf des BIOS bzw. UEFI finden Sie im SBS-Anwenderhandbuch, Kapitel **8.2 Bootmenü-/BIOS-Tasten** auf Seite 71.

3rd-Party-CA-Zertifikate für Secure Boot auf einem Microsoft Surface erlauben

1

Schalten Sie Ihr Surface aus.

Ziehen Sie ggf. den SBS ab.

2

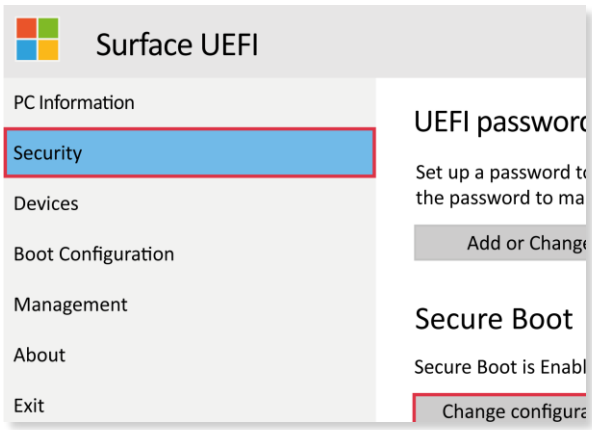
Halten Sie die **Lauter**-Taste gedrückt und drücken Sie gleichzeitig die **Power**-Taste.

Lassen Sie die **Lauter**-Taste los, sobald das Surface-Logo auf dem Bildschirm erscheint.

Das UEFI-Menü wird eingeblendet.

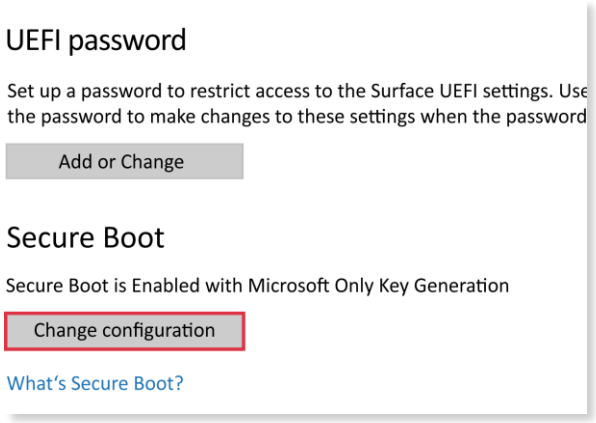
3

Wählen Sie in der linken Navigation des Surface-UEFI den Menüpunkt **Security**.



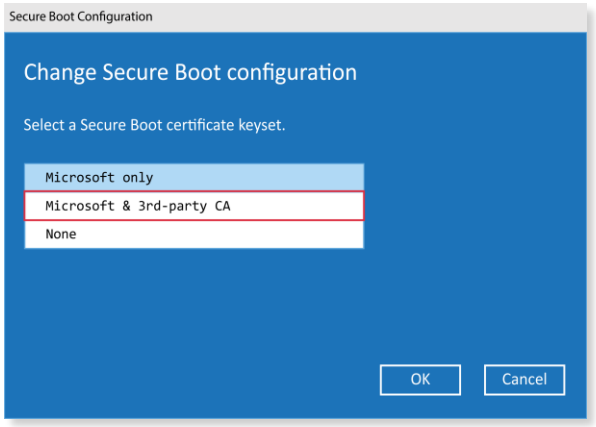
4

Klicken Sie auf den Button **Change configuration**.



5

Wählen Sie die Option **Microsoft & 3rd-party CA** und bestätigen Sie die Einstellung mit **OK**.



3rd-Party-CA-Zertifikate für Secure Boot auf einem Lenovo ThinkPad erlauben

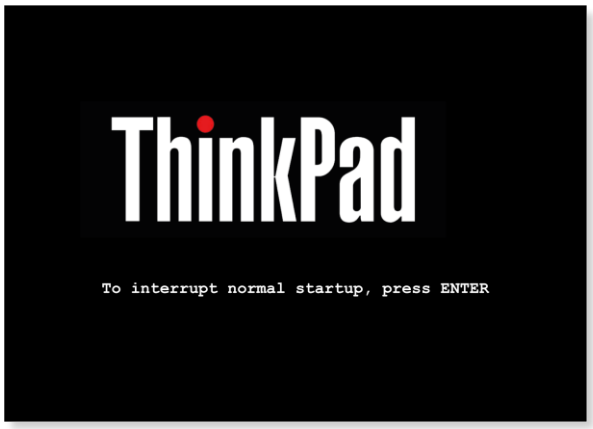
1

Schalten Sie Ihr ThinkPad aus und ziehen Sie ggf. den SBS ab.

2

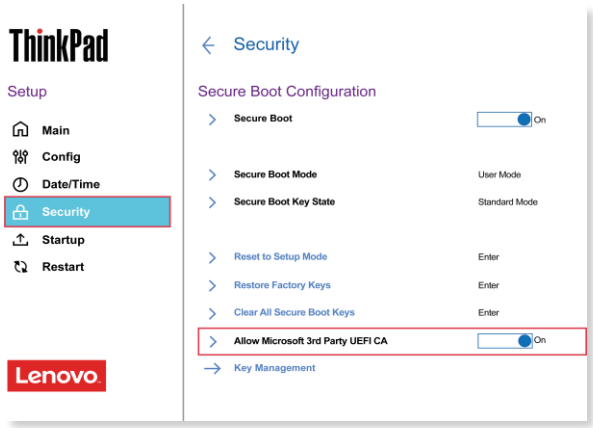
Schalten Sie das ThinkPad ein.

Drücken Sie die **F1**-Taste, sobald die Meldung *"To interrupt normal startup, press Enter"* erscheint.



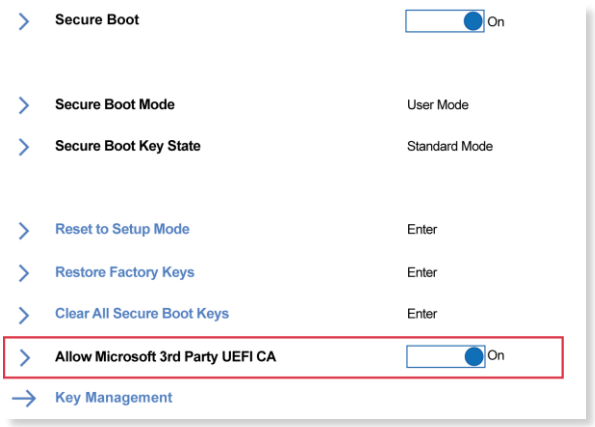
3

Wählen Sie in der linken Navigation des ThinkPad-UEFI den Menüpunkt **Security**.



4

Aktivieren Sie die Option **Allow Microsoft 3rd Party UEFI CA**.



5

Bestätigen Sie die Einstellung mit **F10**.