

Secure Boot Zertifikat-Check

Anleitung und Ergebniserklärung | v2.3

Wichtig: Die Frist läuft bereits

Die alten Secure-Boot-Zertifikate von 2011 sind seit Juni 2026 stufenweise abgelaufen (Microsoft Corporation KEK CA 2011: 24.06.2026, Microsoft UEFI CA 2011: 27.06.2026). Das letzte Zertifikat, Microsoft Windows Production PCA 2011, folgt am 19.10.2026. Betroffene Systeme verlieren danach die Fähigkeit, neue Secure-Boot-Sicherheitsupdates (inkl. Sperrlisten-Aktualisierungen) zu erhalten.

Was macht das Tool?

Das Tool prüft, ob dein Windows-System die neuen Microsoft Secure-Boot-Zertifikate von 2023 besitzt und ob die Sperrliste (DBX) aktuell ist. Es liest dafür mehrere UEFI-Datenbanken sowie den offiziellen Rollout-Status direkt aus deinem System und zeigt alle Ergebnisse übersichtlich in einem Fenster an. Es werden keinerlei Änderungen am System vorgenommen und keine Daten ins Internet gesendet.

Geprüft werden:

- **System:** UEFI-Modus, Secure Boot-Status, Erkennung virtueller Maschinen, Windows-Version
- **Zertifikat-Datenbank:** Windows UEFI CA 2023 und Microsoft UEFI CA 2023 (mit SHA-1-Thumbprint)
- **Key Exchange Key:** Microsoft KEK 2023 (benötigt für automatische db/dbx-Updates)
- **Sperrliste (DBX):** Anzahl gesperrter Bootloader (Schutz vor BlackLotus und ähnlichen Angriffen)
- **Servicing-Status:** Offizieller Microsoft-Rollout-Status aus der Registry (UEFICA2023Status)

Enthaltene Dateien

Datei	Beschreibung
SecureBootCheck.bat	Startdatei – diese Datei ausführen
SecureBootCheck.ps1	PowerShell-Skript (wird automatisch aufgerufen)
Anleitung.pdf	Diese Anleitung

Schritt-für-Schritt-Anleitung

1

ZIP-Paket entpacken

Entpacke das ZIP-Archiv in einen beliebigen Ordner, z. B. auf den Desktop oder in deinen Downloads-Ordner. Alle drei Dateien müssen sich im selben Ordner befinden.

2

SecureBootCheck.bat starten

Doppelklicke auf SecureBootCheck.bat. Das Tool erkennt fehlende Adminrechte automatisch und fordert sie per UAC-Abfrage an. Klicke auf "Ja". Das CMD-Fenster schließt sich danach sofort – das ist normal.

3

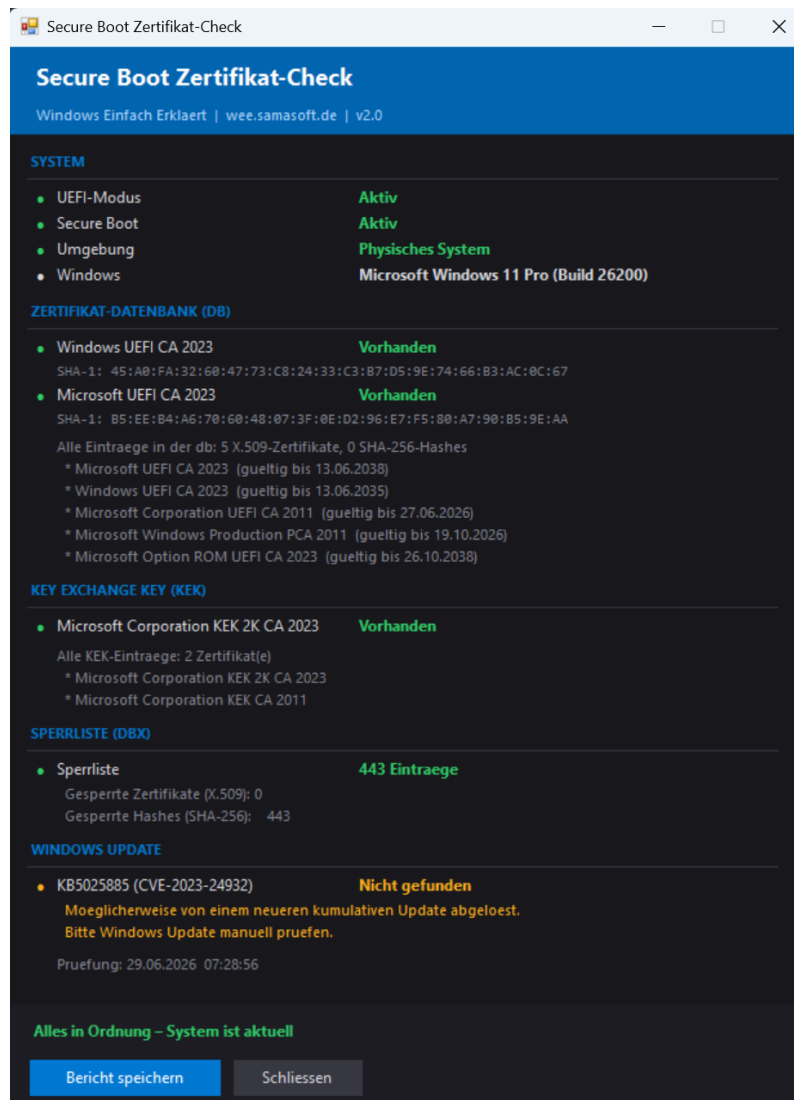
Ergebnis ablesen und ggf. Bericht speichern

Das Prüffenster öffnet sich und zeigt alle Ergebnisse an. Über "Bericht speichern" lässt sich eine TXT-Datei mit allen Details (inkl. Zertifikat-Thumbprints und Zeitstempel) exportieren. Eine ausführliche Erklärung der Ergebnisse findest du auf der nächsten Seite.

Sicherheitshinweis

Die BAT-Datei umgeht die PowerShell-Ausführungsrichtlinie nur fuer diesen einen Aufruf – keine dauerhafte Systemeinstellung wird veraendert. Das Skript liest ausschliesslich UEFI-Variablen und nimmt keinerlei Aenderungen am System vor.

So sieht das Prueffenster aus



Secure Boot Zertifikat-Check v2.3 – Ergebnis auf einem aktuellen Windows-11-System

Moegliche Gesamtergebnisse

Alles in Ordnung – System ist aktuell

Secure Boot ist aktiv und beide 2023er-Zertifikate (Windows UEFI CA 2023 und Microsoft UEFI CA 2023) sind in der UEFI-Datenbank vorhanden. Kein Handlungsbedarf.

Dringender Handlungsbedarf: 2023-Zertifikate fehlen

Secure Boot ist aktiv, aber mindestens eines der 2023er-Zertifikate fehlt. Da die alten 2011er-Zertifikate bereits ablaufen bzw. abgelaufen sind, sollte dieses System zeitnah aktualisiert werden. Oeffne Windows Update und installiere alle verfuegbaren Updates – Microsoft verteilt die neuen Zertifikate automatisch per Windows Update.

Secure Boot deaktiviert – kein Handlungsbedarf

Dein System startet ohne Secure Boot. Das Zertifikat-Update ist fuer dieses System derzeit nicht relevant.

System nutzt Legacy-BIOS – kein Handlungsbedarf

Dein System laeuft im Legacy-BIOS-Modus (kein UEFI). Secure Boot wird nicht unterstuetzt, die Zertifikatspruefung entfaellt.

Hinweise zu einzelnen Pruefbereichen

Sperrliste (DBX)

Eine aktuelle DBX enthaelt typischerweise mehrere hundert Eintraege. Wenige Eintraege (unter 50) deuten auf eine veraltete Sperrliste hin – bekannte Angriffe wie BlackLotus koennten dann moeglicherweise ausgenutzt werden. Die Aktualisierung erfolgt automatisch ueber Windows Update.

Key Exchange Key (KEK)

Der KEK autorisiert Schreibzugriffe auf die UEFI-Datenbanken (db und dbx). Fehlt ein aktueller KEK, koennen Windows-Update-seitige Aktualisierungen der Datenbanken moeglicherweise nicht automatisch eingespielt werden.

Servicing-Status (UEFICA2023Status)

Microsoft speichert den Fortschritt des automatischen Zertifikats-Rollouts in der Registry unter HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing. "Updated" bedeutet vollstaendig umgestellt, "InProgress" bedeutet der Rollout laeuft noch im Hintergrund, "NotStarted" kann sowohl "bereits konform" als auch "Rollout noch nicht ausgeloeset" bedeuten. Ein Neustart kann einen haengenden Rollout oft anstossen.

Virtuelle Maschinen (VM)

Bei Hyper-V, VMware, VirtualBox u. a. beziehen sich alle Ergebnisse auf den virtuellen UEFI-Bereich der VM, nicht auf das Host-System. Fuer eine vollstaendige Pruefung das Tool zusaetzlich direkt auf dem Host-System ausfuehren.

"Bericht speichern"-Funktion

Ueber die Schaltflaeche im Fenster laesst sich ein vollstaendiger Pruefbericht als TXT-Datei exportieren. Dieser enthaelt alle Zertifikat-Thumbprints, Eintrags-Zahlen und den genauen Zeitstempel der Pruefung – nuetzlich zur Dokumentation oder wenn du die Ergebnisse mit jemandem teilen moechtest.