FAQ

TPM 2.0

Für Windows 11 verlangt Microsoft ein Hardware-Sicherheitsmodul vom Typ TPM 2.0. Solche Module sind zwar schon seit Jahren auf dem Markt, aber in drei Varianten, und auch nicht bei jedem Computer aktiviert.

Von Christof Windeck

Was ist ein TPM?

Ein Trusted Platform Module (TPM) bietet ähnliche Funktionen wie eine SmartCard, ist aber in einen Computer eingebaut, also mit der Plattform verbunden. Das TPM dient als separater Vertrauensanker (Root of Trust) unabhängig von Hauptprozessor (CPU), Arbeitsspeicher (RAM), Massenspeicher und Betriebssystem. Dazu speichert es einen Geheimwert, der das TPM nie verlässt, aber als Wurzel einer kryptografischen Zertifikatskette dient. Das TPM kann andere digitale Zertifikate signieren und prüfen sowie sichere Schlüssel erzeugen. Schließlich stellt ein TPM noch geschützten Speicherplatz bereit, sogenannte Platform Configuration Registers (PCRs). Darin kann der Computer Hashes speichern, etwa um Manipulationen an der Firmware zu erkennen.

Ein Trusted Platform Module (TPM) – hier der TPM-2.0-Chip SLB9665TT20 von Infineon – arbeitet als Hardware-Vertrauensanker im Computer unabhängig von CPU, RAM und Betriebssystem.

TPM oder fTPM?

Was ist der Unterschied zwischen TPM 2.0 und fTPM 2.0?

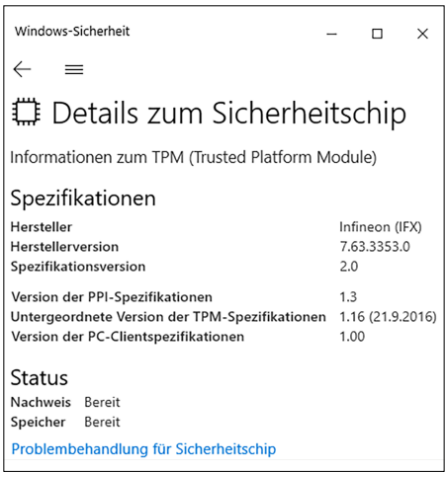
Windows 11 kann sowohl ein TPM 2.0 nutzen als auch ein fTPM 2.0. Ein TPM 2.0 ist ein separater (diskreter) Chip, der zusätzlich aufs Mainboard gelötet ist oder auf einem Steckmodul sitzt. Zertifizierte TPM-2.0-Chips liefern die Firmen Infineon (IFX), STMicroelectronics (STM) und Nuvoton. Das „f“ in fTPM steht hingegen für „Firmware“ (Firmware-TPM); ein fTPM ist kein separater Chip, sondern ein integrierter Funktionsblock in einem Prozessor, System-on-Chip (SoC) oder Mainboard-Chipsatz. Weil die fTPM-Firmware dabei auf einem zwar eingebetteten, aber separaten Mikrocontroller-Kern läuft, arbeitet auch ein fTPM unabhängig von CPU, RAM und Massenspeicher.

Bisher gibt es ausschließlich fTPMs nach TPM-2.0-Spezifikation (fTPM 2.0), also mit demselben Funktionsumfang wie diskrete TPM-2.0-Chips. Letztere gibt es aber in Versionen, die schärfere Sicherheitsstandards erfüllen, beispielsweise das Common Criteria Elevated Assurance Level 4+ (CC EAL4+).

Vorhandenes TPM erkennen

Wie erkenne ich, ob mein System ein TPM 2.0 hat?

Wenn das TPM aktiv ist, führt es Windows 10 im Geräte-Manager unter „Sicherheitsgeräte“ auf und zeigt, ob es sich um ein TPM 1.2 oder TPM 2.0 handelt – aber nicht, ob es sich um ein fTPM oder einen separaten Chip handelt. Leichter zu entschlüsseln sind die Angaben unter „Gerätesicherheit“, wo ein TPM als „Sicherheitschip“ auftaucht. Unter „Details zum Sicherheitschip“ finden sich Hinweise zum „Hersteller“. Steht da „Intel“, „AMD“ oder „Qualcomm“, handelt es sich um ein fTPM; sonst ist es ein diskreter Chip – mit einer Ausnahme: In Virtuellen Maschinen (VMs) unter Hyper-V lässt sich ein emuliertes TPM (Virtual TPM, vTPM) einschalten, das sich als Microsoft-Produkt meldet (Hersteller MSFT).



Unter Windows 10 taucht ein TPM in der Systemsteuerung unter „Gerätesicherheit“ als „Sicherheitschip“ auf. Dort zeigt Windows auch „Details“ an, etwa den Hersteller (hier Infineon) und die „Spezifikationsversion“ (2.0 für TPM 2.0). Leider stören schiefe Übersetzungen; mit „Nachweis“ ist „TPM Key Attestation“ gemeint.

TPM 1.2 veraltet?

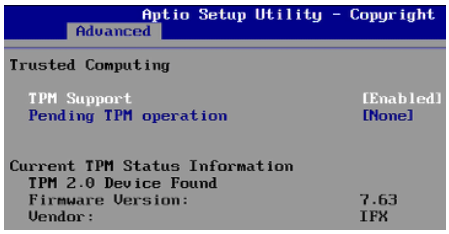
Was unterscheidet TPM 2.0 von TPM 1.2?

Beim TPM 1.2 war als Secure-Hash-Algorithmus (SHA) nur das veraltete und geknackte Verfahren SHA-1 verpflichtend und AES-Verschlüsselung nicht zwingend vorgeschrieben. Ein TPM 2.0 muss SHA-256 und mindestens AES-128 beherrschen. Außerdem ist die TPM-2.0-Spezifikation präziser.

TPM aktivieren

Wie schalte ich das TPM im BIOS-Setup ein?

Ist ein TPM aufgelötet oder als fTPM in der Hardware integriert, aber unter



Ist ein TPM vorhanden, lässt es sich möglicherweise im BIOS-Setup des Computers einschalten.

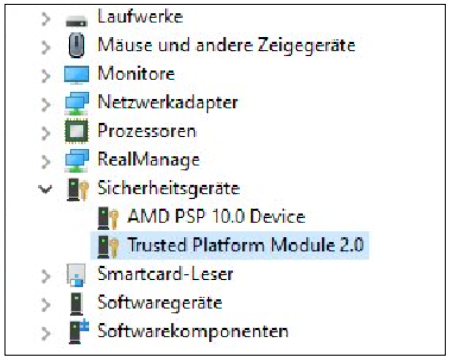
Windows nicht sichtbar, ist es möglicherweise durch eine Option im BIOS-Setup aktivierbar – allerdings nur, wenn der jeweilige Mainboard-Hersteller das vorgesehen hat. Die nötigen Optionen finden sich oft in Menüs mit Namen wie „Security“, „Security Chip“ oder „Platform Security“.

TPM-Verbreitung

Seit wann haben PCs, Notebook und Tablets üblicherweise ein TPM 2.0?

Die TPM-2.0-Spezifikation erschien 2012, 2013 kündigte Infineon die ersten kompatiblen Chips an. Sie kamen seither vor allem in Bürocomputern mit „vPro“-Hardware von Intel zum Einsatz, später auch in welchen mit AMD Ryzen Pro, sowie in Notebooks aus den Business-Baureihen von HP (Elite), Dell (Latitude/Precision), Lenovo (ThinkPad), Fujitsu (Lifebook) und Toshiba/Dynabook.

AMD baut seit 2014 den sogenannten Platform Security Processor (PSP, später „Secure Processor“) auf Basis eines ARM Cortex-A5 in alle Prozessoren ein, beginnend ab Beema/Mullins und Carrizo. Bei Intel läuft das fTPM in der sogenannten Converged Security and Management Engine (CSME, früher ME) von Chipsätzen seit der Serie 100 (Z170, Q170, H170, B150) für Core i-6000 (Skylake) aus dem Jahr 2015. Auch in „Atom-Celerons“ ab 2014 (Bay Trail, Celeron N2000) stecken fTPMs, dort in der Trusted Execution Engine (TXE). Nicht immer sind diese fTPMs tatsächlich nutzbar, sondern nur, wenn die nötige Firmware auch an Bord ist und das BIOS sie einschaltet. Manche Systeme haben wiederum zwei TPMs, nämlich zusätzlich zum fTPM einen TPM-Chip.



Manche Computer mit diskretem TPM-2.0-Chip haben zusätzlich ein fTPM, in diesem Falle eines von AMD, das im Platform Security Processor (PSP) steckt.

TPM nachrüsten

Kann ich ein TPM in meinem PC nachrüsten?

Manche Mainboards haben Pfostenstecker (TPM Header), um eine kleine Steckplatine mit einem TPM-Chip nachzurüsten. Allerdings muss das BIOS darauf vorbereitet sein und es gibt unterschiedliche Bauformen sowie Schnittstellen wie Low-Pincount-(LPC-)Interface, Serial Peripheral Interconnect (SPI) oder I2C. Man braucht also ein zum jeweiligen Board passendes TPM-Kärtchen.

TPM-Nutzen

Wofür nutzt Windows überhaupt das TPM und was habe ich davon?

Der bekannteste Einsatzzweck eines TPM unter Windows ist die Festplatten- beziehungsweise SSD-Verschlüsselung BitLocker, die aber nur bei den Pro- und Enterprise-Versionen von Windows vorhanden ist. Der Schlüssel für die Verschlüsselung kann (muss aber nicht) dabei an das TPM gebunden werden (Key Sealing), um gespeicherte Daten zu schützen, wenn das Speichermedium vom System getrennt wurde. Ähnlich wie BitLocker funktioniert bei Tablets und 2-in-1-Hybriden mit „Modern Standby“ die Laufwerksverschlüsselung „Automatic Device Encryption“, die das PCR 7 verwendet.

Auch in die biometrische Authentifizierung mit Windows Hello for Business lässt sich ein TPM einbinden. Außerdem hat Microsoft seit 2019 in Kooperation etwa mit Dell, HP und Lenovo Notebooks vorgestellt, deren Firmware besser gegen Manipulationen (wie BIOS-Rootkits) geschützt sein soll. Diese „Secured-Core PCs“ verwenden das TPM als Dynamic Root of Trust for Measurement (DRTM). Für die Schutzfunktion virtualisierungsbasierte Sicherheit (Virtualization-Based Security, VBS) lässt sich ebenfalls ein TPM nutzen sowie zum kryptografischen Nachweis des Systemzustands für den Zugriff auf Cloud-Anwendungen (Microsoft Azure Attestation).

TPM und UEFI Secure Boot

Was hat ein TPM mit dem kryptografisch gesicherten Startmodus „UEFI Secure Boot“ zu tun?

Nichts: UEFI Secure Boot alias „sicherer Startzustand“ funktioniert auch ohne TPM. Spezielle Bootloader, die etwa bei manchen Sicherheits-Softwarepaketen zum Einsatz kommen, können ein TPM nach dem Booten aber einbinden, um Manipulationen des UEFI-BIOS zu erkennen, siehe „DRTM“ oben.

TPM-Sicherheit

Gibt es TPM-Sicherheitslücken?

Im Jahr 2017 wurde in TPM-1.2-Chips von Infineon die Schwachstelle „ROCA“ im Algorithmus zur Erzeugung von RSA-Schlüsseln aufgedeckt. Sie wurde durch Firmware-Updates geschlossen. 2019 kam die Sicherheitslücke „TPM-Fail“ in TPM-2.0-Chips von STMicroelectronics und in fTPM-Implementierungen von Intel ans Licht; auch diese wurden mit Patches geschlossen. TPM-Fail betraf ausschließlich den Elliptic Curve Digital Signature Algorithm (ECDSA).

Windows 11 ohne TPM

Lässt sich Windows 11 auch ohne TPM nutzen?

Das ist derzeit (Stand Juli 2021) noch unklar. Microsoft verlangt ein TPM 2.0 für Computer mit Windows-11-Logo. Allerdings lässt sich Windows 11 auf anderem Wege auch auf Systemen ohne TPM installieren (siehe Seite 20). Welche Folgen das hat, ist bisher nicht absehbar.

(ciw@ct.de)