

ZACHTE HARDE EISEN

Windows 11: hardware-eisen getest in de praktijk

Sinds Microsoft Windows 11 heeft aangekondigd, hebben de systeemeisen die ervoor worden genoemd voor heel wat opschudding gezorgd. Sinds kort kunnen ze in de praktijk worden gecontroleerd. We hebben een paar verrassingen ontdekt.

Axel Vahldiek en Noud van Kruysbergen

Op 24 juni kondigde Microsoft aan dat Windows 10 een opvolger krijgt. Op dit moment is bekend dat de eerste uitrol vanaf 5 oktober voornamelijk bij nieuwe pc's gebeurt, en dat de rest van de Windows 10-installaties later aan de beurt komt. Medio 2022 moeten alle apparaten die voldoen aan de hardware-eisen Windows 11 hebben kunnen installeren.

De systeemeisen van Windows Vista tot Windows 10 zijn nauwelijks veranderd. Bij Windows 11 is dat anders is, omdat Microsoft de eisen drastisch opvoert [1]. Met de PC Health Check-app (zie de link) kun je controleren of je pc daaraan voldoet – en zo niet, waar je nog in moet investeren. Maar zal Microsoft dat ook echt afdwingen?

Eind augustus heeft Microsoft ISO-bestanden beschikbaar gesteld om te downloaden die complete sets Windows 11-installatiegegevens bevatten, inclusief het installatieprogramma. Dat maakte nieuwe installaties van Windows 11 voor het eerst mogelijk. We hebben die op verschillende testcomputers uitgeprobeerd. Spoiler-alert: met de prerelease-versie kunnen de eisen nog wel omzeild worden. En aangezien Microsoft tot de release van de definitieve versie nauwelijks nog tijd heeft gehad voor serieuze wijzigingen, zou dat ook daarvoor kunnen gelden.

```
VerifyRAMRequirements: System has SUFFICIENT system memory: [8192 MB] vs [3686 MB]
VerifyProcessorSupported: number of cores SUFFICIENT: [8] vs [2]
VerifyProcessorSupported: Sufficient processor frequency: [1800 MHz] vs [1000 MHz]
VerifyProcessorSupported: Processor Frequency Check Returned [0x0]
VerifySecureBoot: Capable of SecureBoot
VerifyTPMSupported: TPM Version SUPPORTED.
Callback_ValidateHardwareRequirements: HW Requirements checks passed
```

In het bestand Setupact.log noteert het set-upprogramma de resultaten van de controle van de hardware-eisen.

AANKONDIGING

Ter herinnering de officiële eisen van Microsoft voor Windows 11: de computer moet ten minste een dualcore-processor hebben met een kloksnelheid van 1 GHz en 4 GB RAM, en een interne gegevensdrager met niet minder dan 64 GB vrije ruimte. De eis dat de cpu 'compatibel' moet zijn veroorzaakte de meeste opwinding.

Een blik op Microsofts compatibiliteitslijst kan beangstigend zijn omdat de vermelde processors allemaal relatief jong zijn. Intel begint bijvoorbeeld pas met de 7e Core i-generatie, AMD met Ryzen 2000 (Zen+), hoewel ook Athlon-processors met Zen 1-kernen vermeld worden. De lijst vind je via de link bij dit artikel.

De eisen aan het moederbord worden ook steeds hoger. Microsoft wil af van het klassieke legacy-BIOS en heeft UEFI opgenomen bij de eisen voor Windows 11. Dat betekent niet alleen dat het moederbord UEFI als firmware moet gebruiken, maar ook dat Windows moet opstarten met UEFI-mechanismen, dus niet via de BIOS-compatibiliteitsmodus (CSM). Bovendien moet er een TPM 2.0 in het systeem aanwezig zijn (zie ook pagina 102 in deze c't). Ten slotte moet UEFI Secure Boot niet alleen aanwezig, maar ook geactiveerd zijn.

UITVOERING

Maar welke eisen worden werkelijk gehandhaafd? Eerste tests van de prerelease-versie maakten duidelijk dat het Windows helemaal niet uitmaakt op welke hardware het draait: opstarten via legacy-BIOS zonder TPM en Secure Boot met slechts 2 GB RAM en een miezerige 17 GB schijfruimte bleek geen enkel probleem.

Het set-upprogramma van Windows 11 zorgt ervoor dat aan de eisen voldaan wordt. Wat het controleert kan worden gelezen, want het schrijft een logbestand met de naam Setupact.log tijdens het installeren van Windows. Dat bevindt zich tijdens het installeren in X:\Windows\Panther en erna in C:\Windows\Panther. Je kunt dat bestand openen met een teksteditor. In het logbestand staat wat er is gecontroleerd en met welk resultaat door te zoeken op Verify.

CONTROLES

Het eerste criterium is het RAM. Officieel is 4 GB vereist, maar het set-upprogramma is tevreden met 3686 MB. Als er minder is, weigert het set-upprogramma.

De volgende twee testcriteria moeten door de processor worden vervuld: twee kernen en een klokfrequentie van 1000 MHz zijn vereist. Een andere controle levert de log-invoer `VerifyProcessorSupported: Processor Frequency Check Returned [0x0]` op, maar wat daar precies gecontroleerd wordt is nog niet duidelijk.

Het set-upprogramma controleert of de pc geschikt is voor Secure Boot, maar dat is waar de eerste openlijke tegenstrijdigheid tussen de eisen en uitvoering optreedt. Secure Boot moet niet alleen aanwezig zijn, maar ook actief. Maar het installeren werkt ook zonder een actieve Secure Boot. Het is echter denkbaar dat dit alleen geldt voor de prerelease-versie omdat Microsoft anders een probleem heeft. Omdat er nog geen Media Creation Tool is voor het maken van een set-upstick voor een

schone nieuwe installatie, verwijst Microsoft in plaats daarvan naar de freeware Rufus. Sticks die daarmee gemaakt zijn, zullen echter niet opstarten als Secure Boot actief is.

Het set-upprogramma controleert verder of er een TPM aanwezig is, en ook daar negeert het de aankondiging van Microsoft. Hoewel Microsoft aandringt op TPM 2.0, accepteerde het set-upprogramma bij onze test ook een TPM 1.2.

ANDERE CONTROLES

Hoewel er 64 GB vrij moeten zijn op de beoogde data-drager, neemt het set-upprogramma genoeg met slechts 52 GB, wat het resultaat is van het mooie ronde getal van 0xd000000 bytes. Het resultaat van die controle staat in het logbestand in de regel 'Location total capacity is [0x7470c06000] and required capacity is [0xd00000000]'. Als niet aan die voorwaarde voldaan wordt, wijst het installatieprogramma daarop, maar zet zijn werk zonder klagen voort. We kregen Windows 11 zelfs op een 20GB-partitie genstalleerd.

DE PROCESSOR

Een 'compatibele' cpu is tot slot een van de belangrijke vereisten, maar ook dat blijft voorlopig zonder gevolgen. Bij onze tests accepteerde het Windows 11 set-upprogramma zelfs de oudste cpu's zonder klagen, zolang ze maar voldoende cores en klokfrequentie boden.

Niettemin zijn er sporen van de aangekondigde controle te ontdekken. In de Sources-map op het set-up-medium staat een bestand genaamd cpufms.ini, dat blijkbaar een zwarte lijst van processors bevat. Volgens dat bestand worden Intel-cpu's t/m de 6e generatie uitgesloten, evenals AMD-cpu's tot en met processorfamilie 22, hoewel er uitzonderingen zijn (zie de afbeelding).

EISEN OMZEILEN

Het set-upprogramma probeert het voldoen aan de hardware-eisen gedeeltelijk af te dwingen, maar er zijn manieren om dat te voorkomen. Voor de prerelease-versie heeft Microsoft al gedocumenteerd dat ze niet van belang zijn als je Windows 11 in een virtuele machine installeert. Voor Hyper-V, VMware Workstation en Virtual Box kunnen we dat bevestigen.

Maar er zijn andere manieren om het te omzeilen. Microsoft heeft daar mechanismen voor ingebouwd in het set-upprogramma van de huidige prerelease-versies. Dat draait onder een soort mini-Windows genaamd Preinstallation Environment (PE) en heeft zijn eigen register (druk op Shift+F10 tijdens het installeren, typ `Regedit` in). Daar kun je verschillende eenduidige strings aanmaken onder HKEY_LOCAL_MACHINE\SYSTEM\Setup\LabConfig, zoals `BypassTPMCheck`, `BypassSecureBootCheck`, `BypassRAMCheck`, `BypassStorageCheck` en `BypassCPUCheck`. De waarde 1 laat de betreffende controle overslaan.

CONCLUSIE

Wat Microsoft als prerelease heeft gepubliceerd maakt duidelijk dat in ieder geval een aantal van de hardware-eisen serieus bedoeld zijn. Hoewel de generatie van de

```
CpuStepping=9
CpuModel=142
PlatformIDException=0x00000010
```

```
[BlockIntelKabyLake2]
```

```
CpuFamily=6
CpuStepping=9
CpuModel=158
PlatformIDException=0x00000008
```

```
[BlockAMD]
```

```
CpuFamilyLessThanOrEqual=22
```

```
[BlockAMDRaven]
```

```
CpuFamily=23
CpuModel=17
```

```
[BlockAMDSummitRidge]
```

```
CpuFamily=23
CpuModel=1
```

100% Windows (CRLF) UTF-8

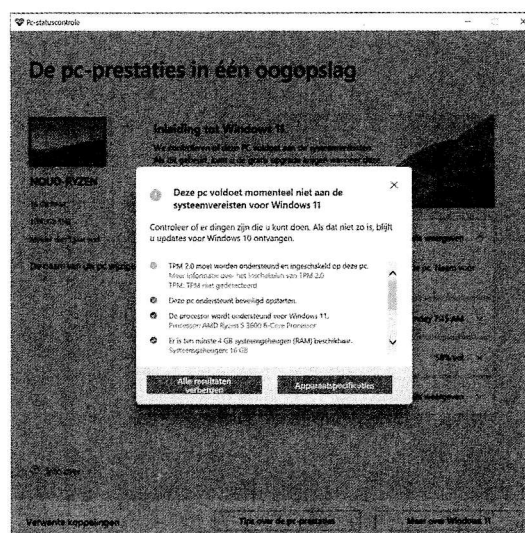
Het ISO-bestand met de prerelease-versie bevat een INI-bestand met cpu's waarvoor het set-upprogramma verondersteld wordt niet te werken – maar tot nu toe wordt dat bestand genegeerd.

processor tot dusverre geen rol speelt, wijst het bestaan van het INI-bestand er sterk op dat dit waarschijnlijk zal veranderen. Het installatieprogramma zou bij de definitieve versie meer daadwerkelijke eisen kunnen stellen aan Secure Boot en TPM dan nu het geval is.

Het bestaan van registervermeldingen die het set-upprogramma ertoe aanzetten de eisen te negeren, toont echter aan dat er waarschijnlijk manieren en middelen zullen zijn om de definitieve versie van Windows 11 op bijna elke x86-pc te kunnen installeren. Het is echter onduidelijk welke gevolgen dat zal hebben: zal een dergelijke installatie van updates worden voorzien? Microsoft heeft op het moment van schrijven nog geen antwoord gegeven op die vraag. **ct**



www.ct.nl/softlink/2111016



Met het programma PC Health Check kun je controleren of je pc voldoet aan de systeemeisen van Windows 11.

Literatuur

- [1] Axel Vahldiek en Noud van Kruysbergen, Windows 11: prijzen, licenties, systeemeisen, updates en upgrades, c't 10/2021, p.40

FAQ

TPM 2.0

Microsoft vereist voor Windows 11 een hardwarebeveiligingsmodule van het type TPM 2.0. Die zijn al enige tijd op de markt, maar er zijn drie varianten – en ze zijn niet bij elke pc geactiveerd.

Christof Windeck en Marco den Teuling

WAT IS EEN TPM?

! Een Trusted Platform Module (TPM) biedt soortgelijke functies als een smartcard, maar is ingebouwd in een computer, oftewel verbonden met het platform. De TPM fungeert als een afzonderlijke vertrouwensbasis (Root-of-Trust), geheel onafhankelijk van de hoofdprocessor (cpu), het werkgeheugen (RAM), de massaopslag en het besturingsstelsel. Daartoe bewaart het een geheime waarde die de TPM nooit verlaat, maar die dient als de root van een cryptografische certificatenketen. De TPM kan andere digitale certificaten ondertekenen en verifiëren en veilige sleutels genereren. Ten slotte biedt een TPM beveiligde opslag, de zogenaamde Platform Configuration Registers (PCR's). De computer kan er hashes in opslaan, om bijvoorbeeld manipulaties van de firmware op te sporen.

TPM OF fTPM?

? Wat is het verschil tussen de begrippen TPM 2.0 en fTPM 2.0?

! Windows 11 kan zowel een TPM 2.0 als een fTPM 2.0 gebruiken. Een TPM 2.0 is een afzonderlijke (discrete) chip die apart op het moederbord wordt gesoldeerd of op een insteekmodule zit. Gecertificeerde TPM 2.0-chips worden geleverd door Infineon (IFX), STMicroelectronics (STM) en Nuvoton. De f in fTPM staat daarentegen voor firmware. Een fTPM is geen afzonderlijke chip, maar een geïntegreerd functieblok in een processor, System-on-Chip (SoC) of chipset op een moederbord. Omdat de fTPM-firmware op een ingebedde maar afzonderlijke microcontroller kern draait, werkt een fTPM ook onafhankelijk van de cpu, het RAM en de massaopslag.

Tot dusver zijn er alleen fTPM's volgens de TPM 2.0-specificatie (fTPM 2.0), dat wil zeggen met

hetzelfde scala aan functies als discrete TPM 2.0-chips. Die laatste zijn beschikbaar in versies die aan strengere veiligheidsnormen voldoen, bijvoorbeeld Common Criteria Elevated Assurance Level 4+ (CC EAL4+).

BESCHIKBARE TPM BEPALEN

? Hoe kan ik herkennen of mijn systeem een TPM 2.0 heeft?

! Als de TPM geactiveerd is, vind je in Apparaatbeheer van Windows 10 een item onder Beveiligingsapparaten. Je ziet daarbij ook vermeld of het om een TPM 1.2 of TPM 2.0 gaat, maar niet of het gaat om een discrete chip of een fTPM. Je hebt meer aan de gegevens die je vindt bij het Configuratiescherm onder Apparaatbeveiliging. Bij Beveiligingsprocessor vind je via 'Details beveiligingsprocessor' de naam van de fabrikant. Staat daar Intel, AMD of Qualcomm, dan gaat het om een fTPM, in andere gevallen is het een discrete chip. Daarop is nog een uitzondering: bij virtuele machines kan een geëmuleerde TPM (Virtual TPM, vTPM) worden geactiveerd waarbij Microsoft als fabrikant verschijnt (fabrikant: MSFT).

TPM ACTIVEREN

? Hoe kan ik TPM bij de BIOS-instellingen inschakelen?

! Als een TPM-chip aanwezig is of als fTPM in de hardware geïntegreerd is, maar niet opduikt in Windows, moet die mogelijk nog worden geactiveerd via een optie bij de BIOS-instellingen. Daarvoor moet de moederbordfabrikant zo'n optie wel hebben ingebouwd. Je vindt de betreffende optie in het BIOS vaak terug in menu's met namen als Security, Security Chip of Platform Security.

BESCHIKBAARHEID TPM

? Sinds wanneer hebben pc's, laptops en tablets normaliter een TPM 2.0?

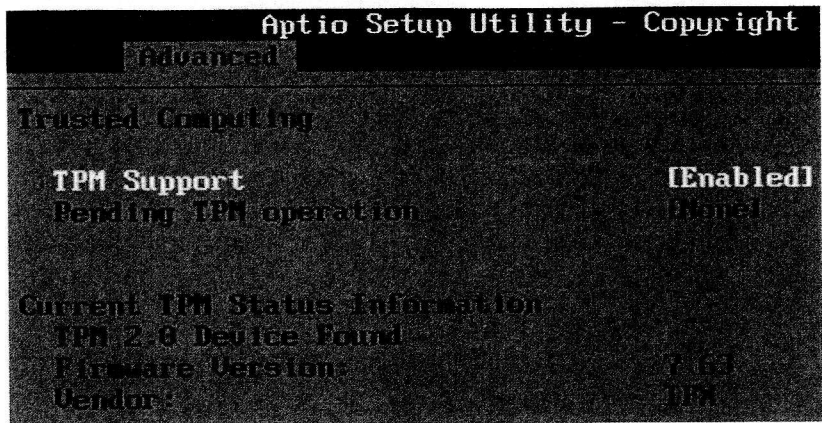
! De TPM 2.0-specificatie verscheen in 2012, en Infineon kondigde de eerste compatibele chips aan in 2013. Sindsdien worden ze vooral gebruikt in kantoorcomputers met vPro-hardware van Intel, later



Bij Windows 10 verschijnt een TPM in het Configuratiescherm als 'beveiligingsprocessor'. Bij de details staat ook informatie over de fabrikant (hier Infineon) en de specificatieversie (hier 2.0 voor TPM 2.0).

ook in die met AMD Ryzen Pro, en in laptops uit de zakelijke reeks van HP (Elite), Dell (Latitude/Precision), Lenovo (ThinkPad), Fujitsu (Lifebook) en Toshiba/Dynabook.

AMD integreert sinds 2014 de zogeheten Platform Security Processor (PSP, later Secure Processor) op basis van een ARM Cortex-A5 in alle processors, te beginnen met Beema/Mullins en Carrizo. Bij Intel draait de fTPM in de zogeheten Converged Security and Management Engine (CSME, voorheen ME) van chipsets sinds de 100-serie (Z170, Q170, H170, B150) voor Core i-6000 (Skylake) uit 2015. Je vindt fTPM's ook in de Atom-Celerons uit 2014 (Bay Trail, Celeron N2000), daar in de Trusted Execution Engine (TXE). Die fTPM's zijn niet altijd daadwerkelijk bruikbaar, maar alleen als de nodige firmware ook aan boord is en het BIOS ze activeert. Sommige systemen hebben zelfs twee TPM's, namelijk een TPM-chip naast de fTPM.



Als een TPM aanwezig is, moet die misschien worden geactiveerd via de BIOS-set-up van de computer.

de systeemstatus voor toegang tot cloudapplicaties (Microsoft Azure Attestation).

TPM INBOUWEN

? Kan ik later achteraf nog een TPM in mijn pc inbouwen?

! Veel moederborden beschikken over een header (TPM Header) waarop een kleine printplaat met een TPM-chip kan worden geplaatst. Het BIOS moet daar wel voor zijn ingericht en er zijn verschillende fysieke interfaces zoals een Low-Pincount-(LPC-) interface, Serial Peripheral Interconnect (SPI) of I2C. Je hebt dus een TPM-module nodig die specifiek op jouw moederbord past.

TPM-TOEPASSINGEN

? Waarvoor gebruikt Windows eigenlijk de TPM en wat heb ik daaraan?

! De bekendste toepassing van een TPM onder Windows is de versleuteling van harde schijven of ssd's met BitLocker, dat alleen beschikbaar is in de Pro- en Enterprise-versies van Windows. De encryptiesleutel kan (maar hoeft niet) aan de TPM worden gebonden (Key Sealing) om opgeslagen bestanden te beschermen als het opslagmedium van het systeem wordt losgekoppeld. Net als BitLocker werkt de schijfversleuteling Automatic Device Encryption, die de PCR 7 gebruikt, ook voor tablets en 2-in-1 hybriden met Modern Standby.

Een TPM kan ook worden geïntegreerd in biometrische verificatie met Windows Hello for Business. Daarnaast introduceerde Microsoft in 2019 in samenwerking met bijvoorbeeld Dell, HP en Lenovo laptops waarvan de firmware beter beschermd moet zijn tegen manipulatie (zoals door BIOS-rootkits). Deze Secured-Core-pc's gebruiken de TPM als Dynamic Root of Trust for Measurement (DRTM). Een TPM kan ook worden gebruikt voor de op virtualisatie gebaseerde beveiliging (VBS) en voor cryptografisch bewijs van

TPM EN UEFI SECURE BOOT

? Wat heeft een TPM te maken met de cryptografisch beveiligde opstartmodus UEFI Secure Boot?

! Niets. UEFI Secure Boot oftewel 'veilig opstarten', werkt ook zonder TPM. Speciale bootloaders, die bijvoorbeeld bij veel beveiligingssoftware worden toegepast, kunnen een TPM echter integreren na het booten om manipulatie van het UEFI-BIOS te detecteren (zie ook het DRTM in het voorgaande item).

TPM EN VEILIGHEID

? Zijn er bekende veiligheidsgevoelens bij het gebruik van TPM?

! In 2017 werd in TPM 1.2-chips van Infineon het veiligheidslek ROCA ontdekt in het algoritme voor het genereren van RSA-sleutels. Dat werd gedicht middels firmware-updates. Verder kwam in 2019 het veiligheidslek TPM-Fail in TPM 2.0-chips van STMicroelectronics en in fTPM-implementaties van Intel aan het licht. Ook die werden met behulp van patches gedicht. TPM-Fail had alleen betrekking op het Elliptic Curve Digital Signature Algorithm (ECDSA).

WINDOWS 11 ZONDER TPM

? Kun je de nieuwe Windows 11 ook zonder TPM gaan gebruiken?

! Dat is op het moment van schrijven nog niet helemaal duidelijk. Microsoft vereist TPM 2.0 voor een computer met het Windows 11-logo. Windows 11 kan via omwegen wel worden geïnstalleerd op systemen zonder TPM. Hoe dat uiteindelijk uitpakt is nog niet zeker.

ct