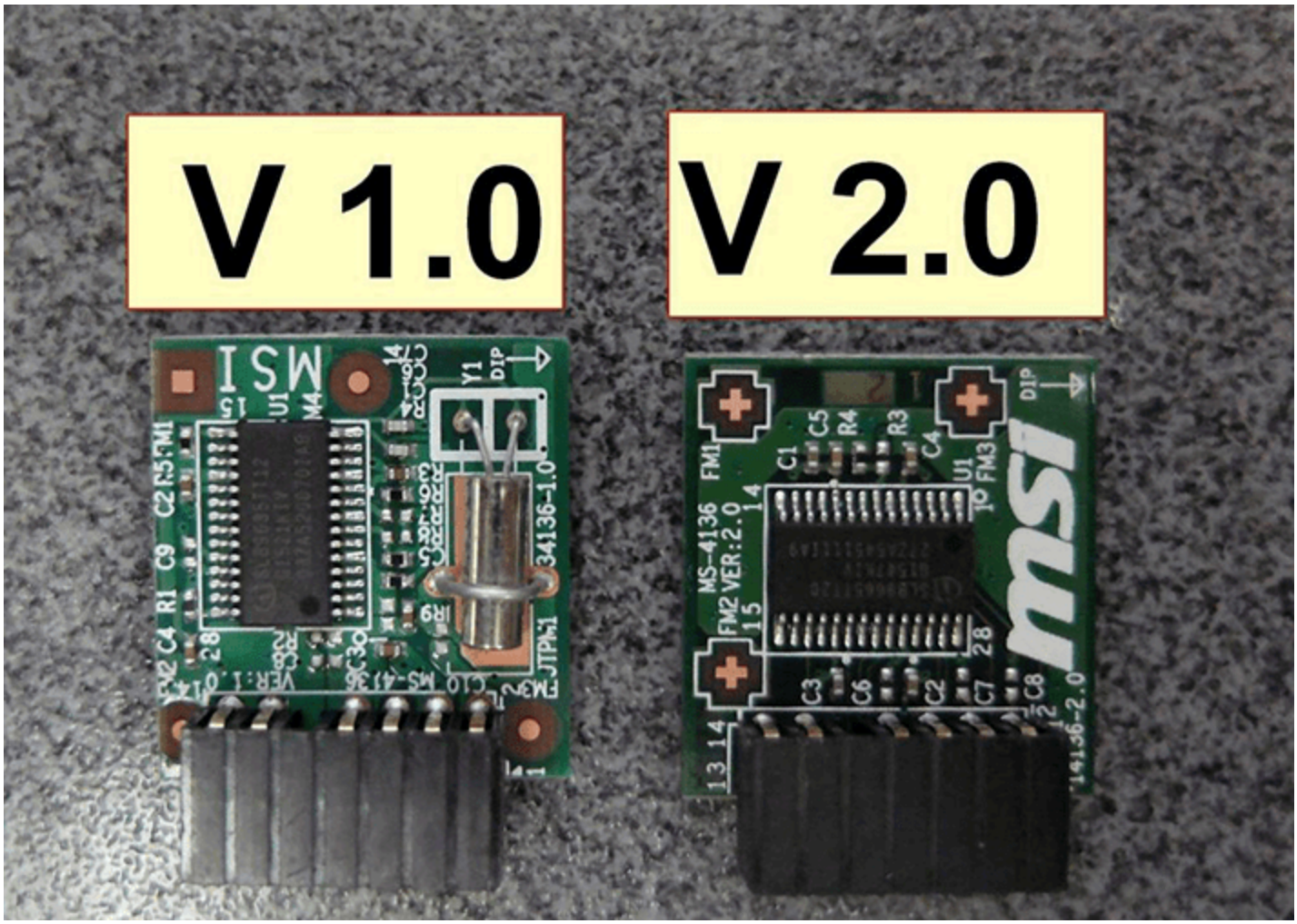
TPM là viết tắt của **T**rusted **P**latform **M**odule, nó được tích hợp trên bo mạch chủ (Mainboard) để bảo mật dữ liệu có trên máy tính.
Vâng, đó là một câu trả lời mà bạn sẽ thường thấy trên các diễn đàn công nghệ, tuy nhiên câu trả lời này chưa thực sự đầy đủ cho lắm.
Chính vì vậy mà trong bài viết này, mình sẽ giải thích thêm cho các bạn một cách đầy đủ và cặn kẽ hơn về con chip TPM này, về những câu hỏi xoay quanh TPM, ví dụ như:
TPM sử dụng và bảo mật cái gì, cách kiểm tra máy tính đã có TPM hay chưa, tại sao Windows 11 lại yêu cầu TPM 2.0, TPM 1.2 và TPM 2.0 khác nhau như thế nào….. vân vân, mây mây..

#1. Giới thiệu một chút về chip TPM

TPM được giới thiệu lần đầu tiên vào năm 2005, đây là một con chip vật lý nằm trên bo mạch chủ (hoặc có thể là nằm trong CPU) nhằm cung cấp các tính năng mã hóa và tạo ra những lớp bảo mật bổ sung cho máy tính.
TPM là con chip có khả năng tạo ra các key mã hóa và cung cấp các chức năng xác thực cho cả phần cứng lẫn phần mềm, từ đó giúp tăng cường khả năng bảo mật của máy tính.
Hiểu nôm na thì TPM là nhà máy sản xuất ổ khóa cho các hộ gia đình (software – phần mềm) và các nhà máy, xí nghiệp (hardware – phần cứng).
Các máy tính và Laptop hiện đại (được sản xuất từ năm 2018 trở lại đây) hầu hết đều có một con chip TPM được hàn sẵn trong bo mạch chủ (mainboard).
Trong trường hợp bạn tự build một chiếc máy tính, và bạn mua phải một bo mạch chủ không tích hợp sẵn TPM thì bạn hoàn toàn có thể mua một module TPM từ bên ngoài và gắn vào.
Tuy nhiên ở thời điểm hiện tại, các module TPM đều khá đắt và nếu bo mạch chủ của bạn không hỗ trợ TPM thì việc mua một module TPM chỉ làm lãng phí tiền của của bạn.
Vậy nên bạn hãy kiểm tra kỹ thông tin trước khi quyết định nâng cấp nhé, một số bo mạch chủ sẽ có đầu nối TMP, bạn chỉ cần mua thêm TPM gắn vào là xong.

Như mình có nói bên trên, chip TPM không chỉ được gắn trên bo mạch chủ, mà một số loại TPM còn có thể được tích hợp trực tiếp vào CPU.
Và cũng có một số loại khác gọi là TPM ảo không cần chip vật lí để hoạt động, mà thay vào đó, nó được tích hợp như một dạng phần mềm (software) cho máy tính. Nhưng chắc chắn là loại TPM ảo này thì mức độ bảo mật sẽ không cao.
Bạn tham khảo bài viết này để có thêm nhiều thông tin hơn về TPM nhé: TPM 2.0 trên Windows 11 là gì? và kiểm tra nó như thế nào?

#2. Sự khác nhau giữa chip TPM 1.2 và 2.0



—1—
TPM 1.2 được phát hành lần đầu tiên vào năm 2005 và nhận được bản sửa đổi cuối cùng vào năm 2011.
Trong khi đó, TPM 2.0 được phát hành lần đầu vào năm 2014 và nhận được bản sửa đổi mới nhất vào năm 2019, tính tới thời điểm mình viết bài này (2021).
Mặc dù TPM 2.0 là một phiên bản nâng cấp của TPM 2.0, nhưng TPM 2.0 không tương thích với TPM 1.2
—2—
Đối với thuật toán trên TPM 1.2 thì thuật toán SHA-1 và RSA là bắt buộc, còn thuật toán AES là tùy chọn.

Còn đối với TPM 2.0 thì thuật toán SHA-1 và SHA-256 là bắt buộc đối với hàm băm. Ngoài ra, TPM 2.0 đang sử dụng thuật toán HMAC và 128-bit AES cho các thuật toán khóa đối xứng. Sự khác biệt giữa 2 thuật toán là rất lớn, và rõ ràng là TPM 2.0 là một giải pháp an toàn hơn rất nhiều so với TPM 1.2

—3—

Về phân cấp, TPM 1.2 chỉ có phân cấp lưu trữ, trong khi đó thì TPM 2.0 có phân cấp nền tảng, lưu trữ và xác nhận.

—4—

Còn về các khóa gốc (root keys)? TPM 1.2 chỉ hỗ trợ thuật toán SRK RSA-2048, trong khi đó thì TPM 2.0 hỗ trợ nhiều khóa và thuật toán hơn trên mỗi hệ thống phân cấp.

—5—

Đối với ủy quyền (authorization) thì TPM 1.2 sử dụng thuật toán HMAC, PCR, Locality và physical presence (sự hiện diện thực tế). Trong khi đó, TPM 2.0 cung cấp các tính năng ủy quyền cũng như bảo vệ bằng mật khẩu tương tự.

—6—

Về NVRAM thì TPM 1.2 chỉ hỗ trợ dữ liệu phi cấu trúc, trong khi đó thì TPM 2.0 hỗ trợ cả: dữ liệu phi cấu trúc, bộ đếm (counter), bitmap, mở rộng (Extend), PIN pass – vượt qua mã PIN và thất bại.

=> Một lần nữa, TPM 2.0 đã cung cấp cho chúng ta hàng loạt các cải tiến đáng chú ý và rất thực tế.

Bảng so sánh về thuật toán của TPM 1.2 và TPM 2.0 hỗ trợ STT KIỂU THUẬT TOÁN TÊN THUẬT TOÁN TPM 1.2 TPM 2.0 1 Asymmetric (không đối xứng) RSA 1024 Có Không bắt buộc RSA 2048 Có Có ECC P256 Không Có ECC BN256 Không Có 2 Symmetric (đối xứng) AES 128 Không bắt buộc Có AES 256 Không bắt buộc Không bắt buộc 3 Hash (băm) SHA-1 Có Có SHA-2 256 Không Có 4 HMAC SHA-1 Có Có SHA-2 256 Không Có

#3. Ưu điểm nổi bật của TPM 2.0 so với TPM 1.2?

TPM 1.2 chỉ sử dụng thuật toán băm (Hash) SHA-1, đây có lẽ là một điểm yếu vì SHA-1 không an toàn và người ta đã chuyển sang SHA-256 từ năm 2014.

Bằng chứng của việc SHA-1 không an toàn là 2 ông lớn Google và Microsoft đã loại bỏ hỗ trợ chứng chỉ dựa trên thuật toán SHA-1 vào năm 2017.

Trong khi đó, TPM 2.0 hỗ trợ các thuật toán mới hơn, từ đó tăng mức độ bảo mật lên cao hơn. Và một số tính năng như mã hóa thiết bị, Windows Defender System Guard, Autopilot và SecureBIO chỉ sử dụng được khi máy tính có gắn chip TPM 2.0

Bảng danh sách các tính năng mà TPM 1.2 và TPM 2.0 hỗ trợ: STT TÍNH NĂNG TPM 1.2 TPM 2.0 1 Measured Boot ✓ ✓ 2 BitLocker ✓ ✓ 3 Device Encryption ✘ ✓ 4 Windows Defender Application Control ✓ ✓ 5 Windows Defender System Guard ✘ ✓ 6 Credential Guard ✓ ✓ 7 Device Health Attestation ✓ ✓ 8 Windows Hello ✓ ✓ 9 UEFI Secure Boot ✓ ✓ 10 TPM Platform Crypto Provider Key Storage Provider ✓ ✓ 11 Virtual Smart Card ✓ ✓ 12 Autopilot ✓ ✓ 13 SecureBIO ✘ ✓ 14 Certificate storage ✘ ✓

#4. TPM hoạt động như thế nào?

Chip TPM được sử dụng để bảo vệ và mã hóa dữ liệu (tạo và lưu các thành phần của khóa mã hóa – encryption keys), TPM sẽ lưu trữ thông tin bảo mật như mật khẩu, keys mã hóa và chứng chỉ bảo mật bằng phần cứng.
Điều này có nghĩa là, để mở khóa được một ổ cứng đã được mã hóa thì bạn cần phải dùng đến chính con chip TPM đã tạo ra mã khóa đấy.
Và cũng vì tính chất đặc trưng của một con chip vật lý (khóa mã hóa không được lưu trên ổ cứng) nên hacker sẽ phải vất vả hơn trong việc giải mã dữ liệu vì họ không có quyền kiểm soát chip TPM.
Các chip TPM cũng được tích hợp tính năng chống giả mạo, chính vì thế mà trong trường hợp chip và mainboard bị hacker giả mạo thì TPM vẫn có thể khóa dữ liệu của bạn bình thường.
Khi phát hiện ra virus hoặc các phần mềm độc hại trên thiết bị của bạn, TPM lập tức tự cách ly (cùng với các dữ liệu mã hóa bên trong).
TPM cũng có thể quét BIOS khi khởi động và chạy các bản test nhằm kiểm tra các phần mềm trước khi chạy nó.
TPM cũng có thể ngăn chặn khởi động máy tính và khóa máy nếu như phát hiện dữ liệu bị đánh cắp. Ngoài ra, TPM cũng có thể lưu trữ các dữ liệu sinh trắc học của Windows Hello (mở khóa bằng khuôn mặt).
Vai trò phổ biến nhất của TPM là tạo ra các key mã hóa duy nhất, một phần key sẽ được lưu trên con chip TPM đó. Từ đó, ổ cứng có key mã hóa đó sẽ không thể đọc được dữ liệu được

khi ổ cứng được cắm vào một máy tính khác. (Bitlocker yêu cầu TPM vì lí do như vậy).

#4. Lí do Windows 11 bắt buộc phải có chip TPM 2.0

Những gì ta biết hiện tại về các yêu cầu hệ thống của Windows 11 đều khá mơ hồ, kể cả về việc Microsoft liệu có hỗ trợ TPM 1.2 cho Windows 11 hay không?

Theo tài liệu mà Microsoft công bố lần đầu thì Windows 11 sẽ hoạt động với TPM 1.2 và TPM 2.0, và hiển nhiên TPM 1.2 được hỗ trợ (nhưng không được khuyến nghị).

Tuy nhiên sau đó không lâu, Microsoft đã cập nhật lại tài liệu của họ và hiện tại thì chỉ những máy có chip TPM 2.0 mới được hỗ trợ.

Hiện tại Microsoft đang rất chú trọng về bảo mật cho Windows 11. Chính vì vậy, việc yêu cầu TPM 2.0 là điều dễ hiểu. TPM 2.0 sẽ đáp ứng được các tính năng bảo mật mới nhất và hiện đại nhất của Windows 11.

Không những vậy, Microsoft cũng đã cảnh báo về các cuộc tấn công Firmware, từ đó gây ra các cuộc tấn công Ransomware gây mất mát dữ liệu cho người dùng.

Vậy nên, việc Microsoft đang nỗ lực tăng cường khả năng bảo mật cho hệ điều hành của họ là để giảm thiểu những cuộc tấn công đó và để đảm bảo cho sự an toàn của người dùng trong tương lai.

Nhưng cũng có một bộ phận người dùng cho rằng, Microsoft yêu cầu cấu hình hệ thống cao hơn chỉ là âm mưu về tài chính.

Người dùng sẽ phải từ bỏ các máy tính từ Windows 8 trở xuống và một số các máy tính chạy Windows 10 để mua các máy tính hoặc Laptop có các phần cứng hỗ trợ Windows 11.

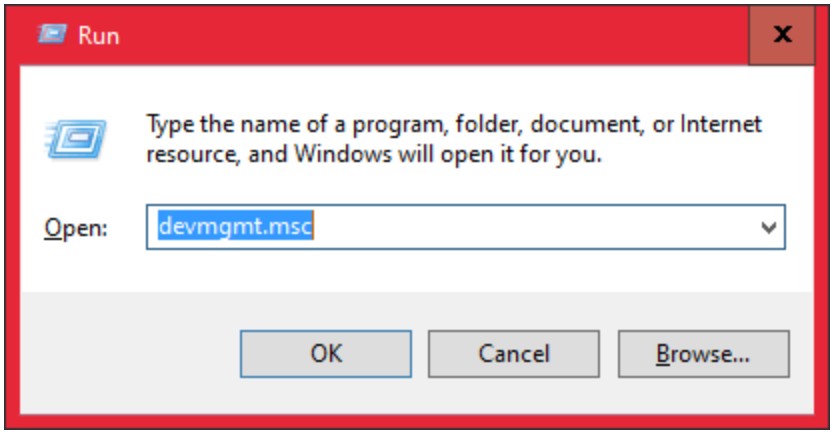
Có khả năng cao các máy tính chỉ từ 4 năm tuổi trở về trước sẽ không thể được cập nhật lên Windows 11 theo một cách chính thống.

Đồng thời việc yêu cầu phần cứng cao sẽ khiến linh kiện máy tính trở nên đắt đỏ hơn và sẽ có những người tích trữ linh kiện để bán trong khi nguồn hàng khan hiếm với giá cao khủng khiếp.

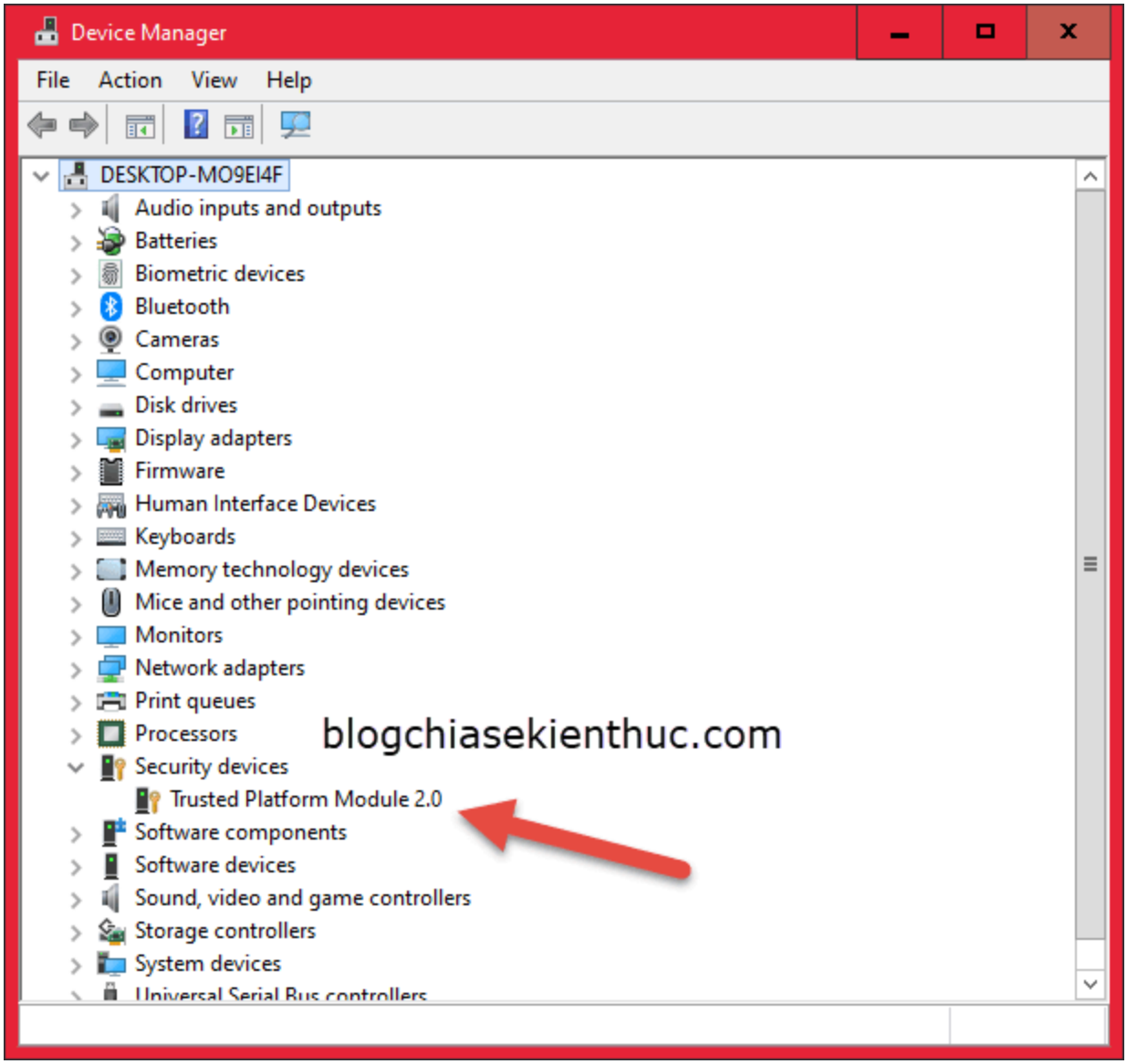
Microsoft chưa bao giờ yêu cầu phần cứng nghiêm ngặt đến vậy đối với bất kì phiên bản Windows nào trước đây. Vậy nên, giả thiết này cũng rất có thể chứ.

#5. Cách nhận biết máy tính có TPM hay không?

+ Bước 1: Mở hộp thoại Run ra (Windows + R) => và nhập lệnh devmgmt.msc => sau đó nhấn Enter.



+ Bước 2: Bạn tìm đến phần Security devices => sau đó click để xem chi tiết. Nếu là Trusted Platform Module 2.0 thì máy bạn đã đủ điều kiện về TPM rồi đó.



Nếu bạn không thấy phần Security devices thì máy tính của bạn không có TPM hoặc là TPM đang bị vô hiệu hóa trong BIOS.
Việc của bạn là kích hoạt TPM trong BIOS, để làm được điều này thì các bạn tham khảo bài viết này nhé: TPM 2.0 trên Windows 11 là gì? và kiểm tra nó như thế nào?

#6. Lời kết

Trên đây là toàn bộ những thông tin quan trọng về con chip TPM mà mình đã tổng hợp lại được.
Qua bài viết này thì bạn cũng đã thấy được **sự khác nhau giữa chip TPM 1.2 và TPM 2.0** rồi đúng không, và bạn cũng biết được lý do tại sao TPM 2.0 là yêu cầu bắt buộc để cài Windows 11 rồi..
Chúc các bạn thành công, và mong mọi người hãy cùng nhau thảo luận thêm về con chip TPM này để anh em có thêm nhiều kiến thức hữu ích khác nhé..

CTV: Hoàng Tuấn – FIFA4.NET
Edit by Kiên Nguyễn

Note: Bài viết này hữu ích với bạn chứ? Đừng quên đánh giá bài viết, like và chia sẻ cho bạn bè và người thân của bạn nhé !

https://fifa4.net/
Bài viết Sự khác nhau giữa chip TPM 1.2 và chip TPM 2.0? đã xuất hiện đầu tiên vào ngày FIFA ONLINE 4.

Nguồn: FIFA ONLINE 4
https://fifa4.net/su-khac-nhau-giua-chip-tpm-1-2-va-chip-tpm-2-0/
Xem thêm tại:
https://drive.google.com/drive/folders/1-0bVOVvGLHaDfWs3B_LKIlgWNYqgo9pF