What is TPM? – Microsoft Support

Windows · https://cleversupport.ca/docs/windows/what-is-tpm-microsoft-support/

What is TPM?

A TPM (Trusted Platform Module) is used to improve the security of your PC. It's used by services like BitLocker drive encryption, Windows Hello, and others, to securely create and store cryptographic keys, and to confirm that the operating system and firmware on your device are what they're supposed to be, and haven't been tampered with.

Typically, it's a separate chip on the motherboard though the TPM 2.0 standard allows manufacturers like Intel or AMD to build the TPM capability into their chipsets rather than requiring a separate chip.



TPM has been around for over 20 years, and has been part of PCs since around 2005. In 2016 TPM version 2.0 - the current version as of this writing - became standard in new PCs.

What's a cryptographic key?

Does my PC already have TPM?

The odds are that your PC does already have TPM, and if it's less than 5 years old you should have TPM 2.0.

To find out if your Windows 10 PC already has it go to **Start** > **Settings** > **Update and Security** > **Windows Security** > **Device Security**. If you have it, you'll see a **Security processor** section on the screen.

[Security processor details link]

Tip: If you don't see the Security processor section it may be that your device has TPM but that the TPM is turned off. To learn how to turn it on see Enable TPM 2.0 on your PC.

The next step is to find out what version of TPM your PC has. Select **Security processor details** and on the screen that appears you're looking for the **Specification version**. It should say either "1.2" or "2.0".

Important: Windows 11 requires TPM version 2.0. For more information see Windows 11 System Requirements.