Trusted Platform Module

Have you ever wondered, why your laptop is not compatible with Windows 11? It might not have the necessary security features such as, securely store encryption keys.

What about the famous bit locker used to encrypt machines mainly with windows as the main operating system?

Encryption keys are important because, they are used to keep your data secure. It's more like a password that unlocks your safe (cash safe lol!)

Where are these keys stores? Maybe in your hard? If anyone get access to your hard drive or ram, they will your "password" or your keys.

TPM chip provides an additional layer of security by storing encryption keys and other sensitive data, which makes it harder for attackers to access them.

TPM (Trusted Platform Module) is a chip that is designed specifically for cryptographic security functions. It can encrypt and decrypt keys when needed, but it also provides a secure place to store them.

Some of the advantages of using the TPM chip include improved security, controlled access to sensitive data, and enhanced authentication. Windows 11 uses the TPM chip for controlling and authenticating access to the operating system and other sensitive data. This means that when you log in to your computer, Windows can check to make sure that the TPM is present and that it hasn't been tampered with. This helps to prevent unauthorized access to your data.

Practical Applications

When a file or disk is encrypted with BitLocker, the encryption key is stored on the TPM chip. When the user wants to access the file or disk, the TPM chip decrypts the key and provides it to the operating system. This process ensures that the encryption key is secure and cannot be easily accessed by attackers.

There are different versions of the TPM, including ones made by IBM and Intel.

As per the timing for this article TPM is in version. 2.0. But they all serve the same purpose - to provide a secure place to store encryption keys and to help keep your data safe.

In summary, the TPM chip provides an additional layer of security and helps improve the overall security of the operating system and sensitive data. The TPM chip is required for Windows 11 compatibility and helps in encrypting and decrypting the BitLocker key.