Microsoft Lists Why TPM, Secure Boot Are Mandatory on Windows 11

More than three years ago, when Microsoft announced Windows 11, the operating system immediately caused a lot of controversy.

When Microsoft announced Windows 11 more than three years ago, it was immediately controversial. Not only because of its unconventional interface, but also because of its high hardware requirements, which left many systems unable to run Windows 11 properly, such as TPM and Secure Boot.

Microsoft has repeatedly explained why features like TPM (Trusted Platform Module) 2.0, VBS (Virtualization-based Security), and Secure Boot are important for Windows 11 PCs. Microsoft requires that users' PCs support these features in order to use Windows 11, because of the enhanced security benefits they provide, and has released visual demos to better explain how these features work.

Recently, with the Windows 11 24H2 feature update, Microsoft updated one of the support articles on its official website titled 'Automatic Device Encryption via BitLocker', which Microsoft calls "Auto-DE". Notably, the document mentions why TPM and Secure Boot are required for Device Encryption.

Below is the content of the supporting document before being edited.

> Why is Device Encryption not available?
>
> Here are the steps to determine why Device Encryption might be unavailable:
>
> 1. From the Start menu, type System Information, right-click System Information in the results list, and then select Run as administrator.
>
> 2. In the System Summary - Item list, look for the value Automatic Device Encryption Support or Device Encryption Support.
>
> 1. The value provides the reason why Device Encryption cannot be enabled.
> 2. If the value shows Meets prerequisites then Device Encryption is currently available on your device.

And here is the content of the supporting document after it has been edited.

Why is Device Encryption not available?

Here are the steps to determine why Device Encryption might be unavailable:

1. From the Start menu, type System Information, right-click System Information in the results list, and then select Run as administrator.

2. In the System Summary - Item list, look for the value Automatic Device Encryption Support or Device Encryption Support.

The value describes the support status of Device Encryption:

1. Meets prerequisites: Device Encryption available on your device
2. TPM is not usable: Your device does not have a Trusted Platform Module (TPM), or TPM is not enabled in the BIOS or UEFI.
3. WinRE is not configured: Your device does not have Windows Recovery Environment configured.
4. PCR7 binding is not supported: Secure Boot is disabled in BIOS/UEFI, or you have peripherals connected to your device during boot (such as a dedicated network interface, docking station, or external graphics card)

The article basically details what those missing 'prerequisites' are. They include TPM, WinRE (Windows Recovery Environment), and Secure Boot.

Additionally, Microsoft also mentioned PCR7. PCR, or Platform Configuration Register, is a memory location on the TPM that is used to store hashing algorithms. PCR profile 7, or PCR7, is what BitLocker binds to. This binding ensures that the cryptographic key, in this case the BitLocker key, is only loaded during a certain time during the boot process, not before or after.

This is where Secure Boot comes into play as it verifies and authenticates the required Microsoft Windows PCA 2011 certificate during boot, as an invalid signature will result in BitLocker using profiles other than 7.

The resurgence of interest in BitLocker and encryption on Windows 11 24H2 came about recently when the Redmond giant unexpectedly lowered the OEM requirements for Auto-DE on the latest version of Windows, so that even home PCs can be automatically encrypted. Shortly after, the company also released a handy backup and recovery guide for BitLocker keys.

Not long ago, Microsoft also reaffirmed TPM 2.0 as a non-negotiable standard on its operating systems.