

# BitLocker Drive Encryption

**BitLocker** je proprietární technologie pro šifrování celých diskových oddílů (Full Disk Encryption – FDE), kterou vyvinula společnost Microsoft. Je integrována do profesionálních verzí systému Windows (Pro, Enterprise, Education).

Hlavním účelem BitLockeru je zabránit neoprávněnému přístupu k datům v případě, že je počítač ztracen, odcizen nebo neodborně vyřazen. Chrání data tím, že celý obsah disku transformuje do nečitelné podoby, kterou lze dešifrovat pouze pomocí správného klíče.

## Jak BitLocker funguje?

BitLocker používá šifrovací algoritmus **AES** (Advanced Encryption Standard) s délkou klíče 128 nebo 256 bitů.

## Role čipu TPM

Většina moderních instalací BitLockeru spoléhá na hardware zvaný **TPM (Trusted Platform Module)**.

- TPM je specializovaný čip na základní desce, který bezpečně uchovává šifrovací klíče.
- Při startu počítače TPM zkontroluje, zda nebyl hardware nebo spouštěcí soubory systému změněny (např. útokem typu **bootkit**).
- Pokud je vše v pořádku, čip uvolní klíč a systém se automaticky dešifruje a spustí.

## Režimy autentizace

BitLocker lze nakonfigurovat několika způsoby podle požadované úrovně zabezpečení:

- **Transparentní režim (Pouze TPM):** Uživatel si ničeho nevšimne. Počítač nastartuje přímo k přihlašovací obrazovce Windows. Data jsou chráněna proti vyjmutí disku a čtení v jiném PC.
- **Uživatelský PIN:** Při každém startu PC musí uživatel zadat číselný PIN předtím, než se začne načítat Windows. Toto je nejbezpečnější metoda (dvoufaktorová ochrana: „mám hardware“ + „znám PIN“).
- **USB klíč:** Šifrovací klíč je uložen na flash disku, který musí být připojen k PC během startu.

# BitLocker To Go

Tato funkce umožňuje šifrovat přenosná média, jako jsou **externí pevné disky** a **USB flash disky**.

- Na rozdíl od systémového disku se zde k dešifrování používá heslo.
- Takto zašifrovaný disk lze číst i na jiných počítačích se systémem Windows po zadání správného hesla.

## Obnovovací klíč (Recovery Key)

Při aktivaci BitLockeru je vygenerován 48místný **klíč pro obnovení**. Je to kriticky důležitý údaj pro případ, že:

- Dojde k poruše čipu TPM.
- Zapomenete PIN.
- Dojde k významné změně hardwaru (např. výměna základní desky).

Bez tohoto klíče jsou data na disku trvale a nenávratně ztracena. Microsoft umožňuje uložení tohoto klíče do uživatelského účtu Microsoft v cloudu.

## Výhody a nevýhody

| Výhody  | Nevýhody   |
|---|--|
| <b>Vysoká bezpečnost:</b> Data jsou nečitelná bez klíče.                        | <b>Výkon:</b> Mírné zpomalení diskových operací (u moderních SSD téměř nezatelné). |
| <b>Integrace:</b> Je součástí OS, není třeba instalovat software třetích stran. | <b>Riziko ztráty:</b> Ztráta obnovovacího klíče znamená definitivní ztrátu dat.    |
| <b>Ochrana integrity:</b> Detekuje pokusy o manipulaci s bootloaderem.          | <b>Dostupnost:</b> Není součástí základní verze Windows Home.                      |

*Související pojmy: TPM, AES, Encryption, SSD, Bootkit, Windows Pro, UEFI.*

From:  
<https://serviceit.cz/> - IT ENCYKLOPEDIIE

Permanent link:  
<https://serviceit.cz/doku.php?id=bitlocker>

Last update: **2025/12/31 19:18**

