

# Adatok titkosítása

## Rendszerlemez titkosítása BitLocker segítségével

- 1. Telepítse fel a Windows 7 Enterprise verzióját. A telepítés közben törölje a meglévő partíciókat, majd az üres diszket válassza ki a telepítésre.
- 2. A titkosítás során nem használunk TPM-et, ezért annak kötelező használatát ki kell kapcsolni a következő módon:
  - a. A telepítés után belépve indítsa el a Group Policy Editort a gpedit.msc begépelésével.

		[e	E E
😋 🔍 🗣 🏘 « All Control Panel It	terns + BitLocker Drive Encryption		Q
Control Panel Home	Help protect your files and folde BitLocker Drive Encryption helps prevent below. You are able to use the computer	ers by encrypting your drives unauthorized access to any files stored on the driv normally, but unauthorized users cannot read or u	es shown se your files.
Programs (1)	What should I know about BitLocker Drive we Encryption - Hard Disk Dri	e Encryption before i turn it on? Wes	
₽ See more results	ive Encryption - BitLocker To gvable drive to use BitLocker	Go To Go.	
gpedit.msd × Log off			
🚯 🎓 🚞 🔍 🐺			H9 ( <b>** 10</b> )

 b. Az editorban keresse meg a "Computer Configuration \ Administrative Templates \ Windows Components \ Bit Locker Drive Encryption \ Operating System Drives" pontot.





c. Állítsa "Enabled"-re a "Require additional authentication at startup"-ot.

Require additional authentication at	startup	Previous Setting
Not Configured Comment     Enabled     Disabled     Supported on:	Windows 7 fan	nay
Options:		Help:
Allow BitLocker without a compatible (requires a startup key on a USB flash dri Settings for computers with a TPM: Configure TPM startup PIN: Allow TPM • Configure TPM startup PIN: Allow startup PIN with TPM Configure TPM startup key: Allow startup key with TPM Configure TPM startup key and PIN: Configure TPM startup key and PIN:	e TPM *	This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker. Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs. If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode a USB drive is required for start-up and the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is subtencicated and the drive is accessible. Jith USB key is lost or unavailable you will need to use one of the BitLocker recovery options to access the drive. Con a computer with a compatible TDM four types of
relow startup key and PIN with TPM		authentication methods can be used at startup to provide added

- d. Tanulmányozza át a lehetséges beállításokat.
- 3. BitLocker segítségével titkosítsa le a rendszerlemezt:
  - a. Indítsa el a "Control Panel"-t.



b. Indítsa el a BitLocker-t.



#### Hálózatok biztonsága

Széchenyi István Egyetem

Távközlési Tanszék

Control Panel + All Cont	trol Panel Items		4. 50	irch Control Parnel	0.0
			1.1		
Adjust your computer's settings				View by: Small icons	•
Action Center	Administrative Tools		autoPlay		
Backup and Restore	RELocker Drive Encrypt	ion 5	Color Ma	inagement	
Credential Manager	Date and Time	BitLocker Drive Er	cryption	pgrams	
Desktop Gadgets	Device Manager	Protect your com	puter using	d Printers	
Display	SEase of Access Center	Distantis Inite D	Folder Og	ptions	
A Fonts	- Getting Started		HomeGri	que	
A Indexing Options	🐑 Internet Options		Keyboard	1	
108 Location and Other Sensors	@ Mouse	5	Network	and Sharing Center	
Notification Area Icons	B Parental Controls		Performa	nce Information and To	ools
Personalization	Phone and Modern	2	Power Or	ptions	
Programs and Features	P Recovery	\$	Region a	nd Language	
RemoteApp and Desktop Connections	Sound	4	Speech R	ecognition	
Sync Center	👯 System	1	Taskbar a	and Start Menu	
Troubleshooting	& User Accounts		Windows	CardSpace	
Mil Windows Defender	Windows Firewall	2	Windows	Update	

c. Kapcsolja be a BitLocker-t.

🖉 🖉 🗣 🕊 All Control Pa	nel Items 🔸 BitLocker Drive Encry	ption	+ 4g	Search Control Panel	
Control Panel Home	Unio exetudi unus Ele	and fold on her			
	Help protect your file	Help protect your files and folders by encrypting your drives			
	BitLocker Drive Encryption below. You are able to use t	helps prevent unauthor the computer normally	, but unas	ss to any files stored on t uthorized users cannot re	the drives shown ad or use your file
	What should I know about	BitLocker Drive Encrypt	ion befor	eltum it on?	
	BitLocker Drive Encryption	- Hard Disk Drives			
	Ci Off	-	Jum O	n Bitlocker	
	BitLocker Drive Encryption	- BitLocker To Go			
	Insert a removable drive to	use BitLocker To Go.			
See alto					
TPM Administration					
Disk Management					
Read our privacy statement					

d. Válassza a "Require a Startup key at startup" pontot. E pont kiválasztása esetén minden bootolást megelőzően USB kulcsot kér a rendszer, melyen a diszk titkosításához használt kulcs található.

The second	
BitLocker Drive Encryption (C:)	
Set BitLocker startup preferences	
This computer does not appear to have a TPM. To use BitLocker Drive flash drive will be required every time you start the computer.	Encryption, a startup key on a USB
$\bar{\diamondsuit}$ Use BitLocker without additional keys	
Require a <u>PIN</u> at every startup	
<ul> <li>Require a Startup key at every startup</li> </ul>	
<ol> <li>Some settings are managed by your system administrator.</li> </ol>	
What is a BitLocker Drive Encryption startup key or PIN?	
	Cancel





Széchenyi István Egyetem Győr Távközlési Tanszék

- e. Értelemszerűen haladjon tovább.
- f. Ha végzett, indítsa újra számítógépét, figyelje meg a rendszerindítás folyamatát, belépés után tanulmányozza a pendrive tartalmát.

# Pendrive titkosítása BitLocker To Go segítségével

- 1. Egy üres pendrivera másoljon fel néhány tetszőlegesen kiválasztott állományt.
- 2. A Control panelen válassza ki a BitLocker-t.
- 3. A BitLocker To Go segítségével titkosítsa le a pendrive tartalmát.
- 4. Ha elkészült a titkosítás, távolítsa el a pendriveot.
- 5. Csatlakoztassa újra a pendriveot, eközben figyelje meg a rendszer viselkedését.
- 6. Nézze meg, hogy a pendriveon megtalálhatóak-e a felmásolt állományok.
- 7. Próbálja ki szomszédjával is az ő számítógépén a pendrive működését.
- 8. Lépjen ki "Command prompt"-ba.
- 9. A manage-bde -status parancs segítségével kérdezze le a titkosított diszkek állapotát, és a titkosítás módját.
- 10. Sikerült a lekérdezés? Oldja meg a problémát.

## Titkosított konténer létrehozása TrueCrypt segítségével

- 1. Töltse le a TrueCrpyt 7.1a verzióját a https://www.grc.com/misc/truecrypt/truecrypt.htm oldalról.
- 2. Telepítse a letöltött programot.
- 3. Indítsa el a feltelepített programot Administratorként.
- 4. Klikklejen a "Create Volume" gombra, majd tanulmányozza a felkínált lehetőségeket.
- 5. Válassza a "Create an encrypted file container" menüpontot, majd "Next".
- 6. Tanulmányozza a felkínált lehetőségeket.
- 7. Válassza a "Standard TrueCrypt volume" menüpontot, majd "Next".
- 8. Válasszon tetszőleges nevet a container részére, és a C:\ könyvtárban helyezze el.
- 9. Tanulmányozza a felkínált titkosítási algoritmusokat (leírásukkal együtt).
- 10. Tanulmányozza a felkínált hash algoritmusokat.
- 11. Válassza ki az "AES-Twofish-Serpent" titkosítást, majd "Next".
- 12. Méretnek 1GB-t állítson be, majd "Next".
- 13. Tanulmányozza, a megjelenő leírást, majd válasszon tetszőleges jelszót, majd "Next".
- 14. Figyelje meg a titkosítás sebességét.
- 15. Tallózza ki a létrehozott Containert tartalmazó állományt, majd a "Mount" gomb segítségével csatolja fel azt tetszőleges meghajtónak.
- 16. A "Volume Properties…" gomb segítségével tanulmányozza a meghajtó titkosítását.
- 17. "Dismount All" segítségével csatoljon le minden titkosított Containert.