

Adatok titkosítása

Rendszerlemez titkosítása BitLocker segítségével

- 1. Telepítse fel a Windows 10 pro 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 segítségével.

Necycle bill				
	💻 🖸 📕 🖛	Manage This PC	— E	- ×
	File Computer V	iew Drive Tools		~ 🕐
	← → ~ ↑ 💻 > Th	nis PC	v ひ Search This PC	Q
Microsoft				
Euge	🖈 Quick access	V Folders (7)		
	📃 Desktop 🛛 🖈	3D Objects	Desktop	
	👆 Downloads 🛛 🖈			
BitLocker	🔮 Documents 🛛 🖈	Documents	Downloads	
ecovery Ke	📰 Pictures 🛛 🖈			
	Music	Music	Pictures	
	Videos			
	a OneDrive			
	This PC	Videos		
	USB Drive (E:)	 Devices and drives (3) 		
	Network	Local Disk (C:)	CD Drive (D:) ESD-ISO	
	-	38.9 GB free of 49.4 GB	0 bytes free of 6.74 GB	
		(E:)		
🖅 Run		× (
Type the resource,	name of a program, folder, do , and Windows will open it for y	cument, or Internet		
Open: gpedit.n	nsc	~		
				811 📰
	OK Cancel	Browse		
- P =	e 📄 🔒	<	Å ∧ ₪ ₽	(小) ENG HU に

 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.
 Kapcsolja be az "Allow BitLocker without a compatible TPM"-et.
 A "Configure TPM startup:" pontban válassza ki a "Do not allow TPM"-et!

Hálózatok biztonsága



SZÉCHENYI ISTVÁN EGYETEM

Távközlési Tanszék

Require additiona	l authentication a	startup									×
Require additiona	l authentication a	t startup			Previous S	etting	Ne	ext Setting	3		
O Not Configured	Comment:										^
Enabled											
 Disabled 											\sim
	Supported on:	At least Win	dow	s Server 2008	R2 or Wind	ows 7					^
											~
Options:				Help:							
Allow BitLocker (requires a passwoi USB flash drive) Settings for computer Configure TPM startup Do not allow TPM Configure TPM startup Allow startup PIN wit Configure TPM startup Allow startup key wit Configure TPM startup Allow startup key and C	s with a TPM: p: p PIN: h TPM p key: h TPM p key: h TPM p key and PIN: 4 PIN with TPM	v v	•	requires ad and whethe Platform M I urn on Bit Note: Only required at If you want select the ", box. In this start-up. W encrypt the When the L authenticat unavailable need to use drive. On a comp	titional authors odule (TPM) occker. one of the astartup, other to use BitLo Allow BitLoc mode either hen using a : drive is stor SB key is ins ed and the d or if you have one of the E	dditional envise a p cker on a ker witho a passwo startup ke erted the trive is ac ve forgot BitLocker ompatibl	authe olicy se authe olicy com out a co ord or ey, the uUSB acce cessib ten th recov	h time think with or with entication error occ puter with compatibl a USB dri- e key info drive, cre ss to the co- ple. If the le passwo rery optio	not a com hout pplied optic urs. nout a le TPN ve is r rmatin ating trive i USB k ord the ns to	a TPM, a TPM, a TPM, a TPM, M" check required on used a USB ke is ey is lost en you w access th	for to y. or ill ne
			-				_				
						OK		Cano	el	Ap	ply

- d. Tanulmányozza át a lehetséges beállításokat.
- 3. BitLocker segítségével titkosítsa le a rendszerlemezt:
 - a. Jobb gomb a rendszerköteten, majd "Turn on BitLocker".



- b. Indítsa el a BitLocker-t.
- c. Válassza ki a kívánt indításkori hitelesítési módot!



e. Nyomtassa ki egy PDF állományba a visszaállítási kulcsot! (Próbálja meg pendrivera is lementeni!)

÷	RitLocker Drive Encryption (C:)
	How do you want to back up your recovery key?
	Some settings are managed by your system administrator.
	A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.
	ightarrow Save to your Microsoft account
	ightarrow Save to a USB flash drive
	ightarrow Save to a file
	\rightarrow Print the recovery key

- f. Értelemszerűen haladjon tovább.
- g. Ha végzett, indítsa újra számítógépét, figyelje meg a rendszerindítás folyamatát, belépés után tanulmányozza a pendrive tartalmát.
- h. Kapcsolja ki a rendszerlemez titkosítását!

Pendrive titkosítása BitLocker To Go segítségével

- 1. Egy üres pendrivera másoljon fel néhány tetszőlegesen kiválasztott állományt.
- 2. Válassza ki a pendriveot, majd jobb klikk és "Turn on BitLocker"!



3. A BitLocker To Go segítségével titkosítsa le a pendrive tartalmát (jelszó használatával)!

USB Drive (E: 57.1 GB free of 57.6 GB

Properties

矂 BitLocker Drive Encryption (E:)					
Choose how you wan	t to unlock this drive				
Use a password to unlock	the drive				
Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.					
Enter your password	•••••				
Reenter your password	•••••				
Use my smart card to uni You'll need to insert your	ock the drive smart card. The smart card PIN will be required when you unlock the dri				

4. A helyreállítási kulcsot mentse le az asztalra!

🙀 BitLocker Drive Encryption (E:)				
How do you want to back up your recovery key?				
Some settings are managed by your system administrator.				
If you forget your password or lose your smart card, you can use your recovery key to access your drive.				
\rightarrow Save to your Microsoft account				
ightarrow Save to a file				
\rightarrow Print the recovery key				

- 5. Ha elkészült a titkosítás, távolítsa el a pendriveot.
- 6. Csatlakoztassa újra a pendriveot, eközben figyelje meg a rendszer viselkedését.
- 7. Nézze meg, hogy a pendriveon megtalálhatóak-e a felmásolt állományok.
- 8. Próbálja ki szomszédjával is az ő számítógépén a pendrive működését.
- 9. Lépjen ki "Command prompt"-ba.
- 10. A manage-bde -status parancs segítségével kérdezze le a titkosított diszkek állapotát, és a titkosítás módját.
- 11. Sikerült a lekérdezés? Ha nem, oldja meg a problémát.
- 12. Szüntesse meg a pendrive titkosítását!

Titkosított konténer létrehozása VeraCrypt segítségével

1. Töltse le a VeraCrpyt legfrissebb verzióját a https://www.veracrypt.fr oldalról.

Hálózatok biztonsága





Széchenyi István Egyetem

- Távközlési Tanszék
 - VeraCrypt Free Open : X Start + v - X
 A https://www.veracryptfr/my/Downloads.html
 A btps://www.veracryptfr/my/Downloads.html
 A btps://www.veracryptfr/my/Downloads.html
 A btps://www.veracryptfr/my/Downloads.html
 A btps://www.veracryptfr/my/Downloads.html
 A btps://www.veracryptfr/my/Downloads.html
 A btp://www.veracryptfr/my/Downloads.html
 Matcoss:
 Immass:
 Immass
- 2. Telepítse a letöltött programot.
- 3. Indítsa el a feltelepített programot Administratorként.
- 4. Klikklejen a "Create Volume" gombra, majd tanulmányozza a felkínált lehetőségeket.

🐱 VeraCrypt Volume Creation Wizard	– 🗆 X		
in this in the second second	VeraCrypt Volume Creation Wizard	× VersCrypt —	×
	Create an encrypted file container	Volumes System Favorites Tools Settings Help Homes	793e
	Creates a virtual encrypted disk within a file. Recommended for inexperienced users.	Drive Volume Size Encryption Algorithm Type	^
The second		i G:	
and the state of t	O Encrypt a non-system partition/drive	mi Ht	
	Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.		
	\bigcirc Encrypt the system partition or entire system drive	M:	
VeraCrypt	Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.	Caste Volume Traper tes When Caster Volume Traper tes	~
	More information about system encryption	VenCost Select Dir Select Dir Select Dir	
	Help < Back Next > Cancel	Mount Devices Digmount All Egit	

- 5. Válassza a "Create an encrypted file container" menüpontot, majd "Next".
- 6. Tanulmányozza a felkínált lehetőségeket.
- 7. Válassza a "Standard VeraCrypt volume" menüpontot, majd "Next".
- 8. Válasszon tetszőleges nevet a container részére, és a pendriveon helyezze el.
- 9. Tanulmányozza a felkínált titkosítási algoritmusokat (leírásukkal együtt).
- 10. Tanulmányozza a felkínált hash algoritmusokat.
- 11. Válassza ki az "AES" titkosítást, majd "Next".
- 12. Méretnek 1GB-t állítson be, majd "Next".
- 13. Válasszon jelszót!

VeraCrypt	Volume Password Password: Confirm: Display password Display password Display password Display password Display password State of the third state of the the the the the third state of the
	Help < Back Next > Cancel



14. Az egér mozgatásával segítse a véletlenszámgenerálás folyamatát, majd "Format"!

	Volume Format Options Filesystem FAT v Cluster Default v Dynamic
	Random Pool: -//**/, -+/.++//-, +++*/-*, +**/ Header Key: Master Key:
VeraCrypt	Done Speed Left DPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
	Randomness Collected From Mouse Movements

- 15. Figyelje meg a titkosítás sebességét.
- 16. Tallózza ki a létrehozott Containert tartalmazó állományt, majd a "Mount" gomb segítségével csatolja fel azt tetszőleges meghajtónak.
- 17. A "Volume Properties…" gomb segítségével tanulmányozza a meghajtó titkosítását.
- 18. "Dismount All" segítségével csatoljon le minden titkosított Containert.