# Hard disk encryption

## General

Please note the difference between password, PIN and extended PIN.

- **Password**: Passwords are used to refer to authentication of the user to the system **without** using **TPM**.
- **PIN/Extended PIN**: The term PIN is used when the user is authenticated to the system **with** the use of TPM.
  - **PIN:** Numbers from 0-9
  - **Extended PIN:** Various characters (upper and lower case letters, symbols, characters, spaces)

At Jade University, BitLocker is offered for **systems without a connection to the Active Directory** - i.e. primarily for mobile devices.

## **Preparations**

- 1. Back up your personal data or the system!
- 2. Is the computer used by one or more persons?
  - Recommendation for single use: Unlock the drive with a password (see below).
  - Recommendation for use by several people: Unlock the drive with a USB memory stick (see below).
- 3. Assign password for local Windows account, if not already done
- 4. Update the operating system to the latest version (Windows update)
- 5. Check the TPM status in BIOS/UEFI **Please activate!** Depending on the model, the display in the BIOS/UEFI may differ.
  - Call up BIOS/UEFI on Dell: F2

PPI Bypass for Enable Commands PPI Bypass for Disable Commands PPI Bypass for Clear Command Olisabled Enabled	Attestation Enable Key Storage Enable SHA-256
PPI Bypass for Enable Commands PPI Bypass for Disable Commands PPI Bypass for Clear Command O Disabled Enabled	Attestation Enable  Key Storage Enable  SHA-256
PPI Bypass for Disable Commands PPI Bypass for Clear Command O Disabled Enabled	C Key Storage Enable
PPI Bypass for Disable Commands  PPI Bypass for Clear Command  Disabled  Enabled	C Key Storage Enable
PPI Bypass for Clear Command  Disabled  Enabled	P SHA-256
PPI Bypass for Clear Command  Disabled  Enabled	D SHA-256
Disabled     Enabled	
Disabled     Enabled	
Enabled	
Enabled	
This option lets you control whether the Truste	d Platform Module (TPM) Endorsement Hierarchy is availabl
operations	restricts the ability to use the TPM for signing and signature
operations.	
Key Storage Enable :	
This option lets you control whether the Truste	d Platform Module (TPM) Storage Hierarchy is available to th
operating system. Disabling this setting restrict	ts the ability to use the TPM for storing owner data.
SHA-256 : This setting controls the type of bash algorithm	that is used by the TBM. When this option is checked, the
BIOS and the TPM will use the SHA-256 bash a	gorithm to extend measurements into the TPM PCRs during
BIOS boot. When this option is unchecked, the	BIOS and the TPM will use the SHA-1 hash algorithm. This
setting should be left in the default configuration	on (checked) under most circumstances.
Disabled/Enabled :	- The second sec
bisabled - when this option is selected, the	e TPM will be disabled. It will not execute any commands
information.	area nor this is anothing access to stored office
Enabled = When this option is selected, the	e TPM will be enabled. This is the normal operating state for
the TPM when you want to use	its complete array of canabilities
	the complete analy of capabilities.
	to the operating system. Disabiling this setting operations. Key Storage Enable : This option lets you control whether the Truste operating system. Disabiling this setting restrict SHA-256 : This setting controls the type of hash algorithm BIOS and the TPM will use the SHA-256 hash a BIOS boot. When this option is unchecked, the setting should be left in the default configuratis Disabled/Enabled : Disabled = When this option is selected, th hast require the use of TPM reso information.

0

					HPC
-	TPM Embedded Secu	rity			Þ
	TPM Specification Ve	rsion	2.0		~
	TPM Device		Available 💙 💿		
	TPM State 🕢				
	Clear TPM		On next boot		
	TPM Activation Polic		No prompts		
lupl	BIOS/UEFI on Ler	10vo: F1, F2	or ESC (depending o	ın model)	
l up I	BIOS/UEFI on Ler	10vo: F1, F2 ecurity Ch	or ESC (depending o Security	in model)	em Specific Hel
up Secu Secu	BIOS/UEFI on Ler S rity Chip Type rity Chip	novo: F1, F2 ecurity Ch	or ESC (depending o Security ilp TPM 2.0 (Enabled)	on model) Ite IEnal Secur funct	em Specific Hel blel rity chip is
up Secu Secu	BIOS/UEFI on Ler S Trity Chip Type Trity Chip	novo: F1, F2 ecurity Ch	or ESC (depending o Security 11p TPH 2.0 (Enabled)	on model) Ita IEnal Secur funct	em Specific Hel ble] rity chip is tional.
up Secu Secu Clea	BIOS/UEFI on Ler S rity Chip Type rity Chip rity Reporting ar Security Ch	novo: F1, F2 Recurity Ch	or ESC (depending o Security ilp TPM 2.0 (Enabled) (Enter]	on model) Ite IEnal Secur funct IDisa Secur hidde	em Specific Hel ble] rity chip is tional. bled] rity chip is m and is not
up Secu Secu Secu Int	BIOS/UEFI on Ler S Trity Chip Type Trity Chip Trity Reporting The Security Chip an Security Chip	ovo: F1, F2 ecurity Ch g Options ip ture	or ESC (depending o Security ip TPH 2.0 (Enabled) (Enter] (Disabled]	on model) Ite IEnal Secur funct IDisa Secur hidde funct	em Specific Hel ble] rity chip is tional. bled] rity chip is m and is not ional.
up Secu Secu Clea Int Phy	BIOS/UEFI on Ler S rity Chip Type rity Chip arity Reporting ar Security Ch el (R) TXT Fear sical Presence	novo: F1, F2 Security Ch g Options ip ture for Clear	or ESC (depending o Security ip TPM 2.0 (Enter] (Enter] (Disabled] (Disabled]	on model) Ite IEnal Secur funct Disa Secur hidde funct	em Specific Hel bleJ rity chip is tional. bledJ rity chip is en and is not tional.
up Secu Secu Secu Secu Phy	BIOS/UEFI on Ler S rity Chip Type rity Chip rity Reporting ar Security Ch el (R) TXT Feat sical Presence	novo: F1, F2 Security Ch g Options ip ture for Clear	or ESC (depending o Security ip TPM 2.0 (Enabled) (Enter] (Disabled) (Disabled)	on model) It IEnal Secur funct Disa Secur hidde funct	em Specific Hel bleJ rity chip is tional. bledJ rity chip is en and is not tional.

- 6. Adjust local group policies for BitLocker (see below)
- 7. Create a password/PIN for BitLocker
- 8. Have USB stick ready for the decryption key (only very small storage capacity required)
  - For authentication via USB stick another USB stick is required

## Setup

### Adjustment of local group policies

Procedure:

1. open the local group policies by entering gpedit.msc in the Windows search mask. Then expand to

the folder Computerkonfiguration (ENG: "Computer Configuration")  $\rightarrow$  Administrative Vorlagen (ENG: "Administrative Templates")  $\rightarrow$  Windows-Komponenten (ENG: "Windows Components")  $\rightarrow$  BitLocker Drive Encryption (ENG: "BitLocker Laufwerksverschlüsselung"). Next, click on Betriebssystemlaufwerke (ENG: "Operating System Drives").

2. under Operating System Drives, double-click to open "Zusätzliche Authentifizierung beim Start anfordern" (ENG: "Request additional authentication at startup").



3. activate the option and make sure that "BitLocker ohne kompatibles TPM zulassen (...)" (ENG: "Allow BitLocker without compatible TPM (...)") **no** check mark is set. Now accept the selection and confirm with "OK".

Zusätzliche Authent	tifizierung beim Sta	rt anfordern			-		$\times$
Zusätzliche Authen	tifizierung beim Sta	rt anfordern		Vorherige Einstellung	Nächste Eins	tellung	
<ul> <li>Nicht konfiguriert</li> <li>Aktiviert</li> <li>Deaktiviert</li> </ul>	Kommentar:						×
	Unterstützt auf:	Mindestens	Windows Ser	ver 2008 R2 oder Windows	;7		< >
Optionen:			Hilfe:				
BitLocker ohne komp ein Kennwort oder ein Systemstartschlüssel Einstellungen für Compu TPM-Start konfigurieren TPM-Systemstart-PIN ko	atibles TPM zulasse n USB-Flashlaufwer erforderlich) uter mit einem TPM : TPM zulassen onfigurieren:	n (hierfür ist k mit	Mit dieser F BitLocker b Authentifiz TPM (Trust Richtliniene angewende Hinweis: Be Authentifiz Pichtliniene	Richtlinieneinstellung könr ei jedem Computerstart ei ierung erfordert und ob Sie ed Platform Module) verw einstellung wird bei Aktivie et. eim Start kann nur eine der ierungsoptionen erforderli	nen Sie konfigur ine zusätzliche e BitLocker mit d renden. Diese erung von BitLoo r zusätzlichen ich sein, da ande	ieren, ob oder ohne cker ernfalls ein	
Systemstart-PIN bei TPM TPM-Systemstartschlüss	M zulassen el konfigurieren:	~	Falls Sie Bit möchten, a	Locker auf einem Comput ktivieren Sie das Kontrollk	er ohne TPM ve ästchen "BitLoc	rwenden ker ohne	
Systemstartschlüssel be TPM-Systemstartschlüssel un	i TPM zulassen el und -PIN konfigi d PIN bei TPM zula	v urieren:	kompatible entweder e Verwendun Schlüsselin verwendet	s TPM zulassen". In diesen in Kennwort oder ein USB- g eines Systemstartschlüss formationen, die zum Vers werden auf dem USB-Lauf	n Modus ist für Laufwerk erford sels werden die ichlüsseln des La fwerk gespeiche	den Start Ierlich. Bei aufwerks	h
<		>	ein USB-Sti wird der Zu das Laufwe	ck entsteht. Wenn der USB griff auf das Laufwerk auti rk zugegriffen werden. We	B-Stick eingester hentifiziert, und enn der USB-Stic	kt wird, es kann au k verloren	uf v
				ОК	Abbrechen	Übernehr	men

## Encryption

Open the BitLocker administration by entering "BitLocker verwalten" (ENG: "Manage BitLocker") in the Windows search mask. Activate BitLocker for the desired drive by clicking on "**BitLocker**" **aktivieren**" (ENG: "Enable BitLocker").

Startseite der Systemsteuerung	BitLocker-Laufwerkverschlüsselung
	Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff zu schützen.
	Betriebssystemlaufwerk
	System-Win10E-64 (C:) BitLocker deaktiviert
	SitLocker aktivieren
	Festplattenlaufwerke
	BitLocker (E:) BitLocker deaktiviert
	SitLocker aktivieren
	Wechseldatenträger - BitLocker To Go
Siehe auch	Schließen Sie einen USB-Speicherstick an, um BitLocker To Go zu verwenden.
TPM-Verwaltung	
-	
Datenträgerverwaltung	

Laufwerk auswählen [Bildquelle: Lennart Thurow]

**Note**: Please note that if the system hard disk is encrypted, a previously set password will be requested during the computer startup process. If a hard disk or partition is encrypted that only functions as data storage, no password is requested here.

#### Specify how the drive is to be unlocked at startup.

Select here

- USB-Speicherstick anschließen bei Nutzung mit mehreren Personen (ENG: "Connect USB memory stick - for use with several people")
- Pin eingeben bei Einzelnutzung (ENG: "Enter PIN for single use")

#### Create a PIN to unlock the drive.

Due to the version of Windows 10, different options may be offered to unlock the drive. The University Computing Center only offers the use of a PIN or a stick.

#### How should the recovery key be saved.

- Option 1: Auf USB-Speicherstick speichern (ENG: "Save to USB memory stick").
  - However, use this only to back up the recovery key, not for other tasks.
- Option 2: In Datei speichern (ENG: "Save to file") (HRZ recommendation).
  - Save the recovery file in a location outside your PC (e.g. Laufwerk Z:\ (ENG: "drive Z:\")).
- Option 3: Print recovery key
  - Print on paper

 $\times$ 

The recovery key must never be on the encrypted device. Depending on the version and release status of Windows 10, it may be offered to save the recovery key on a Microsoft account - which we do not recommend this. It is generally advisable to save the key on a medium that is not accessible at all times.

#### Select how much disk space of the drive should be encrypted.

Select the option "Gesamtes Laufwerk verschlüsseln" (ENG: "Encrypt entire drive") here.

BitLocker-Laufwerkverschlüsselung (C:)

#### Auswählen, wie viel Speicherplatz des Laufwerks verschlüsselt werden soll

Bei der Einrichtung von BitLocker auf einem neuen Laufwerk oder PC muss nur der derzeit verwendete Teil des Laufwerks verschlüsselt werden. Beim Hinzufügen neuer Daten werden diese von BitLocker automatisch verschlüsselt.

Falls Sie BitLocker auf einem bereits verwendeten PC oder Laufwerk aktivieren, sollten Sie das gesamte Laufwerk verschlüsseln. Durch die Verschlüsselung des gesamten Laufwerks wird der Schutz aller Daten sichergestellt. Dazu gehören auch gelöschte Daten, die möglicherweise immer noch abrufbare Informationen enthalten.

- O Nur verwendeten Speicherplatz verschlüsseln (schneller, optimal für neue Computer und Laufwerke)
- Gesamtes Laufwerk verschlüsseln (langsamer, aber optimal für PCs und Laufwerke, die bereits verwendet werden)

Weiter Abbrechen	Weiter Abbrechen

"Neuer Verschlüsselungsmodus" (ENG: "Select encryption mode to use").

Select the option "**Neuer Verschlüsselungsmodus**" (ENG: "New encryption mode") here.

🟘 BitLocker-Laufwerkverschlüsselung (E:)

### Zu verwendenden Verschlüsselungsmodus auswählen

Mit Windows 10 (Version 1511) wird ein neuer Datenträger-Verschlüsselungsmodus (XTS-AES) eingeführt. Dieser Modus unterstützt zusätzliche Integrität, ist mit älteren Windows-Versionen aber nicht kompatibel.

Bei einem Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchten, sollten Sie den kompatiblen Modus wählen.

Bei einem Festplattenlaufwerk oder einem Laufwerk, das nur mit Geräten eingesetzt wird, auf denen Windows 10 (Version 1511) oder höher ausgeführt wird, sollten Sie den neuen Verschlüsselungsmodus wählen.

Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)

O Kompatibler Modus (am besten für Laufwerke geeignet, die von diesem Gerät entfernt werden können)

Weiter Abbrechen
------------------

#### Do you want to encrypt the drive now?

Activate the option "BitLocker-Systemüberprüfung ausführen" (ENG: "Run BitLocker system check") and follow the instructions. The computer must then be restarted for BitLocker drive encryption.

### **Options**

#### **Encryption of external data carriers**

1. Enable Bitlocker on the corresponding drive

Real BitLocker Drive Encryption				- 🗆	$\times$
<ul> <li>→ ・ 个 🎨 Contro</li> </ul>	ol Panel > All Control Panel Items > BitLi	ocker Drive Encryption	v Ö		P,
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders t	rom unauthorised access by protecting your drives with BitLocker.			0
	Operating system drive				
	OS (C:) BitLocker on			$\odot$	
	<b>1</b>	<ul> <li>Suspend protection</li> <li>Change how drive is unlocked at start-up</li> <li>Bock up your recovery key Change PIN</li> <li>Turn off BitLocker</li> </ul>			
	Fixed data drives				
	Removable data drives - Bi	tLocker To Go			
	F: BitLocker off			$\odot$	
See also TPM Administration Disk Management Privacy statement	\$	Turn BitLocker on			

2. enter the password and click on "weiter" (ENG: "continue")

3. print the recovery key and save it on an external data storage device. This data storage should only be used for keeping the recovery key. Please also note the possibility of our custody function under drive "x" (See section: "How should the recovery key be stored")

←	RitLocker Drive Encryption (F:)	×
	How do you want to back up your recovery key?	
	<ul> <li>Some settings are managed by your system administrator.</li> <li>If you forget your password or lose your smart card, you can use your recovery key to access your drive.</li> </ul>	
	ightarrow Save to your Microsoft account	
	$\rightarrow$ Save to a file	
	$\rightarrow$ Print the recovery key	
	How can I find my recovery key later?	
	Next Cance	I

4. please select "gesamtes Laufwerk verschlüsseln" (ENG: "encrypt entire drive").

🙀 BitLocker-Laufwerkverschlüsselung (E:)

### Auswählen, wie viel Speicherplatz des Laufwerks verschlüsselt werden soll

Bei der Einrichtung von BitLocker auf einem neuen Laufwerk oder PC muss nur der derzeit verwendete Teil des Laufwerks verschlüsselt werden. Beim Hinzufügen neuer Daten werden diese von BitLocker automatisch verschlüsselt.

Falls Sie BitLocker auf einem bereits verwendeten PC oder Laufwerk aktivieren, sollten Sie das gesamte Laufwerk verschlüsseln. Durch die Verschlüsselung des gesamten Laufwerks wird der Schutz aller Daten sichergestellt. Dazu gehören auch gelöschte Daten, die möglicherweise immer noch abrufbare Informationen enthalten.

Nur verwendeten Speicherplatz verschlüsseln (schneller, optimal für neue Computer und Laufwerke)

Gesamtes Laufwerk verschlüsseln (langsamer, aber optimal für PCs und Laufwerke, die bereits verwendet werden)

5. please select the "kompatiblen Modus" (ENG: "compatible mode").

🙀 BitLocker-Laufwerkverschlüsselung (E:)

#### Zu verwendenden Verschlüsselungsmodus auswählen

Mit Windows 10 (Version 1511) wird ein neuer Datenträger-Verschlüsselungsmodus (XTS-AES) eingeführt. Dieser Modus unterstützt zusätzliche Integrität, ist mit älteren Windows-Versionen aber nicht kompatibel.

Bei einem Wechseldatenträger, den Sie mit einer älteren Windows-Version verwenden möchten, sollten Sie den kompatiblen Modus wählen.

Bei einem Festplattenlaufwerk oder einem Laufwerk, das nur mit Geräten eingesetzt wird, auf denen Windows 10 (Version 1511) oder höher ausgeführt wird, sollten Sie den neuen Verschlüsselungsmodus wählen.

Neuer Verschlüsselungsmodus (am besten für Festplattenlaufwerke auf diesem Gerät geeignet)

Kompatibler Modus (am besten f
ür Laufwerke geeignet, die von diesem Ger
ät entfernt werden k
önnen)

|--|

6. confirm the process. Finally, your external data carrier is encrypted

#### **Decryption of drives**

To decrypt the drive you have to click on more options and then select "Wiederherstellungsschlüssel eingeben" (ENG: "Enter recovery key").

Info: If you have already entered the password to unlock the drive before or if the drive is unlocked automatically, entering the recovery key is not necessary or possible during a subsequent decryption\*.

BitLocker can accordingly be completely deactivated by entering the password without the need for additional identification. In this case, deactivation is the same as decryption.

\*refers to a user with administrator rights. The deactivation of BitLocker can be prevented by restricting the rights of a standard user.

### **Unlocking drives**

- You can activate or deactivate the automatic unlocking of a drive. To do this, right-click on the drive and select "BitLocker verwalten" (ENG: "Manage BitLocker")
- Unlock by double-clicking on the drive and entering the password (if it is not a system partition)
- Automatic unlocking of the drive on certain computers. To do this, check the box "Auf diesem PC automatisch entsperren" (ENG: "Unlock automatically on this PC") and confirm by entering the password

### BitLocker (F:)

Geben Sie das Kennwort ein, um dieses Laufwerk zu entsperren.

Weniger Optionen

Wiederherstellungsschlüssel eingeben

Auf diesem PC automatisch entsperren



Entsperrung von Laufwerken

### Save system startup key on multiple USB memory sticks

Right-click on a BitLocker-protected drive to open the "BitLocker verwalten" (ENG: "Manage BitLocker") menu. Here the system startup key can be duplicated. Alternatively, the file can also be copied. However, this is marked as a system file by default and is therefore hidden.

## Information

## **Sources**

From: https://hrz-wiki.jade-hs.de/ - HRZ-Wiki

Permanent link: https://hrz-wiki.jade-hs.de/en/tp/pc-t/hdd-encryption

Last update: 2024/04/26 08:39

