# 

#### Features:

- A lightweight but high secure file encryption tool.
- Keeps your sensitive files always encrypted by default.
- Temporary decryption of files requires to enter your Switch 

  Crypt password which is nowhere stored except in your mind.
- Automatically encrypts all files when you step away from your PC.
- When converting unencrypted files to encrypted files: Overwrites unencrypted files with random data before deleting them <sup>1</sup>.
- Easy to install and easy use.
- Runs on your local machine only, doesn't require any internet service.
- Freeware sponsored by DKF, no user activity data are collected, no backdoor and no advertisement.

<sup>1</sup> = Overwriting a file with a random pattern does not protect against forensic investigations on SSD disks.

Dual Purpose: You can use Switch≓Crypt either as mentioned above to keep your own data encrypted, or - alternatively - you can use Switch≓Crypt to exchange encrypted data with another person via untrusted email or via an untrusted storage. Consider that you can use Switch≓Crypt only for one of these two purposes - but not for both of them.

Switch 

Crypt is based and latest security standards and uses a large cryptographic "Salt". You are fully protected against rainbow table attacks.

## **Background and Technical Concept**

Switch≓Crypt is a lightweight but high secure file encryption tool that works at directory / file level. It was originally developed to encrypt sensitive files on laptop computers when travelling in "untrusted countries".

Switch≓Crypt is mostly used to:

- Encrypt OpenVPN client configuration files.
- Encrypt text files which contain usernames and passwords.
- Encrypt Selenium IDE \*.side files which contain username and passwords (browser automation files).

Switch 

Crypt is easy to use, works out of the box, and does not install any driver. It works as a standard application without needing any special privileges or OS settings.

The encryption is based on a RSA keypair where the public key is used to encrypt the files and the private key is used to decrypt the files. Furthermore, the private key itself is encrypted by an symmetric AES algorithm which uses as key your arbitrary password plus a salt.

Choosing such an approach has the effect that encrypting any file does not require the password. This means also that encryption can be automated; for example you can automatically encrypt all files when the lid of your laptop is closed or when you lock your screen.

On the other hand, because your password is nowhere stored and remains only in your mind, decrypting a file cannot automated. To decrypt a file, or a couple of files, you have always to enter your password.

There are two programs delivered by the installation kit:

- 1. **SwitchCryptUI** which is the graphical user interface where you can configure the tool and manually encrypt and decrypt file or folders. From here you can also launch the default application for a (temporary) decrypted file.
- SwitchCryptAll which is a command line utility that encrypts all of your files. You can call this utility from various OS tools like for example from Windows Task Scheduler or from a Linux Cron job. SwitchCryptAll will synchronize its actions with SwitchCryptUI in order that you see always the latest state of the files in the graphical user interface.

# **Initial Setup and Configuration**

After installing Switch $\rightleftharpoons$ Crypt you have first to start **SwitchCryptUI** and to choose an arbitrary password.  $\rightarrow$  This effects that the RSA key pair will generated and a random salt will generated. The private key will be encrypted with your password and the salt.

The following files are created in your home directory ~/.SwitchCrypt

- public.key
- salt.dat
- encryptedPrivate.key

It's strongly recommended that you backup these 3 files to an USB stick. There is no extra protection required for the USB stick because none of these files contains your password. However, if these files are accidently deleted on your machine there is no way do decrypt any file if you don't have a backup.

Next you have to choose respectively to configure the directories (folders) wherein all files should be encrypted by default. For Example  $\sim$ /Documents/private. Please start first with some small folders and perform some tests until you are confident to operate the tool ( $\rightarrow$  see next chapter: Testing the Installation). That's basically all what is needed.

#### Don't encrypt any directory that is part of the operating system. $\rightarrow$ Reboot will fail!

## Don't encrypt the $\sim$ /.SwitchCrypt configuration directory. $\rightarrow$ Then you are locked out by yourself

**Optimally, but recommended**: You may additionally configure various OS tools like for example Windows Task Scheduler to call **SwitchCryptAll** on specific events or times.

This will effect that all files are encrypted by default even when you step away from your PC.

Recommended calls of **SwitchCryptAll** on **Windows** systems:

- On Workstation Lock of Any User
- On Workstation Unlock of Any User
- On Remote Connection to Any User Session
- On Remote Disconnect from Any User Session
- At Log On of Any User
- At System Startup

Note that SwitchCryptAll must run under the same user account as SwitchCryptUl.

#### ightarrow See Appendix A: Windows Example of calling SwitchCryptAll from Task Scheduler

#### Special Notes for Windows Systems:

The synchronization between **SwitchCryptAll** and **SwitchCryptUl** is made by **UTP multicast messages** which are send on the local loopback interface only. No data are transmitted over the internet. Depending on your firewall software you may get a security alert on your Windows machine. You have to allow this localhost – localhost UDP communication in order that the synchronization works.

Fire	ewall Alert ?			- ×
!	Suspicious network activity has bee	en detected.		
1	Very Few Users Fewer than 5 users in the Norton Community have used this file.	switchcrypt	tui.exe Info	
ø	Very New This file was released less than 1 week ago. Unproven There is not enough information about this file to recommend it.	localhost 127.0.0.1:11887	UDP 224.0.0.15 Port 11887 224.0.0.153:1	53 1887
		Date and Time:	20 May 2018 19:14:53	
		Options Do not notify me agai Applying default option in	Allow always n 1: 44 Stop Timer	Ŧ
<b>N</b>	Vorton Symantec		<u>More Detail</u>	s OK

# **Testing the Installation**

Once you have generated your key pair you should test the installation:

1. Create a directory named Test in your Documents folder and copy any file to this test directory (for example an image):

C:\Users\fisch\Docur	- 0	×		
← → ~ ↑ 🔒 ›		Q		
🛃 Ouick access	▲ Name	Date modified Type	Size	
Desktop	🗹 🖬 Screenshot (1).png	20 May 2018 20:05 PNG File	1.146 KB	
🕂 Downloads 🖈				
🔮 Documents 🖈				
📊 fisch 🛛 🖈				
1 item   1 item selecte	ed 1,11 MB			:==

2. Add the Test directory in the SwitchCryptUI:

Switch=Crypt	– 🗆 X
This Tool	
Configure Directories Excluded Files Initial Setup Settings Export Key Pair Help	
Encrypt All / Decrypt All Encrypt Directory / Decrypt Directory	Encrypt File / Decrypt File
List of directories in which all files are encrypted by default	
C:\Users\fisch\Documents\Test	<ul> <li>Add or remove directories you want to encrypt. All subdirectories will be encrypted also (recursively, but without following symbolic links).</li> <li>Don't encrypt any directory that is part of the operating system.</li> <li>Don't encrypt the Switch ≠Crypt configuration directory.</li> </ul>
Remove Selected	Add Directory

# 3. Switch to the "Encrypt File / Decrypt File" Tab:

Switch		– 🗆 X
This Tool		
Configure Directories Excluded	Files Initial Setup Settings Export Key Pair Help	]
Encrypt All / Decrypt All	Encrypt Directory / Decrypt Directory	Encrypt File / Decrypt File
Current Status: No files are encry	pted	
Plain Files 1		
Encrypted Files 0		
Excluded Files 0		
File Name		✓ Ignore Case
List of Files C:\Users\fisch\D	ocuments\Test\Screenshot (1).png	
Password	View Content Open Fil	e Encrypt File Decrypt File
<ul> <li>Viewing an encrypted file requires</li> <li>Decrypting a file requires the pass</li> <li>Encrypting a file does not require to</li> </ul>	the password but leaves the file encrypted on disk. word. he password.	

4. Start a terminal and locate to the SwitchCrypt installation directory (C:\Program Files\SwitchCrypt). Then call **SwitchCryptAll**:

cmd.exe	_		$\times$
			^
C:\Program Files\SwitchCrypt>SwitchCryptAll.exe			
2018-05-20 20:13:36   1 files in C:\Users\fisch\Documents\Test			
2018-05-20 20:13:36   Start encryption for 1 files			
2018-05-20 20:13:36   Encrypting C:\Users\fisch\Documents\Test\Screenshot (1).png to C:\Users	s\fis	sch\Doo	cum
ents\Test\Screenshot (1).png-\$enc			
2018-05-20 20:13:36   Encryption completed. 1 files new encrypted, 0 files already encrypted.	, 0 <del>(</del>	files e	exc
luded. Warnings = 0, Errors = 0   Execution time = 0 seconds			
C:\Program Files\SwitchCrypt>			

#### 5. The file(s) in your test directory should now be encrypted (= test passed):

Switch		-	- 🗆	×
This Tool				
Configure Directories Excluded Fi	les Initial Setup Settings Export Key Pair Help			
Encrypt All / Decrypt All	Encrypt Directory / Decrypt Directory	Encrypt File / I	Decrypt File	
Current Status: All files are encrypt	ed			
Plain Files 0				
Encrypted Files 1				
Excluded Files 0				
File Name			🖌 Ignore (	Case
List of Files C:\Users\fisch\Doc	uments\Test\Screenshot (1).png-\$enc			▲ ●
Password     Viewing an encrypted file requires the     Decrypting a file requires the password	view Content Open File e password but leaves the file encrypted on disk. rd.	Encrypt File	Decrypt	File
- Ericrypung a me does not require the	passwora.			

6. Finally remove the Test directory from the **SwitchCryptUI** configuration and delete the Test directory at OS level.

# Addition notes for using Switch≓Crypt to exchange sensitive encrypted data with another person (dual use of the tool, second case)

If you plan to use Switch a Crypt to exchange sensitive encrypted data with another person then Switch Crypt should <u>installed and tested first only on one PC</u> as described before. After the first PC is tested, the keypair can be exported and send to the second person. Then the second person should install Switch Crypt and import the key pair during the "Initial Setup" dialog.

#### First PC $\rightarrow$ Export Key Pair:

■ Switch≓Crypt	_		$\times$
This Tool			
Configure Directories Excluded Files Initial Setup Settings Export Key Pair Help			
Encrypt All / Decrypt All Encrypt Directory / Decrypt Directory Encrypt F	ile / Decryp	ot File	
Export Key Pair / Share Encrypted Files with Other Persons			
If you wish to share or exchange your encrypted files with other persons proceed as follows:			
<ol> <li>Export your key pair and store it in any non-encrypted directory (for example on desktop). You have to set ar export-password which should not be the same as your own password. A ZIP file named keypair.zip will get</li> </ol>	n arbitrary enerated.		
<ol><li>The ZIP file can transferred via an non-secure channel to the corresponding persons, therefore you can se never include the export-password in the email.</li></ol>	nd it by em	ail. But	
3. The receiving persons have to import your key pair in the "Initial Setup" menu.			
4. Give the receiving persons a direct phone call (no voice mail) and tell them the export-password.			
<ol><li>Finally, the receiving persons should call the "Settings" menu and change the export-password to an arbitr password.</li></ol>	ary, own pi	rivate	
After that all involved persons are ready to store, update and exchange the encrypted files in a common untrusted sto the encrypted files to each other.	orage, and	to email	I
Your Password			
Enter Arbitrary Export-Password			
Confirm Arbitrary Export-Password	Export	Key Pair	r )

#### Second PC $\rightarrow$ Import Key Pair:

Switch = Crypt	- 🗆 X
This Tool	
Configure Directories Excluded Files Initial Setup Setting	Export Key Pair Help
Encrypt All / Decrypt All Encrypt Directory /	Decrypt Directory Encrypt File / Decrypt File
Welcome to Switch 2 Crypt. The initial setup is only one time require The Select the file keypair.zip	ed. × Recommended Instructions:
wit Th Look In: fisch	screenshot of this dialog and print it out. In arbitrary password and click on e Key Pair". p the 3 generated key files to an USB stick. Iown your password on the print out and
- p android J.dealC2017.3 s.s. - e .cordova install4j7 s.s - dotnet s.nuget s.s It's J.dealC2017.2 g.qaguard s.t Yo or	papuios witchCrypt witchCryptDevelop emplateengine
File <u>Name: keypair.zip</u> Files of <u>Type</u> : ZIP Files	
Cor Select Import File	Cancel

In case if you are planning to use an untrusted storage to exchange your encrypted files then <u>the untrusted storage</u> <u>should \*not\* be configured as an encryption/decryption directory</u> in **SwitchCryptUI**. Each person should have its own local encryption/decryption directory.

Encrypted files can be exported from the local directory to the untrusted storage by performing a right mouse click to the file name at the "Encrypt File / Decrypt File" tab.

And the encrypted files can imported from the untrusted storage by performing a right mouse click to the local directory at the "Encrypt Directory / Decrypt Directory" tab.

Alternatively, the files can also be moved to or from the untrusted storage by any other tool like by using the file manager of the OS.

**Rule of Thumb:** Never add a directory of an untrusted storage in the SwitchCryptUI "Configure Directories" tab. Use instead of this the export and import functions to copy the encrypted files. Store only encrypted files on the untrusted storage.

Exporting an encrypted file (Save As ..) from the local directory to the untrusted storage:

■ Switch≓Crypt		– 🗆 X
This Tool		
Configure Directories Excluded Files Initial Setup Se	ettings Export Key Pair Help	
Encrypt All / Decrypt All Encrypt Direct	ory / Decrypt Directory	Encrypt File / Decrypt File
Current Status: All files are encrypted		
Plain Files 0		
Encrypted Files 1		
Excluded Files 0		
File Name		Ignore Case
List of Files	(1) ppg-\$epc	
	(1).prig ¢ene	
	Save As	×
	Save In: Scratch (X:)	
<b>.</b>	Backup	
Password		
<ul> <li>Viewing an encrypted file requires the password but leaves the - Decrypting a file requires the password</li> </ul>	•1	
<ul> <li>Encrypting a file does not require the password.</li> </ul>		
	File Name: Screenshot (1).png	j-\$enc
	Files of Lype: All Files	•
		Save Cancel

Importing an encrypted file from the untrusted storage to the local directory:

Switch						— [	) ×	7
This Tool								
Configure Directories	Excluded Files	Initial Setup	Settings	Export Key Pair	Help			
Encrypt All / Decr	ypt All	Encrypt D	irectory / Dec	crypt Directory		Encrypt File / Decrypt	File	
Current Status: All dire	ectories are encry	/pted						
Plain Directories	0							
Partially Encrypted Dire	ectories 0							
Fully Encrypted Directo	ries 1							
Directory Name							oro Cono	
						ign	ore case	
List of Directories	C:\Users\fisch\Do	cuments\Test						
			Import File	s to C:\Users\fisch\D	ocuments\Test	t		×
		1	.ook <u>I</u> n: 😂	Scratch (X:)			-	a 🗇 🗅 🙁 🚝
			📑 Backup				7	
			Screens	hot (1).png-\$enc				
Password							Del	ete Files at Origin Location
								C C
- Decrypting a directory	requires the passw	iord.						
- Encrypting a directory	does not require th	e password.						
			File <u>N</u> ame:	Screenshot (1).pr	ig-\$enc			
			Files of Type	All Files				•
			The of The					
								Import Cancel

#### FAQs

#### Q: Can the Switch≓Crypt password be cracked by a brute force attack?

**A:** This depends on how long your password is. If your password contains less than 8 characters it can be cracked in seconds. If you choose a password length which is equal or lager than 14 characters then you are at the secure side, as long as such a password is not a common, single word, or a combination of common words. For example "IloveMySweetheart" is not a good password because it contains common words only. Be creative, use several languages, use exotic words, add some spelling errors, and use special chars. For example "bruchita\$\$irversiede+-" is much better.

Rule of thumb: Any common word counts always as two characters only, independently of how long the word is. So, to reach a secure password with common words only you need 14/2 = 7 common words.

#### 

**A:** No. That's technically impossible. For each installation Switch≓Crypt generates a random salt on your machine of 24 bytes (= 192 bits).

#### Q: I forgot my Switch≓Crypt password. Is there a way to decrypt the files anyway?

A: No, no way. Suggestion: Step away from your PC, relax and try to remember the password.

#### Q: Can I accidently (double) encrypt an already encrypted file?

A: No, that's technically impossible. The tool will take care to prevent this.

# Q: If I have renamed an encrypted file and/or did change the file extension of an encrypted file, can I decrypt the file anyway?

A: Yes.

#### Q: Can I change my Switch Crypt password?

A: Yes, at any time: Settings  $\rightarrow$  Change Password. Note that in such a case a new random salt will generated also, even if you if the new password is the same as the old password.

# Q: If I have chosen first a weak Switch Crypt password and changed it later to a strong password, does this make sense, respectively does this increase the security? A: Yes.

# Q: If I install the tool twice on different PCs and choose each time the same password, can I then encrypt a file on one PC, send it to the other PC, and decrypt it on the other PC?

**A:** The standard answer is "no", because you have normally generated two different key pairs. However, you can export the key pair from the first installed PC and import it on the second installed PC. Then this works.

## Q: Does Switch≓Crypt act in a similar way like a disk encryption tool?

A: No. A disk encryption tools protects your data only at the time when you are <u>not</u> logged in. For example in cases when your laptop is lost or stolen, or when you replace an old disk by a new disk. In opposite to this, Switch≓Crypt protects your data also at the time when you are logged in. That's because Switch≓Crypt works on file level, rather than on disk level. However, the technical approach of Switch≓Crypt has the disadvantage that you cannot encrypt any files needed by the operating system. For example you cannot encrypt /etc/passwd or any files in C:\Windows.

## 

**A:** Yes, and we recommend to do that. Rule of thumb: If you combine Switch≓Crypt with a disk encryption tool, your sensitive data are substantially much more secure than when using a disk encryption tool only.

#### Q: Does Switch≓Crypt protect me against trojan horses?

A: This depends on the time when you detect the trojan horse. If you detect the trojan horse before you have manually entered the Switch 

Crypt password then your files are still protected. Of course, in such a case you have first to make a backup of your sensitive data and then to reinstall the OS. After that restore your key pair, reinstall Switch 
Crypt and copy the sensitive, encrypted data to the new installed OS.

#### 

**A:** No. You have to backup your (encrypted) files and keep the backup offline. We recommend that the backup includes also the Switch≓Crypt configuration directory.

#### Q: What can happen if the backup device is stolen?

## Q: What can I do if I get caught at the workplace?

**A:** Just close the lid of your laptop, or press the two keys <Windows><L> to lock your screen (on PC or laptop). If you have followed the "optional but recommended" installation suggestions all of your sensitive data will be automatically encrypted at this moment.

## Q: If somebody knows the password of my login account, does Switch Crypt protect my sensitive files anyway? A: Yes, because Switch Crypt use a separate password to encrypt your data.

# Q: If I use Switch Crypt to exchange sensitive encrypted data with another person (dual use of the tool, second case), how secure is this?

A: High secure. Nobody on this earth can decrypt the encrypted data during transmission via Email, or on your (insecure) shared storage, as long as you have used a strong export password as mentioned before in the FAQs. Follow the instructions at "Export Key Pair". If you have paranoia and don't trust any messenger, you can use Switch≓Crypt as an alternative to exchange you encrypted files with one or two persons (but not with many persons) in a high secure way. Please keep in mind that all persons use the same key pair, even if they use different passwords. Therefore, if one computer of any person is hacked, all files can be decrypted on all computers. That's the reason why you should share the key pair with only with one or with maximum two other persons. If you are worried that your phone is wiretapped when telling the export password to the other person(s), then use another way to tell them the export password.

#### Q: In which programing language is Switch Crypt written?

A: It's written in Java 9.

#### Q: Which cryptographic algorithm are used by Switch≓Crypt?

**A:** RSA key pair length: 2048 bit, hash algorithm for the password and salt: SHA 256, random salt: 24 bytes = 192 bit, random AES key per encrypted file: 256 bit. Random initial vector per encrypted file: 16 bytes.

# Q: The Switch≓Crypt tool is freeware, but it's not open source. How can I verify that all encryption algorithms are properly implemented?

A: The core Java class of the Switch Crypt tool that does all encryptions is licensed under the GNU General Public License, V3 (GPL V3). You can check the source code <a href="https://www.dkfqa.com/switchcrypt/src/InitialKeyPair-java.html">https://www.dkfqa.com/switchcrypt/src/InitialKeyPair-java.html</a>. All other code of the tool is closed source.

# Appendix A: Windows Example of calling SwitchCryptAll from Task Scheduler

1. Call "Schedule tasks" from Windows Settings:

Settings		- 🗆 ×
	Windows Settings	
	sched ×	
	C Schedule your restart	
System Display, sound, notifications, power	Schedule tasks	<b>Phone</b> Link your Android, iPhone
Network & Internet Wi-Fi, airplane mode, VPN	Personalization Background, lock screen, colors	<b>Apps</b> Uninstall, defaults, optional features

2. Create a new task. Name it SwitchCryptAll, select "Run whether user is logged on or not" and set "Configure for" to "Windows 10":

🕒 Create Task			×							
General Trigg	gers Actions Condi	tions Settings								
Na <u>m</u> e:	Name: SwitchCryptAll									
Location:	X.									
Author:	DESKTOP-L02BL11\fi	sch								
Description:										
-Security opt	ons									
When runni	ng the task, use the fo	ollowing user account:								
DESKTOP-L	02BL11\fisch	Change <u>U</u> ser or Gro	oup							
O Run only	when user is logged	on								
Run whee	ther user is logged on	or not								
🗌 Do n	ot store <u>p</u> assword. Th	e task will only have access to local computer resources.								
🗌 Run w <u>i</u> th	highest privileges									
Hidd <u>e</u> n	<u>C</u> onfigure for:	Windows 10	$\sim$							
		ОК С	ancel							

# 3. Add the following triggers:

- At log on
- At startup
- On connection to user session
- On disconnect from user session
- On workstation lock
- On workstation unlock

Create Task							
General Triggers Actions Cond	itions Settings						
When you create a task, you can specify the conditions that will trigger the task.							
Trigger	Details	Status					
At log on	At log on of any user	Enabled					
At startup	At system startup	Enabled					
On connection to user session	On remote connection to any user session	Enabled					
On disconnect from user sessi	On remote disconnect from any user session	Enabled					
On workstation lock	On workstation lock of any user	Enabled					
On workstation unlock	On workstation unlock of any user	Enabled					
<u>N</u> ew <u>E</u> dit	<u>D</u> elete						
		OK Cancel					

4. Set as action to start SwichCryptAll.exe

🕒 Create	Task										×
General	Triggers	Actions	Conditions	Settings							
When	you create	a task, yo	u must speci	fy the acti	on that wi	ll occur wł	nen your	task starts			
Actio	n	Det	tails							7	
Start a	a program	"C:'	\Program File	es\Switch(	Crypt\Swit	chCryptAll	l.exe"				
										<b>^</b>	
										*	
<									)	•	
<u>N</u> e	w	<u>E</u> dit	<u>D</u> elet	te							
								ОК		Canc	el

#### 5. Disable all conditions:

General	Triggers	Actions	Conditions	Settings		
Specify run if a Idle	the condi any condit	tions that, ion specifi	along with t ied here is no	he trigger, deter t true.	mine whether the task sho	ould run. The task will not
Star	t the task o	only if the	<u>c</u> omputer is i	dle for:	10 minutes	~
	W <u>a</u> it for idle for:				1 hour	$\sim$
S	Stop if the	comput <u>e</u> r	ceases to be i	idle		
	Restart if	f the idle s	tate res <u>u</u> mes			
Power						
Star	t the task o	only if the	computer is o	on AC <u>p</u> ower		
$\sim$ S	Stop if the	computer	switches to <u>b</u>	attery power		
<u>W</u> al	ke the com	puter to r	un this task			
	-L.					
Netwo	rк — —			nnaction is susi	lable	
Netwo	тк t onl <u>v</u> if th	e followin	g network co	nnection is avai	lable.	
Netwo	t only if th	<b>e followin</b>	g network co	nnection is avai		~
Netwo Star	rκ t onl <u>y</u> if th r connectio	e followin on	g network co	nnection is avai		~
Netwo Star Any	t only if th	e followin	g network co	nnection is avai		~
Netwo	t only if th	e followin on	g network co	nnection is avai		~
Netwo	rk — t onl <u>y</u> if th	e followin	g network co			~
Netwo	t onl <u>y</u> if th	e followin	g network co			~

6. Set the value of "Stop the task if it runs longer than" to a small value (1 hour), then click on the OK button at the bottom of the window:

Create Task	×						
General Triggers Actions Conditions Settings							
Specify additional settings that affect the behavior of the task.							
Allow task to be run on demand							
Run task as soon as possible after a <u>s</u> cheduled start is missed							
$\square$ If the <u>t</u> ask fails, restart every: 1 minute $\sim$							
Attempt to restart up to:							
Stop the tas <u>k</u> if it runs longer than:							
✓ If the running task does not end when requested, <u>force it to stop</u>							
If the task is not scheduled to run again, <u>d</u> elete it after: 30 days $\sim$							
If the task is already ru <u>n</u> ning, then the following rule applies:							
Do not start a new instance $\checkmark$							
OK Canc	el						

7. Finally, enter the password of your Windows account:

Task Scheduler		?	$\times$				
Enter user account information for running this task.							
<u>U</u> ser name:	DESKTOP-L02BL11	\fisch	×				
Password:							
	OK	Can	icel				

8. Perform a small test. Manually decrypt some files with **SwitchCryptUI**. Then lock and unlock your workstation. All files should now be encrypted.