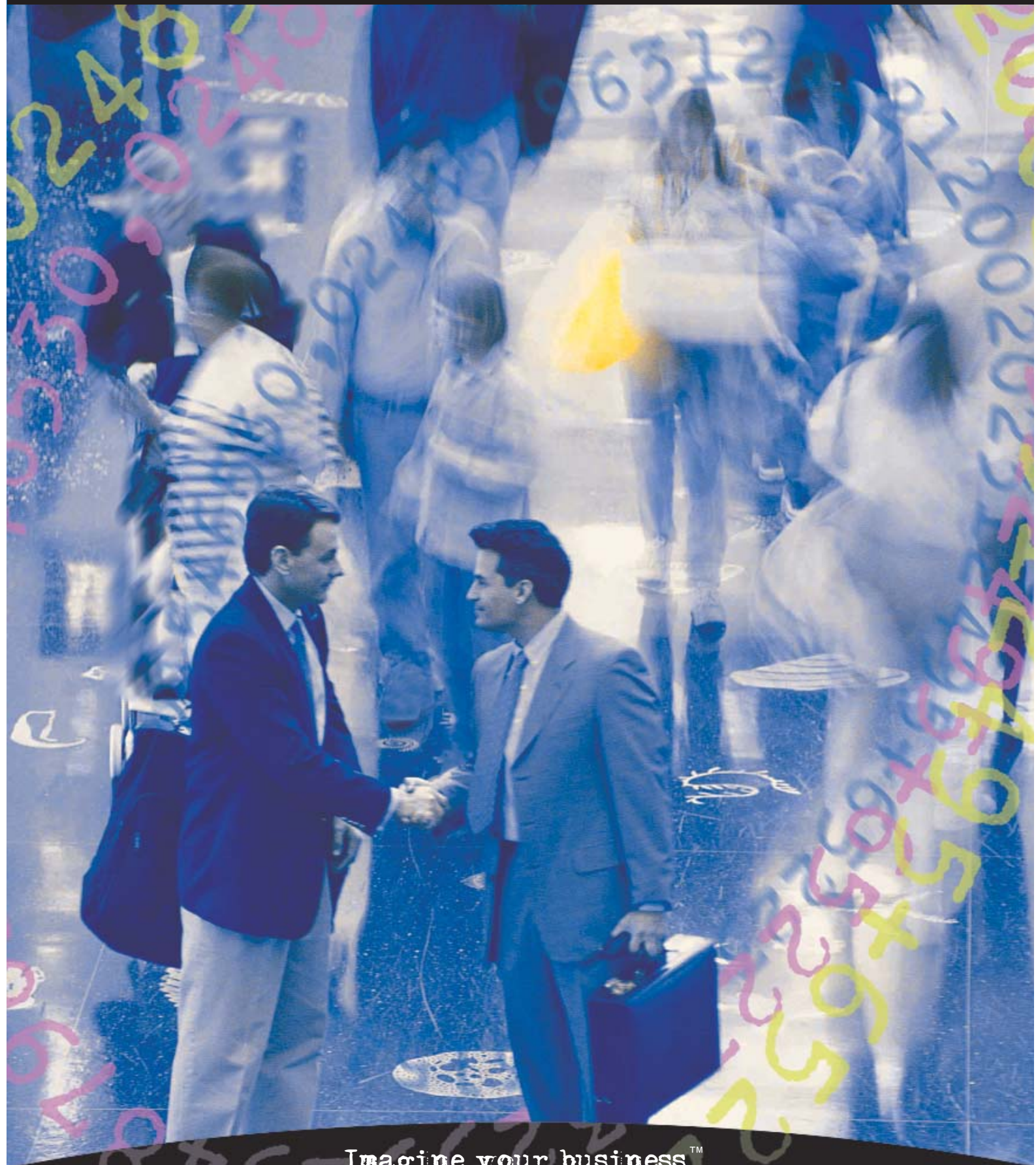


VALIDY FILE CRYPT USER DOCUMENTATION



Imagine your business.™



www.validy.com

TABLE OF CONTENTS

| | |
|---|-----------|
| Introduction..... | 1 |
| 1 - Installing Validy File Crypt..... | 2 |
| 1.1 Kit contents..... | 2 |
| 1.2 Required configuration..... | 2 |
| 1.3 Installation..... | 2 |
| 2 - Using Validy File Crypt..... | 3 |
| 2.1 Using your Validy File Crypt USB key..... | 3 |
| 2.2 Encrypting files..... | 4 |
| 2.3 Decrypting files..... | 5 |
| 2.4 Personal code (PIN)..... | 5 |
| 2.5 Changing PINs..... | 6 |
| 3 - Customizing Validy SIMs..... | 7 |
| 3.1 Passphrases and secret keys..... | 7 |
| 3.2 Adding a PIN, modifying PIN parameters, unlocking a Validy File Crypt SIM..... | 8 |
| 3.3 Erasing a key and a PIN from a Validy File Crypt SIM..... | 10 |
| 3.4 Loading an encryption key and a PIN to a Validy File Crypt SIM..... | 11 |
| 4 - Usage advice..... | 12 |
| 5 - Validy guarantee..... | 13 |

INTRODUCTION

Validy File Crypt is an easy to use and extremely robust file encryption solution.

Files are encrypted and decrypted using a 128-bit secret key stored in the SIM of your USB key.

Files encrypted with Validy File Crypt can be decrypted only with the SIM used to encrypt them or with a SIM containing the same secret key. Validy File Crypt users can very simply load a personal secret key to their SIM so as to make sure they are the only ones able to access their encrypted files.

In order to reinforce security, users may add a PIN (Personal Identification Number) code to protect their Validy File Crypt SIM.

Validy File Crypt is easy to use. Encrypting and decrypting files is done from the Windows contextual menu, with a simple mouse click.

Any kind of file can be encrypted with Validy File Crypt.



1 - Installing Validy File Crypt

1.1 KIT CONTENTS

- 1 SIM.
- 1 CD-Rom containing the USB key driver and the Validy File Crypt software.
- 1 USB key.

1.2 REQUIRED CONFIGURATION

- PC-compatible computer with USB interface.
- Windows 2000 or Windows XP.
- 2 Mb of hard disk space.

The smart card version of Validy File Crypt is compatible with Windows 95, 98, NT 4.0, Millennium, 2000 and XP. Contact us (info@validy.com).

1.3 INSTALLATION

Insert the Validy CD-Rom in your reader. The installation program starts automatically. Else, run the program **Validy_File_Crypt_2.x.x.x_Setup.exe** from the CD-Rom, and follow on-screen instructions.

- If you have a connection to the Internet:
USB keys' drivers are available on Windows Update.

Windows 2000:

- Insert the USB key in an available USB port. Upon USB key insertion, the **Found New Hardware** wizard starts.
- Press **Next**.
- Select **Search for a suitable driver for my device (recommended)** then press **Next**.
- Check the **Microsoft Windows Update** box and make sure the other boxes are not checked. Press **Next**.
- After a few moments, the wizard indicates that Windows found a driver for the device. Press **Next**.
- The window displays **Completing the Found New Hardware** wizard, press **Finish**.

Windows XP:

- Insert the USB key in an available USB port. Upon USB key insertion, the **Found New Hardware** wizard automatically connects to Windows Update and installs the drivers. If it is not the case, follow the Windows 2000 procedure described above.

- If you do not have a connection to the Internet:
 - Insert the USB key in an available USB port. Upon USB key insertion, the **Found New Hardware** wizard starts.
 - Press **Next**.
 - Select **Search for a suitable driver for my device (recommended)** then press **Next**.
 - Check the **Specify a location** box and make sure the other boxes are not checked. Press **Next**.
 - Press **Browse** and select the folder **C:\Program Files\Validy\egate**.
 - Press **Open** and **Ok**.
 - The wizard indicates that **The wizard found a driver for the following device: Cryptoflex e-gate**, press **Next**.
 - The window displays **Completing the Found New Hardware wizard**, press **Finish**.
 - Your system may prompt you to reboot it, do it if need be.

You are now ready to use Validy File Crypt.

2 - Using Validy File Crypt

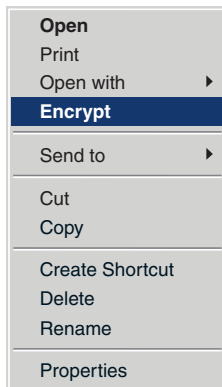
2.1 USING YOUR VALIDY FILE CRYPT USB KEY

The SIM of your USB key contains the secret key used to encrypt/decrypt files.

You must therefore connect your USB key before using Validy File Crypt.

Note: the SIM contains a default secret key which we advise to modify for optimal security. (see *Chapter 3: Customizing Validy SIMs*).

2.2 ENCRYPTING FILES



- To encrypt a file, insert your key in the USB port.
- Select the file(s) to be encrypted.
- Right click and select **Encrypt** in the contextual menu.


- The file is then encrypted.
- The extension **.vldy** is added to the encrypted file name. For instance **file.txt** becomes **file-txt.vldy**. *
- The icon of the encrypted file is replaced with the Validy icon.



file.txt



file-txt.vldy

 All file types can be encrypted with Validy File Crypt. Be careful, encrypting certain files can prevent some programs or even your operating system from working properly!

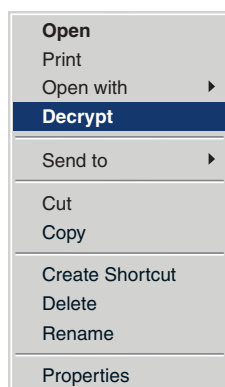
Validy recommends encrypting only work documents.

Validy advises against encrypting files of the following types: .bat, .bin, .cfg, .com, .dll, .drv, .exe, .fon, .fot, .grp, .ico, .ini, .ovl, .pif, .sys, .ttf, .vbx, .lnk

Validy cannot be held responsible for the direct or indirect damages suffered by the customer due to bad use of Validy File Crypt.

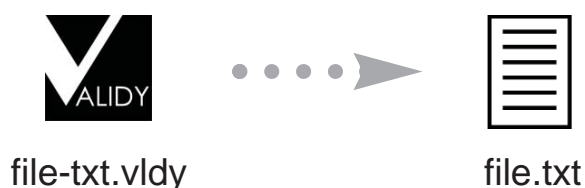
* If your system is configured to hide file extensions, you won't be able to see the **.vldy** extension. In order to show the extensions, in Windows explorer, click on **Tools, Folder Options, View**, and uncheck the box **Hide file extensions for known file types**.

2.3 DECRYPTING FILES



- To decrypt a file, insert your key in the USB port.
- Select the file(s) to be decrypted.
- Right click and select **Decrypt** in the contextual menu (you can also double-click on an encrypted file to decrypt it).

- The file is then decrypted.
- The extension **.vldy** disappears.* (see page 4)
- The Validy icon is replaced with the original icon and the file becomes accessible again.



Note: when you receive an encrypted file as an attachment to an email, you must save the attachment to your hard disk before decrypting and opening it.
(see 4 - Usage advice)

2.4 PERSONAL CODE (PIN)

It is possible to protect your SIM with a Personal Identification Number (PIN).

This PIN will have to be keyed in before each use of Validy File Crypt. Once the correct PIN is keyed in, you will not be required to key it in again for the following encryption/decryption operations as long as the computer remains on or the USB key inserted.

Consequently, do not leave your USB key connected when you leave your computer unattended as an intruder may access your encrypted files while you're away.

The customization tool enables you to add a PIN to your SIM. Besides, you have the possibility to lock the SIM after 7 erroneous keying attempts. You are then the only one able to unlock a locked SIM (see 3.2 *Adding a PIN, modifying PIN parameters, unlocking a Validy File Crypt SIM*). It protects you against any illicit use of your USB key.

2.5 CHANGING PINs

You can very easily change the PIN of a Validy File Crypt SIM.

- In Windows' **Start menu**, go to **Programs -> Validy File Crypt**, and select **Change PIN**.
- The change PIN program starts.
- Connect your USB key.
- Key in its current PIN.
- Key in its new PIN.
- Key in the new PIN again.
- Press **Ok**.
- If the current PIN keyed in is correct, it is then replaced with the new PIN.
- Unconnect the USB key.
- If you wish to modify the PIN of another SIM, connect the USB key and repeat the procedure, otherwise, press **Quit** to quit the program.

Remarks:

To add a PIN to a Validy File Crypt SIM that does not have one, you have to use the Validy File Crypt customization program (see 3.2 *Adding a PIN, modifying PIN parameters, unlocking a Validy File Crypt SIM*).

When you try to modify a PIN and fail to key in correctly the current PIN, the program behaves depending on the chosen option for the PIN:

- If it's a blocking PIN, you have up to 7 attempts before the SIM is locked.
- If it's a non blocking PIN, the number of attempts is unlimited.

3 - Customizing Validy SIMs

3.1 PASSPHRASES AND SECRET KEYS

Validy File Crypt uses a secret key, stored in the SIM, to encrypt and decrypt files.

The Validy File Crypt SIMs contains a default secret key.

It is however recommended that you replace this key with your own. A key management tool is provided, it enables you to generate a personal secret key from a passphrase of your choosing.

The default secret key of Validy File Crypt SIMs is generated from the passphrase **validy protects your data**.

A signature is associated to each passphrase. The slightest modification in the passphrase radically modifies the signature, which allows you to make sure that you typed the expected passphrase.

Data encrypted with a Validy File Crypt SIM can be decrypted only with the SIM used to encrypt it, or with a SIM containing the same secret key.

If you wish to exchange encrypted information with other people, they must use Validy File Crypt and load their secret key using the same passphrase as yours.

The Validy File Crypt customization program is accessible through Windows' **Start Menu**. To launch it, go to **Programs** then **Validy File Crypt**, and click on **Customize card**.

Passphrase

Your passphrase is the secret that keeps your encrypted files confidential. It is recommended you choose it carefully so that no one can guess it, and to keep it in a safe place.

It is mandatory to archive your passphrase and its signature. In case you lose your USB key, you will absolutely need your passphrase in order to generate a Validy File Crypt SIM able to decrypt your previously encrypted files. The passphrase must contain between 10 and 200 characters. So as to avoid any ambiguity, you can use only non-accentuated small letters, numerals, and spaces.

This program allows you to:

- Add a PIN, modify the PIN parameters, unlock a Validy File Crypt SIM.
- Erase the key and the PIN of a Validy File Crypt SIM.
- Load a key and a PIN to a Validy File Crypt SIM.

Run this program on a healthy machine (no virus), and if possible not connected to the internet.

Use this program away from prying eyes.

 **Warning:**

If you attempt to update an already customized SIM with an erroneous passphrase, you have 7 attempts before the SIM is permanently put out of order, so as to foil fraud attempts.

3.2 ADDING A PIN, MODIFYING PIN PARAMETERS, UNLOCKING A VALIDY FILE CRYPT SIM

- Launch the customization program (**Start Menu, Programs, Validy File Crypt, Customize card**).
- Choose **Add a PIN, Modify PIN parameters, Unlock a Validy File Crypt SIM** and press **Next**.
- Type the passphrase corresponding to your SIM. *Reminder:* if you have never customized your SIM, the default passphrase is **validy protects your data**, and the corresponding signature **d793d7de**.
- Make sure that the signature matches, then press **Next**.
- Choose the PIN parameters (see opposite page), then press **Next**.
- The program recapitulates the actions to carry out. Make sure the information is correct, then connect your USB key so that the update starts.
- Your SIM's PIN is then modified.
- When the modification is done, unconnect your USB key.
- The program goes back to the previous screen.
- If you wish to modify the PIN of another SIM with the same parameters, connect another USB key. Otherwise, press **Quit** to quit the program.

PIN

You can choose from the following types of PINs:

- **No PIN:** the SIM is not protected by a PIN and usable by anyone.
- **Non-blocking PIN:** the SIM is protected by a PIN, which must be keyed in. The number of keying attempts is not limited.
- **Blocking PIN:** the SIM is protected by a PIN, which must be keyed in. The user has up to 7 attempts, after which the SIM is locked and unusable. The only way to unlock it is to know its passphrase and to use the function **Unlock a SIM** of the Vality File Crypt customization program.

PIN Value: key in this box the PIN you wish to set for the Vality File Crypt SIM. The PIN can be keyed in equally in small or capital letters.

Option: pre-expired PIN.

With this option checked, the user will be required to change the PIN of the Vality File Crypt SIM on its first use.

This option is useful if you wish to supply Vality File Crypt USB keys to other persons and guarantee them that you don't know their PIN.

Option: periodic PIN change mandatory.

With this option checked, the user will be required to periodically change the PIN of the Vality File Crypt SIM, every **n** days. Enter the value of **n** in the **Maximum age** box.

Minimum PIN size: minimum size of the new PIN which will have to be entered after the expiration of the old one (this box appears only when the **Pre-expired PIN** or **periodic PIN change mandatory** option is checked).

3.3 ERASING A KEY AND A PIN FROM A VALIDY FILE CRYPT SIM

Note: you have to erase the secret key of a Validy File Crypt SIM before being able to load a new one (see 3.4 *Loading an encryption key and a PIN to a Validy File Crypt SIM*).

- Launch the customization program (**Start Menu, Programs, Validy File Crypt, Customize card**).
- Choose **Erase the key and the PIN from a Validy File Crypt SIM** and press **Next**.
- Type the passphrase corresponding to your SIM. *Reminder:* if you have never customized your SIM, the default passphrase is **validy protects your data**, and the corresponding signature **d793d7de**.
- Make sure that the signature matches, then press **Next**.
- The program recapitulates the actions to carry out. Make sure the information is correct, then connect your USB key so that the update starts.
- Your SIM's secret key is then erased, as well as its PIN if it had one.
- When the modification is done, unconnect your USB key.
- The program goes back to the previous screen.
- If you wish to erase the secret key of another SIM with the same passphrase, connect another USB key. Otherwise, press **Quit** to quit the program.

3.4 LOADING AN ENCRYPTION KEY AND A PIN TO A VALIDY FILE CRYPT SIM

Note: you have to erase the secret key of a Validy File Crypt SIM before being able to load a new one (see 3.3 *Erasing a key and a PIN from a Validy File Crypt SIM*).

- Launch the customization program (**Start Menu, Programs, Validy File Crypt, Customize card**).
- Choose **Load a key and a PIN to a Validy File Crypt SIM** and press **Next**.
- Choose a passphrase for your SIM and type it. (see *Passphrase, page 7*).
- Carefully write it down, as well as the corresponding signature, and press **Next**.
- Choose the PIN parameters (see *PIN, page 9*), and press **Next**.
- The program recapitulates the actions to carry out. Make sure the information is correct, then connect your USB key so that the update starts.
- The secret key corresponding to your passphrase is then loaded to the SIM, as well as the PIN if there is one.
- When the modification is done, unconnect your USB key.
- The program goes back to the previous screen.
- If you wish to load the same secret key to another SIM with the same parameters, connect another USB key. Otherwise, press **Quit** to quit the program.

4 - Usage advice

When you receive an encrypted file as an attachment to an email, save it to your hard disk before decrypting and opening it. Indeed, if you try to open it directly from your email client, the file will be decrypted and saved in the Temporary Internet Files, but won't be opened. It will therefore be stored on your computer's hard disk in clear, and anyone having access to your hard disk may be able to read it. If you accidentally carry out that operation, manually erase the saved file, or delete the Temporary Internet Files (**Internet Explorer, Tools menu, Internet Options, General tab, Temporary Internet Files, Delete Files**).

Common programs use a directory to store their temporary work files. This directory is by default **C:\Documents and settings\\Local settings\Temp**.

When a program ends abnormally ("bug", etc.), it doesn't close the temporary files it had opened and they remain on the hard disk. Remember to regularly check that this directory doesn't contain copies of your sensitive files in a non-encrypted form.

Note:

You can find out where this directory is located by proceeding as follows: On your desktop, select the **My Computer** icon and press the right mouse button. In the contextual menu, click on **Properties**. In the **Advanced** tab, press the **Environment variables** button. In the **User variables** window, look for the directory that corresponds to the variables **TEMP** and **TMP**.

5 - Validy guarantee

Validy declaration of guarantee

Validy guarantees the proper state of functioning of this product as well as its conformity to the Validy specifications for a period of one year from its initial purchase by an end user. The customer must present an invoice or a guarantee certificate duly dated and trademarked in order to qualify for guarantee services.

Responsibilities

In no case can Validy be held responsible for the particular, incidental or indirect damage ensuing from owning or using this product or from any defect it might have, including material damage and, depending on the scope set by the law, corporal harm, even if Validy has been advised of such damage.

Validy does not guarantee the performance of this software when it is used with non-standard hardware or operating systems. The programs errors and related problems may ensue from an inappropriate configuration of the user's computer.

Hardware compatibilty

Validy guarantees the proper functioning of Validy File Crypt only with the referenced USB key.



www.validy.com