

VALIDY FILE CRYPT

Data theft protection file encryption

To protect files containing confidential data against any undesirable intervention it is indispensable to encrypt them.

So that the protection is solid, it is necessary to shelter the encryption secret from prying eyes, in a safe place. Nowadays the best way to preserve an encryption secret is to hide it in a smart card or a SIM.

Validy File Crypt stores the 128-bit secret key used for encryption in a chip.

The user can encrypt files whose data must stay confidential with a simple mouse click. An intruder wishing to read the confidential data is unable to do so without having the legitimate user's card or USB key in his possession. The theft of computer equipment containing confidential data would not allow the thief to read, use, exploit, publish or even sell said data.

The final choice of whether to encrypt data on a computer is up to the user. With Validy File Crypt, encrypted and non-encrypted files can co-exist on a computer or a network without presenting a problem.

Exchange of files by e-mail

The user can encrypt the confidential files that he wishes to send to a correspondent, and transmit them in complete security as e-mail attachments.

The confidential data travels encrypted over the Internet and the recipient decrypts the attachment using his Validy Confidential Mail smart card or USB key. The files received are then normally accessible.

Any individual or organization intercepting the confidential data during its transmission is unable to decrypt it without the transmitter's (or the recipient's) smart card or USB key.

Extremely solid protection

All security experts agree that the smart card is the best way to keep a secret.

The "simplest" attack consists in trying all the possible 2^{128} keys. The pirate then faces a mathematical problem: breaking a 128-bit encryption key requires 1 billion PC's that can test 1 billion keys per second, for 30 billion years (about twice the universe's age!).

Data theft protection

- Encryption of sensitive files
- Exchange of encrypted files by e-mail



Imagine your business.™



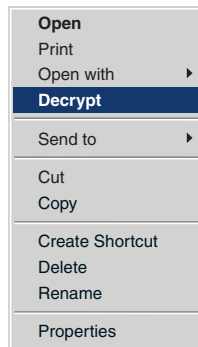
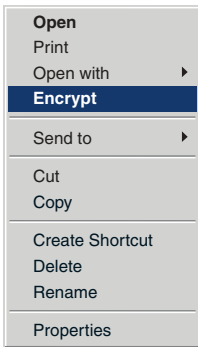
www.validy.com

File encryption

To encrypt a file, the user inserts his Validy File Crypt® smart card in the reader or connects his USB key. He next selects the file(s) to be encrypted and clicks the right mouse button to activate the **encryption command**. A few seconds later the files are protected. The extension of the encrypted file changes as well as its icon. The displayed icon carries the Validy trademark and the extension is ".vldy".

File decryption

To decrypt a file, the user inserts his Validy File Crypt® smart card in the reader or connects his USB key. He double-clicks with the mouse on the file to be decrypted (he may also select the file(s) to be decrypted and click on the right mouse button to activate the **decryption command**). The ".vldy" extension disappears and the original file icon reappears. The file then becomes normally accessible.



Validy File Crypt®, kit contents:

- a Validy File Crypt® smart card or SIM,
- an installation CD-ROM and a documentation,
- a smart card reader or a USB key.

Minimum requirements:

- PC with USB, or COM and PS/2, or PCMCIA interface,
- 4 Mb of hard disk space.

Operating system:

- COM and PCMCIA versions:
Windows 95, 98, NT, 2000, Millennium or XP.
- USB reader version:
Windows 98, 2000, Millennium or XP.
- USB key version:
Windows 2000 ou XP.



Transmit an encrypted file

Any file format can be encrypted and attached to an e-mail. Two Validy File Crypt users can therefore exchange encrypted files and decrypt them provided that they have the same secret key loaded in their smart card or SIM.

Security level choice

The user may add a PIN to protect himself from any illicit use of his card or USB key. He may also change the default secret key stored in his smart card or SIM and replace it with his own.

Smart card readers

The smart card readers provided by Validy have been qualified to work with Validy File Crypt®.

Products for connection to a PC:

- stand-alone reader with serial or USB interface,
- PCMCIA reader (for laptops),
- USB keyboard including a reader,
- USB key.

SAS VALIDY

ZI - 5, rue Jean Charcot - 26100 ROMANS / ISERE - FRANCE
Tel. +33 (0)4 75 717 717 - Fax +33 (0)4 75 717 718
RCS : Romans 382 975 639
info@validy.com

VALIDY Inc.

1001 SW Fifth Avenue, Suite 1100
PORTLAND, OR 97204 USA
Tel. +1 (503) 535 8078 - Fax +1 (503) 535 8077
info@validy.com