

VALIDY FILE CRYPT

Protection contre le vol d'informations

Pour protéger les fichiers contenant des données confidentielles contre toute lecture indésirable, il est indispensable de les crypter.

Pour que cette protection soit solide, il est nécessaire de conserver le secret de cryptage à l'abri de tout regard dans un support sûr.

Aujourd'hui, le meilleur moyen de préserver un secret est de le cacher dans une carte à puce ou un SIM.

Validy File Crypt utilise une puce pour conserver la clef secrète de 128 bits nécessaire au cryptage.

L'utilisateur peut donc encrypter d'un simple clic de souris les fichiers dont les données doivent rester confidentielles. Un intrus souhaitant lire ces données confidentielles est dans l'incapacité de le faire sans avoir en sa possession la carte à puce ou la clef USB de l'utilisateur. Le vol du matériel informatique contenant des données confidentielles ne permet pas au voleur, de les lire, de les exploiter, de les publier, ou même de les vendre.

Le choix de crypter ou non les fichiers appartient à l'utilisateur, il peut donc faire cohabiter sans aucun problème des fichiers cryptés et des fichiers non cryptés sur son ordinateur ou son réseau.

Echanges de fichiers par e-mail

L'utilisateur peut encrypter les fichiers sensibles qu'il souhaite envoyer à ses correspondants et les transmettre en toute sécurité en tant que pièces jointes à un e-mail.

Les données confidentielles voyagent cryptées sur l'Internet et le destinataire décrypte la pièce jointe reçue à l'aide de sa carte ou sa clef USB, les fichiers reçus sont alors accessibles normalement.

Tout individu ou organisme interceptant les données confidentielles lors de leur transmission est dans l'incapacité de les décrypter sans la carte à puce ou la clef USB de l'émetteur ou du récepteur.

Extrêmement robuste

Tous les experts en matière de sécurité s'accordent sur le fait que la carte à puce est le meilleur moyen de préserver un secret.

L'attaque la plus "simple" consiste à tester l'ensemble des 2^{128} clefs. Le pirate se retrouve alors face à un problème mathématique : casser une clef de 128 bits nécessite 1 milliard de PC capables de tester 1 milliard de clefs par seconde, pendant 30 milliards d'années (soit environ 2 fois l'âge de l'univers!).

Protection contre le vol d'informations

- cryptage des fichiers sensibles sur les PC
- échange par e-mail de fichiers cryptés



Imagine your business.™



www.validy.com

Cryptage d'un fichier

Pour encrypter un fichier, l'utilisateur insère sa carte à puce dans le lecteur, ou connecte sa clef USB.

Il sélectionne ensuite le ou les fichiers à encrypter, accède au menu contextuel d'un clic droit de souris, et choisit la commande "Encrypter".

Quelques secondes plus tard les fichiers sont protégés. L'extension du fichier encrypté change, ainsi que son icône. L'icône affichée est alors celle du logo Vality et l'extension ".vldy" lui est ajoutée.

Décryptage d'un fichier

Pour décrypter un fichier, l'utilisateur insère sa carte à puce dans le lecteur, ou connecte sa clef USB.

Il double-clique sur le fichier à décrypter (il peut aussi sélectionner le ou les fichiers à décrypter et cliquer sur le bouton droit de la souris pour activer la commande "Décrypter"). Le suffixe ".vldy" disparaît et l'icône originale du fichier réapparaît. Le fichier redevient alors accessible normalement.



■ Contenu du logiciel Vality File Crypt® :

- une carte à puce ou un SIM Vality File Crypt®,
- un CD-ROM d'installation et une documentation,
- un lecteur de cartes à puce ou une clef USB.

■ Configuration minimum :

- PC avec interface USB, ou COM et PS/2, ou PCMCIA,
- 4 Mo d'espace disque.

■ Système d'exploitation :

- version lecteur COM et PCMCIA : Windows 95, 98, NT, 2000, Millennium ou XP.
- version lecteur USB : Windows 98, 2000, Millennium ou XP.
- version clef USB : Windows 2000 ou XP.



Transmettre un fichier crypté

Tout format de fichier peut être crypté et attaché à un e-mail. Deux possesseurs de produits Vality File Crypt® peuvent donc s'échanger des fichiers cryptés et les décrypter s'ils ont la même clef secrète chargée dans leur carte à puce ou leur SIM.

Choix du niveau de sécurité

L'utilisateur peut ajouter un PIN code afin de se prémunir contre toute utilisation illicite de sa carte ou de sa clef USB. Il peut également changer la clef secrète par défaut contenue dans sa carte ou son SIM et la remplacer par une autre qui lui est propre.

Lecteurs

Les lecteurs de cartes à puce fournis par Vality ont été qualifiés pour fonctionner avec Vality File Crypt®.

Sont connectables au PC :

- un lecteur déporté sur port COM ou USB,
- un lecteur au format PCMCIA (pour les portables),
- un clavier USB intégrant un lecteur de cartes à puce,
- une clef USB.

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

© Copyright Mars 2001
Vality File Crypt est la propriété intellectuelle de SAS Vality
Vality et Imagine your business sont des marques déposées par SAS Vality et Vality Inc.
Distribution pour l'Union Européenne : SAS Vality
Distribution pour les Etats-Unis, le Canada, le Mexique, et les autres Etats hors Union Européenne : Vality Inc.