

PGP Personal Privacy pour Windows 95, 98 et NT

Manuel de l'Utilisateur

Version 6.0

[traduction française: <news:fr.misc.cryptologie>, 1998]

[Le texte de ce manuel reste la propriété de Network Associates Inc. (NAI).
NAI n'a pas donné son accord pour cette traduction, qui n'est procurée par
ses auteurs qu'à titre temporaire dans l'attente d'une version française
officielle de NAI]

Copyright © 1990-1998 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved.

PGP*, Version 6.0.2

11-98. Printed in the United States of America.

PGP, Pretty Good, and Pretty Good Privacy are registered trademarks of Network Associates, Inc. and/or its Affiliated Companies in the US and other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

Portions of this software may use public key algorithms described in U.S. Patent numbers 4,200,770, 4,218,582, 4,405,829, and 4,424,414, licensed exclusively by Public Key Partners; the IDEA(tm) cryptographic cipher described in U.S. patent number 5,214,703, licensed from Ascom Tech AG; and the Northern Telecom Ltd., CAST Encryption Algorithm, licensed from Northern Telecom, Ltd. IDEA is a trademark of AscomTech AG. Network Associates Inc. may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents. The compression code in PGP is by Mark Adler and Jean-Loup Gailly, used with permission from the free Info-ZIP implementation. LDAP software provided courtesy University of Michigan at Ann Arbor, Copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>). Copyright © 1995-1997 The Apache Group. All rights reserved. See text files included with the software or the PGP web site for further information. This software is based in part on the work of the Independent JPEG Group. Soft TEMPEST font courtesy of Ross Anderson and Marcus Kuhn.

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement and Limited Warranty provided with the software. The information in this document is subject to change without notice. Network Associates Inc. does not warrant that the information meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by Network Associates Inc.

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restrict the export and re-export of certain products and technical data.

Network Associates, Inc.	(408) 988-3832 main
3965 Freedom Circle	(408) 970-9727 fax
Santa Clara, CA 95054	http://www.nai.com
	info@nai.com

* is sometimes used instead of the ® for registered trademarks to protect marks registered outside of the U.S.

LIMITED WARRANTY

Limited Warranty. Network Associates Inc. warrants that the Software Product will perform substantially in accordance with the accompanying written materials for a period of sixty (60) days from the date of original purchase. To the extent allowed by applicable law, implied warranties on the Software Product, if any, are limited to such sixty (60) day period. Some jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Customer Remedies. Network Associates Inc's and its suppliers' entire liability and your exclusive remedy shall be, at Network Associates Inc's option, either (a) return of the purchase price paid for the license, if any or (b) repair or replacement of the Software Product that does not meet Network Associates Inc's limited warranty and which is returned at your expense to Network Associates Inc. with a copy of your receipt. This limited warranty is void if failure of the Software Product has resulted from accident, abuse, or misapplication. Any repaired or replacement Software Product will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, neither these remedies nor any product support services offered by Network Associates Inc. are available without proof of purchase from an authorized international source and may not be available from Network Associates Inc. to the extent they subject to restrictions under U.S. export control laws and regulations.

NO OTHER WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT FOR THE LIMITED WARRANTIES SET FORTH HEREIN, THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" AND NETWORK ASSOCIATES, INC. AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, CONFORMANCE WITH DESCRIPTION, TITLE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM JURISDICTION TO JURISDICTION.

LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL NETWORK ASSOCIATES, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES OR LOST PROFITS WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF NETWORK ASSOCIATES, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, NETWORK ASSOCIATES, INC'S CUMULATIVE AND ENTIRE LIABILITY TO YOU OR ANY OTHER PARTY FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS OR ACTIONS ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED THE PURCHASE PRICE PAID FOR THIS LICENSE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Table des Matières

Préface	9
Comment contacter Network Associates.....	9
Service clients	9
Assistance technique.....	9
Vos réactions sont bienvenues	10
Formation Network Associates.....	10
Lectures recommandées	10
Chapitre 1. Introduction à PGP	13
Quoi de neuf dans PGP version 6.0.....	13
Utiliser PGP	15
Un rapide aperçu	15
Les étapes fondamentales pour utiliser PGP.....	15
Chapitre 2. Commencer	19
Lancer PGP.....	19
Utiliser PGP depuis la barre des tâches.....	19
Exécuter les fonctions de PGP depuis le presse-papiers	19
Ouvrir la fenêtre de PGPkeys.....	20
Régler les préférences de PGP	20
Obtenir de l'aide	20
Quitter PGP	20
Utiliser PGP depuis les applications e-mail gérées.....	21
Utiliser PGP/MIME	21
Utiliser PGP depuis PGPtools.....	21
Utiliser PGP depuis l'Explorateur Windows.....	22
Sélectionner les destinataires	22
Prendre les raccourcis	23
Description des icônes de PGPkeys	23
Chapitre 3. Créer et Echanger des Clés	27
Notion de clé	27
Créer une paire de clés	28
Créer une phrase secrète dont vous vous rappellerez.....	32
Ajouter un ID photographique à votre clé.....	33
Créer de nouvelles sous-clés	35
Scission de clé	36

Protéger vos clés	39
Distribuer votre clé publique	40
Rendre votre clé publique disponible via un serveur de clés	40
Mettre à jour votre clé sur un serveur de clés.....	41
Enlever des signatures ou des noms d'utilisateur associés à votre clé.....	41
Inclure votre clé publique dans un message e-mail	42
Exporter votre clé publique dans un fichier.....	43
Obtenir les clés publiques d'autrui	43
Récupérer des clés publiques depuis un serveur de clés.....	43
Ajouter une clé publique depuis un message e-mail.....	44
Importer une clé publique depuis un fichier	45
Vérifier l'authenticité d'une clé.....	45
Signer la clé publique	46
Obtenir des clés publiques via des avals de confiance	46
Chapitre 4. Envoyer et Recevoir des E-mails Sécurisés	49
Crypter et signer des e-mails.....	49
Crypter et signer avec des applications e-mail gérées.....	49
Crypter un e-mail pour des groupes de destinataires	53
Travailler avec des listes de distribution	54
Envoyer un e-mail crypté et signé à des listes de distribution	54
Décrypter et vérifier un e-mail	55
Chapitre 5. Utiliser PGP pour le Stockage Sécurisé de Fichiers	59
Utiliser PGP pour crypter et décrypter des fichiers.....	59
Utiliser le menu du clic-droit de PGP pour crypter et signer.....	59
Utiliser PGPtools pour crypter et signer	61
Utiliser PGPtray pour décrypter et vérifier.....	63
Utiliser PGPtools pour décrypter et vérifier	64
Signer et décrypter des fichiers avec une clé scindée.....	64
Utiliser PGP Wipe pour effacer des fichiers.....	69
Utiliser le PGP Free Space Wiper pour nettoyer l'espace libre sur vos disques.....	70
Chapitre 6. Gestion des Clés et Réglage des Préférences	73
Gérer vos clés	73
La fenêtre PGPkeys.....	73
Description des attributs PGPkeys.....	74
Examiner les propriétés d'une clé.....	76
Fenêtre key properties, onglet General	77
Fenêtre key properties, onglet Subkey.....	78
Spécifier une paire de clés par défaut.....	79

Ajouter un nouveau nom d'utilisateur ou adresse à une paire de clés.....	79
Vérifier une clé publique	80
Signer une clé publique	81
Accorder sa confiance pour valider des clés.....	84
Désactiver et activer des clés.....	84
Effacer une clé, une signature ou un ID d'utilisateur.....	85
Changer votre phrase secrète	85
Importer et Exporter des Clés.....	86
Révoquer une clé	87
Régler vos préférences.....	88
Rechercher une clé	98
Chapitre 7. PGPdisk.....	101
Qu'est-ce que PGPdisk?	101
Fonctionnalités PGPdisk	101
Pourquoi utiliser PGPdisk?	102
Démarrer PGPdisk.....	102
Travailler avec des Volumes PGPdisk	103
Créer un nouveau volume PGPdisk.....	103
Changer une phrase secrète.....	105
Ajouter des phrases secrètes auxiliaires	106
Retirer une phrase secrète.....	107
Retirer toutes les phrases secrètes auxiliaires.....	108
Ajouter ou retirer des clés publiques	108
Ouvrir un volume PGPdisk	109
Utiliser un volume PGPdisk ouvert	110
Fermer un volume PGPdisk.....	110
Spécifier les Préférences	111
Entretenir des Volumes PGPdisk	112
Ouvrir des fichiers PGPdisk sur un serveur distant.....	112
Ouverture automatique des volumes PGPdisk.....	112
Sauvegarder des volumes PGPdisk.....	112
Echanger des volumes PGPdisk	113
Changer la taille d'un volume PGPdisk.....	113
Détails Techniques et Réflexions sur la Sécurité	114
A propos des volumes PGPdisk.....	114
L'algorithme de chiffrement de PGPdisk	114
Qualité de la Phrase Secrète.....	115
Précautions Spéciales de Sécurité prises par PGPdisk.....	116
Effacement de la phrase secrète	116

Protection relative à la mémoire virtuelle.....	116
Protection contre la rémanence électrostatique en mémoire vive.....	116
Autres réflexions à propos de la sécurité	117
Appendice A. Dysfonctionnements de PGP	119
Appendice B. Echanger des Fichiers entre Mac et Windows	123
Transmettre de MacOS vers Windows	124
Recevoir des fichiers Windows sous MacOS	125
Applications reconnues	126
Appendice C. Phil Zimmermann sur PGP	129
Pourquoi j'ai écrit PGP.....	129
Les chiffres symétriques de PGP	133
A propos des routines de compression de données PGP	134
A propos des nombres aléatoires utilisés comme clés de session.....	135
A propos des contractions de message.....	135
Comment protéger les clés publiques de la falsification	136
Comment PGP reconnaît-il les clés valides?	139
Comment protéger ses clés secrètes de la divulgation	141
Que faire si vous perdez votre clé secrète?	142
Méfiez-vous de la poudre de perlimpinpin	142
Vulnérabilités	146
Phrase secrète et clé privée compromises	147
La falsification de clé publique.....	147
Fichiers pas tout à fait effacés.....	147
Virus et chevaux de Troie	148
Fichiers d'échange et/ou mémoire virtuelle	149
Brèche dans la sécurité physique	150
Les attaques Tempest	150
Se protéger contre les fausses empreintes de date	151
Divulgation sur des systèmes multi utilisateurs.....	152
Analyse de trafic.....	152
Cryptanalyse.....	152
Glossaire.....	155
Index	159

Préface

Ce livre explique comment utiliser PGP® pour Windows 95, 98 et NT.

PGP dispose de nombreuses nouvelles fonctionnalités, qui sont décrites dans le [Chapitre 1, “Introduction à PGP.”](#)

Si vous êtes novice en cryptographie et aimeriez un aperçu de la terminologie et des concepts que vous rencontrerez en utilisant PGP, voir *Une Introduction à la Cryptographie*.

Comment contacter Network Associates

Il y a plusieurs façons de trouver plus d'informations à propos de PGP et de ses produits.

Service clients

Pour acheter des produits ou obtenir de l'information sur le produit, contactez le département clients de Network Associates au (408) 988-3832, ou écrivez à l'adresse suivante:

Network Associates, Inc.
McCandless Towers
3965 Freedom Circle
Santa Clara, CA 95054-1203
U.S.A.

Assistance technique

Network Associates est célèbre pour l'attention portée à la satisfaction de ses clients. Nous poursuivons cette tradition en faisant de notre site Internet une ressource de valeur pour répondre aux questions relevant de l'assistance technique. Nous vous encourageons à l'utiliser comme votre première ressource afin d'y trouver des réponses aux questions fréquemment posées, pour les mises à jour des logiciels de Network Associates, et pour consulter les informations et les nouveautés de Network Associates en matière de cryptographie.

World Wide Web

<http://www.nai.com>

[Une filiale de Network Associates, Inc. est installée aux Pays-Bas:

<http://www.pgpinternational.com/>]

L'assistance technique pour vos produits PGP est également accessible par les moyens suivants:

Téléphone

(408) 988-3832

E-mail

PGPSupport@pgp.com

Pour que nous puissions vous donner rapidement et efficacement les réponses que vous demandez, le personnel d'assistance technique a besoin de certaines informations concernant votre ordinateur et vos logiciels. Veuillez tenir cette information prête avant de nous appeler:

- Nom du produit PGP
- Version du produit PGP
- Type d'ordinateur et de processeur
- Taille de la mémoire RAM disponible
- Système d'exploitation, avec sa version, et type de réseau
- Texte précis de tout message d'information ou d'erreur qui serait apparu à l'écran, ou enregistré dans un fichier journal (tous les produits n'offrent pas la fonctionnalité d'un fichier-journal)
- Nom et version de l'application e-mail utilisée (si le problème provient de l'intégration de PGP avec un logiciel d'e-mail, comme par exemple le plug-in Eudora)
- Etapes spécifiques pour reproduire le problème

Vos réactions sont bienvenues

Nous améliorons continuellement les produits PGP et nous faisons bon accueil aux réactions des clients quand nous concevons les nouvelles versions. Nous apprécions votre intérêt pour les produits PGP et vos avis sur le contenu du produit et sa fonctionnalité. Des réactions comme les vôtres nous aident à développer des logiciels et des services plus riches et faciles à utiliser. Tout en ne pouvant pas incorporer toutes les suggestions, nous prendrons votre contribution en considération lors du développement des futurs produits.

Formation Network Associates

Pour tout renseignement au sujet de programmes de formation sur site pour tout produit Network Associates, téléphoner au (800) 338-8754.

Lectures recommandées

Livres non techniques et techniques pour débutants

- Whitfield Diffie and Susan Eva Landau, "Privacy on the Line," *MIT Press*; ISBN: 0262041677
Ce livre est une discussion de l'histoire et de la politique autour de la cryptographie et de la sécurité des communications. C'est un excellent livre, même pour les débutants et les gens non rompus à la technique, mais avec une information que même beaucoup d'experts ne connaissent pas.
- David Kahn, "The Codebreakers" *Scribner*; ISBN: 0684831309
Ce livre est une histoire des codes et des casseurs de codes depuis l'époque

des Egyptiens jusqu'à la fin de la Seconde Guerre Mondiale. Kahn l'a d'abord écrit dans les années 60, et il y a eu une édition révisée en 1996. Ce livre ne vous enseignera rien sur la façon dont la cryptographie est mise en œuvre, mais il a été l'inspiration de toute la génération moderne des cryptographes.

- Charlie Kaufman, Radia Perlman, and Mike Spencer, "Network Security: Private Communication in a Public World," *Prentice Hall*; ISBN: 0-13-061466-1
C'est une bonne description des systèmes de sécurité des réseaux et des protocoles, incluant des descriptions de ce qui marche, ce qui ne marche pas, et pourquoi. Publié en 1995, il n'a pas beaucoup des dernières progrès, mais c'est encore un bon livre. Il contient aussi une des plus claires descriptions jamais écrites de la façon dont marche le DES.

Livres de niveau intermédiaire

- Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," *John Wiley & Sons*; ISBN: 0-471-12845-7
C'est un bon livre pour débiter dans la technique sur la façon dont beaucoup de cryptographie fonctionne. Si vous voulez devenir un expert, c'est ici qu'il faut commencer [ouvrage traduit en français aux Editions ITP].
- Alfred J. Menezes, Paul C. van Oorschot, and Scott Vanstone, "Handbook of Applied Cryptography," *CRC Press*; ISBN: 0-8493-8523-7
C'est un livre technique que vous devriez prendre après Schneier. Il y a beaucoup de maths pures et dures dans ce livre, mais il est néanmoins utilisable pour ceux qui ne comprennent pas les maths.
- Richard E. Smith, "Internet Cryptography," *Addison-Wesley Pub Co*; ISBN: 020192480
Ce livre décrit beaucoup de protocoles de sécurité d'Internet. Surtout, il explique comment les systèmes bien conçus finissent pourtant par avoir des défauts à travers certaines opérations. Ce livre est léger sur les maths et chargé d'informations pratiques.
- William R. Cheswick and Steven M. Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker" *Addison-Wesley Pub Co*; ISBN: 0201633574
Ce livre est écrit par deux chercheurs importants des laboratoires AT&T Bell Labs, à propos de ses expériences dans le maintien et la remise à plat de la connexion Internet de AT&T. Très lisible.

Livres de niveau avancé

- Neal Koblitz, "A Course in Number Theory and Cryptography" *Springer-Verlag*; ISBN: 0-387-94293-9
Un excellent livre de niveau manuel pour diplômé en mathématiques sur de nombreuses théories et la cryptographie.
- Eli Biham and Adi Shamir, "Differential Cryptanalysis of the Data Encryption Standard," *Springer-Verlag*; ISBN: 0-387-97930-1
Ce livre décrit la technique de la cryptanalyse différentielle telle qu'appliquée au DES. C'est un excellent livre pour apprendre des choses sur cette technique.

Bienvenue dans PGP. Avec PGP, vous pouvez aisément et en toute sécurité protéger la confidentialité de vos données en les cryptant de telle façon que seuls les individus concernés puissent les lire. Vous pouvez aussi signer numériquement l'information, ce qui garantit son authenticité.

Quoi de neuf dans PGP version 6.0

Cette version de PGP comprend ces nouvelles fonctionnalités:

- **Visionneuse sécurisée.** Secure Viewer est une solution logicielle de PGP pour protéger l'information confidentielle affichée sur l'écran de votre moniteur d'une interception par capture de ses émissions électromagnétiques – connue sous le nom d'attaque TEMPEST. Il est notoire que les intercepteurs, avec l'équipement spécial, peuvent capturer et reconstruire le contenu visuel d'un écran à partir du rayonnement de fréquence radio. Quand le texte est crypté avec l'option Secure Viewer activée, le texte décrypté est affiché dans une police et une fenêtre spéciales résistantes à l'attaque TEMPEST, illisibles par l'équipement de capture de rayonnement. Le dispositif Secure Viewer vous permet de regarder votre texte décrypté en sécurité. [NdT: cette police de caractères ne gère pas le format ASCII étendu, par exemple les caractères accentués français]
- **Fonctionnalité PGPdisk.** La fonctionnalité PGPdisk est intégrée dans la version 6.0. PGPdisk de PGP est une application de cryptage facile d'emploi qui vous permet de réserver une partie de l'espace disque pour stocker vos données sensibles.
- **Plug-ins supplémentaires.** Des plug-ins e-mail pour Outlook Express [des dysfonctionnements peuvent apparaître avec la version française d'Outlook Express] et Outlook 98 sont inclus. Un plug-in Groupwise est disponible séparément.
- **ID d'utilisateur photographiques.** Vous pouvez ajouter votre photographie à votre clé publique. Les ID [nom identifiant l'utilisateur] photographiques peuvent être signés exactement comme un ID d'utilisateur pour donner une information supplémentaire lors de la vérification de la clé.
- **Communications sécurisées avec le Serveur de Certificat de clé PGP 2.0.** PGP fournit une connexion sécurisée quand une demande est envoyée au serveur. Cette connexion sécurisée empêche toute analyse de trafic qui pourrait déterminer les clés que vous récupérez du serveur ou lui envoyez.
- **Effacement sécurisé depuis le Serveur de Certificat PGP.** Vous pouvez effacer ou désactiver votre propre clé en vous authentifiant vous-même à travers la Transport Layer Security [couche de transport sécurisé] (TLS).

- **Barre d'outils PGPkeys.** Une barre d'outils avec icônes a été ajoutée à PGPkeys pour un accès facile aux fonctions de gestion des clés les plus fréquemment utilisées.
- **Recherche des destinataires ou des signataires inconnus sur les serveurs.** Quand vous décryptez un message, vous pouvez automatiquement exécuter une recherche sur le serveur de toutes les clés pour lesquelles il a été crypté ou par lesquelles il a été signé pour déterminer leur identité.
- **Gestion des sous-clés.** (clés Diffie-Hellman/DSS seulement) Avec la fonction de gestion des sous-clés, vous pouvez gérer séparément vos clés de cryptage (DH) et de signature (DSS).
- **Revérification de signature.** Les signatures attachées aux clés sont vérifiées automatiquement quand elles sont ajoutées à votre trousseau de clés. Il est possible, cependant, à travers une altération des données ou une falsification malicieuse, que des signatures invalides existent. Cette nouvelle fonction vous permet de revérifier les signatures pour s'assurer qu'elles sont valides.
- **Expiration de signature.** Vous pouvez créer des signatures sur d'autres clés qui expireront après une date donnée.
- **Interface améliorée.** Une barre d'outils intuitive a été ajoutée à PGPkeys pour un accès aisé aux fonctions les plus fréquemment utilisées de gestion des clés.
- **Intégration à l'application améliorée.** PGPTray permet de procéder aux opérations de cryptage/décryptage/vérification avec la plupart des applications sans qu'il y ait besoin pour l'utilisateur de faire un copier-coller explicite.
- **Nettoyage de l'espace libre.** PGPtools a maintenant la capacité de nettoyer (wipe) tout l'espace libre sur vos disques.
- **Nettoyage amélioré.** Le nettoyage (wipe) de fichier et de disque utilisent maintenant tous les deux un jeu d'instructions significativement améliorées pour l'effacement multiple spécialement réglé pour le type de support utilisé dans les ordinateurs d'aujourd'hui.
- **Scission de clé.** Toute clé privée de haute sécurité peut être scindée entre plusieurs "dépositaires de fragments" (shareholders) en utilisant un procédé cryptographique connu sous le nom de scission Blakely-Shamir.
- **Révocateurs désignés.** Vous pouvez maintenant spécifier qu'une autre clé publique de votre trousseau de clés est autorisée à révoquer votre clé. Cela peut être utile dans des situations où vous craignez de perdre votre clé privée, d'oublier votre phrase secrète, ou dans des cas extrêmes telle une incapacité physique d'utiliser la clé. Dans certains cas, le tiers que vous avez désigné pourra révoquer votre clé, l'envoyer au serveur et ce sera exactement comme si vous l'aviez révoquée vous-même.

Nouvelles fonctionnalités de PGPdisk

- **Gestion des clés publiques.** Une ou plusieurs clés publiques peuvent désormais être configurées pour ouvrir un volume PGPdisk. Cette possibilité est intégrée à PGP 6.0 et à ses trousseaux de clés. Par exemple, si Robert veut permettre à sa femme Marie d'accéder à ses volumes PGPdisk, il peut le faire

en ajoutant sa clé publique à ses volumes PGPdisk. La clé pour ouvrir le volume sera cryptée avec la clé de Marie.

- **Assistant de création de nouveau disque.** Le processus de création de volume a été simplifié par un New Disk Wizard qui vous guide pas à pas à travers ce processus.
- **Compatibilité avec Windows NT.** PGPdisk fonctionne maintenant aussi sous Windows NT 4.0 en plus de Windows 95, 98 et MacOS.

Utiliser PGP

PGP est un logiciel de sécurité qui permet à vous et à vos collaborateurs d'échanger et de stocker de l'information de manière sûre, de telle sorte que personne d'autre ne puisse la lire.

Une des façons les plus commodes d'utiliser PGP est de le faire avec l'un des logiciels d'e-mail courants gérés par les plug-ins PGP. Avec ces plug-ins, vous cryptez et signez aussi bien que décryptez et vérifiez vos messages tout en composant et en lisant votre e-mail avec un simple clic sur un bouton.

Si vous utilisez une application e-mail qui n'est pas gérée par les plug-ins, vous pouvez aisément crypter le texte du message en utilisant PGPTray [disponible dans la barre des tâches]. En outre, si vous avez besoin de crypter ou décrypter des fichiers attachés, vous pouvez le faire directement depuis le presse-papiers de Windows en choisissant l'option de menu appropriée. Vous pouvez aussi utiliser PGP pour crypter et signer des fichiers sur le disque dur de votre ordinateur aux fins de stockage sécurisé, pour nettoyer des fichiers de votre disque dur ou pour nettoyer l'espace libre du disque de telle sorte que des données sensibles ne puissent pas être récupérées avec des logiciels de restauration de disque.

Un rapide aperçu

PGP est basé sur une technologie largement admise connue sous le nom de *cryptographie à clé publique* dans laquelle deux clés complémentaires, appelées *paire de clés*, sont utilisées pour assurer des communications sécurisées. Une de ces clés est désignée comme *clé privée* à laquelle vous seul avez accès et l'autre clé est une *clé publique* que vous échangez librement avec les autres utilisateurs de PGP. Votre clé privée et votre clé publique sont stockées toutes les deux dans des fichiers de trousseaux de clés, qui sont accessibles depuis la fenêtre de PGPkeys. C'est depuis cette fenêtre que vous effectuez toutes vos opérations de gestion des clés.

Pour un aperçu exhaustif de la technologie de cryptage de PGP, veuillez vous référer à "*Une Introduction à la Cryptographie.*" qui est inclus dans ce produit.

Les étapes fondamentales pour utiliser PGP

Cette partie donne un aperçu des procédures que vous suivez normalement au cours de l'utilisation de PGP. Pour des détails concernant certaines de ces procédures, veuillez vous référer aux chapitres appropriés de ce livre.

1. Installez PGP sur votre ordinateur. Veuillez vous référer au *PGP Installation Guide* inclus dans ce produit pour des instructions complètes sur l'installation.
2. Créez une paire de clés privée et publique.

Avant de pouvoir commencer à utiliser PGP, vous devez générer une paire de clés. Une paire de clés PGP est composée d'une clé privée à laquelle vous seul avez accès et d'une clé publique que vous pouvez copier et rendre librement accessible à quiconque avec qui vous voulez échanger de l'information.

Vous avez la possibilité de créer une nouvelle paire de clés immédiatement après avoir fini la procédure d'installation de PGP, ou vous pouvez le faire à n'importe quel moment en ouvrant PGPkeys.

Pour plus d'informations à propos de la création de la paire de clés privée et publique, veuillez vous référer à [“Créer une paire de clés” en page 28](#).

3. Echanger des clés publiques avec autrui.

Après avoir créé une paire de clés, vous pouvez commencer à correspondre avec d'autres utilisateurs de PGP. Vous aurez besoin d'une copie de leur clé publique et ils auront besoin d'une copie de la vôtre. Votre clé publique est tout simplement un bloc de texte, il est donc très facile d'échanger des clés avec quelqu'un. Vous pouvez inclure votre clé publique dans un message e-mail, la copier dans un fichier, ou la poster sur un serveur public ou un serveur d'entreprise où n'importe qui pourra en obtenir une copie quand il en aura besoin.

Pour plus d'informations à propos de l'échange des clés publiques, veuillez vous référer à [“Distribuer votre clé publique” en page 40](#) et [“Obtenir les clés publiques d'autrui” en page 43](#).

4. Valider des clés publiques.

Une fois que vous avez une copie de la clé de quelqu'un, vous pouvez l'ajouter à votre trousseau de clés publiques. Vous devriez ensuite la vérifier afin d'être sûr que la clé n'a pas été falsifiée et qu'elle appartient bien au propriétaire indiqué. Vous faites cela en comparant *l'empreinte* unique sur votre copie de la clé à l'empreinte de la clé originale de cette personne. Quand vous êtes sûr que vous avez une clé publique authentique, vous la signez pour indiquer que vous estimez que la clé est d'usage sûr. En outre, vous pouvez accorder au propriétaire de la clé un niveau de fiabilité indiquant le degré de confiance que vous mettez dans cette personne pour se porter garante de l'authenticité de la clé publique d'autrui.

Pour plus d'informations à propos de la validation des clés publiques, veuillez vous référer à [“Vérifier l'authenticité d'une clé” en page 45](#).

5. Crypter et signer vos e-mails et vos fichiers.

Après avoir généré votre paire de clés et avoir échangé des clés publiques, vous pouvez commencer à crypter et signer des messages e-mails et des fichiers.

- Si vous utilisez une application e-mail gérée par les plug-ins, vous pouvez crypter et signer en sélectionnant l'option appropriée depuis la barre d'outils de l'application.

- Si votre application e-mail n'est pas gérée par les plug-ins, vous pouvez utiliser les fonctions appropriées depuis GPGtray. Vous pouvez aussi crypter et signer des fichiers depuis GPGtools avant de les attacher à votre e-mail. Crypter assure que seuls vous et vos destinataires concernés pouvez décrypter le contenu des fichiers; signer assure que toute falsification sera immédiatement apparente.

Pour plus d'informations à propos du cryptage et de la signature de l'information, veuillez vous référer à [“Crypter et signer des e-mails” en page 49](#).

6. Décrypter et vérifier vos e-mails et fichiers.

Quand quelqu'un vous envoie des données cryptées, vous pouvez décrypter le contenu et vérifier toute signature attachée pour être sûr que les données proviennent de l'expéditeur déclaré et qu'elles n'ont pas été altérées.

- Si vous utilisez une application e-mail qui est gérée par les plug-ins, vous pouvez décrypter et vérifier vos messages en sélectionnant l'option appropriée depuis la barre d'outils de votre application.
- Si votre application e-mail n'est pas gérée par les plug-ins, vous pouvez copier le message vers le presse-papiers et de là effectuer les opérations appropriées. Si vous voulez décrypter et vérifier les fichiers attachés, vous pouvez le faire depuis le presse-papiers de Windows. Vous pouvez aussi décrypter les fichiers cryptés stockés sur votre ordinateur, et vérifier les fichiers signés pour vous assurer qu'ils n'ont pas été falsifiés.

Pour plus d'informations à propos du décryptage et de la vérification des données, veuillez vous référer à [“Décrypter et vérifier un e-mail” en page 55](#).

7. Nettoyer des fichiers.

Quand vous avez besoin de détruire un fichier de façon définitive, vous pouvez utiliser la fonction Wipe [nettoyer] pour vous assurer que le fichier est irrécupérable. Le fichier est immédiatement écrasé de telle sorte qu'il ne puisse pas être récupéré en utilisant un utilitaire de récupération de disque.

Pour plus d'informations à propos du nettoyage des fichiers, veuillez vous référer à [“Utiliser PGP Wipe pour effacer des fichiers” en page 69](#).

Ce chapitre explique comment lancer PGP et donne un rapide aperçu des procédures que vous suivrez normalement dans l'utilisation de ce produit. Il contient aussi une table des icônes utilisées par PGPkeys.

Lancer PGP

PGP travaille sur les données générées par d'autres applications. Par conséquent, les fonctions appropriées de PGP sont conçues pour être immédiatement à votre disposition en fonction de la tâche que vous effectuez à un moment donné. Il y a quatre façons principales d'utiliser PGP:

- Depuis la barre des tâches (PGPtray)
- Depuis une application e-mail (PGP e-mail plug-ins)
- Depuis le menu Fichier de l'Explorateur Windows
- Depuis la barre d'outils de PGPtools

Utiliser PGP depuis la barre des tâches

Vous pouvez accéder à beaucoup des fonctions principales de PGP en cliquant sur l'icône en forme de verrou, qui est normalement placée dans la barre des tâches, et ensuite choisir la commande appropriée du menu. (Si vous ne trouvez pas cette icône dans la barre des tâches, lancez PGPtray depuis le menu Démarrer).

Exécuter les fonctions de PGP depuis le presse-papiers

Vous noterez que beaucoup des options de la barre des tâches se réfèrent aux fonctions de PGP que vous réalisez depuis le presse-papiers de Windows. Si vous utilisez une application e-mail qui n'est pas gérée par les plug-ins de PGP, ou si vous êtes en train de travailler avec du texte généré par d'autres applications, vous exécutez vos opérations de cryptage/décryptage et signature/vérification depuis le presse-papiers de Windows.

Par exemple, pour crypter ou signer du texte, vous le copiez de votre application vers le presse-papiers, le cryptez et le signez en utilisant les fonctions appropriées de PGP, puis le collez à nouveau dans votre application avant de l'envoyer aux destinataires concernés. Quand vous recevez un message crypté ou signé, vous renversez simplement le processus et copiez le texte crypté, connu sous le nom de *texte chiffré*, depuis l'application jusqu'au presse-papiers, décryptez et vérifiez l'information, et ensuite en voyez le contenu. Après avoir vu le message décrypté, vous pouvez décider soit de sauvegarder l'information, soit de la laisser sous sa forme cryptée.

Ouvrir la fenêtre de PGPkeys

Quand vous choisissez Launch PGPkeys depuis le menu déroulant de PGP, la fenêtre de PGPkeys s'ouvre, montrant la paire de clés privée et publique que vous avez créée pour vous-même ainsi que toutes les clés publiques des autres utilisateurs que vous avez ajoutées à votre trousseau de clés publiques. (Si vous n'avez pas déjà créé une nouvelle paire de clés, le PGP Key Generation Wizard [Assistant de Génération de Clé de PGP] vous guide à travers les étapes nécessaires. Cependant, avant d'entamer le processus de création d'une nouvelle paire de clés, vous devriez voir le [Chapitre 3](#) pour les détails complets sur les diverses options.)

Depuis la fenêtre de PGPkeys, vous pouvez créer une nouvelle paire de clés et gérer toutes vos autres clés. Par exemple, c'est là que vous examinez les propriétés d'une clé particulière, spécifiez le degré de certitude que la clé appartient réellement au propriétaire prétendu, et indiquez la confiance que vous placez dans le propriétaire de la clé pour se porter garant de l'authenticité des clés des autres utilisateurs. Pour une description exhaustive des fonctions de gestion des clés que vous effectuez depuis la fenêtre de PGPkeys, voir le [Chapitre 6](#).

Régler les préférences de PGP

Quand vous choisissez PGP Preferences depuis le menu déroulant de PGP, vous accédez à la boîte de dialogue des préférences de PGP dans laquelle vous spécifiez les réglages qui influent sur le fonctionnement de PGP sur votre ordinateur.

En cliquant sur l'onglet approprié, vous pouvez aller aux réglages des préférences que vous voulez modifier. Pour une description complète de ces réglages, voir le [Chapitre 6](#).

Obtenir de l'aide

Quand vous choisissez Help depuis le menu ou la fenêtre PGP, vous accédez à l'aide de PGP, qui donne un aperçu général et des instructions pour la totalité des opérations que vous désirez effectuer. La plupart des boîtes de dialogue disposent aussi d'aides contextuelles, auxquelles vous accédez en cliquant sur le point d'interrogation dans le coin droit de la fenêtre et en pointant ensuite vers l'endroit qui vous intéresse sur l'écran. Une courte explication apparaît.

Quitter PGP

Par défaut, PGPTray se lance à chaque fois que vous démarrez votre ordinateur, comme l'indique la présence de l'icône en forme de verrou dans la barre des tâches. Si pour une raison ou une autre vous avez besoin de fermer PGPTray, vous pouvez le faire en choisissant Exit PGPTray dans le menu déroulant de PGP.

Utiliser PGP depuis les applications e-mail gérées

Si vous disposez de l'une des applications gérées par les plug-ins PGP, vous pouvez accéder aux fonctions nécessaires de PGP en cliquant sur le bouton approprié dans la barre d'outils de l'application:

- Qualcomm Eudora
- Microsoft Exchange
- Microsoft Outlook
- Microsoft [Outlook] Express
- Novell Groupwise (disponible séparément)

Par exemple, vous cliquez sur l'icône figurant l'enveloppe et le verrou () pour indiquer que vous voulez crypter votre message et sur celle figurant le crayon et le papier () pour indiquer que vous voulez signer votre message. Certaines applications possèdent aussi une icône représentant un verrou et une plume (), qui vous permet de réaliser les deux opérations en une seule fois.

Quand vous recevez un e-mail d'un autre utilisateur de PGP, vous décryptez le message et vérifiez la signature numérique de la personne en cliquant sur le verrou ouvert et l'enveloppe (), ou en sélectionnant "Decrypt/Verify" depuis le menu PGP ().

Vous pouvez aussi accéder à la fenêtre de PGPkeys à tout moment pendant la composition ou la récupération de votre e-mail en cliquant sur le bouton PGPkeys () dans certains plug-ins.

Utiliser PGP/MIME

Si vous utilisez une application e-mail avec un des plug-ins qui gère le standard PGP/MIME, et que vous communiquez avec un autre utilisateur dont l'application e-mail gère aussi cette norme, vous pouvez tous les deux crypter et décrypter vos messages e-mail et automatiquement tous les fichiers attachés quand vous envoyez ou récupérez votre e-mail. Tout ce que vous avez à faire est d'activer les fonctions de cryptage et de signature depuis la boîte de dialogue PGP Preferences.

Quand vous recevez un e-mail de quelqu'un qui utilise la fonctionnalité PGP/MIME, il arrive avec une icône attachée dans la fenêtre du message indiquant que c'est encodé en PGP/MIME.

Pour décrypter les textes et fichiers attachés dans un e-mail encapsulé en PGP/MIME, et pour vérifier les signatures numériques, vous cliquez simplement sur l'icône verrou et plume (). Les attachements sont quand même cryptés si PGP/MIME n'est pas utilisé, mais le processus de décryptage est alors plus compliqué pour le destinataire.

Utiliser PGP depuis PGPtools

Si vous utilisez une application e-mail qui n'est pas gérée par les plug-ins, ou si vous voulez exécuter des fonctions de PGP depuis une autre application, vous

pouvez crypter et signer, décrypter et vérifier, ou nettoyer de façon sécurisée des messages et des fichiers directement depuis la fenêtre PGTools. Vous pouvez ouvrir la fenêtre de PGTools ainsi:

- Cliquer sur Démarrer -->Programs-->PGP-->PGTools.
- Cliquer sur l'icône PGTools (🔑) dans la barre des tâches.

Quand la fenêtre PGTools (Figure 2-1) s'ouvre, vous pouvez commencer votre travail de cryptage.



Figure 2-1. Fenêtre de PGTools

Si vous travaillez avec du texte ou des fichiers, vous pouvez crypter, décrypter, signer, et vérifier en sélectionnant texte ou fichier et en le déposant ensuite sur le bouton approprié dans la fenêtre de PGTools.

Si vous travaillez avec des fichiers, cliquez sur le bouton approprié dans la fenêtre de PGTools pour choisir un fichier ou sélectionnez le presse-papiers.

Utiliser PGP depuis l'Explorateur Windows

Vous pouvez crypter et signer ou décrypter et vérifier des fichiers tels que des documents de traitement de texte, de tableur et de vidéo clips directement depuis l'Explorateur Windows. Si vous n'utilisez pas une application e-mail comme Qualcomm Eudora, qui gère le standard PGP/MIME, ou une application comme Exchange ou Outlook qui ne requiert pas PGP pour crypter ou signer des fichiers, vous devez utiliser cette méthode pour les fichiers attachés que vous voulez envoyer avec vos messages e-mails. Vous pourriez aussi vouloir crypter et décrypter les fichiers que vous stockez sur votre propre ordinateur pour empêcher autrui d'y avoir accès.

Pour accéder aux fonctions de PGP depuis l'Explorateur Windows, choisissez l'option appropriée depuis le sous-menu PGP du menu Fichier. Les options qui apparaissent dépendent de l'état actuel du fichier que vous avez sélectionné. Si le fichier n'a pas encore été crypté ou signé, alors les options pour réaliser ces opérations apparaissent dans le menu. Si le fichier est déjà crypté ou signé, alors apparaissent les options pour décrypter et vérifier le contenu du fichier.

Sélectionner les destinataires

Quand vous envoyez un e-mail à quelqu'un dont l'application e-mail est gérée par les plug-ins de PGP, l'adresse e-mail du destinataire détermine quelles clés utiliser lors du cryptage du contenu. Toutefois, si vous saisissez un nom d'utilisateur ou une adresse e-mail qui ne correspond à aucune des clés de votre trousseau de clés ou si vous cryptez depuis le presse-papiers ou depuis l'Explorateur Windows, vous devez sélectionner manuellement la clé publique du destinataire depuis la

boîte de dialogue PGP Key Selection. Pour sélectionner la clé d'un destinataire, glissez simplement l'icône représentant sa clé dans la zone liste des destinataires puis cliquez sur OK.

Pour des instructions complètes sur la façon de crypter et signer ou décrypter et vérifier un e-mail, voir le [Chapitre 4](#). Si vous voulez crypter des fichiers à stocker sur votre disque dur ou à envoyer comme fichier attachés, voir le [Chapitre 5](#).

Prendre les raccourcis

Bien que vous trouverez PGP facile à utiliser, plusieurs raccourcis sont disponibles pour vous aider à accomplir vos tâches de cryptage encore plus vite. Par exemple, pendant que vous gérez vos clés dans la fenêtre de PGPkeys, vous pouvez presser le bouton droit de la souris pour effectuer toutes les fonctions nécessaires de PGP, plutôt que d'y accéder depuis la barre de menu. Vous pouvez aussi glisser un fichier contenant une clé dans la fenêtre de PGPkeys pour l'ajouter à votre trousseau de clés.

Les raccourcis clavier sont aussi disponibles pour la plupart des opérations effectuées via les menus. Ces raccourcis clavier sont indiqués sur tous les menus PGP, et d'autres raccourcis sont décrits dans leur contexte dans ce manuel.

Description des icônes de PGPkeys

Les icônes de la barre d'outils de PGPkeys

Le tableau suivant montre toutes les icônes utilisées dans la barre d'outils de PGPkeys, accompagnées d'une description de leurs fonctions.

Icône	Fonction
	Lance le Key Generation Wizard. Cliquez sur ce bouton pour créer une nouvelle paire de clés.
	Révoque la clé ou la signature sélectionnée. Cliquez sur ce bouton pour désactiver une clé ou révoquer une clé ou une signature. Révoquer une clé empêchera quelqu'un de crypter des données avec.
	Vous permet de signer la clé sélectionnée. En signant la clé, vous certifiez que la clé et l'ID d'utilisateur appartiennent à l'utilisateur identifié.
	Efface ce qui est sélectionné. Cliquez sur ce bouton pour retirer une clé, une signature, ou un ID photographique.
	Ouvre la fenêtre Key Search [Recherche de Clé] qui vous permet de rechercher des clés sur des trousseaux [de clés] locaux ou des serveurs distants.
	Envoie la clé sélectionnée au serveur. Cliquez sur ce bouton pour envoyer votre clé sur le serveur. Cliquer sur ce bouton envoie votre clé sur le serveur de clés ou de domaine.



Met à jour la clé sélectionnée depuis un serveur de clés ou de domaine. Cliquez sur ce bouton pour importer des clés depuis un serveur de clés ou de domaine vers votre trousseau de clés.



Affiche la boîte de dialogue des propriétés pour la clé sélectionnée. Cliquez sur ce bouton pour voir les propriétés General et Subkey [Sous-clé] d'une clé.



Vous permet d'importer des clés depuis un fichier vers votre trousseau de clés.



Vous permet d'exporter la clé sélectionnée vers un fichier.

Les icônes de la fenêtre PGPkeys

Le tableau suivant montre toutes les mini icônes utilisées dans la fenêtre de PGPkeys, accompagnées d'une description de ce qu'elles représentent.

Icône	Description
	Une clé dorée avec un utilisateur représente votre paire de clés Diffie-Hellman/DSS, constituée de votre clé privée et de votre clé publique.
	Une clé dorée seule représente une clé publique Diffie-Hellman/DSS.
	Une clé grise avec un utilisateur représente votre paire de clés RSA, constituée de votre clé privée et de votre clé publique.
	Une clé grise seule représente une clé publique RSA.
	Quand une clé ou une paire de clés est estompée, les clés sont temporairement indisponibles pour le cryptage ou la signature. Vous pouvez désactiver une clé depuis la fenêtre de PGPkeys, ce qui empêche une clé d'usage peu fréquent d'encombrer la boîte de dialogue Key Selection.
	Cette icône indique qu'un ID photographique accompagne la clé publique.
	Une clé avec un X rouge indique que la clé a été révoquée. Les utilisateurs révoquent leurs clés quand elles ne sont plus valides ou ont été compromises d'une façon ou d'une autre.
	Une clé avec une horloge indique que la clé a expiré. Une date d'expiration de clé est instituée lorsque la clé est créée.
	Une enveloppe représente le propriétaire de la clé et recense les noms d'utilisateur et adresses e-mail associées à la clé.
	Un cercle gris indique que la clé n'est pas valide.
	Un cercle vert indique que la clé est valide. Un cercle rouge supplémentaire dans la colonne ADK indique que la clé est associée à une Additional Decryption Key [Clé de Décryptage Supplémentaire imposée]; un cercle gris supplémentaire dans la colonne ADK indique que la clé n'a pas de clé de décryptage supplémentaire imposée associée.



Un cercle vert et un utilisateur indique que vous possédez la clé, et qu'elle est implicitement digne de confiance.



Un crayon ou un stylo à plume indique la signature des utilisateurs de PGP qui se sont portés garants de l'authenticité de la clé. Une signature avec un X rouge en travers indique une signature révoquée. Une signature avec une icône de crayon estompé indique une mauvaise signature ou une signature invalide. Une signature avec une flèche bleue à côté indique que cette signature est exportable.



Une barre vide indique une clé invalide ou un utilisateur non digne de confiance.



Une barre à moitié pleine indique une clé marginalement valide ou un utilisateur marginalement digne de confiance.



Une barre striée indique une clé valide dont vous êtes propriétaire et est implicitement digne de confiance, sans égard à ses signatures.



Une barre pleine indique une clé complètement valide ou un utilisateur complètement digne de confiance.

Ce chapitre explique comment générer les paires de clés publique et privée dont vous avez besoin pour correspondre avec les autres utilisateurs de PGP. Il explique aussi comment distribuer votre clé publique et obtenir les clés publiques d'autrui de telle sorte que vous puissiez commencer à échanger des e-mails sécurisés et authentifiés.

Notion de clé

PGP est basé sur un système de *cryptographie à clé publique* largement accepté et hautement éprouvé, comme montré dans la [Figure 3-1](#), par lequel vous et les autres utilisateurs de PGP générez une paire de clés consistant en une clé privée et une clé publique. Comme son nom l'implique, vous êtes le seul à avoir accès à votre clé privée; mais pour correspondre avec les autres utilisateurs de PGP vous avez besoin d'une copie de leur clé publique, et eux ont besoin d'une copie de la vôtre. Vous utilisez votre clé privée pour signer les messages e-mail et les fichiers attachés que vous envoyez à autrui, et pour décrypter les messages et fichiers qu'ils vous envoient. Inversement, vous utilisez les clés publiques d'autrui pour leur envoyer un e-mail crypté, et vérifier leurs signatures numériques.

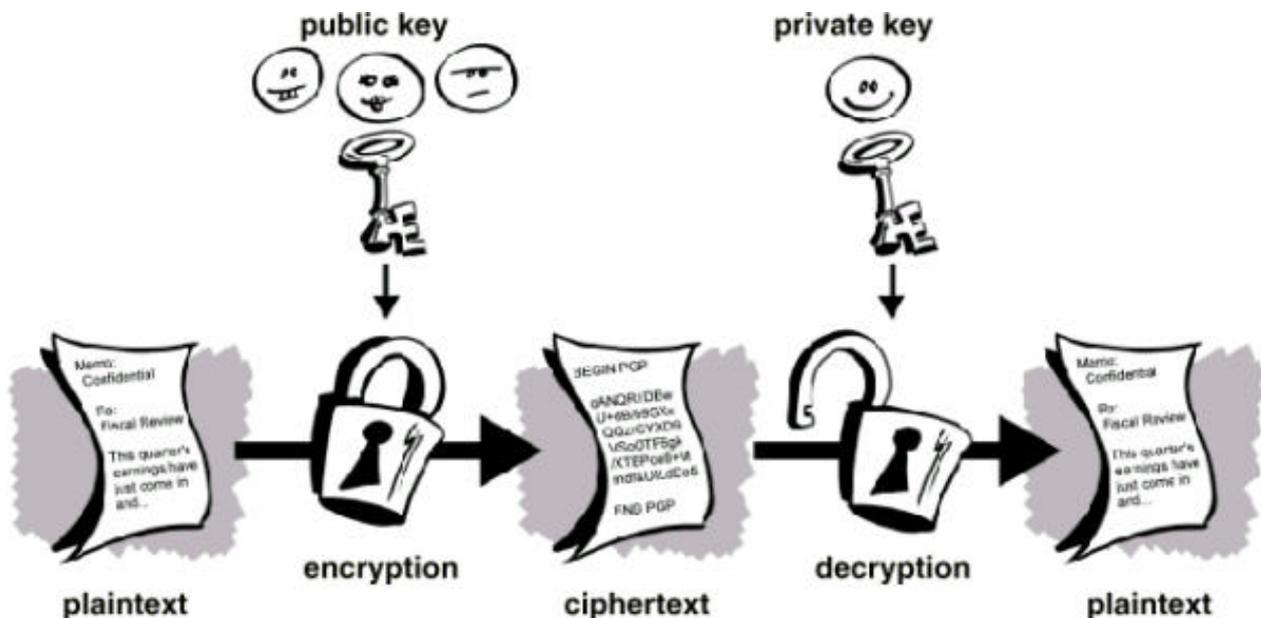


Figure 3-1. Diagramme de la cryptographie à clé publique

Créer une paire de clés

A moins que vous l'ayez déjà fait en utilisant une autre version de PGP, la première chose que vous avez besoin de faire avant d'envoyer ou de recevoir des e-mails cryptés et signés est de créer une nouvelle paire de clés. Une paire de clés consiste en deux clés: une clé privée que vous êtes le seul à posséder et une clé publique que vous distribuez librement à ceux avec qui vous correspondez. Vous générez une nouvelle paire de clés depuis la fenêtre de PGPkeys en utilisant le PGP Key Generation Wizard, qui vous guide à travers le processus.

❑ **NOTE:** Si vous faites une mise à jour depuis une version plus ancienne de PGP, vous avez probablement déjà généré une clé privée et avez distribué sa clé publique correspondante à ceux avec qui vous correspondez. Dans ce cas, vous n'avez pas à créer une nouvelle paire de clés (comme décrit dans la prochaine partie). A la place, vous spécifiez l'emplacement de vos clés quand vous lancez PGPkeys. Vous pouvez aller à l'onglet Files de la boîte de dialogues Preferences et localiser votre fichier de trousseau de clés à tout moment.

Pour créer une nouvelle paire de clés

1. Ouvrez la fenêtre de PGPkeys. Vous pouvez ouvrir cette fenêtre ainsi:
 - Cliquer sur Démarrer -->Programs-->PGP-->PGPkeys.
 - Cliquer sur l'icône PGPtray () dans la barre des tâches, puis cliquer sur PGPkeys.
 - Cliquez sur () dans la barre d'outils de votre application e-mail.
2. PGPkeys apparaît, comme montré dans la [Figure 3-2](#).

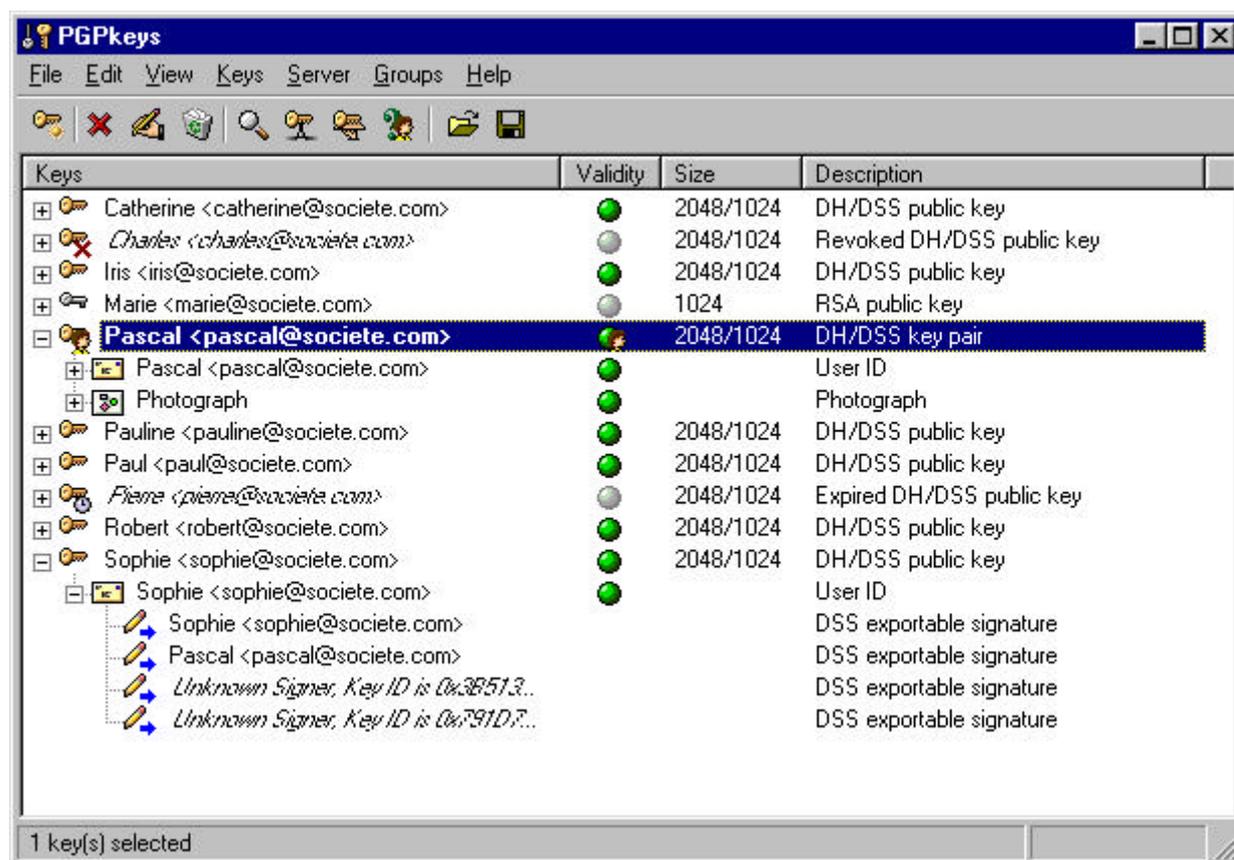


Figure 3-2. La fenêtre de PGPkeys

3. Cliquez sur (🔑) dans la barre d'outils de PGPkeys.

Le PGP Key Generation Wizard donne quelques informations introductives sur le premier écran.

4. Quand vous avez fini de lire ces informations, cliquez sur Suivant pour avancer jusqu'à l'encart suivant.

Le PGP Key Generation Wizard vous demande de saisir vos nom et adresse e-mail.

5. Saisissez votre nom sur la première ligne et votre adresse e-mail sur la seconde ligne.

Il n'est pas absolument nécessaire de saisir votre nom réel ou même votre adresse e-mail. Cependant, utiliser votre vrai nom rend plus facile pour autrui votre identification en tant que propriétaire de votre clé publique. En outre, en utilisant votre adresse e-mail correcte, tout le monde bénéficiera des fonctionnalités du plug-in qui cherche automatiquement la clé appropriée dans votre trousseau de clés quand vous adressez un e-mail à un destinataire particulier.

6. Cliquez sur Suivant pour avancer à la boîte de dialogue suivante.

Le Key Generation Wizard vous demande de sélectionner un type de clé.

7. Sélectionnez un type de clé, soit Diffie-Hellman/DSS, soit RSA, puis cliquez sur Suivant.

Les précédentes versions de PGP utilisent une technologie plus ancienne appelée RSA pour générer des clés. Avec PGP Version 5.0 et ultérieure, vous avez la possibilité de créer un nouveau et meilleur type de clé basée sur la variante ElGamal de la technologie Diffie-Hellman/DSS.

- Si vous prévoyez de correspondre avec des gens qui utilisent encore des clés RSA, vous pouvez vouloir générer une paire de clés RSA qui est compatible avec les anciennes versions du programme.
- Si vous prévoyez de correspondre avec des gens qui disposent de PGP Version 5.0 ou ultérieure, vous tirerez avantage de la nouvelle technologie et générerez une paire de clés Diffie-Hellman.
- Si vous voulez échanger des e-mails avec tous les utilisateurs de PGP, créez une paire de clés RSA et une paire de clés Diffie-Hellman/DSS, puis utilisez la paire appropriée selon la version de PGP utilisée par le destinataire. Vous devez créer une paire de clés séparée pour chaque type de clé dont vous avez besoin.

NOTE: Si votre version de PGP ne gère pas les clés RSA, cette étape peut ne pas vous concerner. Pour plus d'informations sur la gestion RSA, voir le fichier ReadMe.txt, qui accompagne ce produit.

8. Le Key Generation Wizard vous demande de spécifier une taille pour vos nouvelles clés.

Sélectionnez une taille de clé de 768 à 3072 bits, ou saisissez une taille sur mesure entre 768 et 4096 bits.

NOTE: Une clé de taille sur mesure peut prendre un long moment à générer, selon la vitesse de l'ordinateur que vous utilisez.

La taille de clé correspond au nombre de bits utilisés pour construire votre clé numérique. Plus la clé est grande, moins quelqu'un a de chance d'être capable de la craquer, mais plus lent est le processus de décryptage et de cryptage. Vous avez besoin de trouver le bon compromis entre la commodité qu'il y a à réaliser les fonctions de PGP rapidement avec une plus petite clé et le niveau de sécurité renforcé fourni par une plus grande clé. A moins que vous n'échangiez des informations ultra sensibles d'un intérêt tel que quelqu'un serait disposé à lancer une attaque cryptographique onéreuse et coûteuse en temps pour les lire, vous êtes en sécurité en utilisant une clé de 1024 bits.

NOTE: Quand vous créez une paire de clés Diffie-Hellman/DSS, la taille de la portion DSS de la clé est inférieure ou égale à la taille de la portion Diffie-Hellman de la clé, et est limitée à une taille maximum de 1024 bits.

9. Cliquez sur Suivant pour avancer jusqu'à l'encart suivant.

Le PGP Key Generation Wizard vous demande d'indiquer quand la paire de clés devra expirer.

10. Indiquez la date à laquelle vous voulez que votre paire de clés expire. Vous pouvez soit utiliser la sélection par défaut, qui est Never [Jamais], soit saisir une date spécifique à laquelle la clé expirera.

Une fois que vous avez créé une paire de clés et distribué votre clé publique, vous utiliserez probablement dès lors les mêmes clés. Cependant, dans certaines conditions, vous pouvez vouloir créer une paire de clés spéciale que vous prévoyez d'utiliser seulement pour une période limitée dans le temps. Dans ce cas, quand la clé publique expire, elle ne peut plus être utilisée par quelqu'un pour vous crypter un e-mail, mais elle peut encore servir pour vérifier votre signature numérique. De façon similaire, quand votre clé privée expire, elle peut encore être utilisée pour décrypter un e-mail qui vous avait été envoyé avant que la clé publique n'expire mais ne peut plus être utilisée pour signer un e-mail.

11. Cliquez sur Suivant pour avancer jusqu'à l'encart suivant.

Le PGP Key Generation Wizard vous demande de saisir une phrase secrète.

12. Dans la boîte de dialogue Passphrase [phrase secrète], saisissez la chaîne de caractères ou de mots que vous voulez utiliser pour garantir un accès exclusif à votre clé privée. Pour confirmer votre saisie, pressez la touche TAB pour avancer à la ligne suivante, puis saisissez à nouveau la même phrase secrète.

Normalement, à titre de sécurité supplémentaire, les caractères que vous saisissez pour la phrase secrète ne s'affichent pas à l'écran. Cependant, si vous êtes sûr que personne ne regarde, et que vous aimeriez voir les caractères de votre phrase secrète tels que vous les tapez, décochez la case Hide Typing [Cacher les caractères tapés].

NOTE: Votre phrase secrète devrait contenir de multiples mots et peut inclure des espaces, nombres, et caractères de ponctuation. Choisissez quelque chose dont vous pouvez vous rappeler facilement mais que d'autres ne pourront pas deviner. La phrase secrète est sensible à la casse, ce qui signifie qu'elle distingue les majuscules et les minuscules. Plus longue sera votre phrase secrète, plus variés seront les caractères qu'elle contient, et plus elle sera sûre. Les phrases secrètes sûres incluent des majuscules et des minuscules, des nombres, des ponctuations et des espaces, mais sont plus faciles à oublier. Voir "[Créer une phrase secrète dont vous vous rappellerez](#)" en page 32, pour plus d'informations sur le choix d'une bonne phrase secrète.

 **AVERTISSEMENT:** Personne, y compris Network Associates, ne peut retrouver une phrase secrète oubliée.

13. Cliquez sur Suivant pour commencer le processus de génération de clé.

Le PGP Key Generation Wizard indique qu'il est occupé à la génération de votre clé.

Si vous avez saisi une phrase secrète insuffisante, un message de mise en garde apparaît avant que les clés soient générées et vous devez choisir d'accepter la mauvaise phrase secrète ou d'en saisir une plus sûre avant de

continuer. Pour plus d'informations sur les phrases secrètes, voir [“Créer une phrase secrète dont vous vous rappellerez”](#) en page 32.

S'il n'y a pas assez d'informations aléatoires avec lesquelles construire la clé, la boîte de dialogue du générateur de données aléatoires apparaît. Comme il est demandé dans la boîte de dialogue, remuez votre souris et tapez une série de frappes de touches aléatoires jusqu'à ce que la barre de progression soit complètement remplie. Les mouvements de votre souris et les frappes de touches génèrent de l'information aléatoire, ce qui est nécessaire pour créer une paire de clés unique.

NOTE: PGPkeys rassemble continuellement des données depuis plusieurs sources du système, incluant les positions de la souris, les rythmes et les frappes de touches. Si la boîte de dialogue des données aléatoires n'apparaît pas, cela indique que PGP a déjà collecté toutes les données aléatoires dont il a besoin pour créer la paire de clés.

Après que le processus de génération des clés ait commencé, il faudra un certain temps pour générer les clés. En fait, si vous spécifiez une taille autre que les valeurs par défaut pour une clé Diffie-Hellman/DSS, l'option génération de clé rapide n'est pas utilisée et cela peut prendre des heures pour générer votre clé avec de plus grandes tailles. Finalement, le PGP Key Generation Wizard indique que le processus de génération de clé est achevé.

14. Cliquez sur Suivant pour avancer jusqu'à l'encart suivant.

Le PGP Key Generation Wizard indique que vous avez généré avec succès une nouvelle paire de clés et demande si vous voulez envoyer votre clé publique au serveur de clés.

15. Spécifiez si vous voulez ou non que votre nouvelle clé publique soit envoyée au serveur, puis cliquez sur Suivant (le serveur par défaut est spécifié dans vos Préférences).

Quand vous envoyez votre clé publique au serveur de clés, quiconque ayant accès à ce serveur peut obtenir une copie de votre clé quand il en a besoin. Pour des détails complets, voir [“Distribuer votre clé publique”](#) en page 40.

Quand le processus de génération de clé est achevé, l'écran final apparaît.

16. Cliquez sur Done [Fait].

Une nouvelle paire de clés représentant votre clé nouvellement créée apparaît dans la fenêtre de PGPkeys. Alors vous pouvez examiner vos clés en vérifiant leurs propriétés et attributs; vous pouvez aussi vouloir ajouter une autre adresse e-mail. Voir [“Ajouter un nouveau nom d'utilisateur ou adresse à une paire de clés”](#) en page 79, pour des détails sur l'ajout de nouveaux noms d'utilisateur à votre clé.

Créer une phrase secrète dont vous vous rappellerez

Crypter un fichier que l'on est ensuite incapable de décrypter constitue une douloureuse expérience dans l'apprentissage du choix d'une phrase secrète dont vous vous rappellerez. La plupart des applications requièrent un mot de passe de

trois à huit lettres. Un simple mot de passe est vulnérable à une attaque par dictionnaire, qui consiste à faire essayer à un ordinateur tous les mots du dictionnaire jusqu'à ce qu'il trouve votre mot de passe. Pour se protéger contre cette sorte d'attaque, il est généralement recommandé de créer un mot composé d'une combinaison de lettres alphabétiques majuscules et minuscules, de nombres, de signes de ponctuation et d'espaces. Cela donne un mot de passe plus résistant, mais un mot de passe obscur que vous ne retiendrez probablement pas facilement. Nous ne vous recommandons pas d'utiliser un mot de passe d'un seul mot. Une phrase secrète est moins vulnérable à une attaque par dictionnaire. Cela est réalisé facilement en utilisant de multiples mots dans votre phrase, plutôt qu'en essayant de contrer une attaque par dictionnaire en insérant arbitrairement beaucoup d'amusants caractères non alphabétiques, ce qui a pour effet de rendre votre phrase secrète trop facile à oublier et pourrait conduire à une désastreuse perte d'informations parce que vous ne pouvez plus décrypter vos propres fichiers. Toutefois, à moins que la phrase secrète que vous choisissez ne soit quelque chose de facile à apprendre par cœur pour longtemps, vous avez peu de chance de vous la rappeler mot pour mot. Choisir une phrase sous l'inspiration du moment va déboucher sur son oubli total. Choisissez quelque chose qui réside déjà dans votre mémoire. Peut-être une idiotie que vous avez entendue il y a des années et qui est restée gravée dans votre tête durant tout ce temps. Ce ne devrait pas être quelque chose que vous avez répété à d'autres récemment, ni une citation célèbre, parce que vous voulez qu'elle soit difficile à deviner pour un attaquant sophistiqué. Si elle est déjà profondément gravée dans votre mémoire, vous ne l'oublierez probablement pas.

Bien sûr, si vous êtes assez imprudent pour écrire votre phrase secrète quelque part et la laisser sur votre moniteur ou à l'intérieur du sous-main de votre bureau, peu importera ce que vous choisirez.

Ajouter un ID photographique à votre clé

Vous pouvez inclure un ID photographique à votre clé Diffie-Hellman/DSS.

⚠ Avertissement: Bien que vous puissiez voir l'ID photographique accompagnant la clé de quelqu'un pour la vérification, vous devriez toujours vérifier et comparer les empreintes numériques. Voir "[Vérifier une clé publique](#)" en page 80 pour plus d'informations sur l'authentification.

Pour ajouter votre photographie à votre clé

1. Ouvrez PGPkeys.
2. Sélectionnez votre paire de clés et cliquez ensuite sur Add Photo dans le menu Keys.

La boîte de dialogue Add Photo s'ouvre, comme montré dans la [Figure 3-3](#).



Figure 3-3. La boîte de dialogue Add Photo

3. Glissez ou collez votre photographie dans la boîte de dialogue Add Photo ou parcourez vos fichiers en cliquant sur Select File.

NOTE: La photographie doit être un fichier .JPG ou .BMP. Pour une image de qualité maximum, réduisez l'image à 120x144 avant de l'ajouter à la boîte de dialogue Add Photo. Si vous ne le faites pas, PGP réduira l'image pour vous.

4. Cliquez sur OK.

La boîte de dialogue Passphrase apparaît, comme montré dans la [Figure 3-4](#).



Figure 3-4. Boîte de dialogue Passphrase

5. Saisissez votre phrase secrète dans l'espace prévu, puis cliquez sur OK.

Votre ID d'utilisateur photographique est ajouté à votre clé publique et est répertorié dans la fenêtre de PGPkeys. Vous pouvez maintenant envoyer votre

clé au serveur. Voir [“Pour envoyer votre clé publique à un serveur de clés”](#) en page 40, pour des informations supplémentaires.

Pour remplacer votre ID photographique

1. Ouvrez la fenêtre de PGPkeys.
2. Sélectionnez votre paire de clés.
3. Sélectionnez la photographie que vous voulez remplacer.
4. Choisissez Delete [Effacer] depuis le menu Edit [Edition].
5. Ajoutez votre nouvel ID photographique en suivant les instructions données dans [“Pour ajouter votre photographie à votre clé”](#) en page 33.

Créer de nouvelles sous-clés

Chaque clé Diffie-Hellman/DSS est constituée en réalité de deux clés: une clé de signature DSS et une sous-clé de cryptage Diffie-Hellman. PGP Version 6.0 donne la possibilité de créer et révoquer de nouvelles clés de cryptage sans sacrifier votre clé principale de signature et les signatures rassemblées dessus. Une des utilisations les plus courantes de cette fonctionnalité est de créer de multiples sous-clés destinées à être utilisées pendant différentes périodes de la durée de vie de la clé. Par exemple, si vous créez une clé qui expirera dans 3 ans, vous pourriez aussi créer 3 sous-clés et utiliser chacune d'elle pour une des années de la durée de vie de la clé. Cela peut être une mesure de sécurité utile et donner un moyen automatique de basculer périodiquement sur une nouvelle clé de cryptage sans avoir à recréer et distribuer une nouvelle clé publique.

Pour créer de nouvelles sous-clés

1. Ouvrez PGPkeys.
2. Sélectionnez votre paire de clés et cliquez ensuite sur Properties [Propriétés] dans le menu Keys, ou cliquez sur .

La boîte de dialogue Properties s'ouvre.

3. Cliquez sur l'onglet Subkeys.

La boîte de dialogue Subkeys s'ouvre, comme montré dans la [Figure 3-5](#).

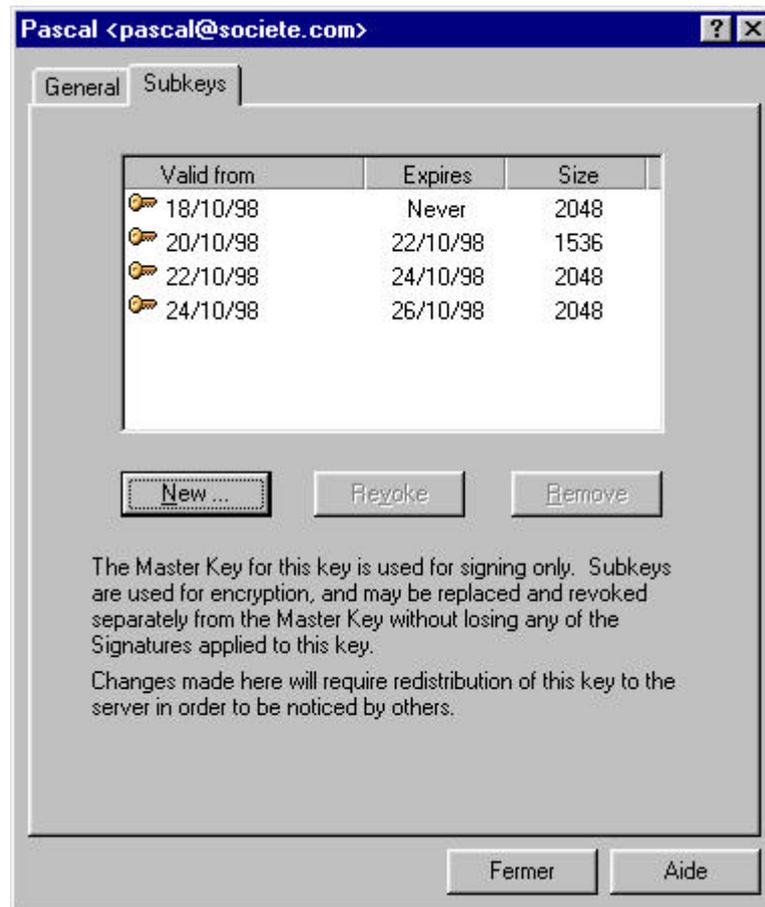


Figure 3-5. La boîte de dialogue Key Properties (onglet Subkeys)

4. Pour créer une nouvelle sous-clé, cliquez sur New.
La boîte de dialogue New Subkey s'ouvre.
5. Saisissez une taille de clé de 768 à 3072 bits, ou saisissez une taille de clé de votre choix de 768 à 4096 bits.
6. Indiquez la date à partir de laquelle votre sous-clé sera active.
7. Indiquez quand votre sous-clé expirera. Vous pouvez soit utiliser la sélection par défaut, qui est Never, soit saisir une date spécifique après laquelle la sous-clé expirera.
8. Cliquez sur OK.
La boîte de dialogue Passphrase apparaît.
9. Saisissez votre phrase secrète et cliquez sur OK.
Votre nouvelle sous-clé est répertoriée dans la fenêtre Subkey.

Scission de clé

Toute clé privée peut être scindée en segments détenus par plusieurs "shareholders" [dépositaires de fragments] en utilisant un procédé cryptographique appelé Blakely-Shamir key splitting [scission de clé Blakely-

Shamir]. Cette technique est recommandée pour les clés d'une sécurité extrêmement élevée. Par exemple, Network Associates garde une clé d'entreprise scindée entre plusieurs individus. Chaque fois que nous avons besoin de signer avec cette clé, les fragments de la clé sont rassemblés temporairement. Pour scinder une clé, sélectionnez la paire de clés à scinder et choisissez Share Split [Scinder en Segments] dans le menu Keys. Il vous est alors demandé d'indiquer combien de personnes différentes seront requises pour rassembler la clé. Les segments sont sauvegardés dans des fichiers cryptés chacun avec la clé publique du dépositaire de fragment ou cryptés de manière conventionnelle si le dépositaire de fragment n'a pas de clé publique. Après que la clé ait été scindée, tenter de signer ou de décrypter avec déclenchera automatiquement une tentative de rassemblement de la clé. Pour plus d'informations sur le rassemblement d'une clé scindée, voir [“Signer et décrypter des fichiers avec une clé scindée”](#) en page 64.

Pour créer une clé scindée en de multiples segments

1. Ouvrez PGPkeys.
2. Dans la fenêtre PGPkeys, créez une nouvelle paire de clés ou sélectionnez une paire de clés existante que vous voulez scinder.
3. Dans le menu Keys, cliquez sur Share Split.

La boîte de dialogue Share Split s'ouvre (Figure 3-6) par dessus la fenêtre PGPkeys

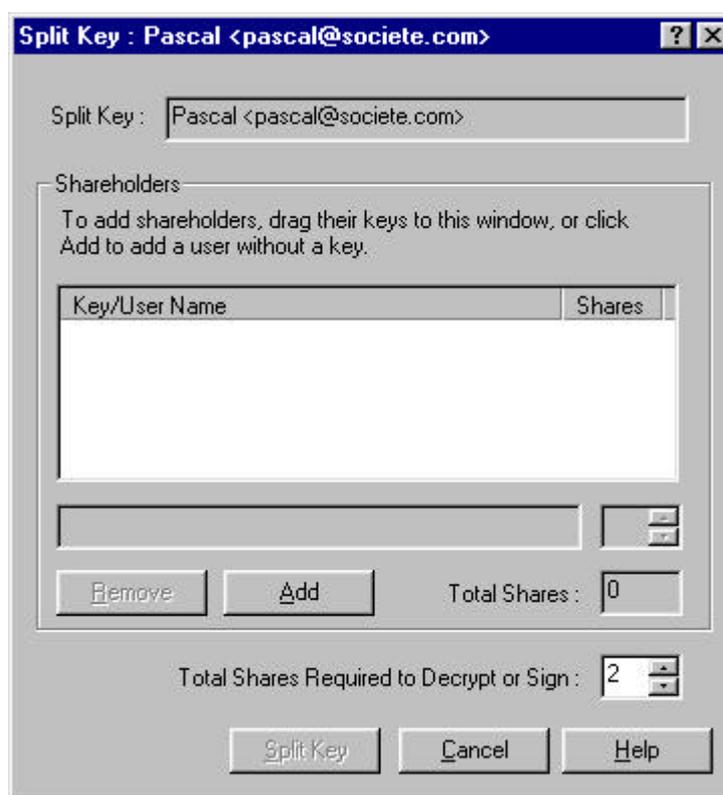


Figure 3-6. La boîte de dialogue Share Split

- Ajoutez les dépositaires de fragments à la paire de clés en glissant leurs clés de la fenêtre PGPkeys jusqu'à la liste des dépositaires de fragments dans la boîte de dialogue Share Split.

Pour ajouter un dépositaire de fragment qui n'a pas de clé publique, cliquez sur Add dans la boîte de dialogue Share Split, saisissez le nom de la personne, puis permettez à cette personne de taper sa phrase secrète.

- Quand tous les dépositaires de fragments sont répertoriés, vous pouvez spécifier le nombre de segments requis pour décrypter ou signer avec cette clé.

Dans la [Figure 3-7](#), par exemple, le nombre total de segments qui reconstituent la clé du responsable de l'entreprise "Société" est de quatre et le nombre total de segments requis pour décrypter ou signer est de trois. Cela donne une marge au cas où l'un des dépositaires serait incapable de produire son fragment de clé ou oublierait la phrase secrète.

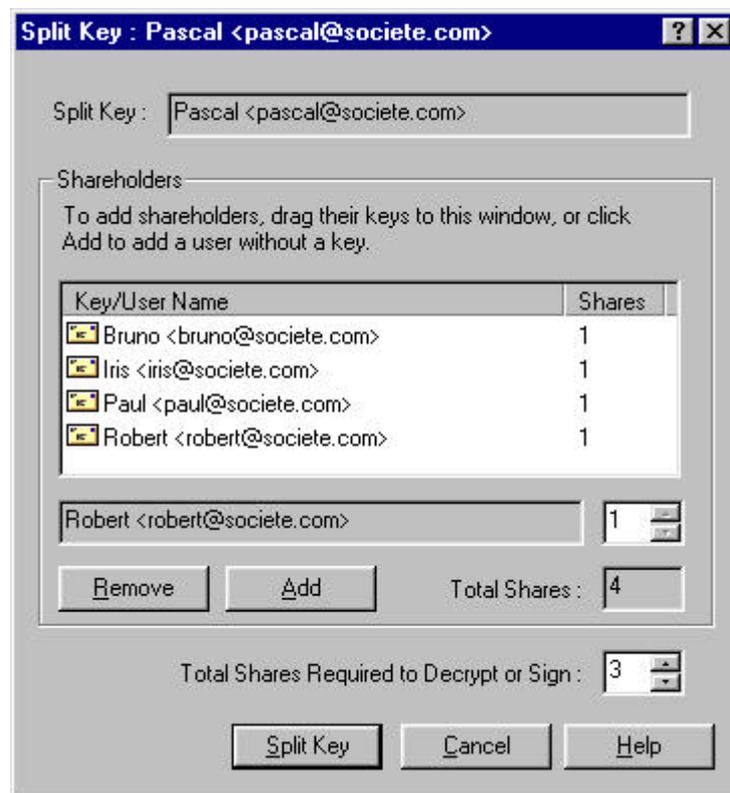


Figure 3-7. La boîte de dialogue Share Split (Exemple)

Par défaut, chaque dépositaire de fragment détient un seul segment. Pour augmenter le nombre de segments qu'un dépositaire de fragment possède, cliquez sur le nom dans la liste des dépositaires de fragments pour l'afficher dans la zone de texte au-dessous. Saisissez le nouveau nombre de segments de clé ou utilisez les flèches pour sélectionner un nouveau chiffre.

- Cliquez sur Split Key [Scinder la clé].

Une boîte de dialogue s'ouvre et vous demande de sélectionner un répertoire dans lequel stocker les fragments.

- Sélectionnez un endroit où stocker les fragments de clé.

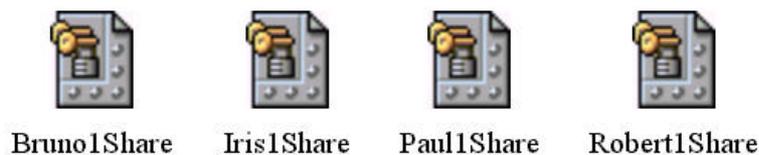
La boîte de dialogue Passphrase apparaît.

- Saisissez la phrase secrète pour la clé que vous voulez scinder et cliquez ensuite sur OK.

Une boîte de dialogue de confirmation s'ouvre.

- Cliquez sur Yes pour scinder la clé.

La clé est scindée et les fragments sont sauvegardés à l'endroit que vous avez spécifié. Chaque segment de clé est sauvegardé avec le nom du dépositaire de fragment comme nom de fichier et une extension .SHF, comme montré dans l'exemple ci-dessous:



- Distribuez les segments de clé aux propriétaires, puis effacez les copies locales.

Une fois la clé scindée entre plusieurs dépositaires de fragments, tenter de signer ou décrypter avec fera que PGP tentera automatiquement de rassembler la clé. Pour apprendre comment rassembler une clé scindée pour signer ou décrypter des fichiers, voir [“Signer et décrypter des fichiers avec une clé scindée” en page 64.](#)

Protéger vos clés

Une fois que vous avez généré une paire de clés, il est prudent d'en conserver une copie dans un endroit sûr au cas où quelque chose arriverait à l'original. PGP vous propose de faire une copie de sauvegarde quand vous fermez PGPkeys après avoir créé une nouvelle paire de clés.

Vos clés privées et vos clés publiques sont stockées dans des trousseaux de clés séparés, que vous pouvez copier exactement comme tous les autres fichiers vers un autre endroit sur votre disque dur ou sur une disquette. Par défaut, le trousseau de clés privées (secring.skr) et le trousseau de clés publiques (pubring.pkr) sont stockés avec les autres fichiers du programme dans le sous-répertoire “PGP Keyrings” du répertoire “PGP 6.0”, mais vous pouvez sauvegarder vos copies à l'endroit que vous voulez.

Quand vous spécifiez que vous voulez effectuer une copie de sauvegarde de vos clés, la boîte de dialogue Save As [Sauvegarder Sous] apparaît, vous demandant d'indiquer l'emplacement de la sauvegarde des trousseaux de clés.

En plus de sauvegarder vos clés, vous devriez faire particulièrement attention à l'endroit où vous stockez votre clé privée. Quand bien même votre clé serait protégée par une phrase secrète connue de vous seul, il est possible que quelqu'un puisse découvrir votre phrase secrète et utilise ensuite votre clé privée pour déchiffrer votre e-mail ou contrefaire votre signature numérique. Par exemple,

quelqu'un pourrait regarder par-dessus votre épaule et voir les touches que vous frappez ou les intercepter à travers le réseau ou même à travers les ondes.

Pour empêcher que quiconque intercepterait votre phrase secrète soit capable d'utiliser votre clé privée, vous devriez stocker votre clé privée uniquement sur votre propre ordinateur. Si votre ordinateur est relié à un réseau, vous devriez aussi vous assurer que vos fichiers ne sont pas automatiquement inclus dans une sauvegarde du système total où d'autres pourraient avoir accès à votre clé privée. Etant donnée la facilité avec laquelle les ordinateurs sont accessibles sur les réseaux, si vous travaillez sur des informations extrêmement sensibles, vous pouvez vouloir garder votre clé privée sur une disquette, que vous pouvez insérer comme une bonne vieille clé chaque fois que vous voulez lire ou signer une information privée.

A titre de précaution supplémentaire, envisagez d'assigner un nom différent à votre trousseau de clés privées et ensuite stockez-le ailleurs que dans le répertoire par défaut de PGP où il ne sera pas aussi facile à localiser. Vous pouvez utiliser l'onglet de la boîte de dialogue Preferences de PGPkeys pour spécifier un nom et un emplacement pour vos trousseaux de clés privées et publiques.

Distribuer votre clé publique

Après avoir créé vos clés, vous avez besoin de les mettre à la disposition d'autrui afin de pouvoir vous envoyer des informations cryptées et vérifier votre signature numérique.

Vous avez trois choix pour distribuer votre clé publique:

- Rendez votre clé publique disponible via un serveur de clés publiques.
- Incluez votre clé publique dans un message e-mail.
- Exportez votre clé publique ou copiez-la dans un fichier.

Votre clé publique se compose d'un bloc de texte, aussi est-il assez facile de la rendre disponible via un serveur de clés, de l'inclure dans un message e-mail, ou de l'exporter ou de la copier dans un fichier. Le destinataire peut ensuite utiliser toute méthode qui lui convient pour ajouter votre clé publique à son trousseau de clés publiques.

Rendre votre clé publique disponible via un serveur de clés

La meilleure méthode pour rendre votre clé publique disponible est de la placer sur un serveur de clés publiques auquel n'importe qui peut avoir accès. De cette manière, les gens peuvent vous envoyer un e-mail sans avoir à réclamer explicitement une copie de votre clé. Cela vous évite aussi, comme d'autres, d'avoir à maintenir un grand nombre de clés publiques que vous utilisez rarement. Il y a de nombreux serveurs de clés dans le monde entier, y compris ceux offerts par Network Associates, Inc., via lesquels vous pouvez rendre vos clés accessibles à n'importe qui.

Pour envoyer votre clé publique à un serveur de clés

1. Connectez-vous à Internet.

2. Ouvrez PGPkeys.
3. Sélectionnez l'icône qui représente la clé publique que vous voulez poster sur le serveur de clés.
4. Ouvrez le menu Server [Serveur], puis sélectionnez le serveur de clés sur lequel vous voulez poster depuis le sous-menu Send To [Envoyer à].

Une fois que vous avez placé une copie de votre clé publique sur un serveur de clés, vous pouvez dire aux gens qui veulent vous envoyer des données cryptées ou vérifier votre signature numérique de se procurer une copie de votre clé depuis le serveur. Même si vous ne les dirigez pas explicitement sur votre clé publique, ils peuvent obtenir une copie en cherchant votre nom ou votre adresse e-mail sur le serveur de clés. Beaucoup de gens incluent l'adresse Web de leur clé publique à la fin de leur message e-mail; dans la plupart des cas le destinataire peut juste double-cliquer sur l'adresse pour accéder à une copie de votre clé sur le serveur. Des gens mettent même leur empreinte de clé PGP sur leurs cartes de visite pour une vérification encore plus facile.

Mettre à jour votre clé sur un serveur de clés

Si jamais vous avez besoin de changer votre adresse e-mail, ou si vous acquérez de nouvelles signatures, tout ce que vous avez à faire pour remplacer votre vieille clé est d'envoyer une nouvelle copie au serveur; l'information est automatiquement mise à jour. Toutefois, vous devriez garder présent à l'esprit que les serveurs de clés publiques sont seulement capables de mettre à jour une nouvelle information et ne permettent pas de retirer les noms d'utilisateurs ou des signatures de votre clé. Pour effacer des signatures ou des noms d'utilisateurs de votre clé, voir [“Enlever des signatures ou des noms d'utilisateur associés à votre clé” ci-dessous](#) pour informations. Si votre clé vient à être compromise, vous pouvez la révoquer, ce qui dira à tous de ne plus faire confiance à cette copie de votre clé. Voir le [Chapitre 6, “Gestion des Clés et Réglage des Préférences”](#) pour plus de détails sur la façon de révoquer une clé.

Enlever des signatures ou des noms d'utilisateur associés à votre clé

Les serveurs de clés publiques sont seulement capables de mettre à jour une information nouvelle et ne permettent pas d'enlever un nom d'utilisateur ou une signature de votre clé. Si vous voulez enlever des signatures ou des noms d'utilisateur associés à votre clé, vous devez préalablement enlever la clé elle-même du serveur.

Pour effacer votre clé publique d'un serveur de clés

1. Ouvrez la fenêtre PGPkeys.
2. Choisissez Search [Rechercher] depuis le menu Server ou cliquez sur le bouton Search () dans la barre d'outils de PGPkeys.

La fenêtre PGPkeys Search apparaît.

3. Choisissez le serveur sur lequel vous souhaitez effectuer la recherche depuis le menu Search for Keys On [Rechercher des Clés Sur].
4. Spécifiez votre critère de recherche pour localiser votre clé publique:
Par défaut, il s'agit de User ID, mais vous pouvez cliquer sur les flèches pour sélectionner Key ID, Key Status, Key Type, Key Size, Creation Date ou Expiration Date. Par exemple, vous pourriez rechercher toutes les clés avec Fred comme User ID.
5. Pour commencer la recherche, cliquez sur Search.
Le résultat de la recherche apparaît dans la fenêtre.
6. Cliquez avec le bouton droit sur la clé que vous voulez enlever du serveur, puis sélectionnez Delete.
La boîte de dialogue Passphrase apparaît.
7. Saisissez la phrase secrète pour la clé que vous voulez enlever du serveur, puis cliquez sur OK.
Une demande de confirmation apparaît et la clé est enlevée.
8. Si vous voulez envoyer une clé mise à jour sur le serveur, voir [“Rendre votre clé publique disponible via un serveur de clés” en page 40](#) pour les instructions.

⚠ AVERTISSEMENT: Si vous effacez votre clé d'un serveur, vous devez savoir que quelqu'un qui aurait votre clé publique dans son trousseau peut l'envoyer à nouveau sur le serveur. Vous devriez vérifier périodiquement le serveur pour voir si la clé est réapparue – vous pourriez avoir à effacer votre clé du serveur plus d'une fois.

Inclure votre clé publique dans un message e-mail

Une autre méthode commode pour donner votre clé publique à quelqu'un est de l'inclure dans un message e-mail.

Pour inclure votre clé publique dans un message e-mail

1. Ouvrez PGPkeys.
2. Sélectionnez votre paire de clés, puis cliquez sur Copy [Copier] dans le menu Edit.
3. Ouvrez l'éditeur que vous utilisez pour composer vos messages e-mail, placez le curseur à l'endroit désiré, et puis cliquez sur Paste [Coller] dans le menu Edit. Dans les plus récentes applications e-mail, vous pouvez simplement glisser votre clé depuis la fenêtre PGPkeys dans le texte de votre e-mail pour y copier la clé.

Exporter votre clé publique dans un fichier

Une autre méthode de distribution de votre clé publique est de la copier dans un fichier et de mettre ensuite le fichier à la disposition de la personne avec qui vous voulez communiquer.

Pour exporter votre clé publique dans un fichier

Il y a deux façons d'exporter ou de sauver votre clé publique dans un fichier:

- Sélectionnez l'icône représentant votre paire de clés dans le fenêtre PGPkeys, puis cliquez sur Export dans le menu Keys et saisissez le nom du fichier dans lequel vous voulez que la clé soit sauvegardée.
- Sélectionnez l'icône représentant votre paire de clés dans la fenêtre de PGPkeys, cliquez sur Copy dans le menu Edit, puis cliquez sur Paste pour insérer la copie de la clé dans un document texte.

NOTE: Si vous envoyez votre clé à des collègues qui utilisent des PC, saisissez un nom de moins de huit caractères et trois caractères additionnels pour l'extension de fichier (par exemple, email.txt).

Obtenir les clés publiques d'autrui

Tout comme vous avez besoin de distribuer votre clé publique à ceux qui veulent vous envoyer un e-mail crypté ou vérifier votre signature numérique, vous avez besoin d'obtenir les clés publiques d'autrui de telle sorte que vous puissiez leur envoyer des e-mails cryptés ou vérifier leurs signatures numériques.

Pour obtenir la clé publique de quelqu'un

Il y a trois façons d'obtenir la clé publique de quelqu'un:

- Récupérer la clé via un serveur de clés publiques.
- Ajouter la clé à votre trousseau de clés directement depuis un message e-mail.
- Importer la clé publique depuis un fichier exporté.

Les clés publiques sont juste des blocs de texte, aussi sont-elles faciles à ajouter à votre trousseau en les important depuis un fichier ou en les copiant depuis un message e-mail et en les collant dans votre trousseau de clés publiques.

Récupérer des clés publiques depuis un serveur de clés

Si les personnes à qui vous voulez envoyer un e-mail crypté sont des utilisateurs expérimentés de PGP, il y a des chances pour qu'elles aient placé une copie de leur clé publique sur un serveur de clés. Cela fait qu'il est très commode pour vous de récupérer la copie la plus récente de leur clé dès que vous voulez leur envoyer un e-mail et vous dispense aussi d'avoir à stocker une grande quantité de clés dans votre trousseau de clés.

Vous pouvez chercher des clés sur un serveur de clés en utilisant ces critères:

- ID d'utilisateur
- Clé ID (ou identificateur de clé)
- Statut de la clé (Revoked [Révoquée] ou Disabled [Désactivée])
- Type de clé (Diffie-Hellman ou RSA)
- Date de création
- Date d'expiration
- Clés révoquées
- Clés désactivées
- Taille de clé
- Clés signées par une clé particulière

L'inverse de la plupart de ces opérations est aussi possible. Par exemple, vous pouvez chercher en utilisant "l'ID d'utilisateur n'est pas Bob" comme critère.

Il y a de nombreux serveurs de clés publiques, comme celui maintenu par Network Associates, Inc., où vous pouvez localiser les clés de la plupart des utilisateurs de PGP. Si le destinataire ne vous a pas indiqué l'adresse Web où sa clé publique est stockée, vous pouvez accéder à tout serveur de clés et faire une recherche sur son nom d'utilisateur ou son adresse e-mail, parce que tous les serveurs de clés sont régulièrement mis à jour pour inclure les clés stockées sur tous les autres serveurs.

Pour récupérer une clé publique depuis un serveur de clés

1. Ouvrez PGPkeys.
2. Cliquez sur Search Server [Rechercher sur Serveur] dans le menu Keys ou cliquez sur  pour ouvrir la boîte de dialogue Search.

La boîte de dialogue Search s'ouvre.

3. Dans la boîte Search For Keys On, sélectionnez l'endroit ou le serveur sur lequel vous voulez chercher.
4. Saisissez le critère de recherche à utiliser pour localiser la clé publique de l'utilisateur. Pour restreindre votre recherche, cliquez sur More Choices [Choix Supplémentaires] afin de spécifier un critère additionnel.

Quand la clé publique est trouvée, vous pouvez l'examiner dans la boîte de dialogue Search pour vous assurer qu'elle est valide. Si vous décidez d'ajouter la clé à votre trousseau de clés publiques, glissez-la dans la fenêtre principale de PGPkeys.

Ajouter une clé publique depuis un message e-mail

Un moyen commode d'obtenir une copie de la clé publique de quelqu'un est que cette personne l'insère dans un e-mail. Quand une clé publique est envoyée par e-mail, elle apparaît comme un bloc de texte dans le corps du message.

Pour ajouter une clé publique depuis un message e-mail

Faites une des choses suivantes:

- Si vous avez une application e-mail qui est gérée par les plug-ins de PGP, alors cliquez sur  pour ajouter la clé de l'expéditeur à votre trousseau de clés publiques.
- Si vous utilisez une application e-mail qui ne gère pas les plug-ins, vous pouvez ajouter la clé publique au trousseau de clés en copiant le bloc de texte qui représente la clé publique et en le collant dans la fenêtre de PGPkeys.

Importer une clé publique depuis un fichier

Une autre méthode pour obtenir une clé publique est que cette personne la sauvegarde dans un fichier d'où vous pouvez l'importer ou la copier dans votre trousseau de clés publiques.

Pour importer une clé publique depuis un fichier

Il y a trois méthodes pour extraire une clé publique et l'ajouter à votre trousseau de clés:

- Cliquez sur Import dans le menu Keys et ensuite naviguez jusqu'au fichier où la clé publique est stockée.
- Glissez le fichier contenant la clé publique dans la fenêtre principale de PGPkeys.
- Ouvrez le document texte où la clé publique est stockée, sélectionnez le bloc de texte représentant la clé, puis cliquez sur Copy dans le menu Edit. Allez dans la fenêtre de PGPkeys et cliquez sur Paste dans le menu Edit pour copier la clé. L'icône de la clé s'affiche dans la fenêtre PGPkeys.

Vérifier l'authenticité d'une clé

Quand vous échangez des clés avec quelqu'un, il est parfois difficile de dire si la clé appartient réellement à cette personne. PGP vous donne plusieurs moyens de vérifier l'authenticité d'une clé et de certifier que cette clé appartient à un propriétaire particulier (c'est-à-dire la *valider*). PGP vous met en garde également si vous tentez d'utiliser une clé qui n'est pas valide et aussi, par défaut, quand vous êtes sur le point d'utiliser une clé à la validité marginale.

Pourquoi vérifier l'authenticité d'une clé?

Une des vulnérabilités majeures de la cryptographie à clé publique est la possibilité pour les auteurs d'une interception sophistiquée de monter une attaque dite "man-in-the-middle" [personne interposée] en remplaçant la clé publique de quelqu'un par une de leurs propres clés. De cette façon, ils peuvent intercepter tout e-mail crypté à l'intention de cette personne, le décrypter en utilisant leur propre clé, puis le crypter à nouveau avec la véritable clé de la personne et le lui envoyer comme si rien ne s'était passé. En fait, tout cela peut être effectué

automatiquement au moyen d'un programme sophistiqué d'ordinateur interposé qui déchiffre toute votre correspondance.

Sur la base de ce scénario, vous et ceux avec qui vous échangez des e-mails avez besoin d'une méthode pour déterminer si chacun possède effectivement de copies authentiques de la clé de l'autre. La meilleure façon d'être complètement sûr qu'une clé publique appartient réellement à une personne déterminée est de la faire copier par le propriétaire sur une disquette et de vous la faire remettre ensuite physiquement par lui. Toutefois, vous êtes rarement assez près pour remettre personnellement une disquette à quelqu'un; vous échangez généralement des clés publiques par e-mail ou les récupérez sur un serveur de clés publiques.

Vérifier avec une empreinte numérique

Vous pouvez déterminer si une clé appartient réellement à une personne déterminée en vérifiant son empreinte numérique, une série unique de nombres générée quand la clé est créée. En comparant l'empreinte de votre copie d'une clé publique avec l'empreinte sur sa clé originale, vous pouvez être absolument sûr qu'en fait vous détenez bien une copie authentique de sa clé. Pour apprendre comment vérifier une empreinte numérique, voir [“Vérifier une clé publique” en page 80](#).

Signer la clé publique

Une fois que vous êtes absolument convaincu que vous détenez une copie authentique d'une clé publique, vous pouvez la signer. En signant une clé publique avec votre clé privée, vous certifiez que vous êtes sûr que la clé appartient à l'utilisateur présumé. Par exemple, quand vous créez une nouvelle clé, elle est automatiquement certifiée avec votre propre signature numérique. Par défaut, les signatures numériques que vous apposez sur les clés ne sont pas exportables, ce qui signifie qu'elles s'appliquent à la clé uniquement quand elle se trouve dans votre trousseau de clés local. Pour des instructions détaillées pour signer une clé, voir [“Signer une clé publique” en page 81](#).

Obtenir des clés publiques via des avals de confiance

La clé publique des utilisateurs de PGP porte souvent des signatures d'autres utilisateurs dignes de confiance afin d'attester davantage de son authenticité. Par exemple, vous pourriez envoyer à un collègue digne de confiance une copie de votre clé publique en lui demandant de la certifier et de vous la retourner pour que vous puissiez inclure la signature quand vous posterez votre clé sur un serveur de clés publiques. En utilisant PGP, quand des gens récupèrent une copie de votre clé publique, ils n'ont pas à vérifier l'authenticité de la clé eux-mêmes, mais peuvent s'en remettre à leur confiance dans les personnes ayant signé votre clé. PGP permet de moduler le niveau de validité pour chacune des clés publiques que vous ajoutez à votre trousseau de clés et montre le niveau de confiance et de validité associé à chaque clé dans la fenêtre de PGPkeys. Cela signifie que quand vous récupérez une clé auprès de quelqu'un dont la clé est signée par un aval de confiance, vous pouvez être à peu près sûr que la clé appartient bien à l'utilisateur

prétendu. Pour des détails sur la manière de signer des clés et de valider des utilisateurs, voir [“Signer une clé publique” en page 81](#).

Ce chapitre explique comment crypter et signer les e-mails que vous envoyez à autrui ou décrypter et vérifier les e-mails que les autres vous envoient.

Crypter et signer des e-mails

Il y a trois façons de crypter et signer des messages e-mails. La manière la plus rapide et la plus facile de crypter et signer des e-mails est de le faire avec une application gérée par les plug-ins e-mail de PGP. Bien que la procédure varie légèrement selon les différents logiciels, vous réalisez le processus de cryptage et de signature en cliquant sur les boutons appropriés de la barre d'outils de l'application.

Si vous utilisez une application e-mail qui n'est pas gérée par les plug-ins de PGP, vous pouvez crypter et signer vos messages e-mail via le presse-papiers de Windows en sélectionnant l'option appropriée depuis l'icône en forme de verrou dans la barre des tâches. Pour inclure des fichiers attachés, vous cryptez les fichiers depuis l'Explorateur Windows avant de les attacher.

✦ **ASTUCE:** Si vous envoyez des e-mails sensibles, envisagez de laisser vierge la ligne du sujet ou d'y inscrire un sujet qui ne révèle pas le contenu de votre message crypté.

Si vous ne disposez pas de l'une des applications e-mail gérée par PGP, voir le [Chapitre 5](#) pour des informations sur comment crypter des fichiers.

Comme alternative à l'utilisation des plug-ins, vous pouvez utiliser PGTools pour crypter et signer le texte de votre e-mail et les fichiers attachés avant de les envoyer, voir "[Pour crypter et signer en utilisant PGTools](#)" en page 61.

Crypter et signer avec des applications e-mail gérées

Quand vous cryptez et signez avec une application e-mail gérée par les plug-ins de PGP, vous avez deux choix, selon le type d'application e-mail que le destinataire utilise. Si vous communiquez avec un utilisateur de PGP dont l'application gère le standard PGP/MIME, vous pouvez profiter d'une fonctionnalité de PGP/MIME pour crypter et signer vos messages et tout fichier attaché automatiquement quand vous les envoyez. Si vous communiquez avec quelqu'un dont l'application n'est pas conforme à PGP/MIME, vous devriez crypter votre e-mail en désactivant l'option PGP/MIME pour éviter des problèmes de compatibilité. Reportez-vous au [Tableau 4-1, "Fonctionnalités des plug-ins de PGP"](#), pour une liste des plug-ins et de leurs fonctionnalités.

Tableau 4-1. Fonctionnalités des plug-ins de PGP

	Eudora 3.0.x	Eudora 4.0.x	Exchange/ Outlook	Outlook Express (*)
PGP/MIME	Oui	Oui	Non	Non
Auto décrypte	Oui	Non	Oui	Oui
Crypte le HTML	N/A	Oui	Convertit en texte avant de crypter	Non
Affiche le HTML décrypté comme document HTML	Non	Oui	Non	Non
Crypte les attachements	Oui	Oui	Oui	Non
Crypte/signé par défaut	Oui	Oui	Oui	Oui

[(*) des dysfonctionnements peuvent apparaître avec la version française d'Outlook Express]

Pour crypter et signer avec des applications e-mail gérées

1. Utilisez votre application e-mail pour composer votre message comme vous le feriez normalement.
2. Quand vous avez fini de composer le texte de votre message, cliquez sur  pour crypter le texte de votre message, puis cliquez sur  pour le signer.

NOTE: Si vous savez que vous allez utiliser PGP/MIME régulièrement, vous pouvez laisser cette option activée en sélectionnant les réglages appropriés dans l'onglet Email de la boîte de dialogue Preferences.

3. Envoyez votre message comme vous le feriez normalement.

Si vous avez une copie des clés publiques de chacun des destinataires, les clés appropriées sont utilisées. Toutefois, si vous spécifiez un destinataire pour lequel il n'y a pas de clé publique correspondante ou si une ou plusieurs clés ont une validité insuffisante, la boîte de dialogue de PGPkeys apparaît (Figure 4-1) pour que vous puissiez spécifier la clé correcte.

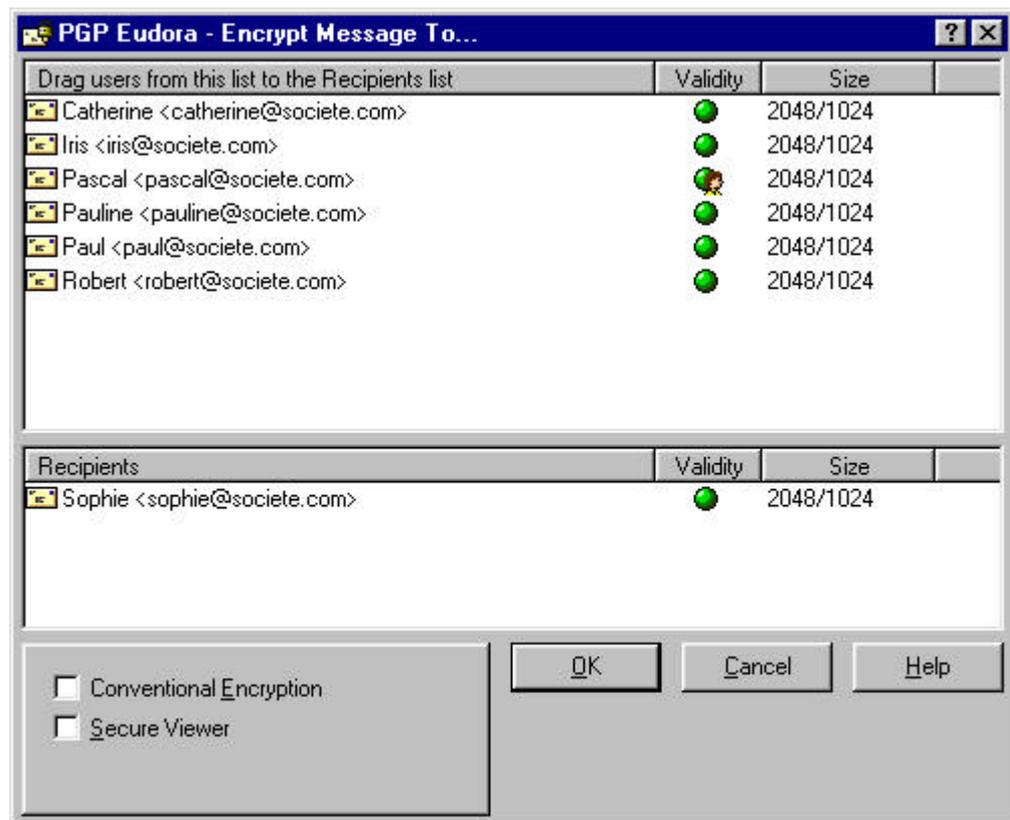


Figure 4-1. La fenêtre Recipients de PGP

4. Glissez les clés publiques de ceux qui doivent recevoir une copie du message crypté dans la boîte de la liste Recipients [Destinataires]. Vous pouvez aussi double-cliquer sur une des clés pour la déplacer d'une zone de l'écran à l'autre.

L'icône de validité indique le niveau minimum de confiance requis pour que les clés publiques dans la liste de destinataires soient valides. Cette validité est fondée sur les signatures associées à la clé. Voir le [Chapitre 6, "Gestion des Clés et Réglage des Préférences"](#) pour les détails.

5. Sélectionnez l'option Conventional Encrypt [Cryptage Conventionnel] pour utiliser une phrase secrète commune au lieu du cryptage à clé publique. Si vous sélectionnez cette option, le message est crypté avec une clé de session, qui crypte (ou décrypte) en utilisant une phrase secrète qu'il vous sera demandé de choisir.
6. Sélectionnez l'option Secure Viewer pour protéger les données d'une attaque TEMPEST au moment du décryptage. Si vous sélectionnez cette option, les données sont affichées avec une police spéciale résistante à l'attaque TEMPEST, illisible par l'équipement de capture de rayonnement au moment du décryptage. Les messages cryptés avec ce dispositif activé peuvent seulement être lus au moment du décryptage et ne peuvent pas être sauvegardés décryptés. Pour plus d'informations au sujet des attaques TEMPEST, voir "[Vulnérabilités](#)" en page 146.

NOTE: L'option Secure Viewer ne sera pas compatible avec les précédentes versions de PGP. Les messages cryptés avec cette option

activée peuvent être décryptés avec les précédentes versions de PGP, mais ce dispositif sera ignoré.

7. Cliquez sur OK pour crypter et signer votre e-mail.

Si vous avez décidé de signer les données cryptées, la boîte de dialogue Passphrase apparaît, comme dans la [Figure 4-2](#), demandant votre phrase secrète avant que l'e-mail soit envoyé.

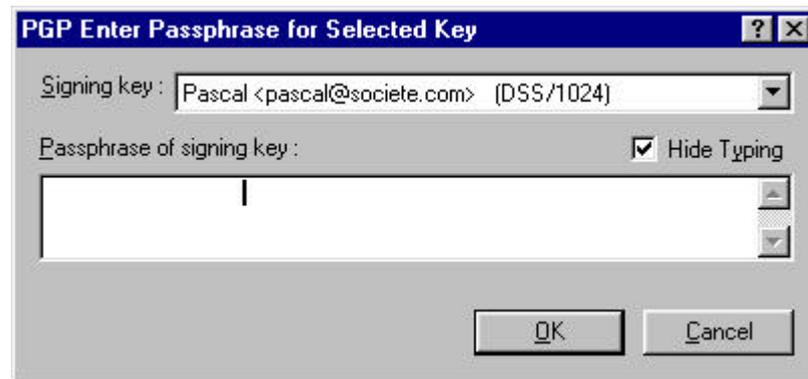


Figure 4-2. Boîte de dialogue Passphrase

8. Saisissez votre phrase secrète et cliquez sur OK.

⚠ AVERTISSEMENT: Si vous n'envoyez pas votre e-mail immédiatement mais à l'inverse le stockez dans votre file d'attente, vous devez savoir que l'information n'est pas cryptée tant que l'e-mail n'est pas réellement transmis. Avant de mettre des messages cryptés en file d'attente, vous devriez vérifier pour voir si votre application a bien effectivement crypté le message dans votre boîte d'envoi. Si elle ne l'a pas fait, vous pouvez utiliser PGPTray pour crypter vos messages avant de les mettre dans la file d'attente.

Pour crypter et signer du texte en utilisant PGPtools

1. Copiez le texte que vous voulez crypter et signer dans le presse-papiers.
2. Glissez le texte sur les boutons Encrypt [Crypter], Sign [Signer], ou Encrypt and Sign [Crypter et Signer] dans la fenêtre de PGPtools.



Figure 4-3. La fenêtre de PGPtools

La boîte de dialogue PGP Key Recipients [Clé PGP des Destinataires] apparaît ([Figure 4-1](#)).

3. Sélectionnez les clés publiques de ceux qui doivent recevoir une copie du message crypté en les glissant dans la liste Recipients. Vous pouvez aussi double-cliquer sur n'importe quelle clé pour la déplacer d'une zone de l'écran à l'autre.

L'icône de Validité indique le niveau minimum de confiance requis pour que les clés affichées dans la liste Recipients soient valides. Cette validité est fondée sur les signatures associées à la clé. Voir le [Chapitre 6, "Gestion des Clés et Réglage des Préférences"](#) pour des détails.

4. Sélectionnez l'option Conventional Encrypt pour utiliser une phrase secrète commune au lieu du cryptage à clé publique. Si vous sélectionnez cette option, le message est crypté avec une clé de session, qui crypte (ou décrypte) en utilisant une phrase secrète qu'il vous sera demandé de choisir.
5. Sélectionnez l'option Secure Viewer pour protéger les données d'une attaque TEMPEST au moment du décryptage. Si vous sélectionnez cette option, les données sont affichées avec une police spéciale résistante à l'attaque TEMPEST, illisible par l'équipement de capture de rayonnement au moment du décryptage. Les messages cryptés avec ce dispositif activé peuvent seulement être lus au moment du décryptage et ne peuvent pas être sauvegardés décryptés. Pour plus d'informations au sujet des attaques TEMPEST, voir "[Vulnérabilités](#)" en page 146.

NOTE: L'option Secure Viewer ne sera pas compatible avec les précédentes versions de PGP. Les messages cryptés avec cette option activée peuvent être décryptés avec les précédentes versions de PGP, mais ce dispositif sera ignoré.

6. Cliquez sur OK pour crypter et signer votre mail.
Si vous avez choisi de signer les données cryptées, la boîte de dialogue Passphrase apparaît comme dans la [Figure 4-2](#), demandant votre phrase secrète avant d'envoyer le message.
7. Saisissez votre phrase secrète et cliquez sur OK.
8. Collez le texte dans votre e-mail, puis envoyez le message.

Crypter un e-mail pour des groupes de destinataires

Vous pouvez utiliser PGP pour créer des groupes de listes de distribution. Par exemple, si vous voulez envoyer un e-mail crypté pour 10 personnes à chacun@adresse.com, vous pourrez créer une liste de distribution avec ce nom. Le menu Groups dans PGPkeys contient une option Show Groups qui bascule sur l'écran de la fenêtre Groups dans PGPkeys.

NOTE: Si vous avez l'intention de crypter une information pour tous les membres d'une liste de distribution existante, vous devez créer un groupe PGP avec le même nom, et incluant les mêmes membres, que la liste de distribution e-mail. Par exemple, s'il y a une liste chacun@adresse.com enregistrée dans votre application e-mail, vous devez créer un groupe chacun@adresse.com dans PGP.

Travailler avec des listes de distribution

Utilisez la fonctionnalité Groups pour créer des listes de distribution et éditer la liste des gens à qui vous voulez envoyer des e-mails cryptés.

Pour créer un groupe (liste de distribution)

1. Choisissez Show Group dans le menu Groups.
2. Choisissez New Group depuis le menu Groups.
3. Saisissez un nom pour le groupe de liste de distribution. Eventuellement, saisissez une description du groupe.
4. Cliquez sur OK pour créer la liste de distribution.

Le groupe de liste de distribution est sauvegardé comme un groupe PGP dans le répertoire des préférences et la liste est ajoutée à votre trousseau de clés.

Pour ajouter des membres à une liste de distribution

1. Dans la fenêtre PGPkeys, sélectionnez les utilisateurs ou les groupes que vous voulez ajouter à votre liste de distribution.
2. Glissez les utilisateurs depuis la fenêtre de PGPkeys jusqu'à la liste de distribution désirée dans la fenêtre Groups.

NOTE: Des membres d'une liste de distribution peuvent être ajoutés à d'autres listes de distribution.

Pour effacer des membres d'une liste de distribution

1. A l'intérieur d'une liste de distribution, sélectionnez le membre à effacer.
2. Appuyez sur Delete.
PGP vous demande de confirmer votre choix.

Pour effacer une liste de distribution

1. Sélectionnez la liste de distribution à effacer depuis la fenêtre Groups.
2. Appuyez sur Delete.

Pour ajouter une liste de distribution à une autre liste de distribution

1. Sélectionnez la liste de distribution que vous voulez ajouter à une autre liste.
2. Glissez la liste sélectionnée dans la liste à laquelle elle sera ajoutée.

Envoyer un e-mail crypté et signé à des listes de distribution

Vous pouvez envoyer un e-mail crypté à des groupes de destinataires une fois que vos listes de distribution sont créées. Voir "[Travailler avec des listes de distribution](#)" ci-dessus pour plus d'informations sur la création et l'édition de listes de distribution.

Pour envoyer un e-mail crypté et signé à une liste de distribution

1. Adressez l'e-mail à votre liste de distribution.

Le nom de votre liste de distribution pour laquelle vous cryptez doit correspondre au nom de la liste de distribution e-mail.

- Utilisez votre application e-mail pour composer votre message exactement comme vous le feriez d'habitude.
2. Quand vous avez fini de composer le texte de votre message, cliquez sur  pour crypter le texte de votre message, puis cliquez sur  pour le signer.
 3. Envoyez le message.

Décrypter et vérifier un e-mail

La façon la plus rapide et la plus facile de crypter et vérifier l'e-mail qui vous a été envoyé est de le faire avec une application gérée par les plug-ins de PGP. Bien que la procédure varie légèrement entre les différentes applications, vous pouvez effectuer les opérations de décryptage et de vérification en cliquant sur l'icône de l'enveloppe dans le message ou dans la barre d'outils de votre application. Dans certains cas vous pouvez avoir besoin de sélectionner Decrypt/Verify depuis le menu de votre application. En outre, si vous utilisez une application qui gère le standard PGP/MIME, vous pouvez décrypter et vérifier vos messages aussi bien que tout fichier attaché en cliquant sur une icône attachée à votre message.

Si vous utilisez une application qui n'est pas gérée par les plug-ins de PGP, vous décrypterez et vérifierez vos messages via PGPTray. En outre, si votre e-mail inclut des fichiers attachés cryptés, vous devez les décrypter séparément via PGPtools ou PGPTray.

Pour décrypter et vérifier depuis des applications e-mails gérées

1. Ouvrez votre message exactement comme vous le faites d'habitude.

Vous verrez un bloc de texte crypté inintelligible dans le corps de votre message.

2. Pour décrypter et vérifier le message, faites une des choses suivantes:
 - Si vous communiquez avec d'autres utilisateurs de PGP, et qu'ils ont crypté et signé leur e-mail en utilisant le standard PGP/MIME, cliquez sur l'icône représentant une enveloppe déverrouillée ()
 - Si vous recevez un e-mail de quelqu'un qui n'utilise pas une application e-mail compatible avec le standard PGP/MIME, cliquez sur l'icône représentant une enveloppe ouverte () dans la barre d'outils de votre application ou cliquez sur Decrypt/Verify Clipboard [Presse-papiers] dans le menu Plugins.

Pour décrypter et vérifier les fichiers attachés, décryptez-les séparément en utilisant PGPtools ou PGPTray.

La boîte de dialogue Enter Passphrase de PGP apparaît, comme dans la [Figure 4-4](#), vous demandant de saisir votre phrase secrète.



Figure 4-4. Boîte de dialogue Signing Key Passphrase

3. Saisissez votre phrase secrète, puis cliquez sur OK.

Le message est décrypté. S'il a été signé et que vous avez la clé publique de l'expéditeur, un message apparaît vous indiquant si la signature est valide.

Si le message est crypté avec l'option Secure Viewer activée, un message d'avertissement apparaît. Cliquez sur OK pour continuer. Le message décrypté apparaît dans un écran PGP sécurisé, dans une police spéciale résistante aux attaques TEMPEST.

4. Vous pouvez sauvegarder le message dans sa forme décryptée, ou vous pouvez sauvegarder la version originale du message afin qu'il reste sécurisé.

NOTE: Les messages cryptés avec l'option Secure Viewer activée ne peuvent pas être sauvegardés décryptés.

Pour décrypter et vérifier depuis des applications e-mail non gérées

1. Ouvrez votre message exactement comme vous le faites d'habitude.

Vous verrez un bloc de texte chiffré inintelligible dans le corps de votre message.

2. Copiez le texte chiffré dans le presse-papiers.

3. Dans PGPtray, sélectionnez Decrypt/Verify.

Si le message inclut des fichiers attachés cryptés, décryptez-les séparément via PGPtools ou PGPtray.

La boîte de dialogue Enter Passphrase de PGP apparaît, comme dans la [Figure 4-4](#), vous demandant de saisir votre phrase secrète.

4. Saisissez votre phrase secrète, puis cliquez sur OK.

Le message est décrypté. S'il a été signé et que vous avez la clé publique de l'expéditeur, un message apparaît vous indiquant si la signature est valide.

Si le message est crypté avec l'option Secure Viewer activée, un message d'avertissement apparaît. Cliquez sur OK pour continuer. Le message décrypté apparaît dans un écran PGP sécurisé, dans une police spéciale résistante aux attaques TEMPEST.

5. Vous pouvez sauvegarder le message dans sa forme décryptée, ou vous pouvez sauvegarder la version originale du message afin qu'il reste sécurisé.

NOTE: Les messages cryptés avec l'option Secure Viewer activée ne peuvent pas être sauvegardés décryptés.

Utiliser PGP pour le Stockage Sécurisé de Fichiers

5

Ce chapitre explique comment utiliser PGP pour conserver des fichiers en sécurité. Il explique comment utiliser PGP pour crypter, décrypter, signer et vérifier des fichiers tant pour l'e-mail que pour le stockage sécurisé sur votre ordinateur. Il décrit aussi les fonctions PGP Wipe [Nettoyage] et Free Space Wipe [Nettoyage de l'Espace Libre], qui effacent les fichiers en supprimant complètement leur contenu de votre ordinateur.

Utiliser PGP pour crypter et décrypter des fichiers

Vous pouvez utiliser PGP pour crypter et signer les fichiers mis en attachement des e-mails. Vous pouvez aussi utiliser les techniques décrites dans ce chapitre pour crypter et signer des fichiers de telle sorte que vous puissiez les stocker de façon sécurisée sur votre ordinateur.

Utiliser le menu du clic-droit de PGP pour crypter et signer

Utilisez le menu du clic-droit de PGP pour envoyer un fichier crypté comme attachement avec votre e-mail, ou pour crypter un fichier afin de le protéger sur votre ordinateur.

Pour crypter et signer en utilisant le menu du clic-droit

1. Dans l'Explorateur Windows, faites un clic-droit sur le ou les fichiers que vous voulez crypter.
2. Choisissez une de ces options dans le menu du clic-droit de PGP:
 - **Encrypt.** Sélectionnez cette option uniquement pour crypter le ou les fichiers que vous avez sélectionnés.
 - **Sign.** Sélectionnez cette option uniquement pour signer le ou les fichiers que vous avez sélectionnés.
 - **Encrypt and Sign.** Sélectionnez cette option pour à la fois crypter et signer le ou les fichiers que vous avez sélectionnés.

La boîte de dialogue PGP Recipients apparaît, comme montré dans la [Figure 5-1](#).

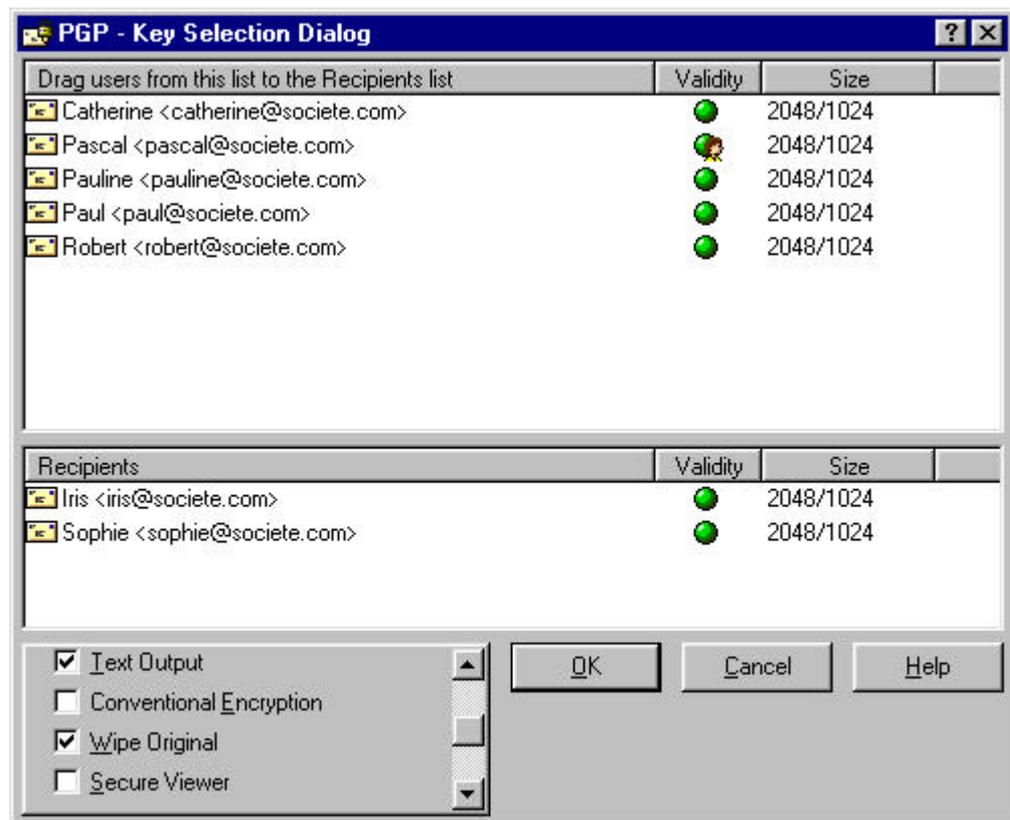


Figure 5-1. PGP Recipients

Vous pouvez sélectionner les clés publiques des destinataires pour le fichier que vous cryptez ou signez.

3. Sélectionnez les clés publiques en les glissant dans la liste des destinataires, puis cliquez sur OK.

Cliquez sur Options, puis choisissez entre les options de cryptage suivantes:

- **Conventional Encrypt [Cryptage Conventionnel].** Cochez cette case pour vous appuyer sur une phrase secrète plutôt que sur la cryptographie à clé publique. Le fichier est crypté en utilisant une clé de session, qui crypte (et décrypte) à l'aide d'une phrase secrète qu'il vous sera demandé de choisir.
- **Text Output [Sortie Texte].** En envoyant des fichiers attachés avec des applications e-mail, vous pouvez avoir besoin de cocher Text Output pour sauvegarder le fichier en texte ASCII. Cela est parfois nécessaire dans le but d'envoyer un fichier binaire en utilisant une application e-mail ancienne. Sélectionner cette option augmente la taille du fichier crypté d'environ 30 %.
- **Wipe Original [Nettoyer l'Original].** Cochez cette case pour écraser le document original que vous cryptez ou signez, de telle sorte que vos informations sensibles soient illisibles pour quiconque accède à votre disque dur.
- **Secure Viewer [Visionneuse Sécurisée].** Cochez cette option pour protéger les données d'une attaque TEMPEST au moment du décryptage.

Si vous sélectionnez cette option, les données sont affichées avec une police spéciale résistante à l'attaque TEMPEST, illisible par l'équipement de capture de rayonnement au moment du décryptage. Les fichiers cryptés avec ce dispositif activé peuvent seulement être lus au moment du décryptage et ne peuvent pas être sauvegardés décryptés. Pour plus d'informations au sujet des attaques TEMPEST, voir [“Vulnérabilités” en page 146](#).

❑ NOTE: L'option Secure Viewer ne sera pas compatible avec les précédentes versions de PGP. Les fichiers cryptés avec cette option activée peuvent être décryptés avec les précédentes versions de PGP, mais ce dispositif sera ignoré.

Si vous signez les fichiers, il vous sera demandé une phrase secrète.

Après le cryptage, si vous regardez dans le répertoire où se trouvaient les fichiers originaux, vous trouverez un fichier avec le nom spécifié représenté par une de ces deux icônes:



crypté avec sortie standard



crypté avec sortie texte

Si vous cryptez ou signez un répertoire, le fichier de sortie peut être dans un nouveau répertoire, selon les options que vous avez sélectionnées.

Utiliser PGPtools pour crypter et signer

Pour crypter et signer en utilisant PGPtools

1. Ouvrez PGPtools.



Figure 5-2. Le menu de PGPtools

2. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) que vous voulez crypter.

Vous pouvez sélectionner plusieurs fichiers, mais vous devez crypter et signer chacun d'eux individuellement.

3. Glissez le(s) fichier(s) sur le bouton Encrypt, Sign, ou Encrypt and Sign dans la fenêtre de PGPtools.

La boîte de dialogue PGP Recipients apparaît (Figure 5-1).

4. Sélectionnez les clés publiques en les glissant dans la liste Recipients.

5. Vous pouvez choisir parmi les options de cryptage suivantes en fonction du type de donnée que vous cryptez:
- **Conventional Encrypt.** Cochez cette case pour vous appuyer sur une phrase secrète plutôt que sur la cryptographie à clé publique. Le fichier est crypté en utilisant une clé de session, qui crypte (et décrypte) à l'aide d'une phrase secrète qu'il vous sera demandé de choisir.
 - **Text Output.** En envoyant des fichiers attachés avec des applications e-mail, vous pouvez avoir besoin de cocher Text Output pour sauvegarder le fichier en texte ASCII. Cela est parfois nécessaire dans le but d'envoyer un fichier binaire en utilisant une application e-mail ancienne. Sélectionner cette option augmente la taille du fichier crypté d'environ 30 %.
 - **Wipe Original.** Cochez cette case pour écraser le document original que vous cryptez ou signez, de telle sorte que vos informations sensibles soient illisibles pour quiconque accède à votre disque dur.
 - **Secure Viewer.** Cochez cette case pour protéger les données d'une attaque TEMPEST au moment du décryptage. Si vous sélectionnez cette option, les données sont affichées avec une police spéciale résistante à l'attaque TEMPEST, illisible par l'équipement de capture de rayonnement au moment du décryptage. Les fichiers cryptés avec ce dispositif activé peuvent seulement être lus au moment du décryptage et ne peuvent pas être sauvegardés décryptés. Pour plus d'informations au sujet des attaques TEMPEST, voir "[Vulnérabilités](#)" en page 146.

NOTE: L'option Secure Viewer ne sera pas compatible avec les précédentes versions de PGP. Les fichiers cryptés avec cette option activée peuvent être décryptés avec les précédentes versions de PGP, mais ce dispositif sera ignoré.

6. Cliquez sur OK.

Si vous signez les fichiers, il vous sera demandé une phrase secrète.

Après le cryptage, si vous regardez dans le répertoire où se trouvaient les fichiers originaux, vous trouverez un fichier avec le nom spécifié représenté par une de ces deux icônes:



crypté avec sortie standard



crypté avec sortie texte

Si vous cryptez ou signez un répertoire, le fichier de sortie peut être dans un nouveau répertoire, selon les options que vous avez sélectionnées.

Utiliser PGPTray pour décrypter et vérifier

Si l'e-mail que vous avez reçu a des fichiers attachés, et que vous n'utilisez pas une application e-mail compatible PGP/MIME, vous devez les décrypter via le presse-papiers de Windows.

Pour décrypter et vérifier des fichiers en utilisant PGPTray

1. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) que vous voulez décrypter et vérifier.
2. Choisissez Decrypt/Verify depuis PGPTray.

La boîte de dialogue Passphrase apparaît, comme dans la [Figure 5-3](#).



Figure 5-3. Boîte de dialogue Passphrase

3. Saisissez votre phrase secrète puis cliquez sur OK.

Si le fichier a été signé, un message apparaît indiquant si la signature est valide.

Si le message est crypté avec l'option Secure Viewer activée, un message d'avertissement apparaît. Cliquez sur OK pour continuer. Le message décrypté apparaît dans un écran PGP sécurisé, dans une police spéciale résistante aux attaques TEMPEST.

4. Vous pouvez sauvegarder le message décrypté en cet état, ou vous pouvez sauvegarder la version originale cryptée de sorte qu'il demeure sécurisé.

NOTE: Les messages cryptés avec l'option Secure Viewer activée ne peuvent pas être sauvegardés décryptés. Ils ne peuvent qu'être visualisés dans l'écran PGP sécurisé après décryptage.

Utiliser PGTools pour décrypter et vérifier

Pour décrypter et vérifier en utilisant PGTools

1. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) que vous voulez décrypter.
2. Glissez le fichier sur le bouton Decrypt/Verify dans la fenêtre PGTools (Figure 5-2).

La boîte de dialogue PGP Enter Passphrase apparaît, comme montré dans la Figure 5-3, vous demandant de saisir votre phrase secrète.

3. Saisissez votre phrase secrète, puis cliquez sur OK.

Si le fichier a été signé, un message apparaît indiquant si la signature est valide.

Si le message est crypté avec l'option Secure Viewer activée, un message d'avertissement apparaît. Cliquez sur OK pour continuer. Le message décrypté apparaît dans un écran PGP sécurisé, dans une police spéciale résistante aux attaques TEMPEST.

4. Vous pouvez sauvegarder le message décrypté en cet état, ou vous pouvez sauvegarder la version originale cryptée de sorte qu'il demeure sécurisé.

❑ NOTE: Les messages cryptés avec l'option Secure Viewer activée ne peuvent pas être sauvegardés décryptés. Il ne peuvent qu'être visualisés dans l'écran PGP sécurisé après décryptage.

Signer et décrypter des fichiers avec une clé scindée

Une fois qu'une clé est scindée entre plusieurs dépositaires de fragments, tenter de signer ou décrypter avec elle conduira automatiquement PGP à tenter de rassembler la clé. Il y a deux façons de rassembler la clé, localement et à distance.

Rassembler localement les segments de clé requiert la présence des dépositaires de fragments devant l'ordinateur rassembleur. Chaque dépositaire de fragment est requis pour saisir la phrase secrète pour son segment de clé.

Rassembler à distance les segments de clé requiert que les dépositaires de fragments éloignés authentifient et décryptent leurs clés avant de les envoyer sur le réseau. Le PGP Transport Layer Security (TLS) procure un lien sécurisé pour transmettre des segments de clé, ce qui permet à plusieurs individus situés à des endroits éloignés de signer et décrypter leur segment de clé de manière sécurisée.

🚨 IMPORTANT: Avant de recevoir des segments de clé du réseau, vous devriez vérifier l'empreinte de clé de chaque dépositaire de fragment et signer leur clé publique pour s'assurer que la clé les authentifiant est authentique. Pour savoir comment vérifier une paire de clés, voir "[Vérifier avec une empreinte numérique](#)" en page 46.

Pour signer ou décrypter avec une clé scindée

1. Contactez chacun des dépositaires de fragments de la clé scindée. Pour rassembler localement une clé scindée, les dépositaires de fragments de la clé doivent être présents. Pour rassembler les segments de clé à travers le réseau, assurez-vous que les dépositaires de fragments distants sont préparés à envoyer le fichier de leur segment de clé. Les dépositaires de fragments distants doivent avoir:
 - le fichier de leur segment de clé et leur mot de passe
 - une clé publique (pour authentification par l'ordinateur qui rassemble les segments de clé)
 - une connexion au réseau
 - l'adresse IP ou le nom de domaine de l'ordinateur qui rassemble les segments de clé
2. Sur l'ordinateur rassembleur, utilisez l'Explorateur Windows pour sélectionner le ou les fichiers que vous voulez signer ou décrypter avec la clé scindée.
3. Faites un clic-droit sur le ou les fichiers et sélectionnez Sign ou Decrypt depuis le menu de PGP.

La boîte de dialogue Enter Passphrase for Selected Key [Phrase secrète pour Clé Sélectionnée] apparaît avec la clé scindée sélectionnée.
4. Cliquez sur OK pour rassembler la clé sélectionnée.

La boîte de dialogue Key Share Collection [Rassemblement de Clé Scindée] apparaît, comme dans la [Figure 5-4](#).



Figure 5-4. Boîte de dialogue Key Share Collection

5. Si vous rassemblez les segments de clé localement, cliquez sur Select Share File [Sélectionner le segment de clé] puis localisez les segments de fichier associés à la clé scindée. Les segments de fichier peuvent être rassemblés depuis un disque dur, une disquette, ou un lecteur ouvert. Continuez avec l'étape 6.

Si vous rassemblez des segments de clé à travers le réseau, cliquez sur Start Network [Lancer le réseau].

La boîte de dialogue Passphrase s'ouvre. Dans la boîte Signing Key [Clé de Signature], sélectionnez la paire de clés que vous voulez utiliser pour l'authentification du système distant et saisissez la phrase secrète. Cliquez sur OK pour préparer l'ordinateur à recevoir les segments de clé.

L'état de la transaction est affiché dans la boîte Network Shares [Segments sur le réseau].

Quand l'état bascule sur "Listening" [Ecoule], PGP est prêt à recevoir les segments de clé.

A ce moment, les dépositaires de fragments doivent envoyer leur segment de clé. Pour savoir comment envoyer des segments de clé à l'ordinateur rassembleur, voir ["Pour envoyer votre segment de clé à travers le réseau" en page 67](#).

Quand une clé est reçue, la boîte de dialogue Remote Authentication [Authentification à distance] apparaît, comme montré dans la [Figure 5-5](#).

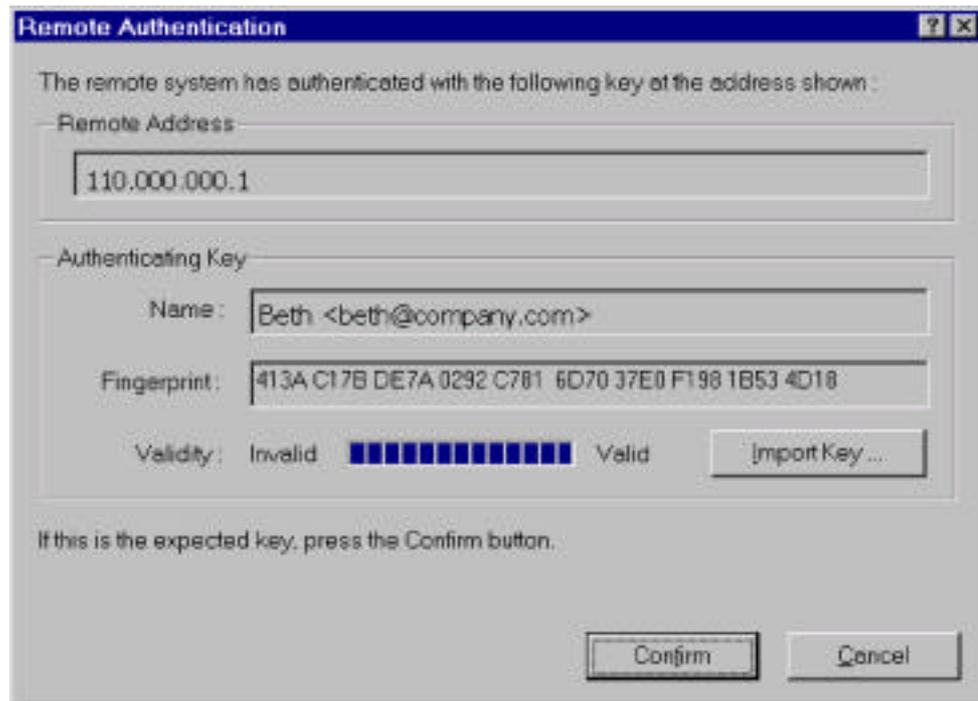


Figure 5-5. Boîte de dialogue Remote Authentication

Si vous n'avez pas signé la clé qui a été utilisée pour authentifier le système distant, la clé sera considérée comme invalide. Bien que vous puissiez rassembler la clé avec une clé d'authentification invalide, cela n'est pas recommandé. Vous devriez vérifier l'empreinte de clé de chaque dépositaire de fragment et signer leur clé publique pour vous assurer que la clé d'authentification est authentique. Cliquez sur Confirm [Confirmer] pour accepter le segment.

6. Continuez le rassemblement des segments de clé jusqu'à ce que la valeur pour Total Shares Collected [Total des segments rassemblés] corresponde à la valeur pour Total Shares Needed [Total des segments nécessaires] dans la boîte de dialogue Key Shares Collection.
7. Cliquez sur OK.

Le fichier est signé ou décrypté avec la clé scindée.

Pour envoyer votre segment de clé à travers le réseau

1. Quand vous êtes contacté par la personne qui rassemble la clé scindée, assurez-vous que vous avez ces choses:
 - le segment de clé et le mot de passe
 - une paire de clés (pour authentification par l'ordinateur qui rassemble les segments de clé)
 - une connexion au réseau
 - l'adresse IP ou le nom de domaine de l'ordinateur qui rassemble les segments de clé.

2. Sélectionnez Send Key Shares [Envoyer segments de clé] dans le menu File de PGPkeys.

La boîte de dialogue Select Share File apparaît.

3. Localisez votre segment de fichier puis cliquez sur Open [Ouvrir].

La boîte de dialogue PGP Enter Passphrase apparaît.

4. Saisissez votre phrase secrète puis cliquez sur OK.

La boîte de dialogue Send Key Shares apparaît, comme dans la [Figure 5-6](#).

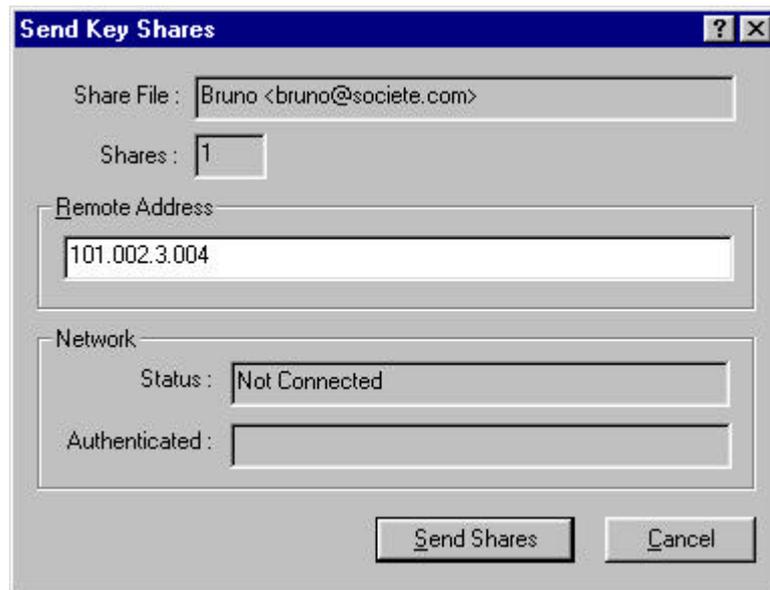


Figure 5-6. Boîte de dialogue Send Key Shares

5. Saisissez l'adresse IP ou le nom de domaine de l'ordinateur rassembleur dans la boîte Remote Address [Adresse distante], puis cliquez sur Send Shares [Envoyer les segments].

L'état de la transaction est affiché dans la boîte de dialogue Network Status [Etat du Réseau]. Quand l'état bascule sur "Connected" [Connecté], il vous est demandé de vous authentifier auprès de l'ordinateur rassembleur.

La boîte de dialogue Remote Authentication apparaît, vous demandant de confirmer que l'ordinateur distant est celui auquel vous voulez envoyer votre segment de clé.

6. Cliquez sur Confirm pour conclure la transaction.

Après que l'ordinateur distant ait reçu vos segments de clé et confirmé la transaction, un message apparaît indiquant que les segments ont été envoyés avec succès.

7. Cliquez sur OK.

8. Cliquez sur Done dans la fenêtre Key Shares quand vous avez terminé l'envoi de votre segment de clé.

Utiliser PGP Wipe pour effacer des fichiers

Le bouton Wipe dans PGTools efface les fichiers et leur contenu. La fonctionnalité Wipe est une manière sécurisée de supprimer définitivement un fichier et son contenu du disque dur de votre ordinateur. Quand vous effacez un fichier de manière normale en le plaçant dans la corbeille [puis en vidant la corbeille], le nom de ce fichier est effacé du répertoire des fichiers, mais les données contenues dans le fichier restent sur le disque. Le wipe efface toute trace des données d'un fichier de telle sorte que personne ne puisse utiliser un utilitaire pour récupérer le fichier.

Pour effacer définitivement un fichier en utilisant le menu du clic-droit de PGP

1. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) que vous voulez nettoyer.

Pour arrêter le nettoyage avant que la tâche soit terminée, cliquez sur Cancel [Annuler].

NOTE: Cliquer sur Cancel pendant le nettoyage du fichier peut laisser des bribes du fichier [sur le disque].

2. Cliquez avec le bouton droit sur le fichier puis choisissez Wipe dans le menu. Une boîte de dialogue de confirmation apparaît.
3. Cliquez sur OK pour effacer définitivement le fichier.

Pour effacer définitivement un fichier en utilisant PGTools

1. Dans l'Explorateur Windows, sélectionnez le fichier que vous voulez effacer.
2. Glissez le fichier sur le bouton Wipe () dans la fenêtre PGTools.

Une boîte de dialogue de confirmation apparaît.

3. Cliquez sur OK pour effacer définitivement le fichier.

Pour arrêter le nettoyage du fichier avant que la tâche soit terminée, cliquez sur Cancel.

NOTE: Cliquer sur Cancel pendant le nettoyage du fichier peut laisser des bribes du fichier [sur le disque].

Même sur les systèmes avec une mémoire virtuelle, PGP écrit correctement par-dessus tout le contenu du fichier. Il faut remarquer que certaines applications sauvegardent le fichier avant qu'il ne soit crypté, ce qui peut laisser des fragments du fichier sur le disque à des endroits qui ne sont plus considérés comme faisant partie du fichier. Pour plus d'informations, voir [“Fichiers d'échange et/ou mémoire virtuelle” en page 149](#). Vous pouvez utiliser la fonction PGP Freespace Wipe pour nettoyer tout l'espace libre sur votre disque afin de résoudre ce problème. Voir la partie suivante pour informations à propos du nettoyage de l'espace libre. Prenez garde aussi aux nombreux programmes qui sauvegardent automatiquement des fichiers en cours, de telle sorte qu'il peut exister des copies de sauvegarde du fichier que vous voulez effacer.

Utiliser le PGP Free Space Wiper pour nettoyer l'espace libre sur vos disques

A chaque fois que vous créez et effacez des fichiers de votre ordinateur, les données contenues dans ces fichiers restent sur le lecteur. PGPtools peut être utilisé pour nettoyer de manière sécurisée les données [contenues] dans un fichier avant qu'il ne soit effacé pour empêcher que les données soient jamais récupérées.

Beaucoup de programmes créent des fichiers temporaires pendant que vous éditez le contenu des documents. Ces fichiers sont effacés quand vous fermez les documents, mais les données du document sont laissées éparpillées sur tout votre disque. Pour aider à réduire les chances que les données de vos documents soient plus tard récupérées, Network Associates vous recommande de nettoyer l'espace libre de vos lecteurs et d'effacer de manière sécurisée les documents sensibles.

Pour nettoyer l'espace libre sur vos disques

⚠ AVERTISSEMENT: Avant de lancer le PGP Free Space Wiper, le partage de fichiers doit être désactivé et toutes les applications du volume ou du disque que vous voulez nettoyer doivent être fermées.

1. Ouvrez PGPtools.
2. Cliquez sur le bouton Wipe Free Space () dans la fenêtre de PGPtools. L'écran d'accueil du PGP Free Space Wiper apparaît.
3. Lisez l'information attentivement, puis cliquez sur Next [Suivant] pour avancer jusqu'à la boîte de dialogue suivante.

Le PGP Free Space Wiper vous demande de sélectionner le volume que vous voulez nettoyer et le nombre de passes que vous voulez effectuer.

4. Dans la boîte Volume, sélectionnez le disque ou volume que vous voulez voir nettoyé par PGP. Puis sélectionnez le nombre de passes que que PGP doit effectuer. Les indications recommandées sont:
 - 3 passes pour l'utilisation personnelle.
 - 10 passes pour l'utilisation commerciale.
 - 18 passes pour l'utilisation militaire.
 - 26 passes pour une sécurité maximale.

❑ NOTE: Des sociétés commerciales spécialisées peuvent récupérer des données qui ont été recouvertes par des écritures jusqu'à 9 fois. PGP utilise des motifs hautement sophistiqués durant chaque nettoyage pour s'assurer que vos données sensibles ne puissent pas être récupérées.

5. Cliquez sur Next pour continuer.

La boîte de dialogue Perform Wipe [Effectuer le nettoyage] s'ouvre, comme montré dans la [Figure 5-7](#), et affiche une information statistique à propos du lecteur ou volume sélectionné.



**Figure 5-7. Nettoyage de l'Espace Libre
(boîte de dialogue Perform Wipe)**

6. Cliquez sur le bouton Begin Wipe [Commencer le nettoyage] pour démarrer le nettoyage de l'espace libre de votre disque ou volume.

Le PGP Free Space Wiper inspecte puis nettoie les résidus de votre disque ou volume.

7. Quand la session de nettoyage est terminée, cliquez sur Finish [Terminer].

Ce chapitre explique comment examiner et gérer les clés stockées dans vos trousseaux. Il explique aussi comment régler vos préférences pour vous adapter à votre environnement particulier.

Gérer vos clés

Les clés que vous créez, ainsi que celles que vous recevez d'autres personnes, sont conservées dans des trousseaux, qui sont fondamentalement des fichiers stockés sur votre disque dur ou sur une disquette. Normalement, vos clés privées sont conservées dans un fichier nommé `secring.skr` et vos clés publiques sont conservées dans un autre fichier nommé `pubring.pkr`. Ces fichiers sont habituellement placés dans votre dossier PGP Keyrings.

❑ **NOTE:** Du fait que votre clé privée est cryptée automatiquement et que votre phrase secrète n'est pas compromise, il n'y a aucun danger à laisser vos trousseaux sur votre ordinateur. Cependant, si vous préférez garder vos clés ailleurs que dans les dossiers par défaut, vous pouvez choisir des noms de fichiers ou de dossiers différents. Pour des détails à ce sujet, voir "[Régler vos préférences](#)" plus loin dans ce chapitre.

Occasionnellement, vous pourriez vouloir examiner ou changer les attributs de vos clés. Par exemple, quand vous obtenez une clé publique, vous pourriez vouloir identifier son type (RSA ou Diffie-Hellman/DSS), vérifier son empreinte ou déterminer sa validité au moyen de toute signature numérique attachée à la clé. Vous pouvez aussi vouloir signer une clé publique pour indiquer que vous croyez qu'elle est valide, assigner un niveau de fiabilité au propriétaire de la clé, ou changer une phrase secrète pour votre clé privée. Vous pouvez même vouloir chercher une clé sur un serveur de clés. Vous pouvez faire toutes ces opérations de gestion des clés depuis la fenêtre PGPkeys.

La fenêtre PGPkeys

Pour ouvrir PGPkeys, cliquez sur Démarrer --> Programs --> PGP --> PGPkeys, ou cliquez sur l'icône PGPtray dans la barre des tâches, puis cliquez sur Launch PGPkeys.

La fenêtre PGPkeys ([Figure 6-1](#)) affiche les clés que vous avez créées pour vous-même, ainsi que toute clé publique que vous avez ajoutée à votre trousseau de clés publiques.

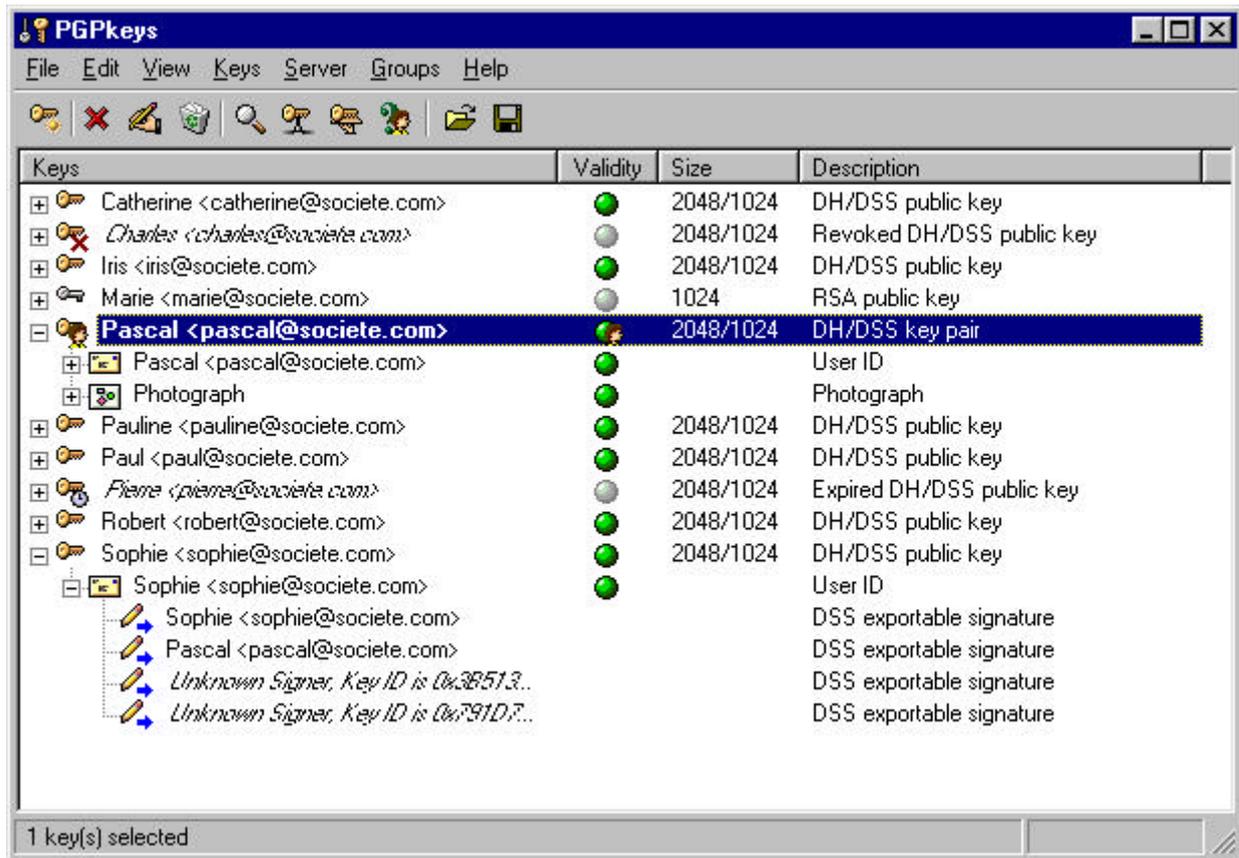


Figure 6-1. Fenêtre PGPkeys

L'icône d'une clé et d'un utilisateur (👤) représente les paires de clés publique et privée que vous avez créées pour vous-même, et les clés seules (🔑) représentent les clés publiques que vous avez récupérées. Si vous avez plus d'un type de clés, vous remarquerez que les clés RSA sont argentées et les clés Diffie-Hellman/DSS sont dorées.

En cliquant sur le signe plus à gauche de la clé, vous pouvez développer les entrées pour visualiser l'ID d'utilisateur et l'adresse e-mail du propriétaire de la clé comme représenté par l'icône de l'enveloppe (✉). En cliquant sur le signe plus à côté d'une icône d'enveloppe, vous pouvez voir les signatures de tous les utilisateurs qui ont certifié l'ID d'utilisateur. Si vous ne voulez pas développer chaque clé individuellement, sélectionnez simplement les clés qui vous intéressent puis choisissez Expand Selection depuis le menu Edit.

Description des attributs PGPkeys

Certains des attributs associés aux clés peuvent être affichés dans la fenêtre principale PGPkeys. Vous pouvez choisir les attributs que vous voulez rendre visibles en les sélectionnant dans le menu View. Pour chaque élément sélectionné dans le menu View, PGPkeys affiche une colonne dans la fenêtre principale. Si vous souhaitez changer l'ordre de ces colonnes, cliquez sur le titre de la colonne que vous voulez déplacer et glissez-la.

Keys	Montre une représentation en icône de la clé avec le nom de l'utilisateur et l'adresse e-mail du propriétaire, et les noms des signataires de la clé.
Validity	<p>Indique le degré de certitude que la clé appartient réellement à son propriétaire allégué. La validité est fondée sur l'identité de celui qui a signé la clé et la confiance que vous placez dans le(s) signataire(s) pour se porter garant de l'authenticité de la clé. Les clés publiques que vous signez vous-même ont le plus haut degré de validité, fondé sur l'hypothèse que vous ne signez la clé de quelqu'un que si vous êtes totalement convaincu qu'elle est valide. La validité de toutes les autres clés que vous n'avez pas personnellement signées, dépend du niveau de confiance que vous avez accordé à tous les autres utilisateurs qui ont signé la clé. S'il n'y a pas de signature associée à la clé, alors elle n'est pas considérée comme valide, et un message signalant ce fait apparaît lorsque vous cryptez avec cette clé.</p> <p>La validité est figurée par des icônes en forme de cercle ou de barre, en fonction du réglage adopté dans vos Advanced Preferences "Display marginal validity level" (voir "Pour régler les préférences, onglet Advanced" dans ce chapitre). Si elle est cochée, alors la validité apparaît comme:</p> <p style="margin-left: 40px;">, une barre vide pour des clés invalides</p> <p style="margin-left: 40px;">, une barre à moitié pleine pour des clés marginalement valides</p> <p style="margin-left: 40px;">, une barre pleine pour les clés valides autres que les vôtres</p> <p style="margin-left: 40px;">, une barre striée pour vos propres clés</p> <p>Si elle n'est pas cochée, alors la validité apparaît comme:</p> <p style="margin-left: 40px;">, un cercle gris pour les clés invalides et marginalement valides si dans les Advanced Preferences "Treat marginally valid keys as invalid" est coché</p> <p style="margin-left: 40px;">, un cercle vert pour les clés valides autres que les vôtres</p> <p>Dans un environnement d'entreprise, le responsable de la sécurité peut signer les clés des utilisateurs avec la Clé de Signature d'Entreprise. Les clés signées avec celle-ci sont habituellement considérées comme complètement valides. Voir Chapitre 3, "Créer et Echanger des Clés" pour plus d'informations.</p>
Size	Montre le nombre de bits utilisés pour construire la clé. En général, plus la clé est grande, moins il y a de chances qu'elle puisse jamais être compromise. Cependant, de grandes clés exigent un temps significativement plus important pour crypter et décrypter des données que n'en exigent des clés plus petites. Lorsque vous créez une clé Diffie-Hellman/DSS, il y a un nombre pour la portion Diffie-Hellman, et un autre nombre pour la portion DSS. La portion DSS est utilisée pour signer et la portion Diffie-Hellman pour crypter.
Description	Décrit le type d'information affiché dans la colonne Keys: type de clés, type d'ID, ou type de signature.
Additional Decryption Key	Montre si la clé possède une Additional Decryption Key associée.
Key ID	Un nombre d'identification unique associé à chaque clé. Ce nombre d'identification est pratique pour distinguer entre deux clés qui partagent les mêmes nom d'utilisateur et adresse e-mail.

- Trust** Indique le niveau de confiance que vous avez accordé au propriétaire de la clé pour servir d'aval pour les clés publiques d'autres personnes. Cette confiance entre en jeu lorsque vous êtes incapable de vérifier la validité d'une clé publique par vous-même et qu'à la place vous fiez au jugement d'autres utilisateurs qui ont signé la clé. Lorsque vous créez une paire de clés, elles sont considérées comme implicitement fiables, comme indiqué par les hachures dans les barres de confiance et de validité, ou par une icône affichant un cercle vert et un utilisateur.
- Quand vous recevez dans votre trousseau de clés publiques une clé publique qui a été signée par quelqu'un d'autre que son propriétaire, le niveau d'authenticité est fondé sur la confiance que vous avez accordée au signataire de cette clé. Vous assignez un niveau de confiance, qui peut-être fiable, marginale ou non fiable, dans la boîte de dialogue Key Properties.
- Expiration** Montre la date à laquelle la clé expirera. La plupart des clés sont réglées sur Never; cependant, il peut y avoir des cas où le propriétaire de la clé souhaite qu'elle puisse être utilisée seulement pour une période déterminée.
- Creation** Montre la date à laquelle la clé a été créée. Vous pouvez quelquefois faire une hypothèse au sujet de la validité de la clé sur la base du temps passé depuis qu'elle a été mise en circulation. Si la clé a été utilisée depuis un bon bout de temps, il y a moins de chances que quelqu'un essaiera de la remplacer parce qu'il y a beaucoup d'autres copies en circulation. Ne vous fiez jamais à la date de création comme seul indicateur de validité.

Examiner les propriétés d'une clé

En plus des attributs généraux affichés dans la fenêtre PGPkeys, vous pouvez aussi examiner et changer d'autres propriétés des clés et des sous-clés. Pour accéder aux propriétés d'une clé particulière, sélectionnez la clé désirée et choisissez Properties depuis le menu Keys.



Figure 6-2. Boîte de dialogue Key Properties (Onglet General)

Fenêtre key properties, onglet General

Key ID	Un nombre d'identification unique associé à chaque clé. Ce nombre d'identification est pratique pour distinguer entre deux clés qui partagent le même nom d'utilisateur et la même adresse e-mail.
Key Type	Le type de clé, que ce soit RSA ou Diffie-Hellman/DSS.
Key Size	La taille de la clé.
Created	La date à laquelle la clé a été créée.
Expires	La date à laquelle la clé expire. Les propriétaires indiquent cette date lorsqu'ils créent leurs clés et la valeur est habituellement réglée sur Never. Cependant, quelques clés sont réglées pour expirer à une date particulière si le propriétaire veut les utiliser pour un temps limité.
Cypher	CAST, Triple-DES, ou IDEA. C'est le chiffre de cryptage "preferred" [préféré] avec lequel le propriétaire de la clé vous demande de crypter quand vous utilisez sa clé publique. Si l'utilisation de ce chiffre est autorisé dans vos Advanced preferences, il sera utilisé lorsque vous crypterez avec cette clé.

- Join Key** Ouvre la boîte de dialogue Key Share Collection. Uniquement disponible pour scinder des clés. Voir [“Signer et décrypter des fichiers avec une clé scindée”](#) en page 64 pour informations sur le rassemblement de clés scindées.
- Enabled** Indique si la clé est actuellement activée. Quand une clé est désactivée, elle est estompée dans la fenêtre PGPkeys et n'est pas disponible pour exécuter une fonction PGP à l'exception du décryptage et de la vérification. Cependant, la clé reste dans votre trousseau et vous pouvez la réactiver à tout moment. Pour activer ou désactiver une clé, cochez ou décochez Enabled. (La boîte n'est pas visible pour les clés implicitement fiables.) Cette fonctionnalité est pratique pour éviter que des clés peu utilisées viennent encombrer la boîte de dialogue Key Selection lorsque vous envoyez des e-mail cryptés.
- Change Passphrase** Change la phrase secrète pour une clé privée. Si jamais vous pensez que votre phrase secrète n'est plus un secret cliquez sur ce bouton pour saisir une nouvelle phrase secrète.
- C'est une bonne idée de changer votre phrase secrète tous les six mois à peu près. Pour des instructions sur le changement de votre phrase secrète, voir [“Changer votre phrase secrète”](#) plus loin dans ce chapitre.
- Fingerprint** Un nombre d'identification unique qui est généré lorsque la clé est créée. C'est le premier critère par lequel vous pouvez vérifier l'aloï de cette clé. La meilleure manière de vérifier une empreinte est que le propriétaire vous la lise au téléphone de sorte que vous puissiez la comparer avec l'empreinte affichée sur votre copie de sa clé publique.
- Trust Model** Indique la validité de la clé sur la base de sa certification et de la confiance que vous accordez à la personne du propriétaire pour se porter garant de l'authenticité d'une clé publique. Vous réglez le niveau de fiabilité en déplaçant la barre au niveau approprié (Trusted, Marginal, ou Untrusted [Fiable, Marginale, ou Non fiable]). La barre est désactivée pour les clés révoquées, expirées et implicitement fiables.

Fenêtre key properties, onglet Subkey

- Valid From** La date à laquelle la sous-clé devient active.
- Expires** La date à laquelle la sous-clé expire. Les propriétaires indiquent cette date lorsqu'ils créent leurs sous-clés. Les sous-clés sont habituellement en activité pour un temps limité.
- Key Size** La taille de la sous-clé.
- New** Crée une nouvelle sous-clé. Pour des informations concernant la création d'une nouvelle sous-clé, voir [“Créer de nouvelles sous-clés”](#) en page 35.
- Revoke** Révoque la sous-clé sélectionnée. Après que vous aurez révoqué la sous-clé et redistribué votre clé, les autres ne seront plus en mesure de crypter des données avec cette sous-clé.
- Remove** Efface définitivement la sous-clé sélectionnée. Cette procédure est irréversible. Toute donnée qui a été cryptée avec la sous-clé sélectionnée peut toujours être décryptée.
- ASTUCE:** Utilisez l'option Revoke (décrite ci-dessus) si vous voulez désactiver la sous-clé et mettre à jour le serveur de clés. Une fois que la sous-clé a été envoyée au serveur, elle ne peut plus en être retirée.

Spécifier une paire de clés par défaut

Lorsque vous cryptez des messages ou des fichiers, PGP vous donne la possibilité de crypter en plus avec une paire de clés que vous spécifiez comme étant votre paire de clés par défaut. Quand vous signez un message ou une clé publique, PGP utilisera cette paire de clés par défaut. Votre paire de clés par défaut est affichée en gras pour la distinguer de vos autres clés. Si vous n'avez qu'une seule paire de clés dans votre trousseau, elle est automatiquement votre paire de clés par défaut. Si vous avez plus d'une paire de clés, vous pouvez désigner telle paire donnée comme paire par défaut.

Pour spécifier votre paire de clés par défaut

1. Ouvrez PGPkeys.
2. Mettez en surbrillance la paire de clés dont vous voulez faire la paire par défaut.
3. Choisissez Set Default depuis le menu Keys.

La paire de clés sélectionnée est affichée en gras, indiquant qu'elle est votre paire de clés par défaut.

Ajouter un nouveau nom d'utilisateur ou adresse à une paire de clés

Vous pouvez avoir plus d'un nom d'utilisateur ou adresse e-mail pour lesquels vous voulez utiliser la même paire de clés. Après la création d'une nouvelle paire de clés, vous pouvez ajouter d'autres noms et adresses à ces clés. Vous ne pouvez ajouter un nouveau nom d'utilisateur ou adresse e-mail que si vous détenez à la fois les clés publique et privée.

Pour ajouter un nouveau nom d'utilisateur ou adresse à une clé existante

1. Ouvrez PGPkeys.
2. Sélectionnez la paire de clés pour laquelle vous voulez ajouter un autre nom d'utilisateur ou adresse.
3. Choisissez Add/Name depuis le menu Keys.

La boîte de dialogue PGP New User Name [Nouveau Nom d'utilisateur] apparaît ([Figure 6-3](#)).



Figure 6-3. Boîte de dialogue PGP New User Name

4. Saisissez le nouveau nom et l'adresse e-mail dans les champs appropriés, puis cliquez sur OK.

La boîte de dialogue PGP Enter Passphrase apparaît.

5. Saisissez votre phrase secrète, puis cliquez sur OK.

Le nouveau nom est ajouté à la fin de la liste des noms d'utilisateurs associés à la clé. Si vous voulez régler le nouveau nom d'utilisateur et l'adresse en tant que premier identificateur pour votre clé, sélectionnez le nom et l'adresse puis choisissez Set as Primary Name [Etablir comme Premier Nom d'utilisateur] depuis le menu Keys.

Vérifier une clé publique

Par le passé il était difficile de savoir à coup sûr si une clé appartenait à un individu particulier à moins que cette personne vous ait remis physiquement la clé sur une disquette. Echanger des clés de cette façon n'est pas très pratique, spécialement pour des utilisateurs séparés par de longues distances.

Il y a plusieurs manières de vérifier l'empreinte d'une clé, mais la plus sûre est d'appeler la personne au téléphone et de lui demander de vous lire l'empreinte. Sauf si cette personne est l'objet d'une attaque, il est hautement improbable que quelqu'un soit capable d'intercepter cet appel imprévisible et puisse prendre la place de la personne que vous vous attendez à entendre de l'autre côté. Vous pouvez aussi comparer l'empreinte ou la photographie sur votre copie d'une clé publique à l'empreinte ou à la photographie de sa clé originale sur un serveur de clés publiques.

Pour vérifier une clé publique par son empreinte numérique

1. Ouvrez PGPkeys.
2. Mettez en surbrillance la clé publique que vous voulez vérifier.
3. Choisissez Properties depuis le menu Keys ou cliquez sur  pour ouvrir la boîte de dialogue Properties.

La boîte de dialogue Properties s'ouvre comme indiqué dans la [Figure 6-4](#).



Figure 6-4. Boîte de dialogue PGP Key Properties

- Utilisez les caractères affichés dans la zone de texte Fingerprint [Empreinte] pour comparer avec l’empreinte originale.

Signer une clé publique

Lorsque vous créez un jeu de clés, les clés sont automatiquement signées en utilisant votre clé privée. De la même manière, lorsque vous êtes sûr que la clé publique appartient à telle personne, vous pouvez la signer, indiquant que vous êtes sûr qu’elle est valide. Quand vous signez une clé publique, une icône associée à votre nom d’utilisateur est affichée pour cette clé.

Pour signer une clé publique

- Ouvrez PGPkeys.
- Mettez en surbrillance la clé publique que vous voulez signer.
- Choisissez Sign depuis le menu Keys ou cliquez sur  pour ouvrir la boîte de dialogue Sign Keys [Signer les Clés].

La boîte de dialogue Sign Keys apparaît (Figure 6-5) avec la clé publique et l’empreinte affichée dans la zone de texte.



**Figure 6-5. Boîte de dialogue PGP Sign Keys
(fewer Choices)**

4. Cochez “Allow signature to be exported...”, pour permettre à votre signature d’être exportée avec cette clé.

Une signature exportable est celle qui est autorisée à être envoyée sur les serveurs et à voyager avec la clé lorsqu’elle est exportée, ainsi que lorsqu’elle est déposée dans un e-mail. La case offre un raccourci pour indiquer que vous souhaitez exporter votre signature.

Ou

Cliquez sur le bouton More Choices pour configurer les options, telles que le type de signature et l’expiration de la signature (Figure 6-6).

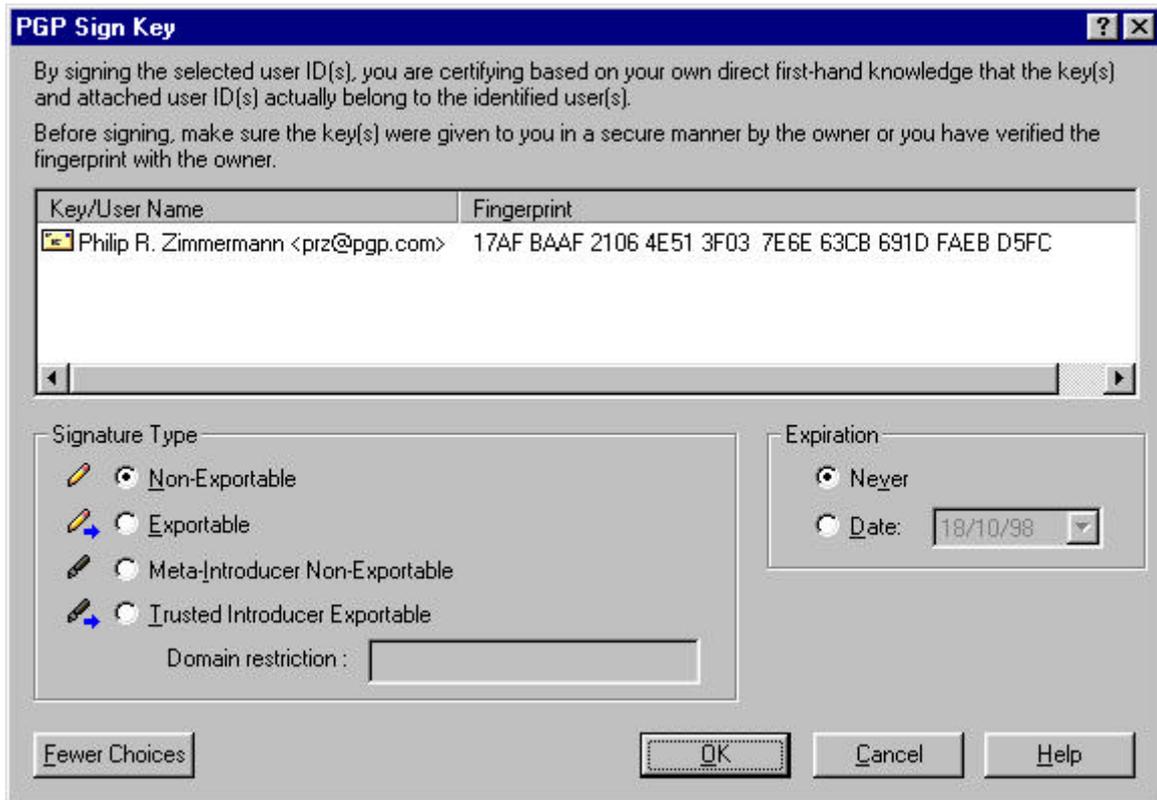


Figure 6-6. Boîte de dialogue PGP Sign Keys
(More Choices)

Choisissez un type de signature pour signer. Vos options sont:

- **Non-exportable.** Utilisez cette signature lorsque vous croyez que la clé est valide mais que vous ne voulez pas que d'autres s'appuient sur votre certification. Ce type de signature ne peut pas être envoyé avec la clé sur un serveur de clés, ni exporté en aucune manière.
- **Exportable.** Utilisez les signatures exportables dans les cas où votre signature est envoyée avec la clé au serveur de clés de sorte que d'autres puissent s'appuyer sur votre signature s'ils vous font confiance. Cela équivaut à cocher "Allow signature to be exported..." dans le menu Sign Keys.
- **Meta-Introducer [Méta-Aval].** Certifie que vous considérez comme aval de confiance cette clé et toutes les clés signées par elle avec une Trusted Introducer Validity Assertion [Affirmation de Validité d'Aval de Confiance]. Ce type de signature n'est pas exportable.
- **Trusted Introducer [Aval de Confiance].** Utilisez cette signature dans les cas où vous voulez certifier que cette clé est valide, et que le propriétaire de la clé est complètement fiable pour garantir d'autres clés. Ce type de signature est exportable. Vous pouvez restreindre les capacités de validation de l'aval de confiance à un domaine e-mail particulier.

5. Cliquez sur le bouton Sign.

La boîte de dialogue Passphrase apparaît.

6. Saisissez votre phrase secrète, puis cliquez sur OK.

Une icône associée à votre nom d'utilisateur est maintenant associée à la clé publique que vous venez de signer.

Accorder sa confiance pour valider des clés

En plus de certifier qu'une clé appartient à quelqu'un, vous pouvez assigner un niveau de fiabilité à l'utilisateur des clés indiquant combien vous le jugez digne d'agir comme aval envers d'autres dont vous pourriez vous procurer les clés à l'avenir. Cela signifie que si jamais vous récupérez une clé qui a été signée par celui que vous avez désigné comme fiable, la clé est considérée comme valide même si vous ne l'avez pas vérifiée vous-même.

Pour accorder sa confiance à une clé

1. Ouvrez PGPkeys.
2. Dans la fenêtre PGPkeys, sélectionnez la clé pour laquelle vous voulez changer le niveau de confiance.

NOTE: Vous devez signer la clé avant de pouvoir régler son niveau de confiance. Si vous n'avez pas déjà signé la clé, voir [“Signer la clé publique” en page 46](#) pour instructions.

3. Choisissez Properties depuis le menu Keys ou cliquez sur  pour ouvrir la boîte de dialogues Properties, comme montré dans la [Figure 6-4](#).
4. Utilisez la barre Trust Level [Niveau de fiabilité] pour choisir le niveau de confiance approprié pour la paire de clés.

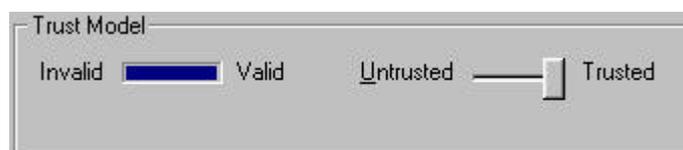


Figure 6-7. Boîte de dialogue Trust Level

5. Fermez la boîte de dialogue pour accepter le nouveau réglage.

Désactiver et activer des clés

Quelquefois, vous pourriez vouloir désactiver provisoirement une clé. La possibilité de désactiver des clés est pratique quand vous voulez conserver une clé publique pour un usage ultérieur, mais que vous ne voulez pas qu'elle vienne encombrer votre liste de destinataires chaque fois que vous envoyez des messages.

Pour désactiver une clé

1. Ouvrez PGPkeys.
2. Dans la fenêtre PGPkeys, sélectionnez la clé que vous voulez désactiver.
3. Sélectionnez Disable dans le menu Keys.

La clé est estompée et provisoirement inutilisable.

Pour activer une clé

1. Ouvrez PGPkeys.
2. Sélectionnez la clé que vous voulez activer.
3. Sélectionnez Enable dans le menu Keys.

La clé [estompée] devient visible et peut être utilisée comme avant.

Effacer une clé, une signature ou un ID d'utilisateur

Il pourra arriver que vous vouliez effacer une clé, une signature, ou un ID d'utilisateur associés à une clé particulière.

-
- NOTE:** Quand vous effacez une clé, une signature ou un ID d'utilisateur d'une clé, ils sont effacés et ne sont pas récupérables. Les signatures et les ID d'utilisateur peuvent être ajoutés à nouveau à une clé, et une clé publique importée peut être importée à nouveau dans votre trousseau. Cependant, une clé privée qui n'existe que dans ce trousseau ne peut pas être recréée, et tous les messages cryptés avec sa clé publique ne peuvent plus désormais être décryptés.
-

Pour effacer une clé, une signature, ou un ID d'utilisateur

1. Ouvrez PGPkeys.
2. Sélectionnez la clé, la signature, ou l'ID d'utilisateur que vous voulez effacer.
3. Choisissez Delete depuis le menu Edit ou cliquez sur  dans la barre d'outils.

La boîte de dialogue Confirmation apparaît.

4. Cliquez sur OK.

Changer votre phrase secrète

C'est une bonne habitude de changer votre phrase secrète à intervalles réguliers, par exemple tous les trois mois. Plus important encore, vous devriez changer votre phrase secrète si vous avez des raisons de penser qu'elle a été compromise, par exemple, par quelqu'un qui aura pu la voir par-dessus votre épaule pendant que vous la tapiez.

Pour changer votre phrase secrète

1. Ouvrez PGPkeys.
2. Mettez en surbrillance votre clé affichée dans la fenêtre PGPkeys.
3. Choisissez Properties depuis le menu Keys ou cliquez sur  pour ouvrir la boîte de dialogues Properties.

La boîte de dialogue Properties apparaît (voir [Figure 6-4](#)).

4. Cliquez sur Change Passphrase.

La boîte de dialogue Passphrase apparaît.

-
- NOTE:** Si vous voulez changer la phrase secrète pour une clé scindée, vous devez d'abord rassembler la clé. Cliquez sur Join [Joindre] pour collecter les segments de clé. Voir "[Signer et décrypter des fichiers avec une clé scindée](#)" en page 64 pour des informations au sujet du rassemblement de clé.
-

5. Saisissez votre phrase secrète actuelle dans la zone adéquate, puis cliquez sur OK.

La boîte de dialogue Change Passphrase apparaît.

6. Saisissez votre nouvelle phrase secrète dans la première zone de texte. Appuyez sur la touche TAB pour avancer à la prochaine zone de texte et confirmez votre saisie en saisissant votre nouvelle phrase secrète encore une fois.
7. Cliquez sur OK.

-
-  **AVERTISSEMENT:** Si vous êtes en train de changer votre phrase secrète parce que vous pensez qu'elle a été compromise, vous devriez nettoyer toutes vos sauvegardes de trousseaux de clés et nettoyer votre espace libre.
-

Importer et Exporter des Clés

Bien que vous distribuiez souvent votre clé publique et obteniez celles d'autrui en copiant et collant le texte depuis un serveur de clés publiques ou d'entreprise, vous pouvez aussi échanger des clés en les important et en les exportant sous forme de fichier texte séparé. Par exemple, quelqu'un peut vous remettre une disquette contenant sa clé publique, ou vous pouvez vouloir rendre votre clé publique disponible en la mettant sur un serveur FTP.

Pour importer une clé depuis un fichier

1. Ouvrez PGPkeys.
2. Choisissez Import depuis le menu Keys.
La boîte de dialogue Import apparaît.
3. Sélectionnez le fichier qui contient la clé que vous voulez importer puis cliquez sur Open.
La boîte de dialogue Import Selection apparaît.
4. Sélectionnez la clé(s) que vous voulez importer dans votre trousseau, puis cliquez sur Import.
5. La clé(s) importée(s) apparaît dans la fenêtre PGPkeys, d'où vous pouvez l'utiliser pour crypter des données ou pour vérifier une signature numérique.

Pour ajouter une clé depuis un message e-mail

Si un collègue vous envoie un message contenant sa clé (comme un bloc de texte), vous pouvez l'ajouter à votre trousseau.

1. Pendant que la fenêtre du message est ouverte, ouvrez la fenêtre PGPkeys.
2. Superposez les deux fenêtres de sorte que vous puissiez voir une partie de la fenêtre PGPkeys derrière celle du message.
3. Sélectionnez le texte de la clé, en incluant le BEGIN PGP PUBLIC KEY BLOCK et le END PGP PUBLIC KEY BLOCK, et déposez le texte dans la fenêtre PGPkeys.

La boîte de dialogue Import Selection apparaît.

4. Sélectionnez la clé(s) que vous voulez importer dans votre trousseau, puis cliquez sur Import.
5. La clé(s) importée(s) apparaît dans la fenêtre PGPkeys, d'où vous pouvez l'utiliser pour crypter des données ou pour vérifier une signature numérique.

Pour exporter une clé vers un fichier

1. Ouvrez PGPkeys.
2. Sélectionnez la clé que vous voulez exporter dans un fichier.
3. Choisissez Export depuis le menu Keys.

La boîte de dialogue Export apparaît.

4. Saisissez le nom du fichier ou parcourez le disque jusqu'à l'endroit où la clé doit être exportée puis cliquez sur Save.

La clé exportée est sauvegardée dans le fichier nommé dans le répertoire de destination spécifié.

Révoquer une clé

S'il arrivait que vous ne puissiez plus vous fier à votre paire de clés personnelle, vous pouvez créer et diffuser un certificat de révocation disant à tout le monde de cesser d'utiliser votre clé publique. La meilleure manière d'annoncer qu'une clé a été révoquée est de la mettre sur un serveur de clés publiques.

Pour révoquer une clé

1. Ouvrez PGPkeys.
2. Sélectionnez la paire de clés que vous voulez révoquer.
3. Choisissez Revoke depuis le menu Keys.

La boîte de dialogue Revocation Confirmation apparaît.

4. Cliquez sur OK pour confirmer votre intention de révoquer la clé sélectionnée.

La boîte de dialogue PGP Enter Passphrase apparaît.

5. Saisissez votre phrase secrète, puis cliquez sur OK.

Quand vous révoquez une clé, elle est barrée d'un trait rouge pour indiquer qu'elle n'est plus valide.

6. Envoyez la clé révoquée au serveur de sorte que tout le monde puisse savoir qu'il ne faut plus utiliser votre vieille clé.

Il est possible qu'un jour, vous oubliiez votre phrase secrète ou perdiez votre clé privée. Dans ce cas, vous ne serez plus capable d'utiliser votre clé, et vous n'aurez plus moyen de révoquer votre vieille clé lorsque vous en créez une nouvelle. Pour vous prémunir contre cette éventualité, vous pouvez instituer un tiers révocateur de clés dans votre trousseau de clés publiques pour révoquer votre clé. Le tiers que vous désignez pourra révoquer votre clé Diffie-Hellman/DSS, l'envoyer au serveur et ce sera exactement comme si vous l'aviez révoquée vous-même.

Pour instituer un révocateur désigné

1. Ouvrez PGPkeys.
2. Sélectionnez la clé pour laquelle vous voulez désigner un révocateur.
3. Sélectionnez Add/Revoker [Ajouter/Révocateur] depuis le menu Keys.
Une boîte de dialogue s'ouvre et affiche une liste de clés.
4. Sélectionnez la clé(s) dans la liste des ID d'utilisateur que vous voulez instituer en tant que révocateur désigné.
5. Cliquez sur OK.
Une boîte de dialogue de confirmation apparaît.
6. Cliquez sur OK pour continuer.
La boîte de dialogue Passphrase apparaît.
7. Saisissez votre phrase secrète, puis cliquez sur OK.
8. La clé(s) sélectionnée(s) est maintenant autorisée à révoquer votre clé. Pour rendre cela effectif, distribuez une copie de votre clé au(x) révocateur(s) ou envoyez-la au serveur. Voir "[Distribuer votre clé publique](#)" en page 40 pour instructions.

Régler vos préférences

PGP est configuré pour satisfaire les besoins de la plupart des utilisateurs, mais vous avez la possibilité d'ajuster certains des réglages pour les adapter à votre environnement particulier. Vous spécifiez ces réglages via la boîte de dialogue Preferences à laquelle vous accédez en choisissant Preferences depuis le menu Edit de PGPkeys.

Pour régler les préférences, onglet general

1. Ouvrez PGPkeys.
2. Dans le menu Edit de PGPkeys, sélectionnez Preferences.
Le menu Preferences s'ouvre sur l'onglet General affichant ([Figure 6-8](#)).

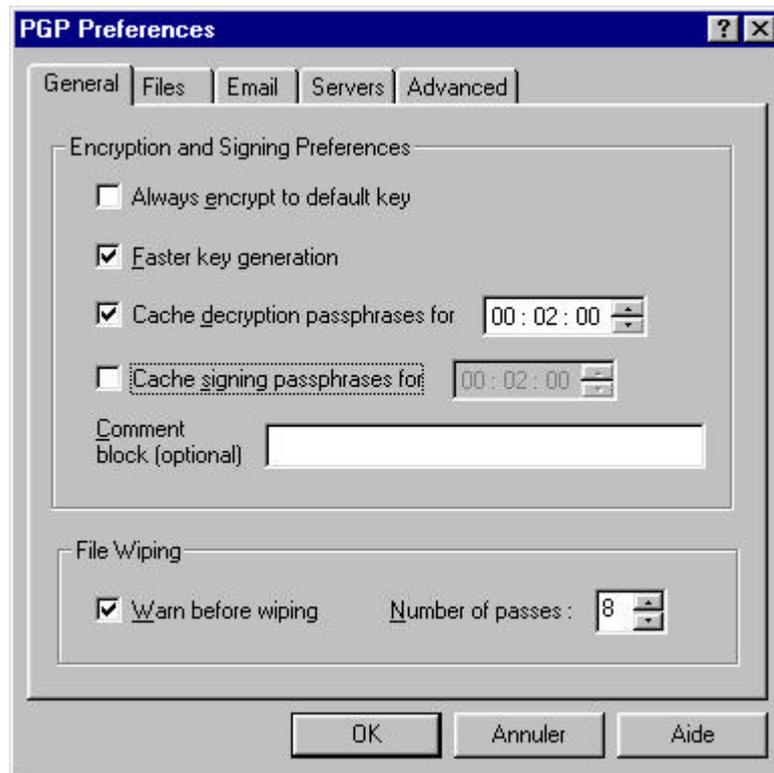


Figure 6-8. Boîte de dialogue PGP Preferences (onglet General)

3. Sélectionnez Encryption depuis l'onglet General. Vos options sont:
- **Always encrypt to default key [Toujours crypter avec la clé par défaut].** Quand cette option est cochée, tous les messages et les fichiers attachés que vous cryptez avec la clé publique du destinataire sont aussi cryptés avec votre clé publique par défaut. Il est intéressant de laisser ce réglage activé de sorte que vous avez la possibilité de décrypter le contenu de tous messages ou fichiers que vous aurez cryptés.
 - **Faster Key Generation [Génération de Clé Rapide].** Quand cette option est cochée, il faudra moins de temps pour générer une nouvelle paire de clés Diffie-Hellman/DSS. Ce processus est accéléré en utilisant un jeu de nombres premiers préalablement calculés plutôt qu'en recourant au long processus d'en créer à partir de rien chaque fois qu'une nouvelle clé est générée. Cependant, rappelez-vous que cette génération de clés rapide ne s'applique qu'à des clés de tailles prédéfinies comprises entre 1024 et 4096 telles qu'elles sont affichées lorsque vous créez une clé et n'est pas utilisée lorsque vous saisissez une autre valeur. Bien qu'il y ait peu de chance que quelqu'un puisse craquer votre clé en connaissant ces nombres premiers fixes, certains peuvent vouloir dépenser plus de temps pour créer une paire de clés avec le niveau maximum de sécurité.

L'opinion généralement admise dans la communauté cryptographique est que l'utilisation de ces nombres premiers fixes n'altère pas la sécurité pour les algorithmes Diffie-Hellman/DSS. Si cette fonctionnalité vous inquiète, vous pouvez la désactiver. Pour plus d'informations, lisez la FAQ située sur le site Web de Network Associates.

- **Cache Decryption Passphrases for... [Mettre la Phrase secrète de Décryptage en cache pour]** Lorsque cette option est cochée, votre phrase secrète de décryptage est automatiquement stockée dans la mémoire de votre ordinateur. Spécifiez la durée (en heures: minutes: secondes) pendant laquelle vous voulez conserver votre phrase secrète. Le réglage par défaut est de 2 minutes.
 - **Cache Signing Passphrases for... [Mettre la Phrase secrète de Signature en cache pour]** Quand cette option est cochée, votre phrase secrète de signature est automatiquement stockée dans la mémoire de votre ordinateur. Spécifiez la durée (en heures: minutes: secondes) pendant laquelle vous voulez conserver votre phrase secrète. Le réglage par défaut est de 2 minutes.
 - **Comment block [Texte de commentaire].** Vous pouvez ajouter votre texte de commentaire dans cette zone. Le texte sera toujours inclus dans les messages et les fichiers que vous crypterez ou signerez.
 - **Warn before wiping files [Avertir avant de nettoyer des fichiers].** Lorsque cette option est cochée, une boîte de dialogue apparaît avant de nettoyer un fichier pour vous donner une dernière chance de changer d'avis avant que PGP écrive par dessus le contenu du fichier et l'efface de votre ordinateur.
4. Cliquez sur OK pour sauvegarder vos modifications et retourner au menu PGPkeys ou choisissez un autre onglet pour continuer à configurer vos préférences PGP.

Pour régler les préférences, onglet Files

Utilisez l'onglet Files pour spécifier l'endroit où sont stockés vos trousseaux de clés publiques et privées.

1. Ouvrez PGPkeys.
2. Sélectionnez Preferences depuis le menu Edit de PGPkeys, puis cliquez sur l'onglet Files [Fichiers].

Le menu Preferences s'ouvre sur l'onglet Files affichant ([Figure 6-9](#)).

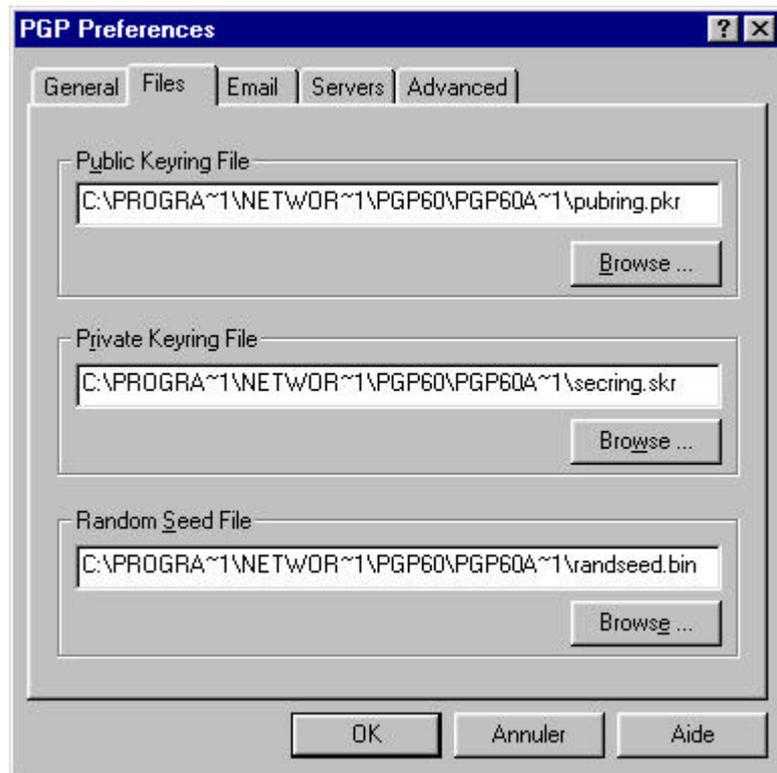


Figure 6-9. Boîte de dialogue PGP Preferences (onglet Files)

3. Utilisez les zones affichées dans l'onglet Files pour déterminer les emplacements appropriés pour vos trousseaux de clés publiques et privées et/ou le fichier de semence de nombres aléatoires:
 - **Public Keyring File [Trousseau de Clés Publiques].** Montre l'emplacement actuel et le nom du fichier où PGP s'attend à trouver votre trousseau de clés publiques. Si vous projetez de stocker vos clés publiques dans un fichier avec un nom différent ou à un autre endroit, vous l'indiquez ici. L'endroit que vous spécifiez sera aussi utilisé pour stocker toutes les sauvegardes automatiques du trousseau de clés publiques.
 - **Private Keyring File [Trousseau de Clés Privées].** Montre l'emplacement actuel et le nom du fichier où PGP s'attend à trouver votre trousseau de clés privées. Si vous projetez de stocker vos clés privées dans un fichier avec un nom différent ou à un autre endroit, vous l'indiquez ici. Quelques utilisateurs préfèrent garder leur trousseau de clés privées sur une disquette, qu'ils insèrent comme une clé à chaque fois qu'ils ont besoin de signer ou de décrypter des messages. L'endroit que vous indiquez sera aussi utilisé pour stocker toutes les sauvegardes automatiques de votre trousseau de clés privées.
 - **Random Seed Location [Emplacement du Fichier de Semence de Nombres Aléatoires].** Montre l'endroit où le fichier Random Seed est placé. Quelques utilisateurs peuvent préférer garder leur fichier Random Seed à un endroit sûr pour empêcher une falsification. Etant donné que cette attaque est très difficile et a été prévue par PGP, déplacer le fichier Random Seed de son emplacement par défaut n'offre qu'un intérêt limité.

4. Cliquez sur OK pour sauvegarder vos modifications et revenir au menu PGPkeys ou choisissez un autre onglet pour continuer à configurer vos préférences PGP.

Pour régler les préférences, onglet Email

Utilisez l'onglet Email pour indiquer les préférences qui affecteront la manière dont les fonctions de PGP s'exécuteront pour votre logiciel d'e-mail spécifique. Rappelez-vous que vos choix ne s'appliqueront pas tous à votre logiciel d'e-mail spécifique.

1. Ouvrez PGPkeys.
2. Sélectionnez Preferences depuis le menu Edit de PGPkeys, puis cliquez sur l'onglet Email.

Le menu Preferences s'ouvre avec l'onglet Email affichant (Figure 6-10).

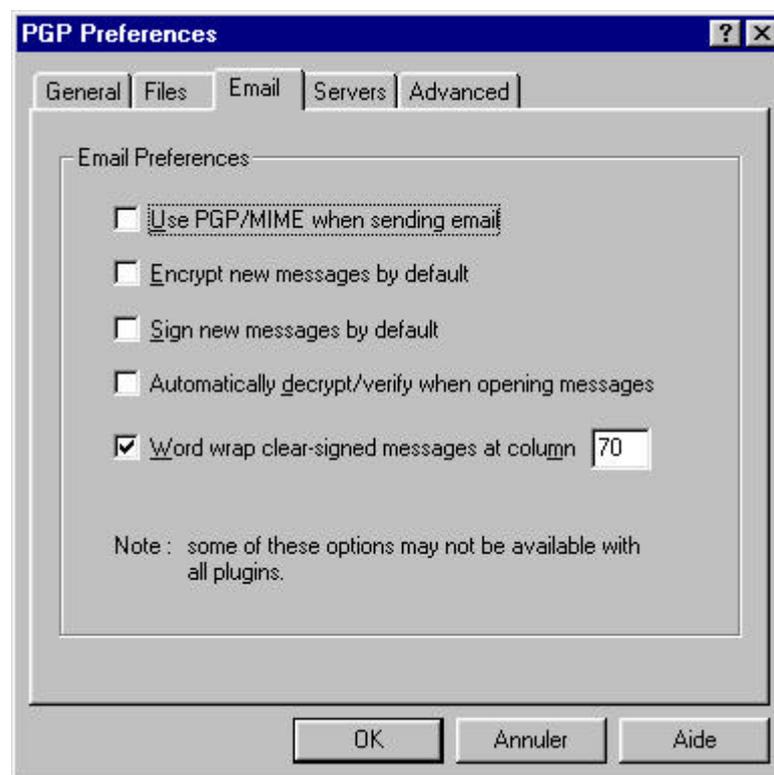


Figure 6-10. Boîte de dialogue PGP Preferences (onglet Email)

3. Sélectionnez vos préférences Email Encryption depuis l'onglet Email. Vos options sont:
 - **Use PGP/MIME when sending mail [Utiliser PGP/MIME en envoyant les e-mails]**. Si vous utilisez Eudora et que vous activez cette option, tous vos messages et fichiers attachés sont automatiquement cryptés à l'intention du destinataire. Cette option est sans effet sur les autres opérations de cryptage que vous effectuez à partir du presse-papiers ou avec l'Explorateur Windows et ne devrait pas être utilisée si vous projetez d'envoyer des messages à des destinataires qui utilisent des logiciels d'e-

mail qui ne gèrent pas la norme PGP/MIME. En utilisant Eudora, les attachements seront toujours cryptés quel que soit ce réglage, mais si le destinataire ne dispose pas de PGP/MIME, le processus de décryptage devra être fait manuellement.

- **Encrypt new messages by default [Crypter les nouveaux messages par défaut].** Si vous cochez cette case, tous vos messages et fichiers attachés sont automatiquement cryptés. Quelques logiciels d'e-mail ne peuvent pas gérer cette fonctionnalité.
- **Sign new messages by default [Signer les nouveaux messages par défaut].** Si vous cochez cette case, tous vos messages et fichiers attachés sont automatiquement signés. Quelques logiciels d'e-mail ne gèrent pas cette fonctionnalité. Ce réglage est sans effet sur les autres signatures que vous ajoutez depuis le presse-papiers ou avec l'Explorateur Windows.
- **Automatically decrypt/verify when opening messages [Décrypter / vérifier automatiquement en ouvrant les messages].** Si vous cochez cette case, tous vos messages et fichiers attachés cryptés et/ou signés sont automatiquement décryptés et vérifiés. Quelques logiciels d'e-mail ne gèrent pas cette fonctionnalité.
- **Word warp clear-signed messages at column [Découper les lignes des messages signés en clair à la colonne].** Cette option spécifie à quelle colonne un retour chariot est ajouté pour insérer un saut de ligne dans votre signature numérique. Cette fonctionnalité est nécessaire parce que tous les logiciels ne gèrent pas les coupures de lignes de la même façon, ce qui rendrait incompréhensibles les coupures de lignes dans vos messages signés. Le réglage par défaut est 70 ce qui évite des problèmes avec la plupart des logiciels.

⚠ AVERTISSEMENT: Si vous changez le réglage des coupures de ligne dans PGP, assurez-vous qu'il est inférieur à ceux de votre logiciel d'e-mail. Si vous le réglez sur une longueur égale ou supérieure, des retours chariot seraient ajoutés qui invalideraient votre signature PGP.

4. Cliquez sur OK pour sauvegarder vos modifications et revenir au menu PGPkeys ou choisissez un autre onglet pour continuer à configurer vos préférences PGP.

Pour régler les préférences, onglet Servers

Utilisez l'onglet Server pour spécifier les réglages pour les serveurs de clés publiques que vous utilisez habituellement pour envoyer et récupérer des clés publiques et avec lesquels vous synchroniserez automatiquement vos clés.

1. Ouvrez PGPkeys.
2. Sélectionnez Preferences depuis le menu Edit de PGPkeys, puis cliquez sur l'onglet Server.
3. Le menu Preferences s'ouvre avec un onglet Server affichant (Figure 6-11).

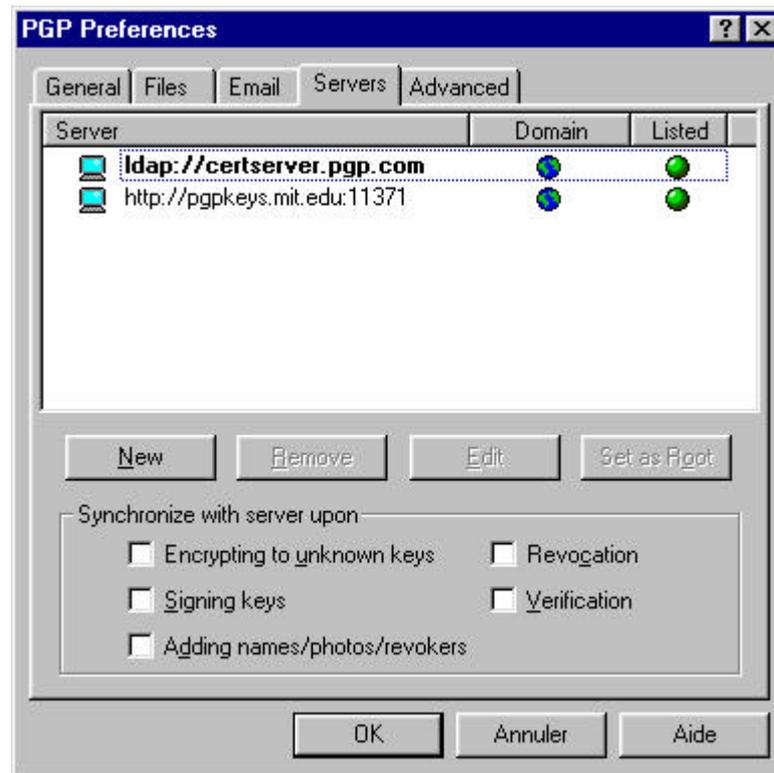


Figure 6-11. Boîte de dialogue PGP Preferences (onglet Server)

La colonne Domain [Domaine] liste le domaine Internet (tel “societe.com”) du serveur(s) disponible(s). Lors de l’envoi de clés au serveur, PGP essaie de trouver le domaine de la clé dans la liste puis retrouve le serveur approprié. Si le domaine n’est pas trouvé, le premier serveur de domaine mondial qui propose des clés sera utilisé, et les autres serveurs situés en dessous dans la liste seront explorés si la première recherche est infructueuse.

4. Pour régler vos préférences de serveur, utilisez ces boutons:
 - **New.** Ajoute un nouveau serveur à votre liste.
 - **Remove.** Enlève le serveur sélectionné de la liste.
 - **Edit.** Vous permet d’éditer les informations du serveur sélectionné.
 - **Set Root Server.** Identifie le serveur Root [Racine] qui est utilisé pour des opérations spécifiques d’entreprise, telle que la mise à jour de listes de groupe, l’envoi de listes de groupe, la mise à jour d’avals, etc. Dans les réglages des sociétés, votre administrateur les aura déjà configurés.
5. Dans la zone “Synchronize with server upon” [Synchroniser avec serveur sur], sélectionnez les options à utiliser lorsque vous synchronisez votre trousseau personnel avec le(s) serveur(s) de clés. Vos options sont:
 - **Encrypting to unknown keys [Crypter pour des clés inconnues].** Cochez cette case pour que PGP recherche automatiquement sur le serveur les destinataires dont les clés ne se trouvent pas dans votre trousseau lorsque vous cryptez l’e-mail.

- **Adding names/photo/revokers [Ajouter des noms/photo/révocateurs].** Cochez cette case pour que les clés auxquelles vous ajoutez des noms, des photographies ou des révocateurs soient d'abord mises à jour depuis le serveur, puis vos modifications envoyées sur le serveur lorsque vous effectuez la mise à jour. Mettre d'abord à jour la clé assure que, par exemple, elle n'a pas été révoquée depuis la dernière mise à jour.
 - **Signing keys [Signature de clés].** Cochez cette case pour que les clés auxquelles vous allez ajouter votre signature soient d'abord mises à jour depuis le serveur, puis vos modifications envoyées sur le serveur lorsque vous effectuez la mise à jour.
 - **Revocations [Révocations].** Cochez cette case pour que les clés que vous révoquez soient d'abord mises à jour depuis le serveur, puis vos modifications envoyées sur le serveur lorsque vous effectuez la mise à jour.
 - **Verification.** Cochez cette case pour que PGP recherche et importe automatiquement depuis le serveur la clé publique de l'expéditeur lorsque vous vérifiez la signature d'un message ou d'un fichier signé, si elle ne se trouve pas dans votre trousseau.
6. Cliquez sur OK pour sauvegarder vos modifications et revenir au menu PGPkeys ou choisissez un autre onglet pour continuer à configurer vos préférences PGP.

Pour ajouter un serveur de clés à la liste des serveurs

1. Ouvrez PGP Preferences, puis cliquez sur l'onglet Servers.
2. Cliquez sur le bouton New.

La boîte de dialogue Add New Server [Ajouter un Nouveau Serveur] apparaît, comme montré dans la [Figure 6-12](#).

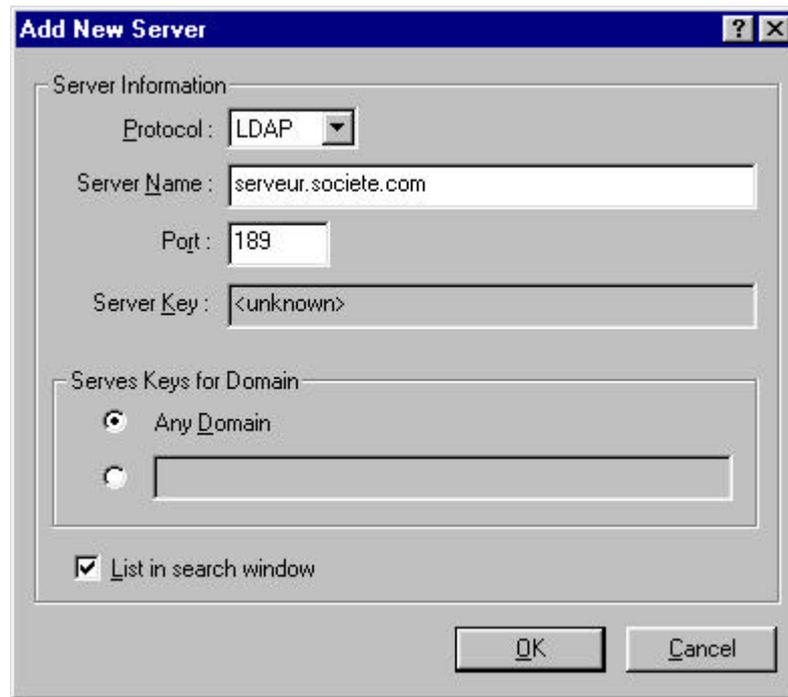


Figure 6-12. Boîte de dialogue Add New Server

3. Dans le champ Protocol [Protocole], choisissez un protocole à utiliser pour accéder au serveur. Vos options sont LDAP, LDAPS et HTTP.
4. Dans le champ Server Name [Nom du Serveur], saisissez le nom de domaine ou l'adresse IP du serveur. Par exemple, serveur.societe.com ou 123.445.67.89.
5. Saisissez le numéro du port dans le champ Port box. Par exemple, 1137 est utilisé pour les serveurs de clés HTTP ancienne manière, 389 est communément utilisé pour les serveurs de clés LDAP.
6. Le Server Key box sert pour les serveurs LDAPS. La clé du serveur est utilisée par le serveur pour authentifier la connexion. (Les informations de clé ne sont pas affichées jusqu'à ce que vous soyez connecté au serveur.)
7. Cochez l'option Any Domain [Tout Domaine] pour permettre à PGP d'envoyer des clés de n'importe quel domaine sur ce serveur de clés. Cette option est activée par défaut.

Si vous voulez que PGP n'envoie que des clés d'un domaine spécifique sur ce serveur de clés, cochez l'option sous Any Domain. Puis, saisissez le nom du domaine dans le champ approprié. Par exemple, si vous spécifiez le domaine societe.com, seules celles des clés dont l'adresse e-mail se termine par societe.com seront envoyées sur ce serveur.

8. Cochez List in Search Window [Afficher dans la Fenêtre de Recherche] si vous voulez que ce serveur de clés apparaisse dans la fenêtre PGPkeys Search.

Pour régler les préférences, onglet Advanced

Cliquez sur l'onglet Advanced [Avancé] pour aller à la fenêtre où vous sélectionnez le chiffre de cryptage et vos options de fiabilité de clé.

PGP vous donne le choix de sélectionner et/ou de changer les chiffres de cryptage. Vous pouvez sélectionner le chiffre de cryptage pour vos clés PGP: CAST (par défaut), IDEA, ou Triple-DES. Si vous voulez utiliser IDEA ou Triple-DES, vous devez les choisir avant de générer vos clés. CAST est un nouveau chiffre en lequel PGP et d'autres cryptographes ont une grande confiance, et Triple-DES est un chiffre du Gouvernement des USA qui a surmonté l'épreuve du temps. IDEA est le chiffre utilisé pour toutes les clés RSA générées par PGP. Pour plus d'informations au sujet de ces chiffres, voir [“Les chiffres symétriques de PGP” en page 133](#).

Le choix Preferred Algorithm [Chiffre Préféré] affecte les éléments suivants:

- Quand on utilise le cryptage conventionnel, le chiffre préféré est utilisé pour crypter.
- Quand on crée une clé, le chiffre préféré est enregistré comme partie intégrante de la clé de sorte que les autres utiliseront ce chiffre lorsqu'ils crypteront à votre intention.

Le choix Allowed Algorithm [Chiffre Autorisé] affecte les éléments suivants:

- Quand on crée une clé, les chiffres autorisés sont enregistrés comme partie intégrante de la clé de sorte que les autres utiliseront un de ces chiffres lorsqu'ils crypteront à votre intention si le chiffre préféré est indisponible pour eux.

NOTE: Crypter avec une clé publique échouera si ni le chiffre préféré ni les chiffres autorisés ne sont disponibles pour celui qui crypte le message.

 **AVERTISSEMENT:** Utilisez les cases de CAST, IDEA et Triple-DES seulement si vous avez tout à coup décidé qu'un chiffre particulier n'est pas sûr. Par exemple, si vous êtes informés que Triple-DES a été cassé, vous pouvez désélectionner sa case et toutes les nouvelles clés que vous générerez enregistreront que Triple-DES ne doit pas être utilisé lorsque l'on crypte à votre intention.

PGP vous donne le choix de sélectionner et/ou de changer la manière dont la fiabilité d'une clé est affichée, et si vous voulez ou non être averti quand vous cryptez un message avec une clé publique munie d'une Additional Decryption Key associée. Dans la zone Trust Model, choisissez:

- **Display marginal validity level [Afficher la validité marginale].** Utilisez cette case pour indiquer si vous voulez que soient affichées comme telles les clés marginalement valides, ou simplement si la validité est activée ou pas. La validité marginale apparaît comme une icône en forme de barre avec des hachures estompées. La validité apparaît en icône en forme de cercle; vert pour valide, gris pour invalide (la clé n'a pas été validée; elle n'a été signée ni par un aval de confiance, ni par vous-même).
- **Treat marginally valid keys as invalid [Traiter les clés marginalement valides comme des clés invalides].** Utilisez cette case pour indiquer que toutes les clés marginalement valides seront traitées comme si elles étaient

invalides. Cocher cette option fait apparaître la boîte de dialogue Key Selection lorsque vous cryptez avec des clés marginalement valides.

- **Warn when encrypting to an ADK [Avertir quand cryptage avec une ADK].** Utilisez cette case pour indiquer s'il faut afficher un avertissement lorsque une clé de cryptage possède une Additional Decryption Key associée.
- **Export Format.**
 - **Compatible:** exporte les clés dans un format compatible avec les versions antérieures de PGP.
 - **Complete:** exporte au nouveau format de clé qui inclut les ID photographiques.

Rechercher une clé

Vous pouvez rechercher des clés sur les trousseaux locaux et sur des serveurs de clés distants.

Pour rechercher une clé d'utilisateur

1. Ouvrez PGPkeys.
2. Choisissez Search depuis le menu Server ou cliquez sur le bouton Search () dans le menu PGPkeys.
La fenêtre PGPkeys Search apparaît.
3. Choisissez le serveur sur lequel chercher depuis le menu Search for Key On.
4. Indiquez vos critères de recherche.
Par défaut il s'agit de User ID, mais vous pouvez cliquer sur les flèches pour sélectionner Key ID, Key Status, Key Type, Key Size, Creation Date, ou Expiration Date. Par exemple, vous pourriez rechercher toutes les clés avec Fred comme User ID.
5. Spécifiez le critère pour lequel vous recherchez.

Vous pouvez utiliser n'importe lequel des critères suivants:

- Contains [contient]
- Does not contain [ne contient pas]
- Is [est]
- Is not [n'est pas]
- Is signed by [est signé par]
- Is not signed by [n'est pas signé par]
- Is at least (for creation or expiration date) [est au moins (pour les dates de création ou d'expiration)]
- Is at most (for creation or expiration date) [est au plus (pour les dates de création ou d'expiration)]

6. Saisissez la valeur pour laquelle vous voulez faire la recherche.
7. Cliquez sur More Choices pour ajouter des critères additionnels à votre recherche; par exemple, les clés ID avec le nom Fred créées antérieurement ou le 6 octobre 1997.
8. Pour commencer la recherche cliquez sur Search.

Une barre de progression montre l'avancement de la recherche.

NOTE: Pour arrêter une recherche en cours, cliquez sur Stop Search.

Le résultat de la recherche apparaît dans la fenêtre.

9. Pour importer les clés déposez-les dans la fenêtre principale PGPkeys.
10. Cliquez sur Clear Search pour effacer vos critères de recherche.



Ce chapitre décrit PGPdisk, ses fonctionnalités, et explique comment l'utiliser.

Qu'est-ce que PGPdisk?

PGPdisk est une application de cryptage facile d'emploi qui vous permet d'affecter une partie de votre espace disque au stockage de vos données sensibles. Cet espace réservé est utilisé pour créer un fichier appelé volume PGPdisk.

Bien qu'il ne soit en fait rien de plus qu'un simple fichier, un volume PGPdisk se comporte plutôt comme un disque dur en ce sens qu'il fournit un espace de stockage pour vos fichiers et vos applications. Vous pouvez vous le représenter comme une disquette ou un disque dur externe. Pour utiliser les applications et les fichiers stockés dans le volume, vous l'ouvrez, ou vous vous le rendez accessible.

Quand un volume PGPdisk est ouvert, vous pouvez l'utiliser comme vous le feriez de n'importe quel autre disque. Vous pouvez y installer des applications ou y sauvegarder vos fichiers. Quand le volume n'est pas ouvert, il est inaccessible à quiconque ignore votre phrase secrète, qui est une sorte de long mot de passe.

Même ouvert, un volume protège encore: sauf si un fichier ou une application sont en cours d'utilisation, ils y restent cryptés. Si votre ordinateur devait planter pendant qu'un volume est ouvert, son contenu restera crypté.

❑ **NOTE:** Les produits PGP vous encouragent à utiliser une phrase entière ou une longue série de caractères pour protéger vos données sensibles. De telles phrases secrètes sont en général plus sûres que les traditionnels mots de passe de 6-10 caractères.

Fonctionnalités PGPdisk

Le programme PGPdisk:

- Vous permet de créer des volumes sécurisés de données cryptées qui fonctionnent exactement comme n'importe quel support que vous avez l'habitude d'utiliser pour stocker vos fichiers.
- Offre un cryptage rapide et sûr de vos données sans ralentissement sensible du temps d'accès à vos programmes et fichiers.
- Utilise CAST, un puissant algorithme de cryptage de qualité "militaire", qui jouit d'une solide réputation de résistance à tout accès non autorisé.
- Stocke le contenu de chaque volume sécurisé dans un fichier crypté qui peut être aisément sauvegardé et échangé avec des collègues.

Pourquoi utiliser PGPdisk?

Bien que d'autres produits offrent la possibilité de restreindre l'accès à des fichiers au moyen de droits d'accès et de protection par mot de passe, ces mesures de sécurité peuvent être aisément tournées par des individus déterminés à mettre le nez dans vos affaires. C'est seulement en cryptant vos données que vous êtes assuré que, même à l'aide des technologies les plus sophistiquées connues à ce jour, il est quasiment impossible pour quiconque de décrypter le contenu de vos fichiers.

Voici quelques raisons d'utiliser PGPdisk pour sécuriser le contenu de vos fichiers:

- Pour protéger des informations sensibles, financières, médicales ou intimes, auxquelles vous ne voulez pas que d'autres accèdent. Ceci est particulièrement important en ces temps d'environnement réseau où les données de votre ordinateur sont exposées au monde entier quand vous surfez sur Internet.
- Pour délimiter des zones personnelles de travail sur une machine partagée sur laquelle chaque utilisateur s'assure un accès exclusif à ses propres programmes et fichiers. Chaque utilisateur peut ouvrir son ou ses volumes pendant qu'il utilise la machine, tout en étant assuré que personne d'autre ne pourra accéder aux fichiers une fois que les volumes auront été fermés.
- Pour créer des volumes de données qui ne sont accessibles qu'à des membres déterminés d'un groupe de travail donné. Un volume pourra être ouvert quand des membres de l'équipe voudront travailler à un projet déterminé, puis refermé et ainsi verrouillé lorsqu'ils auront fini.
- Pour empêcher quiconque d'accéder à des informations personnelles stockées sur un portable. En général, si vous perdez votre portable (ou si quelqu'un le vole), toutes vos informations personnelles (accès et mots de passe à des services en ligne, contacts professionnels et personnels, données financières, etc.) sont exposées à une utilisation inappropriée entre des mains indelicates et peuvent finir par coûter plus cher que le prix du portable lui-même.
- Pour sécuriser le contenu de supports externes, tels que des disquettes ou des cartouches de sauvegarde. La possibilité de crypter un support externe ajoute à la sécurité pour la conservation et l'échange d'informations sensibles.

Démarrer PGPdisk

Pour démarrer PGPdisk

1. Sélectionnez Start—>Programs—>PGP—>PGPdisk.

Ceci ouvre la barre d'outils PGPdisk comme montré dans la [Figure 7-1](#).

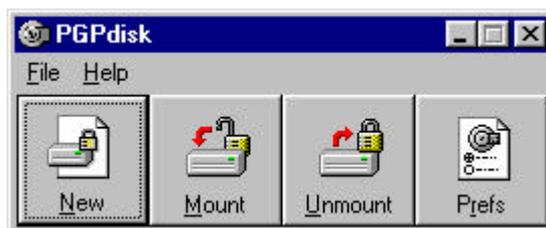


Figure 7-1. La barre d'outils PGPdisk

La barre d'outils PGPdisk offre un moyen commode de créer et d'ouvrir des volumes. Voici une brève description de chaque bouton :

New	Affiche l'assistant PGPdisk, qui vous guide à travers le processus de création d'un nouveau volume PGPdisk.
Mount	Ouvre le volume PGPdisk spécifié si la bonne phrase secrète est saisie.
Unmount	Ferme le volume PGPdisk spécifié.
Preferences	Spécifie comment vous souhaitez fermer vos volumes.

Travailler avec des Volumes PGPdisk

Ce chapitre explique comment créer, ouvrir et fermer des volumes PGPdisk et comment régler les paramètres qui protégeront leur contenu en les refermant dans certaines circonstances particulières.

NOTE: Vous pouvez effectuer la plupart des opérations PGPdisk en cliquant avec le bouton droit sur l'icône du fichier de volume PGPdisk.

Créer un nouveau volume PGPdisk

Pour créer un nouveau volume PGPdisk

1. Démarrez PGPdisk. La barre d'outils PGPdisk apparaît.
2. Cliquez sur New. L'assistant PGPdisk apparaît sur votre écran. Lisez l'information introductive.
3. Cliquez sur Next.
4. Spécifiez le nom et l'emplacement du nouveau volume.
5. Cliquez sur Save.
6. Saisissez la quantité d'espace que vous voulez affecter au nouveau volume (champ PGPdisk Size). Utilisez des nombres entiers, sans décimale. Vous pouvez utiliser les flèches pour augmenter ou diminuer le nombre affiché. La quantité d'espace libre sur le disque sur lequel il sera créé est affichée au-dessus du champ Size.

7. Cliquez sur le bouton approprié pour sélectionner kilo-octets, méga-octets, ou giga-octets.

En fonction de l'espace disque disponible, vous pouvez créer un volume de n'importe quelle taille comprise entre 100 Ko et 2 Go.

8. Sélectionnez la lettre de lecteur sous laquelle vous voulez que s'ouvre votre volume PGPdisk (champ PGPdisk Drive Letter). Vous pouvez utiliser la flèche pour afficher et sélectionner une lettre de lecteur différente.
9. Cliquez sur Next.
10. Saisissez la chaîne de mots ou de caractères qui vous servira de phrase secrète pour accéder au nouveau volume (aussi appelée phrase secrète principale du volume). Pour confirmer votre saisie, appuyez sur TAB pour avancer à la zone de saisie suivante, puis saisissez à nouveau la même phrase secrète. La taille minimum requise pour une phrase secrète est de 8 caractères.

En principe, à titre de mesure de sécurité supplémentaire, les caractères que vous saisissez pour la phrase secrète ne sont pas visibles à l'écran. Cependant, si vous êtes sûr que personne ne regarde (que ce soit physiquement ou par le réseau) et que vous voudriez voir les caractères de votre phrase secrète pendant que vous les saisissez, décochez la case Hide Typing.

NOTE: Votre sécurité est totalement tributaire de la qualité de votre phrase secrète. Votre phrase secrète devrait contenir plus d'un mot, avec des espaces, des nombres et d'autres caractères imprimables. La phrase secrète est sensible à la casse. Sa taille minimum autorisée est de 8 caractères. Choisissez quelque chose qui vous est familier et se trouve déjà bien ancré dans votre mémoire. En choisir une sur l'inspiration du moment vous amènera à l'oublier complètement. Il est vital que vous n'oubliez pas votre phrase secrète, ou bien vous perdrez vos données! Pour plus d'informations, voir ["Qualité de la Phrase Secrète" en page 115](#).

11. Cliquez sur Next.
12. Déplacez votre souris d'une manière aléatoire dans la fenêtre de l'Assistant et/ou frappez des touches sur le clavier jusqu'à ce que la barre de progression dans la boîte de dialogue soit complètement remplie.

Vos mouvements de souris et vos frappes sont utilisées pour générer de l'information aléatoire utilisée par PGPdisk comme partie intégrante du processus de cryptage (brouillage des données).
13. Cliquez sur Next. Une barre de progression indique l'état d'avancement de la création du volume PGPdisk.
14. Cliquez sur Next pour ouvrir votre PGPdisk.
15. Cliquez sur Finish. La fenêtre de formatage apparaît sur votre écran.
16. Saisissez un nom pour le nouveau volume (ce nom identifie le volume dans l'Explorateur Windows).
17. Cliquez sur Start. Une boîte de dialogue d'avertissement apparaît.
18. Cliquez sur OK (puisque'il n'y a aucune donnée sur le nouveau disque). Le système vous informe que le formatage est effectué.

19. Cliquez sur Close dans la fenêtre de formatage.

Votre volume PGPdisk apparaît dans la fenêtre de l'Explorateur.

Une icône représentant votre volume apparaît à l'endroit que vous avez spécifié. Double-cliquez sur l'icône pour ouvrir le volume.

Une icône représentant votre volume crypté apparaît à l'endroit que vous avez spécifié, comme montré ci-dessous.



Volume PGPdisk ouvert



Volume PGPdisk crypté

Changer une phrase secrète

Vous pouvez changer la phrase secrète principale ou auxiliaire d'un fichier PGPdisk.

Pour changer votre phrase secrète

1. Assurez-vous que le fichier PGPdisk n'est pas ouvert. Vous ne pouvez pas changer une phrase secrète si le fichier PGPdisk est ouvert.
2. Sélectionnez Change Passphrase depuis le menu File.
3. Sélectionnez le fichier PGPdisk concerné.
4. Saisissez la phrase secrète actuelle comme montré dans la [Figure 7-2](#).



Figure 7-2. La boîte de dialogue Passphrase

Cliquez sur OK. La fenêtre New Passphrase apparaît.

5. Saisissez la chaîne de mots ou de caractères qui vous servira de phrase secrète pour accéder au nouveau volume (aussi appelée phrase secrète principale du volume). Pour confirmer votre saisie, appuyez sur la touche TAB pour avancer à la zone de saisie suivante, puis saisissez à nouveau la même phrase secrète. La taille minimum requise pour une phrase secrète est de 8 caractères.

6. Cliquez sur OK.

La boîte de dialogue New Passphrase se referme.

Ajouter des phrases secrètes auxiliaires

Une fois que vous avez saisi la phrase secrète principale (celle utilisée lors de la création du disque), vous pouvez ajouter jusqu'à sept autres phrases secrètes auxiliaires qui peuvent être utilisées pour ouvrir le volume. Vous pouvez vouloir le faire si vous utilisez régulièrement la même phrase secrète principale et voulez autoriser quelqu'un d'autre à accéder au volume avec sa propre phrase secrète personnelle. Seul celui qui connaît la phrase secrète principale peut ajouter des phrases secrètes auxiliaires.

Tout utilisateur connaissant une phrase secrète peut changer celle-ci, mais vous serez toujours en mesure d'accéder au contenu du volume si nécessaire.

Vous avez aussi la possibilité d'assigner au volume un attribut "lecture seule", qui permettra aux personnes autorisées de lire les fichiers mais les empêchera de les modifier de quelque façon que ce soit.

Pour ajouter des phrases secrètes auxiliaires

1. Assurez-vous que le volume PGPdisk n'est pas ouvert. Vous ne pouvez pas changer une phrase secrète pendant que le volume PGPdisk est ouvert.
2. Sélectionnez Add Passphrase depuis le menu File.

La boîte de dialogue Passphrase apparaît, vous demandant de saisir la phrase secrète principale du volume. Si vous avez plusieurs volumes PGPdisk sur votre ordinateur, vous devez sélectionner un volume.

3. Saisissez la phrase secrète principale et cliquez sur OK.

La boîte de dialogue New Passphrase apparaît, comme montré dans la [Figure 7-3](#).

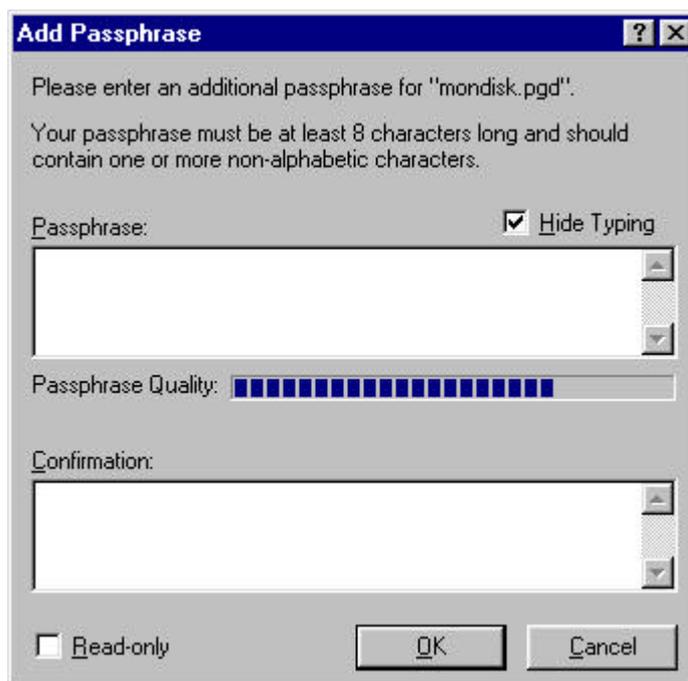


Figure 7-3. La boîte de dialogue New Passphrase

4. Saisissez une phrase secrète auxiliaire pour ce volume puis appuyez sur TAB. Saisissez la phrase secrète encore une fois pour la confirmer.

Arrivé là, vous avez aussi la possibilité de cocher la case Read-only pour indiquer que vous voulez que tout le contenu du volume soit accessible en “lecture seule.”

5. Cliquez sur OK.

Une fois que vous avez créé une phrase secrète auxiliaire, vous (ou quiconque la connaît) pouvez retirer la phrase secrète en choisissant la commande Remove Passphrase depuis le menu File. Les phrases secrètes principales ne peuvent pas être retirées. (Pour plus d’informations, voir [“Retirer une phrase secrète”](#), ci-dessous.

Retirer une phrase secrète

Le retrait d’une phrase secrète est une opération similaire à son addition ou à son changement. Vous ne pouvez pas retirer une phrase secrète principale.

Pour retirer une phrase secrète

1. Assurez-vous que le volume PGPdisk n’est pas ouvert. Vous ne pouvez pas retirer une phrase secrète si le volume PGPdisk est ouvert.
2. Choisissez Remove Passphrase depuis le menu File.
Une boîte de dialogue apparaît, vous demandant de saisir la phrase secrète à retirer.
3. Saisissez la phrase secrète, puis cliquez sur OK.

Retirer toutes les phrases secrètes auxiliaires

Vous pouvez aussi retirer toutes les phrases secrètes d'un seul coup. Cela peut être utile si d'autres utilisateurs disposent de phrases secrètes auxiliaires pour un volume PGPdisk, et que vous ne voulez plus qu'ils aient accès au volume.

Pour retirer toutes les phrases secrètes auxiliaires

1. Assurez-vous que le volume PGPdisk n'est pas ouvert. Vous ne pouvez pas retirer une phrase secrète si le volume PGPdisk est ouvert.
2. Gardez appuyée la touche MAJ et sélectionnez Remove Alternate Passphrases depuis le menu File.

Une boîte de dialogue apparaît pour confirmer que vous voulez retirer toutes les phrases secrètes auxiliaires.

3. Cliquez sur Yes.

Une boîte de dialogue apparaît, vous annonçant que vous avez réussi à retirer toutes les phrases secrètes auxiliaires.

Ajouter ou retirer des clés publiques

Vous pouvez ajouter et retirer des clés publiques à un fichier PGPdisk. Cette fonctionnalité permet à ceux qui connaissent la phrase secrète pour ces clés de l'utiliser pour ouvrir le volume.

Pour ajouter une clé publique à votre volume PGPdisk

1. Assurez-vous que le volume PGPdisk n'est pas ouvert. Vous ne pouvez pas ajouter une clé publique si le volume est ouvert.
2. Choisissez Add/Remove Public Keys depuis le menu File.
3. Sélectionnez le disque PGPdisk depuis la barre d'outils Select PGPdisk.
Il vous sera demandé de saisir la phrase secrète principale.
La fenêtre Recipient Selection Dialog apparaît.
4. Glissez la ou les clés de la fenêtre du haut vers celle du bas.
5. Cliquez sur OK.

Pour retirer une clé publique de votre volume PGPdisk

1. Assurez-vous que le volume PGPdisk n'est pas ouvert. Vous ne pouvez pas retirer une clé publique si le volume est ouvert.
2. Choisissez Add/Remove Public Keys depuis le menu File.
3. Sélectionnez le disque PGPdisk depuis la barre d'outils Select PGPdisk.
Il vous sera demandé de saisir la phrase secrète principale.
La fenêtre PGP Key Selection Dialog apparaît, comme montré dans la [Figure 7-4](#).

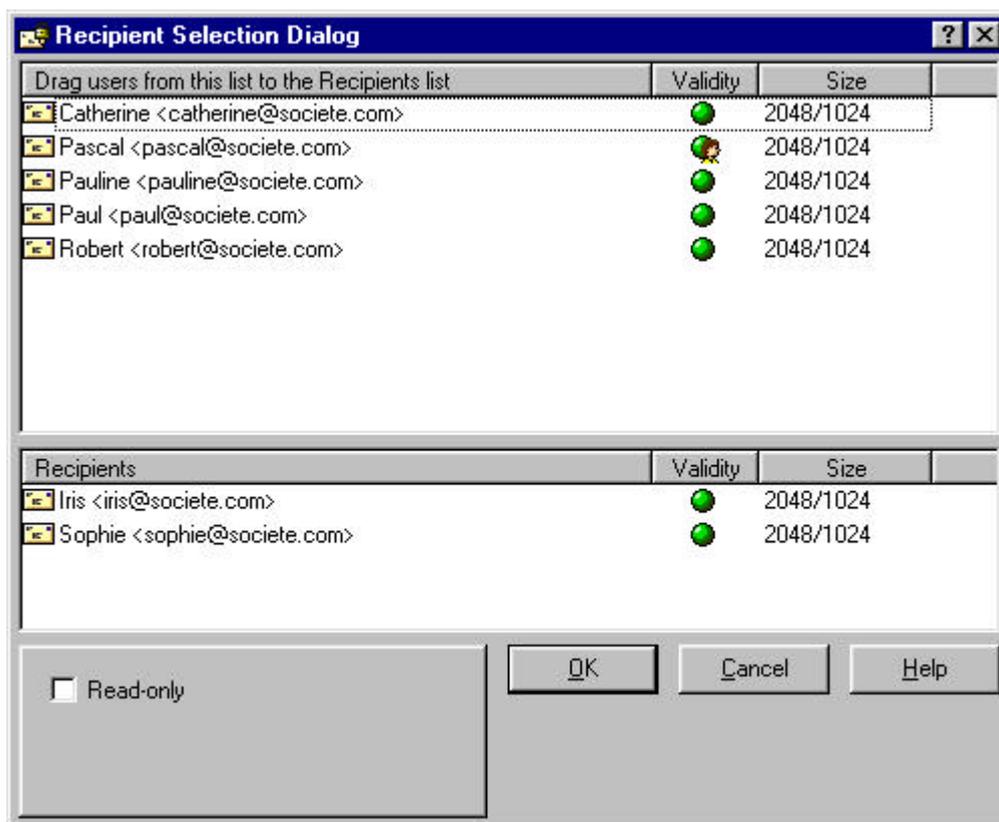


Figure 7-4. PGP Key Selection Dialog

4. Glissez la ou les clés depuis la fenêtre du bas vers celle du haut.
5. Cliquez sur OK.

Ouvrir un volume PGPdisk

Quand vous créez un nouveau volume, PGPdisk l'ouvre automatiquement de manière à ce que vous puissiez commencer à l'utiliser pour stocker vos fichiers. Quand vous êtes prêt à sécuriser le contenu du volume, vous devez le fermer. Une fois qu'un volume est fermé, son contenu demeure verrouillé dans un fichier crypté à l'intérieur duquel il est inaccessible jusqu'à ce que le volume soit ouvert à nouveau.

Il y a cinq façons d'ouvrir un volume.

- Double-cliquer sur l'icône du volume.
- Glisser l'icône du volume sur l'icône PGPdisk dans le répertoire de PGP 6.0.
- Glisser l'icône du volume sur le bouton Mount de la barre d'outils PGPdisk.
- Cliquer avec le bouton droit sur l'icône du volume. Sélectionnez PGPdisk → Mount PGPdisk.
- Utiliser le bouton Mount dans la barre d'outils PGPdisk.

Pour ouvrir un volume avec le bouton Mount

1. Démarrez PGPdisk.

La barre d'outils PGPdisk apparaît.

2. Cliquez sur Mount ou utilisez la commande Mount PGPdisk depuis le menu File.

La boîte de dialogue Mount PGPdisk apparaît.

3. Localisez et sélectionnez le volume crypté que vous voulez ouvrir, puis cliquez sur Open.

Il vous est demandé de saisir la phrase secrète pour le volume sélectionné.

4. Saisissez la phrase secrète et cliquez sur OK. Si vous ne voulez pas modifier les fichiers contenus dans le volume, cochez la case "read-only". Si vous avez saisi la phrase secrète correcte, le volume est ouvert et le contenu du fichier crypté est rendu accessible. Le volume apparaît dans l'Explorateur Windows.

Utiliser un volume PGPdisk ouvert

Vous pouvez créer, copier, déplacer et effacer fichiers et répertoires d'un volume PGPdisk exactement de la même manière que vous le faites avec n'importe quel autre disque. De la même façon, quiconque a accès au volume (que ce soit sur la même machine ou à travers le réseau) peut aussi accéder aux données stockées dans le volume. Ce n'est que lorsque vous fermez le volume que les données contenues dans le fichier crypté associé au volume deviennent inaccessibles.

⚠ AVERTISSEMENT: Bien que le fichier crypté associé à chaque volume soit à l'abri de l'indiscrétion, il peut quand même être effacé. Si une personne non autorisée est capable d'accéder à vos données, elle pourrait éventuellement effacer le fichier crypté qui sert de support au volume. Il est judicieux de conserver une copie de sauvegarde du fichier crypté.

Fermer un volume PGPdisk

Quand vous avez fini d'utiliser un volume donné et que vous voulez en verrouiller le contenu, vous devez fermer le volume. Vous ne pouvez pas fermer un volume dont des fichiers [qui s'y trouvent] sont ouverts.

Pour fermer un volume PGPdisk

1. Fermez tous les fichiers du volume PGPdisk que vous voulez fermer.
2. Sélectionnez Unmount PGPdisk depuis le menu File de PGPdisk.

Voici d'autres manières de fermer un volume PGPdisk:

- Cliquez sur Unmount dans la barre d'outils PGPdisk
- Cliquez avec le bouton droit sur sa lettre de lecteur dans la fenêtre de l'Explorateur
- Cliquez avec le bouton droit sur le fichier de volume

Une fois qu'un volume est fermé, son contenu est verrouillé dans le fichier crypté associé au volume. Le contenu du volume est stocké dans le fichier crypté et demeure inaccessible jusqu'à ce que le volume soit ouvert à nouveau. On peut

considérer le volume PGPdisk [ouvert] comme une sorte de fenêtre par laquelle on voit les données contenues dans le fichier crypté. Le contenu d'un fichier volume PGPdisk ne devient disponible que lorsque le fichier est ouvert en tant que volume par quelqu'un qui connaît la phrase secrète adéquate.

Spécifier les Préférences

Le bouton Preferences de la barre d'outils PGPdisk vous permet de spécifier comment vous préférez fermer et créer vos volumes.

Pour spécifier les Préférences

1. Cliquez sur Preferences dans la barre d'outils PGPdisk ou sélectionnez Preferences depuis le menu File.

La boîte de dialogue Preferences apparaît.

2. Sélectionnez les options désirées en cliquant sur les onglets et les cases appropriées.

Onglet Auto Unmount

- Auto unmount after [15] minutes of inactivity [fermeture automatique après [15] minutes d'inactivité]. Quand cette option est cochée, PGPdisk ferme automatiquement tous les volumes PGPdisk ouverts si votre ordinateur est inactif pendant le nombre de minutes indiqué. Vous pouvez saisir une valeur de 1 à 999 minutes.

NOTE: PGPdisk ne peut pas fermer automatiquement un volume PGPdisk si des fichiers stockés dans ce volume sont ouverts.

- Auto unmount on computer sleep [fermeture automatique si l'ordinateur est en veille]. Quand cette option est cochée, PGPdisk ferme automatiquement tous les volumes PGPdisk ouverts si votre ordinateur est en veille. (Les ordinateurs ne disposent pas tous de la fonction de mise en veille)

L'option Prevent sleep if any PGPdisks could not be unmounted [empêcher la mise en veille si l'un des volumes ne peut pas être fermé] garantit que votre ordinateur ne basculera pas en mode veille si un volume PGPdisk ne peut pas être fermé.

NOTE: Ces deux options (Auto unmount on computer sleep et Prevent sleep if any PGPdisks could not be unmounted) sont désactivées sous NT.

- Enable Unmount HotKey [activer la fermeture par raccourci clavier vous saisissez une combinaison de touches dans cette zone de texte et cochez cette case, vous créez et activez un raccourci clavier qui vous permet de fermer tous les volumes PGPdisk ouverts en appuyant sur une seule touche.

Cliquez sur OK quand vous avez fini de régler vos préférences.

NOTE: Les réglages de fermeture automatique sont commodes si vous devez laisser votre ordinateur sans surveillance pendant un certain temps.

Vous devriez régler les délais en fonction des exigences de sécurité requises pour empêcher un accès non autorisé. Vous pouvez régler tous ces paramètres en même temps.

Entretenir des Volumes PGPdisk

Ce chapitre décrit comment ouvrir automatiquement des volumes PGPdisk au démarrage de votre ordinateur, comment sauvegarder et échanger les données contenues dans ces volumes avec autrui.

Ouvrir des fichiers PGPdisk sur un serveur distant

Vous pouvez placer des volumes PGPdisk sur n'importe quel type de serveur (NT, 95, 98 ou UNIX) et en autoriser l'accès à un client Windows 95.

NOTE: La première personne à ouvrir le volume en local accède au volume en lecture écriture. Personne d'autre ne peut dès lors accéder à ce volume. Si vous voulez que d'autres puissent accéder aux fichiers contenus dans ce volume, vous devez l'ouvrir en mode lecture seule. Tous les utilisateurs de ce volume pourront alors y accéder en lecture seule.

Si le volume se trouve sur un serveur Windows 95, vous pouvez aussi ouvrir le volume à distance sur le serveur et permettre l'accès partagé au volume ouvert. Cependant, la sécurité des fichiers placés dans le volume sera compromise.

Ouverture automatique des volumes PGPdisk

Si vous le souhaitez, vous pouvez ouvrir automatiquement des volumes PGPdisk lorsque vous démarrez votre ordinateur.

Pour ouvrir automatiquement des volumes PGPdisk

1. Créez un raccourci pour chacun des fichiers PGPdisk que vous voulez ouvrir au démarrage de votre ordinateur.
2. Placez le(s) raccourci(s) dans le dossier Démarrage [dont le chemin d'accès varie suivant votre version de Windows].

Une fois que vous avez placé vos raccourcis dans ce dossier, les volumes PGPdisk sont ouverts chaque fois que vous démarrez votre ordinateur. Il vous sera demandé de saisir la phrase secrète pour chaque volume PGPdisk à ouvrir.

Sauvegarder des volumes PGPdisk

Vous pouvez vouloir sauvegarder le contenu de vos volumes PGPdisk afin de le protéger de la corruption ou des accidents. Bien qu'il soit possible de sauvegarder le contenu d'un volume PGPdisk ouvert tout comme vous le feriez avec n'importe quel autre disque, ce ne serait probablement pas très judicieux parce que son

contenu ne serait alors pas crypté et serait donc accessible à quiconque pourrait restaurer la sauvegarde.

Au lieu de sauvegarder le contenu d'un volume PGPdisk ouvert, vous devriez plutôt faire une sauvegarde du volume PGPdisk crypté lui-même.

Pour sauvegarder des volumes PGPdisk

1. Cliquez sur l'icône du volume PGPdisk. Sélectionnez Unmount PGPdisk.
2. Copiez le fichier crypté fermé sur une disquette, une bande ou un support amovible comme vous le feriez pour n'importe quel autre fichier. Même si des personnes non autorisées accédaient à la sauvegarde, elles ne pourraient pas décrypter son contenu.

Echanger des volumes PGPdisk

Vous pouvez échanger des volumes PGPdisk avec des collègues disposant de PGPdisk en leur envoyant une copie du fichier crypté qui contient les données. Voici quelques moyens d'échanger des volumes PGPdisk:

- En attachement de messages e-mail
- Sur des disquettes ou des supports amovibles
- Par réseau

✦ **ASTUCE:** Vous devriez réfléchir soigneusement à la manière de communiquer la phrase secrète permettant d'accéder à un volume PGPdisk. En général, à moins que vous n'utilisiez un programme de cryptage pour protéger votre message, l'e-mail n'est pas un bon moyen d'échanger des phrases secrètes. Les lignes téléphoniques sont également vulnérables à l'interception et votre conversation peut être écoutée. Plus vous prendrez de précautions, mieux vous garantirez la confidentialité de vos informations sensibles. Si vous ne disposez pas d'e-mail sécurisé, il est alors probablement plus sûr de rencontrer la personne concernée et de la lui dire de vive voix ou même de la lui envoyer par courrier postal.

Une fois que les destinataires convenus possèdent la copie du fichier crypté, tout ce dont ils ont besoin pour accéder au contenu du volume est de saisir la bonne phrase secrète ou, si le volume a été crypté avec leur clé publique, leur clé secrète. Ils ont aussi besoin d'une copie du programme PGPdisk. Pour plus d'informations sur la manière d'ouvrir un volume PGPdisk, voir: "[Ouvrir un volume PGPdisk](#)" en page 109.

Changer la taille d'un volume PGPdisk

Bien que vous ne puissiez pas changer la taille d'un volume PGPdisk une fois qu'il a été créé, vous pouvez toutefois créer un [autre] volume, plus petit ou plus grand, puis copier le contenu de l'ancien vers le nouveau.

Pour changer la taille d'un volume PGPdisk

1. Créez un nouveau volume PGPdisk et spécifiez la taille désirée.
2. Copiez le contenu du volume PGPdisk ouvert existant dans le volume nouvellement créé.
3. Fermez l'ancien volume PGPdisk puis effacez le fichier crypté associé pour libérer de l'espace disque.

Détails Techniques et Réflexions sur la Sécurité

Ce chapitre examine les questions relatives au cryptage et à la sécurité et fournit aux utilisateurs astuces et informations techniques à propos de PGPdisk.

A propos des volumes PGPdisk

Vous pouvez utiliser des volumes PGPdisk pour organiser votre travail, conserver en des endroits séparés des fichiers portant le même nom ou plusieurs versions des mêmes documents.

Bien que les volumes que vous créez avec PGPdisk fonctionnent exactement de la même façon que les disques avec lesquels vous avez l'habitude de travailler, les données sont en réalité conservées dans un grand fichier crypté. C'est seulement lorsque vous ouvrez le fichier que son contenu se présente sous la forme d'un volume. Il est important de comprendre que toutes vos données demeurent sécurisées dans le fichier crypté et ne sont décryptées que lorsque vous accédez à l'un de ces fichiers. Conserver ainsi les données facilite la manipulation et l'échange de volumes PGPdisk mais facilite aussi la perte de ces données si le fichier lui-même était effacé. Il est prudent de conserver une copie de sauvegarde de ces fichiers cryptés de sorte que les données puissent être récupérées au cas où quelque chose arriverait à l'original. Il est important aussi de noter que vous ne pouvez pas compresser un fichier crypté pour essayer de réduire sa taille, mais vous pouvez compresser les fichiers individuels contenus dans le volume ouvert et donc y entreposer davantage de données cryptées. Vous pouvez aussi stocker des volumes PGPdisk les uns dans les autres à la manière de poupées gigognes pour une plus grande sécurité.

L'algorithme de chiffrement de PGPdisk

Le chiffrement a recours à une formule mathématique pour brouiller vos données de sorte que personne d'autre ne puisse les utiliser. Quand vous appliquez la bonne clé mathématique, vos données redeviennent intelligibles. La formule de chiffrement de PGPdisk utilise des données aléatoires pour une partie du processus de chiffrement. Quelques-unes proviennent des mouvements de votre souris pendant le chiffrement et d'autres proviennent aussi directement de votre phrase secrète.

Le processus de chiffrement de PGPdisk est une formule mathématique complexe qui, pour autant que nous le sachions, est actuellement incassable. Quelqu'un pourrait trouver un moyen de casser cette formule dans l'avenir, mais les

informations sensibles ne le sont en général que pour un temps limité. PGPdisk utilise un algorithme de chiffrement sophistiqué dénommé CAST, considéré comme un excellent chiffre par blocs parce qu'il est rapide et incassable – pour autant qu'on sache. Son nom est tiré des initiales de ses concepteurs Carlisle Adams et Stafford Tavares de Northern Telecom (Nortel). Nortel a déposé un brevet pour CAST, mais ils ont ajouté une disposition pour rendre CAST disponible à tous sans avoir à payer de royalties. CAST apparaît comme étant exceptionnellement bien conçu, par des gens jouissant d'excellentes réputations dans ce domaine. La conception est fondée sur une approche très formelle, avec un nombre d'assertions formellement démontrables qui donnent de bonnes raisons de penser qu'il exige une recherche exhaustive des clés pour casser sa clé de 128 bits. CAST n'a pas de clés faibles. Il existe de solides arguments permettant de penser que CAST est complètement immunisé aussi bien contre la cryptanalyse linéaire que différentielle, les deux formes de cryptanalyse les plus puissantes dans la recherche publique, toutes deux ayant été utilisées pour craquer le Data Encryption Standard (DES).

Qualité de la Phrase Secrète

Votre sécurité est seulement aussi bonne que votre phrase secrète. Cependant, crypter un fichier que l'on est ensuite incapable de décrypter constitue une douloureuse expérience dans l'apprentissage du choix d'une phrase secrète dont vous vous rappellerez.

La plupart des applications requièrent un mot de passe de trois à huit lettres. Un simple mot de passe est vulnérable à une attaque par dictionnaire, qui consiste à faire essayer à un ordinateur tous les mots du dictionnaire jusqu'à ce qu'il trouve votre mot de passe. Pour se protéger contre cette sorte d'attaque, il est généralement recommandé de créer un mot composé d'une combinaison de lettres alphabétiques majuscules et minuscules, de nombres, de signes de ponctuation et d'espaces. Cela donne un mot de passe plus résistant, mais un mot de passe obscur que vous ne retiendrez probablement pas facilement. Nous ne vous recommandons pas d'utiliser un mot de passe d'un seul mot.

Une phrase secrète est moins vulnérable à une attaque par dictionnaire. Cela est réalisé facilement en utilisant de multiples mots dans votre phrase, plutôt qu'en essayant de contrer une attaque par dictionnaire en insérant arbitrairement beaucoup d'amusants caractères non alphabétiques, ce qui a pour effet de rendre votre phrase secrète trop facile à oublier et pourrait conduire à une désastreuse perte d'informations parce que vous ne pouvez plus décrypter vos propres fichiers. Toutefois, à moins que la phrase secrète que vous choisissez ne soit quelque chose de facile à apprendre par cœur pour longtemps, vous avez peu de chance de vous la rappeler mot pour mot. Choisir une phrase sous l'inspiration du moment va déboucher sur son oubli total. Choisissez quelque chose qui réside déjà dans votre mémoire. Ce ne devrait pas être quelque chose que vous avez répété à d'autres récemment, ni une citation célèbre, parce que vous voulez qu'elle soit difficile à deviner pour un attaquant sophistiqué. Si elle est déjà profondément gravée dans votre mémoire, vous ne l'oublierez probablement pas. Ne l'écrivez pas!

Votre phrase secrète fait partie des données aléatoires utilisées pour crypter vos fichiers PGPdisk. La barre de progression Passphrase Quality devrait être au moins à moitié pleine lorsque vous saisissez votre phrase secrète. Vous n'obtiendrez la sécurité maximum que lorsque la barre sera complètement pleine.

Vous pouvez créer des phrases secrètes principales ou auxiliaires différentes pour chacun des volumes PGPdisk que vous créez. Cela vous permet d'individualiser l'accès d'autres utilisateurs aux fichiers PGPdisk volume par volume. Vous pouvez utiliser une phrase secrète donnée pour les fichiers PGPdisk que vous envoyez à un collègue, tout en empêchant celui-ci d'accéder à vos autres fichiers PGPdisk.

Précautions Spéciales de Sécurité prises par PGPdisk

A la différence d'autres programmes, PGPdisk apporte un soin particulier à remédier à certains problèmes de sécurité. Ceux-ci incluent ce qui suit:

Effacement de la phrase secrète

Quand vous saisissez une phrase secrète, PGPdisk ne l'utilise que pour un temps très bref, puis l'efface de la mémoire. PGPdisk évite également de faire des copies de la phrase secrète. Il en résulte que votre phrase secrète ne reste en mémoire que pendant une fraction de seconde. Ce dispositif est essentiel – si la phrase secrète restait en mémoire, quelqu'un pourrait l'y récupérer si vous vous éloigniez de votre ordinateur. A votre insu, on pourrait alors accéder à n'importe quel volume PGPdisk protégé par cette phrase secrète.

Protection relative à la mémoire virtuelle

Votre phrase secrète ou d'autres clés pourraient être écrites sur le disque dur par le biais du fichier d'échange de la mémoire virtuelle. PGPdisk veille à ce que les phrases secrètes et les clés ne soient jamais écrites sur le disque. Ce dispositif est important parce que quelqu'un pourrait examiner le fichier de mémoire virtuelle à la recherche de phrases secrètes.

Protection contre la rémanence électrostatique en mémoire vive

Quand vous ouvrez un PGPdisk, votre phrase secrète est transformée en clé. Cette clé est utilisée pour crypter et décrypter les données dans votre volume PGPdisk. Tandis que la phrase secrète est immédiatement effacée de la mémoire, la clé (de laquelle votre phrase secrète ne peut pas être dérivée) y demeure pendant que le disque est ouvert. Cette clé est certes protégée de la mémoire virtuelle; cependant, si une certaine zone de la mémoire [vive] stocke exactement les mêmes données pendant de très longues périodes sans être éteinte ou réinitialisée, cette mémoire tend à conserver une charge statique, qui pourrait être lue par des attaquants. Si votre PGPdisk reste ouvert pendant de longues périodes, avec le temps, des traces discernables de votre clé pourraient demeurer en mémoire. Vous ne trouverez certes pas de tels outils [de récupération] au magasin d'électronique à côté de chez vous, mais les grands Etats sont susceptibles d'en posséder.

PGPdisk se protège de ça en conservant deux copies de la clé en RAM, une copie normale et une copie bit inversé, et en intervertissant fréquemment les copies.

Autres réflexions à propos de la sécurité

En général, votre capacité à protéger vos données dépend des précautions que vous prenez, et aucun programme de cryptage ne peut vous protéger de négligences dans les habitudes de sécurité. Par exemple, si vous quittez votre bureau en laissant accessible votre ordinateur contenant des fichiers sensibles, n'importe qui peut accéder à ces informations ou même obtenir la clé utilisée pour accéder aux données. Voici quelques conseils pour maintenir une sécurité optimale:

- Veillez à fermer les volumes PGPdisk quand vous quittez votre ordinateur. De cette manière, leur contenu demeurera en sécurité dans le fichier crypté associé au volume jusqu'à ce que vous vouliez y accéder à nouveau.
- Utilisez un économiseur d'écran muni d'un mot de passe de sorte qu'il soit plus difficile à quelqu'un d'accéder à votre ordinateur ou de voir votre écran quand vous vous éloignez de votre bureau.
- Veillez à ce que vos volumes PGPdisk ne puissent pas être vus par d'autres ordinateurs sur le réseau. Pour cela, vous pourriez avoir besoin d'en parler aux administrateurs de votre réseau. Les fichiers contenus dans un volume PGPdisk ouvert peuvent être consultés par quiconque peut le voir sur le réseau.
- N'écrivez jamais vos phrases secrètes. Sélectionnez quelque chose dont vous pouvez vous rappeler. Si vous avez du mal à vous rappeler de votre phrase secrète, utilisez quelque chose qui se grave facilement en mémoire, comme un slogan, une chanson, un poème, une blague, mais n'écrivez pas vos phrases secrètes.
- Si vous utilisez PGPdisk à la maison et partagez votre ordinateur avec d'autres personnes, elles seront probablement en mesure de voir vos fichiers PGPdisk. Aussi longtemps que vous fermez les volumes PGPdisk quand vous avez fini de les utiliser, personne d'autre ne sera capable d'en lire le contenu.
- Si un autre utilisateur peut accéder à votre ordinateur, il peut effacer vos fichiers PGPdisk aussi bien que n'importe quels autres fichiers ou volumes. Si le contrôle de l'accès physique est une solution envisageable, essayez de mettre ou de conserver vos fichiers PGPdisk sur un support externe sur lequel vous avez un contrôle physique exclusif.
- Ne perdez pas de vue que les copies de votre volume PGPdisk utilisent la même clé secrète que l'original. Si vous donnez une copie de votre volume à quelqu'un et changez tous les deux vos phrases secrètes principales, vous utilisez toujours la même clé pour crypter les données. Bien qu'une récupération de la clé par ce biais ne soit pas à la portée du premier venu, elle n'est pas impossible.

Dysfonctionnements de PGP

A

Ce chapitre présente des informations sur les problèmes éventuels et suggère des solutions.

Erreur	Cause	Solution
Authentication rejected by remote SKEP connection	L'utilisateur distant de la connexion pour fichier partagé par réseau a rejeté la clé que vous avez donnée pour authentification.	Utilisez une clé différente pour authentifier la connexion pour fichier partagé, ou contactez l'utilisateur distant pour l'assurer que la clé que vous utilisez est valide.
Cannot perform the requested operation because the output buffer is too small.	Le fichier de sortie est plus grand que ce que peuvent contenir les tampons.	Si vous cryptez ou signez, vous pouvez être obligé de découper le message et crypter/signer de plus petits morceaux à la fois. Si vous décryptez ou vérifiez, demandez à l'expéditeur de crypter/signer de plus petits morceaux et de vous les renvoyer.
Could not encrypt to specified key because it is a sign-only key.	La clé sélectionnée ne peut être utilisée que pour signer.	Choisissez une clé différente, ou générez une nouvelle clé qui puisse crypter les données.
Could not sign with specified key because it is an encrypt-only key.	La clé sélectionnée ne peut être utilisée que pour crypter.	Choisissez une clé différente, ou générez une nouvelle clé qui puisse signer les données.
Error in domain name systemic	L'adresse de destination que vous avez donnée est incorrecte, ou votre connexion au réseau est mal configurée.	Vérifiez et assurez-vous que l'adresse de destination que vous avez donnée est la bonne. Si vous en êtes certain, vérifiez votre connexion au réseau.
Identical shares cannot be combined	Vous avez tenté de combiner les mêmes segments deux fois.	Si vous avez reçu les segments d'un fichier partagé, essayez de choisir un autre fichier partagé. Si vous avez reçu les segments du réseau, vous pouvez avoir besoin de contacter l'utilisateur distant et lui dire d'envoyer un jeu différent de segments.
No secret keys could be found on your keyring.	Il n'y a pas de clés privées dans votre trousseau de clés.	Générez votre propre paire de clés dans PGPkeys.
Socket is not connected	La connexion réseau au PGP Cert Server ou au réseau de fichier partagé a été rompue.	Essayez de rétablir la connexion en répétant la procédure que vous avez utilisée pour commencer la connexion. Si cela échoue, vérifiez votre connexion au réseau.

Erreur	Cause	Solution
The action could not be completed due to an invalid file operation.	Le programme n'a pas pu lire ou écrire des données dans un certain fichier.	Le fichier est probablement corrompu. Essayez de modifier vos PGP Preferences pour utiliser un fichier différent, si c'est possible.
The evaluation time for PGP encrypting and signing has passed. Operation aborted.	La période d'évaluation du produit a expiré.	Téléchargez la version freeware ou achetez la version commerciale du produit.
The keyring contains a bad (corrupted) PGP packet.	Le message PGP avec lequel vous travaillez a été corrompu, ou votre trousseau de clés a été corrompu.	Demandez à l'expéditeur de renvoyer le message si c'est avec un message que vous travaillez. Si c'est votre trousseau de clés, essayez de le restaurer depuis votre trousseau de sauvegarde.
The keyring file is corrupt.	Le programme n'a pas pu lire ou écrire des données dans un certain fichier.	Il y a probablement un fichier qui est corrompu ou manquant. Ce peut être ou non le trousseau de clés. Essayez d'utiliser un nom de fichier ou un chemin différent, si c'est possible.
The message/data contains a detached signature.	La signature pour le message/fichier est située dans un fichier séparé.	Double-cliquez d'abord sur le fichier de signature séparée.
The passphrase you entered does not match the passphrase on the key.	La phrase secrète que vous avez saisie n'est pas correcte.	Vous avez peut-être activé CAPS LOCK, ou peut-être simplement mal tapé la phrase secrète. Essayez à nouveau.
The PGP library has run out of memory.	Le système d'exploitation est à court de mémoire.	Fermez les autres programmes ouverts. Si cela ne marche pas, vous pouvez avoir besoin de davantage de mémoire dans votre machine.
The specified user ID was not added because it already exists on the selected key.	Vous ne pouvez pas ajouter un ID d'utilisateur à une clé s'il y en a déjà un identique sur la clé.	Essayez d'ajouter un ID d'utilisateur différent, ou effacez d'abord l'ID correspondant.
The specified key could not be found on your keyring.	La clé nécessaire pour décrypter le message actuel n'est pas dans votre trousseau de clés.	Demandez à l'expéditeur du message de renvoyer le message et assurez-vous qu'il crypte le message pour votre clé publique.
The specified input file does not exist.	Le nom de fichier saisi n'existe pas.	Parcourez [vos fichiers] pour trouver le nom exact et le chemin du fichier que vous voulez.
There is not enough random data currently available.	Le générateur pseudo aléatoire a besoin de davantage de données afin de générer de bons nombres aléatoires.	Quand cela vous est demandé, bougez la souris, ou pressez des touches au hasard, afin de générer des données.

Erreur	Cause	Solution
There was an error during the writing of the keyring or the exported file.	Le programme n'a pas pu écrire des données dans un certain fichier.	Votre disque dur est peut-être plein, ou si le fichier est sur une disquette, la disquette n'est pas présente dans le lecteur de disquette.
There was an error opening or writing the keyring or the output file.	Un fichier qui est nécessaire n'a pas pu être ouvert.	Assurez-vous que les réglages des PGP Preferences sont corrects. Si vous avez effacé récemment des fichiers dans le répertoire où vous avez installé PGP, vous avez peut-être besoin de réinstaller le produit.
This key is already signed by the specified signing key.	Vous ne pouvez pas signer une clé que vous avez déjà signée.	Vous avez peut-être choisi la mauvaise clé. Dans ce cas, choisissez une clé à signer différente.
Unable to perform operation because this file is read-only or otherwise protected. If you store your keyring files on removable media the media may not be inserted.	Un fichier qui est nécessaire est configuré en lecture seule ou est actuellement utilisé par un autre programme.	Fermez les autres programmes qui peuvent accéder aux mêmes fichiers que le programme que vous utilisez. Si vous gardez vos fichiers de trousseau de clés sur une disquette, assurez-vous que la disquette est dans le lecteur de disquette.

Echanger des Fichiers entre Mac et Windows

B

Echanger des fichiers avec MacOS est un problème classique qu'on retrouve dans quasiment tout type de logiciel d'échange de données, tels que les applications de messagerie, FTP, utilitaires de compression, et PGP. Cet appendice est destiné à expliquer comment la version 6.0 de PGP corrige ce problème de manière définitive, et détaille la compatibilité avec les anciennes versions de PGP.

MacOS conserve les fichiers différemment des autres plates-formes. Même le format de texte est différent sous MacOS. Sous ce système, les fichiers sont tous en réalité deux fichiers distincts, le premier constituant le segment de données et le second le segment de ressources. Pour pouvoir déplacer un fichier de MacOS vers Windows sans perte de données, les deux segments doivent être assemblés pour ne plus en former qu'un seul. La méthode classique par laquelle un fichier MacOS est converti en un seul fichier de telle sorte qu'il puisse être transmis à un autre Macintosh ou PC sans perdre aucune de ses parties est appelé MacBinary.

Le problème est que, sans logiciel spécialement adapté, Windows et les autres plates-formes ne peuvent pas comprendre le format MacBinary. S'il arrive lors de la réception d'un fichier MacBinary que la conversion échoue à le transformer en fichier Windows, le fichier obtenu est inutilisable. Des utilitaires Windows existent pour convertir le fichier et le rendre utilisable sous Windows, mais ils sont peu adaptés.

Les versions précédentes de PGP et la plupart des utilitaires présents sur le marché ont tendance à ignorer ce problème autant que possible et laissent toutes les décisions à la charge de l'utilisateur, qui doit décider si le fichier doit être converti sous MacBinary ou non avant de l'envoyer vers une plate-forme MacOS. Ainsi, le choix d'envoyer le fichier avec MacBinary, sans perte de données, ou sans, en espérant que peu de données importantes seront perdues, dépend de l'utilisateur, qui bien souvent ne sait pas quelle est la bonne décision. Celle-ci dépend en fait de la destination du fichier: Windows ou MacOS. Mais comment faire lorsque vous voudrez l'envoyer vers les deux plates-formes en même temps? Il n'y a aucune solution envisageable à ce problème avec les anciennes versions de PGP et de nombreux autres utilitaires. Pour les utilisateurs, il n'en est résulté que confusion et incommodité.

L'inverse, envoyer un fichier de Windows vers MacOS, a aussi été un problème majeur. Windows utilise les extensions des noms de fichiers, comme .doc, pour identifier le type de fichier. Ceci n'a aucun sens sous MacOS [car le système conserve de manière invisible le type de chaque fichier, et de son créateur, et gère automatiquement l'ouverture des fichiers]. Les fichiers se retrouvent donc envoyés de Windows à MacOS sans aucun type, car le fichier reçu n'en dispose pas. Pour rendre le fichier utilisable sous MacOS, il faut alors effectuer des opérations obscures lors de l'ouverture du fichier, et dans la plupart des cas il faudra attribuer un code créateur et de type de fichier, ce qui est hors de portée de l'utilisateur qui ne dispose pas de cette connaissance et de l'utilitaire indispensable pour le faire.

Heureusement, les dernières versions de PGP (versions 5.5 et 6.0) résolvent ces problèmes. Si tous les utilisateurs migrent vers ces dernières versions, plus personne n'aura à se soucier de l'envoi de fichiers d'une plate-forme vers l'autre, quel qu'en soit le sens.

Transmettre de MacOS vers Windows

Sous MacOS, il y a trois options lors du cryptage ou de la signature d'un fichier:

- **MacBinary: Yes.** C'est l'option recommandée pour tous les cryptages à l'intention d'un destinataire utilisateur de PGP 5.5 ou ultérieure sur toute plate-forme. Ceci signifie que les utilisateurs de MacOS recevront le fichier correctement, tandis que les utilisateurs de Windows recevront et décodent le fichier, qui recevra automatiquement son extension, comme .doc pour les fichiers Microsoft Word ou .ppt pour Microsoft PowerPoint. PGP dispose d'une information étendue sur les extensions de fichiers et les codes créateurs qui correspondent sous MacOS. Au cas où le fichier serait d'un type inconnu de PGP ou si le fichier est un fichier qui ne peut être utilisé que sous MacOS, comme une application MacOS, le fichier sera conservé sous la forme MacBinary pour qu'il puisse être transmis à un Macintosh sans aucune perte d'information [décrypter un fichier spécifique au Macintosh, comme une application, provoquera la perte du segment de ressources sous Windows, or ce segment contient le code même de l'application, et ceci détruit le fichier qui ne pourra plus être utilisé sous MacOS].
- **MacBinary: No.** Si vous communiquez avec des utilisateurs qui ne disposent que d'anciennes versions de PGP, la décision finale quant à l'utilisation de MacBinary dépendra uniquement de l'expéditeur, qui devra le spécifier à chaque fois, que ce soit sous PGP ou sous la plupart des programmes plus anciens. Lorsque vous envoyez un fichier à un autre PC avec une ancienne version, si vous savez que le fichier peut être lu par Windows sans avoir besoin de MacBinary, sélectionnez cette option. Ceci devrait correspondre à la plupart des fichiers qui sont multi plates-formes comme ceux créés par les applications Microsoft Office, les fichiers graphiques, les fichiers compressés, et beaucoup d'autres. Une fois le fichier reçu par votre destinataire, il devra le renommer manuellement pour obtenir l'extension correcte sous Windows. C'est nécessaire car le destinataire Windows ne dispose pas de l'information type/créateur normalement intégrée par l'utilisation de MacBinary.
- **MacBinary: Smart.** Dans certains cas cette option sera utile lorsque vous communiquerez avec des utilisateurs de versions antérieures de PGP. Cette option décidera de l'utilisation de MacBinary en fonction du type de fichier et des données qu'il contient. Si le fichier est d'un type figurant dans la liste, MacBinary ne sera pas utilisé, ce qui fait qu'il sera lisible sur tout PC disposant de n'importe quelle version de PGP:
 - fichier compressé PKzip
 - fichier compressé Lempel-Ziv
 - fichier au format MIDI music
 - fichier compressé PackIt

- fichier graphique sous GIF
- fichier compressé par StuffIt (format de compression Macintosh)
- fichier compressé par Compactor
- fichier compressé par Arc
- fichier graphique JPEG

Comme vous le voyez, seul un nombre limité de fichiers seront lisibles par les anciennes versions de PGP sur d'autres plates-formes, lorsque l'option Smart est sélectionnée. Tout autre type de fichier reçu par une ancienne version de PGP sera illisible sans l'exploitation des données codées avec MacBinary, ce qui imposera l'utilisation d'un utilitaire. D'autre part, le fichier n'aura pas sur PC son extension correcte, à moins que cette extension ne soit manuellement ajoutée par le destinataire du fichier. Lors de l'utilisation du Smart Mode, le fichier résultant pourrait ne pas correspondre à l'original lorsqu'il sera reçu sous Macintosh, car le code du créateur et du type de fichier seront perdus. Ce mode a été conservé uniquement parce qu'il était présent dans la version 5.0 de PGP et que des utilisateurs pourraient n'avoir besoin d'envoyer que des fichiers de ce type. Cette option est déconseillée dans la plupart des cas.

En résumé, si vos destinataires disposent des versions 6.0 et ultérieures de PGP, sélectionnez toujours MacBinary: Yes (par défaut). Ainsi, dans ce cas, vous n'avez plus à vous soucier de problèmes de transmission de fichiers. Lors de l'envoi vers des utilisateurs d'anciennes versions de PGP, vous devriez sélectionner MacBinary: No, pour les fichiers multi plate-forme et MacBinary: Yes pour les fichiers qui sont uniquement lisibles sous MacOS.

-
- **NOTE:** PGP version 5.0 ne dispose pas d'une option MacBinary: No. Pour pouvoir envoyer des fichiers sans MacBinary, le fichier doit recevoir un type créateur/type de la liste ci-dessus avant d'être envoyé.
-

Recevoir des fichiers Windows sous MacOS

Lors du décryptage, PGP version 6.0 essaye de traduire automatiquement le type du fichier, en lui donnant une extension qui correspond au type de fichier sous MacOS. Par exemple, si un utilisateur Mac reçoit de Windows un fichier avec une extension .doc, le fichier sera enregistré sous la forme d'un document Microsoft Word [de manière invisible, le fichier reçoit un code créateur "MSWD" et un type de fichier "W6BN", et le Finder de MacOS lui donne l'icône qui correspond au fichier, et tout double-clic ouvre automatiquement le fichier par Microsoft Word, ou s'il n'est pas présent, par une application capable de le faire]. La même liste d'applications utilisées quand on ajoute l'extension au nom de fichier à réception d'un fichier MacBinary sous Windows est utilisée pour l'opération inverse en équivalent MacOS lorsqu'il est reçu sur Macintosh. Dans la plupart des cas, les fichiers obtenus sont directement utilisables par double-clic sous MacOS.

Les versions précédentes de PGP pour MacOS ne disposent pas de cette fonction. L'utilisateur devra déterminer manuellement le type de fichier; ainsi un fichier "rapport.doc" sera un fichier Microsoft Word, etc. Après avoir déterminé le type de fichier, il pourra être ouvert à partir du dialogue d'ouverture de l'application

correspondante, en sélectionnant “Voir Tout Type” dans le menu pop-up du dialogue d’ouverture. Beaucoup d’applications disposent de cette fonction, mais pas toutes. Certaines applications refuseront ainsi d’ouvrir un fichier qu’elles ne reconnaissent pas, et l’utilisateur devra manuellement attribuer le bon couple créateur/type au fichier, avant de pouvoir ouvrir le fichier, ce qui requiert un utilitaire, dont la plupart sont gratuits. Evoluer vers la version 6.0 de PGP est dans ce cas la solution la plus simple, puisqu’elle élimine ce problème.

Applications reconnues

Voici la liste des applications dont les documents sont reconnus par PGP 6.0 et automatiquement traduits lors d’un envoi de Windows vers MacOS et vice-versa. A ce jour, il n’y a pas moyen de la modifier, cependant, nous pensons intégrer prochainement une option qui permettra à l’utilisateur d’ajouter des types supplémentaires.

- PhotoShop (GIF, documents Photoshop natifs, TGA, JPEG)
- PageMaker (Versions 3.X, 4.X, 5.X, 6.X)
- Microsoft Project (fichiers de projet et de modèle)
- FileMaker Pro
- Adobe Acrobat
- Lotus 123
- Microsoft Word (documents, RTF et modèles)
- PGP
- Microsoft PowerPoint
- StuffIt
- QuickTime
- Corel WordPerfect
- Microsoft Excel (de nombreux types de fichier)
- Quark XPress

Les extensions de fichiers suivantes sont aussi reconnues et automatiquement converties (dans les deux sens):

.cvs	.arj	.ima	.eps	.mac	.cgm
.dl	.fli	.ico	.iff	.img	.lbm
.msp	.pac	.pbm	.pcs	.pcx	.pgm
.plt	.pm	.ppm	.rif	.rle	.shp
.spc	.sr	.sun	.sup	.wmf	.flc
.gz	.vga	.hal	.lzh	.Z	.exe
.mpg	.dvi	.tex	.aif	.zip	.au
.mod	.svx	.wav	.tar	.pct	.pic
.pit	.txt	.mdi	.pak	.tif	.eps

Ce chapitre contient une introduction et des informations de référence à propos de la cryptographie et de PGP, écrites par Phil Zimmermann.

Pourquoi j'ai écrit PGP

“Quoi que vous ferez, ce sera insignifiant, mais il est très important que vous le fassiez.” – Mahatma Gandhi

[*“Whatever you do will be insignificant, but it is very important that you do it.”* – Mahatma Gandhi.]

C'est personnel. C'est privé. Et cela ne regarde personne d'autre que vous. Vous pouvez être en train de préparer une campagne électorale, de discuter de vos impôts, ou d'avoir une romance secrète. Ou vous pouvez être en train de communiquer avec un dissident politique dans un pays répressif. Quoiqu'il en soit, vous ne voulez pas que votre courrier électronique (e-mail) ou vos documents confidentiels soient lus par quelqu'un d'autre. Il n'y a rien de mal à défendre votre intimité. L'intimité est aussi fondamentale que la Constitution.

Le droit à la vie privée est disséminé implicitement tout au long de la Déclaration des Droits. Mais quand la Constitution des Etats-Unis a été élaborée, les Pères Fondateurs ne virent aucun besoin d'explicitement le droit à une conversation privée. Cela aurait été ridicule. Il y a deux siècles, toutes les conversations étaient privées. Si quelqu'un d'autre était en train d'écouter, vous pouviez aller tout simplement derrière la grange et y tenir une conversation. Personne ne pouvait vous écouter sans que vous le sachiez. Le droit à une conversation privée était un droit naturel, non pas seulement au sens philosophique, mais au sens des lois de la physique, étant donnée la technologie de l'époque.

Mais avec l'arrivée de l'âge de l'information, commençant avec l'invention du téléphone, tout cela a changé. Maintenant, la plupart de nos conversations sont acheminées électroniquement. Cela permet à nos conversations les plus intimes d'être divulguées sans que nous le sachions. Les appels des téléphones cellulaires peuvent être enregistrés par quiconque possède une radio. Le courrier électronique, envoyé à travers Internet, n'est pas plus sûr que les appels de téléphone cellulaire. L'e-mail est en train de remplacer rapidement le courrier classique, devenant la norme pour tout le monde, et non plus la nouveauté qu'il était par le passé. Et l'e-mail peut être systématiquement et automatiquement fouillé à la recherche de mots clés, sur une grande échelle, sans que cela soit détecté. C'est comme la pêche aux filets dérivants.

Peut-être pensez-vous que le courrier électronique que vous recevez est assez légitime pour que le chiffrement ne se justifie pas. Si vous êtes vraiment un citoyen au-dessus de tout soupçon, pourquoi n'envoyez-vous pas toujours votre correspondance papier sur des cartes postales? Pourquoi ne vous soumettez-vous pas aux tests de consommation de drogue sur simple demande? Pourquoi exigez-vous un mandat de perquisition pour laisser la police fouiller votre maison? Essayez-vous de cacher quelque chose? Si vous cachez votre courrier dans des

enveloppes, cela signifie-t-il que vous êtes un [élément] subversif ou un trafiquant de drogue, ou peut-être un paranoïaque aigu? Est-ce que les citoyens honnêtes ont un quelconque besoin de chiffrer leurs e-mails?

Que se passerait-il si tout le monde estimait que les citoyens honnêtes devraient utiliser des cartes postales pour leur courrier? Si un non-conformiste s'avisait alors d'imposer le respect de son intimité en utilisant une enveloppe, cela attirerait la suspicion. Peut-être que les autorités ouvriraient son courrier pour voir ce que cette personne cache. Heureusement, nous ne vivons pas dans ce genre de société car chacun protège la plupart de son courrier avec des enveloppes. Aussi personne n'attire la suspicion en protégeant son intimité avec une enveloppe. La sécurité vient du nombre. De la même manière, ce serait excellent si tout le monde utilisait la cryptographie de manière systématique pour tous ses e-mails, qu'ils soient innocents ou non, de telle sorte que personne n'attirerait la suspicion en protégeant la confidentialité de ses e-mails par la cryptographie. Voyez cela comme une forme de solidarité.

Jusqu'à aujourd'hui, si le Gouvernement désirait violer l'intimité de citoyens ordinaires, il devait consentir une certaine dépense d'argent et de travail pour intercepter, ouvrir et lire les lettres. Ou il devait écouter et si possible transcrire le contenu des conversations téléphoniques, du moins avant que la technologie de la reconnaissance vocale automatique soit disponible. Cette méthode, coûteuse en travail, n'était pas praticable sur une grande échelle. Cela était fait seulement dans les cas importants, quand cela en valait la peine.

En 1991 aux Etats-Unis, le projet de loi 266 du Sénat, un texte anti criminalité, comportait une disposition troublante cachée à l'intérieur du texte. Si cette résolution était devenue une véritable loi, cela aurait contraint les fabricants d'équipements de communications sécurisées à insérer des "portes dérobées" spéciales dans leurs produits, de telle sorte que le gouvernement puisse lire les messages chiffrés par n'importe qui. Le texte disait: "La recommandation du Sénat est que les fournisseurs de services de communications électroniques et les fabricants d'équipements de communication électronique devront s'assurer que les systèmes de communication permettent au gouvernement d'obtenir le contenu en clair des communications vocales, des données, et des autres communications dans les cas prévus par la loi". Ce fut cette loi qui me conduisit à publier PGP gratuitement sous forme électronique cette année-là, peu de temps avant que la mesure ne soit retirée après de vigoureuses protestations des groupes de défense des libertés civiles et des groupes industriels.

Le "Digital Telephony bill" de 1994 a fait obligation aux compagnies de téléphone d'installer des dispositifs d'interception à distance dans leurs commutateurs centraux, créant une nouvelle infrastructure technologique pour cette interception "pointer et cliquer", de telle sorte que les agents fédéraux n'aient plus à sortir et attacher des pinces crocodiles sur les lignes de téléphone. Maintenant, ils auront la possibilité de rester assis dans leur quartier général à Washington et d'écouter vos appels téléphoniques. Bien sûr, les lois requièrent encore une réquisition judiciaire pour une interception. Mais alors que les infrastructures techniques peuvent durer des générations, les lois et politiques changent du jour au lendemain. Une fois que l'infrastructure des communications est optimisée pour la surveillance, une modification dans les conditions politiques peut conduire à abuser de ce pouvoir fondé sur de nouvelles bases. Les conditions politiques peuvent se modifier avec l'élection d'un nouveau gouvernement, ou

peut-être même encore plus brusquement après l'attentat à la bombe contre un immeuble fédéral.

Un an après que le "Digital Telephony bill" de 1994 soit passé, le FBI dévoila des plans pour exiger des compagnies de téléphone d'intégrer dans leurs infrastructures la capacité d'intercepter simultanément 1 % de tous les appels téléphoniques dans toutes les grandes villes américaines. Cela représentait une multiplication par plus de mille du nombre d'appels qui peuvent être interceptés. Dans les années précédentes, il y avait eu seulement à peu près un millier de réquisitions d'interceptions judiciaires par an aux Etats-Unis, à la fois au niveau fédéral, au niveau des Etats et au niveau local. Il est difficile de savoir comment le gouvernement pourrait ne serait-ce qu'employer assez de juges pour signer assez d'ordres d'interception pour intercepter 1 % de tous les appels téléphoniques, encore moins embaucher assez d'agents fédéraux pour s'asseoir et écouter tout ce trafic en temps réel. La seule façon plausible de traiter toute cette quantité de trafic est une application massivement Orwellienne de la technologie de reconnaissance vocale pour passer au crible tout cela, à la recherche de mots clés intéressants ou de la voix d'un interlocuteur particulier. Si le gouvernement ne trouve pas la cible dans le premier échantillon de 1 %, les interceptions peuvent être étendues à un 1 % différent jusqu'à ce que la cible soit trouvée, ou jusqu'à ce que la ligne de téléphone de chacun ait été inspectée à la recherche de trafic subversif. Le FBI dit qu'ils ont besoin de cette capacité pour prévoir le futur. Ce plan a provoqué un tel scandale qu'il a été retiré au Congrès, en peu de temps, en 1995. Mais le simple fait que le FBI ait été jusqu'à demander ces pouvoirs élargis révèle leur programme. Et la défaite de ce plan n'est pas si rassurante quand vous considérez que le "Digital Telephony bill" de 1994 avait aussi été retiré la première fois qu'il a été introduit, en 1993.

Les avancées technologiques ne permettent pas le maintien du statu quo, à partir du moment où la vie privée est concernée. Le statu quo est instable. Si nous ne faisons rien, des nouvelles technologies donneront au gouvernement de nouvelles capacités de surveillance dont Staline n'aurait jamais pu rêver. La seule façon de préserver la vie privée à l'ère de l'information est de recourir à la cryptographie sûre.

La crainte d'abus de pouvoir du gouvernement n'est pas la seule raison pour vouloir recourir à la cryptographie. Votre correspondance d'affaires peut être interceptée par des concurrents, le crime organisé, ou des gouvernements étrangers. Plusieurs gouvernements, par exemple, admettent utiliser leurs services d'écoutes contre les compagnies d'autres pays pour donner à leurs propres sociétés un avantage sur la concurrence. L'ironie est que les restrictions du gouvernement des Etats-Unis sur la cryptographie ont affaibli les défenses des entreprises américaines contre les services de renseignement étrangers et le crime organisé.

Le gouvernement sait quel rôle pivot la cryptographie est appelée à jouer dans le rapport de force avec son peuple. En avril 1993, l'administration Clinton dévoila une audacieuse nouvelle initiative dans la politique cryptographique, qui avait été préparée à l'Agence de Sécurité Nationale ("National Security Agency" NSA) depuis le début de l'administration Bush. La pièce centrale de ce dispositif est le microprocesseur construit par le gouvernement et appelé puce "Clipper", contenant un chiffre de la NSA classé top secret. Le gouvernement est en train d'encourager l'industrie privée à l'insérer dans leurs équipements de

communications sécurisées, comme les téléphones sécurisés, les fax sécurisés, etc. AT&T insère dès à présent la "Clipper" dans ses équipements vocaux sécurisés. Ce que cela cache: au moment de la fabrication, chaque puce "Clipper" sera chargée avec sa propre clé, et le gouvernement en gardera une copie, placée entre les mains d'un tiers. Il n'y a pas à s'inquiéter, cependant: le gouvernement a promis qu'il utiliserait ces clés pour lire le trafic des citoyens uniquement dans les cas dûment autorisés par la loi. Bien sûr, pour rendre la "Clipper" complètement efficace, la prochaine étape devrait être de mettre hors-la-loi toute autre forme de cryptographie.

Le gouvernement avait déclaré au début que l'utilisation de Clipper serait volontaire, que personne ne serait forcé de l'utiliser à la place d'autres types de cryptographie. Mais la réaction du public contre le Clipper a été forte, si forte que le gouvernement a anticipé. L'industrie informatique a affirmé de manière unanime son opposition à l'usage de Clipper. Le directeur du FBI, Louis Freeh, répondit à une question lors d'une conférence de presse en 1994 en disant que si Clipper n'arrivait pas à obtenir le soutien du public, et que les interceptions du FBI étaient réduites à néant par une cryptographie non contrôlée par le gouvernement, son Bureau n'aurait pas d'autre choix que de chercher une solution législative. Plus tard, dans les suites de la tragédie d'Oklahoma City, M. Freeh témoignant devant la Commission Judiciaire du Sénat, déclara que la disponibilité publique de cryptographie sûre devait être restreinte par le gouvernement (bien que personne n'eût suggéré que la cryptographie avait été utilisée par les auteurs de l'attentat).

L'Electronic Privacy Information Center (EPIC) a obtenu des documents révélateurs par le biais du "Freedom of Information Act" [loi sur la liberté de l'information]. Dans un document de travail intitulé "Encryption: The Threat, Applications and Potential Solutions" [Chiffrement: la menace, les applications, et les solutions possibles], et envoyé au Conseil national de sécurité en février 1993, le FBI, la NSA, et le Ministère de la Justice (DOJ) concluaient que "Les solutions techniques, telles qu'elles existent, marcheront seulement si elles sont incorporées dans tous les produits de chiffrement. Pour s'assurer qu'il en sera ainsi, une loi obligeant à l'utilisation de produits de chiffrement approuvés par le Gouvernement ou l'adhésion aux critères de chiffrement du Gouvernement est requise."

Le Gouvernement a eu un comportement qui n'inspire pas confiance dans le fait qu'il n'abuseront pas de nos libertés civiles. Le programme COINTELPRO du FBI avait ciblé les groupes qui s'opposaient aux politiques du Gouvernement. Ils ont espionné les mouvements pacifistes et le mouvement des droits civils. Ils ont intercepté le téléphone de Martin Luther King Jr. Nixon avait sa liste d'ennemis. Et ensuite il y a eu la pagaille du Watergate. Le Congrès paraît maintenant prêt à faire passer des lois restreignant nos libertés civiles sur Internet. A aucun moment dans le passé la méfiance envers le Gouvernement n'a été si largement partagée sur tout le spectre politique qu'aujourd'hui.

Si nous voulons résister à cette tendance inquiétante du gouvernement pour rendre illégale la cryptographie, une mesure que nous pouvons adopter est d'utiliser la cryptographie autant que nous le pouvons actuellement pendant que c'est encore légal. Quand l'utilisation de cryptographie sûre devient populaire, il est plus difficile pour le gouvernement de la criminaliser. Par conséquent, utiliser PGP est bon pour préserver la démocratie.

Si l'intimité est mise hors la loi, seuls les hors-la-loi auront une intimité. Les agences de renseignement ont accès à une bonne technologie cryptographique. De même les trafiquants d'armes et de drogue. Mais les gens ordinaires et les organisations politiques de base n'avaient pour la plupart pas eu accès à une technologie cryptographique de "qualité militaire" abordable. Jusqu'à présent.

PGP donne aux gens le pouvoir de prendre en main leur intimité. Il y a un besoin social croissant pour cela. C'est pourquoi je l'ai créé.

Les chiffres symétriques de PGP

PGP offre une sélection de différents chiffres à clé secrète pour chiffrer un message. Par chiffre à clé secrète, nous entendons un algorithme de chiffrement par blocs conventionnel, ou symétrique, qui utilise la même clé aussi bien pour chiffrer que pour déchiffrer. Les trois chiffres symétriques par blocs offerts par PGP sont CAST, Triple-DES, IDEA. Il ne s'agit pas de chiffres "maison". Ils furent tous développés par des équipes de cryptographes de réputation incontestable.

Pour les curieux de cryptographie, ces trois chiffres opèrent sur des blocs de 64 bits de texte clair et de texte chiffré. CAST et IDEA ont des tailles de clés de 128 bits, alors que Triple-DES utilise une clé de 168 bits. Comme le Data Encryption Standard (DES), ces trois chiffres peuvent être utilisés en mode cipher feedback (CFB) et cipher block chaining (CBC). PGP les utilise en mode CFB 64 bits.

J'ai inclus le chiffre CAST dans PGP parce qu'il s'annonce comme un bon chiffre par blocs avec une taille de clé de 128 bits, il est très rapide, et il est libre. Son nom est tiré des initiales de ses concepteurs Carlisle Adams et Stafford Tavares de Northern Telecom (Nortel). Nortel a déposé un brevet pour CAST, mais ils ont ajouté une disposition pour rendre CAST disponible à tous sans avoir à payer de royalties. CAST apparaît comme étant exceptionnellement bien conçu, par des gens jouissant d'excellentes réputations dans ce domaine. La conception est fondée sur une approche très formelle, avec un nombre d'assertions formellement démontrables qui donnent de bonnes raisons de penser qu'il exige une recherche exhaustive des clés pour casser sa clé de 128 bits. CAST n'a pas de clés faibles ou semi faibles. Il existe de solides arguments permettant de penser que CAST est complètement immunisé aussi bien contre la cryptanalyse linéaire que différentielle, les deux formes de cryptanalyse les plus puissantes dans la recherche publique, toutes deux ayant été utilisées pour craquer DES. CAST est trop récent pour que se soit développée une longue série d'études à son sujet, mais sa conception formelle et la bonne réputation de ses concepteurs attirera sans aucun doute l'attention et les tentatives d'attaques cryptanalytiques d'une partie de la communauté cryptographique universitaire. Je ne suis pas loin d'éprouver la même bonne impression au sujet de CAST qu'il y a quelques années au sujet d'IDEA, le chiffre que j'avais choisi pour l'utiliser dans les versions précédentes de PGP. A cette époque, IDEA était aussi trop récent pour avoir fait l'objet d'une série d'études, mais il a très bien tenu.

Le chiffre par blocs IDEA (International Data Encryption Algorithm) est fondé sur le concept du "mixage d'opérations depuis différents groupes algébriques". Il a été développé au ETH à Zurich par James L. Massey et Xuejia Lai, et publié en 1990. Les premiers articles publiés sur le chiffre l'appelaient IPES (Improved

Proposed Encryption Standard), mais ils ont ensuite changé le nom en IDEA. Depuis, IDEA a beaucoup mieux résisté que d'autres chiffres tels que FEAL, REDOC-II, LOKI, Snefru et Khafre. Et IDEA est plus résistant que DES à la très puissante attaque par cryptanalyse différentielle de Biham et Shamir, aussi bien qu'aux attaques par cryptanalyse linéaire. Comme ce chiffre continue à attirer les attaques des plus formidables milieux du monde de la cryptanalyse, la confiance en IDEA grandit avec le temps. Malheureusement, le plus grand obstacle à ce que IDEA devienne un standard a été le fait que Ascom Systec détient un brevet sur sa conception, et à la différence de DES et de CAST, IDEA n'est pas disponible gratuitement.

En plus, PGP inclut le Triple-DES à trois clés parmi ses chiffres disponibles. Le DES a été développé par IBM au milieu des années 70. Alors qu'il est de bonne conception, sa taille de clé de 56 bits est trop petite pour les normes d'aujourd'hui. Triple-DES est très robuste, et a été bien étudié depuis plusieurs années, aussi peut-il être considéré comme un pari plus sûr que les nouveaux chiffres tels que CAST et IDEA. Triple-DES est le DES appliqué trois fois au même bloc de données, en utilisant trois clés différentes, à ceci près que la seconde opération DES est lancée en arrière-plan, en mode déchiffrement. Bien que Triple-DES soit beaucoup plus lent que CAST ou IDEA, la vitesse n'est habituellement pas déterminante pour les logiciels d'e-mail. Bien que Triple-DES utilise une taille de clés de 168 bits, il apparaît avoir une taille effective de clé d'au moins 112 bits contre un attaquant, à supposer qu'il ait la capacité de réunir d'immenses quantités de données à utiliser dans l'attaque. Selon un article présenté par Michael Weiner à Crypto96, toute quantité de données plausible pour l'attaquant permettrait une attaque qui requerrait autant de travail que de casser une clé de 129 bits. Triple-DES n'est pas encombré de brevets.

Les clés publiques PGP qui ont été générées par PGP version 5.0 ou ultérieure intègrent des informations qui indiquent à l'expéditeur quels chiffres sont reconnus par le logiciel du destinataire, de telle sorte que le logiciel de l'expéditeur sait quels chiffres peuvent être utilisés pour chiffrer. Les clés Diffie-Hellman/DSS acceptent CAST, IDEA, ou Triple-DES comme chiffres, avec CAST comme sélection par défaut. A ce jour, pour des raisons de compatibilité, les clés RSA n'offrent pas cette fonctionnalité. Seul le chiffre IDEA est utilisé par PGP pour envoyer des messages avec des clés RSA, parce que les anciennes versions de PGP ne géraient que RSA et IDEA.

A propos des routines de compression de données PGP

Normalement PGP compresse le texte clair avant de le chiffrer, parce qu'il est trop tard pour le compresser après qu'il ait été chiffré; des données chiffrées ne sont pas compressibles. La compression de données économise le temps de transmission par modem et l'espace disque et, plus important, augmente la sécurité cryptographique. De nombreuses techniques cryptanalytiques exploitent les redondances trouvées dans le texte clair pour craquer le chiffre. La compression de données réduit cette redondance dans le texte clair, et par là augmente considérablement la résistance à la cryptanalyse. La compression du texte clair demande un temps supplémentaire, mais du point de vue de la sécurité cela en vaut la peine.

Les fichiers qui sont trop petits pour être compressés, ou qui ne se compressent pas bien, ne sont pas compressés par PGP. En plus, le programme reconnaît les fichiers produits par les programmes de compression les plus courants, tels que PKZIP, et n'essaye pas de compresser un fichier qui a déjà été compressé.

Pour les amateurs de technique, le programme utilise les routines de compression gratuites ZIP écrites par Jean-Loup Gailly, Marc Adler, et Richard B. Wales. Ce logiciel ZIP utilise des algorithmes de compression qui sont fonctionnellement équivalents à ceux utilisés par PKZIP 2.x de PKWare. Ce logiciel de compression ZIP a été sélectionné pour PGP principalement parce qu'il a un taux de compression vraiment bon et parce qu'il est rapide.

A propos des nombres aléatoires utilisés comme clés de session

PGP utilise un générateur de nombres pseudo aléatoires cryptographiquement robuste pour créer les clés de session temporaires. Si ce fichier de semence n'existe pas, il est automatiquement créé et alimenté avec de véritables nombres aléatoires dérivés par PGP de vos actions aléatoires à partir de l'intervalle entre vos frappes clavier et les mouvements de la souris.

Le générateur réalimente le fichier de semence chaque fois qu'il est utilisé, en y mélangeant un nouveau matériau partiellement issu de l'heure du jour et d'autres sources réellement aléatoires. Il utilise le chiffre conventionnel comme un moteur pour le générateur de nombres aléatoires. Le fichier de semence contient des éléments de semence aléatoires et des éléments de clés aléatoires utilisés pour alimenter le moteur de chiffrement conventionnel pour le générateur aléatoire.

Ce fichier de semence aléatoire devrait être protégé de la divulgation, pour réduire le risque qu'un attaquant puisse en déduire vos prochaines ou précédentes clés de session. L'attaquant aurait les plus grandes difficultés à tirer quoi que se soit d'utilisable en s'emparant de ce fichier de semence aléatoire, parce que le fichier est cryptographiquement blanchi avant et après chaque utilisation. Néanmoins, il semble prudent d'essayer de l'empêcher de tomber en de mauvaises mains. Si possible, faites en sorte que ce fichier ne soit identifiable que par vous. Sinon, ne laissez pas n'importe qui copier des disques depuis votre ordinateur.

A propos des contractions de message

La contraction de message est une "condensation" compacte (160 bits ou 128 bits) de votre message ou de la somme de contrôle de fichier. Vous pouvez aussi la voir comme une "empreinte" du message ou du fichier. La contraction de message "représente" votre message d'une manière telle que si le message était altéré en quelque façon, une contraction de message différente serait calculée à partir de lui. Cela permet de détecter tout changement apporté au message par un contrefacteur. La contraction de message est calculée par l'application d'une fonction de hachage à sens unique, cryptographiquement robuste, au message. Il sera cryptographiquement impraticable pour un attaquant d'élaborer un message de substitution qui produirait une contraction de message identique. Sous ce rapport, une contraction de message est bien meilleure qu'une somme de contrôle, parce qu'il est facile d'élaborer un message différent qui produirait la même

somme de contrôle. Mais de même qu'avec une somme de contrôle, vous ne pouvez pas déduire le message originel de la contraction de ce message.

Le chiffre de contraction de message maintenant utilisé dans PGP (version 5.0 et ultérieure) est appelé SHA, acronyme de Secure Hash Algorithm conçu par la NSA pour le National Institute of Standards and Technology (NIST). SHA est un algorithme de hachage sur 160 bits. Quelques personnes pourraient considérer tout ce qui vient de la NSA avec suspicion, parce que la NSA est en charge d'intercepter les communications et de casser les codes. Mais ne perdez pas de vue que la NSA n'a aucun intérêt à contrefaire des signatures, et que le Gouvernement tirera profit d'une bonne norme de signature numérique infalsifiable, qui empêchera quiconque de répudier sa signature. Il y a aussi des avantages distincts dans le cas de poursuites judiciaires et de la recherche de renseignements. De plus, SHA a été publié dans la littérature publique et a été intensivement examiné par la plupart des meilleurs cryptographes du monde spécialisés dans les fonctions de hachage, et l'opinion unanime est que SHA est extrêmement bien conçu. Il comporte quelques innovations de conception qui pallient aux faiblesses constatées dans les algorithmes de contraction précédemment publiés par les cryptographes universitaires. Toutes les nouvelles versions de PGP utilisent SHA en tant qu'algorithme de contraction de messages pour créer des signatures avec les nouvelles clés DSS qui sont compatibles avec le NIST Digital Signature Standard. Pour des raisons de compatibilité, les nouvelles versions de PGP utilisent toujours MD5 pour les signatures RSA, parce que les anciennes versions de PGP utilisaient MD5 pour les signatures RSA.

Le chiffre de contraction de message utilisé par les anciennes versions de PGP est le MD5 Message Digest Algorithm, placé dans le domaine public par RSA Data Security, Inc. MD5 est un algorithme de hachage sur 128 bits. En 1996, MD5 a été presque cassé par un cryptographe Allemand, Hans Dobbertin. Bien que MD5 n'ait pas été complètement cassé cette fois-là, on lui a découvert de sérieuses faiblesses, telles que personne ne devrait l'utiliser pour créer des signatures. Des travaux ultérieurs dans ce domaine pourraient le casser complètement, permettant de contrefaire des signatures. Si vous ne voulez pas qu'un jour votre signature numérique PGP figure sur de faux aveux, vous feriez bien de migrer vers les nouvelles clés PGP DSS comme méthode préférée pour créer des signatures numériques, parce que DSS utilise SHA comme algorithme de hachage.

Comment protéger les clés publiques de la falsification

Dans un cryptosystème à clé publique, vous n'avez pas à protéger les clés publiques de la divulgation. En fait, mieux vaut qu'elles soient largement diffusées. Mais il est important de protéger les clés de la falsification, pour être sûr que la clé publique appartient réellement à la personne à qui elle semble appartenir. C'est peut-être la plus importante vulnérabilité des cryptosystèmes à clé publique. Voyons d'abord un désastre potentiel, avant de voir comment l'éviter sûrement avec PGP.

Supposons que vous vouliez envoyer un message privé à Alice. Vous téléchargez la clé publique d'Alice depuis un BBS [quelconque, ou un site Internet inconnu]. Vous chiffrez votre lettre à Alice avec cette clé publique et vous la lui envoyez par e-mail.

Malheureusement, à votre insu ou à l'insu d'Alice, un autre utilisateur appelé Charlie a infiltré le BBS et a lui-même généré une clé publique avec l'ID d'utilisateur "Alice" attaché à cette clé. Il a secrètement substitué cette fausse clé à la véritable clé d'Alice. Vous utilisez sans le savoir cette fausse clé appartenant [en réalité] à Charlie au lieu de la clé publique d'Alice. Tout semble normal parce que cette fausse clé affiche "Alice" comme ID d'utilisateur. Maintenant, Charlie peut déchiffrer le message destiné à Alice parce qu'il a la clé secrète correspondante. Il peut même chiffrer à nouveau le message préalablement déchiffré, avec la vraie clé publique d'Alice et le lui envoyer pour que personne ne se doute de la fraude. Pire encore, il peut même faire des signatures, en apparence authentiques, d'Alice avec sa [fausse] clé secrète parce que tout le monde utilisera la fausse clé publique pour vérifier la signature d'Alice.

La seule façon d'éviter ce désastre est d'empêcher que qui ce soit puisse falsifier les clés publiques. Si vous avez obtenu la clé publique d'Alice directement d'Alice, il n'y a pas de problème. Mais cela peut être difficile si Alice est à des milliers de kilomètres de là, ou si elle est actuellement injoignable.

Peut-être pourriez-vous vous procurer la clé publique d'Alice par l'intermédiaire de David, un ami commun en qui vous avez tous les deux confiance, et qui sait qu'il détient une copie authentique de la clé publique d'Alice. David pourrait signer la clé publique d'Alice, se portant ainsi garant de l'intégrité de la clé publique d'Alice. David créerait cette signature avec sa propre clé secrète.

Cela créerait une signature de la clé publique, et prouverait que la clé d'Alice n'a pas été falsifiée. Cela exige de disposer d'une copie reconnue authentique de la clé publique de David pour vérifier sa signature. Peut-être David pourrait-il aussi fournir à Alice une copie signée de votre clé publique. De cette manière, David sert d'"Aval" entre vous et Alice.

Cette signature de la clé publique d'Alice pourrait être mise en ligne par David ou Alice sur un BBS, et vous pourriez la télécharger ultérieurement. Vous pourriez alors vérifier la signature via la clé publique de David et être ainsi assuré qu'il s'agit réellement de la clé publique d'Alice. Aucun imposteur ne peut vous duper en vous faisant accepter sa propre fausse clé comme étant la clé d'Alice parce que personne ne peut contrefaire la signature créée par David.

Une personne largement reconnue comme digne de confiance pourrait même se spécialiser dans ce service [consistant à] "certifier" les utilisateurs les uns aux autres en signant leurs clés publiques. Cette personne de confiance pourrait être considérée comme une "Autorité Certifiante". On aurait l'assurance que toute clé publique portant la signature de l'Autorité Certifiante appartient réellement à la personne à qui elle semble appartenir. Tout utilisateur intéressé n'aurait dès lors besoin que d'une copie reconnue authentique de la clé publique de l'Autorité Certifiante, de sorte que les signatures de l'Autorité Certifiante puissent être vérifiées [sur les clés publiques des utilisateurs]. Dans certains cas, l'Autorité Certifiante peut aussi faire office de serveur de clés, permettant aux utilisateurs d'un réseau de consulter des clés publiques en interrogeant le serveur de clés, mais il n'y a pas de raison pour qu'un serveur de clés doive aussi certifier des clés.

Une Autorité Certifiante centralisée fiable est particulièrement adaptée aux grandes institutions contrôlées depuis un centre unique comme les grandes entreprises ou les administrations. Quelques milieux institutionnels recourent au modèle de telles Autorités Certifiantes.

Pour des milieux plus décentralisés, permettre à tous les utilisateurs d'agir comme avals de confiance pour leurs amis se révélera probablement mieux adapté que le recours à une autorité de certification centralisée.

Une des fonctionnalités les plus séduisantes de PGP est qu'il est aussi bien adapté à un milieu centralisé avec une Autorité Certifiante qu'à un milieu plus décentralisé dans lequel des individus échangent leurs clés personnelles.

Toute cette affaire de la protection des clés publiques contre la falsification est le problème le plus délicat à résoudre pour les applications pratiques de la cryptographie à clé publique. C'est le "talon d'Achille" de la cryptographie à clé publique, et une grande partie de la complexité du logiciel est liée à la résolution de ce seul problème.

Vous ne devriez utiliser une clé publique qu'après vous être assuré qu'il s'agit d'une clé publique authentique qui n'a pas été falsifiée, et qui appartient réellement à la personne à qui la clé prétend appartenir. Vous pouvez en être sûr si vous tenez cette clé publique directement de son propriétaire, ou si elle est signée par quelqu'un en qui vous avez confiance, dont vous détenez déjà une clé publique authentique. Aussi, l'ID d'utilisateur devrait être le nom complet du propriétaire de la clé, et non pas seulement son nom de famille.

Peu importe combien vous pouvez être tenté, ne cédez *jamais* à la facilité en faisant confiance à une clé publique que vous avez téléchargée depuis un BBS, à moins qu'elle ne soit signée par quelqu'un en qui vous avez confiance. Cette clé non certifiée pourrait avoir été falsifiée, peut-être même par l'administrateur système du BBS.

Si on vous demande de signer la clé publique d'autrui, assurez-vous qu'elle appartient réellement à la personne nommée dans l'ID d'utilisateur de cette clé publique. Et cela parce que votre signature sur sa clé est votre promesse que cette clé publique lui appartient réellement. D'autres personnes qui vous font confiance accepteront sa clé parce qu'elle porte votre signature. Il peut être malavisé de se fier au oui-dire – ne signez pas sa clé publique sauf si vous avez une connaissance indépendante et de première main qu'elle lui appartient vraiment. De préférence, vous ne devriez la signer que si vous l'obtenez directement d'elle.

Pour signer une clé publique, vous devez être encore bien plus certain de l'appartenance de cette clé que si vous vouliez simplement utiliser cette clé pour chiffrer un message. Pour être convaincu qu'une clé est d'un aloi suffisant pour être utilisée, les signatures par des avals de confiance devraient suffire. Mais pour signer une clé vous-même, vous devriez recourir à votre connaissance directe, personnelle et indépendante du propriétaire de cette clé. Peut-être pourriez-vous téléphoner au propriétaire de la clé et lui lire l'empreinte de la clé pour qu'il confirme que la clé que vous détenez est réellement sa clé – et assurez-vous que vous parlez réellement à la bonne personne.

Gardez présent à l'esprit que votre signature sur une clé publique ne garantit pas l'intégrité de cette personne, mais seulement l'intégrité (l'appartenance) de la clé publique de cette personne. Vous ne risquez pas de compromettre votre crédibilité en signant la clé publique d'un débile mental, si vous êtes absolument sûr que la clé lui appartient réellement. D'autres personnes accepteront cette clé parce que vous l'avez signée (en admettant qu'elles vous fassent confiance), mais elles

n'auront pas confiance dans le propriétaire de cette clé. Avoir confiance en une clé n'est pas la même chose que d'avoir confiance dans le propriétaire de la clé.

Ce serait une bonne idée de garder sous la main une copie de votre propre clé publique signée par de nombreux "avals", dans l'espoir que beaucoup de gens feront confiance à au moins un des avals qui se sont portés garants de la validité de votre propre clé. Vous pourriez poster votre clé avec sa collection de signatures sur divers BBS. Si vous signez la clé publique d'autres personnes, renvoyez-la leur avec votre signature de telle sorte qu'elles puissent l'ajouter à leur propre collection de garants de leur propre clé publique.

Assurez-vous que personne ne peut falsifier votre propre trousseau de clés. La vérification d'une nouvelle signature certifiant une clé publique doit dépendre en dernier ressort de l'intégrité des clés publiques certifiées qui se trouvent déjà dans votre propre trousseau de clés publiques. Gardez un contrôle physique de votre trousseau de clés publiques, de préférence sur votre propre ordinateur personnel plutôt que sur un système distant et/ou partagé, exactement comme vous le feriez pour votre clé secrète. Ceci pour le protéger de la falsification, non de la divulgation. Gardez une copie de sauvegarde fiable de vos trousseaux de clés publiques et secrètes sur un support protégé en écriture.

Dans la mesure où votre propre clé publique certifiée est utilisée comme référence pour certifier directement ou indirectement toutes les autres clés de votre trousseau, c'est celle qu'il faut protéger avec le plus grand soin de la falsification. Vous devriez en garder une copie de sauvegarde sur un support protégé en écriture.

D'une manière générale, PGP présume que vous conserverez le contrôle physique de votre système et de vos trousseaux de clés, ainsi que de votre copie de PGP elle-même. Si un intrus peut accéder à votre disque, alors en théorie il peut falsifier PGP lui-même, remettant en cause l'efficacité des dispositifs de sécurité dont dispose PGP pour détecter une falsification des clés.

Une méthode plus complexe pour protéger votre propre trousseau de toute falsification est de signer ce trousseau entier avec votre propre clé secrète. Vous pouvez le faire en créant une signature détachée du trousseau de clés publiques.

Comment PGP reconnaît-il les clés valides?

Avant de lire ce chapitre, vous devriez lire le chapitre précédent, "[Comment protéger les clés publiques de la falsification](#)".

PGP reconnaît les clés convenablement certifiées de votre trousseau de clés publiques à l'aide des signatures des avals en qui vous avez confiance. Tout ce que vous avez à faire est de dire à PGP qui sont les gens fiables en tant qu'avals, et de certifier leurs clés avec votre propre clé la plus certifiée. PGP peut utiliser cette information, validant automatiquement toutes les autres clés qui ont été signées par les avals. Et bien sûr, vous pouvez directement signer d'autres clés vous-même.

PGP utilise deux critères bien distincts pour apprécier l'aloï d'une clé publique – ne les confondez pas:

1. La clé appartient-elle réellement à la personne à qui elle semble appartenir? En d'autres termes, a-t-elle été certifiée avec une signature fiable?
2. Appartient-elle à quelqu'un en qui vous pouvez avoir confiance pour certifier d'autres clés?

PGP peut évaluer la réponse à la première question. Pour répondre à la deuxième question, vous devez le dire explicitement à PGP. Quand vous répondez à la question 2, PGP peut ensuite évaluer la réponse à la question 1 pour les autres clés signées par l'aval que vous avez désigné comme fiable.

Les clés qui ont été certifiées par un aval de confiance sont considérées comme valides par PGP. Les clés appartenant aux avals de confiance doivent être certifiées soit par vous soit par un autre aval de confiance.

PGP offre aussi la possibilité d'établir des nuances quant au crédit que méritent les avals. Votre confiance dans les propriétaires de clés pour agir en tant qu'avals ne reflète pas seulement votre estimation de leur intégrité personnelle – cela devrait refléter également la sagacité que vous leur supposez dans la compréhension de la gestion des clés et dans celle de signer les clés à bon escient. Vous pouvez désigner à PGP une personne comme inconnue, non fiable, marginalement fiable, ou complètement fiable pour certifier les autres clés publiques. Cette information sur la fiabilité est conservée avec leurs clés dans votre trousseau, mais quand vous demandez à PGP de copier [extraire] une clé de votre trousseau, PGP ne copie pas l'information sur la fiabilité avec la clé, parce que vos opinions personnelles sur la fiabilité sont considérées comme confidentielles.

Quand PGP évalue la validité d'une clé publique, il examine le niveau de fiabilité de toutes les signatures attachées. Il calcule un résultat pondéré de la validité – deux signatures marginalement fiables sont considérées comme équivalentes à une signature complètement fiable. L'évaluation critique de PGP est modulable – par exemple, vous pouvez régler PGP pour exiger deux signatures complètement fiables ou trois signatures marginalement fiables pour décider qu'une clé est valide.

Votre propre clé est "axiomatiquement" valide pour PGP, n'ayant pas besoin de la signature d'un aval pour prouver sa validité. PGP sait quelles clés publiques sont les vôtres, en regardant la clé secrète correspondante dans le trousseau de clés secrètes. PGP présume également que vous vous considérez vous-même comme complètement fiable pour certifier d'autres clés.

Avec le temps, vous accumulerez des clés d'autres personnes que vous pouvez vouloir désigner comme avals de confiance. Chacun choisira ses propres avals de confiance. Et chacun accumulera progressivement et distribuera avec sa clé une collection de signatures d'autres personnes, dans l'espoir que parmi ceux qui en détiendront une copie, il s'en trouvera pour faire confiance à au moins une ou deux des signatures. Cela permettra l'émergence d'un réseau de confiance décentralisé, à tolérance d'erreurs, pour toutes les clés publiques.

Cette approche originale par la base tranche nettement avec les schémas de la norme de gestion des clés publiques développés par le gouvernement et d'autres institutions centralisées, tel le "Internet Privacy Enhanced Mail" (PEM), qui sont basés sur un contrôle et une obligation de confiance centralisés. Le modèle

normatif repose sur une hiérarchie d'Autorités Certifiantes qui vous dictent à qui vous devez faire confiance. La méthode probabiliste décentralisée de PGP pour déterminer l'aloï des clés publiques est la poutre maîtresse de l'architecture de son modèle de gestion des clés. PGP vous laisse choisir vous-même ceux qui méritent votre confiance, vous plaçant au sommet de votre propre pyramide personnelle de certification. PGP est destiné aux gens qui préfèrent plier eux-mêmes leur propre parachute.

Notez que si PGP tend à privilégier cette approche par la base, décentralisée, cela ne signifie pas qu'il ne soit pas aussi bien adapté à des modèles plus hiérarchisés et centralisés de gestion des clés publiques. Dans les grandes sociétés, par exemple, les utilisateurs voudront probablement avoir affaire à un seul interlocuteur, personne physique ou non, qui signera toutes les clés des employés. PGP gère ce scénario centralisé comme un sous-cas particulier de son modèle général de confiance.

Comment protéger ses clés secrètes de la divulgation

Protégez votre propre clé secrète et votre phrase secrète très soigneusement. Si jamais votre clé secrète est compromise, vous feriez mieux de le faire savoir à toutes les parties concernées avant qu'on l'utilise pour signer en votre nom. Par exemple, on pourrait l'utiliser pour créer de fausses vraies signatures, qui pourraient créer des problèmes à beaucoup de monde, surtout si votre signature est largement considérée comme fiable. Et bien sûr, une compromission de votre propre clé secrète compromettrait tous les messages qui vous sont envoyés.

Pour protéger votre clé secrète, vous pouvez commencer par la maintenir toujours sous votre contrôle physique. Il est bon de la conserver sur votre ordinateur personnel à la maison, ou sur un ordinateur portable que vous pouvez emmener avec vous. Si vous devez utiliser au bureau un ordinateur dont vous n'avez pas en permanence le contrôle physique, alors gardez vos trousseaux de clés publiques et secrètes sur une disquette protégée en écriture, et ne l'oubliez pas en quittant le bureau. Ce ne serait pas une bonne idée de conserver votre clé secrète sur un ordinateur distant et/ou partagé, comme un système de type Unix connecté en permanence. Quelqu'un pourrait intercepter la ligne de votre modem et capturer votre phrase secrète, et ensuite se procurer votre clé secrète depuis le système distant. Vous ne devriez utiliser votre clé secrète que sur une machine placée sous votre contrôle physique.

Ne conservez pas votre phrase secrète sur l'ordinateur sur lequel se trouve votre clé secrète. Conserver ensemble la clé secrète et la phrase secrète sur le même ordinateur est aussi dangereux que de garder votre code secret de carte bancaire dans le même portefeuille que la carte. Vous ne voulez pas que quelqu'un mette la main sur votre disque contenant à la fois la phrase secrète et le fichier de clé secrète. Il serait plus sûr de simplement mémoriser votre phrase secrète et de ne pas la conserver ailleurs que dans votre cerveau. Si vous sentez que vous devez écrire votre phrase secrète, protégez-la bien, peut-être mieux encore que la clé secrète.

Et conservez des copies de sauvegarde de votre clé secrète – rappelez-vous, vous détenez l'unique exemplaire de votre clé secrète, et la perdre rendra inutilisables toutes les copies de votre clé publique que vous avez diffusées à travers le monde.

L'approche décentralisée non institutionnelle utilisée par PGP pour gérer les clés publiques a ses avantages, mais malheureusement elle signifie aussi qu'on ne peut pas compter sur une liste centralisée unique des clés compromises. Cela rend beaucoup plus difficile de limiter les dégâts causés par une compromission de clé secrète. Vous ne pouvez que le faire savoir et espérer que tout le monde en entendra parler.

Si le pire des cas survient – votre clé secrète et votre phrase secrète sont toutes les deux compromises (espérons que vous vous en apercevrez) – vous devrez émettre un certificat de “révocation de clé”. Ce type de certificat est utilisé pour prévenir les gens d'arrêter d'utiliser votre clé publique. Vous pouvez utiliser PGP pour créer un tel certificat en utilisant la commande Revoke du menu PGPkeys ou bien en le faisant faire par votre Designated Revoker. Ensuite, vous devez l'envoyer à un serveur de clés de sorte que d'autres puissent le trouver. Leur propre logiciel PGP installera ce certificat de révocation dans leur trousseau de clés publiques et les empêchera automatiquement d'utiliser votre clé publique à l'avenir. Vous pouvez alors générer une nouvelle paire de clés secrète/publique et publier la nouvelle clé publique. Vous pourriez diffuser un “lot” contenant votre nouvelle clé publique et le certificat de révocation de votre ancienne clé.

Que faire si vous perdez votre clé secrète?

Normalement, si vous voulez révoquer votre propre clé secrète, vous pouvez utiliser la commande Revoke du menu PGPkeys pour émettre un certificat de révocation, signé avec votre propre clé secrète.

Mais que pouvez-vous faire si vous perdez votre clé secrète, ou si votre clé secrète est détruite? Vous ne pouvez pas la révoquer vous-même, parce que vous devez utiliser votre propre clé secrète pour la révoquer, et vous ne l'avez plus. Si vous n'avez pas de révocateur désigné pour votre clé, quelqu'un spécifié dans PGP pour révoquer la clé à votre place, vous devez demander à chaque personne qui a signé votre clé de retirer sa certification. Ainsi, quiconque essaiera d'utiliser votre clé sur la foi de l'un de vos avals saura qu'il ne faut plus faire confiance à votre clé publique.

Pour plus d'explications au sujet des révocateurs désignés, voir [“Pour instituer un révocateur désigné”](#) au [Chapitre 6](#).

Méfiez-vous de la poudre de perlimpinpin

Quand vous examinez un logiciel de cryptographie, la question revient toujours: pourquoi devriez-vous faire confiance à ce produit? Même si vous examinez vous-même le code source, tout le monde n'a pas l'expérience cryptographique pour en apprécier la sécurité. Même si vous êtes un cryptographe expérimenté, de subtiles faiblesses dans les algorithmes peuvent toujours vous échapper.

Quand j'étais au collège, au début des années 70, j'avais conçu ce que je croyais être un schéma de chiffrement génial. Un simple flux pseudo aléatoire était ajouté au flux de texte clair pour créer un texte chiffré. Cela devait apparemment contrecarrer toute analyse de fréquence sur le texte chiffré, et être incassable même pour les services gouvernementaux de renseignement disposant des plus

grandes ressources qui soient. Je me sentais tellement suffisant à propos de mon exploit.

Des années plus tard, je découvris le même schéma dans de nombreux textes d'introduction à la cryptographie et des articles de cours. Comme c'était charmant. Les autres cryptographes avaient pensé au même schéma. Malheureusement, le schéma était présenté comme un simple devoir d'écolier sur la manière d'utiliser des techniques cryptographiques élémentaires pour les craquer simplement. Autant pour mon schéma génial.

De ma modeste expérience, j'ai appris combien il est facile de verser dans une conception erronée de la sécurité quand on conçoit un chiffre. La plupart des gens ne réalisent pas combien il est fichtrement difficile de concevoir un chiffre qui puisse résister à une attaque prolongée et déterminée par un adversaire possédant de grandes ressources. Beaucoup d'ingénieurs informaticiens sur grands systèmes ont développé des schémas de chiffrement aussi naïfs (souvent même exactement le même schéma), et certains d'entre eux ont été incorporés dans des logiciels de chiffrement commerciaux et vendus contre argent sonnante et trébuchant à des milliers d'utilisateurs ne soupçonnant rien.

C'est comme vendre des ceintures de sécurité d'automobile qui ont bonne apparence et semblent efficaces, mais s'ouvrent même au plus petit test d'accident. Compter sur elles peut être pire que de ne pas porter de ceinture du tout. Personne ne suspecte qu'elles sont mauvaises jusqu'à l'accident réel. Compter sur un logiciel de cryptographie faible peut faire mettre inconsciemment en danger des informations sensibles. Vous ne l'auriez pas fait si vous n'aviez pas eu du tout de logiciel de cryptographie. Peut-être ne découvrirez-vous jamais que vos données ont été compromises.

Parfois, les logiciels commerciaux utilisent le standard fédéral américain Data Encryption Standard (DES), un assez honnête chiffre conventionnel recommandé par le Gouvernement américain pour l'utilisation commerciale (mais pas pour l'information classée secret défense, curieusement – Hmmm). Il y a plusieurs "modes d'opération" que le DES peut utiliser, certains d'entre eux sont meilleurs que d'autres. Le Gouvernement recommande expressément de ne pas utiliser le mode le plus simple et le plus faible pour les messages, le mode Electronic Codebook (ECB). En revanche, on recommande les modes plus résistants et plus complexes Cipher Feedback (CFB) ou Cipher Block Chaining (CBC).

Malheureusement, la plupart des logiciels commerciaux de cryptographie que j'ai examinés utilisent le mode ECB. Quand j'en ai parlé aux auteurs de plusieurs de ces réalisations, ils ont dit qu'ils n'avaient jamais entendu parler des modes CBC ou CFB, et qu'ils ne savaient rien au sujet de la faiblesse du mode ECB. Le fait même qu'ils n'aient jamais étudié assez de cryptographie pour connaître ces concepts élémentaires n'est pas rassurant. Et ils gèrent parfois leurs clés DES d'une manière inadéquate ou non sûre. De même, ces logiciels incluent souvent un second chiffre plus rapide qui peut être utilisé à la place du DES plus lent. L'auteur du logiciel pense souvent que son chiffre propriétaire plus rapide est aussi sûr que le DES, mais après l'avoir questionné je découvre habituellement que c'est juste une variation de mon génial schéma de l'époque du collègue. Ou peut-être ne révélera-t-il jamais comment son schéma de chiffrement propriétaire fonctionne, mais il m'assure que c'est un schéma génial et que je devrais lui faire

confiance. Je suis sûr qu'il croit que son chiffre est génial, mais comment puis-je le savoir sans le voir?

En toute justice, je dois signaler que dans la plupart des cas ces produits lamentables ne proviennent pas de sociétés qui se spécialisent dans la technologie cryptographique.

Même les très bons logiciels, qui utilisent le DES dans le mode d'opération correct présentent encore des problèmes. Le standard DES utilise une clé de 56 bits, ce qui est trop petit pour les normes actuelles, et peut maintenant être aisément cassée par des recherches exhaustives de la clé sur des machines ultra rapides spéciales. Le DES a atteint la fin de sa vie utile, et voilà pourtant encore des logiciels qui y font appel.

Il y a une société appelée AccessData (<http://www.accessdata.com/>) qui vend très bon marché un ensemble qui craque le schéma de chiffrement intégré utilisé par WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox, MS Word et PKZIP. Il ne recherche pas simplement les mots de passe – il fait vraiment de la cryptanalyse. Des gens l'achètent quand ils ont oublié leur mot de passe pour leurs propres fichiers. Les services de police judiciaire l'achètent aussi, ainsi peuvent-ils lire les fichiers qu'ils saisissent. J'ai parlé à Eric Thompson, l'auteur, et il a dit que son programme prend seulement une demi seconde pour les craquer, mais qu'il a intégré une boucle retardatrice pour le ralentir de sorte que cela ne semble pas trop facile au client.

Dans le domaine du téléphone sécurisé, vos choix sont plutôt limités. Le ténor est le STU-III (Secure Telephone Unit), fabriqué par Motorola et AT&T pour un prix de 2 à 3.000 \$, utilisé par le Gouvernement pour des applications classées secret défense. Il dispose d'une cryptographie forte, mais l'achat de cette version forte est soumise à une autorisation spéciale du Gouvernement. Une version commerciale du STU-III est disponible, mais édulcorée pour le confort de la NSA, ainsi qu'une version pour l'exportation, encore plus sévèrement affaiblie. On trouve ensuite le AT&T Surity 3600, qui utilise la fameuse puce gouvernementale Clipper pour le chiffrement, avec séquestre des clés à l'usage du Gouvernement et pour le confort des intercepteurs. Ensuite, bien sûr, on trouve les brouilleurs vocaux analogiques (non numériques) qui vous pouvez acheter sur les catalogues du parfait espion, qui sont des joujoux insignifiants sur le plan cryptographique, mais qui sont vendus comme étant des équipements de communication "sécurisés" à des clients qui de toute façon ne connaissent rien de mieux.

D'un certain point de vue, la cryptographie est comme la pharmacie. Sa qualité peut être absolument cruciale. La mauvaise pénicilline a la même apparence que la bonne. Vous pouvez juger que votre tableur est mauvais, mais comment juger que votre logiciel de cryptographie est faible? Le texte chiffré produit par un chiffre faible paraît aussi bon que le texte chiffré produit par un chiffre résistant. Il y a beaucoup de poudre de perlimpinpin là-dedans. Beaucoup de remèdes de charlatan. Contrairement aux colporteurs d'élixirs de charlatans, ces programmeurs de logiciels ne savent habituellement même pas que leur truc est de la poudre de perlimpinpin. Ils sont peut-être de bons ingénieurs informaticiens, mais ils n'ont habituellement même pas lu d'ouvrages universitaires de cryptographie. Mais ils croient quand même qu'ils peuvent écrire de bons logiciels de cryptographie. Et pourquoi pas? Après tout, cela semble intuitivement facile à faire. Et leurs logiciels semblent bien marcher.

Quiconque croit avoir inventé un schéma de chiffrement incassable est, soit un véritable génie, soit un naïf inexpérimenté. Malheureusement, j'ai quelquefois affaire à ces prétendus cryptographes qui veulent apporter des "améliorations" à PGP en lui ajoutant des chiffres de leur cru.

Je me souviens d'une conversation avec Brian Snow, un cryptographe de haut rang de la NSA. Il me dit qu'il ne ferait jamais confiance à un chiffre conçu par quelqu'un qui ne s'était pas "fait les os" en passant d'abord beaucoup de temps à casser des codes. Cela tombait sous le sens. J'observai que pratiquement personne dans le monde de la cryptographie commerciale n'était qualifié selon ce critère. "Oui", répondit-il avec un sourire entendu, "Et cela rend notre travail à la NSA tellement plus facile." Une réflexion à vous glacer le sang. Je n'en aurais pas jugé autrement.

Le Gouvernement américain a également colporté la poudre de perlimpinpin. Après la Seconde Guerre mondiale, les USA vendirent les machines à chiffrer allemandes Enigma aux gouvernements du Tiers monde. Mais ils ne leur dirent pas que les Alliés avait cassé le code Enigma pendant la guerre, un fait qui resta classé secret défense pendant de nombreuses années. Aujourd'hui encore, de nombreux systèmes Unix dans le monde entier utilisent le chiffre d'Enigma pour le chiffrement de fichiers, en partie parce que le Gouvernement a dressé des obstacles légaux contre l'utilisation de meilleurs chiffres. Ils essayèrent même d'empêcher la publication initiale de l'algorithme RSA en 1977. Et ils ont étouffé dans l'œuf toutes les tentatives [de l'industrie] pour développer des téléphones réellement sécurisés pour le grand public.

La principale activité de la NSA (National Security Agency) du Gouvernement américain consiste à recueillir des renseignements, principalement en enregistrant secrètement les communications privées des gens (voir le livre de James Bamford, *The Puzzle Palace*). La NSA a accumulé des compétences et des ressources considérables pour casser des codes. Quand les gens ne peuvent pas disposer de bonne cryptographie pour se protéger, cela rend le travail de la NSA plus facile. La NSA a également pour mission d'approuver et de recommander des chiffres. Des critiques soutiennent que c'est une source de conflits d'intérêts, comme mettre le renard à garder le poulailler. La NSA a poussé en avant un chiffre conventionnel qu'elle avait conçu (le COMSEC Endorsement Program), et elle ne dira à personne comment il fonctionne parce que c'est classé secret défense. Elle veut qu'on lui fasse confiance et qu'on l'utilise. Mais n'importe quel cryptographe vous dira qu'un chiffre bien conçu n'a pas à être classé secret défense pour rester sûr. Seules les clés auraient besoin de protection. Comment fait-on pour savoir vraiment si le chiffre classé secret défense de la NSA est sûr? Il n'est pas difficile pour la NSA de concevoir un chiffre qu'elle seule peut craquer, si personne ne peut examiner le chiffre.

Il y a trois facteurs principaux qui ont miné la qualité des logiciels commerciaux de cryptographie aux Etats-Unis.

- Le premier est le manque virtuellement universel de compétence des programmeurs de logiciels commerciaux de cryptographie (quoique cela commence à changer depuis la sortie de PGP). Chaque ingénieur informaticien se prend pour un cryptographe, ce qui a conduit à la prolifération de logiciels de crypto vraiment mauvais.

- Le second est que la NSA a délibérément et systématiquement éliminé toutes les bonnes technologies commerciales de chiffrement, par l'intimidation légale et la pression économique. Une partie de cette pression a été portée à son maximum par les rigoureux contrôles à l'exportation sur les logiciels de cryptographie ce qui, vu l'aspect financier du marketing logiciel, a eu pour résultat d'éliminer les logiciels de chiffrement domestiques.
- La troisième méthode d'élimination consiste à concéder tous les brevets portant sur tous les algorithmes de chiffrement à clé publique à une seule société, constituant un goulot d'étranglement pour empêcher l'extension de cette technologie (cependant le monopole de cette concession est tombé fin 1995).

Le résultat tangible de tout cela est qu'avant la sortie de PGP, il n'y avait presque pas de logiciels de chiffrement de haute sécurité disponibles aux USA. Je ne suis pas aussi certain de la sécurité de PGP que je l'étais autrefois de celle de mon génial logiciel de chiffrement du collègue. Si je l'étais, ce serait mauvais signe. Mais je suis à peu près sûr que PGP ne contient pas de faiblesses manifestes (bien qu'il puisse contenir des bogues). J'ai choisi les meilleurs chiffres publiés dans les milieux de la cryptographie universitaire civile. Pour la plupart, ces chiffres ont fait individuellement l'objet d'un examen approfondi étendu. Je connais beaucoup des cryptographes d'autorité mondiale, et j'ai beaucoup discuté avec certains d'entre eux des chiffres et des protocoles utilisés par PGP. Il est bien étudié, et cela a pris des années pour le réaliser. Et je ne travaille pas pour la NSA. Mais vous n'avez pas à me croire sur parole au sujet de l'intégrité cryptographique de PGP, parce que le code source est disponible pour faciliter son examen approfondi.

Encore une chose au sujet de mon engagement en faveur de la qualité cryptographique de PGP. Depuis qu'à l'origine j'ai développé et réalisé gratuitement PGP en 1991, j'ai fait l'objet pendant trois ans, d'une enquête judiciaire diligente à la requête des Douanes américaines sous la prévention d'avoir diffusé PGP à l'étranger, avec le risque de poursuites pénales et d'années d'emprisonnement. Par comparaison, vous n'avez pas vu le Gouvernement s'émouvoir à propos d'autres logiciels cryptographiques – c'est PGP qui les a rendus furieux. N'est-ce pas là un aveu quant à la puissance de PGP? J'ai bâti ma réputation sur l'intégrité cryptographique de mes produits. Je ne trahirai pas mon engagement en faveur de notre droit au respect de l'intimité, pour lequel j'ai risqué ma liberté. Je ne suis pas près de permettre à un produit portant mon nom d'être muni d'une quelconque porte cachée.

Vulnérabilités

“Si tous les ordinateurs personnels du monde – 260 millions – étaient mis à travailler sur un seul message chiffré avec PGP, cela prendrait encore un temps estimé à 12 millions de fois l'âge de l'univers, en moyenne, pour casser un simple message.”

– William Crowell, Directeur délégué, National Security Agency, 20 Mars 1997.

Aucun système de sécurité n'est impénétrable. PGP peut être circonvenu par une variété de biais. Dans tout système de sécurité de données, vous devez vous

interroger pour savoir si l'information que vous cherchez à protéger a plus de valeur pour l'attaquant que le coût de l'attaque. Cela devrait vous amener à vous protéger des attaques les moins coûteuses, tout en ne vous préoccupant pas des attaques plus onéreuses.

Des passages de la discussion qui suit peuvent paraître excessivement paranoïaques, mais une telle attitude est appropriée pour une discussion raisonnable des problèmes de vulnérabilité.

Phrase secrète et clé privée compromises

L'attaque probablement la plus simple intervient si vous laissez la phrase secrète de votre clé privée écrite quelque part. Si quelqu'un l'obtient et obtient aussi votre clé privée, il peut lire vos messages et faire des signatures en votre nom.

Voici quelques recommandations pour protéger votre phrase secrète:

1. N'utilisez pas de phrases secrètes évidentes qui peuvent être aisément devinées, comme les noms de vos enfants ou conjoint.
2. Utilisez des espaces et une combinaison de nombres et de lettres dans votre phrase secrète. Si vous ne mettez qu'un seul mot dans votre phrase secrète, elle peut être aisément devinée à l'aide d'un ordinateur qui essaie tous les mots d'un dictionnaire jusqu'à ce qu'il trouve votre mot de passe. C'est pourquoi une phrase secrète est bien meilleure qu'un mot de passe. Un attaquant plus sophistiqué peut fouiller avec son ordinateur un livre de citations connues pour trouver votre phrase secrète.
3. Soyez créatif. Utilisez une phrase secrète facile à mémoriser mais difficile à deviner; vous pouvez facilement en construire un en utilisant un dicton insensé ou une obscure citation littéraire.

La falsification de clé publique

Une vulnérabilité majeure existe si les clés publiques ont été falsifiées. Cela peut être une vulnérabilité d'une importance cruciale pour un cryptosystème à clé publique, en partie parce que la plupart des novices ne la reconnaissent pas immédiatement.

Pour résumer: quand vous utilisez une clé publique, assurez-vous qu'elle n'a pas été falsifiée. Une nouvelle clé publique ne devrait être digne de confiance que si vous l'obtenez directement de son propriétaire, ou si elle a été signée par quelqu'un en qui vous avez confiance. Assurez-vous que personne n'a pu falsifier votre propre clé publique. Maintenez un contrôle physique à la fois sur votre trousseau de clés publiques et votre clé privée, de préférence sur votre propre ordinateur personnel plutôt que sur un système distant et/ou partagé. Conservez une copie de sauvegarde de vos deux trousseaux de clés.

Fichiers pas tout à fait effacés

Un autre problème potentiel de sécurité vient de la façon dont la plupart des systèmes d'exploitation effacent les fichiers. Quand vous chiffrez un fichier puis

effacez le texte clair originel, le système d'exploitation ne détruit pas réellement les données. Il se contente de marquer ces secteurs du disque comme effacés, permettant à l'espace d'être réutilisé plus tard. C'est un peu comme de mettre des papiers sensibles dans la corbeille à papier plutôt que dans le broyeur. Les secteurs du disque contiennent encore les données sensibles originelles que vous vouliez détruire, et qui seront probablement effacées par de nouvelles données dans le futur. Si un attaquant lit ces blocs de fichier effacés peu de temps après qu'ils aient été retirés de l'espace alloué, il pourrait retrouver votre texte clair.

En fait, cela pourrait même arriver accidentellement, si quelque chose a mal fonctionné sur le disque et que des fichiers ont été accidentellement effacés ou corrompus. Un programme de récupération de disque peut être lancé pour récupérer les fichiers endommagés, mais cela signifie souvent que des fichiers précédemment effacés sont ressuscités en même temps que tout le reste. Vos fichiers confidentiels que vous pensiez partis à jamais peuvent ensuite réapparaître et être inspectés par quiconque tente de récupérer votre disque endommagé. Même pendant que vous créez le message originel avec un traitement de texte ou un éditeur de texte, l'éditeur peut créer de multiples copies temporaires de votre texte sur le disque, uniquement pour son fonctionnement interne. Ces copies temporaires de votre texte sont effacées par le traitement de texte une fois le travail effectué, mais ces fragments sensibles sont encore quelque part sur votre disque.

La seule façon d'empêcher le texte clair de réapparaître est de provoquer d'une façon ou d'une autre l'écrasement par écriture des textes clairs effacés. A moins que vous teniez pour sûr le fait que tous les secteurs de disque effacés seront bientôt réutilisés, vous devez prendre des dispositions positives pour écrire par-dessus le texte clair, et aussi tout fragment du texte clair laissé sur le disque par votre traitement de texte. Vous pouvez vous occuper de tout fragment du texte clair laissé sur le disque en utilisant les fonctions de nettoyage sécurisé et de nettoyage de l'espace libre de PGP.

Virus et chevaux de Troie

Une autre attaque pourrait impliquer un virus informatique spécialement ajusté ou un "ver" qui pourrait infecter PGP ou votre système d'exploitation. Cet hypothétique virus pourrait être conçu pour capturer votre phrase secrète ou votre clé privée ou vos messages déchiffrés, et pour écrire à la dérobée dans un fichier l'information capturée ou l'envoyer à travers un réseau au propriétaire du virus. Ou il pourrait altérer le comportement de PGP de telle sorte que les signatures ne soient pas convenablement vérifiées. Cette attaque est moins coûteuse qu'une attaque cryptanalytique.

Se défendre contre ce type d'attaque tombe dans la catégorie de la défense contre les infections virales en général. Il y a des produits commerciaux relativement capables qui sont disponibles, et il y a des procédures prophylactiques à suivre qui peuvent réduire grandement les risques d'une infection virale. Un traitement complet de contre-mesures antivirales et anti vers sort du cadre de ce document. PGP n'a pas de défenses contre les virus, et présume que votre propre ordinateur personnel est un environnement d'exécution digne de confiance. Si un tel virus ou

un ver apparaissait réellement, avec un peu de chance le monde serait aussitôt au courant.

Une attaque similaire implique quelqu'un créant une habile imitation de PGP qui se comporte comme PGP à bien des égards, mais qui ne marche pas de la façon dont il est supposé le faire. Par exemple, il pourrait être délibérément mutilé pour ne pas vérifier les signatures correctement, permettant à de fausses clés d'être acceptées. Cette version *cheval de Troie* de PGP n'est pas difficile à créer pour un attaquant, parce que le code source de PGP est largement disponible, aussi n'importe qui pourrait modifier le code source et produire un zombie lobotomisé imité de PGP qui ait l'air conforme mais qui répond aux ordres de ses maîtres diaboliques. Cette version cheval de Troie de PGP pourrait ensuite être largement distribuée, se déclarant provenir d'une source légitime. Comme c'est insidieux.

Vous devriez faire un effort pour obtenir votre copie de PGP directement de Network Associates, Inc.

Il y a d'autres façons de vérifier si PGP a été falsifié, en utilisant des signatures numériques. Vous pourriez utiliser une autre version digne de confiance de PGP pour vérifier la signature sur une version suspecte de PGP. Mais cela n'aidera pas du tout si votre système d'exploitation est infecté, ni ne le détectera si votre copie originale de `pgp.exe` a été malicieusement altérée d'une façon ou d'une autre pour altérer sa propre capacité à vérifier les signatures. Ce test présume aussi que vous avez une bonne copie fiable de la clé publique que vous utilisez pour vérifier la signature de l'exécutable de PGP.

Fichiers d'échange et/ou mémoire virtuelle

PGP a été développé à l'origine pour MS-DOS, un système d'exploitation primitif par rapport aux normes actuelles. Mais alors qu'il était porté vers d'autres systèmes d'exploitation plus complexes, comme Microsoft Windows et Macintosh OS, une nouvelle vulnérabilité a émergé. Cette vulnérabilité découle du fait que ces systèmes d'exploitation de connaisseurs utilisent une technique appelée *mémoire virtuelle*.

La mémoire virtuelle vous permet de lancer d'énormes programmes sur votre ordinateur qui sont plus gros que l'espace disponible dans le microprocesseur de la mémoire vive de votre ordinateur. Cela est pratique parce que les logiciels sont devenus de plus en plus hypertrophiés depuis que les interfaces graphiques adaptées à l'utilisateur sont devenues la norme et que les utilisateurs ont commencé à lancer de nombreuses grosses applications en même temps. Le système d'exploitation utilise le disque dur pour stocker des portions du logiciel qui ne sont pas utilisées à ce moment. Cela signifie que le système d'exploitation pourrait, sans que vous le sachiez, recopier sur le disque des choses dont vous pensiez qu'elle resteraient seulement en mémoire – des choses comme des clés, des phrases secrètes, et du texte déchiffré. PGP ne garde pas cette sorte de données sensibles exposées en mémoire plus longtemps que nécessaire, mais il y a de toute façon un risque que le système d'exploitation les copie sur le disque.

Les données sont copiées dans l'espace mémoire du disque, appelé *fichier d'échange* (ou de swap). Les données sont relues depuis ce fichier d'échange dès que c'est nécessaire, de telle sorte que seule une partie de votre programme ou de vos données est physiquement en mémoire à un moment précis. Toute cette

activité est invisible pour l'utilisateur, qui voit juste le disque en train de mouliner. Microsoft Windows échange des segments de mémoire, appelés pages, en utilisant un algorithme de remplacement de page appelé "Least Recently Used" (LRU). Cela signifie que les pages qui n'ont pas été consultées depuis le plus longtemps sont les premières à être échangées vers le disque. Cette approche suggère que dans la plupart des cas le risque sera relativement faible que des données sensibles soient échangées vers le disque, parce que PGP ne les laisse pas en mémoire très longtemps. Mais nous ne garantissons rien.

Le fichier d'échange peut être consulté par quiconque peut obtenir un accès physique à votre ordinateur. Si vous êtes concernés par ce problème, vous pouvez le résoudre en récupérant un logiciel spécial qui écrit par-dessus votre fichier d'échange. Un autre remède possible est de désactiver la fonction mémoire virtuelle de votre système d'exploitation. Microsoft Windows le permet, ainsi que Mac OS. Désactiver la mémoire virtuelle peut vouloir dire que vous aurez besoin de plus de mémoire physique sous forme de barrettes de RAM installée, afin de tout gérer dans la RAM.

Brèche dans la sécurité physique

Une brèche dans la sécurité physique peut permettre à quelqu'un de recueillir physiquement vos textes clairs ou vos messages imprimés. Un adversaire déterminé pourrait accomplir cela par le cambriolage, le tri des poubelles, les fouilles et saisies illégales, ou la corruption, l'ouverture du courrier, ou l'infiltration de votre équipe. Certaines de ces attaques peuvent être spécialement réalisables contre les organisations politiques de base qui dépendent dans une large mesure de volontaires.

Ne vous endormez pas dans une fausse sécurité uniquement parce que vous avez un outil cryptographique. Les techniques cryptographiques ne protègent les données que lorsqu'elles sont chiffrées – une violation directe de la sécurité physique peut encore compromettre les données en clair ou les informations écrites ou orales.

Ce type d'attaque est moins coûteux qu'une attaque cryptanalytique sur PGP.

Les attaques Tempest

Une autre sorte d'attaque qui a été utilisée par des adversaire bien équipés implique la détection à distance des signaux électromagnétiques [émis par] votre ordinateur. Cette coûteuse et parfois laborieuse attaque est probablement toujours moins coûteuse que l'attaque cryptanalytique directe. Une camionnette équipée des instruments appropriés se gare près de votre bureau et capture à distance toutes les frappes du clavier et les messages affichés sur l'écran vidéo de votre ordinateur. Cela compromettrait tous vos mots de passes, messages, etc. Cette attaque peut être contrecarrée en protégeant correctement votre équipement informatique et câblage de réseau de telle sorte qu'ils n'émettent pas ces signaux. Cette technologie de protection, appelée "Tempest," est utilisée par certaines agences gouvernementales et entreprises travaillant avec la Défense Nationale. Il y a des vendeurs d'équipements qui proposent ces boucliers Tempest.

Quelques versions récentes de PGP (postérieures à la version 6.0) peuvent afficher le texte clair déchiffré en utilisant une police spécialement conçue qui peut réduire le niveau d'émission radio de l'écran de votre moniteur. Cela peut rendre plus difficile la capture des signaux à distance. Cette police spéciale est disponible dans quelques versions de PGP qui gèrent le dispositif "Secure Viewer".

Se protéger contre les fausses empreintes de date

Une vulnérabilité quelque peu obscure de PGP implique que des utilisateurs malhonnêtes créent de fausses empreintes de date sur leurs propres copies de clés publiques et signatures. Vous pouvez sauter cette partie si vous êtes un utilisateur occasionnel et n'êtes pas versé dans les obscurs protocoles de clés publiques.

Il n'y a rien à faire pour empêcher un utilisateur malhonnête de modifier les réglages de date et d'heure de l'horloge système [de son ordinateur], et de générer ses propres clés publiques et signature qui paraissent avoir été créées à une époque différente. Il peut feindre d'avoir signé quelque chose plus tôt ou plus tard qu'il ne le prétend, ou bien que sa paire de clés publique/privée a été créée plus tôt ou plus tard. Il peut y avoir des avantages juridiques ou financiers pour lui, par exemple en créant un ensemble d'échappatoires qui pourrait lui permettre de répudier sa signature.

Je pense que ce problème de la falsification de l'empreinte de date dans les signatures numériques n'est pas pire qu'il n'est déjà dans les signatures manuscrites. N'importe qui peut écrire n'importe quelle date à côté de sa signature manuscrite sur un contrat, mais personne ne semble s'alarmer de cet état de choses. Dans certains cas, une date "incorrecte" sur une signature manuscrite pourrait ne pas être associée avec la fraude en question. L'empreinte de date pourrait être celle du moment où le signataire déclare qu'il a signé le document, ou peut-être celle à laquelle il veut que la signature prenne effet.

Dans les situations où il est d'importance critique qu'une signature soit authentifiée pour une date véritable, les gens peuvent simplement utiliser des notaires pour attester et dater une signature manuscrite. L'équivalent dans les signatures numériques est d'avoir un tiers vraiment digne de confiance pour signer un certificat de signature, appliquant une empreinte de date fiable. Des protocoles exotiques ou trop formels ne sont pas nécessaires pour cela. Des signatures témoins ont été reconnues depuis longtemps comme un moyen légitime de déterminer l'époque à laquelle un document a été signé.

Une Autorité Certifiante inspirant une large confiance ou un notaire pourraient créer des signatures notariales avec une empreinte de date fiable. Cela ne requerrait pas nécessairement une autorité centralisée. Peut-être que des avals de confiance ou des tiers désintéressés pourraient assurer cette fonction, comme le font les vrais notaires. Quand un notaire signe les signatures d'autres personnes, il crée un certificat de signature d'un certificat de signature. Cela servirait de certification de la signature de la même façon que les notaires réels certifient aujourd'hui des signatures manuscrites. Le notaire pourrait déposer le certificat de signature détaché (sans la totalité du document qui a été signé) dans un registre spécial contrôlé par le notaire. N'importe qui pourrait lire ce registre. La signature du notaire aurait une empreinte de date digne de confiance, ce qui aurait une plus

grande crédibilité ou de signification légale que l’empreinte de date dans la signature originale.

Il y a une bonne analyse de ces questions dans l’article de Denning de 1983 dans IEEE Computer. Les futures améliorations de PGP pourraient inclure des fonctionnalités pour gérer facilement les signatures notariées de signatures, avec des empreintes de date fiables.

Divulgence sur des systèmes multi utilisateurs

PGP a été conçu à l’origine pour un système mono utilisateur sous votre contrôle physique direct. Si vous lancez PGP à la maison sur votre propre PC, vos fichiers chiffrés sont généralement sûrs, à moins que quelqu’un pénètre par effraction chez vous, vole votre PC et vous persuade de lui donner votre phrase secrète (ou que votre phrase secrète soit assez facile à deviner).

PGP n’est pas conçu pour protéger vos données alors qu’elles sont sous une forme lisible sur un système compromis. Il ne peut pas non plus empêcher un intrus d’utiliser des moyens sophistiqués pour lire votre clé privée pendant qu’elle est utilisée. Vous devrez reconnaître ces risques sur les systèmes multi utilisateurs, et adapter vos habitudes en conséquence. Peut-être que votre situation est telle que vous devriez envisager de ne lancer PGP que sur un système isolé et mono utilisateur sous votre contrôle physique direct.

Analyse de trafic

Même si l’attaquant ne peut pas lire le contenu de vos messages chiffrés, il peut en déduire au moins des informations utiles en observant d’où viennent les messages et où ils vont, la taille des messages, et le moment de la journée où les messages sont envoyés. Pour l’attaquant, c’est comme examiner votre facture de téléphone pour voir qui vous appelez, quand et pour combien de temps, quand bien même le contenu actuel de vos appels lui demeure inconnu. Cela s’appelle l’analyse de trafic. PGP seul ne protège pas contre l’analyse de trafic. Résoudre ce problème requerrait des protocoles de communication spécialement conçus pour réduire l’exposition à l’analyse de trafic dans votre environnement de communication, éventuellement avec une assistance cryptographique.

Cryptanalyse

Une coûteuse et formidable attaque cryptanalytique pourrait éventuellement être montée par quelqu’un avec les ressources d’énormes super calculateurs, comme les agences de renseignement gouvernementales. Ils pourraient craquer votre clé publique en utilisant une quelconque nouvelle percée mathématique. Mais la [recherche] universitaire civile a intensément attaqué la cryptographie à clé publique sans succès depuis 1978.

Peut-être que le gouvernement possède des méthodes classées top secret de craquage des chiffres conventionnels utilisés dans PGP. C’est le pire cauchemar de tout cryptographe. Il ne peut pas y avoir de garanties absolues de sécurité dans les réalisations cryptographiques pratiques.

Tout de même, l'optimisme semble justifié. Les algorithmes de clé publique, les algorithmes de contraction de message, et les chiffres par blocs utilisés dans PGP ont été conçus par les meilleurs cryptographes du monde. Les chiffres de PGP ont subi des analyses de sécurité approfondies et des examens méticuleux de la part des meilleurs cryptographes dans le monde non classé top secret.

En outre, même si les chiffres par blocs utilisés dans PGP ont certaines faiblesses subtiles inconnues, PGP compresse le texte clair avant le chiffrement, ce qui devrait réduire considérablement ces faiblesses. Le temps de calcul pour le craquer revient largement plus cher que la valeur du message.

Si votre situation justifie de s'inquiéter d'attaques vraiment formidables de ce calibre, alors peut-être devriez-vous contacter un consultant en sécurité des données pour des approches sur mesure de la sécurité des données qui soit adaptée à vos besoins particuliers.

Pour résumer, sans une bonne protection cryptographique de vos communications de données, il peut être facile en pratique et peut-être même banal pour un adversaire d'intercepter vos messages, particulièrement ceux envoyés par un modem ou un système e-mail. Si vous utilisez PGP et prenez des précautions raisonnables, l'attaquant aura à dépenser nettement plus d'efforts et d'argent pour violer votre vie privée.

Si vous vous protégez par vous-même des attaques les plus simples, et que vous estimez que votre intimité ne va pas être violée par un attaquant déterminé et doté de grandes ressources, alors vous serez probablement en sécurité en utilisant PGP. PGP vous donne une Assez Bonne Confidentialité [en anglais: *Pretty Good Privacy*].

Glossaire

ASCII-armored text [texte avec armure ASCII]	Information binaire qui a été encodée dans un jeu de caractères 7 bits ASCII standard, imprimable, pour faciliter son transport à travers des systèmes de communication. Dans PGP, les fichiers munis d'une armure texte ASCII se voient attribuer l'extension par défaut, et ils sont encodés et décodés au format ASCII radix-64.
authentication [authentification]	La détermination de l'origine d'une information cryptée via la vérification d'une signature numérique ou d'une clé publique en vérifiant son empreinte unique.
certify [certifier ou avaliser]	Signer une clé publique.
certifying authority [autorité certifiante]	Une ou plusieurs personnes de confiance à qui est confiée la responsabilité de certifier l'origine des clés et de les ajouter à une base de données commune.
cyphertext [texte chiffré ou crypté, ou cryptogramme]	Texte clair converti en format illisible par l'utilisation d'un algorithme de cryptage. Une clé de cryptage peut retrouver le texte clair originel à partir du texte chiffré.
conventional encryption [cryptage conventionnel]	Cryptage fondé sur une phrase secrète commune au lieu de la cryptographie à clé publique. Le fichier est crypté à l'aide d'une clé de session, qui crypte en utilisant une phrase secrète que vous serez invité à choisir.
decryption [décryptage]	Une méthode de décryptage de l'information cryptée de sorte qu'elle redevienne lisible. La clé privée du destinataire est utilisée pour le décryptage.
digital signature [signature numérique]	Voir signature.
encryption [cryptage]	Une méthode de brouillage de l'information pour la rendre illisible à n'importe qui excepté le destinataire prévu, qui doit la décrypter pour la lire.
fingerprint [empreinte numérique]	Une série unique de chiffres et de caractères d'identification utilisés pour authentifier les clés publiques. C'est le principal moyen de vérifier l'authenticité d'une clé. Voir Key Fingerprint.
introducer [aval ou certificateur]	Une personne ou une organisation qui est autorisée à garantir l'authenticité d'une clé publique. Vous désignez un aval en signant sa clé publique.
key [clé ou certificat]	Un code numérique utilisé pour crypter et signer ou décrypter et vérifier messages et fichiers. Les clés se présentent sous forme de paire de clés et sont conservées dans des trousseaux.

key escrow
[séquestre de clés]

Une pratique consistant pour l'utilisateur d'un système de cryptographie à clé publique à remettre ses clés privées à des tiers pour leur permettre ainsi de surveiller les communications cryptées.

key fingerprint
[empreinte de clé]

Une série unique de chiffres et de caractères d'identification utilisés pour authentifier les clés publiques. Par exemple, vous pouvez téléphoner au propriétaire de la clé publique pour qu'il vous lise l'empreinte numérique associée à sa clé, de sorte que vous puissiez la comparer à celle de votre copie de sa clé publique pour vous assurer qu'elles correspondent. Si l'empreinte ne correspond pas, alors vous détenez une clé contrefaite.

key ID
[clé ID ou identificateur de clé]

Un code lisible qui identifie de manière unique une paire de clés. Deux paires de clés peuvent avoir le même ID d'utilisateur, mais elles auront des clés ID différents.

key pair
[paire de clés]

Une clé publique et sa clé privée correspondante. Dans les cryptosystèmes à clé publique, comme PGP, chaque utilisateur possède au moins une paire de clés.

keyring
[trousseau]

Un jeu de clés. Chaque utilisateur possède deux types de trousseaux: un trousseau privé et un trousseau public.

key splitting or "secret sharing"
[scission de clé ou "secret partagé"]

Le processus consistant à scinder une clé privée en plusieurs segments, et à répartir ces segments entre un groupe de personnes. Un nombre déterminé d'entre elles doivent réunir leurs segments pour utiliser la clé.

message digest
[empreinte ou contraction de message]

Un "résumé" ramassé d'un message ou d'une somme de contrôle de fichier. Il représente votre message de telle sorte que si le message était altéré en quelque façon, un résumé différent en serait calculé.

meta-introducer
[méta-aval]

Un aval de confiance d'aval de confiance.

passphrase
[phrase secrète]

Une série de frappes qui permettent l'accès exclusif à votre clé privée que vous employez pour signer et pour décrypter des messages et des fichiers attachés.

plaintext
[texte clair ou libellé]

Texte normal, lisible, non crypté, non signé.

private key
[clé privée]

La partie secrète d'une paire de clés utilisée pour signer et décrypter l'information. Une clé privée d'un utilisateur devrait être gardée secrète, connue seulement de l'utilisateur.

private keyring
[trousseau privé]

Un jeu d'une ou plusieurs clés privées, qui appartiennent toutes au propriétaire du trousseau privé.

public key
[clé publique]

Une des deux clés d'une paire de clés, utilisée pour crypter l'information ou vérifier des signatures. Une clé publique peut être largement diffusée à des collègues ou à des tiers. Connaître la clé publique d'une personne n'aide pas à découvrir la clé privée correspondante.

public keyring [trousseau public]	Un jeu de clés publiques. Votre trousseau public inclut vos propres clés publiques.
public-key cryptography [cryptographie à clé publique]	Cryptographie dans laquelle on utilise une clé publique et une clé privée, et qui ne nécessite pas de canal lui-même sécurisé.
Secret sharing [secret partagé]	Voir Key Splitting.
sign [signer]	Apposer une signature.
signature	Un code numérique créé avec une clé privée. Les signatures permettent l'authentification de l'information via la vérification de signature. Quand vous signez un message ou un fichier, PGP utilise votre clé privée pour créer un code numérique unique qui procède à la fois du contenu du message et de votre clé privée. N'importe qui peut utiliser votre clé publique pour vérifier votre signature.
Subkey [sous-clé]	Une sous-clé est une clé de cryptage Diffie-Hellman qui est ajoutée comme un sous ensemble à votre clé principale. Une fois qu'une sous-clé est créée, elle peut expirer ou être révoquée sans affecter votre clé principale ou les signatures qui y sont attachées.
text	Du texte 7 bits ASCII standard, imprimable.
trusted [fiable]	Une clé publique est dite avalisée par vous si elle a été certifiée par vous-même ou par quelqu'un que vous avez désigné comme aval.
trusted introducer [aval de confiance]	Quelqu'un en qui vous avez confiance pour vous fournir des clés valides. Quand un aval de confiance signe des clés, vous vous fiez à lui quant à leur validité, et vous n'avez pas besoin de vérifier les clés [qu'il a signées] avant de les utiliser.
user ID [identifiant (ou ID) d'utilisateur]	Une expression qui identifie une paire de clés. Par exemple, un format commun pour un identifiant d'utilisateur est le nom du propriétaire et son adresse e-mail. L'ID d'utilisateur aide les utilisateurs (aussi bien le propriétaire que les collègues) à identifier le propriétaire de la paire de clés.
verification	L'acte de comparer une signature créée avec une clé privée à l'aide de sa clé publique. La vérification prouve que l'information provient effectivement du signataire, et que le message n'a ensuite été altéré par personne.
web of trust [Toile d'araignée (ou réseau) de confiance]	Un modèle de confiance distribuée utilisé par PGP pour valider l'appartenance d'une clé publique, dans lequel le niveau de confiance est cumulatif, basé sur les connaissances individuelles des avals.

Index

A

- accorder sa confiance
 - pour valider des clés 84
- activer (propriété) 78
- activer des clés 84
- adresse
 - ajouter une à une clé existante 32, 79
- ajouter un ID photographique 33
- aléatoires
 - fichier de semence 91, 135
 - générer des données 32, 104
 - nombres utilisés comme clés de session 135
- analyse de trafic, attaques 152
- aperçu
 - clés privées 15
 - notion de clé 27
 - trousseaux 15
- assistance technique
 - adresse e-mail 9
 - en ligne 9
 - informations requises de l'utilisateur 10
- attaquants
 - protection contre les 39, 136, 139
- attaques
 - analyse de trafic 152
 - brèche dans la sécurité physique 150
 - chevaux de Troie 148
 - cryptanalyse 152
 - fichiers d'échange 69, 149
 - mémoire virtuelle 149
 - personne interposée 45
 - Tempest 150
 - virus 148
- attributs des clés
 - changer 73 à 78

- voir 73 à 78
- automatique
 - fermeture des volumes 111
 - ouverture des volumes 112
- automatique (préférences)
 - fermeture après n minutes d'inactivité 111
 - fermeture si mise en veille 111
- Autorité Certifiante
 - description 137
- avals 137
 - de confiance 137, 139
 - description 137
 - et signatures numériques 138, 151

B

- barre d'outils de PGPkeys
 - description des icônes 23
- brèche dans la sécurité physique
 - description 150

C

- CAST 133
 - taille de clé 133
- CBC 133
- certificat de révocation de clé
 - émission 142
- certificateurs *Voir* avals
- certification
 - de clés publiques 16, 137
- CFB 133
- changer
 - votre phrase secrète 78, 85
- changer la phrase secrète (propriété) 78
- chevaux de Troie 148
- chiffrement *Voir* cryptage
- chiffrer *Voir* crypter

- chiffres par blocs 133
- cipher block chaining 133
- cipher feedback 133
- clés
 - accorder sa confiance pour valider 84
 - ajouter un ID photographique 33
 - créer 28
 - définir la taille 30, 36
 - désactiver 84
 - déterminer l'aloi 45
 - distribuer 40
 - effacer 85
 - effacer d'un serveur 41
 - examiner 20
 - exporter vers un fichier 87
 - gérer 73
 - localiser 98
 - notion 27
 - protéger 39, 141
 - réapparition sur serveur 42
 - rechercher 98
 - révoquer 87
 - sauvegarder 39
 - scission 36
 - signer 81
 - trouver 98
 - vérifier l'authenticité 45
 - vérifier les empreintes 80
- clés par défaut
 - spécifier 79
- clés privées
 - aperçu 15
 - compromises 147
 - création 16
 - avec PGP Key Generation Wizard 20
 - emplacement 73, 91
 - protection 39
 - de la divulgation 141
 - stocker 39
 - visualiser 20
- clés publiques
 - avantage à les mettre sur un serveur 40
 - avantages de l'envoi au serveur 32
 - certifier 16, 137
 - copier depuis un e-mail 44
 - création 16
 - avec PGP Key Generation Wizard 20
 - distribuer 40
 - distribuer à autrui 16
 - échanger avec autrui 16
 - emplacement 73, 91
 - envoi sur serveur de clés 32
 - envoi sur un serveur de clés 40
 - exporter dans un fichier 43
 - falsification 147
 - importer depuis un fichier 45
 - inclure dans un e-mail 42
 - obtenir d'autrui 43 à 45, 43 à 45
 - protection 39, 136, 139
 - récupérer depuis un serveur 43
 - signer 81, 137
 - stocker 39
 - valider 16
 - visualiser 20
- Clipper (puce) 131
- comparer
 - l'empreinte 46
- compression de données
 - routines 134
- confiance 137
 - accorder pour valider des clés 84
- contraction de message, description 135
- créer
 - des sous-clés 35
 - la paire de clés privée et publique 20
 - un groupe (liste de distribution) 54
 - une paire de clés 28
 - régler les préférences 89
- créer un volume PGPdisk 103
- Crowell, William 146
- cryptage
 - régler les préférences 88

- cryptage (options)
 - e-mail
 - conventionnel 51
 - fichiers
 - conventionnel 60, 62
 - Secure Viewer 60
 - text output 60, 62
 - wipe original 60, 62
 - cryptage conventionnel 51, 53, 60, 62
 - crypter
 - depuis le presse-papiers 19
 - e-mail 16, 17, 49
 - groupes de destinataires 53
 - en utilisant Eudora 49
- D**
- déchiffrement *Voir* décryptage
 - déchiffrer *Voir* décrypter
 - décrypter
 - avec une clé scindée 37, 39, 64, 78, 86
 - depuis le presse-papiers 19
 - e-mail 17, 55
 - en utilisant PGPtools 64
 - en utilisant PGPtray 63
 - fichiers 63
 - département clients
 - contacter 9
 - DES 133
 - désactiver des clés 84
 - Diffie-Hellman/DSS
 - créer des clés 30
 - Digital Telephony bill 130
 - disques
 - effacer l'espace libre 70
 - effacer un fichier du 69
 - nettoyer l'espace libre 70
 - divulgaration
 - protéger les clés secrètes de la 141
- E**
- échanger
 - des clés publiques 16
 - obtenir celles d'autrui 16, 43
 - des volumes PGPdisk 113
 - votre clé publique 40
 - effacer
 - avec PGP Wipe 17, 69
 - des clés 85
 - des fichiers 17, 69
 - des ID d'utilisateur 85
 - des listes de distribution 54
 - des signatures 85
 - des signatures d'un serveur 41
 - une clé d'un serveur 41
 - e-mail
 - ajouter une clé publique depuis un 44
 - ajouter une nouvelle adresse 32, 79
 - créer des groupes de destinataires 53
 - crypter 16, 49
 - avec Eudora 49
 - pour des groupes de destinataires 53
 - décrypter 17, 55
 - effacer des groupes de destinataires 54
 - inclure votre clé publique dans un 42
 - privé (envoyer) 49
 - privé (recevoir) 49
 - signer 16, 49
 - avec Eudora 49
 - utiliser les plug-ins 49
 - utiliser PGP avec des applications 21
 - vérifier 17, 55
 - emplacement d'un volume
 - spécifier 103
 - empreinte (propriété) 78
 - empreintes
 - comparer 46
 - description 135
 - vérifier 80
 - Enigma 145
 - Eudora
 - avec PGP/MIME 55
 - sans PGP/MIME 56

expiration (date)

- fixer pour une paire de clés 31
- propriété 76

Explorateur Windows

- utiliser PGP depuis 22

exportation (format) 98

exporter

- une clé vers un fichier 43, 87

F

fichiers 63

- déterminer l'emplacement de vos trousseaux 91
- effacer 69
- exporter des clés publiques vers un 43
- exporter des clés vers un 87
- importer des clés publiques depuis un 45
- nettoyer 69

fonctionnalités

- de PGPdisk 101

Free Space Wiper 70

G

général (propriété) 77

groupes

- créer 54
- effacer 54

H

hachage (fonction de), description 135

I

icônes (description des) 23

ID d'utilisateur

- d'une clé publique (vérifier) 138

ID photographique, ajouter 33

IDEA 133 à 34

- taille de clé 133 à 34

importer

- des clés publiques depuis un fichier 45

K

Key ID (propriété) 77

Key Type (propriété) 77

L

listes de distribution

- créer 54
- effacer 54

N

Network Associates

- formation 10
- service clients 9

nom d'utilisateur

- ajouter 32, 79

nommer le volume 103

nouveau volume PGPdisk 103

nouvelle adresse e-mail

- ajouter 32, 79

NSA 131

O

obtenir

- les clés publiques d'autrui 43

ouvrir

- la fenêtre de PGPkeys 20

ouvrir des volumes 109, 113

- automatiquement 112
- sur un serveur distant 112

P

paire de clés

- créer 16, 28 à 32
- créer avec le PGP Key Wizard 20
- description de la 28
- examiner 20
- fixer une date d'expiration 31
- par défaut 79
- scission 36

PGP

- chiffres symétriques 133

- depuis des applications e-mail gérées 21
 - façons d'utiliser 19
 - lancer 19
 - réactions 10
 - utiliser depuis la barre des tâches 19
 - utiliser depuis le presse-papiers 19
 - utiliser depuis PGPtools 21
 - vulnérabilités 146
 - PGP Free Space Wiper 70
 - PGP Key Generation Wizard 20, 28
 - PGP/MIME (standard) 21
 - crypter 49
 - décrypter 55
 - PGPdisk 101 à 17
 - algorithme de chiffrement 114
 - échanger des volumes 113
 - enchâsser des volumes 114
 - fonctionnalités 101
 - précautions de sécurité 116
 - sauvegarder des volumes 112
 - spécifier les préférences 111
 - PGPdisk volume
 - fermer 110
 - fermer automatiquement 111
 - ouvrir 109
 - PGPkeys
 - attribut Size 75
 - attribut Trust 76
 - attribut Validity 75
 - Creation (date) 76
 - créer une paire de clés avec 28 à 32
 - description 74
 - examiner les propriétés 76
 - Change Passphrase 78
 - Enabled 78
 - Expires 77
 - Fingerprint 78
 - Key ID 77
 - Key Type 77
 - Trust Model 78
 - icônes de 23
 - ouvrir 20
 - utilisation 73
 - PGPtools
 - utiliser 61, 64
 - utiliser PGP depuis 22
 - utiliser PGP Free Space Wiper 70
 - utiliser PGP Wipe 69
 - PGPtray
 - lancer 19
 - quitter 20
 - utiliser 19, 63
 - utiliser pour décrypter 63
 - Phil Zimmermann 129
 - phrase secrète
 - Change Passphrase (propriété) 78
 - changer 85
 - choisir une 31
 - compromise 147
 - créer une robuste 104
 - oubli 88
 - principale créer 104, 105
 - se rappeler 104
 - suggestions 31, 32
 - PKZIP 135
 - plug-ins e-mail
 - utiliser PGP avec des 49
 - poudre de perlimpinpin 142
 - préférences
 - cryptage 88
 - fermeture automatique 111
 - fermeture par raccourci clavier 111
 - générales 88
 - génération de clé 89
 - régler 88
 - serveur de clés 93
 - Privacy Enhanced Mail 140
- R**
- raccourcis clavier
 - fermeture des volumes 111
 - réactions

faire connaître à Network Associates 10
 résidus de fichiers 147
 révoquer des clés 87
 RSA
 créer des clés 30

S

saut de ligne 93
 scission de clé 36
 Secure Viewer *Voir aussi* Tempest
 nouvelle fonctionnalité 13
 option pour e-mail 51
 serveur
 distant
 ouvrir des volumes 112
 instituer racine 94
 préférences 93
 synchroniser avec 94
 serveur de certificats *Voir* serveur de clés
 serveur de clés
 ajouter 95
 effacer des clés d'un 41
 envoyer votre clé publique sur un 32, 40
 obtenir une clé depuis un 43
 rechercher sur un 98
 régler les préférences 93
 utiliser pour diffuser un certificat de
 révocation 87
 signature
 avec Eudora 49
 avec une clé scindée 37, 39, 64, 78, 86
 des clés publiques 46, 47, 81, 137
 effacer 85
 e-mail 16, 17, 49
 signatures numériques
 effacement 85
 et authenticité 46
 somme de contrôle 135
 sous-clés
 créer 35
 effacer 78
 expiration 78

propriétés 78
 révoquer 78
 taille 78
 validité 78

T

taille de clé
 définir 30, 36
 portion Diffie-Hellmann 30
 portion DSS 30
 sur mesure 30, 36
 Tempest *Voir aussi* Secure Viewer
 Tempest, attaques 150
 Triple-DES 134
 taille de clé 134
 trousseaux de clés
 aperçu 15
 changer les attributs 73 à 78
 définition 73
 emplacement 73
 entreposer ailleurs 73
 rechercher 98
 visualiser les attributs 73 à 78
 Trust Model (propriété) 78

V

valider
 des clés publiques 16
 accorder sa confiance pour 84
 validité 136
 des clés publiques, vérifier la 45
 veille (mode)
 fermeture si mise en 111
 ver, attaques 148
 vérifier
 e-mail 17, 55
 l'authenticité d'une clé 16, 45
 l'empreinte d'une clé 80
 virus, attaques 148
 visualiser
 attributs des clés 20

attributs des trousseaux 73 à 78
paire de clés 20
propriétés des clés 73 à 78
volume PGPdisk
 créer 103
 fermer 110
 ouvrir 109
vulnérabilités 146

W

Wipe
 disques 70
 fichiers 17, 69

Z

Zimmermann, Phil 129

