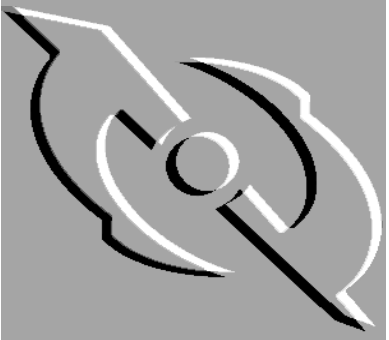


PGP Desktop Security et Personal Privacy

pour Windows 95, Windows 98 et Windows NT

Guide de l’utilisateur

Version internationale 6.5.

DROITS D'AUTEUR

Imprimé dans la CE. PGP, Version Internationale 6.5.1, 24-12-99.*

L'exportation de ce logiciel et des documentations doit être conforme aux règles et décrets, promulgués occasionnellement par le bureau de gestion des exportations du ministère du commerce américain, qui limitent l'exportation et la réexportation de certains produits et données techniques.

Network Associates International BV.
Gatwickstraat 25
-1043 GL Amsterdam
+31(20)5866100
+31(20)5866101 fax
http://www.nai.com
info@nai.com

Le signe * est parfois utilisé à la place de ® pour les marques déposées, afin de les protéger en dehors des Etats-Unis.

GARANTIE LIMITEE

Garantie limitée. Network Associates garantit, pour une période de soixante (60) jours à partir de la date d'achat d'origine, le fonctionnement du logiciel, conformément à la documentation fournie. Légalement, les garanties implicites du logiciel, le cas échéant, sont limitées à cette même période de (60) jours. Certaines juridictions n'autorisant pas les limites de durée relatives à une garantie implicite, les limitations mentionnées ci-dessus peuvent ne pas vous concerner.

Recours du client. La responsabilité de Network Associates Inc. et de ses fournisseurs et le recours exclusif du client seront limités, au choix de Network Associates, (i) au remboursement du prix d'achat de la licence, le cas échéant, ou (ii) à la réparation ou au remplacement du logiciel qui ne correspond pas à la limite de garantie et que vous renverrez à Network Associates Inc. à vos frais avec une copie du reçu. Cette garantie limitée n'est plus valable si la défaillance du logiciel a été provoquée par un accident, une utilisation abusive ou une mauvaise utilisation. Tout logiciel réparé ou de remplacement sera soumis à garantie pour une durée correspondant au reste de la période de garantie d'origine ou à trente (30) jours. Ce recours est limité aux Etats-Unis, car Network Associates Inc. est sujet à des restrictions régies par les lois et les décrets relatifs au contrôle des exportations aux Etats-Unis, et tout service de support produit offert par Network Associates Inc. nécessite une preuve d'achat émanant d'un distributeur agréé.

DENI DE GARANTIES. DANS LES LIMITES PERMISES PAR LA LOI, A L'EXCEPTION DE LA GARANTIE LIMITEE DU PRESENT DOCUMENT, LE LOGICIEL ET SA DOCUMENTATION SONT FOURNIS « TELS QUELS » ET NETWORK ASSOCIATES ET SES FOURNISSEURS DENIENT TOUTE AUTRE GARANTIE OU CONDITION, EXPLICITE OU IMPLICITE, COMPRENANT, ENTRE AUTRES, LES GARANTIES IMPLICITES DE QUALITE MARCHANDE, D'APTITUDE A UN USAGE PARTICULIER, DE CONFORMITE A LA DESCRIPTION, DE TITRE ET DE VIOLATION DES DROITS DES PARTIES TIERCES, AINSI QUE LA FOURNITURE OU NON DE SERVICES DE SUPPORT PRODUIT. CETTE GARANTIE LIMITEE VOUS DONNE DES DROITS JURIDIQUES PARTICULIERS. SELON LA JURIDICTION, VOUS POUVEZ JOUIR D'AUTRES DROITS.

LIMITATION DE LA RESPONSABILITE. DANS LES LIMITES PERMISES PAR LA LOI, EN AUCUN CAS NETWORK ASSOCIATES, INC. OU SES FOURNISSEURS NE SERONT TENUS RESPONSABLES DE TOUT DOMMAGE ACCIDENTEL, INDIRECT, SPECIAL, CONSEQUENT, DE TOUT DOMMAGE-INTERET PUNITIF OU ELEVE POUR PREJUDICE MORAL OU MANQUE A GAGNER DE TOUTE SORTE, Y COMPRIS LA PERTE DE BENEFICES, LA PERTE D'AFFAIRES, LA PERTE D'INFORMATIONS, LA PERTE D’EXPLOITATION OU TOUTE PERTE FINANCIÈRE ET L'ATTEINTE A LA PROPRIETE, DECOULANT DE L'UTILISATION DU LOGICIEL OU DE L'IMPOSSIBILITE DE FOURNIR LES SERVICES DE SUPPORT, MÊME SI NETWORK ASSOCIATES, INC. A ETE AVERTI DE l'EXISTENCE D'UNE TELLE POSSIBILITE. LA RESPONSABILITE CUMULATIVE ET INTEGRALE DE NETWORK ASSOCIATES, INC A VOTRE EGARD OU AUPRES D'UN TIERS POUR TOUTE PERTE OU DOMMAGE LIE(E) A UNE RECLAMATION, EXIGENCE OU ACTION DECOULANT DE CE CONTRAT NE SAURAIT DEPASSER LE PRIX D'ACHAT DE LA LICENCE. CERTAINES JURIDICTIONS N'AUTORISANT PAS L'EXCLUSION OU LA LIMITE DE RESPONSABILITE, LES LIMITES MENTIONNEES PEUVENT NE PAS VOUS CONCERNER.

Table des matières

Préface

PGP fait partie de la boîte à outils de sécurité de votre entreprise en vue de protéger l'un de vos biens les plus précieux : *les informations*. Les entreprises ont depuis longtemps pris l'habitude de poser des verrous sur leurs portes et leurs armoires à fichiers et demander à leurs employés de prouver leur identité avant de pouvoir accéder aux différents secteurs de leur lieu de travail. PGP est un outil précieux qui vous permet de protéger la sécurité et l'intégrité des données et des messages de votre entreprise. Pour de nombreuses entreprises, une perte de confidentialité entraîne une perte en affaires.

Des livres entiers ont traité de l'implémentation de la sécurité réseau. L'objectif de ce guide est d'implémenter PGP en tant qu'outil au sein de la structure globale de sécurité de votre réseau. PGP n'est qu'une partie d'un système de sécurité complet, mais elle est d'une extrême importance. En effet, ce logiciel permet d'effectuer des opérations de cryptage, afin de protéger les données du regard de tous ceux auxquels elles n'étaient pas adressées, même de ceux qui peuvent voir les données cryptées. Il permet de protéger les informations des « étrangers » à la fois internes et externes.

Ce guide décrit l'utilisation de PGP ® Desktop Security pour Windows 95, Windows 98 et Windows NT. Ce logiciel dispose de nombreuses fonctionnalités, décrites dans la section « Nouveautés de la version 6.5.1 de PGP » à la page xiv.

Si vous utilisez la cryptographie pour la première fois et que vous souhaitez connaître la terminologie et les concepts que vous rencontrerez lors de l'utilisation de PGP, consultez la documentation intitulée *Introduction à la cryptographie.*

Nouveautés de la version 6.5.1 de PGP

Cette version de PGP comprend les nouvelles fonctionnalités suivantes :

- **PGPnet.** Le produit PGPnet marque une étape importante dans l'histoire de PGP. Il sécurise l'ensemble des communications TCP / IP entre lui-même et tout autre ordinateur sur lequel PGPnet est installé. Il permet une interaction complète avec la passerelle / pare-feu Gauntlet GVPN et fournit une solution complète pour les VPN internes d'accès distant utilisant les protocoles d'échange standard de l'industrie IPSec (sécurité de protocole Internet) et IKE (échange de clés via Internet). Les tests avec les routeurs Cisco (nécessitant la version 12.0(5) ou une version ultérieure de Cisco et IPSec Triple-Des Feature Pack), la version 1.0 de Linux FreeS / WAN et de nombreux autres produits ont été concluants. En outre, il s'agit du premier produit IPSec gérant parfaitement l'utilisation de clés OpenPGP en vue d'opérations d'authentification en plus des certificats X.509. Pour plus d'informations sur l'utilisation de PGPnet, reportez-vous au Chapitre 8, « Gestion de réseau privé virtuel PGPnet ».

- **Archives d'auto-décryptage.** PGP peut à présent convertir des fichiers ou dossiers en archives d'auto-décryptage (SDA) pouvant être envoyées à des utilisateurs ne possédant pas PGP. Ces archives ne dépendent d'aucune application. Elles sont compressées et protégées par la fonction cryptographique invulnérable de PGP.

- **Prise en charge des certificats X.509 et des CA.** PGP peut désormais interagir avec le format de certificat X.509. Il s'agit du format utilisé par la plupart des navigateurs Web pour sécuriser le transfert de pages Web. PGP gère la demande de certificats provenant de Net Tools PKI de Network Associates, de VeriSign OnSite et des autorités de certificats Entrust. Les certificats X.509 sont analogues à une signature PGP. Ainsi, vous pouvez même les demander pour votre clé PGP existante. Cette fonctionnalité peut également être utilisée via PGPnet pour interagir avec des solutions VPN existantes faisant appel au X.509.

- **Effacement automatique de l'espace libre.** Cette fonctionnalité vous permet à présent d'utiliser le Gestionnaire des tâches Windows pour programmer l'effacement sécurisé périodique de l'espace libre sur votre disque. Ainsi, les fichiers préalablement supprimés sont effacés en toute sécurité.

- **Touches.** L'ajout de cette fonctionnalité améliore nettement l'utilisation de la fenêtre courante. Vous pouvez à présent définir des combinaisons de touches correspondant aux fonctions Crypter / Décrypter / Signer.

- **Liste de mots d'empreinte digitale.** Lorsque vous vérifiez l'empreinte digitale d'une clé publique PGP, vous pouvez maintenant choisir d'afficher cette empreinte sous forme d'une liste de mots au lieu de l'afficher sous forme de caractères hexadécimaux. La liste de mots de la zone de texte de l'empreinte digitale est constituée de mots spéciaux servant à l'authentification. Ces mots sont utilisés par PGP et sélectionnés soigneusement de façon à être phonétiquement distincts et facilement compréhensibles.
- **Prise en charge de proxy HTTP.** Si votre ordinateur est relié à un réseau protégé par un pare-feu interne avec un serveur proxy HTTP, PGP gère à présent l'accès aux serveurs de certificats HTTP via le proxy.
- **Retour à la ligne intelligent.** Le retour à la ligne de PGP porte à présent sur les paragraphes et les paragraphes spécifiés automatiquement, ce qui clarifie les messages signés.
- **PGP Command Line.** PGP Command Line est à présent fourni avec Desktop Security. Cette version de la ligne de commande de PGP a été conçue pour deux types principaux d'applications : le transfert sécurisé d'informations entre des serveurs batch et l'intégration dans des processus automatisés.

Pour contacter Network Associates

Service clientèle

Pour commander des produits ou obtenir des informations complémentaires, contactez le service de support aux clients au +31(20)5866 100 ou écrivez à l'adresse suivante :

Network Associates International BV.
Gatwickstraat 25
1043 GL Amsterdam
Pays-Bas

Support technique

La réputation de Network Associates quant à son engagement à satisfaire ses clients n'est plus à prouver. Notre site Web perpétue cette tradition : il s'agit en effet d'une ressource précieuse en termes de support technique. Nous vous encourageons donc vivement à le visiter pour trouver des réponses aux questions récurrentes, mettre à jour vos logiciels Network Associates et obtenir les dernières informations sur le cryptage de Network Associates.

World Wide Web	http://www.nai.com

Vous pouvez également contacter le support technique de vos produits PGP par les moyens suivants :

Téléphone	+31 (20) 586 6100
E-mail	tech-support-europe@nai.com

Pour répondre rapidement et efficacement à vos questions, le personnel du support technique de Network Associates a besoin de certaines informations sur votre ordinateur et votre logiciel. Veillez à les rassembler avant de nous appeler :

Si vous n'êtes pas satisfait des réponses fournies par nos services automatisés, n'hésitez pas à composer le numéro suivant, du lundi au vendredi, entre 6 h et 18 h.

Téléphone	+31 (20) 586 6100

Pour répondre rapidement et efficacement à vos questions, le personnel du support technique de Network Associates a besoin de certaines informations sur votre ordinateur et votre logiciel. Veillez à les rassembler avant de nous appeler :

- Nom et version du produit
- Marque et modèle de l'ordinateur
- Matériels ou périphériques supplémentaires connectés à votre ordinateur
- Type et version du système d'exploitation
- Type et version du réseau, le cas échéant
- Contenu de tout message d'état ou d'erreur affiché sur l'écran, ou apparaissant dans un fichier journal (tous les produits ne produisent pas de fichier journal)
- Application et version de messagerie (si le problème implique l'utilisation de PGP avec un produit de messagerie, par exemple, le module externe Eudora)
- Etapes spécifiques permettant de reproduire le problème

Compatibilité An 2000

Vous pouvez obtenir des informations concernant les produits NAI compatibles An 2000, les normes de compatibilité An 2000 ou des modèles de test sur le site Web de NAI dont l'adresse est http://www.nai.com/y2k

Pour plus d'informations, contactez y2k@nai.com.

Formations proposées par Network Associates

Pour plus d'informations sur le programme des formations en ligne, appelez le +31(20)5866100.

Commentaires

Vos commentaires sont les bienvenus. Toutefois, sachez que Network Associates n'est en aucune manière engagé par les informations que vous lui soumettez. Veuillez adresser vos commentaires sur la documentation concernant les produits PGP à : Network Associates International BV. Gatwickstraat 25, 1043 GL Amsterdam, Pays-Bas. Vous pouvez également les envoyer par message électronique à tns_documentation@nai.com.

Lectures recommandées

Livres techniques et généralistes pour débutants

- Whitfield Diffie et Susan Eva Landau, « Privacy on the Lin*e* », *MIT Pres*s ; ISBN : 0262041677
  Ce livre traite de l'histoire et de la politique gravitant autour de la cryptographie et de la sécurité des communications. Il constitue une excellente lecture, même pour les débutants et le personnel non technique, et contient des informations que même de nombreux experts ignorent.

- David Kahn, « The Codebreakers », *Scribne*r ; ISBN : 0684831309
  Ce livre relate l'histoire des codes et des casseurs de codes depuis le temps des Egyptiens jusqu'à la fin de la seconde guerre mondiale. Kahn l'a écrit dans les années soixante, puis en a publié une version révisée en 1996.
  Ce livre ne vous apprendra rien sur le mode de fonctionnement de la cryptographie, mais il a inspiré toute la nouvelle génération de cryptographes.

- Charlie Kaufman, Radia Perlman et Mike Spencer, « Network Security : Private Communication in a Public World » Prentice Hall ; ISBN : 0-13-061466-1

Cet ouvrage fournit une description détaillée des systèmes et des protocoles de sécurité de réseau, notamment des explications sur leur bon ou mauvais fonctionnement. Publié en 1995, il traite peu des dernières avancées technologiques, mais reste un livre intéressant. Il contient également une des descriptions les plus claires sur le fonctionnement du DES parmi tous les livres écrits sur le sujet.

Livres intermédiaires

- Bruce Schneier, « Applied Cryptography : Protocols, Algorithms, and Source Code in C » *John Wiley & Son*s ; ISBN : 0-471-12845-7
  Il s'agit d'un bon livre technique pour se familiariser avec le fonctionnement d'une grande partie de la cryptographie. Si vous souhaitez devenir un expert, c'est le livre qu'il vous faut pour commencer.

- Alfred J. Menezes, Paul C. van Oorschot, and Scott Vanstone, « Handbook of Applied Cryptography », *CRC Press ;* ISBN : 0-8493-8523-7
  Voici le livre technique qu'il vous faut lire après le livre de Schneier.
  Le niveau mathématique de ce livre est très élevé, mais celui-ci reste cependant utilisable par ceux qui ne maîtrisent pas bien cette matière.

- Richard E. Smith, « Internet Cryptography », *Addison-Wesley Pub C*o ; ISBN : 020192480
  Ce livre décrit le mode de fonctionnement de nombreux protocoles de sécurité Internet. Il décrit notamment comment des systèmes bien conçus finissent cependant par présenter des défaillances suite à une utilisation négligente. Cet ouvrage contient peu de notions mathématiques et beaucoup d'informations pratiques.

- William R. Cheswick et Steven M. Bellovin, « Firewalls and Internet Security : Repelling the Wily Hacker », *Addison-Wesley Pub C*o ; ISBN : 0201633574
  Ce livre a été écrit par deux éminents chercheurs de chez AT&T Bell Labs et traite de leurs expériences dans le maintien et la restructuration des connexions Internet de AT&T. Très accessible.

Livres très techniques

- Neal Koblitz, « A Course in Number Theory and Cryptography », *Springer-Verla*g ; ISBN : 0-387-94293-9
  Un excellent manuel universitaire de mathématiques sur la théorie des nombres et la cryptographie.

- Eli Biham et Adi Shamir, « Differential Cryptanalysis of the Data Encryption Standard », *Springer-Verla*g ; ISBN : 0-387-97930-1
  Ce livre décrit la technique de cryptanalyse différentielle telle qu'elle est appliquée au DES. C'est un excellent ouvrage pour apprendre cette technique.

Installation de PGP 1

Ce chapitre décrit l'installation et l'exécution du logiciel PGP Desktop Security pour Windows. Il présente également brièvement les procédures à suivre lors de l'utilisation du produit.

Avant de procéder à l'installation de PGP, assurez-vous de disposer de la configuration suivante.

Configuration requise

Pour installer PGP sous Windows 95, Windows 98 ou Windows NT, vous devez disposer de :

- De Windows 95, Windows 98 ou Windows NT 4.0 (Service Pack, version 3 ou ultérieure)
- 32 Mo de RAM
- 16 Mo d'espace disque disponible

En outre, pour utiliser PGPnet, vous avez également besoin de :

- Microsoft TCP / IP
- Un adaptateur de réseau local / étendu compatible
- Windows 95b (OSR2) si vous procédez à l'installation sur un système Windows 95.

Compatibilité avec d'autres versions

PGP a fait l'objet de nombreuses révisions depuis sa distribution gratuite par Phil Zimmermann, en 1991. Bien que cette version de PGP ait été largement modifiée par rapport au programme d'origine et qu'elle soit dotée d'une nouvelle interface utilisateur, sa compatibilité avec les versions antérieures est parfaite, ce qui signifie que vous pouvez échanger des messages électroniques sécurisés avec des personnes utilisant encore une ancienne version du produit :

- PGP 2.6 (distribué par MIT)
- PGP for Personal Privacy, version 5.0 à 5.5

- PGP for Business Security ou PGP for Email and Files, version 5.5
- PGP for Desktop Security ou PGP for Personal Privacy, version 6.0

REMARQUE : Au-delà de la version 5.0, les produits PGP peuvent parfois nécessiter une extension RSA pour une compatibilité descendante.

Mise à jour à partir d'une version précédente

Si vous effectuez une mise à jour à partir d'une version précédente de PGP (PGP, Inc., Network Associates, Inc. ou ViaCrypt), il est recommandé de supprimer les anciens fichiers de programme avant d'installer PGP pour libérer de l'espace disque. Toutefois, vous devez être particulièrement attentif à ne pas détruire les fichiers de trousseaux de clés publiques et privées, utilisés pour le stockage de toutes les clés créées ou collectées avec la version précédente. Lors de l'installation de la nouvelle version de PGP, vous avez la possibilité de conserver ces fichiers, ce qui vous évite ensuite d'avoir à importer toutes vos anciennes clés.

Mise à jour à partir de PGP, version 2.6.2 ou 2.7.1

1. Fermez tous les programmes ou logiciels actuellement ouverts.
2. Sauvegardez vos anciens trousseaux de clés PGP sur un autre volume. Si vous utilisez PGP version 2.6.2 ou 2.7.1 pour Windows, vos clés publiques et privées sont respectivement stockées dans les fichiers « pubring.pgp » et « secring.pgp ». Avec les versions 5.x à 6.5, elles sont stockées dans les fichiers « pubring.pkrv » et « secring.skr ».

   ASTUCE : Pour plus de sécurité, effectuez des copies de sauvegarde distinctes de vos trousseaux de clés sur deux disquettes. Veillez à ne pas perdre votre trousseau de clés privées, car vous ne seriez plus en mesure de décrypter les messages électroniques ou pièces jointes cryptés à l'aide de ces clés. Stockez les trousseaux de clés dans un lieu sûr auquel vous seul avez accès.

3. Une fois cette copie de sauvegarde terminée, supprimez ou archivez votre (ancien) logiciel PGP. A ce stade, vous avez deux possibilités :
   - Suppression manuelle de l'intégralité de l'ancien dossier PGP et de ses fichiers ;
   - Suppression manuelle de l'ancien programme PGP, puis archivage des fichiers restants, notamment des fichiers de configuration et de trousseaux de clés.

4. Installez PGP, version 6.5.1, à l'aide du programme d'installation fourni.
5. Redémarrez votre ordinateur.

Mise à jour à partir de PGP, version 5.x

Si vous effectuez une mise à jour à partir de PGP version 4.x ou 5.x, suivez les instructions d'installation de la section « Installation de PGP ».

Installation de PGP

Vous pouvez installer le logiciel PGP Desktop Security à partir d'un CD-ROM ou du serveur de fichiers de votre entreprise. L'exécutable, Setup.exe, effectue une extraction automatique et vous guide à travers la procédure d'installation. Une fois l'installation terminée, vous pouvez créer votre paire de clés privées et publiques et commencer à utiliser PGP. Pour plus d'instructions sur l'utilisation de PGP, reportez-vous au fichier PGPWinUsersGuide.pdf fourni avec le programme.

Pour installer PGP Desktop Security sous Windows, procédez exactement comme suit.

Installation de PGP

1. Fermez tous les programmes actuellement ouverts, puis effectuez l'une des opérations suivantes :

   - **Pour installer PGP à partir d'un CD-ROM,** insérez ce CD-ROM dans votre lecteur.

     Le programme d'installation est lancé automatiquement. Le cas échéant, cliquez deux fois sur **Setup.exe** dans le dossier PGP, situé sur le CD-ROM.

   - **Pour installer PGP à partir du serveur de fichiers de votre entreprise,** contactez votre agent de sécurité afin d'obtenir des informations sur le serveur à partir duquel télécharger PGP. Connectez-vous ensuite à ce serveur.

     Pour lancer le programme d'installation, cliquez deux fois sur le fichier **Setup.exe** situé dans le dossier PGP.

2. Le programme d'installation recherche les logiciels ouverts et vous invite à les fermer.

   Si PGP, version 4.x à 6.x, est installé sur votre ordinateur, il vous est demandé de supprimer les anciens fichiers PGP. Pour désinstaller automatiquement l'ancienne version, cliquez sur **Oui**. Vos fichiers de trousseaux de clés sont enregistrés dans un fichier appelé **Anciens trousseaux de clés**.

   Une fois l'installation terminée, vous devez redémarrer votre ordinateur. La procédure d'installation se poursuit alors.

   L'écran **Installation de PGP** apparaît.

3. Dans la boîte de dialogue Bienvenue dans PGP, consultez les indications fournies, puis cliquez sur **Suivant**.

   L'accord de licence de Network Associates apparaît alors.

4. Lisez cet accord, puis cliquez sur **Oui** pour en accepter les termes.

   Le fichier Whatsnew.txt apparaît ensuite. Il répertorie les nouvelles fonctionnalités et d'autres informations importantes concernant PGP version 6.5.1.

5. Consultez ce fichier, puis cliquez sur **Suivant**.

6. Dans la boîte de dialogue **Informations utilisateur,** enregistrez votre produit en entrant votre nom et le nom de votre entreprise.

7. Cliquez sur **Suivant**.

8. Cliquez ensuite sur **Parcourir** pour sélectionner un répertoire de destination pour les fichiers PGP ou acceptez le répertoire par défaut. Pour continuer, cliquez sur **Suivant**.

La boîte de dialogue **Sélection des composants** apparaît, comme illustré à la Figure 1-1.

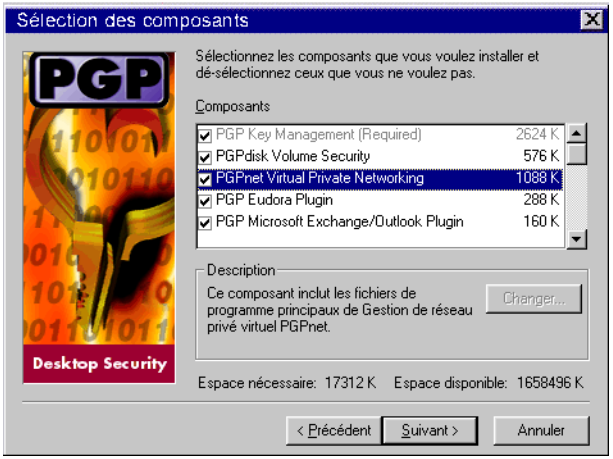


Figure 1-1. Boîte de dialogue Sélection des composants de PGP

9. Désélectionnez les composants que vous ne souhaitez pas installer. Par défaut, tous les composants sont sélectionnés. Choisissez l'une des options d'installation suivantes :

   - **Gestion des clés PGP (requise).** Cette option permet d'installer le programme PGP. Vous devez installer les utilitaires de gestion des clés.

   PGPnet. Pour installer le programme PGPnet, sélectionnez cette option. PGPnet, *Réseau privé virtuel (VPN, Virtual Private Network*), est une application de cryptage simple d'utilisation, vous permettant de communiquer de manière sécurisée et économique avec d'autres utilisateurs PGPnet sur votre propre intranet d'entreprise et avec des utilisateurs du monde entier.

   - **Module externe Eudora PGP.** Pour intégrer les fonctionnalités de PGP à votre application de messagerie Eudora de Qualcomm, sélectionnez cette option. PGP 6.5.1 prend en charge Eudora version 3.05 et ultérieure.

   - **Module externe Microsoft Exchange/Outlook PGP.** Pour intégrer les fonctionnalités de PGP à votre application de messagerie Microsoft Exchange / Outlook, sélectionnez cette option. PGP 6.5.1 prend en charge Outlook 97 et 98.

- **Module externe Microsoft Outlook Express PGP.** Pour intégrer les fonctionnalités de PGP à votre application de messagerie Microsoft Outlook Express, sélectionnez cette option. PGP 6.5.1 prend en charge la version incluse avec Internet Explorer version 4.x.
- **Manuel de l'utilisateur PGP (format Adobe Acrobat).** Pour installer le manuel de l'utilisateur PGP, sélectionnez cette option.
- **PGP CommandLine.** Pour installer la version de ligne de commande PGP pour les systèmes Windows NT, sélectionnez cette option. *Cette option doit être utilisée uniquement par le client. Les processus de serveurs batch nécessitent une distribution de licence supplémentaire.*

10. Cliquez sur **Suivant**.

    Une boîte de dialogue vous informe alors que le programme d'installation est prêt pour la copie de fichiers.

11. Vérifiez les paramètres d'installation, puis cliquez sur **Suivant**.

    Les fichiers PGP sont copiés sur votre ordinateur.

12. Si les trousseaux de clés stockés sur votre ordinateur proviennent d'une version précédente de PGP, cliquez sur **Oui** pour utiliser les trousseaux de clés existants.

    Une boîte de dialogue de navigation apparaît. Recherchez vos trousseaux de clés publiques et privées, Pubring.pkr et Secring.skr.

    Si aucun trousseau de clés n'est stocké sur votre ordinateur, cliquez sur **Non**. Lorsque vous ouvrez l'application PGPkeys pour la première fois, vous êtes alors invité à créer une paire de clés.

13. Si vous avez choisi d'installer l'application PGPnet, la **liste des adaptateurs réseau PGPnet** apparaît pour répertorier tous les adaptateurs détectés sur votre système, comme illustré à la Figure 1-2.

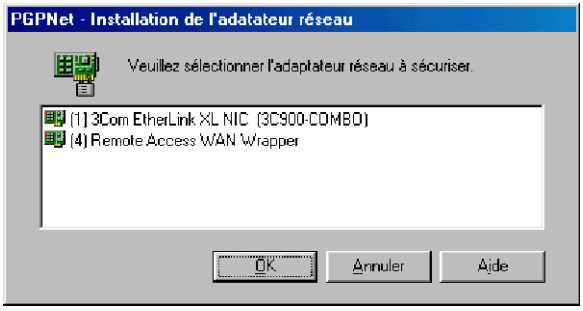


Figure 1-2. Liste des adaptateurs réseau PGPnet.

Pour communiquer de manière sécurisée via un modem, sélectionnez votre adaptateur WAN (par exemple, Encapsulateur de réseau étendu à accès distant ou Carte d'accès distant). Pour une connexion Ethernet, sélectionnez votre adaptateur LAN (par exemple, 3COM Megahertz LAN PC Card). Votre choix effectué, cliquez sur **OK**.

REMARQUE : Sur un ordinateur doté de Windows 98, le réseau étendu est répertorié comme une « Carte d'accès distant » plutôt que comme un « Encapsulateur de réseau étendu à accès distant ».

Le programme d'installation associe le pilote PGPnet à l'adaptateur sélectionné et configure votre ordinateur pour l'utilisation de l'application PGPnet.

14. Pour redémarrer automatiquement votre ordinateur, cliquez sur **Oui, je souhaite redémarrer mon ordinateur maintenant**.

15. Pour mettre fin à l'installation de PGP, puis redémarrer votre ordinateur, cliquez sur **Terminer**.

REMARQUE : Vous devez impérativement redémarrer votre ordinateur si vous avez installé PGPdisk ou PGPnet.

Voilà ! PGP est à présent installé sur votre ordinateur.

Utilisation de PGP 2

PGP repose sur une technologie de cryptage largement reconnue, appelée *cryptographie de clé publique*, qui met en jeu deux clés complémentaires, soit une *paire de clés*, utilisées pour assurer la sécurité des communications. L'une des clés est appelée *clé privée* et vous seul y avez accès. L'autre est appelée *clé publique* et vous pouvez l'échanger librement avec d'autres utilisateurs de PGP. Vos clés publique et privée sont stockées dans des fichiers de trousseaux de clés, accessibles via la fenêtre PGPkeys. Cette fenêtre vous permet d'effectuer toutes les fonctions de gestion de clés.

Cette section offre un bref aperçu des procédures à suivre lors de l'utilisation de PGP. Pour plus de détails sur l'une de ces procédures, reportez-vous aux chapitres correspondants de ce manuel. Pour accéder à une présentation complète de la technologie de cryptage de PGP, reportez-vous au manuel *Introduction à la cryptographie* fourni avec ce produit.

Etapes de base pour l'utilisation de PGP

1. Installez PGP sur votre ordinateur. Pour plus d'informations sur cette installation, reportez-vous au Chapitre 1, « Installation de PGP ».

2. Créez une paire de clés publiques et privées.

   Avant de commencer à utiliser PGP, générez une paire de clés. Une paire de clés PGP se compose d'une clé privée à laquelle vous seul avez accès, et d'une clé publique que vous pouvez copier et rendre librement accessible à tout correspondant.

   Une fois PGP installé, vous avez la possibilité de créer immédiatement une nouvelle paire de clés. Vous pouvez également la créer à tout moment en ouvrant l'application PGPkeys.

   Pour plus d'informations sur la création d'une paire de clés publiques et privées, reportez-vous à la section « Création d'une paire de clés » à la page 24.

3. Echangez des clés publiques avec d'autres utilisateurs.

   Après avoir créé une paire de clés, vous pouvez commencer à correspondre avec d'autres utilisateurs PGP. Pour ce faire, vous devez disposez d'une copie de leur clé publique, et inversement. Votre clé publique étant simplement un bloc de texte, il est aisé de l'échanger avec une autre personne. Vous pouvez inclure votre clé publique dans un message électronique, la copier dans un fichier ou l'envoyer sur un serveur de clés publiques ou d'entreprise, à partir duquel tout utilisateur peut en obtenir une copie si nécessaire.

   Pour plus d'informations sur l'échange de clés publiques, reportez-vous aux sections « Distribution d'une clé publique » à la page 52 et « Obtention des clés publiques des autres utilisateurs » à la page 57.

4. Validez les clés publiques.

   Dès lors que vous disposez de la copie de la clé publique d'un utilisateur, vous pouvez l'ajouter à votre trousseau de clés publiques. Il est ensuite conseillé de s'assurer que cette clé n'a pas été falsifiée et qu'elle appartient réellement à son détenteur supposé. Pour ce faire, comparez l'*empreinte digitale* unique de votre copie de cette clé publique avec celle de la clé d'origine. Lorsque vous êtes certain que vous disposez d'une clé publique valide, signez-la pour indiquer que son utilisation est sûre.
   Par ailleurs, vous pouvez accorder au détenteur d'une clé un niveau de fiabilité indiquant la confiance que vous lui accordez pour répondre de l'authenticité de la clé publique de cet utilisateur.

   Pour plus d'informations sur la validation de clés, reportez-vous à la section « Vérification de l'authenticité d'une clé » à la page 62.

5. Cryptez et signez vos messages et fichiers électroniques.

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

PGP utilise les données générées par d'autres applications. Ainsi, les fonctions de PGP sont conçues pour un accès immédiat, en tenant compte de la tâche que vous effectuez à un moment précis. PGP propose plusieurs méthodes de cryptage et de signature :

- **A partir de la Barre des tâches (PGPtray).** PGPtray comprend des utilitaires permettant d'effectuer des tâches cryptographiques sur les données dans le Presse-papiers ou dans la fenêtre courante. Reportez-vous à la section « Utilisation de PGPtray » à la page 16.
- **A partir d'applications de messagerie prises en charge (modules externes e-mail de PGP).** Ces modules vous permettent de sécuriser vos messages électroniques directement dans l'application de messagerie prise en charge. Reportez-vous à la section « Utilisation de PGP dans des applications de messagerie prises en charge » à la page 19.
- **A partir de PGPtools.** PGPtools vous permet d'effectuer des tâches cyptographiques dans les applications qui ne sont pas prises en charge par les modules externes, ainsi que des tâches de sécurité, telles que l'effacement de fichiers de votre disque. Reportez-vous à la section « Utilisation de PGPtools » à la page 18.
- **A partir du menu de l'Explorateur Windows.** Vous pouvez crypter et signer ou décrypter et vérifier des fichiers tels que les documents provenant d'un traitement de texte, des feuilles de calcul et des clips vidéo, directement dans l'Explorateur Windows. Reportez-vous à la section « Utilisation de PGP à partir de l'Explorateur Windows » à la page 18.

Pour plus d'informations sur le cryptage de messages électroniques, reportez-vous à la section « Cryptage et signature des messages électroniques » à la page 65. Pour plus d'informations sur le décryptage de fichiers, reportez-vous à la section « Utilisation de PGP pour le cryptage et le décryptage des fichiers » à la page 77.

6. Décryptez et vérifiez vos messages et fichiers électroniques.

   Lorsqu'un utilisateur vous envoie des données cryptées, vous pouvez en déchiffrer le contenu et vérifier toute signature apposée afin de vous assurer que ces données proviennent de l'expéditeur supposé et qu'elles n'ont pas été falsifiées.

   - Si vous utilisez une application de messagerie prise en charge par les modules externes, sélectionnez les options appropriées dans la barre d'outils de votre application pour décrypter et vérifier vos messages.
   - Dans le cas contraire, vous pouvez copier les messages dans le Presse-papiers et y lancer les fonctions appropriées. Pour décrypter et vérifier des fichiers, utilisez le Presse-papiers, l'Explorateur Windows ou PGPtools. Vous pouvez également décrypter des fichiers cryptés sur votre ordinateur et vérifier des fichiers signés, afin de garantir qu'ils n'ont pas été falsifiés.

   Pour plus d'informations sur la sécurisation de messages électroniques, reportez-vous à la section « Décryptage et vérification des messages électroniques » à la page 74. Pour plus d'informations sur la sécurisation de fichiers, reportez-vous à la section « Utilisation de PGP pour le cryptage et le décryptage des fichiers » à la page 77.

7. Effacez des fichiers

   Pour effacer définitivement un fichier, vous pouvez utiliser la commande d'effacement afin de garantir que ce fichier ne peut pas être récupéré. Ce fichier est alors immédiatement écrasé de sorte que sa récupération à l'aide de logiciels de récupération de disque devient impossible.

   Pour plus d'informations sur l'effacement de fichiers, reportez-vous à la section « Utilisation de la fonction d'effacement de PGP pour la suppression de fichiers » à la page 88.

Utilisation de PGPkeys

Lorsque vous choisissez **PGPkeys** dans PGPtray, la fenêtre PGPkeys apparaît (Figure 2-1) et affiche les paires de clés publiques et privées que vous vous êtes créées, ainsi que toutes les clés publiques des autres utilisateurs que vous avez ajoutées à votre trousseau de clés publiques.

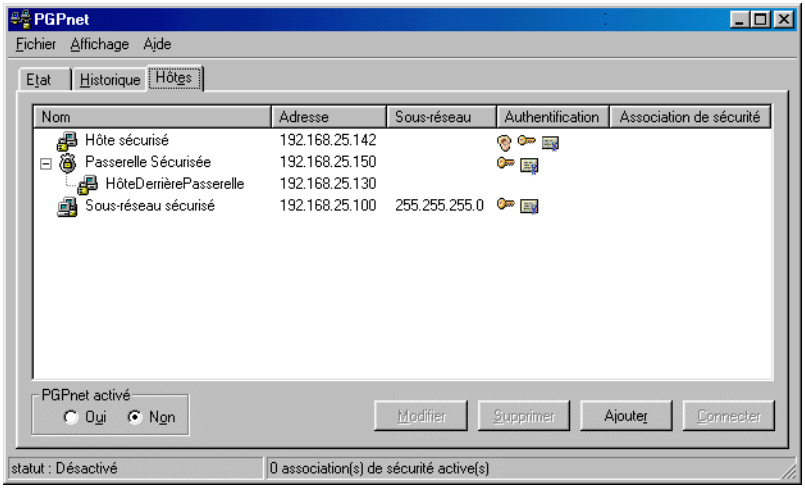


Figure 2-1. PGPkeys.

(Si vous n'avez pas encore créé une nouvelle paire de clés, l'Assistant de génération de clés PGP vous guide tout au long des étapes nécessaires.) Toutefois, pour obtenir plus d'informations sur les diverses options, il est recommandé de consulter la section Chapitre 3, « Création et échange de clés », plus complète sur la création d'une paire de clés.

Dans la fenêtre PGPkeys, vous pouvez créer de nouvelles paires de clés et gérer l'ensemble des clés que vous possédez. Par exemple, cette fenêtre vous permet de consulter les attributs associés à une clé particulière, de spécifier votre niveau de confiance quant à l'appartenance d'une clé au détenteur supposé, et d'indiquer la confiance que vous accordez au détenteur de la clé devant authentifier les clés des autres utilisateurs. Pour une explication complète des fonctions de gestion de clés disponibles dans la fenêtre PGPkeys, reportez-vous au Chapitre 6.

Définitions des icônes de PGPkeys

Icônes de la barre de menus PGPkeys

Le tableau suivant répertorie l'ensemble des icônes de la barre de menus PGPkeys, et décrit leur fonction.

Tableau 2-1. Icônes de la barre de menus PGPkeys

Icône	Fonction
	Lance l'Assistant de génération de clés. Pour créer une nouvelle paire de clés, cliquez sur cette icône.
	Révoque la clé ou la signature sélectionnée. Pour désactiver ou révoquer une clé ou une signature sélectionnée, cliquez sur cette icône. La révocation d'une clé empêche toute personne de l'utiliser pour crypter des données.
	Vous permet de signer la clé sélectionnée. Ce faisant, vous certifiez que cette clé et l'ID utilisateur appartiennent à l'utilisateur identifié.
	Supprime l'élément sélectionné. Pour supprimer une clé, une signature ou un ID photographique, cliquez sur cette icône.
	Ouvre la fenêtre **Recherche des clés** qui vous permet de rechercher des clés dans des trousseaux de clés locaux et sur des serveurs distants.
	Envoie la clé sélectionnée vers le serveur. Pour télécharger votre clé sur le serveur de domaine ou de certificats, cliquez sur cette icône.
	Met à jour la clé sélectionnée à partir du serveur de domaine ou de certificats. Pour importer des clés d'un serveur de domaine ou de certificats vers votre trousseau de clés, cliquez sur cette icône.
	Affiche la boîte de dialogue **Propriétés** pour la clé sélectionnée. Pour afficher les propriétés **générales** et relatives à une **sous-clé** de la clé, cliquez sur cette icône.
	Vous permet d'importer les clés d'un fichier vers votre trousseau de clés.
	Vous permet d'exporter la clé sélectionnée vers un fichier.

Icônes de la fenêtre PGPkeys

Le tableau suivant répertorie toutes les mini-icônes de la fenêtre PGPkeys et décrit leur représentation.

Tableau 2-2. Icônes de la fenêtre PGPkeys

Icône	Description
	Une clé jaune accompagnée d'un utilisateur représente votre paire de clés Diffie-Hellman/DSS, constituée de vos clés privée et publique.
	Une clé jaune unique représente une clé publique Diffie-Hellman/DSS.
	Une clé grise accompagnée d'un utilisateur représente votre paire de clés RSA, constituée de vos clés privée et publique.
	Une clé grise unique représente une clé publique RSA.
	Lorsqu'une clé ou une paire de clés est grisée, il est temporairement impossible de l'utiliser pour procéder à un cryptage ou effectuer une signature. Vous pouvez désactiver une clé dans la fenêtre PGPkeys. Ainsi, les clés rarement utilisées n'apparaissent pas dans la boîte de dialogue Sélection de clé.
	Cette icône indique qu'un ID utilisateur photographique accompagne la clé publique.
	Une clé barrée d'un X rouge indique qu'elle a été révoquée. Les utilisateurs révoquent leurs clés lorsque celles-ci ne sont plus valides ou ont été compromises d'une manière quelconque.
	Une clé accompagnée d'une horloge indique que la clé est arrivée à expiration. La date d'expiration d'une clé est définie lors de sa création.
	Une enveloppe représente le détenteur de la clé et répertorie les noms d'utilisateurs et les adresses e-mail associées à cette clé.
	Un rond gris indique que la clé n'est pas valide.
	Un rond vert indique que la clé est valide. Un rond rouge supplémentaire dans la colonne CDS indique que la clé dispose d'une clé de décryptage supplémentaire associée ; un rond gris supplémentaire dans la colonne CDS indique que cette clé ne dispose pas de clé de décryptage supplémentaire.
	Un rond vert accompagné d'un utilisateur indique que vous êtes le détenteur de la clé et que celle-ci est fiable de manière implicite.

Tableau 2-2. Icônes de la fenêtre PGPkeys

Icône	Description
	Un crayon ou un stylo-plume indique les signatures des utilisateurs de PGP ayant répondu de l'authenticité de la clé. - Une signature barrée d'un X rouge indique une signature révoquée. - Une signature accompagnée d'un stylo grisé indique une signature erronée ou invalide. - Une signature accompagnée d'une flèche bleue placée en regard de la signature indique que celle-ci est exportable.
	Un certificat représente un certificat X.509, un document électronique reconnu permettant de prouver l'identité et la provenance d'une clé publique via un réseau de communication.
	Une horloge indique un certificat X.509 arrivé à expiration.
	Un X rouge indique un certificat X.509 révoqué.
	Une barre vide indique une clé invalide ou un utilisateur non fiable.
	Une barre à moitié pleine indique une clé valide ou un utilisateur fiable de manière marginale.
	Une barre hachurée indique qu'il s'agit de l'une de vos clés valides et qu'elle est fiable de manière implicite, indépendamment de ses signatures.
	Une barre pleine indique une clé entièrement valide ou un utilisateur entièrement fiable.

Utilisation de PGPtray

Pour accéder aux principales fonctions principales de PGP, cliquez sur l'icône représentant un verrou (), normalement située dans la Barre des tâches, puis choisissez la commande de menu appropriée. Si cette icône est introuvable dans la Barre des tâches, lancez PGPtray à partir du menu **Démarrer**. Cette fonctionnalité permet d'accéder immédiatement aux fonctions de PGP, sans tenir compte des applications ouvertes. Elle est particulièrement utile si vous travaillez dans une application de messagerie non prise en charge par les modules externes PGP.

REMARQUE : Si vous avez installé PGPnet, cette icône () apparaît dans votre Barre des tâches, à la place de l'icône représentant un verrou. L'icône PGPtray vous indique si PGPnet est désactivé ou non installé (verrou gris), installé (verrou jaune sur un réseau) ou installé mais désactivé (verrou jaune sur un réseau barré d'un X rouge).

Lancement des fonctions de PGP à partir du Presse-papiers ou de la fenêtre courante

Si vous utilisez une application de messagerie qui n'est pas prise en charge par les - modules externes de PGP ou si vous utilisez du texte généré par d'autres applications, vous pouvez effectuer des opérations de cryptage / décryptage et de signature / vérification via le Presse-papiers de Windows ou dans la fenêtre de l'application courante.

Via le Presse-papiers de Windows

Par exemple, pour crypter ou signer du texte, copiez-le de votre application vers le Presse-papiers (CTRL +C), criptez et signez-le à l'aide des fonctions de PGP appropriées, puis collez-le (CTRL +V) dans votre application avant de l'envoyer aux destinataires souhaités. Lorsque vous recevez un message électronique crypté ou signé, effectuez simplement le processus inverse et copiez le texte crypté, appelé *texte chiffré*, de votre application vers le Presse-papiers, décryptez et vérifiez les informations, puis affichez-en le contenu. Après avoir décrypté le message, vous pouvez choisir entre l'enregistrement des données obtenues ou la conservation de ce texte au format crypté.

Dans la fenêtre courante

Pour procéder aux mêmes tâches cryptographiques, utilisez la commande de menu **Fenêtre courante** permettant de copier le texte de la fenêtre vers le Presse-papiers, puis d'effectuer la tâche sélectionnée.

Figure 2-2. Fonctionnalité Fenêtre courante de PGPtray

Utilisation de PGP à partir de l'Explorateur Windows

Vous pouvez crypter et signer ou décrypter et vérifier des fichiers tels que des documents provenant d'un traitement de texte, des feuilles de calcul et des clips vidéo, directement dans l'Explorateur Windows. Si vous n'utilisez pas d'application de messagerie prenant en charge le standard PGP / MIME, telle que Eudora Qualcomm, ou d'application ne requérant pas le cryptage ou la signature de fichiers, telle que Exchange ou Outlook, utilisez cette méthode pour attacher les fichiers à envoyer avec vos messages électroniques. Il est également conseillé de crypter et décrypter des fichiers stockés sur votre propre ordinateur afin d'empêcher les autres d'y accéder.

Pour accéder aux fonctions de PGP dans l'Explorateur Windows, choisissez l'option appropriée dans le sous-menu **PGP** du menu **Fichier**. Les options qui apparaissent dépendent de l'état courant du fichier sélectionné. Si le fichier n'a pas encore été crypté ou signé, les options permettant d'accéder à ces fonctions apparaissent alors dans le menu. Dans le cas contraire, les options permettant de décrypter et de vérifier le contenu du fichier apparaissent alors.

Utilisation de PGPtools

Si vous utilisez une application de messagerie qui n'est pas prise en charge par les modules externes ou si vous souhaitez utiliser des fonctions PGP à partir d'autres applications, vous pouvez crypter et signer, décrypter et vérifier ou effacer de manière sécurisée les messages et fichiers directement dans PGPtools. Pour ouvrir PGPtools, vous pouvez :

- choisir **Démarrer-->Programmes-->PGP-->PGPtools**

  ou

- cliquer sur l'icône PGPtools ( ) dans la Barre des tâches.

Lorsque PGPtools (Figure 2-3) apparaît, vous pouvez commencer le cryptage.

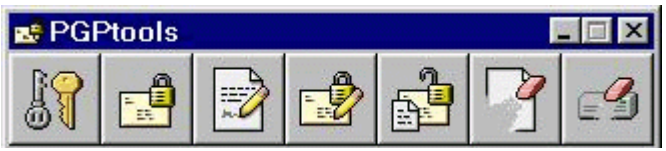


Figure 2-3. PGPtools

Si vous traitez du texte ou des fichiers, sélectionnez le texte ou le fichier, puis faites-le glisser vers le bouton approprié de PGPtools pour effectuer un cryptage, un décryptage, une signature ou une vérification.

Si vous traitez des fichiers, cliquez sur le bouton approprié dans PGPtools pour choisir un fichier ou sélectionnez le Presse-papiers.

Lorsque vous décryptez un fichier, une boîte de dialogue Enregistrer sous apparaît et PGP créée un nouveau fichier de texte en clair affecté de l'extension. txt. L'extension .txt.pgp est affectée au fichier décrypté.

Utilisation de PGP dans des applications de messagerie prises en charge

Le recours aux applications de messagerie courantes, prises en charge par les modules externes PGP, constitue l'une des plus pratiques utilisations de PGP. Utilisez ces modules externes pour procéder à un cryptage et effectuer une signature si votre version de PGP prend en charge les modules externes e-mail PGP, et pour décrypter et signer vos messages par simple clic lorsque vous êtes en train de rédiger ou lire vos messages.

Si vous utilisez une application de messagerie qui n'est pas prise en charge par les modules externes, utilisez PGP pour crypter facilement le texte de vos messages. Par ailleurs, pour crypter ou décrypter des fichiers, vous pouvez utiliser directement le Presse-papiers de Windows ou choisir l'option de menu PGP appropriée dans l'Explorateur Windows. Vous pouvez également utiliser PGP pour crypter et signer des fichiers situés sur le disque dur de votre ordinateur, afin de les stocker de manière sécurisée, et pour effacer l'espace disque libre, de telle sorte que les données ne puissent pas être récupérées à l'aide de logiciels de récupération de disque.

Si vous utilisez l'une des applications de messagerie les plus courantes et que celle-ci est prise en charge par les modules externes PGP, cliquez sur les boutons appropriés de la barre d'outils de votre application pour accéder aux fonctions de PGP requises.

- Qualcomm Eudora
- Microsoft Exchange
- Microsoft Outlook
- Microsoft Outlook Express
- Lotus Notes (disponible séparément)
- Novell Groupwise (disponible séparément)

Par exemple, cliquez sur l'icône représentant une enveloppe et un verrou () pour crypter votre message, puis sur l'icône représentant le papier et le stylo () pour le signer. Certaines applications disposent également d'une icône représentant un verrou et une plume d'oie, vous permettant d'effectuer ces deux opérations simultanément.

Lorsque vous recevez un message d'un autre utilisateur PGP, cliquez sur l'enveloppe et le verrou ouvert ou choisissez **Décrypter/Vérifier** () dans PGPtools pour décrypter le message, puis vérifier la signature numérique de votre correspondant.

Vous pouvez également cliquer sur le bouton **PGPkeys** () dans les modules externes pour accéder à la fenêtre PGPkeys à tout moment lorsque vous rédigez ou récupérez votre message électronique.

Utilisation de PGP/MIME

Si vous et votre correspondant utilisez une application de messagerie dont l'un des modules externes prend en charge le standard PGP / MIME, vous pouvez l'un et l'autre crypter et décrypter automatiquement vos messages électroniques et toute pièce jointe, lors de l'envoi ou de la récupération de vos messages. Pour ce faire, il vous suffit d'activer le cryptage PGP / MIME et les fonctions de signature dans la boîte de dialogue **Options de PGP**.

Lorsque vous recevez un message électronique d'un correspondant utilisant également cette fonctionnalité, ce message apparaît accompagné d'une icône dans la fenêtre de messages, ce qui vous indique qu'il s'agit d'un message codé PGP / MIME.

Pour décrypter le texte et les pièces jointes du message électronique codé PGP / MIME et pour vérifier toute signature numérique, cliquez deux fois sur l'icône représentant un verrou et une plume d'oie (). Si le standard PGP / MIME n'est pas utilisée, les pièces jointes restent cryptées, mais le procédé de décryptage est généralement plus important pour le destinataire.

Sélection des destinataires de fichiers ou messages électroniques cryptés

Lorsque vous envoyez un message électronique dont l'application de messagerie est prise en charge par les modules externes PGP, l'adresse e-mail du destinataire détermine les clés à utiliser lors du cryptage du contenu du message. Toutefois, si vous entrez un nom d'utilisateur ou une adresse e-mail ne correspondant à aucune des clés de votre trousseau de clés publiques, ou si vous procédez à un cryptage dans PGPtray ou PGPtools, vous devez sélectionner manuellement la clé publique du destinataire dans la boîte de dialogue **Sélection de la clé PGP**.

Pour sélectionner la clé publique d'un destinataire, déplacez l'icône représentant cette clé dans la zone de liste **Destinataires**, puis cliquez sur **OK**.

Pour plus d'informations sur le cryptage, la signature, le décryptage et la vérification de messages électroniques, reportez-vous au Chapitre 4, « Envoi et réception de messages électroniques sécurisés ». Pour plus d'informations sur le cryptage de fichiers à stocker sur votre disque dur ou à envoyer sous forme de pièces jointes, reportez-vous au Chapitre 5, « Utilisation de PGP pour le stockage sécurisé de fichiers ».

Utilisation de raccourcis

Même si l'utilisation de PGP est relativement simple, de nombreux raccourcis clavier sont disponibles et vous permettent d'effectuer des opérations de cryptage plus rapidement. Par exemple, lorsque vous procédez à la gestion de vos clés dans la fenêtre PGPkeys, vous pouvez cliquer sur le bouton droit de la souris pour effectuer toutes les fonctions de PGP requises, au lieu d' y accéder via la barre de menus. Par ailleurs, vous pouvez déplacer un fichier contenant une clé dans la fenêtre PGPkeys, afin de l'ajouter à votre trousseau de clés.

Des raccourcis clavier existent également pour la plupart des commandes de menu. Ils apparaissent dans tous les menus PGP. D'autres raccourcis sont indiqués dans certaines sections de ce manuel en fonction du contexte.

Affichage de l'aide

Lorsque vous choisissez **Aide** dans **PGPtray** ou le menu **Aide** de PGPkeys, vous accédez au système d'aide en ligne de PGP, qui offre une présentation générale et des instructions pour l'ensemble des procédures. De nombreuses boîtes de dialogue disposent d'une aide contextuelle, accessible en cliquant sur le point d'interrogation situé dans le coin supérieur droit de la fenêtre, puis en pointant vers la zone souhaitée. Une explication rapide apparaît alors.

Création et échange de clés 3

Ce chapitre décrit la génération des paires de clés publiques et privées nécessaires pour correspondre avec d'autres utilisateurs de PGP. La distribution de votre clé publique et la récupération de clés publiques provenant d'autres utilisateurs, permettant ainsi l'échange de messages électroniques privés et authentifiés, sont également expliquées.

Concepts relatifs aux clés

PGP repose sur un système de *cryptage de clé publique* largement reconnu et hautement fiable, comme indiqué à la Figure 3-1, qui met en jeu une clé publique et une clé privée, afin de permettre aux utilisateurs PGP de générer une paire de clés. Comme son nom l'indique, vous seul avez accès à votre clé privée. Toutefois, pour pouvoir correspondre avec d'autres utilisateurs PGP, vous devez disposer d'une copie de leur clé publique, et inversement. Utilisez alors votre clé privée pour signer les messages électroniques et pièces jointes que vous envoyez aux autres utilisateurs, ainsi que pour décrypter les messages et fichiers qui vous sont adressés. Inversement, vous utilisez les clés publiques des autres utilisateurs pour leur envoyer des messages électroniques cryptés et pour vérifier leurs signatures numériques.

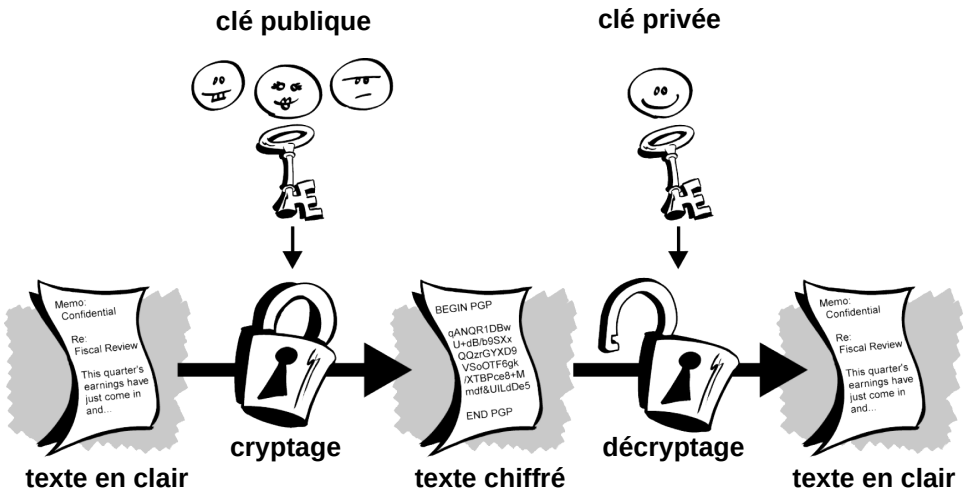


Figure 3-1. Diagramme de cryptographie de clé publique

Création d'une paire de clés

La première chose à effectuer avant d'envoyer ou de recevoir un message électronique crypté et signé est de créer une nouvelle paire de clés, si vous ne l'avez pas déjà fait avec une autre version de PGP. Une paire de clés est constituée de deux clés : une clé privée que vous seul possédez et une clé publique que vous distribuez librement à vos correspondants. Vous générez une nouvelle paire de clés à partir de PGPkeys à l'aide de l'Assistant de génération de clés de PGP qui vous guide étape par étape.

REMARQUE : Si vous avez mis à jour une version précédente de PGP, il est probable que vous ayez déjà créé une clé privée et distribué la clé publique correspondante à vos correspondants. Dans ce cas, vous n'avez pas besoin de créer une nouvelle paire de clés (comme le décrit la section suivante). Lors du lancement de l'application PGPkeys, spécifiez l'emplacement de vos clés. Pour localiser à tout moment vos fichiers de trousseaux de clés, accédez au panneau **Fichiers** de la boîte de dialogue **Options**.

Pour créer une nouvelle paire de clés

1. Ouvrez PGPkeys.

   Pour ouvrir PGPkeys :

   - Cliquez sur **Démarrer-->Programmes-->PGP-->PGPkeys**.
   - Cliquez sur l'icône PGPtray () située dans la barre des tâches, puis sur PGPkeys.

     Ou

   - Cliquez sur  dans la barre d'outils de votre application de messagerie.

L'écran PGPkeys apparaît, comme illustré à la Figure 3-2.

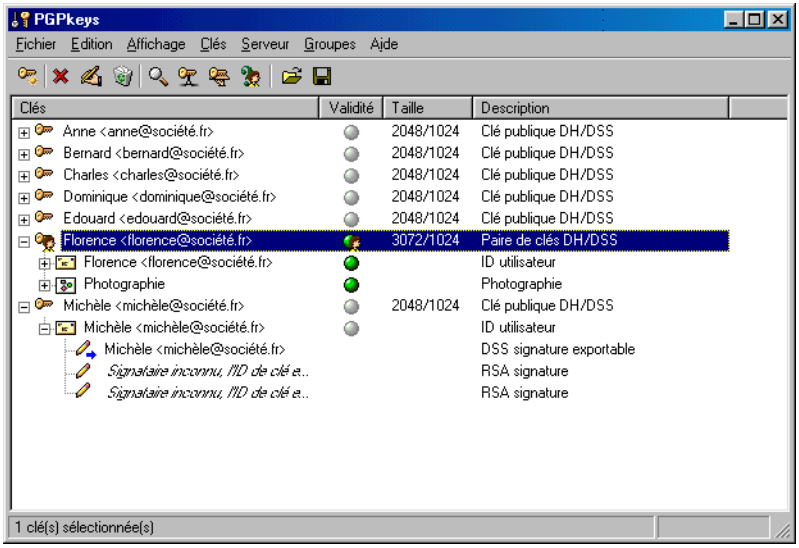


Figure 3-2. Fenêtre PGPkeys

2. Cliquez sur  dans la barre de menus PGPkeys.

   L'Assistant de génération de clés de PGP fournit des informations préliminaires sur le premier écran.

3. Après avoir lu ces informations, cliquez sur **Suivant** pour accéder au volet suivant.

   L'Assistant de génération de clés de PGP vous demande d'entrer votre nom et votre adresse e-mail.

4. Entrez votre nom sur la première ligne, puis votre adresse e-mail sur la seconde.

   Vous n'êtes pas obligé d'entrer vos nom et adresse e-mail réels. Toutefois, si vous utilisez votre vrai nom, les autres personnes peuvent vous identifier plus facilement comme le détenteur de votre clé publique.
   En entrant votre adresse e-mail correcte, vous et les autres utilisateurs pouvez bénéficier de la fonction de module externe permettant de rechercher automatiquement la clé appropriée sur votre trousseau de clés actuel lorsque vous envoyez des messages à un destinataire spécifique. Certaines clés de signature d'entreprise et clés de décryptage supplémentaires s'avèrent inutiles pour une adresse e-mail, car elles ne correspondent pas à des individus.

5. Pour accéder à la boîte de dialogue suivante, cliquez sur **Suivant**.

   L'Assistant de génération de clés vous invite à sélectionner un type de clé.

6. Sélectionnez un type de clé, Diffie-Hellman / DSS ou RSA, puis cliquez sur **Suivant**.

   REMARQUE : Si RSA n'est pas pris en charge par votre version de PGP, cette étape n'est pas disponible. Pour plus d'informations sur la gestion RSA, reportez-vous au fichier WhatsNew fourni avec le produit.

   Les versions antérieures de PGP utilisent une ancienne technologie appelée RSA pour générer des clés. Les versions 5.0 et ultérieures de PGP vous permettent de créer un nouveau type de clé en fonction de la variante Elgamal améliorée de la technologie Diffie-Hellman.

   - Pour correspondre avec des personnes utilisant encore des clés RSA, il est conseillé de créer une paire de clés RSA compatible avec d'anciennes versions de PGP.
   - Pour correspondre avec des personnes qui utilisent PGP version 5.0 ou une version suivante, vous pouvez profiter de la nouvelle technologie proposée et générer une paire de clés Diffie-Hellman / DSS.
   - Si vous souhaitez échanger des messages avec tous les utilisateurs PGP, créez une paire de clés RSA et une paire de clés Diffie-Hellman / DSS, puis utilisez à la paire appropriée à la version de PGP utilisée par le destinataire. Créez une paire de clés séparée pour chaque type de clé dont vous avez besoin.

7. L'Assistant de génération de clés de PGP vous invite à spécifier la taille de vos nouvelles clés.

   Sélectionnez une taille de clé comprise entre 1 024 et 3 072 bits ou entrez une taille de clé personnalisée comprise entre 1 024 et 4 096 bits.

   REMARQUE : La durée de génération d'une clé de taille personnalisée dépendra de la vitesse de l'ordinateur utilisé.

La taille de la clé correspond au nombre de bits utilisés pour constituer votre clé numérique. Plus la clé est grande, moins elle a de chances d'être piratée, mais plus son processus de cryptage et de décryptage est long. Vous devez parvenir à un équilibre entre l'avantage de pouvoir rapidement exécuter les fonctions PGP à l'aide d'une petite clé et le niveau de sécurité accru inhérent à une grande clé. A moins que vous n'échangiez des informations très confidentielles, la mise au point d'une attaque cryptographique coûteuse et longue, dont le but est de lire vos informations, représente peu d'intérêt. L'utilisation d'une clé de 1 024 bits est suffisamment sûre.

REMARQUE : Lorsque vous créez une paire de clés Diffie-Hellman / DSS, la taille de la partie DSS de la clé est inférieure ou égale à celle de la partie Diffie-Hellman, et elle ne doit pas dépasser 1 024 bits.

8. Pour accéder au prochain volet, cliquez sur **Suivant**.

   L'Assistant de génération de clés de PGP vous invite à entrer la date d'expiration de la paire de clés.

9. Indiquez la date d'expiration souhaitée de vos clés. Utilisez le paramètre par défaut, **Jamais**, ou entrez une date d'expiration spécifique.

   En général, une fois que vous avez créé une paire de clés et distribué votre clé publique aux autres utilisateurs, vous continuez à utiliser ces mêmes clés. Cependant, dans certaines conditions, il se peut que vous souhaitiez créer une paire de clés spéciale à utiliser pour un temps limité. Dans ce cas, lorsque la clé publique expire, les utilisateurs ne peuvent plus l'utiliser pour crypter des messages pour vous, mais il peuvent continuer à l'utiliser pour vérifier votre signature numérique. De la même façon, lorsque votre clé privée expire, vous pouvez continuer à l'utiliser pour décrypter des messages qui vous ont été envoyés avant l'expiration de votre clé publique, même si elle ne peut plus servir à signer les messages pour d'autres.

10. Pour accéder au prochain volet, cliquez sur **Suivant**.

    L'Assistant de génération de clés de PGP vous invite à entrer un mot de passe complexe.

11. Dans la boîte de dialogue **Mot de passe complexe**, entrez la chaîne de caractères ou de mots vous garantissant l'accès exclusif à votre clé privée. Pour confirmer votre entrée, appuyez sur la touche Tabulation pour passer à la ligne suivante, puis entrez à nouveau le même mot de passe complexe.

Généralement, pour améliorer la sécurité, les caractères entrés pour le mot de passe complexe n'apparaissent pas à l'écran. Toutefois, si vous êtes sûr que personne ne regarde par-dessus votre épaule et si vous souhaitez voir les caractères de votre mot de passe complexe lors de sa saisie, décochez la case **Masquer la saisie**.

REMARQUE : Votre mot de passe complexe doit comprendre plusieurs mots, des espaces, des nombres, ainsi que des caractères de ponctuation. Choisissez-en un dont vous pourrez facilement vous souvenir, mais que les autres utilisateurs auront du mal à deviner. Un mot de passe complexe est sensible à la casse, ce qui signifie qu'il distingue les lettres majuscules des minuscules. Plus votre mot de passe complexe est long, plus les types de caractères qu'il contient sont nombreux, plus il est sécurisé. Les mots de passe complexes efficaces contiennent des majuscules, des minuscules, des nombres, des caractères de ponctuation et des espaces, mais peuvent s'oublier plus facilement. Pour plus d'informations sur le choix d'un mot de passe complexe, reportez-vous à la section « Création d'un mot de passe complexe facile à mémoriser » à la page 30.

AVERTISSEMENT : Si vous oubliez votre mot de passe complexe, il est impossible, même par Network Associates, de le récupérer.

12. Pour lancer le processus de génération d'une clé, cliquez sur **Suivant**.

    L'Assistant de génération de clés de PGP indique qu'il est en train de générer votre clé.

    Si vous avez entré un mot de passe complexe inadéquat, un message d'avertissement apparaît préalablement à la génération des clés. Vous pouvez alors accepter ce mot de passe ou en entrer un plus sécurisé avant de poursuivre. Pour plus d'informations sur les mots de passe complexes, reportez-vous à la section « Création d'un mot de passe complexe facile à mémoriser » à la page 30.

    Si les informations aléatoires requises pour constituer la clé sont insuffisantes, la boîte de dialogue **Données aléatoires de PGP** apparaît. Comme indiqué dans cette boîte de dialogue, déplacez votre pointeur, puis entrez une séquence de touches aléatoires jusqu'à ce que la barre de progression soit complètement remplie. Les mouvements de la souris et les séquences de touches génèrent des informations aléatoires nécessaires à la création d'une paire de clés unique.

REMARQUE : PGPkeys collecte en permanence les données aléatoires à partir de nombreuses sources du système, parmi lesquelles les positions de la souris, les durées et les séquences de touches. Si la boîte de dialogue des données aléatoires n'apparaît pas, ceci signifie que PGP a déjà collecté toutes les données aléatoires nécessaires à la création de la paire de clés.

Une fois lancé, le processus de génération de clés peut prendre un certain temps. Si vous spécifiez une taille différente de celle par défaut pour une clé Diffie-Hellman / DSS, la fonction de génération de clés rapide n'est pas utilisée. La génération de votre clé peut alors prendre des heures. A la fin du processus, l'Assistant de génération de clés indique qu'il a terminé.

13. Pour accéder au prochain volet, cliquez sur **Suivant**.

    L'Assistant de génération de clés indique que vous venez de générer une nouvelle paire de clés et vous demande si vous souhaitez envoyer votre clé publique vers un serveur de certificats.

14. Indiquez si vous souhaitez envoyer votre nouvelle clé publique vers le serveur, puis cliquez sur **Suivant** (le serveur par défaut est défini dans la boîte de dialogue **Options du serveur**).

    En envoyant votre clé publique vers le serveur de certificats, vous permettez à tout utilisateur pouvant accéder à ce serveur d'obtenir, lorsqu'il en a besoin, une copie de votre clé. Pour plus d'informations, reportez-vous à la section « Distribution d'une clé publique » à la page 52.

    Une fois le processus de génération de clé terminé, le panneau final apparaît.

15. Cliquez sur **Terminer**.

    Une paire de clés représentant vos nouvelles clés apparaît dans la fenêtre PGPkeys. Vous pouvez alors examiner vos clés en vérifiant leurs propriétés, ainsi que les attributs qui y sont associés. Peut-être souhaitez-vous également ajouter vos autres adresses e-mail. Pour plus d'informations sur la modification des informations de votre paire de clés, reportez-vous à la section « Ajout d'un nouveau nom ou d'une nouvelle adresse d'un utilisateur à une paire de clés » à la page 36.

Création d'un mot de passe complexe facile à mémoriser

Se retrouver dans l'incapacité de décrypter un fichier car on a oublié son mot de passe complexe est une expérience douloureuse. La plupart des applications requièrent un mot de passe constitué de trois à huit lettres. Un mot de passe constitué d'un seul mot est vulnérable face à une attaque « au dictionnaire », qui consiste à utiliser un ordinateur testant tous les mots du dictionnaire jusqu'à ce que le bon mot de passe soit découvert. Pour se protéger contre ce type d'attaque, il est vivement conseillé de créer un mot constitué d'une combinaison de lettres majuscules et minuscules, de nombres, de caractères de ponctuation et d'espaces. Il en résulte un mot de passe complexe efficace, mais difficile à mémoriser. Il est donc déconseillé d'utiliser un seul mot dans votre mot de passe complexe.

Un mot de passe complexe est moins vulnérable vis-à-vis d'une attaque « au dictionnaire ». Utilisez plusieurs mots pour le constituer, plutôt que de tenter de déjouer une attaque « au dictionnaire » en juxtaposant arbitrairement plusieurs caractères amusants, pour obtenir un mot de passe complexe difficile à mémoriser et risquer de perdre vos informations, car vous seriez dans l'impossibilité de décrypter vos propres fichiers. Toutefois, à moins que le mot de passe complexe choisi ne corresponde à quelque chose que vous avez en mémoire depuis longtemps, sa mémorisation, caractère pour caractère, paraît très difficile. Si vous choisissez une phrase selon l'inspiration du moment, il ne fait aucun doute que vous l'oublierez totalement. Utilisez des éléments que vous avez en mémoire depuis longtemps, par exemple, une phrase anecdotique que vous avez entendue il y a des années et que vous n'avez pas oubliée. Il ne doit pas s'agir de quelque chose dont vous avez fait part à vos proches récemment, ni d'une citation célèbre, car les experts en piratage ne doivent pas être en mesure de le deviner facilement. S'il s'agit de quelque chose qui est ancré dans votre mémoire depuis longtemps, vous ne l'oublierez probablement pas.

Bien entendu, le choix de votre mot de passe complexe importe peu, si vous êtes insouciant au point de le noter, de l'enregistrer sur votre ordinateur ou de le conserver dans le tiroir de votre bureau.

Copie de sauvegarde des clés

Après avoir généré une paire de clés, il est préférable d'en conserver une copie dans un endroit sûr. Une fois que vous venez de créer une nouvelle paire de clés, PGP vous invite à enregistrer une copie de sauvegarde lors de la fermeture de l'application PGPkeys.

Vos clés privées et publiques sont stockées dans des fichiers de trousseaux de clés séparés, que vous pouvez copier comme tout autre fichier vers un autre emplacement de votre disque dur ou sur une disquette. Par défaut, les trousseaux de clés privées et publiques (secring.skr et pubring.pkr) sont stockés avec les autres fichiers de programmes dans le dossier « PGP Keyrings », lui-même placé dans votre dossier PGP, mais vous pouvez enregistrer vos copies de sauvegarde où vous le souhaitez.

PGP vous invite régulièrement à effectuer une sauvegarde de vos clés. Lorsque vous spécifiez l'enregistrement d'une copie de sauvegarde de vos clés, la boîte de dialogue **Enregistrer sous** apparaît, vous demandant de spécifier l'emplacement de la création de la copie de sauvegarde des fichiers de trousseaux de clés publiques et privées.

Protection des clés

Outre la création de copies de sauvegarde de vos clés, vous devez être particulièrement attentif à l'emplacement de stockage de votre clé privée. Même si votre clé privée est protégée par un mot de passe complexe dont vous seul avez connaissance, il est possible qu'une autre personne parvienne à le découvrir, puis utilise votre clé privée afin de déchiffrer vos messages électroniques ou de falsifier votre signature numérique. Par exemple, une personne peut découvrir vos séquences de touches en regardant par-dessus votre épaule lorsque vous saisissez votre mot de passe complexe ou en les interceptant sur le réseau ou même via les ondes radio.

Pour empêcher quiconque ayant pu intercepter votre mot de passe complexe d'utiliser votre clé privée, stockez cette dernière uniquement sur votre ordinateur. Si celui-ci est relié à un réseau, assurez-vous que vos fichiers ne sont pas automatiquement inclus dans une copie de sauvegarde commune à l'ensemble du système, permettant ainsi à d'autres personnes d'avoir accès à votre clé privée. Etant donné la facilité d'accès aux ordinateurs via les réseaux, si vous utilisez des informations extrêmement confidentielles, il est conseillé de stocker votre clé privée sur une disquette. Vous pouvez alors utiliser cette dernière, de la même façon qu'une clé classique, lorsque vous souhaitez lire ou signer des informations confidentielles.

Une autre précaution consiste à attribuer un nom différent à votre fichier de trousseaux de clés privées, puis à le stocker à un emplacement difficile à localiser, autre que le dossier PGP par défaut. Pour définir le nom et l'emplacement de vos fichiers de trousseaux de clés publiques et privées, utilisez le panneau **Fichiers** situé dans la boîte de dialogue **Options de PGPkeys**.

Ajout et suppression des informations d'une paire de clés

Vous pouvez ajouter, modifier ou supprimer les éléments suivants à tout moment :

- l'ID photographique
- les sous-clés supplémentaires
- le nom et l'adresse de l'utilisateur
- les autorités de révocation désignées
- le certificat X.509
- le mot de passe complexe

Ajout d'un ID photographique à une clé

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

AVERTISSEMENT : Même si vous pouvez afficher l'ID photographique d'une personne avec sa clé à des fins de vérification, vous devez toujours contrôler et comparer les empreintes digitales. Pour plus d'informations sur l'authentification, reportez-vous à la section « Vérification de la clé publique d'un autre utilisateur » à la page 103.

Pour ajouter votre photographie à votre clé

1. Ouvrez PGPkeys.
2. Sélectionnez votre paire de clés, puis cliquez sur **Ajout d'une photo** dans le menu **Clés**.

La boîte de dialogue **Ajout d'une photo** apparaît, comme indiqué à la Figure 3-3.

Figure 3-3. Boîte de dialogue Ajout d'une photo

3. Faites glisser ou collez votre photographie dans cette boîte de dialogue, ou cliquez sur **Sélectionner un fichier** pour accéder à votre photographie.

REMARQUE : La photographie doit se trouver au format .BMP ou .JPG. Pour obtenir une qualité d'image maximale, dimensionnez votre image à une taille de 120 x 144 avant de l'ajouter dans la boîte de dialogue **Ajout d'une photo**. Si vous n'effectuez pas cette opération, PGP dimensionne la photographie pour vous.

---

4. Cliquez sur **OK**.

   La boîte de dialogue **Mot de passe complexe** apparaît, comme illustré à la Figure 3-4.

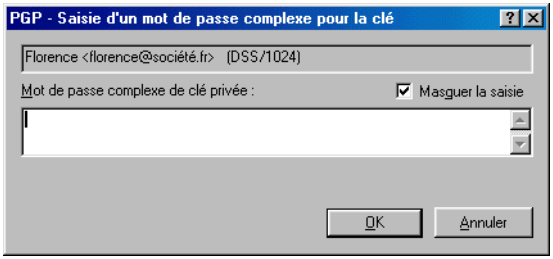


Figure 3-4. Boîte de dialogue Mot de passe complexe

5. Entrez le mot de passe complexe dans la zone correspondante, puis cliquez sur **OK**.

   Votre ID utilisateur photographique s'ajoute à votre clé publique et apparaît dans la fenêtre PGPkeys. Vous pouvez désormais envoyer votre clé vers le serveur. Pour plus d'informations, reportez-vous à la section « Pour envoyer votre clé publique vers un serveur de certificats » à la page 53.

Pour remplacer votre ID photographique

1. Ouvrez PGPkeys.
2. Sélectionnez votre paire de clés.
3. Sélectionnez la photographie à remplacer.
4. Choisissez **Supprimer** dans le menu **Edition**.
5. Ajoutez votre nouvel ID photographique en vous conformant aux instructions fournies dans la section « Pour ajouter votre photographie à votre clé » à la page 32.

Création de nouvelles sous-clés

Chaque clé Diffie-Hellman / DSS comporte en réalité deux clés : une clé de signature DSS et une sous-clé de cryptage Diffie-Hellman. La version 6.5 de PGP offre la possibilité de créer et de révoquer de nouvelles clés de cryptage sans sacrifier votre clé de signature maître et les signatures qui y figurent. L'une des utilisations les plus fréquentes de cette fonction consiste à créer plusieurs sous-clés, conçues pour être utilisées à différents moments de la durée de vie d'une clé. Par exemple, si vous créez une clé dont l'expiration est prévue dans trois ans, vous pouvez également créer trois sous-clés et utiliser chacune d'elles au cours de la durée de vie de cette clé. Cette mesure de sécurité peut s'avérer très utile, car elle permet automatiquement de basculer, à un moment donné, vers une nouvelle clé de cryptage sans avoir à recréer et à distribuer une nouvelle clé publique.

Pour créer de nouvelles sous-clés

1. Ouvrez PGPkeys.
2. Sélectionnez votre paire de clés, puis cliquez sur **Propriétés** dans le menu **Clés**, ou cliquez sur  .

   La boîte de dialogue **Propriétés** apparaît.
3. Cliquez sur l'onglet **Sous-clés**.

   La boîte de dialogue **Sous-clés** apparaît, comme illustré à la Figure 3-5.

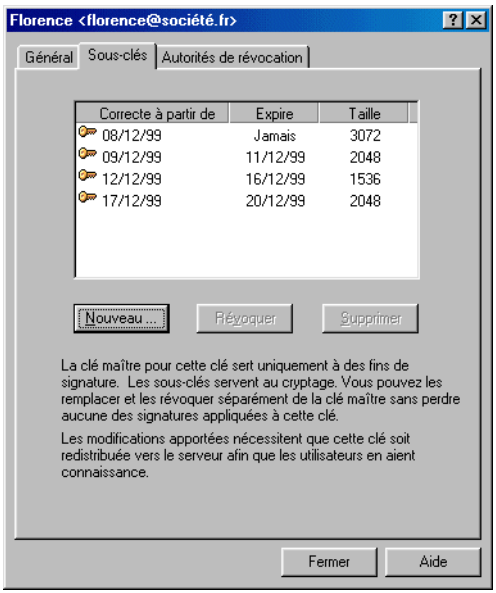


Figure 3-5. Page de propriétés des clés de PGP (boîte de dialogue Sous-clés)

4. Pour créer une nouvelle sous-clé, cliquez sur **Nouveau**.

   La boîte de dialogue **Nouvelle sous-clé** apparaît.
5. Sélectionnez une taille de clé comprise entre 1 024 et 3 072 bits, ou entrez une taille de clé personnalisée comprise entre 1 024 et 4 096 bits.
6. Définissez la date à laquelle vous souhaitez commencer à activer votre sous-clé.
7. Indiquez la date d'expiration souhaitée de votre sous-clé. Utilisez le paramètre par défaut, **Jamais**, ou entrez une date d'expiration spécifique.

8. Cliquez sur **OK**.

   La boîte de dialogue **Mot de passe complexe** apparaît.

9. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

   Votre nouvelle sous-clé apparaît dans la fenêtre correspondante.

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

Vous pouvez utiliser de plusieurs noms ou adresses e-mail d'utilisateurs pour la même paire de clés. Une fois une nouvelle paire de clés créée, vous pouvez ajouter différents noms et adresses à ces clés. Cependant, pour ajouter un nouveau nom d'utilisateur ou une nouvelle adresse e-mail, vous devez disposer de clés publiques et privées.

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

1. Ouvrez PGPkeys.
2. Sélectionnez la paire de clés à laquelle vous souhaitez ajouter un autre nom ou une autre adresse d'utilisateur.
3. Choisissez **Ajouter un nom** dans le menu **Clés**.

   La boîte de dialogue **Nouveau nom utilisateur de PGP** apparaît (Figure 3-6).

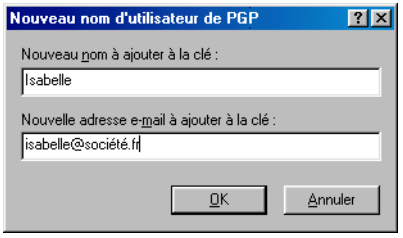


Figure 3-6. Boîte de dialogue Nouveau nom utilisateur de PGP

4. Entrez le nouveau nom et la nouvelle adresse e-mail dans les zones correspondantes, puis cliquez sur **OK**.

   La boîte de dialogue **Saisie d'un mot de passe complexe** de PGP apparaît.

5. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

   Le nouveau nom est ajouté à la fin de la liste des noms d'utilisateurs associée à cette clé. Pour définir le nouveau nom et la nouvelle adresse de l'utilisateur comme identifiants principaux de votre clé, sélectionnez-les, puis choisissez **Définir comme nom principal** dans le menu **Clés**.

Ajout d'une autorité de révocation désignée

Il est possible d'oublier son mot de passe complexe un jour ou de perdre sa clé privée. Si cela devait vous arriver, vous ne pourriez plus jamais utiliser votre clé et vous n'auriez aucune possibilité de révoquer votre ancienne clé lors de la création d'une nouvelle. Pour vous protéger de cette éventualité, vous pouvez désigner une autorité de révocation de clés de partie tierce sur votre trousseau de clés publiques, afin de révoquer votre clé. Cette partie tierce sera en mesure de révoquer votre clé DH / DSS, de l'envoyer au serveur, comme si c'était vous-même qui le faisiez.

Pour ajouter une autorité de révocation désignée à votre clé

1. Ouvrez PGPkeys.
2. Sélectionnez la paire de clés pour laquelle vous souhaitez désigner une autorité de révocation.
3. Sélectionnez **Ajouter une autorité de révocation** dans le menu **Clés**.

   Une liste de clés apparaît dans une boîte de dialogue.
4. Sélectionnez la(les) clé(s) dans la liste ID utilisateur devant être désignée(s) comme autorité de révocation.
5. Cliquez ensuite sur **OK**.

   Une boîte de dialogue de confirmation apparaît.
6. Pour continuer, cliquez sur **OK**.

   La boîte de dialogue **Mot de passe complexe** apparaît.
7. Saisissez votre mot de passe complexe, puis cliquez sur **OK**.
8. La(les) clé(s) sélectionnée(s) est(sont) maintenant autorisée(s) à révoquer votre clé. Pour gérer les clés de manière efficace, distribuez une copie actuelle de votre clé à ou aux autorité(s) de révocation ou téléchargez votre clé vers le serveur. Pour plus d'informations, reportez-vous à la section « Distribution d'une clé publique » à la page 52.

Ajout d'un certificat X.509 à une clé PGP

REMARQUE : Cette section décrit comment ajouter un certificat X.509 à votre paire de clés si vous utilisez Net Tools PKI Server.

Un certificat numérique X.509 est un document électronique reconnu, permettant de prouver l'identité et l'appartenance de la clé publique au sein d'un réseau de communication.

Vous pouvez utiliser les options des menus de PGP et l'*autorité de certification* (CA) de votre société (ou une CA publique, telle que VeriSign) pour faire la demande d'un certificat numérique X.509 et l'ajouter à votre paire de clés.

L'ajout d'un certificat X.509 s'effectue en quatre étapes principales. Récupérez le certificat de la CA par défaut auprès de l'autorité de certification (CA), puis ajoutez-le à votre trousseau de clés PGP. Entrez ensuite des informations relatives à la CA dans le panneau des options de la CA. Faites une demande de certificat auprès de la CA. Votre demande de certificat X.509 est vérifiée, puis signée par la CA. La signature de la CA apposée à ce certificat permet de détecter toute falsification subséquente à l'aide des informations d'authentification ou de la clé publique. Cette signature implique que la CA considère les informations contenues dans le certificat comme valides. Enfin, récupérez le certificat émis par la CA, puis ajoutez-le à votre paire de clés.

Pour ajouter un certificat X.509 à votre paire de clés PGP

1. **Après avoir obtenu le certificat de la CA par défaut, ajoutez-le à votre trousseau de clés PGP.**

   Pour ce faire, procédez comme suit :

   1. Ouvrez votre navigateur Web et connectez-vous au site d'inscription à la CA. Si vous ne connaissez pas l'URL de ce site, consultez l'administrateur PGP ou PKI de votre entreprise.

   2. Cliquez sur le lien **Download a CA Certificate**. Dans la liste déroulante, sélectionnez une autorité de certification et le certificat approprié.

3. Cliquez sur **Examine this Certificate**, copiez le bloc de clé pour le certificat de la CA par défaut, puis collez-le dans votre fenêtre PGPkeys.

   La boîte de dialogue **d'importation de clés** apparaît et importe le certificat de la CA par défaut sur votre trousseau de clés.

4. Signez le certificat de la CA par défaut avec votre clé afin de le rendre valide, ouvrez la boîte de dialogue Propriétés des clés, puis définissez le niveau de fiabilité. La fiabilité doit être définie sur la CA par défaut.

2. Configurez le panneau d'options de la CA.

Pour ce faire, procédez comme suit :

1. Choisissez **Options** dans le menu **Edition** de PGPkeys, puis cliquez sur l'onglet **CA**.

   Le panneau **CA** apparaît, comme illustré à la Figure 3-7.

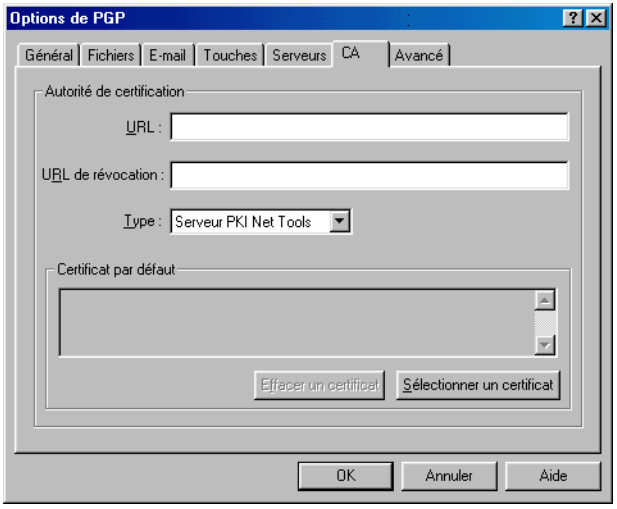


Figure 3-7. Boîte de dialogue Options de PGP (panneau CA)

2. Entrez l'URL de la CA dans la zone de texte **URL de l'autorité de certification**, par exemple, https://nnn.nnn.nnn.nnn:nnnnn (il 'sagit de la même URL que celle utilisée pour récupérer la CA par défaut).

3. S'il existe une URL distincte pour la récupération des listes de révocation des certificats (LRC), entrez-la dans la zone de texte correspondante.

   Si vous ne connaissez pas l'URL de la CA de révocation, ne renseignez pas ce champ, ou consultez l'administrateur PGP ou PKI de votre entreprise.

4. Dans la zone **Type**, spécifiez le nom de l'autorité de certification que vous êtes en train d'utiliser. Sélectionnez l'une des options suivantes :

   - Net Tools PKI Server
   - VeriSign OnSite
   - Entrust

5. Cliquez sur **Sélectionner le certificat**, puis sélectionnez le certificat de la CA par défaut que vous venez de récupérer.

La zone de texte **Certificat par défaut** affiche les informations relatives au certificat de la CA par défaut sélectionné. La terminologie utilisée correspond à une décision de principe. Pour les certificats X.509, la terminologie suivante est généralement respectée :

NC (Nom commun)	Description du type de certificat (par exemple, « Par défaut »).
EMAIL	Adresse e-mail du détenteur du certificat.
UO (Unité organisationnelle)	Service de l'entreprise auquel le certificat appartient (par exemple, la « comptabilité »).
O (Organisme)	Nom de l'entreprise à laquelle le certificat appartient (par exemple, « Securité Cie »).
L (Localité)	Emplacement précis où se trouve le détenteur du certificat (par exemple, « Paris »).

6. Cliquez sur **OK**.

3. Faites une demande de certificat.

Pour ce faire, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur votre paire de clés PGP, puis sélectionnez **Clés --> Ajouter un certificat** dans le menu contextuel.

   La boîte de dialogue **Attributs du certificat** apparaît, comme illustré à la Figure 3-8.

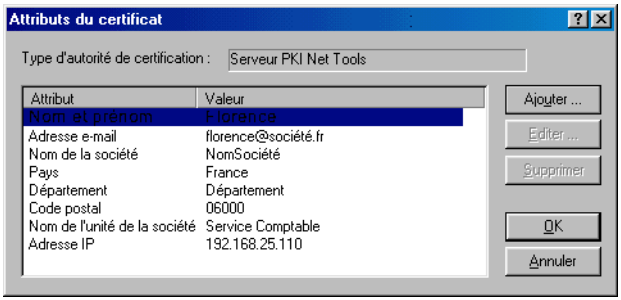


Figure 3-8. Boîte de dialogue Attributs du certificat

2. Vérifiez les attributs du certificat, utilisez les boutons **Ajouter**, **Modifier** et **Supprimer** pour apporter les modifications nécessaires, puis cliquez sur **OK**. La boîte de dialogue **PGP – Saisie d'un mot de passe complexe** apparaît.

3. Entrez le mot de passe complexe pour votre paire de clés, puis cliquez sur **OK**.

   La **barre de progression du serveur PGP** apparaît, comme illustré à la (Figure 3-9).

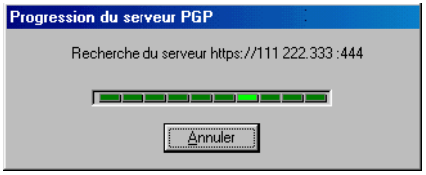


Figure 3-9. Barre de progression du serveur PGP

La demande de certificat est envoyée au serveur CA. Celui-ci est authentifié alors auprès de votre ordinateur et accepte votre demande.

L'administrateur PKI ou PGP de votre entreprise vérifie les informations de votre demande. Les informations d'identification et la clé publique sont rassemblées, puis signées numériquement avec le propre certificat de la CA afin de créer votre nouveau certificat.

L'administrateur vous envoie un message électronique indiquant que votre certificat peut à présent être récupéré.

4. **Récupérez votre certificat, puis ajoutez-le à votre paire de clés.**

   Pour ce faire, procédez comme suit :

   1. Dans PGPkeys, sélectionnez la clé PGP pour laquelle vous avez effectué la demande de certificat.
   2. Dans le menu **Serveur**, sélectionnez **Récupérer le certificat**.

      PGP contacte le serveur CA, récupère automatiquement votre nouveau certificat X.509, puis l'ajoute à votre clé PGP.
   3. Si vous exécutez PGPnet, définissez ce certificat comme votre clé d'authentification X.509 dans PGPnet **(Affichage -> Options -> Authentification**).

Modification d'un mot de passe complexe

Il est judicieux de modifier votre mot de passe complexe à intervalles réguliers, par exemple, tous les trois mois. Il est plus important encore de modifier votre mot de passe complexe lorsque vous pensez qu'il est compromis, par exemple, lorsqu'une perrsonne a regardé par-dessus votre épaule au moment où vous l'avez entré.

Pour modifier votre mot de passe complexe.

1. Ouvrez PGPkeys.
2. Sélectionnez la clé dont vous souhaitez modifier le mot de passe complexe.
3. Sélectionnez **Propriétés** dans le menu **Clés** ou cliquez sur  pour ouvrir la boîte de dialogue **Propriétés**.

La boîte de dialogue **Propriétés** apparaît, comme illustré à la Figure 3-10.

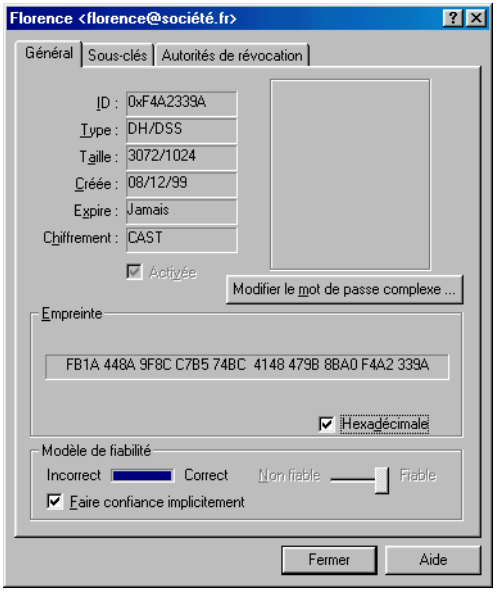


Figure 3-10. Boîte de dialogue Propriétés (panneau Général)

4. Cliquez sur **Modifier le mot de passe complexe**.

   La boîte de dialogue **Mot de passe complexe** apparaît.

   REMARQUE : Si vous souhaitez modifier le mot de passe complexe pour une clé découpée, assemblez d'abord les parties de cette clé. Pour collecter les parties de clé, cliquez sur Assembler. Pour plus d'informations sur la collecte des parties de clé, reportez-vous à la section « Signature et décryptage de fichiers avec une clé découpée » à la page 83.

   ---

5. Entrez votre mot de passe complexe actuel dans la zone correspondante, puis cliquez sur **OK**.

   La boîte de dialogue **Modifier le mot de passe complexe** apparaît.

6. Entrez votre nouveau mot de passe complexe dans la première zone de texte. Pour accéder à la zone de texte suivante, appuyez sur la touche de TABULATION, puis confirmez votre saisie en entrant à nouveau votre mot de passe complexe.

7. Cliquez sur **OK**.

AVERTISSEMENT : Si vous modifiez votre mot de passe complexe car vous pensez qu'il est compromis, effacez tous les trousseaux de clés de sauvegarde, ainsi que l'espace libre de votre ordinateur.

Suppression d'une clé ou d'une signature sur un trousseau de clés PGP

Il se peut que vous souhaitiez supprimer une clé ou une signature de votre trousseau de clés PGP. La suppression d'une clé ou d'une signature à partir d'une clé est définitive. Vous pouvez à nouveau ajouter les signatures et les ID utilisateurs à une clé. Vous pouvez à nouveau importer une clé publique vers votre trousseau. Cependant, vous ne pouvez pas créer à nouveau une clé privée existant uniquement sur ce trousseau et vous ne pouvez plus décrypter tous les messages cryptés vers les copies de clés publiques.

REMARQUE : Pour plus d'informations sur la suppression d'une signature ou d'un ID utilisateur associés à votre clé publique sur un serveur de certificats, reportez-vous à la section « Mise à jour d'une clé sur un serveur de certificats » à la page 54.

Pour supprimer une clé ou une signature sur votre trousseau de clés PGP

1. Ouvrez PGPkeys.
2. Sélectionnez la clé ou la signature à supprimer.
3. Choisissez **Supprimer** dans le menu **Edition** ou cliquez sur  dans la barre d'outils de PGPkeys.

   La boîte de dialogue **Confirmation** apparaît.
4. Cliquez sur **OK**.

Découpage et reconstitution des clés

Il est possible de découper une clé privée quelconque entre plusieurs « détenteurs de parties de clé » à l'aide d'un procédé cryptographique appelé découpage de clé de Blakely-Shamir. Il est recommandé d'utiliser cette technique pour des clés dont le niveau de sécurité est très élevé. Par exemple, Network Associates distribue un découpage de sa clé d'entreprise à plusieurs individus. Cette clé est reconstituée temporairement, chaque fois qu'une signature est nécessaire.

Découpage d'une clé

Pour ce faire, sélectionnez la paire de clés à découper, puis choisissez **Découper la clé** dans le menu **Clés**. Vous êtes ensuite invité à définir le nombre de parties nécessaires à la reconstitution de cette clé. Les parties sont enregistrées en tant que fichiers cryptés vers la clé publique d'un détenteur de parties de clé ou cryptées via une méthode de cryptage conventionnel, dans le cas où le détenteur de parties de clé ne possède pas de clé publique. Une fois la clé découpée, lorsque vous essayez d'effectuer des opérations de signature ou de décryptage à l'aide de cette dernière, une tentative de reconstitution de cette clé est lancée automatiquement. Pour plus d'informations sur la reconstitution d'une clé découpée, reportez-vous à la section « Signature et décryptage de fichiers avec une clé découpée » à la page 83.

Pour découper une clé en plusieurs parties

1. Ouvrez PGPkeys.
2. Dans PGPkeys, créez une nouvelle paire de clés ou sélectionnez une paire existante à découper.
3. Dans le menu **Clés**, cliquez sur **Découper la clé**.

   La boîte de dialogue **Découper la clé** apparaît (Figure 3-11) au-dessus de la fenêtre PGPkeys.

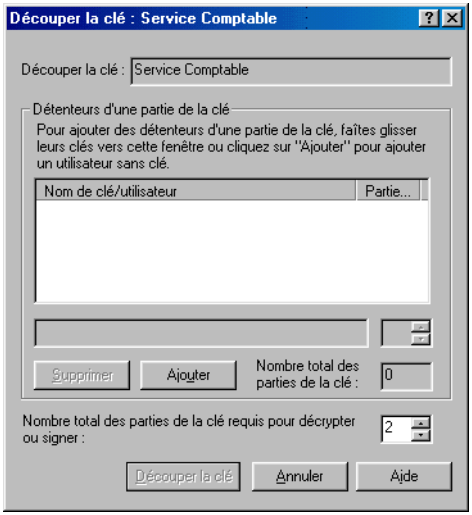


Figure 3-11. Boîte de dialogue Découper la clé

4. Ajoutez des détenteurs de parties de clé à la paire de clés en faisant glisser leurs clés de la fenêtre PGPkeys vers la liste des **détenteurs de parties de clé** de la boîte de dialogue **Découper la clé**.

   Pour ajouter un détenteur de partage qui ne possède pas de clé publique, cliquez sur **Ajouter** dans la boîte de dialogue **Découper en partages**, entrez le nom de cette personne, puis demandez-lui de saisir son mot de passe complexe.

5. Lorsque l'ensemble des détenteurs de parties de clé est répertorié, vous pouvez spécifier le nombre de parties de clé nécessaires au décryptage ou à la signature via cette clé.

   A la Figure 3-12, par exemple, le nombre total de parties constituant la clé du service comptable est égal à quatre et le nombre total de parties de clé nécessaires au décryptage ou à la signature est égal à trois. Ceci fournit une mémoire temporaire, dans le cas où l'un des détenteurs de parties de clé ne serait pas en mesure de fournir sa partie de clé ou qu'il aurait oublié son mot de passe complexe.

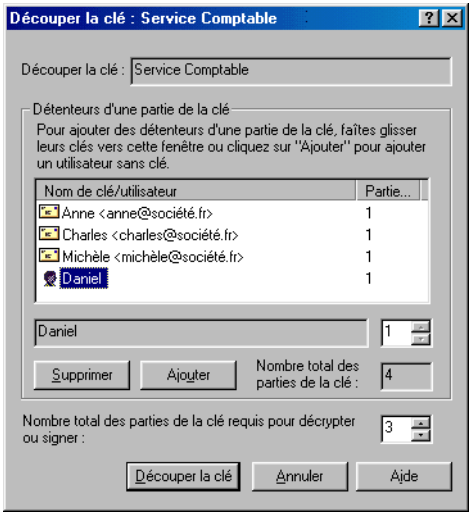


Figure 3-12. Boîte de dialogue Découper la clé (exemple)

Par défaut, chaque détenteur est responsable d'une partie de la clé. Pour augmenter le nombre de parties possédées par un détenteur, cliquez sur le nom souhaité du détenteur figurant dans la liste afin de l'afficher dans la zone de texte apparaissant en dessous. Pour sélectionner un nouveau nombre de parties de clé, saisissez une valeur ou utilisez les flèches.

6. Cliquez sur **Découper la clé**.

   Une boîte de dialogue apparaît, vous invitant à sélectionner un répertoire pour le stockage des parties de clé.

7. Sélectionnez un emplacement de stockage des parties de clé.

   La boîte de dialogue **Mot de passe complexe** apparaît.

8. Entrez le mot de passe complexe de la clé à découper, puis cliquez sur **OK**.

   Une boîte de dialogue de confirmation apparaît.

9. Pour découper la clé, cliquez sur **Oui**.

   La clé est alors découpée et les parties obtenues sont enregistrées à l'emplacement spécifié. Le nom du fichier enregistré pour chaque partie de la clé correspond à celui du détenteur et présente une extension .SHF, comme illustré ci-dessous :

10. Distribuez les parties de clé aux détenteurs, puis supprimez les copies en local.

    Une fois qu'une clé est découpée entre les divers détenteurs d'une partie de la clé, PGP tente de reconstituer automatiquement cette clé si vous souhaitez l'utiliser pour signer ou décrypter. Pour plus d'informations sur la reconstitution d'une clé découpée pour signer ou décrypter des fichiers, reportez-vous à la section « Signature et décryptage de fichiers avec une clé découpée » à la page 83.

Reconstitution des clés découpées

Une fois qu'une clé est découpée entre divers détenteurs de parties de clé, PGP tente de reconstituer automatiquement cette clé si vous souhaitez l'utiliser pour signer ou décrypter. Il existe deux méthodes de reconstitution de clés : la reconstitution locale et la reconstitution distante.

La reconstitution locale nécessite la présence des détenteurs d'une partie de la clé près de l'ordinateur devant effectuer cette opération. Chaque détenteur d'une partie de la clé doit entrer le mot de passe complexe correspondant à sa partie de clé.

La reconstitution distante nécessite que les détenteurs d'une partie de la clé distants s'identifient et décryptent leurs clés avant de les envoyer via le réseau. La sécurité de la couche de transport (TLS) de PGP fournit une liaison sécurisée pour le transport des parties de la clé, ce qui permet à plusieurs personnes distantes les unes des autres d'utiliser leur partie de clé pour signer ou décrypter de manière sécurisée.

IMPORTANT : Avant la réception des parties de la clé via le réseau, il est conseillé de vérifier l'empreinte digitale de chaque détenteur d'une partie et de signer sa clé publique afin de s'assurer que sa clé d'authentification est valide. Pour plus d'informations sur la vérification d'une paire de clés, reportez-vous à la section « Vérification de clés à l'aide d'une empreinte digitale » à la page 63.

Pour reconstituer une clé

1. Contactez chaque détenteur d'une partie de la clé découpée. Pour reconstituer une clé localement, les détenteurs de parties de cette clé doivent être présents.

   Pour collecter les parties de clé via le réseau, assurez-vous que les détenteurs sont prêts à envoyer leur fichier de parties de clé. Les détenteurs distants doivent disposer des éléments suivants :

   – leur fichier de parties de clé et leur mot de passe complexe ;

   – une paire de clés (pour s'identifier sur l'ordinateur collectant les parties de la clé) ;

   – une connexion réseau ;

   – l'adresse IP ou le nom de domaine de l'ordinateur collectant les parties de la clé.

2. Sur l'ordinateur reconstituant la clé, sélectionnez le(les) fichier(s) à signer ou décrypter avec la clé découpée via l'Explorateur Windows.

3. Cliquez sur le(les) fichier(s) avec le bouton droit de la souris, puis sélectionnez **Signer ou Décrypter** dans le menu **PGP**.

   La clé découpée sélectionnée apparaît dans la boîte de dialogue **PGP – Saisie d'un mot de passe complexe pour la clé sélectionnée**.

4. Pour reconstituer la clé sélectionnée, cliquez sur **OK**.

La boîte de dialogue **Collecte de parties de clés** apparaît, comme illustré à la Figure 3-13.

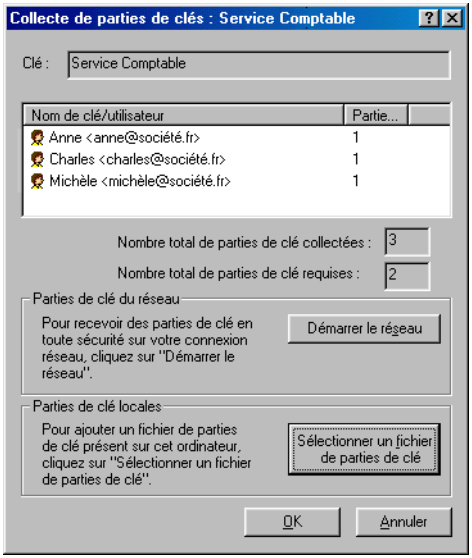


Figure 3-13. Boîte de dialogue Collecte des parties de clés

5. Effectuez l'une des opérations suivantes :

   - **Si vous collectez les parties de la clé localement**, cliquez sur **Sélectionner un fichier de parties de clé**, puis recherchez les fichiers de parties de clé associés à la clé découpée. Ces fichiers peuvent être collectés à partir du disque dur, d'une disquette ou d'un disque monté. Passez à l'etape 6.

   - **Si vous collectez les parties de la clé via le réseau**, cliquez sur **Démarrer le réseau**.

     La boîte de dialogue **Mot de passe complexe** apparaît. Dans la zone **Clé de signature**, sélectionnez la paire de clés à utiliser pour l'authentification sur le système distant, puis entrez le mot de passe complexe. Pour préparer l'ordinateur à la réception de parties de clé, cliquez sur **OK**.

     L'état de la transaction apparaît dans la zone de **Partages du réseau**. Lorsqu'il est défini sur « Ecoute de..», PGP est prêt à recevoir des parties de clé.

A ce stade, les détenteurs doivent envoyer leur partie de la clé. Pour en savoir plus sur l'envoi de parties de clé vers l'ordinateur de reconstitution, reportez-vous à la section « Pour envoyer votre partie de clé sur le réseau » à la page 51.

Lors de la réception d'une partie de la clé, la boîte de dialogue **Authentification distante** apparaît, comme illustré à la Figure 3-14.

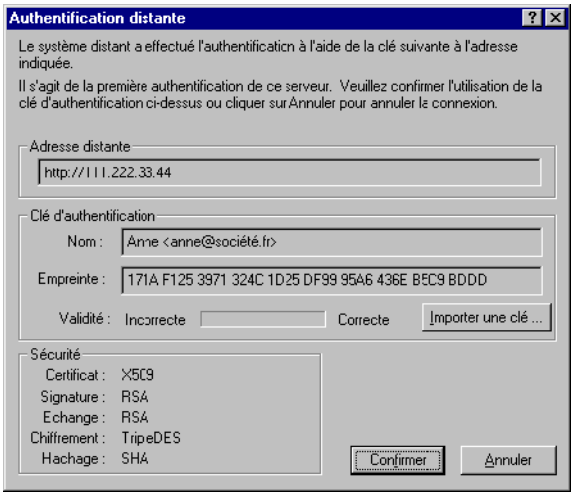


Figure 3-14. Boîte de dialogue Authentification distante

Si vous n'avez pas signé la clé utilisée pour authentifier le système distant, elle n'est pas considérée comme valide. Bien que vous puissiez le faire, il est déconseillé de reconstituer la clé avec une clé d'authentification non valide. Il est recommandé de vérifier l'empreinte digitale de chaque détenteur d'une partie de la clé et de signer sa clé publique afin de s'assurer que sa clé d'authentification est valide.

Pour accepter le fichier de parties de clé, cliquez sur **Confirmer**.

6. Poursuivez la collecte de parties de la clé jusqu'à ce que la valeur de **Nombre total des parties de la clé collectées** corresponde à celle de**Nombre total des parties de la clé requises** dans la boîte de dialogue **Collecte des parties de clés**.

7. Cliquez sur **OK**.

   Le fichier est alors signé ou décrypté avec la clé découpée.

Pour envoyer votre partie de clé sur le réseau

1. Lorsque la personne reconstituant la clé découpée vous contacte, assurez-vous de disposer des éléments suivants :
   - votre fichier de parties de clé et votre mot de passe complexe ;
   - votre paire de clés (pour identifier sur l'ordinateur collectant les parties de la clé) ;
   - une connexion réseau ; User's Guide 65
   - l'adresse IP ou le nom de domaine de l'ordinateur reconstituant la clé.
2. Sélectionnez **Envoyer des parties de clé** dans le menu **Fichier** de PGPkeys.

   La boîte de dialogue **Sélection d'un fichier de parties de clé** apparaît.
3. Recherchez votre partie de la clé, puis cliquez sur **Ouvrir**.

   La boîte de dialogue **PGP – Saisie d'un mot de passe complexe** apparaît.
4. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

   La boîte de dialogue **Envoyer des parties de clé** apparaît, comme illustré à la Figure 3-15.

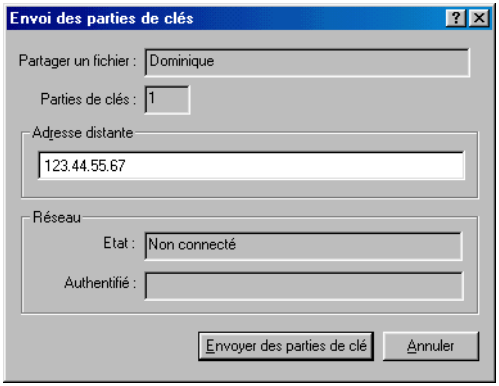


Figure 3-15. Boîte de dialogue Envoyer des parties de clé

5. Dans la zone **Adresse distante**, entrez l'adresse IP ou le nom de domaine de l'ordinateur reconstituant la clé, puis cliquez sur **Envoyer des parties de clé**.

   L'état de la transaction apparaît dans la zone de **l'état du réseau**. Lorsque l'état est défini sur « Connecté », vous devez vous authentifier auprès de l'ordinateur.

   La boîte de dialogue **Authentification distante** apparaît, vous demandant de confirmer que l'ordinateur distant correspond à celui auquel vous souhaitez envoyer votre partie de clé.

6. Pour terminer la transaction, cliquez sur **Confirmer**.

   Après la réception des parties de la clé par l'ordinateur distant et confirmation de la transaction, un message indique que l'envoi des parties de clé s'est correctement déroulé.

7. Cliquez sur **OK**.

8. Une fois l'envoi de vos parties de clé accompli, cliquez sur **Terminé** dans la fenêtre **Parties de clé**.

Distribution d'une clé publique

Après avoir créé vos clés, vous devez les mettre à la disposition des autres utilisateurs, afin que ceux-ci puissent vous envoyer des informations cryptées et vérifier votre signature numérique. Vous pouvez distribuer votre clé publique de trois manières différentes :

- Mettez à disposition votre clé publique via un serveur de certificats publics
- Insérez votre clé publique dans un message électronique

  Ou

- Exportez votre clé publique ou copiez-la vers un fichier texte

Votre clé publique se compose principalement d'un bloc de texte. Sa mise à disposition sur un serveur de certificats publics, son insertion dans un message électronique, son exportation ou sa copie dans un fichier sont donc facilement réalisables. Le destinataire peut alors utiliser la méthode la plus pratique pour ajouter votre clé publique à son trousseau de clés publiques.

Mise à disposition d'une clé publique via un serveur de certificats

La meilleure méthode de mise à disposition de votre clé publique consiste à la placer sur un serveur de certificats de clés publiques accessible à tous. Ainsi, les personnes peuvent vous envoyer un message électronique sans avoir à demander de façon explicite une copie de votre clé. Ceci vous évite de conserver un grand nombre de clés publiques rarement utilisées. Il existe de nombreux serveurs de certificats de par le monde, parmi lesquels ceux fournis par Network Associates, Inc., vous permettant de rendre votre clé accessible à tous. Généralement, votre agent de sécurité préconfigurera votre serveur de clés afin que tout fonctionne correctement sur votre site.

Pour envoyer votre clé publique vers un serveur de certificats

1. Connectez-vous à Internet.
2. Ouvrez PGPkeys.
3. Sélectionnez l'icône représentant la clé publique à envoyer au serveur de certificats.
4. Ouvrez le menu **Serveur**, puis sélectionnez le serveur de certificats de destination dans le sous-menu **Envoyer vers**. PGP vous indique que le téléchargement des clés vers le serveur s'est correctement déroulé.

Une fois que vous avez copié votre clé publique sur un serveur de certificats, vous pouvez demander aux personnes souhaitant vous envoyer des données cryptées ou souhaitant vérifier votre signature numérique de récupérer cette copie de votre clé à partir du serveur. Même si vous n'indiquez pas explicitement l'emplacement de votre clé publique, ils peuvent en obtenir une copie en recherchant votre nom et votre adresse e-mail sur le serveur de certificats. De nombreux utilisateurs indiquent l'adresse Web de leur clé publique à la fin de leurs messages électroniques. Dans la plupart des cas, le destinataire peut simplement cliquer deux fois sur cette adresse afin d'accéder à une copie de la clé sur le serveur. Certaines personnes inscrivent leur empreinte digitale PGP sur leurs cartes de visite pour faciliter la vérification.

Mise à jour d'une clé sur un serveur de certificats

Si vous devez modifier votre adresse e-mail ou si vous acquérez de nouvelles signatures, vous devez simplement envoyer une nouvelle copie de votre clé au serveur pour remplacer l'ancienne ; les informations sont mises à jour automatiquement. Cependant, vous devez garder à l'esprit que les serveurs de certificats publics peuvent uniquement mettre à jour des nouvelles informations et ne permettent pas la suppression de noms d'utilisateurs ou de signatures de votre clé. Pour plus d'informations sur la suppression des signatures ou des noms d'utilisateurs associés à votre clé, reportez-vous à la section « Suppression des signatures ou des noms d'utilisateurs associés à une clé ». Si votre clé est compromise, vous pouvez la révoquer, et indiquer ainsi aux autres utilisateurs de ne plus se fier à cette version de votre clé. Pour plus d'informations sur la révocation d'une clé, reportez-vous à la section Chapitre 6, « Gestion des clés et définition des options de PGP ».

Suppression des signatures ou des noms d'utilisateurs associés à une clé

Il se peut que vous souhaitiez supprimer une clé, une signature ou un ID utilisateur associés à une clé particulière.

Les serveurs de certificats publics peuvent uniquement mettre à jour des nouvelles informations et ne permettent pas la suppression de noms d'utilisateurs ou de signatures de votre clé. Pour supprimer des signatures ou des noms d'utilisateurs associés à votre clé publique, vous devez tout d'abord supprimer votre clé du serveur, procéder à la modification requise, puis replacer votre clé sur le serveur.

Si les paramètres de votre serveur PGP sont définis pour synchroniser les clés avec le serveur lors de l'ajout de noms / photographies / autorités de révocation à votre clé, celle-ci est automatiquement mise à jour sur le serveur. Cependant, si vos clés ne sont pas automatiquement synchronisées avec le serveur, suivez les instructions décrites ci-dessous pour procéder à une mise à jour manuelle de votre clé sur le serveur de certificats.

REMARQUE : La suppression d'une clé, d'une signature ou d'un ID utilisateur à partir sur une clé est définitive. Les signatures et les ID utilisateurs peuvent être à nouveau ajoutés à une clé. Vous pouvez à nouveau importer une clé publique vers votre trousseau. Cependant, vous ne pouvez pas créer à nouveau une clé privée existant uniquement sur ce trousseau et vous ne pouvez plus décrypter tous les messages cryptés vers les copies de clés publiques.

Pour supprimer des signatures ou des noms d'utilisateurs associés à une clé sur un serveur de certificats

IMPORTANT : Cette procédure permet de supprimer des signatures ou des noms d'utilisateurs associés à votre clé uniquement sur des serveurs de certificats LDAP. Par ailleurs, le serveur de certificats doit être configuré de manière à permettre cette action. Si vous ne connaissez pas le type de votre serveur ou ses paramètres de configuration, adressez-vous à l'administrateur du serveur de certificats de votre entreprise avant de mettre à jour votre clé.

1. Ouvrez PGPkeys.
2. Choisissez **Rechercher** dans le menu **Serveur** ou cliquez sur  dans le menu PGPkeys.

   La fenêtre **Rechercher de PGPkeys** apparaît.
3. Sélectionnez le serveur où vous souhaitez effectuer la recherche dans le menu **Rechercher les clés sur**.
4. Pour localiser votre clé publique, définissez vos critères de recherche.

   Le paramètre par défaut est **ID utilisateur**, mais vous pouvez sélectionner **ID de clé**, **Etat d'une clé**, **Type de clé**, **Taille de la clé**, **Date de création** ou **Date d'expiration** à l'aide des flèches. Par exemple, vous pouvez rechercher l'ensemble des clés à l'aide de l'ID utilisateur de Fred.
5. Pour lancer la recherche, cliquez sur **Rechercher**.

   Les résultats de la recherche apparaissent dans la fenêtre.
6. Cliquez avec le bouton droit de la souris sur la clé à supprimer du serveur, puis sélectionnez **Supprimer** dans le menu contextuel.

   La boîte de dialogue **Mot de passe complexe** apparaît.
7. Entrez le mot de passe complexe correspondant à la clé à supprimer du serveur, puis cliquez sur **OK**.

   Une boîte de dialogue de confirmation apparaît, puis la clé est supprimée.
8. Mettez votre clé à jour (supprimez les signatures ou noms d'utilisateurs non souhaités).
9. Copiez la clé mise à jour sur le serveur (pour plus d'informations, reportez-vous à la section « Mise à disposition d'une clé publique via un serveur de certificats » à la page 53.

Si le serveur sur lequel vous procédez à la mise à jour de votre clé publique est configuré de manière à synchroniser les clés avec des serveurs de certificats publics tiers, votre clé sera automatiquement mise à jour sur ces derniers au moment de la synchronisation.

IMPORTANT : Si vous supprimez votre clé d'un serveur de certificats, gardez à l'esprit que quiconque disposant de votre clé publique sur son trousseau peut la télécharger à nouveau vers le serveur. Contrôlez régulièrement le serveur afin de voir si la clé est réapparue. Il est possible que vous ayez à la supprimer du serveur plusieurs fois.

Insertion d'une clé publique dans un message électronique

Pour diffuser facilement votre clé publique, vous pouvez l'insérer avec un message électronique.

Pour insérer votre clé publique dans un message électronique

1. Ouvrez PGPkeys.
2. Sélectionnez votre paire de clés, puis cliquez sur **Copier** dans le menu **Edition**.
3. Ouvrez l'éditeur dans lequel vous composez vos messages électroniques, placez le pointeur dans la zone souhaitée, puis cliquez sur **Coller** dans le menu **Edition**. Dans les applications e-mail plus récentes, vous pouvez simplement faire glisser votre clé de la fenêtre PGPkeys vers le texte de votre message électronique afin d'y transférer les informations relatives à la clé.

Lors de l'envoi de votre clé publique, assurez-vous de signer le message électronique. Ainsi, le destinataire peut vérifier votre signature et s'assurer que personne n'a falsifié d'informations lors du transfert. Si votre clé n'a pas encore été signée par un correspondant fiable, seule la vérification de l'empreinte digitale figurant sur votre clé peut garantir aux destinataires de votre signature que cette dernière émane bien de vous.

Exportation d'une clé publique vers un fichier

Une autre méthode de distribution de votre clé publique consiste à la copier vers un fichier, puis à rendre ce fichier accessible à votre correspondant.

Pour exporter votre clé publique vers un fichier

Il existe trois manières d'exporter ou d'enregistrer votre clé publique dans un fichier

- Sélectionnez l'icône représentant votre paire de clés dans la fenêtre PGPkeys, cliquez sur **Exporter** dans le menu **Clés**, puis entrez le nom du fichier dans lequel vous souhaitez enregistrer la clé.
- Faites glisser l'icône représentant votre paire de clés de la fenêtre PGPkeys vers l'emplacement auquel vous souhaitez enregistrer la clé.

  Ou

- Sélectionnez l'icône représentant votre paire de clés dans la fenêtre PGPkeys, cliquez sur le menu **Edition**, puis sélectionnez **Coller** pour insérer les informations relatives à la clé dans un document texte.

> **REMARQUE :** Pour envoyer votre clé publique à des collègues utilisant des PC, entrez un nom comportant un maximum de huit caractères initiaux, suivis de trois caractères supplémentaires correspondant à l'extension du type de fichier (par exemple, MaClé.text).

Obtention des clés publiques des autres utilisateurs

De la même manière que vous devez distribuer votre clé publique aux correspondants souhaitant vous envoyer des messages cryptés ou vérifier votre signature numérique, vous devez obtenir les clés publiques des autres utilisateurs pour leur envoyer des messages cryptés ou pour vérifier leurs signatures numériques.

Pour obtenir la clé publique d'un utilisateur

Effectuez l'une des opérations suivantes :

- Récupérez la clé à partir d'un serveur de certificats publics
- Ajoutez la clé publique à votre trousseau de clés directement à partir d'un message électronique

  Ou

- Importez la clé publique à partir d'un fichier exporté

Les clés publiques sont des blocs de texte : il est donc facile de les ajouter à votre trousseau de clés en les important à partir d'un fichier ou en les copiant à partir d'un message électronique, puis en les collant dans votre trousseau de clés publiques.

Récupération des clés publiques à partir d'un serveur de certificats

Si la personne à laquelle vous souhaitez envoyer un message électronique crypté est un utilisateur averti de PGP, il est très probable qu'elle ait placé une copie de sa clé publique sur un serveur de certificats. Vous pouvez ainsi récupérer très facilement la copie de sa clé la plus récente lorsque vous souhaitez lui envoyer des messages électroniques. Vous pouvez éviter par ailleurs d'avoir à stocker un grand nombre de clés sur votre trousseau de clés publiques.

L'agent de sécurité de votre entreprise peut vous indiquer d'utiliser un serveur de certificats regroupant toutes les clés fréquemment utilisées dans votre entreprise. Dans ce cas, votre logiciel PGP est probablement déjà configuré de manière à accéder au serveur approprié.

De nombreux serveurs de certificats publics, tels que celui géré par Network Associates, Inc, vous permettent de rechercher les clés de la plupart des utilisateurs PGP. Si votre destinataire ne vous a pas indiqué l'adresse Web de stockage de sa clé publique, vous pouvez accéder à tout serveur de certificats, puis effectuer une recherche sur le nom d'utilisateur ou l'adresse e-mail, tous les serveurs de certificats étant régulièrement mis à jour de manière à inclure les clés stockées sur tous les autres serveurs.

Pour récupérer la clé publique d'un utilisateur à partir d'un serveur de certificats

1. Ouvrez PGPkeys.
2. Choisissez **Rechercher** dans le menu **Serveur** ou cliquez sur **Rechercher** ( ) dans PGPkeys.

   La fenêtre **Rechercher de PGPkeys** apparaît, comme illustré à la Figure 3-16.

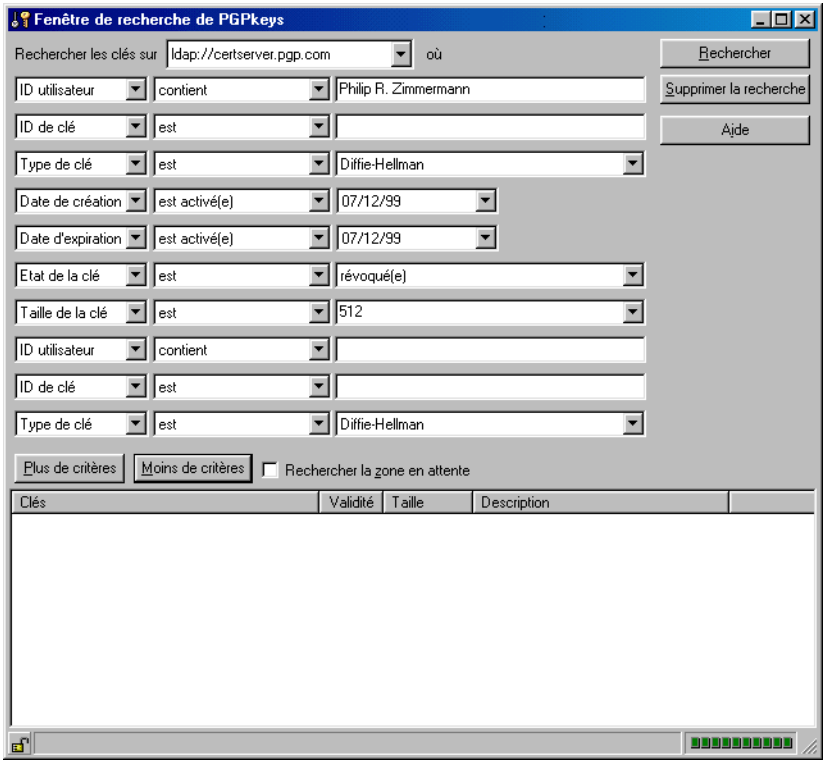


Figure 3-16. Fenêtre Rechercher de PGPkeys (affichage Plus de critères)

3. Sélectionnez le serveur sur lequel vous souhaitez effectuer la recherche dans le menu **Rechercher les clés sur**.

4. Spécifiez vos critères de recherche.

   Pour rechercher des clés sur un serveur de certificats, spécifiez des valeurs pour les caractéristiques suivantes :

   - ID utilisateur
   - ID de clé
   - Etat d'une clé (révoquée ou désactivée)
   - Type de clé (Diffie-Hellman ou RSA)
   - Date de création
   - Date d'expiration
   - Clés révoquées
   - Clés désactivées
   - Taille de la clé
   - Clés signées par une clé spécifique

   Il est possible également d'effectuer une recherche sur les critères contraires à ces opérations. Par exemple, vous pouvez effectuer une recherche avec « l'ID utilisateur n'est pas Robert » comme critère.

5. Entrez la valeur à rechercher.
6. Pour élargir votre recherche, par exemple, les ID de clés avec le nom Fred créés avant le 6 octobre 1997 inclus, cliquez sur **Plus de critères**.
7. Pour lancer la recherche, cliquez sur **Rechercher**.

   Une barre de progression apparaît, indiquant l'état de la recherche.

   REMARQUE : Pour annuler une recherche en cours, cliquez sur **Arrêter la recherche**.

   Les résultats de la recherche apparaissent dans la fenêtre.

8. Pour importer les clés, faites-les glisser dans la fenêtre principale de PGPkeys.
9. Pour effacer vos critères de recherche, cliquez sur **Supprimer la recherche**.

Ajout de clés publiques à partir de messages électroniques

Pour obtenir facilement une copie de la clé publique de l'un de vos correspondants, vous pouvez lui demander d'insérer sa clé dans un message électronique. Lorsqu'une clé publique est envoyée par e-mail, elle apparaît sous forme d'un bloc de texte dans le corps du message.

Pour ajouter une clé publique à partir d'un message électronique

Si votre application de messagerie est prise en charge par les modules externes PGP, cliquez sur l'icone  située dans votre application de messagerie afin de récupérer la clé publique de l'expéditeur à partir du message, puis de l'ajouter à votre trousseau de clés publiques.

Si votre application de messagerie n'est pas prise en charge par les modules externes, vous pouvez ajouter la clé publique à votre trousseau de clés en copiant le bloc de texte représentant la clé publique, puis en le copiant dans PGPkeys.

Importation de clés

Vous pouvez importer des clés publiques et des clés privées PKCS-12 X.509 dans votre trousseau de clés publiques PGP. Cette procédure est utile pour l'importation des clés à partir de votre navigateur, puis en copiant et en les collant dans votre trousseau de clés publiques.

Pour récupérer la clé publique d'un utilisateur, demandez à ce dernier d'enregistrer sa clé dans un fichier, d'où vous pourrez l'importer, la copier, puis la coller dans votre trousseau de clés publiques.

Pour importer une clé publique à partir d'un fichier

Vous pouvez récupérer la clé publique d'un utilisateur, puis l'ajouter à votre trousseau de clés publiques de trois manières différentes :

- Cliquez sur **Importer** dans le menu Clés, puis accédez au fichier dans lequel la clé publique est stockée.
- Faites glisser le fichier contenant la clé publique dans la fenêtre principale de PGPkeys

  Ou

- Ouvrez le document texte dans lequel la clé publique est stockée, sélectionnez le bloc de texte représentant cette clé, puis cliquez sur le menu **Edition**. Pour copier la clé, ouvrez PGPkeys, puis choisissez **Coller** dans le menu **Edition**. La clé apparaît ensuite sous forme d'icône dans PGPkeys.

Vous pouvez également récupérer les clés privées PKCS-12 X.509 en les exportant à partir de votre navigateur, puis en les déposant dans PGPkeys, ou en choisissant **Importer** dans le menu **Clés**.

Vérification de l'authenticité d'une clé

Lors de l'échange de clés avec l'un de vos correspondants, il est parfois difficile de savoir si la clé appartient réellement à celui-ci. Le logiciel PGP offre des protections vous permettant de contrôler l'authenticité d'une clé et de certifier que celle-ci appartient à un détenteur particulier (c'est-à-dire, afin de la *valider*). Le programme PGP vous avertit également si vous tentez d'utiliser une clé qui n'est pas valide et vous avertit par défaut si vous êtes sur le point d'utiliser une clé correcte de manière marginale.

Pourquoi vérifier l'authenticité d'une clé ?

Les systèmes de cryptage de clé publique sont principalement vulnérables aux attaques menées par des pirates expérimentés cherchant à substituer la clé publique d'un utilisateur par leur propre clé. Ils peuvent ainsi intercepter tout message crypté à l'attention de cet utilisateur, le décrypter à l'aide de leur propre clé, le crypter à nouveau avec la vraie clé de l'utilisateur, puis l'envoyer comme si de rien n'était. En fait, ils peuvent effectuer toutes ces opérations automatiquement via un programme informatique central sophistiqué permettant de déchiffrer tous vos messages.

Selon ce scénario, vous et vos correspondants devez déterminer si vous disposez de copies autorisées des clés de chacun. La meilleure façon de vous assurer qu'une clé publique appartient réellement à un utilisateur spécifique consiste à demander au détenteur de cette clé de la copier sur une disquette, puis à vous la remettre en mains propres. Cependant, vous êtes rarement suffisamment proche de votre correspondant pour qu'il puisse vous remettre sa disquette. Aussi vous échangez généralement des clés publiques via votre messagerie ou vous les récupérez à partir d'un serveur de certificats publics.

Vérification de clés à l'aide d'une empreinte digitale

Vous pouvez définir si une clé appartient réellement à un utilisateur spécifique en vérifiant son empreinte digitale, série unique de mots ou de nombres générée lors de la création de la clé. En comparant l'empreinte digitale de votre copie de la clé publique d'un utilisateur à celle de la clé originale, vous pouvez être quasiment certain d'être réellement en possession d'une copie valide de sa clé. Pour plus d'informations sur la vérification de clés à l'aide d'une empreinte digitale, reportez-vous à la section « Vérification de la clé publique d'un autre utilisateur » à la page 103.

Validation de la clé publique

Lorsque vous êtes absolument certain de posséder une copie valide de la clé publique d'un utilisateur, vous pouvez signer cette clé. En signant la clé publique d'un utilisateur avec votre clé privée, vous affirmez être certain que la clé appartient bien à l'utilisateur présumé. Par exemple, lorsque vous créez une nouvelle clé, celle-ci est automatiquement certifiée avec votre propre signature numérique. Par défaut, les signatures apposées à d'autres clés ne sont pas exportables, ce qui signifie qu'elles s'appliquent uniquement à la clé lorsque celle-ci figure dans votre trousseau de clés. Pour plus d'informations sur la signature d'une clé, reportez-vous à la section « Signature de la clé publique d'un autre utilisateur » à la page 105.

Utilisation des correspondants fiables

En général, les utilisateurs PGP demandent à d'autres correspondants fiables de signer leurs clés publiques pour attester de leur authenticité. Par exemple, vous pouvez envoyer une copie de votre clé publique à un collègue fiable en lui demandant de la certifier, puis de vous la renvoyer, de façon à pouvoir inclure sa signature lorsque vous placez votre clé sur un serveur de certificats publics. Lorsqu'une personne obtient une copie de votre clé publique via PGP, elle n'a pas à vérifier elle–même l'authenticité de la clé, mais peut se fier au niveau de confiance qu'elle accorde au signataire de votre clé. PGP permet d'établir ce niveau de validité pour chacune des clés publiques ajoutées à votre trousseau de clés publiques. Il indique également les niveaux de fiabilité et de validité associés à chaque clé PGP. Ainsi, lorsque vous récupérez une clé provenant d'un utilisateur dont la clé a été signée par un correspondant fiable, vous pouvez être quasiment certain que cette clé appartient bien à l'utilisateur supposé. Pour plus d'informations sur la signature des clés et la validation des utilisateurs, reportez-vous à la section « Signature de la clé publique d'un autre utilisateur » à la page 105.

Votre agent de sécurité peut jouer le rôle de correspondant fiable. Toute clé signée par la clé d'entreprise peut ainsi être considérée comme valide et fiable. Si vous travaillez pour une grande entreprise possédant des bureaux sur des sites différents, il se peut que vous ayez des correspondants régionaux. Votre agent de sécurité peut alors jouer le rôle de gestionnaire en chef de la sécurité ou de correspondant fiable de correspondants fiables.

Qu'est-ce qu'un correspondant fiable ?

PGP utilise le concept de correspondant fiable, c'est-à-dire, une personne en qui vous avez confiance pour vous fournir des clés valides. Peut-être connaissez vous ce concept grâce aux romans de l'époque victorienne, dans lesquels les personnes se remettaient mutuellement des lettres de recommandation. Par exemple, si votre oncle connaissait une personne habitant une ville lointaine et avec laquelle vous étiez susceptible de faire des affaires, il pouvait lui rédiger une lettre vous recommandant auprès de lui. Avec PGP, les utilisateurs peuvent mutuellement signer des clés afin de les valider. Vous signez la clé d'un utilisateur pour indiquer que vous êtes sûr de sa validité, c'est-à-dire, qu'elle lui appartient vraiment. Il existe plusieurs manières de procéder. Lorsqu'un correspondant fiable signe la clé d'un autre utilisateur, vous considérez qu'elle est valide et ne jugez pas nécessaire de la vérifier avant de l'utiliser.

Qu'est-ce qu'un gestionnaire en chef de la sécurité ?

PGP prend également en charge le concept de gestionnaire en chef de la sécurité, le correspondant fiable de tous les correspondants fiables. Si vous travaillez dans une grande entreprise, il se peut que vous ayez un agent de sécurité régional, à savoir un correspondant fiable, dont le rôle est de signer les clés des utilisateurs. Vous pourriez considérer que ces clés sont valides, l'agent de sécurité régional ayant effectué les opérations nécessaires afin de garantir cette validité. Votre entreprise peut également disposer d'un agent de sécurité national travaillant conjointement avec les agents de sécurité locaux, de façon à ce qu'une personne située en Bretagne puisse faire confiance à une personne située en Corse. En effet, leurs clés ont été signées par leurs agents de sécurité régionaux qui, à leur tour, ont fait signer leurs clés par l'agent de sécurité national, appelé gestionnaire en chef de la sécurité. Ceci permet la mise en place d'une fiabilité hiérarchique au sein de l'entreprise.

Envoi et réception de messages électroniques sécurisés 4

Ce chapitre décrit le cryptage et la signature des messages envoyés, ainsi que le décryptage et la vérification des messages reçus.

Cryptage et signature des messages électroniques

PGP propose trois méthodes de cryptage et de signature des messages électroniques. L'utilisation d'une application prise en charge par les modules externes e-mail PGP est sans aucun doute la méthode la plus rapide et la plus simple. Bien que la procédure varie légèrement selon l'application de messagerie utilisée, il vous suffit de cliquer sur les boutons situés dans la barre d'outils de votre application pour crypter et signer vos messages.

Si vous utilisez une application de messagerie qui n'est pas prise en charge par les modules-externes PGP, vous pouvez crypter et signer vos messages électroniques via le Presse-papiers de Windows : sélectionnez l'option appropriée à partir de l'icône représentant un verrou, située à droite de la Barre des tâches. Pour insérer des pièces jointes, cryptez au préalable les fichiers via l'Explorateur Windows.

ASTUCE : Si vous envoyez un message électronique confidentiel, laissez la ligne relative à l'objet vierge ou saisissez un objet qui ne dévoile en rien le contenu de votre message crypté.

Si PGP ne prend en charge aucune de vos applications de messagerie, reportez-vous au Chapitre 5 pour plus d'informations sur le cryptage des fichiers.

Au lieu des modules externes, vous pouvez également utiliser PGPtools pour crypter et signer le texte de votre message électronique et vos pièces jointes avant leur envoi. Reportez-vous à la section « Pour crypter et signer du texte à l'aide de PGPtools » à la page 69.

Cryptage et signature avec les applications de messagerie prises en charge

Vous pouvez crypter et signer avec une application de messagerie prise en charge par les modules externes e-mail de deux manières, en fonction du type d'application de messagerie utilisée par le destinataire. Si vous êtes en communication avec d'autres utilisateurs PGP dont l'application de messagerie prend en charge le standard PGP / MIME, vous pouvez tirer parti de la fonctionnalité de PGP / MIME pour crypter et signer automatiquement vos messages électroniques et pièces jointes lors de leur envoi. Si vous communiquez avec une personne ne disposant pas d'une application de messagerie compatible PGP / MIME, vous devez crypter votre message électronique en désactivant PGP / MIME pour éviter tout problème de compatibilité. Pour obtenir une liste des modules externes et de leurs fonctionnalités, reportez-vous au Tableau 4-1, « Fonctionnalités des modules externes PGP ».

Tableau 4-1. Fonctionnalités des modules externes PGP

	Eudora version 3.0x	Eudora version 4.0x	Exchange/ Outlook	Lotus Notes	Outlook Express
PGP/MIME	Oui	Oui	Non	Non	Non
Auto-décryptage	Oui	Non	Oui	Oui	Oui
Cryptage des fichiers HTML	N/D	Oui	Conversion en texte en clair avant le cryptage	Oui	Non
Affichage du fichier HTML décrypté sous forme de document HTML	Non	Oui	Non	Oui	Non
Cryptage des pièces jointes	Oui	Oui	Oui	Oui	Non
Cryptage/signature par défaut	Oui	Oui	Oui	Oui	Oui

Pour crypter et signer avec les applications de messagerie prises en charge

1. Utilisez votre application de messagerie pour rédiger votre message électronique, comme vous le faites habituellement.
2. Une fois votre message rédigé, cliquez sur  , afin de crypter son contenu, puis sur  pour le signer.

   REMARQUE : Si vous pensez utiliser PGP / MIME régulièrement, laissez cette option activée en sélectionnant les paramètres appropriés dans le panneau **Message électronique** de la boîte de dialogue **Options**.

3. Envoyez votre message normalement.

   Si vous détenez une copie des clés publiques de tous les destinataires de votre message, les clés appropriées sont utilisées. Cependant, si vous spécifiez un destinataire pour lequel il n'existe pas de clé publique correspondante ou que vous constatez une validité insuffisante pour une ou plusieurs clés, la boîte de dialogue de sélection apparaît (Figure 4-1), afin que vous puissiez spécifier la clé correcte.

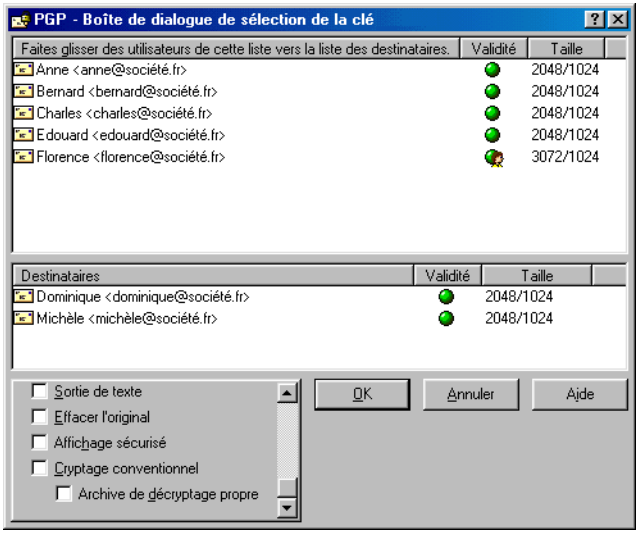


Figure 4-1. Fenêtre Sélection de destinataire(s) PGP

4. Faites glisser les clés publiques des personnes devant recevoir une copie de votre message électronique crypté dans la zone Liste des destinataires. Vous pouvez également cliquer deux fois sur une clé, afin de la déplacer d'une zone de l'écran à l'autre.

   L'icône **Validité** indique le niveau minimal de confiance attribuée à la validité des clés publiques situées dans la liste des **destinataires**. Cette validité dépend des signatures associées à la clé. Pour plus d'informations, reportez-vous au Chapitre 6, « Gestion des clés et définition des options de PGP ».

5. Vous pouvez sélectionner l'une des options de cryptage suivantes en fonction du type de données à crypter :

   - **Affichage sécurisé.** Sélectionnez cette option pour protéger les données contres les attaques TEMPEST lors du décryptage. Dans ce cas, les données décryptées sont affichées dans une police spéciale de prévention contre les attaques TEMPEST. Elles sont ainsi illisibles pour les équipements de capture du rayonnement. Pour plus d'informations sur les attaques TEMPEST, reportez-vous à la section « Vulnérabilités » à la page 246.

     REMARQUE : Il est possible que l'option Affichage sécurisé ne soit pas compatible avec certaines versions précédentes de PGP. Néanmoins, les fichiers cryptés grâce à cette option peuvent être décryptés par les versions précédentes de PGP. Cette fonction peut toutefois être ignorée.

   - Cryptage conventionnel. Sélectionnez cette option pour utiliser un mot de passe complexe commun, plutôt qu'un cryptage de clé publique. Le fichier est alors crypté à l'aide d'une clé de session permettant le cryptage (et le décryptage) à l'aide d'un mot de passe complexe à définir.

   - Archive d'auto-décryptage. Sélectionnez cette option pour créer un fichier exécutable d'auto-décryptage. Le fichier est alors crypté à l'aide d'une clé de session permettant le cryptage (et le décryptage) à l'aide d'un mot de passe complexe à définir. Pour décrypter le fichier exécutable obtenu, cliquez deux fois dessus, puis entrez le mot de passe complexe approprié. Cette option s'avère particulièrement utile pour les utilisateurs qui transmettent des fichiers cryptés à des personnes ne disposant pas de PGP. Veuillez noter que l'expéditeur et le destinataire doivent utiliser la même plate-forme.

6. Pour crypter et signer votre message, cliquez sur **OK**.

   Si vous avez choisi de signer les données cryptées, la boîte de dialogue **Mot de passe complexe de clé de signature** apparaît, comme illustré à la Figure 4-2. Vous êtes alors invité à saisir votre mot de passe complexe avant l'envoi du message électronique.

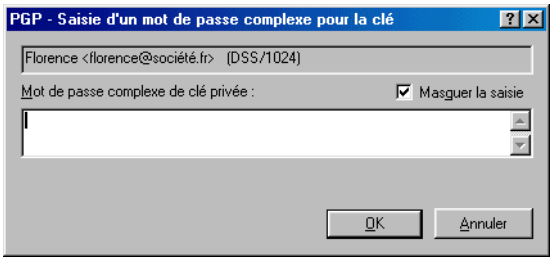


Figure 4-2. Boîte de dialogue du mot de passe complexe de clé de signature

7. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

AVERTISSEMENT : Si vous décidez de stocker votre message dans votre boîte d'envoi plutôt que de l'envoyer immédiatement, soyez conscient du fait que certaines applications de messagerie cryptent uniquement vos messages lors de leur envoi. Avant de mettre en file d'attente vos messages cryptés, assurez-vous que votre application crypte bien les messages dans votre boîte d'envoi. Dans le cas contraire, vous pouvez utiliser l'option **Crypter maintenant** de PGPmenu pour crypter vos messages avant de les mettre en file d'attente dans votre boîte d'envoi.

Pour crypter et signer du texte à l'aide de PGPtools

1. Copiez le texte à crypter et signer dans le Presse-papiers.
2. Cliquez sur **Crypter**, **Signer** ou **Crypter et signer** dans PGPtools.

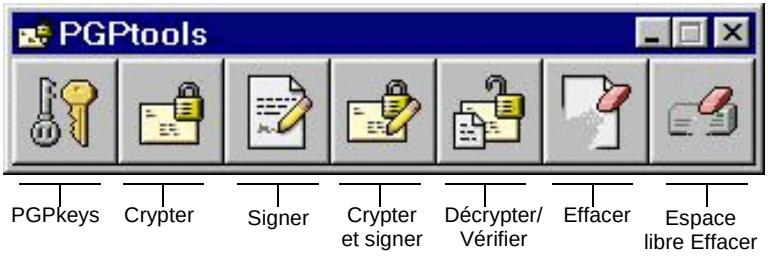


Figure 4-3. Fenêtre PGPtools

La boîte de dialogue de sélection du ou des fichiers apparaît.

3. Cliquez sur **Presse-papiers**.

   La boîte de dialogue **Destinataires** apparaît, comme illustré à la Figure 4-1.

4. Faites glisser les clés publiques des personnes devant recevoir une copie de votre message électronique crypté dans la liste des **destinataires**. Vous pouvez également cliquer deux fois sur une clé, afin de la déplacer d'une zone de l'écran à l'autre.

   L'icône **Validité** indique le niveau minimal de confiance attribuée à la validité des clés publiques situées dans la liste des **destinataires**. Cette validité dépend des signatures associées à la clé. Pour plus d'informations, reportez-vous au Chapitre 6, « Gestion des clés et définition des options de PGP ».

5. Vous pouvez sélectionner l'une des options de cryptage suivantes en fonction du type de données à crypter :

   - **Affichage sécurisé.** Sélectionnez cette option pour protéger les données contres les attaques TEMPEST lors du décryptage. Dans ce cas, les données décryptées sont affichées dans une police spéciale de prévention contre les attaques TEMPEST. Elles sont ainsi illisibles pour les équipements de capture du rayonnement. Pour plus d'informations sur les attaques TEMPEST, reportez-vous à la section « Vulnérabilités » à la page 246.

     REMARQUE : Il est possible que l'option Affichage sécurisé ne soit pas compatible avec certaines versions précédentes de PGP. Néanmoins, les fichiers cryptés grâce à cette option peuvent être décryptés par les versions précédentes de PGP. Cette fonction peut toutefois être ignorée.

   - **Cryptage conventionnel.** Sélectionnez cette option pour utiliser un mot de passe complexe commun, plutôt qu'un cryptage de clé publique. Le fichier est alors crypté à l'aide d'une clé de session permettant le cryptage (et le décryptage) à l'aide d'un mot de passe complexe à définir.

- **Archive d'auto-décryptage.** Sélectionnez cette option pour créer un fichier exécutable d'auto-décryptage. Le fichier est alors crypté à l'aide d'une clé de session permettant le cryptage (et le décryptage) à l'aide d'un mot de passe complexe à définir. Pour décrypter le fichier exécutable obtenu, cliquez deux fois dessus, puis entrez le mot de passe complexe approprié. Cette option s'avère particulièrement utile pour les utilisateurs qui transmettent des fichiers cryptés à des personnes ne disposant pas de PGP. Veuillez noter que l'expéditeur et le destinataire doivent utiliser la même plate-forme.

6. Pour crypter et signer votre message, cliquez sur **OK**.

   Si vous avez choisi de signer les données cryptées, la boîte de dialogue **Mot de passe complexe de clé de signature** apparaît, comme illustré à la Figure 4-2. Vous êtes alors invité à saisir votre mot de passe complexe avant l'envoi du message électronique.

7. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

8. Collez le texte dans votre message électronique, puis envoyez le message.

Cryptage d'un message électronique destiné à des groupes de destinataires

Vous pouvez utiliser PGP pour créer des listes de distribution vers des groupes. Par exemple, si vous souhaitez envoyer un message électronique crypté à 10 personnes à l'adresse ingenierie@entreprise.com, vous pouvez créer une liste de distribution portant ce nom. Le menu **Groupes** de PGPkeys contient l'option **Afficher les groupes** qui permet d'activer l'affichage de la fenêtre Groupes de PGPkeys. La fenêtre **Liste des groupes** apparaît comme illustré à la Figure 4-4.

REMARQUE : Si vous envisagez de crypter des informations pour tous les membres d'une liste de distribution de messages électroniques existante, vous devez créer un groupe PGP identique à cette liste (même nom, mêmes membres). Par exemple, si une liste equipe@entreprise.com est configurée dans votre application de messagerie, vous devez créer un groupe equipe@entreprise dans PGP.

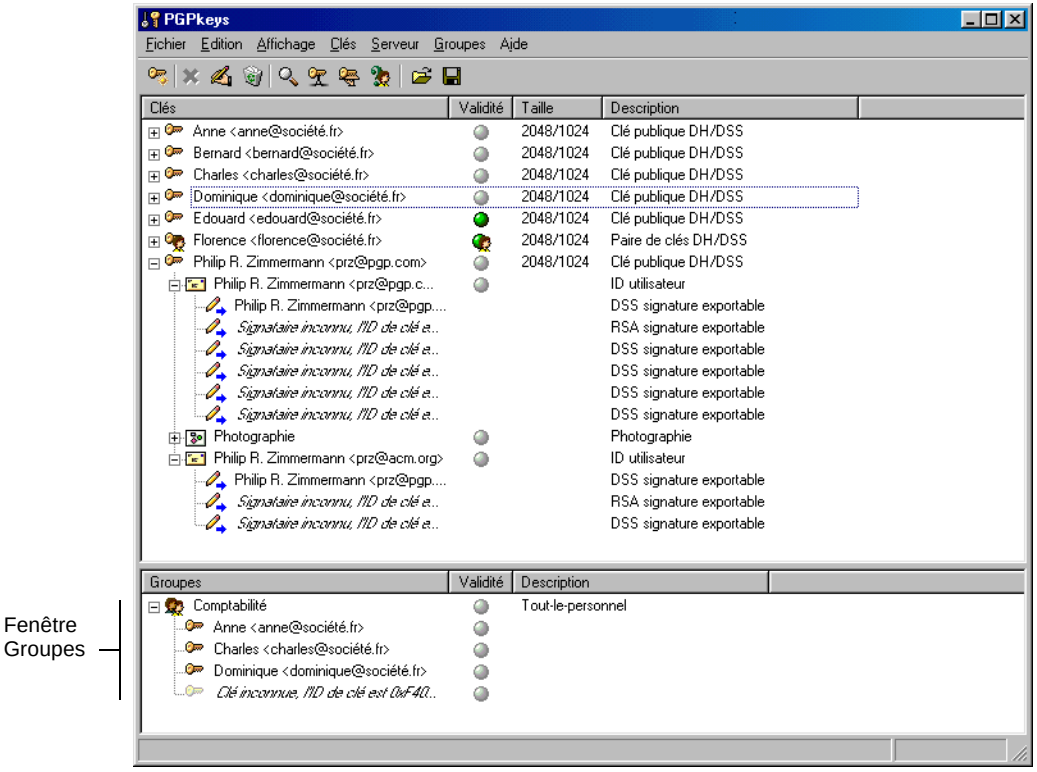


Figure 4-4. PGPkeys avec la fenêtre Groupes

Utilisation de listes de distribution

La fonctionnalité Groupes permet de créer des listes de distribution et de modifier la liste des personnes auxquelles vous souhaitez envoyer un message électronique crypté.

Pour créer un groupe (liste de distribution)

1. Choisissez **Nouveau groupe** dans le menu **Groupes**.
2. Attribuez un nom à la liste de distribution de groupe. Vous avez également la possibilité d'entrer une description du groupe. Par exemple, vous pouvez appeler un groupe « Tous@entreprise.com » avec « Tous les employés » comme description.
3. Cliquez sur **OK** pour créer cette liste de distribution.

   La liste de distribution de groupe est ajoutée à votre trousseau de clés et peut être visualisée dans la fenêtre **Groupes**.

Pour ajouter des membres à une liste de distribution

1. Dans la fenêtre PGPkeys, sélectionnez les utilisateurs ou les listes à ajouter à votre liste de distribution.
2. Faites glisser les utilisateurs de la fenêtre PGPkeys vers la liste de distribution souhaitée dans la fenêtre **Groupes**.

> **REMARQUE :** Les membres d'une liste de distribution peuvent être ajoutés à d'autres listes de distribution.

Pour supprimer des membres d'une liste de distribution

1. Dans la liste de distribution, sélectionnez le membre à supprimer.
2. Appuyez sur SUPPR.

   Vous devez confirmer votre suppression.

Pour supprimer une liste de distribution.

1. Sélectionnez la liste de distribution à supprimer dans la fenêtre **Groupes**.
2. Appuyez sur SUPPR.

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

1. Sélectionnez la liste de distribution à ajouter à une autre liste.
2. Faites glisser la liste sélectionnée vers la liste dans laquelle vous souhaitez l'insérer.

Envoi des messages électroniques cryptés et signés vers les listes de distribution

Une fois vos listes de distribution PGP créées, vous pouvez envoyer un message électronique crypté à des groupes de destinataires. Pour plus d'informations sur la création et la modification de listes de distribution, reportez-vous à la section « Utilisation de listes de distribution » à la page 72.

Pour envoyer des messages électroniques cryptés et signés à une liste de distribution

1. Adressez le message à votre liste de distribution.

   Le nom de votre liste de distribution de cryptage doit correspondre à celui de la liste de distribution de message.

2. Utilisez votre application de messagerie pour rédiger votre message électronique, comme vous le faites habituellement.

3. Une fois votre message rédigé, cliquez sur  , afin de crypter son contenu, puis sur  pour le signer.

   La boîte de dialogue des destinataires apparaît, comme illustré à la Figure 4-1. Vous pouvez alors sélectionner les clés publiques du destinataire pour le texte que vous êtes en train de crypter ou de signer. Les options disponibles sont décrites dans la section « Cryptage et signature avec les applications de messagerie prises en charge » à la page 66.

4. Envoyez votre message.

Décryptage et vérification des messages électroniques

Le décryptage et la vérification des messages électroniques à l'aide d'une application prise en charge par les modules externes PGP est sans aucun doute la méthode la plus rapide et la plus simple. La procédure varie légèrement selon l'application utilisée. Cependant, si vous disposez d'une application de messagerie prise en charge par les modules externes, il vous suffit de cliquer sur l'icône en forme d'enveloppe dans le message ou dans la barre d'outils de votre application pour décrypter et vérifier vos messages. Dans certains cas, vous devez sélectionner **Décrypter/Vérifier** dans le menu de votre application de messagerie. De plus, si vous utilisez une application prenant en charge le standard PGP / MIME, vous pouvez décrypter et vérifier vos messages électroniques, ainsi que les pièces jointes en cliquant sur l'icône associée à votre message.

Si vous utilisez une application de messagerie qui n'est pas prise en charge par les modules externes PGP, vous décryptez et vérifiez vos messages électroniques via PGPtray. De plus, si votre message électronique comprend des pièces jointes cryptées, vous devez les décrypter via PGPtools ou PGPtray.

Pour décrypter et vérifier à partir d'applications de messagerie prises en charge

1. Ouvrez votre message électronique, comme vous le faites habituellement.

   Un bloc de texte chiffré inintelligible apparaît dans le corps de votre message électronique.

2. Copiez ce texte chiffré dans le Presse-papiers.

3. Pour décrypter et vérifier le message, cliquez sur l'icône en forme d'enveloppe verrouillée ( ).

   Pour décrypter et vérifier les fichiers en pièces jointes, décryptez-les séparément via PGPtools ou PGPtray.

   La boîte de dialogue **PGP - Saisie d'un mot de passe complexe** apparaît, comme illustré à la Figure 4-5. Vous êtes invité à saisir votre mot de passe complexe.

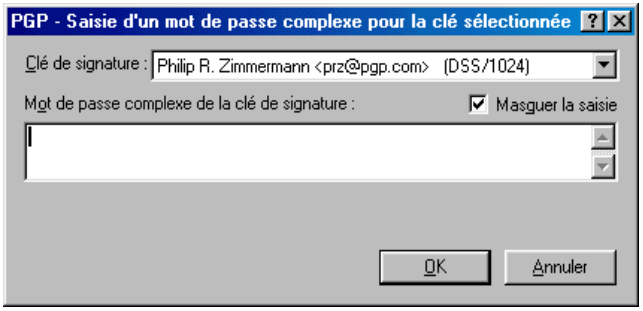


Figure 4-5. Boîte de dialogue Mot de passe complexe de clé de signature

4. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

   Le message est alors décrypté. Si ce message a été signé et que vous disposez de la clé publique de l'expéditeur, un message indiquant que la signature est correcte apparaît.

   Si le message est crypté avec l'option **Affichage sécurisé**, un avertissement apparaît. Pour continuer, cliquez sur **OK**. Le message décrypté apparaît sur un écran PGP sécurisé dans une police spéciale de prévention contre les attaques TEMPEST.

5. Vous pouvez alors enregistrer le message sous sa forme décryptée ou sous sa version cryptée d'origine, de sorte qu'il demeure sécurisé.

> **REMARQUE :** Les messages cryptés dont l'option **Affichage sécurisé** a été activée ne peuvent pas être enregistrés sous forme décryptée.

Pour décrypter et vérifier à partir d'applications de messagerie non prises en charge

1. Ouvrez votre message électronique, comme vous le faites habituellement.

   Un bloc de texte chiffré inintelligible apparaît dans le corps de votre message électronique.

2. Dans PGPtray, sélectionnez **Décrypter/Vérifier**.

   Si le message électronique comprend des pièces jointes cryptées, décryptez-les séparément via PGPtools ou PGPtray.

   La boîte de dialogue **PGP - Saisie d'un mot de passe complexe** apparaît, comme illustré à la Figure 4-5. Vous êtes invité à saisir votre mot de passe complexe.

3. Saisissez-le, puis cliquez sur **OK**.

   Le message est alors décrypté. Si ce message a été signé, un message indiquant que la signature est correcte apparaît.

   Si le message a été crypté avec l'option **Affichage sécurisé** activée, un avertissement apparaît. Pour continuer, cliquez sur **OK**. Le message décrypté apparaît sur un écran PGP sécurisé dans une police spéciale de prévention contre les attaques TEMPEST.

4. Vous pouvez alors enregistrer le message sous sa forme décryptée ou sous sa version cryptée d'origine, de sorte qu'il demeure sécurisé.

> **REMARQUE :** Les messages cryptés dont l'option **Affichage sécurisé** a été activée ne peuvent pas être enregistrés sous forme décryptée.

Utilisation de PGP pour le stockage sécurisé de fichiers 5

Ce chapitre décrit comment utiliser PGP pour conserver des fichiers de manière sécurisée. Vous y trouverez des explications sur le cryptage, le décryptage, la signature et la vérification de fichiers destinés au courrier électronique ou au stockage sur votre ordinateur. Ce chapitre décrit également les fonctions permettant la suppression définitive de fichiers en effaçant leur contenu de votre ordinateur.

Utilisation de PGP pour le cryptage et le décryptage des fichiers

Vous pouvez utiliser PGP pour crypter et signer des fichiers utilisés comme pièces jointes aux messages électroniques. Vous pouvez également avoir recours aux techniques décrites dans ce chapitre pour crypter et signer des fichiers, afin de les stocker de manière sécurisée sur votre ordinateur.

Utilisation du menu contextuel de PGP pour le cryptage et la signature

Pour envoyer un fichier crypté sous forme de pièce jointe à votre message électronique ou pour crypter un fichier à des fins de protection sur votre ordinateur, utilisez le menu contextuel de PGP.

Pour crypter et signer à l'aide du menu contextuel

1. Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le(s) fichier(s) à crypter.
2. Choisissez ensuite l'une des options suivantes :
   - **Crypter.** Pour crypter uniquement le(s) fichier(s) sélectionné(s), choisissez cette option.
   - **Signer.** Pour signer uniquement le(s) fichier(s) sélectionné(s), choisissez cette option.
   - **Crypter et signer.** Pour crypter et signer le(s) fichier(s) sélectionné(s), choisissez cette option.

La boîte de dialogue **Sélection de la clé PGP** apparaît, comme illustré à la Figure 5-1.

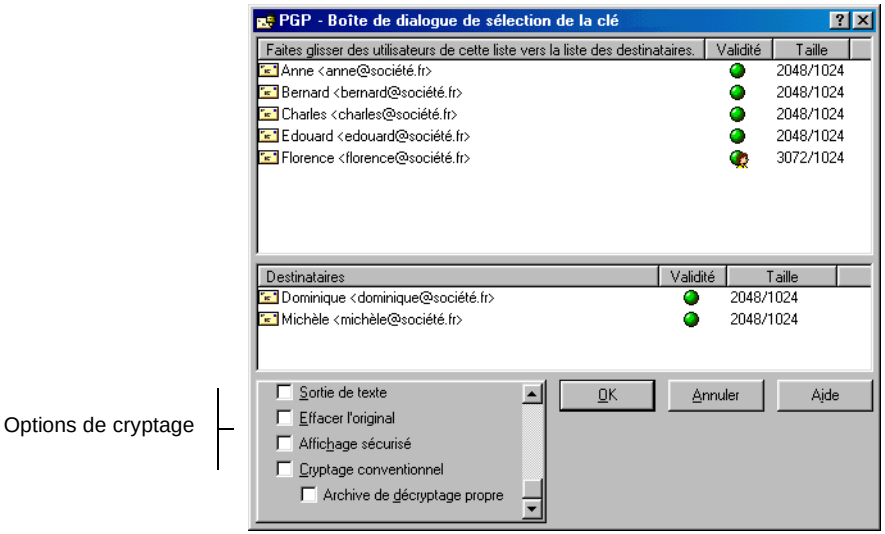


Figure 5-1. Boîte de dialogue Destinataires de PGP

Sélectionnez les clés publiques du destinataire du fichier que vous êtes en train de crypter ou de signer.

3. Sélectionnez les clés publiques en les faisant glisser vers la liste **Destinataires**.

   Vous pouvez sélectionner l'une des options de cryptage suivantes en fonction du type de données que vous êtes en train de crypter :

   - **Sortie de texte.** Lorsque vous utilisez certaines applications de messagerie pour l'envoi de fichiers sous forme de pièces jointes, vous pouvez cocher la case **Sortie de texte** pour enregistrer le fichier sous forme de texte ASCII. Cette procédure est parfois nécessaire lors de l'envoi d'un fichier binaire à l'aide d'anciennes applications de messagerie. Lorsque vous choisissez cette option, la taille du fichier crypté augmente de 30 pour cent environ.

   - **Effacer l'original.** Pour écraser le document d'origine que vous cryptez, cochez cette case de sorte qu'un utilisateur ayant accès à votre disque dur ne puisse pas lire vos informations confidentielles.

- **Affichage sécurisé.** Cochez cette case pour protéger le texte contre les attaques TEMPEST lors du décryptage. Les données sont alors affichées dans une police spéciale de prévention contre les attaques TEMPEST. Elles sont ainsi illisibles par les équipements de capture du rayonnement lors du décryptage. Pour plus d'informations sur les attaques TEMPEST, reportez-vous à la section « Vulnérabilités » à la page 246.

  REMARQUE : Cette option est accessible uniquement lors du cryptage de texte ou de fichiers de texte.

- **Cryptage conventionnel.** Cochez cette case pour que le cryptage repose sur un mot de passe complexe commun plutôt que sur la cryptographie de clé publique. Le fichier est alors crypté à l'aide d'une clé de session permettant le cryptage (et le décryptage) via un mot de passe complexe à définir.

- **Archive d'auto-décryptage.** Cochez cette case pour créer un fichier exécutable d'auto-décryptage. Le fichier est alors crypté à l'aide d'une clé de session permettant le cryptage (et le décryptage) via un mot de passe complexe à définir. Pour décrypter le fichier exécutable obtenu, cliquez deux fois dessus, puis entrez le mot de passe complexe approprié. Cette option s'avère particulièrement utile aux utilisateurs qui transmettent des fichiers cryptés à des correspondants ne disposant pas de PGP. Notez que l'expéditeur et le destinataire doivent utiliser la même plate-forme.

Si vous signez des fichiers, vous devez entrer votre mot de passe complexe.

Une fois le cryptage terminé, le dossier contenant le fichier d'origine comporte un fichier portant le nom spécifié, représenté par l'une de ces quatre icônes :

crypté avec sortie classique

crypté avec sortie de texte

sortie d'archive d'auto-décryptage

sortie d'archive d'auto-extraction

Si vous cryptez ou signez un dossier, la sortie peut se trouver dans un nouveau dossier, en fonction des options sélectionnées.

Utilisation de PGPtools pour le cryptage et la signature

Pour crypter et signer à l'aide de PGPtools

1. Ouvrez PGPtools.
2. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) à crypter.

   Vous pouvez sélectionner plusieurs fichiers, mais vous devez les crypter et les signer un par un.
3. Faites glisser le(s) fichier(s) vers l'un des boutons de PGPtools **Crypter**, **Signer** ou **Crypter** et **signer**.

   La boîte de dialogue **Destinataires de PGP** apparaît, comme illustré à la Figure 5-1
4. Sélectionnez les clés publiques en les faisant glisser vers la liste **Destinataires**.
5. Vous pouvez sélectionner l'une des options de cryptage suivantes en fonction du type de données que vous êtes en train de crypter :

   - **Sortie de texte.** Lorsque vous utilisez certaines applications de messagerie pour l'envoi de fichiers sous forme de pièces jointes, cochez la case **Sortie de texte** pour enregistrer le fichier sous forme de texte ASCII. Cette procédure est parfois nécessaire lors de l'envoi d'un fichier binaire à l'aide d'anciennes applications de messagerie. Lorsque vous choisissez cette option, la taille du fichier crypté augmente de 30 pour cent environ.
   - **Effacer l'original.** Pour écraser le document d'origine que vous cryptez, cochez cette case de sorte qu'un utilisateur ayant accès à votre disque dur ne puisse pas lire vos informations confidentielles.
   - **Affichage sécurisé.** Cochez cette case pour protéger le texte contre les attaques TEMPEST lors du décryptage. Les données sont alors affichées dans une police spéciale de prévention contre les attaques TEMPEST. Elles sont ainsi illisibles par les équipements de capture du rayonnement lors du décryptage. Pour plus d'informations sur les attaques TEMPEST, reportez-vous à la section « Vulnérabilités » à la page 246.

REMARQUE : Cette option est accessible uniquement lors du cryptage de texte ou de fichiers de texte.

- **Cryptage conventionnel.** Cochez cette case pour que le cryptage repose sur un mot de passe complexe commun plutôt que sur la cryptographie de clé publique. Le fichier est alors crypté à l'aide d'une clé de session permettant le cryptage (et le décryptage) via un mot de passe complexe à définir.
- **Archive d'auto-décryptage.** Cochez cette case pour créer un fichier exécutable d'auto-décryptage. Le fichier est alors crypté à l'aide d'une clé de session permettant le cryptage (et le décryptage) via un mot de passe complexe à définir. Pour décrypter le fichier exécutable obtenu, cliquez deux fois dessus, puis entrez le mot de passe complexe approprié. Cette option s'avère particulièrement utile aux utilisateurs qui transmettent des fichiers cryptés à des correspondants ne disposant pas de PGP. Notez que l'expéditeur et le destinataire doivent utiliser la même plate-forme.

6. Cliquez sur **OK**.

   Si vous signez des fichiers, vous devez entrer votre mot de passe complexe.

   Une fois le cryptage terminé, le dossier contenant le fichier d'origine comporte un fichier portant le nom spécifié représenté par l'une de ces quatre icônes :


crypté avec sortie classique


crypté avec sortie de texte


sortie d'archive d'auto-décryptage


sortie d'archive d'auto-extraction

   Si vous cryptez ou signez un dossier, la sortie peut se trouver dans un nouveau dossier, en fonction des options sélectionnées.

Utilisation de PGPtray pour le décryptage et la vérification

Si le message électronique reçu comprend des pièces jointes et que vous n'utilisez pas d'application de messagerie compatible PGP / MIME, vous devez décrypter ces pièces jointes dans le Presse-papiers Windows.

Pour décrypter et vérifier des fichiers à l'aide de PGPtray

1. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) à décrypter et vérifier.
2. Dans PGPtray, choisissez **Décrypter/vérifier**.

   La boîte de dialogue de mot de passe complexe apparaît, comme illustré à la Figure 5-2.

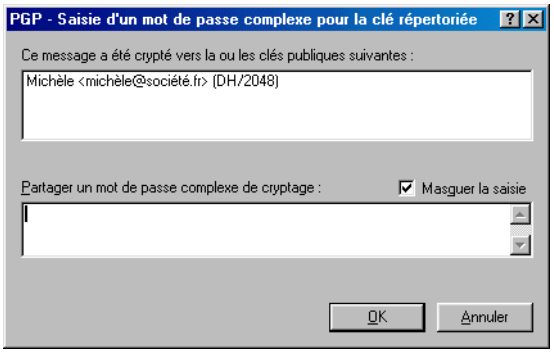


Figure 5-2. Boîte de dialogue de mot de passe complexe

3. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

   Le fichier est alors décrypté. S'il a été signé, un message indique si la signature est valide.

   Si le fichier de texte est crypté avec l'option **Affichage sécurisé**, un message d'avertissement apparaît. Pour continuer, cliquez sur **OK**. Le texte décrypté apparaît sur un écran PGP sécurisé dans une police spéciale de prévention contre les attaques TEMPEST.
4. Vous pouvez enregistrer le message sous sa forme décryptée ou enregistrer la version cryptée d'origine pour qu'elle reste sécurisée.

> **REMARQUE :** Les messages cryptés avec l'option **Affichage sécurisé** ne peuvent pas être enregistrés sous forme décryptée. Il est seulement possible de les afficher sur un écran PGP sécurisé, une fois le cryptage terminé.

Utilisation de PGPtools pour le décryptage et la vérification

Pour le décryptage et la vérification à l'aide de PGPtools

1. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) à décrypter.
2. Dans PGPtools, faites glisser le(s) fichier(s) vers le bouton **Décrypter/vérifier.**

   La boîte de dialogue **PGP - Saisie d'un mot de passe complexe** apparaît, comme illustré à la Figure 5-2, et vous demande d'entrer votre mot de passe complexe.
3. Entrez-le, puis cliquez sur **OK**.

   Si le fichier est signé, un message indique si la signature est valide.

   Si le fichier de texte est crypté avec l'option **Affichage sécurisé**, un message d'avertissement apparaît. Pour continuer, cliquez sur **OK**. Le texte décrypté apparaît sur un écran PGP sécurisé dans une police spéciale de prévention contre les attaques TEMPEST.
4. Vous pouvez enregistrer le message sous sa forme décryptée ou enregistrer la version cryptée d'origine, pour qu'elle reste sécurisée.

> **REMARQUE :** Les messages cryptés avec l'option **Affichage sécurisé** ne peuvent pas être enregistrés sous forme décryptée. Il est seulement possible de les afficher sur un écran PGP sécurisé, une fois le cryptage terminé.

Signature et décryptage de fichiers avec une clé découpée

Une fois qu'une clé est partagée entre les divers détenteurs de parties de clé, PGP tente de reconstituer automatiquement cette clé si vous souhaitez l'utiliser pour signer ou décrypter. Il existe deux méthodes de reconstitution de clés : la reconstitution locale et la reconstitution distante.

La reconstitution locale des parties de clé nécessite la présence des détenteurs près de l'ordinateur reconstituant la clé. Chaque détenteur d'une partie de la clé doit entrer le mot de passe complexe correspondant à sa partie.

La reconstitution distante des parties de la clé nécessite que les détenteurs distants authentifient et décryptent leurs clés avant de les envoyer via le réseau. La sécurité de la couche de transport (TLS) de PGP fournit une liaison sécurisée pour le transport des parties de clé, ce qui permet à plusieurs personnes distantes les unes des autres d'utiliser leur partie de clé pour signer ou décrypter de manière sécurisée.

IMPORTANT : Avant la réception des parties de la clé via le réseau, il est conseillé de vérifier l'empreinte digitale de chaque détenteur et de signer sa clé publique afin d'assurer que la clé d'authentification est valide. Pour plus d'informations sur la vérification d'une paire de clés, reportez-vous à la section « Vérification de clés à l'aide d'une empreinte digitale » à la page 63.

Pour reconstituer une clé découpée

1. Contactez chaque détenteur d'une partie de la clé découpée. Pour reconstituer localement une partie de clé, les détenteurs des parties de cette clé doivent être présents.

   Pour collecter les parties de clé via le réseau, assurez-vous que leurs détenteurs sont prêts à envoyer leur fichier de parties de clé. Les détenteurs distants doivent disposer des éléments suivants :

   – leur fichier de parties de clé et leur mot de passe complexe ;

   – une clé publique (pour l'authentification sur l'ordinateur collectant les parties de la clé) ;

   – une connexion réseau ;

   – l'adresse IP ou le nom de domaine de l'ordinateur collectant les parties de la clé.

2. Sur l'ordinateur reconstituant la clé, utilisez l'Explorateur Windows pour sélectionner le(s) fichier(s) à signer ou décrypter avec la clé découpée.

3. Cliquez sur le(s) fichier(s) avec le bouton droit de la souris, puis sélectionnez **Signer ou Décrypter** dans le menu **PGP**.

   La boîte de dialogue **PGP – Saisie d'un mot de passe complexe pour la clé sélectionnée** apparaît avec la clé découpée sélectionnée.

4. Pour reconstituer la clé sélectionnée, cliquez sur **OK**.

   La boîte de dialogue **Collecte de parties de clés** apparaît, comme illustré à la Figure 5-3

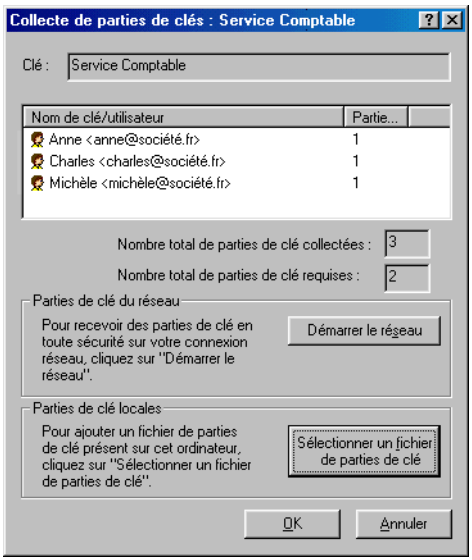


Figure 5-3. Boîte de dialogue Collecte de parties de clés

5. Effectuez l'une des opérations suivantes :

   - **Si vous collectez les parties de la clé localement**, cliquez sur **Sélection d'un fichier de parties de clé**, puis recherchez les fichiers de parties de clé associés à la clé découpée. Ces fichiers peuvent être collectés à partir du disque dur, d'une disquette ou d'un disque monté. Passez à l'Etape 6.

   - **Si vous collectez les parties de la clé via le réseau**, cliquez sur **Démarrer le réseau**.

     La boîte de dialogue **Mot de passe complexe** apparaît. Dans la zone **Clé de signature**, sélectionnez la paire de clés à utiliser pour l'authentification sur le système distant, puis entrez le mot de passe complexe. Pour préparer l'ordinateur à la réception de parties de la clé, cliquez sur **OK**.

     L'état de la transaction apparaît dans la zone **de partages du réseau.** Lorsque l'état est défini sur « Ecoute de…», PGP est prêt à recevoir les parties de clé.

     A ce stade, les détenteurs doivent envoyer leur partie de la clé. Pour plus d'informations sur l'envoi de parties de la clé vers l'ordinateur de reconstitution, reportez-vous à la section « Pour envoyer votre partie de clé sur le réseau » à la page 87.

Lors de la réception d'une clé, la boîte de dialogue **Authentification distante** apparaît, comme illustré à la Figure 5-4.

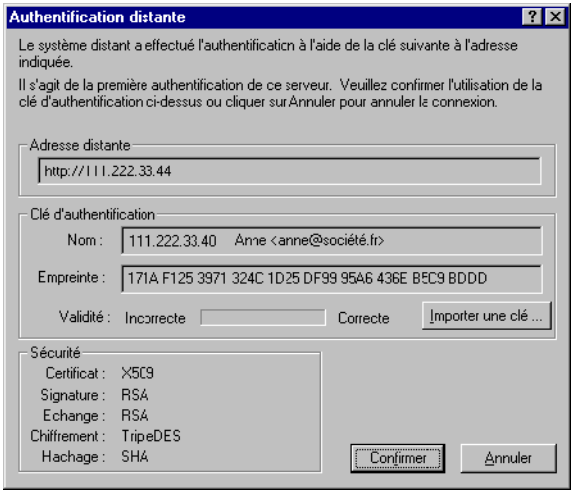


Figure 5-4. Boîte de dialogue Authentification distante

Si vous n'avez pas signé la clé utilisée pour l'authentification du système distant, elle est considérée comme non valide. Bien que vous puissiez le faire, il est déconseillé de reconstituer la clé avec une clé d'authentification non valide. Il est recommandé de vérifier l'empreinte digitale de chaque détenteur d'une partie de la clé et de signer sa clé publique afin d'assurer que la clé d'authentification est valide.

Pour accepter le fichier des parties de clé, cliquez sur **Confirmer**.

6. Poursuivez la collecte de parties de la clé jusqu'à ce que la valeur de **Nombre total des parties de la clé collectées** corresponde à celle de **Nombre total des parties de la clé requises** dans la boîte de dialogue **de collecte de parties de clés**.

7. Cliquez sur **OK**.

   Le fichier est alors signé ou décrypté avec la clé découpée.

Pour envoyer votre partie de clé sur le réseau

1. Lorsque vous êtes contacté par la personne reconstituant la clé découpée, assurez-vous de disposer des éléments suivants :
   - votre fichier de partie de la clé et votre mot de passe complexe ;
   - votre paire de clés (pour l'authentification sur l'ordinateur collectant les parties de la clé) ;
   - une connexion réseau ;
   - l'adresse IP ou le nom de domaine de l'ordinateur reconstituant la clé.
2. Sélectionnez **Envoyer des parties de clé** dans le menu **Fichier** de PGPkeys.

   La boîte de dialogue **Sélection d'un fichier de parties de clé** apparaît.
3. Recherchez votre partie de la clé, puis cliquez sur **Ouvrir**.

   La boîte de dialogue **PGP – Saisie d'un mot de passe complexe** apparaît.
4. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

   La boîte de dialogue **Envoyer des parties de clé** apparaît, comme illustré à la Figure 5-5.

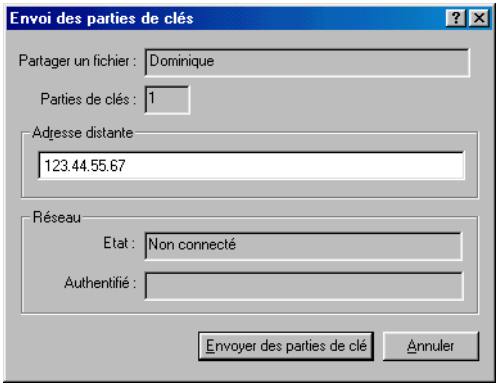


Figure 5-5. Boîte de dialogue Envoyer des parties de clé

5. Dans la zone **Adresse distante**, entrez l'adresse IP ou le nom du domaine de l'ordinateur reconstituant la clé, puis cliquez sur **Envoyer des parties de clé**.

   L'état de la transaction apparaît dans la zone **Etat du réseau**. Lorsque l'état passe à « Connecté », vous devez vous authentifier sur l'ordinateur de reconstitution.

   La boîte de dialogue **Authentification distante** apparaît, vous demandant de confirmer que l'ordinateur distant correspond à celui auquel vous souhaitez envoyer votre partie de clé.

6. Pour terminer la transaction, cliquez sur **Confirmer**.

   Après réception des parties de la clé par l'ordinateur distant et confirmation de la transaction, une zone de message apparaît, indiquant que l'envoi des parties de la clé est terminé.

7. Cliquez sur **OK**.

8. Une fois l'envoi de votre partie de clé achevé, cliquez sur **Terminé** dans la fenêtre **Parties de clé**.

Utilisation de la fonction d'effacement de PGP pour la suppression de fichiers

L'option **Effacer** de PFPtools supprime des fichiers et leur contenu. Cette fonctionnalité permet de supprimer définitivement un fichier et son contenu du disque dur de votre ordinateur en toute sécurité. Lorsque vous supprimez un fichier, vous le placez habituellement dans la Corbeille. Le nom du fichier n'apparaît plus dans le répertoire, mais ses données sont conservées sur le disque. La fonction **Effacer** supprime toute trace des données du fichier, de sorte qu'aucun utilisateur ne peut utiliser d'outil logiciel pour récupérer le fichier.

Pour supprimer définitivement un fichier à l'aide du menu contextuel de PGP

1. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) à effacer.

2. Cliquez sur le(s) fichier(s) avec le bouton droit de la souris, puis choisissez **Effacer** dans le menu.

   Une boîte de dialogue de confirmation apparaît.

3. Pour effacer définitivement le fichier, cliquez sur **OK**.

   Pour interrompre l'effacement des fichiers avant la fin de la procédure, cliquez sur **Annuler**.

> **REMARQUE :** Si vous cliquez sur **Annuler** au cours de la procédure d'effacement, il se peut que le fichier ne soit pas totalement effacé.

Pour supprimer définitivement un fichier à l'aide de PGPtools

1. Dans l'Explorateur Windows, sélectionnez le(s) fichier(s) à effacer.
2. Faites glisser le(s) fichier(s) vers le bouton **Effacer** () de PGPtools.

   Une boîte de dialogue de confirmation apparaît.
3. Pour effacer définitivement le fichier, cliquez sur **OK**.

   Pour interrompre l'effacement des fichiers avant la fin de la procédure, cliquez sur **Annuler**.

> **REMARQUE :** Si vous cliquez sur **Annuler** au cours de la procédure d'effacement, il se peut que le fichier ne soit pas totalement effacé.

PGP écrase l'intégralité du contenu du fichier, même sur les systèmes comportant de la mémoire virtuelle. Il est important de noter que certaines applications enregistrent le fichier avant de le crypter et peuvent laisser des fragments de ce fichier sur votre disque dans des emplacements qui ne sont plus considérés comme appartenant au fichier. Pour plus d'informations, reportez-vous à la section « Fichiers d'échange ou mémoire virtuelle » à la page 249.
Pour résoudre ce problème, vous pouvez utiliser l'Assistant Effacer l'espace libre de PGP. Pour plus d'informations sur cet Assistant, reportez-vous à la section suivante. Soyez également attentif au fait que de nombreux programmes enregistrent automatiquement les fichiers ouverts. Des copies de sauvegarde du fichier à supprimer peuvent donc exister.

Utilisation de l'Assistant Effacer l'espace libre pour nettoyer les secteurs libres de vos disques

Lorsque vous créez des fichiers sur votre ordinateur et les supprimez ensuite, les données qu'ils contiennent restent sur le lecteur. Afin qu'il soit impossible de récupérer les données d'un fichier, PGPtools permet de les effacer de manière sécurisée avant de supprimer ce fichier.

De nombreux programmes créent des fichiers temporaires lorsque vous modifiez le contenu des documents. Ces fichiers sont supprimés lorsque vous fermez les documents, mais les données réelles des documents sont dispersées sur votre lecteur. Afin de réduire les chances de pouvoir récupérer ultérieurement les données de vos documents, Network Associates vous conseille d'effacer l'espace libre sur vos disques, ainsi que de supprimer les documents confidentiels, et ce de manière sécurisée.

Pour effacer l'espace libre sur vos disques

AVERTISSEMENT : Avant de lancer l'Assistant Effacer l'espace libre de PGP, désactivez la fonction de partage de fichiers et fermez l'ensemble des applications sur le volume ou le disque dont vous souhaitez effacer l'espace libre.

1. Ouvrez PGPtools.
2. Dans la fenêtre PGPtools, cliquez sur **Effacer l'espace libre** ().

   L'écran de bienvenue de **l'Assistant Effacer l'espace libre** de PGP apparaît.
3. Lisez les informations avec attention, puis cliquez sur **Suivant** pour accéder à la boîte de dialogue suivante.

   L'Assistant vous invite à sélectionner le volume à effacer et le nombre de passages à effectuer.
4. Dans la zone **Volume**, sélectionnez le disque ou volume à effacer. Sélectionnez ensuite le nombre de passages à effectuer. Les recommandations concernant les passages sont les suivantes :

   - 3 passages pour une utilisation personnelle ;
   - 10 passages pour une utilisation commerciale ;

- 18 passages pour une utilisation militaire ;
- 26 passages pour une sécurité maximale.

REMARQUE : Les sociétés de récupération de données commerciales sont réputées pour être en mesure de récupérer des données ayant été écrasées jusqu'à 9 fois. A chaque effacement, PGP utilise des modèles hautement élaborés rendant impossible toute récupération de vos données confidentielles.

5. Pour continuer, cliquez sur **Suivant**.

   La boîte de dialogue **Effacement** apparaît, comme illustré à la Figure 5-6, puis affiche les informations statistiques relatives au lecteur ou au volume sélectionné.

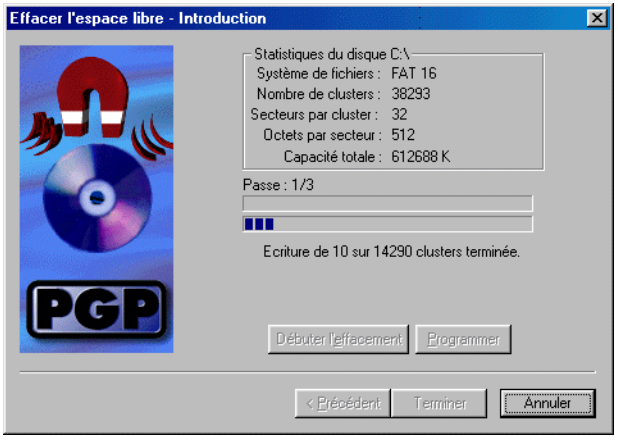


Figure 5-6. Effacement de l'espace libre (boîte de dialogue Effacement)

6. Pour démarrer l'effacement du disque ou du volume, cliquez sur **Débuter l'effacement**.

   L'Assistant Effacer l'espace libre de PGP analyse, puis efface de votre disque ou volume les fragments de données.

7. A la fin de la session, cliquez sur **Terminer**.

AVERTISSEMENT : Si vous cliquez sur **Annuler** au cours de la procédure d'effacement, il se peut que le fichier ne soit pas totalement effacé.

Programmation de l'Assistant Effacer l'espace libre

Pour programmer des effacements sécurisés de l'espace libre sur vos disques à intervalles réguliers, vous pouvez utiliser le programmateur des tâches de Windows.

IMPORTANT : L'utilisation de cette fonction requiert l'installation du programmateur des tâches de Windows sur votre poste. Vous pouvez le télécharger depuis le site de Microsoft (http:/ / www.microsoft.com).

Pour programmer l'effacement de l'espace libre

1. Suivez les étapes 1 à 5 de la section « Pour effacer l'espace libre sur vos disques » à la page 90.

   La boîte de dialogue **Effacement** apparaît, comme illustré à la Figure 5-6, puis affiche les informations statistiques relatives au lecteur ou au volume sélectionné.

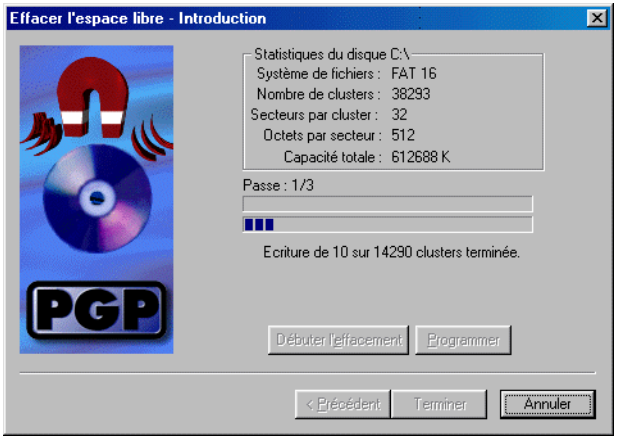


Figure 5-7. Assistant Effacer l'espace libre de PGP (boîte de dialogue Effacement)

2. Pour démarrer l'effacement du disque ou du volume, cliquez sur **Programmer**.

   La boîte de dialogue **Programmation de l'effacement de l'espace libre** apparaît.

3. Pour continuer, cliquez sur **OK**.

   Si vous utilisez Windows NT, la boîte de dialogue de confirmation de mot de passe de Windows NT apparaît.

   Entrez votre mot de passe de connexion à Windows NT dans la première zone. Pour accéder à la zone suivante, appuyez sur la touche de tabulation, puis confirmez votre saisie en entrant à nouveau votre mot de passe. Cliquez sur OK.

   La boîte de dialogue de **programmation des tâches de Windows** apparaît, comme illustré à la Figure 5-8.

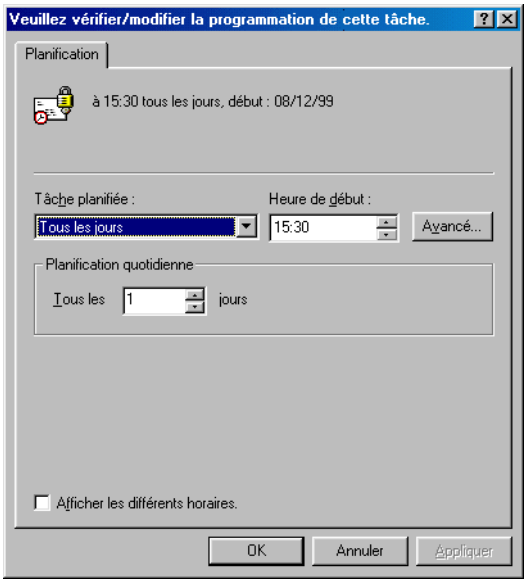


Figure 5-8. Boîte de dialogue de programmation des tâches de Windows

4. Dans la zone de programmation des tâches, sélectionnez la fréquence d'exécution de la tâche souhaitée. Les sélections possibles sont les suivantes :

   - **Quotidienne.** Votre tâche sera exécutée une fois à l'heure et au jour définis. Pour fermer la boîte de dialogue, cliquez sur **OK**, puis entrez, dans la zone **d'heure de début**, l'heure à laquelle la tâche doit être exécutée.

- **Hebdomadaire.** Votre tâche sera exécutée une fois par semaine, à la date et à l'heure spécifiées. Indiquez dans la zone pertinente le nombre de semaines entre chaque effacement de disque, puis sélectionnez un jour dans la liste de **programmation d'exécution hebdomadaire de tâches**.
- **Mensuelle.** Votre tâche sera exécutée une fois par mois, à la date et à l'heure spécifiées. Entrez dans la zone pertinente l'heure souhaitée, puis entrez la date à laquelle la tâche doit être exécutée. Pour définir les mois où la tâche doit être exécutée, cliquez sur le bouton de **sélection de mois**.
- **Unique.** Votre tâche sera exécutée une seule fois par semaine, à la date et à l'heure spécifiées. Entrez dans la zone pertinente l'heure souhaitée, puis sélectionnez un mois et une date dans la zone **d'exécution**.
- **Au démarrage du système.** La tâche sera exécutée uniquement au démarrage de votre système.
- **A la connexion.** La tâche sera exécutée au moment où vous vous connectez à votre ordinateur.
- **En mode inactif.** Votre tâche sera exécutée lorsque votre système est inactif et pendant la durée définie dans la zone des minutes.

5. Vous pouvez ouvrir une boîte de dialogue vous permettant de sélectionner davantage d'options de programmation, comme la date de début, la date de fin et la durée d'exécution de la tâche en cliquant sur **Avancé**.
6. Cliquez sur **OK**.

   Une boîte de dialogue de confirmation apparaît. Votre tâche d'effacement de l'espace libre est à présent programmée.

Gestion des clés et définition des options de PGP 6

Ce chapitre explique comment vérifier et gérer les clés stockées dans vos trousseaux. Il décrit également le paramétrage de vos options de manière à répondre à vos besoins informatiques spécifiques.

Gestion des clés

Les clés que vous créez, ainsi que celles que vous récupérez auprès d'autres utilisateurs, sont stockées dans vos trousseaux de clés, généralement sur votre disque dur ou sur une disquette. Habituellement, vos clés privées sont conservées dans un fichier appelé secring. skr et vos clés publiques dans un autre fichier appelé pubring. pkr. Ces deux fichiers sont plus fréquemment situés dans le dossier PGP Keyrings.

❑ **REMARQUE :** Etant donné que le cryptage de votre clé privée est automatique et dans la mesure où votre mot de passe complexe n'est pas compromis, le stockage de vos trousseaux de clés sur votre ordinateur ne comporte aucun danger. Toutefois, si vous ne souhaitez pas stocker vos clés dans le dossier par défaut, vous pouvez choisir un nom de fichier et un emplacement différents de ceux définis par défaut. Pour plus d'informations, reportez-vous à la section « Définition des options de PGP » de ce chapitre.

Parfois, il peut arriver que vous souhaitiez consulter ou modifier les attributs associés à vos clés. Par exemple, lorsque vous récupérez la clé publique d'un autre utilisateur, vous voulez peut-être identifier son type (RSA ou Diffie-Hellman / DSS), vérifier son empreinte digitale ou déterminer sa validité en fonction de toute signature numérique incluse avec cette clé. Il peut s'avérer également utile de signer la clé publique d'un autre utilisateur afin d'indiquer que vous pensez qu'il s'agit d'une clé valide, attribuer un niveau de confiance au détenteur de cette clé ou modifier le mot de passe complexe de votre clé privée. Enfin, vous souhaitez peut-être rechercher un serveur de clés pour récupérer la clé publique d'un autre utilisateur. PGPkeys vous permet d'effectuer toutes ces fonctions de gestion des clés.

Fenêtre PGPkeys

Pour ouvrir la fenêtre PGPkeys, choisissez

Programmes-->PGP-->PGPkeys dans le menu **Démarrer** ou cliquez sur l'icône PGPtray ( ) dans la Barre des tâches, puis sur **Lancer PGPkeys**.

La fenêtre **PGPkeys** illustrée à la Figure 6-1 apparaît et affiche les clés que avez créées, ainsi que celles que vous avez ajoutées à votre trousseau de clés publiques.

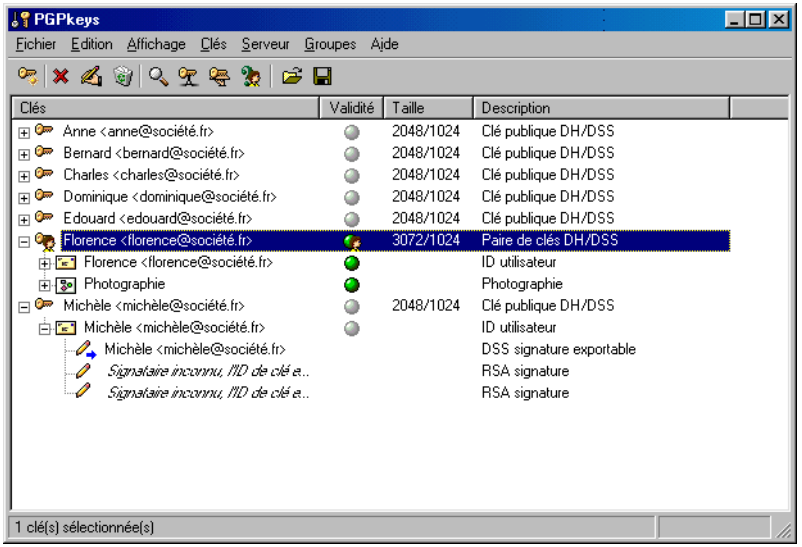


Figure 6-1. Fenêtre PGPkeys

Une icône représentant une clé accompagnée d'un utilisateur ( ) correspond aux paires de clés publiques et privées, et l'icône représentant uniquement une clé ( ) correspond aux clés publiques que vous avez récupérées auprès d'autres utilisateurs. Si vous disposez de plusieurs types de clés, vous remarquerez que les clés de type RSA sont représentées par des clés en argent et celles de type Diffie-Hellman / DSS par des clés en or.

Pour développer l'arborescence des entrées et visualiser l'ID utilisateur et l'adresse e-mail du détenteur de la clé symbolisée une icône représentant une enveloppe ( ), cliquez sur le signe (+), situé en regard de l'icône de la clé. Pour afficher les signatures de tous les utilisateurs ayant certifié l'ID utilisateur, cliquez sur le signe (+), situé en regard de l'icône représentant une enveloppe. Pour développer ces informations pour un ensemble de clés, il vous suffit de sélectionner la(les) clé(s) souhaitée(s), puis de choisir **Développer la sélection** dans le menu **Edition**.

Définitions des attributs PGPkeys

Vous pouvez afficher certains des attributs associés à des clés dans la fenêtre principale PGPkeys à partir du menu **Affichage**. Pour chaque élément sélectionné dans ce menu, PGPkeys affiche une colonne dans la fenêtre principale. Pour modifier l'ordre de ces colonnes, cliquez sur l'en-tête de la colonne à déplacer, puis faites-la glisser vers l'emplacement souhaité.

Tableau 6-1. Présentation des attributs PGPkeys

Clés	Affiche une icône de la clé, suivie du nom d'utilisateur et de l'adresse e-mail de son détenteur, ainsi que des noms des signataires de cette clé.
Validité	Indique le niveau de confiance quant aux informations relatives au détenteur supposé. La validité repose sur l'identité du ou des signataire(s) de la clé et sur le niveau de confiance que vous leur accordez pour répondre de son authenticité. Les clés publiques que vous avez personnellement signées présentent le niveau de validité maximal, selon l'hypothèse que vous signez la clé d'un utilisateur uniquement si vous êtes totalement sûr que cette clé est valide. La validité de toute autre clé, non signée personnellement, dépend du niveau de confiance accordé à ses autres signataires. Si aucune signature n'est associée à la clé, cette clé n'est alors pas considérée comme valide, et un message vous en avertit chaque fois que vous l'utilisez. La validité est indiquée par un cercle ou une barre, selon le réglage du paramètre « Afficher le niveau de validité marginal » des **Options** avancées (reportez-vous à la section « Définition des options avancées » de ce chapitre). Lorsque cette option est cochée, la validité est représentée alors sous forme :  , d'une barre vide pour des clés non valides  , d'une barre à moitié pleine pour des clés valides de manière marginale  , d'une barre pleine pour des clés valides ne vous appartenant pas  , d'une barre hachurée pour des clés valides vous appartenant. Lorsque cette option est cochée, la validité est représentée alors sous forme :  , d'un rond gris pour des clés considérées comme marginalement valides si l'**option** avancée « Traiter les clés correctes marginalement comme incorrectes » est cochée  , d'un rond vert pour des clés valides ne vous appartenant pas. Dans le cadre de votre entreprise, votre agent de sécurité peut utiliser la clé de signature d'entreprise pour signer les clés des utilisateurs. Les clés signées à l'aide de cette dernière sont généralement considérées comme parfaitement valides. Pour plus d'informations, reportez-vous au Chapitre 2, « Utilisation de PGP ».
Taille	Affiche le nombre de bits utilisés pour la construction de la clé. Généralement, plus la clé est volumineuse, moindres sont les chances qu'elle soit compromise. Toutefois, le cryptage et le décryptage de données à l'aide de clés de grande taille sont un peu plus longs qu'avec des clés de plus petite taille. Pour une clé Diffie-Hellman/DSS, le premier chiffre correspond à la partie Diffie-Hellman et le second à la partie DSS. La partie DSS est réservée à la signature et la partie Diffie-Hellman au cryptage.

Tableau 6-1. Présentation des attributs PGPkeys

Description	Décrit le type d'informations apparaissant dans la colonne **Clés** : type de clé, d'ID ou de signature.
Clé de décryptage supplémentaire	Indique si une clé de décryptage supplémentaire est associée à cette clé.
ID de clé	Numéro d'identification unique associé à chaque clé permettant de distinguer deux clés partageant les mêmes nom d'utilisateur et adresse e-mail.
Fiabilité	Indique le niveau de confiance accordé au détenteur de la clé servant de correspondant fiable pour les clés publiques des autres utilisateurs. La confiance intervient lorsque vous ne pouvez pas vérifier la validité d'une clé publique d'un autre utilisateur pour vous-même et que vous vous fiez au jugement des autres signataires de la clé. Lors de la création d'une paire de clés, celle-ci est considérée comme fiable de manière implicite, comme indiqué par hachures des barres de fiabilité et de validité ou par un rond vert accompagné d'une icône d'utilisateur. Lors de la réception d'une clé publique signée par l'un des autres utilisateurs des clés publiques de votre trousseau, son niveau d'authenticité repose sur la confiance que vous avez accordée à cette clé. Dans la boîte de dialogue **Propriétés des clés**, attribuez un niveau de confiance : Fiable, Marginale, Non fiable
Expiration	Indique la date d'expiration de la clé. L'option Jamais est attribuée à la plupart des clés. Toutefois, il peut arriver que le détenteur d'une clé souhaite l'utiliser uniquement pour une durée déterminée.
Création	Indique la date de création de la clé d'origine. Vous pouvez parfois émettre une hypothèse quant à la validité d'une clé en vous appuyant sur sa date de mise en circulation. Si cette clé est utilisée depuis longtemps, il est peu probable qu'un utilisateur tente de la remplacer, car de nombreuses copies sont en circulation. N'utilisez jamais les dates de création comme unique indicateur de validité.

Consultation des propriétés d'une clé

Outre les attributs généraux apparaissant dans la fenêtre **PGPkeys**, vous pouvez également consulter et modifier d'autres propriétés de clé et de sous-clé.

La fenêtre **Propriétés des clés** comprend les panneaux **Général**, **Sous-clés** et **Autorités de révocation**, qui vous fournissent les informations nécessaires sur la clé publique d'un utilisateur ou les possibilités de création, de configuration, de modification et de suppression des attributs associés à votre clé publique. Les sections suivantes décrivent chaque procédure en détail.

Pour accéder aux propriétés d'une clé donnée, sélectionnez-la, puis choisissez **Propriétés** dans le menu **Clés**. La boîte de dialogue **Propriétés des clés** apparaît, comme illustré à la Figure 6-2.

Figure 6-2. Boîte de dialogue Propriétés des clés (panneau Général)

Panneau des propriétés générales des clés

Pour accéder au panneau des **propriétés générales** d'une clé donnée, sélectionnez-la, puis choisissez **Propriétés** dans le menu **Clés**.

Pour obtenir une description de chaque attribut disponible dans le panneau des **propriétés générales des clés**, reportez-vous à la section Tableau 6-2, « Attributs du panneau des propriétés générales d'une clé », à la page 99.

Tableau 6-2. Attributs du panneau des propriétés générales d'une clé

ID de clé	Numéro d'identification unique associé à chaque clé permettant de distinguer deux clés partageant les mêmes nom d'utilisateur et adresse e-mail.
Type de clé	Indique s'il s'agit d'une clé RSA ou Diffie-Hellman/DSS.
Taille de la clé	Indique le nombre de bits de la clé.
Créée	Date de création de la clé.
Expire	Date d'expiration de la clé. Un détenteur spécifie cette date lorsqu'il crée ses clés. L'option Jamais est généralement sélectionnée. Toutefois, une date spécifique est attribuée à certaines clés lorsqu'il est préférable de les utiliser uniquement pour une durée déterminée.

Tableau 6-2. Attributs du panneau des propriétés générales d'une clé

Chiffrement	CAST, DES triple ou IDEA, c'est-à-dire l'algorithme de cryptage que le détenteur de la clé souhaite voir être utilisé en priorité. Le détenteur de la clé y spécifie que vous cryptez vers sa clé publique. Si cet algorithme est autorisé dans vos **Options avancées**, il sera utilisé à chaque cryptage de cette clé.
Assembler une clé	Ouvre la boîte de dialogue **Collecte de parties de clés**. Accessible uniquement pour des clés découpées. Pour plus d'informations sur la reconstitution de clés découpées, reportez-vous à la section « Signature et décryptage de fichiers avec une clé découpée » à la page 83.
Activée	Indique si la clé est actuellement activée. Lorsqu'une clé est désactivée, elle apparaît en grisée dans la fenêtre PGPkeys et aucune fonction de PGP ne peut être utilisée pour cette clé, à l'exception de **Décrypter** et **Vérifier**. Toutefois, la clé reste dans votre trousseau et vous pouvez la réactiver à tout moment. Pour activer ou désactiver une clé, cochez ou décochez la case **Activée**. (Cette case n'apparaît pas pour les clés considérées comme implicitement fiables.) Lors de l'envoi d'un message électronique crypté, cette fonction s'avère utile si vous souhaitez éviter d'encombrer la boîte de dialogue **Sélection des clés**.
Modifier le mot de passe complexe	Modifie le mot de passe complexe d'une clé privée. Si vous pensez que votre mot de passe complexe a été découvert, cliquez sur ce bouton pour en entrer un nouveau. Il est conseillé de modifier son mot de passe complexe tous les 6 mois environ. Pour plus d'informations, reportez-vous à la section « Modification du mot de passe » de ce chapitre.
Empreinte digitale	Numéro d'identification unique généré lors de la création de la clé. Il s'agit de la principale procédure de contrôle de l'authenticité d'une clé. La manière la plus sûre de vérifier une empreinte digitale est d'appeler le détenteur de cette clé par téléphone et de lui demander de lire son empreinte, puis de la comparer à votre copie de sa clé publique. L'empreinte digitale peut être visualisée de deux manières, selon une liste de mots uniques ou selon un format hexadécimal.
Hexadécimale	Affiche l'empreinte digitale sous forme d'une suite de nombres hexadécimaux. Par défaut, cette option est désactivée et l'empreinte digitale apparaît sous forme d'une suite unique de mots.
Modèle de fiabilité	Indique la validité de la clé qui repose sur sa certification et le niveau de confiance que vous accordez au détenteur pour répondre de l'authenticité de la clé publique d'un autre utilisateur. Pour définir ce niveau de confiance, ajustez la réglette jusqu'au niveau souhaité (Fiable, Marginale ou Non fiable). Cette réglette est désactivée pour les clés révoquées, arrivées à expiration et fiables de manière implicite.

Fenêtre des propriétés des sous-clés

Pour accéder au panneau des **propriétés des sous-clés** d'une clé donnée, sélectionnez-la, puis choisissez **Propriétés** dans le menu **Clés**. La boîte de dialogue **Propriétés des clés** apparaît, comme illustré à la Figure 6-2 à la page 99. Cliquez sur l'onglet **Sous-clé**. Le panneau **Sous-clé** apparaît, comme illustré à la Figure 6-3.

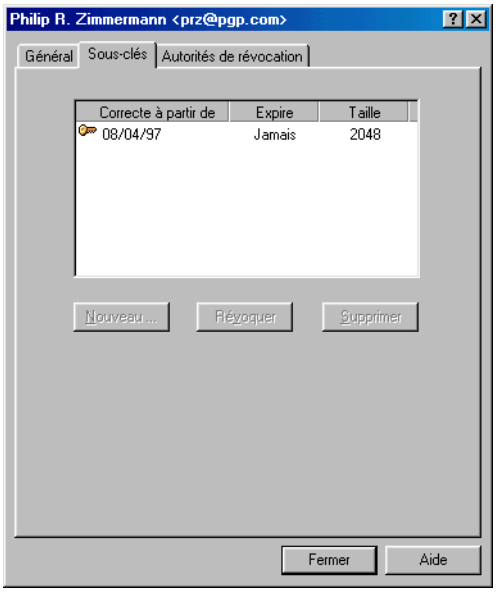


Figure 6-3. Boîte de dialogue Propriétés des clés (panneau Sous-clé)

Pour obtenir une description de chaque attribut et tâche disponibles dans le panneau **Sous-clé**, reportez-vous à la section Tableau 6-2, « Attributs du panneau des propriétés générales d'une clé », à la page 99.

Tableau 6-3. Panneau des propriétés des sous-clés

Correcte à partir de	Date d'activation de la sous-clé.
Expire	Date d'expiration de la sous-clé. Un détenteur spécifie souvent cette date lorsqu'il crée ses sous-clés. Généralement, celles-ci sont actives pour une durée limitée.
Taille de la clé	Taille de la sous-clé.
Nouveau	Crée une nouvelle sous-clé. Pour plus d'informations, reportez-vous à la section « Création de nouvelles sous-clés » à la page 34.

Tableau 6-3. Panneau des propriétés des sous-clés

Révoquer	Révoque la sous-clé de cryptage sélectionnée. Une fois votre sous-clé révoquée et votre clé redistribuée, d'autres utilisateurs ne sont plus en mesure de crypter des données vers cette sous-clé.
Supprimer	Supprime définitivement la sous-clé de cryptage sélectionnée. Vous ne pouvez pas annuler cette procédure. Toute donnée cryptée à l'aide de la sous-clé sélectionnée ne peut plus être décryptée.

ASTUCE : Pour désactiver la sous-clé et mettre à jour le serveur de clés, utilisez l'option Révoquer (décrite ci-dessus). Après transfert d'une sous-clé vers le serveur de clés, vous ne pouvez pas la supprimer.

Fenêtre Autorité de révocation désignée

Pour accéder au panneau **Autorité de révocation** d'une clé donnée, sélectionnez cette clé, puis choisissez **Propriétés** dans le menu **Clés**. La boîte de dialogue **Propriétés des clés** apparaît, comme illustré à la Figure 6-2 à la page 99. Cliquez sur l'onglet **Autorités de révocation**. Le panneau **Autorités de révocation** apparaît, comme illustré à la Figure 6-4.

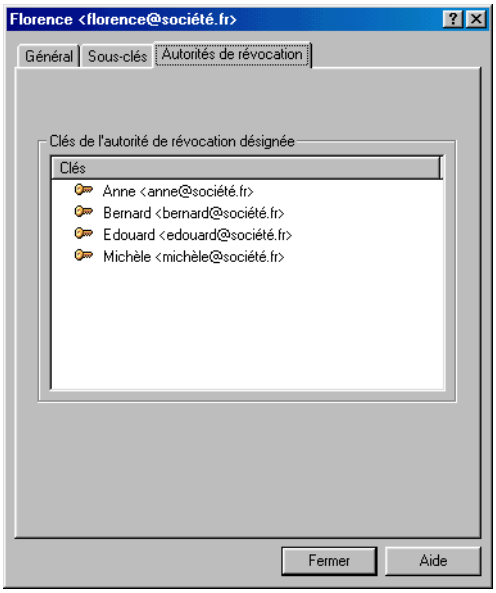


Figure 6-4. Boîte de dialogue Propriétés des clés (panneau Autorités de révocation)

Le panneau Autorités de révocation répertorie toutes les clés autorisées à révoquer votre clé PGP. Pour plus d'informations sur l'ajout d'une autorité de révocation à votre clé, reportez-vous à la section « Ajout d'une autorité de révocation désignée » à la page 37.

Spécification d'une paire de clés par défaut

Lorsque vous cryptez des messages ou des fichiers, PGP vous donne la possibilité de procéder également à un cryptage vers une paire de clés spécifiée comme votre paire de clés par défaut. Lorsque vous signez un message ou la paire de clés d'un autre utilisateur, PGP utilise cette paire de clés par défaut. Cette dernière apparaît en gras pour que vous puissiez la distinguer des autres. Si une seule paire de clés figure dans votre trousseau, celle-ci est désignée automatiquement comme votre paire de clés par défaut. Si vous possédez plusieurs paires de clés, vous souhaitez peut-être définir l'une d'elles comme celle étant par défaut.

Pour spécifier votre paire de clés par défaut

1. Ouvrez PGPkeys.
2. Mettez en surbrillance la paire de clés à désigner comme celle par défaut.
3. Choisissez **Définir** par défaut dans le menu **Clés**.

   La paire de clés sélectionnée apparaît en gras, indiquant qu'il s'agit maintenant de votre paire par défaut.

Vérification de la clé publique d'un autre utilisateur

Auparavant, à moins qu'une personne ne vous remette une clé en main propre sur une disquette, il était difficile d'être absolument certain de l'appartenance d'une clé. Ce mode d'échange de clés n'est généralement pas pratique, en particulier pour des utilisateurs travaillant sur des sites éloignés.

Vous pouvez procéder de différentes manières pour vérifier l'empreinte digitale d'une clé, mais la plus sûre consiste à appeler la personne par téléphone et de lui demander de lire son empreinte digitale. A moins que cette personne ne soit la cible d'une attaque, il est quasiment improbable qu'une autre personne intercepte cet appel et imite celle avec laquelle vous pensez être en ligne. Vous pouvez également comparer l'empreinte digitale de votre copie de clé publique d'un utilisateur à celle de la clé d'origine placée sur un serveur de clés.

L'empreinte digitale peut être visualisée de deux manières, selon une liste de mots uniques ou selon un format hexadécimal.

Pour vérifier la clé publique d'un utilisateur avec son empreinte digitale

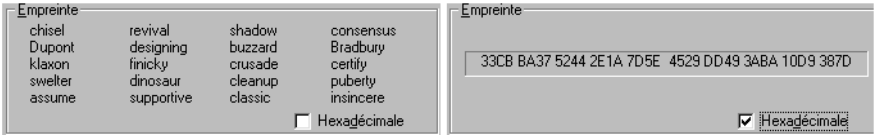
1. Ouvrez PGPkeys.
2. Mettez en surbrillance la clé publique à vérifier.
3. Choisissez **Propriétés** dans le menu **Clés**, ou cliquez sur pour ouvrir la boîte de dialogue **Propriétés**.

   La boîte de dialogue **Propriétés** apparaît, comme illustré à la Figure 6-5.

Figure 6-5. Boîte de dialogue Propriétés de PGP

4. Comparez la série de mots ou de caractères affichée dans la zone de texte **Empreinte digitale** avec l'empreinte d'origine.

   Par défaut, une liste de mots apparaît dans cette zone (exemple illustré à la figure Figure 6-6). Toutefois, pour afficher l'empreinte digitale sous forme de 20 caractères hexadécimaux, vous pouvez cocher la case **Hexadécimale** (exemple illustré à la Figure 6-6).



Affichage de la liste de mots Affichage hexadécimal

Figure 6-6. Zone de texte Empreinte digitale

La liste de mots de la zone de texte de l'empreinte digitale est constituée de mots spéciaux servant à l'authentification. Ces mots sont utilisés par PGP et sélectionnés soigneusement de façon à être phonétiquement distincts et facilement compréhensibles.

La finalité de la liste de mots est identique à celle de l'alphabet militaire : elle permet l'acheminement distinct des informations via un canal radio parasité. Pour plus d'informations sur la technique de hachage et l'affichage de la liste de mots, reportez-vous à la section Annexe D, « Listes de mots biométriques ».

Signature de la clé publique d'un autre utilisateur

Lorsque vous créez une paire de clés, votre clé publique signe automatiquement ces clés. De la même manière, une fois que vous êtes certain qu'une clé appartient bien à un individu, vous pouvez signer sa clé publique, ce qui indique que vous êtes sûr qu'il s'agit d'une clé valide. Ce faisant, une icône associée à votre nom d'utilisateur apparaît pour cette clé.

Pour signer la clé publique d'un utilisateur

1. Ouvrez la fenêtre PGPkeys.
2. Mettez en surbrillance la clé publique à signer.
3. Choisissez **Signer** dans le menu **Clés**, ou cliquez sur  pour ouvrir la boîte de dialogue de **signature de clés**.

   La boîte de dialogue de **signature de clés** apparaît (Figure 6-7) et affiche la clé publique et l'empreinte digitale dans la zone de texte.

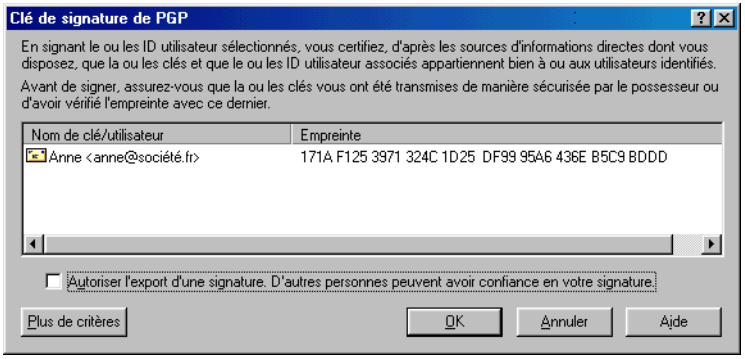


Figure 6-7. Boîte de dialogue de signature de clés PGP (Moins de critères)

4. Pour permettre l'exportation simultanée de votre signature et de cette clé, cochez la case **Autoriser l'export d'une signature**.

   Une signature exportable peut être envoyée à des serveurs et n'est jamais dissociée de la clé lors de l'exportation, par exemple, par elle peut être jointe à un message électronique. Cette option permet d'indiquer rapidement que vous souhaitez exporter votre signature.

   Ou

   Pour configurer certaines options, telles que le type et la date d'expiration de la signature, cliquez sur **Plus de critères** (Figure 6-8).

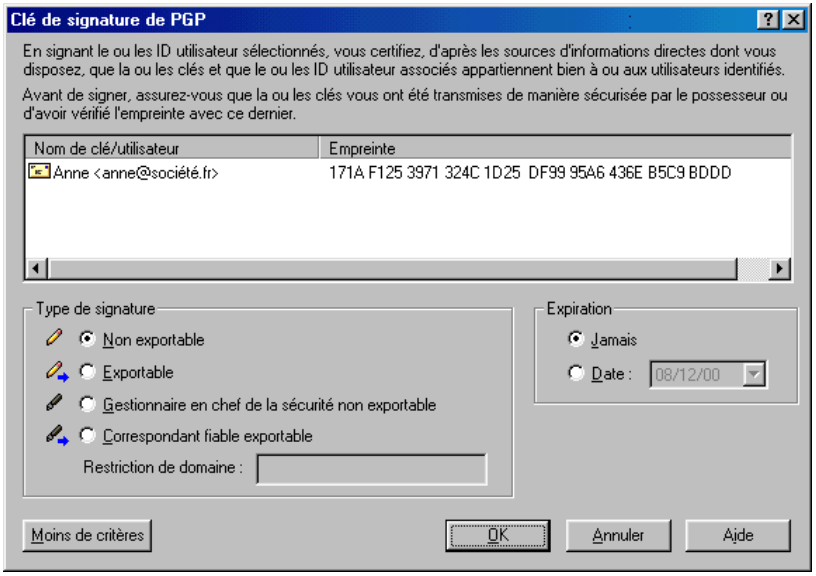


Figure 6-8. Boîte de dialogue de signatures de clés PGP (Plus de critères)

Choisissez un type de signature de la clé publique. Sélectionnez l'une des options suivantes :

- **Non exportable.** Utilisez cette signature lorsque vous pensez que la clé est valide, mais que vous ne souhaitez pas que d'autres utilisateurs se fient à votre avis. Vous ne pouvez pas transférer ce type de signature à un serveur de clés ou l'exporter de quelque façon que ce soit.

- **Exportable.** Recourez à cette option lorsque votre signature est envoyée avec la clé au serveur, de sorte que d'autres utilisateurs peuvent se fier à votre signature et à vos clés. Cela revient à cocher la case **Autoriser l'export d'une signature** dans la fenêtre de **signature de clés**.
- **Gestionnaire en chef de la sécurité non exportable.** Certifie que cette clé et toutes les autres clés signées par cette même clé avec validation d'un correspondant fiable correspondent, pour vous, à des correspondants fiables. Les signatures de ce type ne sont pas exportables.
- **Correspondant fiable exportable.** Utilisez cette signature dans le cas où vous êtes certain que cette clé est valide et que vous faites entièrement confiance au détenteur des clés pour se porter garant d'autres clés. Les signatures de ce type sont exportables.
  Vous pouvez restreindre la possibilité de validation d'un correspondant fiable à un domaine de messagerie particulier.

5. Pour limiter la validation du certificat à un domaine unique, entrez son nom dans la zone Domaine.
6. Pour limiter une signature dans le temps, entrez la date d'expiration souhaitée dans la zone de texte Date. Dans le cas contraire, la signature n'expire jamais.
7. Cliquez sur **OK**.

   La boîte de dialogue **Mot de passe complexe** apparaît.
8. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

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

Attribution d'un niveau de confiance aux validations de clés

Vous pouvez non seulement certifier qu'une clé appartient bien à un utilisateur, mais également attribuer un niveau de confiance à l'utilisateur des clés. Ceci indique la confiance que vous lui accordez en tant que correspondant des autres utilisateurs dont vous pouvez recevoir les clés dans le futur. Ainsi, si vous récupérez une clé d'un utilisateur qui a été signée par un utilisateur désigné comme fiable, cette clé est considérée comme valide même si vous ne l'avez pas vérifiée vous-même.

Pour attribuer un niveau de confiance à une clé

1. Ouvrez PGPkeys.
2. Sélectionnez la clé dont le niveau de confiance est à modifier.

   REMARQUE : Avant de définir le niveau de confiance de la clé, vous devez la signer. Si vous n'avez pas encore signé cette clé, reportez-vous à la section « Validation de la clé publique » à la page 63 pour plus d'informations.

3. Choisissez **Propriétés** dans le menu **Clés**, ou cliquez sur pour ouvrir la boîte de dialogue **Propriétés**, comme illustré à la Figure 6-5.
4. Utilisez la réglette du niveau de fiabilité pour choisir le niveau de confiance approprié pour la paire de clés.

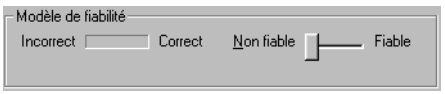


Figure 6-9. Boîte de dialogue Modèle de fiabilité

5. Pour accepter ce nouveau paramètre, fermez la boîte de dialogue.

Si vous affectez un niveau de confiance élevé à une clé accompagnée d'une photographie, PGP supprime le point d'interrogation sur cette photographie.

Désactivation et activation de clés

Il se peut que vous souhaitiez désactiver temporairement une clé. Cette fonction s'avère utile lorsque vous souhaitez conserver une clé publique en vue d'une utilisation future, mais que vous ne souhaitez pas encombrer la liste de vos destinataires à chaque envoi d'un message électronique.

Pour désactiver une clé

1. Ouvrez PGPkeys.
2. Sélectionnez la clé à désactiver.
3. Choisissez **Désactiver** dans le menu **Clés**.

   La clé est alors grisée et non disponible temporairement.

Pour activer une clé

1. Ouvrez PGPkeys.
2. Sélectionnez la clé à activer.
3. Choisissez **Activer** dans le menu **Clés**.

   La clé est à nouveau disponible et peut être utilisée comme précédemment.

Importation et exportation de clés

Bien que vous puissiez distribuer fréquemment votre clé publique et les clés publiques d'autres utilisateurs en copiant et collant la ligne de texte à partir d'un serveur de clés publiques ou d'entreprise, vous pouvez également échanger des clés en les important et les exportant en tant que fichiers de texte distincts. Par exemple, une personne peut vous fournir une disquette contenant sa clé publique ou vous souhaitez peut-être mettre votre clé publique à disposition sur un serveur FTP.

Pour importer une clé à partir d'un fichier

1. Ouvrez PGPkeys.
2. Choisissez **Importer** dans le menu **Clés**.

   La boîte de dialogue d'**importation** apparaît.
3. Sélectionnez le fichier contenant la clé à importer, puis cliquez sur **Ouvrir**.

   Une boîte de dialogue de **sélection** apparaît.
4. Sélectionnez la ou les clé(s) à importer dans votre trousseau, puis cliquez sur **Importer**.
5. Les clés importées apparaissent dans PGPkeys. Utilisez cette application pour crypter ou vérifier la signature numérique d'un utilisateur.

Ajout d'une clé provenant d'un message électronique

Si un collègue vous envoie un message électronique accompagné de sa clé (sous forme d'un bloc de texte), vous pouvez l'ajouter à votre trousseau de clés.

1. Lorsque la fenêtre de votre message électronique est ouverte, lancez PGPkeys.
2. Superposez les deux fenêtres, de façon à voir une partie de la fenêtre PGPkeys derrière celle du message électronique.
3. Sélectionnez le texte de la clé,comprenant le texte `BEGIN PGP PUBLIC KEY BLOCK` et le texte `END PGP PUBLIC KEY BLOCK`, puis faites-le glisser dans la fenêtre PGPkeys.

   La boîte de dialogue de **sélection** apparaît.
4. Sélectionnez la ou les clé(s) à importer dans votre trousseau, puis cliquez sur **Importer**.
5. PGPkeys affiche la ou les clé(s) importée(s). Utilisez cette application pour crypter ou vérifier la signature numérique d'un utilisateur.

Exportation d'une clé vers un fichier

1. Ouvrez la fenêtre PGPkeys.
2. Sélectionnez la clé à exporter vers un fichier.
3. Choisissez **Exporter** dans le menu **Clés**.

   La boîte de dialogue d'**exportation** apparaît.
4. Entrez le nom du fichier de clé à exporter ou recherchez-le, puis cliquez sur **Enregistrer**.

   La clé est alors enregistrée avec le nom de fichier et à l'emplacement spécifiés.

Vous pouvez également récupérer vos clés privées PKCS-12 X.509 en les exportant à partir de votre navigateur, puis en les déposant dans PGPkeys, ou en choisissant **Importer** dans le menu **Clés**.

Révocation d'une clé

S'il arrive que vous ne puissiez plus vous fier à votre paire de clés personnelle, vous pouvez émettre publiquement une révocation, indiquant que vous n'utilisez plus cette clé. La meilleure méthode de mise en circulation d'une clé révoquée consiste à placer cette clé sur un serveur de clés publiques.

Pour révoquer une clé

1. Ouvrez PGPkeys.
2. Sélectionnez la paire de clés à révoquer.
3. Choisissez **Révoquer** dans le menu **Clés**.

   La boîte de dialogue de **confirmation de révocation** apparaît.
4. Cliquez sur **OK** pour confirmer votre intention de révoquer la clé sélectionnée.

   La boîte de dialogue **PGP – Saisie d'un mot de passe complexe** apparaît.
5. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

   Au moment de sa révocation, la clé apparaît barrée en rouge, ce qui indique qu'elle n'est plus valide.
6. Envoyez la clé révoquée au serveur, afin que tout le monde sache qu'il ne faut plus utiliser votre ancienne clé.

Désignation d'une autorité de révocation

Vous pouvez un jour oublier votre mot de passe complexe ou perdre votre clé privée. Dans ce cas, vous ne pourrez plus jamais utiliser votre clé et vous n'aurez aucune possibilité de révoquer votre ancienne clé lors de la création d'une nouvelle. Pour vous protéger contre cette éventualité, vous pouvez désigner une autorité de révocation de clés tierce sur votre trousseau de clés publiques, afin de révoquer votre clé. Cette partie tierce sera en mesure de révoquer votre clé, de l'envoyer au serveur, comme si vous le faisiez personnellement.

Pour désigner une autorité de révocation

1. Ouvrez PGPkeys.
2. Sélectionnez la paire de clés pour laquelle vous souhaitez désigner une autorité de révocation.
3. Choisissez **Ajouter** une autorité de révocation dans le menu **Clés**.

   Une boîte de dialogue apparaît et affiche une liste de clés.
4. Sélectionnez la ou les clé(s) dans la liste ID utilisateur devant être désignée(s) comme autorité de révocation.
5. Cliquez sur **OK**.

   Une boîte de dialogue de confirmation apparaît.
6. Pour continuer, cliquez sur **OK**.

   La boîte de dialogue **Mot de passe complexe** apparaît.
7. Entrez votre mot de passe, puis cliquez sur **OK**.
8. La ou les clé(s) sélectionnée(s) est / sont maintenant autorisée(s) à révoquer votre clé. Pour gérer les clés de manière efficace, distribuez une copie actuelle de votre clé à ou aux autorité(s) de révocation ou téléchargez votre clé vers le serveur. Pour plus d'informations, reportez-vous à la section « Distribution d'une clé publique » à la page 52.

Définition des options de PGP

PGP est configuré de sorte à répondre aux besoins de la plupart des utilisateurs, mais vous avez la possibilité de régler certains paramètres pour répondre à vos besoins informatiques spécifiques. Définissez ces paramètres dans la boîte de dialogue **Options**, à laquelle vous pouvez accéder via la commande **Options** du menu **Edition**.

Définition des options générales

Dans le panneau Général, spécifiez vos préférences de cryptage, de signature et d'effacement de fichiers.

Pour définir les options générales de PGP

1. Ouvrez PGPkeys.
2. Choisissez **Options** dans le menu **Edition**.

   La fenêtre **Options** apparaît et affiche le panneau **Général** (Figure 6-10).

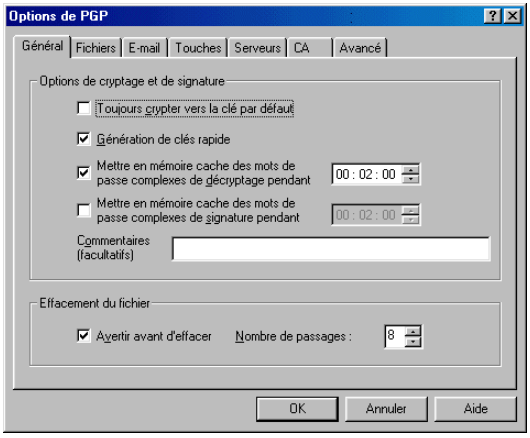


Figure 6-10. Boîte de dialogue Options de PGP (panneau Général)

3. Sélectionnez les paramètres de cryptage généraux dans le panneau **Général**. Sélectionnez l'une des options suivantes :

   - **Toujours crypter vers la clé par défaut.** Lorsque cette case est cochée, tous les messages électroniques et les pièces jointes cryptés à l'aide de la clé publique d'un destinataire sont également chiffrés pour vous à l'aide de votre clé publique par défaut. Il est conseillé de laisser cette option activée car vous avez ainsi la possibilité de décrypter le contenu de tout message électronique ou toute pièce jointe précédemment crypté.
   - **Génération de clés rapide.** Lorsque cette case est cochée, la génération d'une nouvelle paire de clés Diffie-Hellman / DSS est accélérée. L'utilisation d'un ensemble préalablement calculé de nombres premiers accélère ce processus (en comparaison au long processus de création initiale à chaque nouvelle génération de clé). Toutefois, gardez à l'esprit que l'option de génération de clés accélérée est applicable uniquement pour des tailles de clé fixes comprises entre 1 024 et 4 096 bits (en option lors de la création de clés). Cette option

n'est pas disponible lorsque vous entrez d'autres valeurs. Bien qu'il soit peu probable qu'une personne puisse casser votre clé grâce à ses connaissances en matière de nombres premiers, il se peut que vous préfériez tirer partie de cette économie de temps pour créer une paire de clés présentant un niveau de sécurité maximal.

Les spécialistes de la cryptographie mettent en avant l'hypothèse selon laquelle l'utilisation des nombres premiers prédéfinis ne diminue pas la sécurité des algorithmes Diffie-Hellman / DSS. Si vous pensez ne pas pouvoir maîtriser cette fonction, vous pouvez la désactiver.

- **Mettre en mémoire cache des mots de passe complexes de décryptage pour…**Lorsque cette case est cochée, votre mot de passe complexe de décryptage est stocké automatiquement dans la mémoire de votre ordinateur. Cette option indique également la fréquence (en heures : minutes : secondes) d'enregistrement de votre mot de passe complexe. Le paramètre par défaut est de 2 minutes.
- **Mettre en mémoire cache des mots de passe complexes de signature pour…**Lorsque cette case est cochée, votre mot de passe complexe de signature est stocké automatiquement dans la mémoire de votre ordinateur. Cette option indique également la fréquence (en heures : minutes : secondes) d'enregistrement de votre mot de passe complexe de signature. Le paramètre par défaut est de 2 minutes.
- **Zone de commentaires.** Vous pouvez ajouter vos commentaires dans cette zone. Le texte entré est toujours joint aux messages et fichiers que vous cryptez ou signez. Les commentaires entrés dans ce champ apparaissent sous l'en-tête de texte --BEGIN PGP MESSAGE BLOCK -- et le numéro de la version de chaque message.
- **Avertir avant d'effacer.** Lorsque cette case est cochée, une boîte de dialogue apparaît avant l'effacement d'un fichier, ce qui vous donne la possibilité de changer d'avis avant que PGP n'écrase le contenu du fichier de façon sécurisée et ne le supprime de votre ordinateur.
- **Nombre de passages**. Cette option contrôle le nombre d'opérations effectuées sur le disque par les utilitaires d'effacement

4. Pour enregistrer vos modifications et revenir à la fenêtre principale de PGPkeys ou sélectionner un autre onglet afin de poursuivre la configuration de vos options PGP, cliquez sur **OK**.

Définition des options de fichiers

Spécifiez l'emplacement des trousseaux de clés utilisés pour stocker vos clés publiques et privées dans le panneau **Fichiers**.

Pour définir les options de fichier de PGP

1. Ouvrez PGPkeys.
2. Choisissez **Options** dans le menu **Edition** de PGPkeys, puis cliquez sur l'onglet **Fichiers**.

   La fenêtre **Options** apparaît et affiche le panneau **Fichiers** (Figure 6-11).

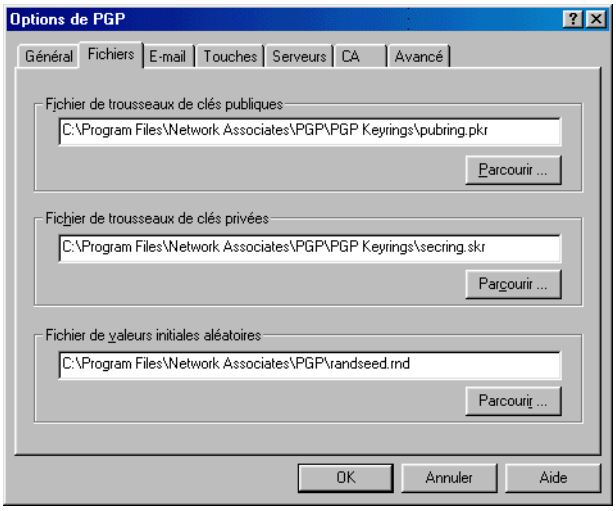


Figure 6-11. Boîte de dialogue Options de PGP (panneau Fichiers)

3. Dans le panneau **Fichiers**, utilisez les boutons pour définir l'emplacement souhaité de vos trousseaux de clés publiques et privées et/ou du fichier de valeurs initiales aléatoires :

   - **Fichier de trousseaux de clés publiques.** Affiche le nom et l'emplacement actuels supposés de votre fichier de trousseaux de clés publiques. Si vous souhaitez stocker vos clés publiques dans un fichier portant un nom différent ou à un autre emplacement, spécifiez ces informations à cet endroit. L'emplacement indiqué permet également de stocker toutes les copies de sauvegarde automatiques du trousseau de clés publiques.

   - **Fichier de trousseaux de clés privées.** Affiche le nom et l'emplacement actuels supposés de votre fichier de trousseaux de clés privées. Si vous souhaitez stocker vos clés privées dans un fichier portant un nom différent ou à un autre emplacement, spécifiez ces informations à cet endroit. Certains utilisateurs préfèrent conserver leur trousseau de clés privées sur une disquette, qu'ils insèrent comme une clé, chaque fois que la signature ou le décryptage d'un message électronique s'avère nécessaire. L'emplacement indiqué permet également de stocker toutes les copies de sauvegarde automatiques du trousseau de clés publiques.

   - **Fichier de valeurs initiales aléatoires.** Affiche l'emplacement du fichier de valeurs initiales aléatoires. Certains utilisateurs préfèrent conserver ce fichier à un emplacement sûr, afin d'éviter toute falsification. Cette méthode d'attaque étant très difficile et ayant été anticipée par PGP, le déplacement de ce fichier de son emplacement par défaut n'est pas indispensable.

4. Pour enregistrer vos modifications et revenir à la fenêtre principale de PGPkeys ou sélectionner un autre onglet afin de poursuivre la configuration de vos options PGP, cliquez sur **OK**.

Définition des options de messagerie

Dans le panneau **Email**, spécifiez les options affectant le mode d'implémentation des fonctions PGP dans votre application de messagerie. Gardez à l'esprit que ces sélections ne s'appliquent pas toutes à votre application de messagerie.

Pour définir les options de messagerie

1. Ouvrez PGPkeys.
2. Choisissez **Options** dans le menu **Edition** de PGPkeys, puis cliquez sur l'onglet **E-mail**.

   La fenêtre **E-mail** apparaît et affiche le panneau **Général** (Figure 6-12).

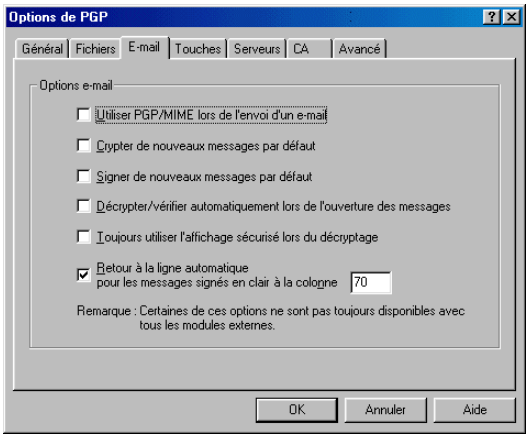


Figure 6-12. Boîte de dialogue Options de PGP (panneau E-mail)

3. Dans le panneau **E-mail**, sélectionnez vos options de cryptage de messagerie. Sélectionnez l'une des options suivantes :

- **Utiliser PGP/MIME lors de l'envoi d'un e-mail.** Si vous utilisez Eudora et que cette case est cochée, tous vos messages électroniques et pièces jointes envoyés au destinataire souhaité sont automatiquement cryptés. Cette option n'affecte pas les autres cryptages effectués à partir du Presse-papiers ou via l'Explorateur Windows. Cette option est déconseillée si vous souhaitez envoyer des messages électroniques à des destinataires utilisant des applications de messagerie ne gérant pas le standard PGP / MIME. Si vous utilisez Eudora, les pièces jointes seront toujours cryptées indépendamment de ce paramètre. Toutefois, si le destinataire n'utilise pas le standard PGP / MIME, le processus de cryptage ne sera pas autant automatisé.

- **Crypter de nouveaux messages par défaut.** Si vous cochez cette case, tous vos messages électroniques et fichiers joints sont automatiquement cryptés. Certaines applications de messagerie ne prennent pas ne charge cette fonction.

- **Signer de nouveaux messages par défaut.** Si vous cochez cette case, tous vos messages électroniques et fichiers joints sont automatiquement signés. Certaines applications de messagerie ne prennent pas en charge cette fonction. Ce paramètre n'a aucune incidence sur les autres signatures effectuées à partir du Presse-papiers ou de l'Explorateur Windows.

- **Décrypter/vérifier automatiquement lors de l'ouverture des messages.** Si vous cochez cette case, tous vos messages électroniques et fichiers joints sont automatiquement décryptés, puis vérifiés. Certaines applications de messagerie ne prennent pas en charge cette fonction.

- **Toujours utiliser l'affichage sécurisé lors du décryptage.** Si vous cochez cette case, tous vos messages électroniques décryptés apparaissent dans la fenêtre Affichage sécurisé avec une police de caractères de prévention contre les attaques TEMPEST. Pour plus d'informations sur les attaques TEMPEST, reportez-vous à la section « Vulnérabilités » à la page 246.

- **Retour à la ligne automatique pour les messages signés en clair à la colonne [ ].** Cette option indique le numéro de colonne, dans votre signature numérique, après lequel un retour chariot manuel doit être utilisé pour passer à la ligne suivante. Cette fonction est nécessaire, car toutes les applications ne gèrent pas les retours à la ligne automatiques de la même manière. Vos messages signés numériquement pourraient alors être décomposés de telle manière que leur lecture deviendrait difficile. Le paramètre par défaut est égal à 70, ce qui permet d'éviter tout problème avec la plupart des applications.

> **AVERTISSEMENT :** Si vous modifiez le paramètre de retour à la ligne dans PGP, assurez-vous que celui de votre application de messagerie est moins puissant. Si vous le définissez comme identique ou plus puissant, des retours à la ligne peuvent être insérés et altérer votre signature PGP.

4. Pour enregistrer vos modifications et revenir à la fenêtre principale de PGPkeys ou sélectionner un autre onglet afin de poursuivre la configuration de vos options PGP, cliquez sur **OK**.

Définition des préférences de touches d'activation

Dans le panneau **Touches**, spécifiez les touches de raccourci des fonctions de PGP.

Pour définir les préférences de touches d'activation

1. Ouvrez PGPkeys.
2. Choisissez **Options** dans le menu Edition de PGPkeys, puis cliquez sur l'onglet **Touches**.

   La fenêtre **Touches** apparaît et affiche le panneau **Général** (Figure 6-13).

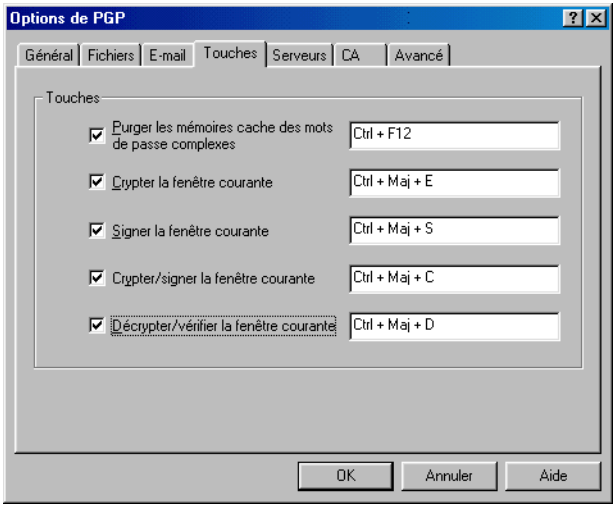


Figure 6-13. Boîte de dialogue Options de PGP (panneau Touches)

3. Dans le panneau **Touches**, sélectionnez la touche de raccourci à utiliser. Sélectionnez l'une des options suivantes :

   - **Purger les mémoires cache des mots de passe complexes.** Cochez cette case pour créer un raccourci vous permettant de supprimer la mémoire cache contenant votre mot de passe complexe de décryptage PGP via une touche ou une séquence de touches. Le raccourci à utiliser par défaut pour cette fonction est CTRL +F12.

   - **Crypter la fenêtre courante.** Cochez cette case pour créer un raccourci vous permettant de crypter toutes les données de la fenêtre courante via une touche ou une séquence de touches. Le raccourci à utiliser par défaut pour cette fonction est CTRL + MAJ + E.

   - **Signer la fenêtre courante.** Cochez cette case pour créer un raccourci vous permettant de signer toutes les données de la fenêtre courante via une touche ou une séquence de touches. Le raccourci à utiliser par défaut pour cette fonction est CTRL + MAJ + S.

   - **Crypter/signer la fenêtre courante.** Cochez cette case pour créer un raccourci vous permettant de crypter et de signer toutes les données de la fenêtre courante via une touche ou une séquence de touches. Le raccourci à utiliser par défaut pour cette fonction est CTRL + MAJ + C.

   - **Décrypter/vérifier la fenêtre courante.** Cochez cette case pour créer un raccourci vous permettant de décrypter et de vérifier toutes les données de la fenêtre courante via une touche ou une séquence de touches. Le raccourci à utiliser par défaut pour cette fonction est CTRL + MAJ + D.

4. Pour poursuivre la configuration de PGP, cliquez sur **OK** ou sélectionnez un autre onglet de la fenêtre **Options**.

Définition des options de serveur

Dans le panneau **Serveur**, paramétrez les options des serveurs de clés publiques utilisés pour envoyer et récupérer des clés publiques, et via lesquels vous synchroniserez des clés.

Pour définir les options de serveur de clés

1. Ouvrez PGPkeys.
2. Choisissez **Options** dans le menu **Edition** de PGPkeys, puis cliquez sur l'onglet **Serveur**.
3. La fenêtre **Options** apparaît et affiche le panneau **Serveur** (Figure 6-14).

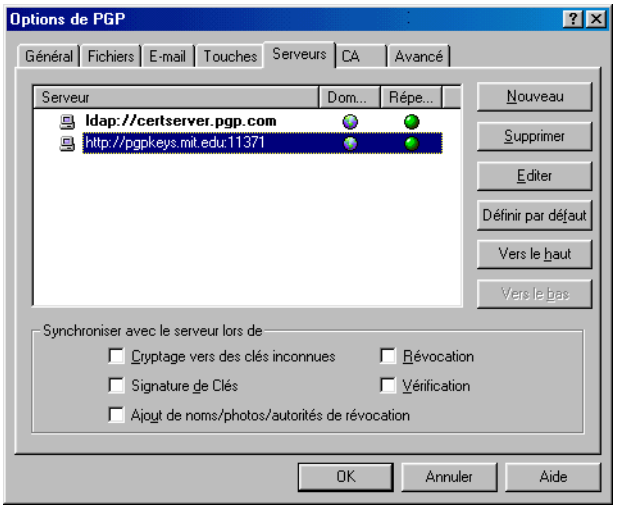


Figure 6-14. Boîte de dialogue Options de PGP (panneau Serveur)

La colonne **Domaine** répertorie le domaine Internet (tel que « entreprise.com ») du ou des serveur(s) de clés disponible(s). Lors de l'envoi de clés vers un serveur, PGP tente de rechercher le domaine de la clé dans cette liste, puis localise ainsi le serveur approprié. Si ce domaine est introuvable, un serveur à l'échelle mondiale prenant en charge toutes les clés sera utilisé, puis tous les autres domaines situés en bas de la liste seront recherchés si le premier serveur ne fonctionne pas.

4. Définissez vos options de serveur à l'aide des boutons suivants :

   - **Nouveau.** Ajoute un nouveau serveur à votre liste.
   - **Supprimer.** Supprime le serveur sélectionné de votre liste.
   - **Modifier.** Vous autorise à modifier les informations relatives au serveur sélectionné.
   - **Définir comme Par défaut.** Identifie le serveur par défaut utilisé pour effectuer des opérations internes spécifiques, telles que la mise à jour ou l'envoi de listes de groupes, la mise à jour de correspondants fiables, etc. Votre agent de sécurité prend en charge la configuration des paramètres de votre entreprise.
   - **Déplacer vers le haut** et **Déplacer vers le bas.** Ces boutons vous permettent de classer les serveurs par ordre de préférence.

5. Dans la zone **Synchroniser avec le serveur lors de**, sélectionnez les options à utiliser lors de la synchronisation de votre trousseau de clés privées avec votre ou vos serveur(s) de clés. Sélectionnez l'une des options suivantes :

   - **Cryptage vers des clés inconnues.** Cochez cette case afin que PGP recherche automatiquement des destinataires inconnus sur le serveur pour localiser les utilisateurs ne se trouvant pas dans votre trousseau de clés lors du cryptage du message électronique.
   - **Signature de clés.** Cochez cette case pour que les clés auxquelles vous avez ajouté votre signature soient d'abord mises à jour sur le serveur, puis que vos modifications soient transférées au serveur.
   - **Ajout de noms/photos/autorités de révocation.** Cochez cette case pour que les clés auxquelles vous avez ajouté des noms, des photographies ou des autorités de révocation soient d'abord mises à jour par le serveur et que vos modifications soient ensuite transférées au serveur. La mise à jour anticipée de la clé garantit, par exemple, que celle-ci n'a pas été révoquée depuis sa dernière mise à jour.
   - **Révocations.** Cochez cette case afin que les clés révoquées soient d'abord mises à jour sur le serveur, puis que vos modifications soient transférées au serveur.
   - **Vérification.** Cochez cette case pour que PGP recherche automatiquement la clé appropriée dans le serveur de clés, puis procède à son importation, lors de la vérification d'un message électronique ou d'un fichier signé pour lequel vous ne disposez pas de la clé publique de l'expéditeur.

6. Pour enregistrer vos modifications et revenir à la fenêtre principale de PGPkeys ou sélectionner un autre onglet afin de poursuivre la configuration de vos options de PGP, cliquez sur **OK**.

Ajout d'un serveur de clés à la liste des serveurs

1. Ouvrez la fenêtre **Options** de PGP, puis cliquez sur l'onglet **Serveurs**.
2. Cliquez ensuite sur **Nouveau**.

   La boîte de dialogue **Ajout d'un nouveau serveur** apparaît, comme illustré à la Figure 6-15.

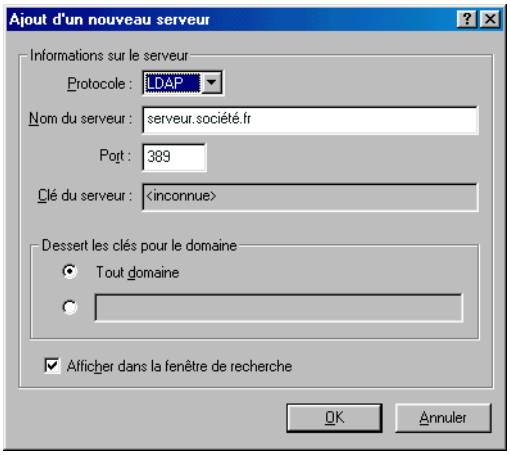


Figure 6-15. Boîte de dialogue Ajout d'un nouveau serveur

3. Dans la zone **Protocole**, sélectionnez le protocole à utiliser pour accéder au serveur. Les options disponibles sont : **LDAP**, **LDAPS** et **HTTP**.
4. Dans la zone **Nom du serveur**, entrez le nom du domaine ou l'adresse IP du serveur. Par exemple, serveur.entreprise.com ou 123.44.55.67
5. Saisissez le numéro de port du serveur dans la zone **Port**. Par exemple, 11371 est réservé aux modèles anciens de serveurs de certificats HTTP ; 389 est généralement utilisé pour les serveurs de certificats LDAP.
6. La zone **Clé du serveur** est destinée aux serveurs LDAPS. Cette option permet au serveur d'authentifier la connexion. Aucune information n'apparaît tant que vous n'êtes pas connecté.

7. Sélectionnez l'option **Tout domaine** pour permettre à PGP d'envoyer des clés à partir d'un domaine quelconque de ce serveur de clés. Cette option est activée par défaut.

   Pour que PGP envoie uniquement les clés d'un domaine spécifique vers ce serveur de clés, sélectionnez l'option apparaissant en-dessous de **Tout domaine**. Entrez ensuite le nom du domaine dans la zone de texte. Par exemple, si vous entrez le domaine « entreprise.com », seules les clés dont l'adresses e-mail se termine par @entreprise.com seront transférées vers ce serveur.

8. Pour que ce serveur de clés soit répertorié dans la fenêtre **Rechercher** de PGPkeys, cochez la case **Afficher dans la fenêtre de recherche**.

Définition des options de CA

Dans le panneau **CA**, ajoutez votre certificat X.509 à votre clé PGP. Toutefois, avant d'ajouter ce certificat, vous devez d'abord obtenir le certificat CA par défaut du serveur de certificats de votre entreprise. Pour plus d'informations sur le serveur de certificats CA par défaut, reportez-vous à la section « Après avoir obtenu le certificat de la CA par défaut, ajoutez-le à votre trousseau de clés PGP. » à la page 38. Pour plus d'informations sur la définition des options CA et l'ajout de votre certificat X.509 à votre clé, reportez-vous à la section « Ajout d'un certificat X.509 à une clé PGP » à la page 38.

Définition des options avancées

Dans le panneau **Avancé**, sélectionnez les algorithmes de cryptage de clé, ainsi que les options relatives à la fiabilité des clés.

PGP vous donne la possibilité de sélectionner et / ou de modifier ces algorithmes. Pour vos clés PGP, vous avez le choix entre divers algorithmes de cryptage : CAST (par défaut), IDEA ou DES triple. Si vous souhaitez utiliser les algorithmes IDEA ou DES triple, vous devez les sélectionner avant de générer vos clés. CAST est un nouvel algorithme pour lequel PGP et d'autres cryptographes ont accordé toute leur confiance. DES triple est utilisé par le gouvernement américain et, jusqu'à présent, n'a pas été cassé. IDEA est réservé aux clés RSA générées par PGP. Pour plus d'informations sur ces algorithmes, reportez-vous à la section « Les algorithmes symétriques de PGP » à la page 230.

L'option **Algorithme préféré** affecte les procédures suivantes :

- Lors d'un cryptage conventionnel, le mode de chiffrement privilégié est utilisé.
- Lors de la création d'une clé, le chiffrement préféré est enregistré comme partie de la clé de sorte que les utilisateurs ont recours à cet algorithme lors du cryptage de données qui vous sont destinées.

L'option **Algorithmes autorisés** affecte les procédures suivantes :

- Lors de la création d'une clé, les chiffrements autorisés sont enregistrés comme partie de la clé, de sorte que d'autres utilisateurs ont recours à ces algorithmes lors du cryptage de données qui vous sont destinées, si l'algorithme préféré n'est pas accessible.

REMARQUE : Le cryptage vers une clé publique échoue si l'utilisateur cryptant le message ne peut accéder à aucun de ces deux types de cryptages.

AVERTISSEMENT : Cochez les cases CAST, IDEA et DES triple si vous apprenez soudainement qu'un algorithme particulier n'est pas sécurisé. Par exemple, si vous apprenez que DES triple a été cassé, vous pouvez désélectionner cette case. Ainsi, toutes les nouvelles clés générées disposeront d'un enregistrement qui ne sera pas utilisé par DES triple lors du cryptage de données qui vous sont destinées.

PGP vous donne la possibilité de sélectionner et/ou modifier le mode d'affichage de la confiance accordée à la clé, mais également de décider si vous souhaitez être averti lorsque vous chiffrez un message vers une clé publique qui possède une clé de décryptage supplémentaire. Dans la section Modèle de fiabilité, choisissez l'une des options suivantes :

- **Afficher le niveau de validité marginal.** Cochez cette case si vous souhaitez connaître le degré de marginalité des clés ou supprimez la coche si seule la validité vous intéresse. La validité marginale est représentée par des barres disposant de modèles de grisage différents. La validité est symbolisée par des ronds, vert si la clé est considérée comme valide ou gris si elle est non valide (selon qu'elle a été signée par un correspondant fiable ou par vous-même).
- **Traiter les clés correctes marginalement comme incorrectes.** Cochez cette case pour considérer toutes les clés dont la validité est considérée comme marginale en tant que clés non valides. L'activation de cette option entraîne l'affichage de la boîte de dialogue de **sélection de la clé** à chaque cryptage vers des clés valides certifiées comme marginales.

- **Avertir lors du cryptage vers des clés avec une CDS.** Cochez cette case pour afficher un avertissement chaque fois qu'une clé de cryptage dispose d'une clé de cryptage supplémentaire.
- **Format d'exportation**
  - **Compatible :** Exporte les clés selon un format compatible avec les versions antérieures de PGP.
  - **Complet :** Exporte le nouveau format de clé, ainsi que les ID photographiques et les certificats X.509.

PGPdisk 7

Ce chapitre décrit non seulement PGPdisk et ses fonctions, mais fournit également des instructions quant à son mode d'utilisation.

Présentation de PGPdisk

PGPdisk est une application de cryptage simple d'utilisation, vous permettant de réserver une zone d'espace disque pour le stockage de vos données confidentielles. Cet espace permet de créer un fichier appelé *volume* PGPdisk.

Même s'il s'agit d'un simple fichier, un volume PGPdisk fonctionne de façon quasi-identique à un disque dur, en ce sens qu'il fournit un espace de stockage pour vos fichiers et vos applications. Il peut être comparé à une disquette ou un disque dur externe. Pour utiliser les applications et les fichiers stockés sur ce volume, vous devez le *monter* ou le rendre accessible.

Lorsqu'un volume PGPdisk est *monté*, vous pouvez l'utiliser comme tout autre disque. Vous pouvez y installer des applications, y déplacer ou y enregistrer vos fichiers. Lorsqu'il est *démonté*, il est impossible à toute personne ne connaissant pas votre mot de passe complexe secret, à savoir une version plus longue d'un *mot de passe*, d'y accéder. Un volume monté est également protégé : tout fichier ou application est stocké sous un format crypté, à moins d'être en cours d'utilisation. Si votre ordinateur tombe en panne alors qu'un volume est monté, le contenu de ce volume demeure crypté.

❑ **REMARQUE :** Les produits PGP vous encouragent à utiliser une phrase complète ou une longue séquence de caractères, afin de protéger vos données confidentielles. Ces types de mots de passe complexes sont généralement plus sécurisés que les mots de passe traditionnels de 6 à 10 caractères.

Fonctions de PGPdisk

Le programme PGPdisk dispose des fonctions suivantes :

- Création de volumes sécurisés de données cryptées fonctionnant comme tout autre volume généralement utilisé pour stocker vos fichiers.
- Cryptage rapide et sécurisé de vos données sans grande incidence sur le temps d'accès à vos programmes et fichiers.
- Utilisation d'un algorithme de cryptage militaire invulnérable, connu sous le nom de CAST, et reconnu pour sa capacité à empêcher tout accès non autorisé.
- Stockage du contenu de chaque volume sécurisé dans un fichier crypté pouvant être facilement sauvegardé et échangé avec des collègues.

Pourquoi utiliser PGPdisk ?

D'autres produits offrent la possibilité de restreindre l'accès aux fichiers de disque via des attributs d'autorisation et une protection par mot de passe simple. Cependant, toute protection peut facilement passer outre ces mesures de protection. Seul le cryptage de vos données peut vous assurer que le déchiffrage du contenu de vos fichiers, même à l'aide des technologies actuelles les plus élaborées, est quasiment impossible.

Les raisons pour lesquelles vous devez utiliser PGPdisk, afin de sécuriser le contenu de vos fichiers, sont les suivantes :

- Pour la protection de la confidentialité des informations financières, médicales et personnelles. Cette protection est particulièrement importante dans le cadre de travail actuel, où les informations de votre ordinateur sont accessibles à tous lorsque vous surfez sur le net.
- Pour la création de zones de travail personnelles sur un ordinateur partagé, où chaque utilisateur possède un accès exclusif à ses propres programmes et fichiers. Chaque utilisateur peut monter ses propres volumes sur cet ordinateur partagé et s'assurer que personne ne peut accéder à ses fichiers une fois les volumes démontés.
- Pour la création de ressources accessibles uniquement aux membres désignés d'un groupe de travail spécifique. Un volume peut être monté lorsque les membres de l'équipe souhaitent travailler sur un projet spécifique et peut être démonté, puis stocké sous son format crypté lorsque ce projet est terminé.

- Pour la protection de l'accès aux informations propriétaires stockées sur un ordinateur portable. Généralement, en cas de perte (ou de vol) de votre ordinateur portable, toutes vos informations personnelles (y compris les mots de passe et l'accès aux services en ligne, les contacts personnels et professionnels, les données financières, etc.) risquent d'être utilisées à des fins criminelles et peuvent s'avérer plus coûteuses que le prix du portable.
- Pour la sécurisation du contenu de supports externes, tels que des disquettes et des cartouches de stockage. La capacité de cryptage d'un support externe fournit un niveau de sécurité supplémentaire pour le stockage et l'échange des informations confidentielles.

Lancement du programme PGPdisk

Pour lancer PGPdisk

Choisissez **Démarrer—>Programmes—>PGP—>PGPdisk**. La barre d'outils de PGPdisk illustrée à la Figure 7-1, apparaît alors.

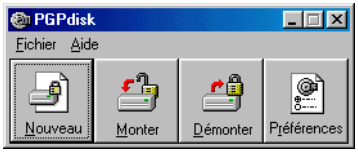


Figure 7-1. Barre d'outils de PGPdisk

Cette barre d'outils vous permet de créer et de monter des volumes en toute simplicité. Une brève explication de chaque bouton est indiquée ci-dessous :

Nouveau	Affiche l'Assistant de PGPdisk, qui vous guide tout au long de la procédure de création d'un nouveau volume PGPdisk.
Monter	Monte le volume PGPdisk spécifié si le mot de passe complexe correct est entré.
Démonter	Démonte le volume PGPdisk spécifié.
Préférences	Spécifie le mode de démontage préféré de vos volumes.

Utilisation des volumes PGPdisk

Cette section explique comment créer, monter et démonter des volumes PGPdisk et comment spécifier les préférences permettant de protéger le contenu des volumes via leur démontage (sous certaines conditions).

REMARQUE : Pour effectuer la plupart des opérations de PGPdisk, cliquez avec le bouton droit de la souris sur l'icône du fichier de volume PGPdisk.

Création d'un volume PGPdisk

Pour créer un volume PGPdisk

1. Lancez PGPdisk. La barre d'outils de PGPdisk apparaît.
2. Cliquez sur **Nouveau**. L'Assistant de PGPdisk apparaît. Lisez les informations préliminaires.
3. Cliquez sur **Suivant**.
4. Spécifiez le nom et l'emplacement du nouveau volume.
5. Cliquez sur **Enregistrer**.
6. Entrez la quantité d'espace à réserver pour le nouveau volume (champ Taille de PGPdisk). Utilisez des nombres entiers, sans décimale. Utilisez les flèches pour augmenter ou diminuer le nombre affiché dans ce champ.

   La quantité d'espace libre pour le lecteur sélectionné est indiquée au-dessus du champ Taille.
7. Pour sélectionner la taille en kilo-, méga- ou giga-octets, sélectionnez le bouton radio approprié.

   Selon la quantité d'espace disque disponible, vous pouvez créer un volume d'une taille comprise entre 100 kilo-octets et 2 giga-octets.
8. Sélectionnez la lettre du lecteur d'installation de votre volume PGPdisk (champ Lettre de lecteur de PGPdisk). Utilisez les flèches pour afficher et sélectionner une lettre de lecteur différente.
9. Cliquez sur **Suivant**.

10. Entrez la séquence de mots ou de caractères servant de mot de passe complexe (également appelé mot de passe complexe maître du volume) pour accéder au nouveau volume. Pour confirmer votre entrée, appuyez sur Tabulation pour passer à la zone suivante, puis entrez à nouveau le même mot de passe complexe. Un mot de passe complexe doit comporter 8 caractères au minimum.

    Généralement, pour renforcer le niveau de sécurité, les caractères entrés pour le mot de passe complexe n'apparaissent pas à l'écran. Toutefois, si vous êtes certain que personne ne regarde les caractères que vous entrez (soit de manière physique, soit via le réseau), cliquez dans la case **Masquer la saisie** pour afficher les caractères lorsque vous entrez votre mot de passe complexe.

    REMARQUE : Votre sécurité dépend de votre mot de passe complexe. Celui-ci doit contenir plusieurs mots, ainsi que des espaces, des nombres et d'autres caractères imprimables. En outre, il est sensible à la casse et doit comporter au moins 8 caractères. Choisissez-en un auquel vous pensez très souvent et ancré dans votre esprit. Si vous choisissez une phrase selon l'inspiration du moment, vous l'oublierez certainement totalement. Il est essentiel de *ne pas oublier votre mot de passe complexe, sinon vous perdrez vos données !* Pour plus d'informations, reportez-vous à la section « Qualité d'un mot de passe complexe » à la page 146.

    ---

11. Cliquez sur **Suivant**.

12. Déplacez votre souris aléatoirement dans la fenêtre de l'Assistant et/ou saisissez des caractères jusqu'à ce que la barre de progression soit complètement remplie.

    Les déplacements de votre souris et les caractères que vous saisissez permettent de générer des informations aléatoires utilisées par le programme PGPdisk comme dans le processus de cryptage (brouillage des données).

13. Cliquez sur **Suivant**. Une barre de progression indique la quantité d'espace du volume PGPdisk ayant été initialisée.

14. Pour monter votre volume PGPdisk, cliquez sur **Suivant**.

15. Cliquez ensuite sur **Terminer**. La fenêtre de formatage apparaît.

16. Entrez un libellé pour le nouveau volume. Celui-ci permet d'identifier le volume dans l'Explorateur Windows.

17. Cliquez sur **Démarrer**. Une boîte de dialogue d'avertissement apparaît.

18. Cliquez sur **OK**. Le nouveau disque ne contient aucune donnée. Le système vous indique que le formatage est terminé.
19. Cliquez sur **Fermer** dans la fenêtre de formatage.

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

    Une icône de volume PGPdisk monté représentant votre volume apparaît à l'emplacement spécifié.

    Une icône de volume PGPdisk crypté représentant votre volume sécurisé apparaît à l'emplacement spécifié, comme indiqué ci-dessous.

Volume PGPdisk monté

Volume PGPdisk crypté

20. Pour ouvrir le volume, cliquez deux fois sur l'icône.

Modification d'un mot de passe complexe

Vous pouvez modifier le mot de passe complexe maître ou secondaire d'un fichier PGPdisk.

Pour modifier votre mot de passe complexe

1. Assurez-vous que le volume PGPdisk n'est pas monté. Vous ne pouvez pas modifier un mot de passe complexe si le volume PGPdisk est monté.
2. Choisissez **Modifier le mot de passe complexe** dans le menu **Fichier**.

   La boîte de dialogue **Ouvrir** apparaît.
3. Recherchez ensuite le fichier souhaité.

4. La boîte de dialogue **Mot de passe complexe** apparaît, comme illustré à la Figure 7-2.

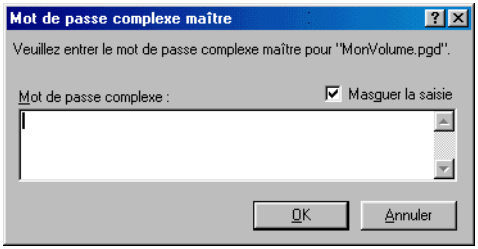


Figure 7-2. Boîte de dialogue Modifier le mot de passe complexe

5. Entrez votre mot de passe complexe, puis cliquez sur **OK**.

   La boîte de dialogue **Nouveau mot de passe complexe** apparaît, comme illustré à la Figure 7-3.

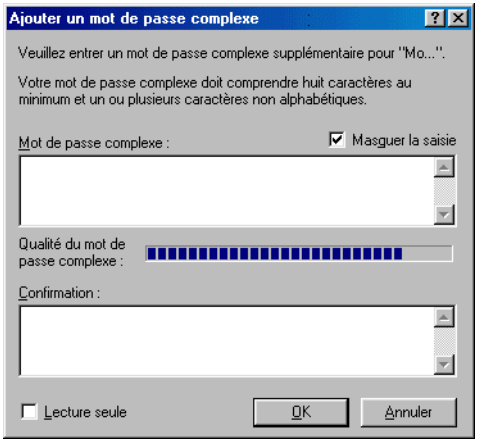


Figure 7-3. Boîte de dialogue Nouveau mot de passe complexe

6. Entrez la séquence de mots ou de caractères servant de nouveau mot de passe complexe (également appelé mot de passe complexe maître de volume) pour accéder au nouveau volume. Pour confirmer votre entrée, appuyez sur TABULATION pour passer à la zone suivante, puis entrez à nouveau le même mot de passe complexe. Un mot de passe complexe doit comporter 8 caractères au minimum.

7. Cliquez sur **OK**.

   La boîte de dialogue **Nouveau mot de passe complexe** se ferme.

Ajout de mots de passe complexes secondaires

Une fois le mot de passe complexe maître entré (celui utilisé initialement pour créer le disque), vous pouvez ajouter jusqu'à sept autres mots de passe complexes pouvant être utilisés pour le montage du volume. Vous pouvez procéder ainsi si vous utilisez régulièrement le même mot de passe complexe maître et si vous souhaitez rendre un volume accessible à une autre personne en utilisant son propre mot de passe complexe unique. Seule une personne connaissant le mot de passe complexe maître peut ajouter d'autres mots de passe complexes.

Tout utilisateur connaissant le mot de passe complexe peut le modifier. Cependant, vous pouvez toujours accéder au contenu du volume si nécessaire. Vous avez également la possibilité de définir le volume en lecture seule, ce qui permet à un utilisateur de lire les fichiers sans les altérer de quelque manière que ce soit.

Pour ajouter des mots de passe complexes secondaires

1. Assurez-vous que le volume PGPdisk n'est pas en cours de montage. Vous ne pouvez pas ajouter ou modifier de mot de passe complexe si le volume PGPdisk est monté.
2. Choisissez **Ajouter un mot de passe complexe** dans le menu **Fichier**.

   La boîte de dialogue **Mot de passe complexe** apparaît, vous demandant d'entrer le mot de passe complexe maître du volume. Si votre ordinateur comporte plusieurs volumes PGPdisk, vous devez sélectionner un volume de disque.

3. Entrez votre mot de passe complexe maître, puis cliquez sur **OK**.

   La boîte de dialogue **Nouveau mot de passe complexe** apparaît, comme illustré à la Figure 7-4.

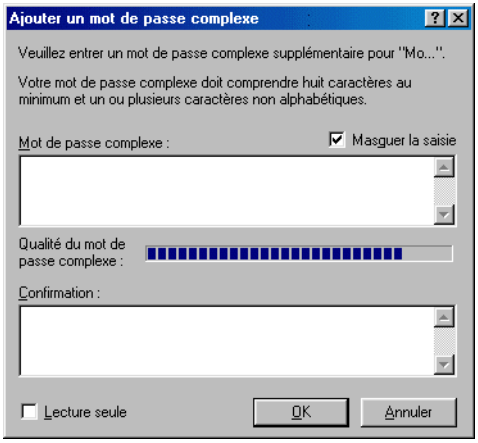


Figure 7-4. Boîte de dialogue Nouveau mot de passe complexe

4. Entrez un autre mot de passe complexe pour le volume nommé, puis appuyez sur la touche Tabulation. Entrez à nouveau le mot de passe complexe pour confirmation.

   A ce stade, vous avez également la possibilité de cocher l'option **Mot de passe en lecture seule** pour que la totalité du volume soit désignée comme étant en lecture seule.

5. Cliquez ensuite sur **OK**.

Après avoir créé un mot de passe complexe secondaire, vous, ou une autre personne le connaissant, pouvez le supprimer en choisissant **Supprimer le mot de passe complexe** dans le menu **Fichier**. Il est impossible de supprimer les mots de passe complexe maîtres. Pour plus d'informations, reportez-vous à la section « Suppression d'un mot de passe complexe ».

Suppression d'un mot de passe complexe

La procédure permettant de supprimer un mot de passe complexe est semblable à celles consistant à en ajouter ou en modifier un. Il est impossible de supprimer un mot de passe maître.

Pour supprimer un mot de passe complexe

1. Assurez-vous que le volume PGPdisk n'est pas monté. Vous ne pouvez pas supprimer un mot de passe complexe si le volume PGPdisk est monté.
2. Choisissez **Supprimer le mot de passe complexe** dans le menu **Fichier**.

   Une boîte de dialogue apparaît, vous invitant à entrer le mot de passe complexe à supprimer.
3. Entrez le mot de passe complexe, puis cliquez sur **OK**.

Suppression de l'ensemble des mots de passe complexes secondaires

Vous pouvez également supprimer tous les mots de passe secondaires d'un volume en une seule fois. Cette opération peut s'avérer utile si d'autres utilisateurs disposent de mots de passe complexes secondaires pour un volume PGPdisk et que vous ne souhaitez plus qu'ils y aient accès.

Pour supprimer l'ensemble des mots de passe complexes secondaires

1. Assurez-vous que le volume PGPdisk n'est pas monté. Vous ne pouvez pas supprimer un mot de passe complexe si ce volume est monté.
2. Tout en maintenant la touche MAJ enfoncée, choisissez **Supprimer les autres mots de passe complexes** dans le menu **Fichier**.

   Une boîte de dialogue apparaît, vous permettant de confirmer la suppression de tous les autres mots de passe complexes.
3. Cliquez sur **Oui**.

   Une boîte de dialogue vous indique que vous avez supprimé correctement tous les autres mots de passe complexes.

Ajout/Suppression de clés publiques

Vous pouvez ajouter et supprimer des clés publiques pour un fichier PGPdisk. Cette fonction vous permet, ainsi qu'à d'autres utilisateurs connaissant les mots de passe complexes de ces clés, de les utiliser pour le montage du volume.

Pour ajouter une clé publique à votre volume PGPdisk

1. Assurez-vous que le volume PGPdisk n'est pas monté. Vous ne pouvez pas ajouter de clé publique si ce volume est monté.
2. Choisissez **Ajouter/Supprimer les clés publiques** dans le menu **Fichier**.
3. Sélectionnez le volume PGPdisk dans la barre d'outils **Sélection de PGPdisk**.

   Vous devez entrer le mot de passe complexe maître.

   La fenêtre **Sélection de destinataire(s)** apparaît.
4. Faites glisser la ou les clés du volet supérieur de la fenêtre vers le volet inférieur.
5. Cliquez sur **OK**.

Pour supprimer une clé publique de votre volume PGPdisk

1. Assurez-vous que le volume PGPdisk n'est pas monté. Vous ne pouvez pas supprimer de clé publique si ce volume PGPdisk est monté.
2. Choisissez **Ajouter/Supprimer les clés publiques** dans le menu **Fichier**.
3. Sélectionnez le volume PGPdisk dans la barre d'outils **Sélection de PGPdisk**.

   Vous devez entrer le mot de passe complexe maître.

   La fenêtre **Sélection de la clé PGP** apparaît, comme illustré à la Figure 7-5.

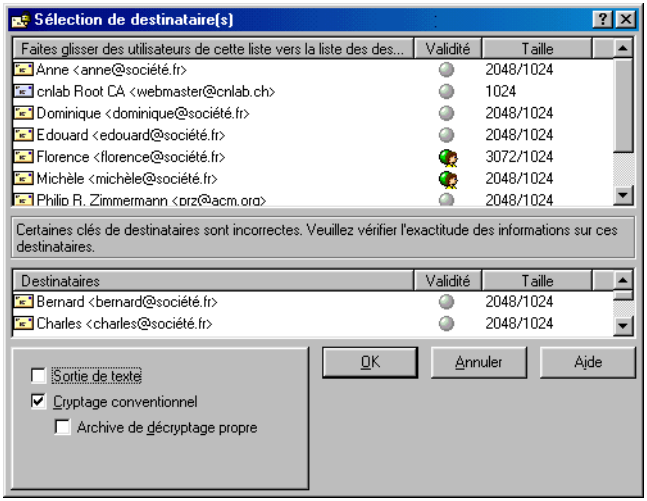


Figure 7-5. Boîte de dialogue Sélection de la clé PGP

4. Faites glisser la ou les clés du volet inférieur de la fenêtre vers le volet supérieur.

5. Cliquez ensuite sur **OK**.

Montage d'un volume PGPdisk

Lorsque vous créez un nouveau volume, PGPdisk le monte automatiquement, vous permettant ainsi de commencer à l'utiliser pour stocker vos fichiers. Pour sécuriser le contenu du volume, vous devez le démonter. Pour plus d'informations, reportez-vous à la section « Démontage d'un volume PGPdisk » à la page 140. Après le démontage d'un volume, son contenu reste sécurisé dans un fichier crypté. Pour pouvoir y accéder, il faut procéder à nouveau au montage du volume.

Vous pouvez effectuer le montage d'un volume de plusieurs manières.

- Cliquez deux fois sur l'icône du volume.
- Faites glisser l'icône du volume vers l'icône PGPdisk dans le dossier PGP 6.5.
- Faites glisser l'icône du volume vers le bouton **Monter** de la barre d'outils de PGPtools.
- Cliquez sur l'icône du volume avec le bouton droit de la souris. Choisissez **PGPdisk—>Monter PGPdisk**.
- Utilisez le bouton **Monter** de la barre d'outils de PGPtools.

Pour monter un volume à l'aide du bouton Monter

1. Lancez PGPdisk.

   La **barre d'outils de PGPdisk** apparaît.

2. Cliquez sur **Monter** ou choisissez **Monter PGPdisk** dans le menu **Fichier**.

   La boîte de dialogue **Monter PGPdisk** apparaît.

3. Sélectionnez le volume crypté à monter, puis cliquez sur **Ouvrir**. Vous devez entrer le mot de passe complexe pour le volume sélectionné.

4. Entrez le mot de passe complexe, puis cliquez sur **OK**. Si vous ne souhaitez pas modifier les fichiers stockés dans ce volume, cochez la case **Lecture seule**. Si vous avez entré le mot de passe complexe correct, le volume est monté et les données du fichier crypté sont accessibles. Le volume apparaît alors dans l'arborescence de l'Explorateur Windows.

   Vous pouvez également monter un volume sans exécuter le programme PGPdisk. Il suffit de cliquer deux fois sur le nom du fichier crypté (ou sur son icône) dans le Finder ou de le faire glisser vers l'icône du programme PGPdisk.

Utilisation d'un volume PGPdisk monté

Vous pouvez créer, copier, déplacer et supprimer des fichiers et des dossiers sur un volume PGPdisk comme pour tout autre volume. De la même manière, toute autre personne que vous ayant accès à ce volume (sur le même ordinateur ou éventuellement via le réseau) peut également accéder aux données stockées dans ce volume. Tant que le volume est démonté, il est impossible d'accéder aux données du fichier crypté associé à ce volume.

AVERTISSEMENT : Bien que le fichier crypté associé à chaque volume soit protégé contre toute intrusion, il peut être supprimé. Si une personne non autorisée peut accéder à vos données, elle peut supprimer le fichier crypté sur lequel le volume est basé. Il est conseillé de conserver une copie de sauvegarde du fichier crypté.

Démontage d'un volume PGPdisk

Pour verrouiller le contenu d'un volume donné une fois que vous y avez accédé, vous devez démonter ce volume. Il est impossible de démonter un volume si l'un de ses fichiers est ouvert.

Pour démonter un volume PGPdisk

1. Fermez tous les fichiers dans le volume PGPdisk à démonter.
2. Choisissez **Démonter PGPdisk** dans le menu **Fichier**.

   Pour démonter un volume PGPdisk, vous pouvez également procéder comme suit :

   - Dans la barre d'outils de PGPdisk, cliquez sur **Démonter**
   - Cliquez avec le bouton droit de la souris sur la lettre du lecteur dans l'Explorateur Windows

     et

   - Cliquez sur le fichier du volume

Une fois le volume démonté, son contenu est verrouillé dans le fichier crypté associé à ce volume. Le contenu du volume est stocké dans le fichier crypté et son contenu est inaccessible tant le volume reste démonté. L'affichage des volumes PGPdisk sous forme d'une fenêtre vous permettant de consulter les données du fichier crypté peut s'avérer utile. Le contenu d'un fichier de volume PGPdisk est accessible uniquement lorsqu'un utilisateur connaissant un mot de passe complexe valide monte le fichier en volume.

Spécification des préférences

Le bouton **Préférences** de la barre d'outils de PGPdisk vous permet de spécifier le mode de montage et de création de vos volumes.

Pour spécifier les préférences

1. Cliquez sur **Préférences** dans la barre d'outils de PGPdisk ou choisissez **Préférences** dans le menu **Fichier**.

   La boîte de dialogue **Préférences** apparaît.

2. Dans les onglets appropriés, cochez les cases correspondant aux options désirées.

Onglet Démonter automatiquement

- **Démonter automatiquement après [15] minutes d'inactivité.** Une fois cochée, cette option permet à PGPdisk de démonter automatiquement tous les volumes PGPdisk montés une fois que la période d'inactivité de l'ordinateur définie en minutes dans cette case est dépassée. Choisissez un nombre de minutes compris entre 1 et 999 à cette valeur.

  REMARQUE : PGPdisk ne peut pas démonter automatiquement un volume PGPdisk si l'un des fichiers de ce volume est ouvert.

- **Démonter automatiquement lors de la mise en veille.** Une fois cochée, cette option permet à PGPdisk de démonter automatiquement tous les volumes PGPdisk montés lorsque votre ordinateur est en veille. Cette mode de mise en veille n'est pas pris en charge par tous les modèles d'ordinateur.

  L'option **Empêcher la mise en veille si le montage de tout PGPdisk est impossible** assure que l'ordinateur ne se mettra pas en veille si le démontage d'un PGPdisk est impossible.

  REMARQUE : Sous Windows NT, ces deux options **(Démonter automatiquement lors de la mise en veille** et **Empêcher la mise en veille si le montage d'un PGPdisk est impossible**) sont désactivées.

Onglet Touche de démontage

- **Activer la touche de démontage.** Si vous entrez une combinaison de touches dans la zone de texte, puis cochez cette option, vous créez et activez une touche de raccourci vous permettant de démonter tous les volumes PGPdisk du système à l'aide d'une seule touche.

3. Cliquez sur **OK** une fois que vous avez spécifié vos préférences.

Les paramètres de démontage automatique sont utiles si vous devez vous éloigner de votre ordinateur pendant une période donnée. Vous devez régler leur temporisation en fonction du niveau de sécurisation de votre système contre tout accès physique non autorisé. Vous pouvez définir ces deux préférences simultanément.

Maintenance des volumes PGPdisk

Cette section décrit comment monter automatiquement des volumes PGPdisk au démarrage de votre système, et comment sauvegarder et échanger les données stockées sur ces volumes avec d'autres utilisateurs.

Montage de fichiers PGPdisk sur un serveur distant

Vous pouvez placer des volumes PGPdisk sur tout type de serveur (NT, 95, 98 ou UNIX) et autoriser toute autre personne à les monter à l'aide d'un ordinateur équipé de Windows 95 ou 98.

❑ **REMARQUE :** La première personne qui monte le volume localement dispose d'un accès en lecture / écriture à ce volume. Aucune autre personne ne peut y accéder. Si vous souhaitez que d'autres personnes accèdent aux fichiers de ce volume, vous devez le monter en mode lecture seule. *Tous* les utilisateurs du volume peuvent alors y accéder en lecture seule.

Si le volume est stocké sur un serveur fonctionnant sous Windows 95, vous pouvez également monter ce volume à distance et permettre aux utilisateurs de le partager une fois monté. Cependant, cette opération ne garantit aucunement la sécurité des fichiers stockés dans ce volume.

Montage automatique de volumes PGPdisk

Si vous le souhaitez, vous avez la possibilité de monter automatiquement des volumes PGPdisk au démarrage de votre système.

Pour monter automatiquement des volumes PGPdisk

1. Créez un raccourci pour chaque fichier PGPdisk à monter au démarrage de votre ordinateur.
2. Placez ce(s) raccourci(s) dans le dossier **Winnt—>Profils—>{nom de l'utilisateur en cours}--> Menu Démarrer —> Programmes**.

   Une fois le(s) raccourci(s) placé(s) dans ce dossier, les volumes PGPdisk sont montés chaque fois que vous démarrez votre ordinateur. Lors du montage de chaque volume PGPdisk, vous devez entrer un mot de passe complexe.

Copies de sauvegarde de volumes PGPdisk

Afin de protéger vos informations de la corruption du système ou des défaillances de disque, il se peut que vous souhaitiez effectuer une copie de sauvegarde du contenu de vos volumes PGPdisk. Même si cette procédure est possible, il est déconseillé de sauvegarder le contenu d'un volume PGPdisk monté, car ce contenu n'est pas crypté et toute personne en mesure de restaurer la sauvegarde pourra y accéder. Effectuez une copie de sauvegarde du volume PGPdisk crypté, au lieu de sauvegarder le contenu du volume PGPdisk monté.

Pour effectuer une copie de sauvegarde des volumes PGPdisk

1. Cliquez deux fois sur l'icône du volume PGPdisk. Choisissez l'option **Démonter PGPdisk**.
2. Copiez le fichier crypté démonté sur une disquette, une bande ou une cartouche amovible comme vous le feriez avec tout autre fichier. Même si certaines personnes non autorisées ont accès à votre copie de sauvegarde, elles seront incapables de déchiffrer son contenu.

Lors de la copie de sauvegarde des fichiers cryptés, gardez les éléments suivants en mémoire :

- PGPdisk est un produit destiné à des utilisateurs et des entreprises pour lesquels la sécurité constitue un enjeu majeur. La sauvegarde de fichiers cryptés sur un lecteur réseau offre aux autres utilisateurs de nombreuses opportunités de deviner un mot de passe complexe mal choisi. Il est conseillé d'effectuer des copies de sauvegarde uniquement sur des périphériques sur lesquels vous exercez un contrôle physique. Dans ce cas, un mot de passe long et invulnérable permet de minimiser les risques. Reportez-vous à la section « Qualité d'un mot de passe complexe » à la page 146.
- Si vous travaillez sur un réseau, assurez-vous que les systèmes de sauvegarde du réseau n'entraînent pas la sauvegarde de vos volumes montés. Informez-vous auprès de votre administrateur système. Dans certains cas, peu importe si des copies de sauvegarde sont effectuées à partir de fichiers cryptés, car ces informations sont sécurisées. Il est vivement déconseillé d'autoriser la sauvegarde du contenu de vos volumes montés, car cela va à l'encontre de l'objectif recherché par la conservation de ces informations cryptées.

Echange de volumes PGPdisk

Pour échanger des volumes PGPdisk avec des utilisateurs possédant leur propre programme PGPdisk, envoyez leur une copie du fichier crypté comportant les données associées au volume. Vous pouvez échanger des volumes PGPdisk en procédant comme suit :

- Sous forme de pièces jointes à vos messages électroniques
- Sur des disquettes ou des cartouches
- Via un réseau

ASTUCE : Portez une attention particulière à la méthode que vous employez pour communiquer à une tierce personne votre mot de passe complexe d'accès à un volume PGPdisk. D'une façon générale, à moins d'utiliser PGP pour protéger votre message, il est déconseillé de recourir à un système de messagerie pour échanger des mots de passe complexes. Quant aux lignes téléphoniques, elles peuvent être mises sur écoute et votre conversation peut être entendue. Plus vous prenez de précautions et plus vous serez assuré que vos informations sensibles restent confidentielles. Si votre messagerie n'est pas sécurisée, il est probablement plus sûr de communiquer le mot de passe complexe à la personne souhaitée en personne ou même par courrier postal.

Une fois que la personne concernée possède une copie du fichier crypté et souhaite accéder au contenu du volume, il lui suffit de procéder à son montage à l'aide du mot de passe complexe correct ou de sa clé privée, si sa clé publique a servi au cryptage du volume. Elle doit également disposer d'une copie du programme PGPdisk. Pour plus d'informations sur le montage d'un volume PGPdisk, reportez-vous à la section « Montage d'un volume PGPdisk » à la page 138.

Modification de la taille d'un volume PGPdisk

Vous ne pouvez plus modifier la taille d'un volume PGPdisk une fois qu'il est créé. Par contre, il vous est possible de créer un volume de taille inférieure ou supérieure, puis de copier le contenu de l'ancien volume vers le nouveau.

Pour modifier la taille d'un volume PGPdisk

1. Créez un nouveau volume PGPdisk, puis spécifiez la taille souhaitée.
2. Copiez le contenu du volume PGPdisk monté existant dans ce volume.
3. Démontez l'ancien volume PGPdisk, puis supprimez le fichier crypté associé au volume afin de libérer de l'espace disque.

Détails techniques et sécurité

Cette section aborde les questions de cryptage et de sécurité. Elle fournit également des astuces et des informations techniques sur PGPdisk.

A propos des volumes PGPdisk

Vous pouvez utiliser les volumes PGPdisk pour organiser votre travail et des fichiers portant le même nom ou conserver séparément plusieurs versions des mêmes documents et programmes.

Bien que les volumes créés avec PGPdisk fonctionnent comme tout autre volume généralement utilisé, les données sont en fait enregistrées dans un fichier crypté volumineux. C'est seulement lorsque vous montez ce fichier que son contenu se présente sous la forme d'un volume. Il est important de savoir que toutes vos données demeurent sécurisées dans le fichier crypté et sont déchiffrées uniquement lorsque vous accédez à l'un des fichiers.
Cette méthode de stockage des données pour un volume facilite la manipulation et l'échange des volumes PGPdisk avec d'autres utilisateurs. Toutefois, si le fichier est supprimé dune manière ou d'une autre, elle augmente le risque de perte intempestive des données. Il est conseillé de conserver une copie de sauvegarde de ces fichiers cryptés afin de récupérer les données en cas de problème lié à l'original. Notez également qu'il est impossible de compresser un fichier crypté, contrairement aux fichiers individuels contenus dans le volume monté. Cette compression permet ainsi de stocker davantage de données dans le volume. Vous pouvez également stocker un volume PGPdisk sécurisé dans un autre volume, puis imbriquer plusieurs volumes, afin d'assurer une sécurité supplémentaire.

Algorithme de cryptage de PGPdisk

Le cryptage emploie une formule mathématique qui brouille vos données, de sorte à les rendre inutilisables. Pour pouvoir lire ces données brouillées, vous devez leur appliquer la clé mathématique correcte. La formule de cryptage de PGPdisk utilise des données aléatoires dans le processus de cryptage. Certaines de ces données aléatoires sont le résultat du déplacement de votre souris au cours du cryptage ou proviennent directement de votre mot de passe complexe.

PGPdisk utilise un algorithme de cryptage élaboré appelé CAST, dont la rapidité et l'invulnérabilité font de lui un chiffrement par bloc performant.
Son nom est composé des initiales de ses inventeurs, à savoir Carlisle Adams et Stafford Tavares de Northern Telecom (Nortel). Nortel a présenté une demande de brevet pour CAST, mais s'est engagé à fournir CAST à quiconque sans versement de droits. CAST semble avoir été particulièrement bien conçu par des personnes jouissant d'une bonne réputation dans ce domaine. Sa conception repose sur un ensemble d'affirmations pouvant être formellement démontrées et laissant à penser qu'un nombre impressionnant de clés est nécessaire pour casser sa clé de 128 bits. Les clés proposées par CAST sont

invulnérables. De nombreux éléments tangibles tendent à démontrer l'immunité de CAST contre la cryptanalyse linéaire et différentielle, les formes de cryptanalyse les plus performantes répertoriées dans les publications disponibles dans le domaine, et qui ont été à même de casser la norme de cryptage de données (DES).

Qualité d'un mot de passe complexe

Votre sécurité dépend de votre mot de passe complexe. Cependant, se retrouver dans l'incapacité de décrypter un fichier, car on a oublié son mot de passe complexe est une expérience douloureuse.

La plupart des applications requièrent un mot de passe constitué de trois à huit lettres. Un mot de passe constitué d'un seul mot est vulnérable face à une attaque « au dictionnaire », qui consiste à utiliser un ordinateur testant tous les mots du dictionnaire jusqu'à ce que le bon mot de passe soit découvert. Pour se protéger contre ce type d'attaque, il est vivement conseillé de créer un mot constitué d'une combinaison de lettres majuscules et minuscules, de nombres, de caractères de ponctuation et d'espaces. Il en résulte un mot de passe efficace, mais difficile à mémoriser. Il est donc déconseillé d'utiliser un seul mot dans votre mot de passe complexe.

Un mot de passe complexe est moins vulnérable vis-à-vis d'une attaque « au dictionnaire ». Utilisez plusieurs mots pour le constituer, plutôt que de tenter de déjouer une attaque « au dictionnaire » en juxtaposant arbitrairement plusieurs caractères amusants, pour obtenir un mot de passe complexe difficile à mémoriser, et risquer de perdre vos informations, car vous seriez dans l'impossibilité de décrypter vos propres fichiers. Toutefois, à moins que le mot de passe complexe choisi ne corresponde à quelque chose que vous avez en mémoire depuis longtemps, sa mémorisation, caractère pour caractère, paraît très difficile. Si vous choisissez une phrase selon l'inspiration du moment, il ne fait aucun doute que vous l'oublierez totalement. Utilisez des éléments que vous avez en mémoire depuis longtemps. Il ne doit pas s'agir de quelque chose dont vous avez fait part à vos proches récemment, ni d'une citation célèbre, car les experts en piratage ne doivent pas être en mesure de le deviner facilement. S'il s'agit de quelque chose qui est ancré dans votre mémoire depuis longtemps, vous ne l'oublierez probablement pas. *Ne l'inscrivez nulle part !*

Votre mot de passe complexe fait partie des données aléatoires utilisées pour le cryptage de vos fichiers PGPdisk. La barre de qualité du mot de passe complexe doit être au moins remplie à moitié lorsque vous le saisissez, autrement, la sécurité maximale n'est pas garantie.

Vous pouvez créer un mot de passe complexe secondaire ou séparé pour chaque volume PGPdisk créé. Cette opération vous permet d'autoriser l'accès d'autres utilisateurs aux fichiers PGPdisk, volume par volume. Vous pouvez utiliser un mot de passe complexe pour les fichiers PGPdisk que vous envoyez à un collègue et empêcher ce dernier d'accéder aux autres fichiers PGPdisk.

Mesures de sécurité spéciales de PGPdisk

PGPdisk prend des précautions spéciales pour éviter les problèmes de sécurité rencontrés éventuellement dans les autres programmes. Ces précautions sont les suivantes :

Effacement du mot de passe complexe

Lorsque vous entrez un mot de passe complexe, PGPdisk l'utilise uniquement pendant une durée limitée, puis l'efface de la mémoire de l'ordinateur. PGPdisk empêche également les copies de mot de passe complexe.
Ainsi, votre mot de passe complexe reste généralement dans la mémoire une fraction de seconde uniquement. Cette fonction est très importante. Si votre mot de passe complexe était conservé dans la mémoire de l'ordinateur, une personne pourrait le rechercher en votre absence. Elle pourrait ensuite accéder à tout volume PGPdisk protégé par ce mot de passe complexe.

Protection de la mémoire virtuelle

Votre mot de passe complexe ou d'autres clés peuvent être enregistrés sur le disque lors du processus d'échange de la mémoire vers le disque effectué par le système de mémoire virtuelle. PGPdisk s'assure que les mots de passes complexes et les clés ne soient jamais écrits sur le disque. Cette fonction est importante, car quiconque pourrait analyser le fichier de mémoire virtuelle pour rechercher vos mots de passe complexes sans que vous le sachiez.

Protection contre la migration d'ions statiques dans la mémoire

Lors du montage d'un volume PGPdisk, votre mot de passe devient une clé, qui est ensuite utilisée pour crypter et décrypter les données de votre volume PGPdisk. Alors que le mot de passe complexe est immédiatement supprimé de la mémoire, la clé (qui ne permet pas d'obtenir votre mot de passe complexe) reste en mémoire lors du montage du disque. Cette clé n'est pas enregistrée dans la mémoire virtuelle ; toutefois, si une partie de la mémoire stocke des données strictement identiques durant des périodes très longues sans être désactivée ou réinitialisée, la mémoire aura tendance à conserver une charge statique, lisible par les pirates. Si votre volume reste monté pendant une très longue période de temps, il peut arriver que des traces de votre clé pouvant être détectées soient conservées dans la mémoire. Les petits revendeurs informatiques ne sont pas en mesure de vous fournir d'appareils susceptibles de vous protéger contre ce phénomène, mais les grands services gouvernementaux en possèdent sans doute quelques uns.

PGPdisk vous protège contre ce phénomène en conservant deux copies de la clé dans la mémoire RAM, une copie normale et une copie à bits inversés et inverse les deux types de copies toutes les deux ou trois secondes.

Autres considérations relatives à la sécurité

Généralement, la capacité à protéger vos données dépend des précautions prises. Aucun programme de cryptage ne peut compenser un manquement à la sécurité. Par exemple, si vous laissez votre ordinateur allumé avec des fichiers confidentiels ouverts lorsque vous quittez votre bureau, toute autre personne peut accéder à ces informations ou même obtenir la clé utilisée pour l'accès à vos données. Vous trouverez ci-dessous quelques astuces permettant d'assurer une sécurité optimale :

- Assurez-vous de démonter les volumes PGPdisk lorsque vous quittez votre ordinateur. Ainsi, leur contenu sera stocké de manière sécurisée dans le fichier crypté qui leur est associé jusqu'à ce que vous souhaitiez à nouveau y accéder.
- Utilisez un économiseur d'écran protégé par mot de passe pour éviter que toute autre personne n'accède à votre ordinateur ou ne visualise votre écran lorsque vous quittez votre bureau.
- Assurez-vous que vos volumes PGPdisk ne puissent pas être vus par d'autres ordinateurs sur le réseau. Vous pouvez contacter votre administrateur réseau pour vous en assurer. Toute personne pouvant visualiser sur le réseau les fichiers d'un volume PGPdisk monté peut y accéder.
- N'écrivez jamais vos mots de passe complexes sur un papier. Choisissez un mot de passe complexe dont vous pouvez vous souvenir. Si vous avez des problèmes pour vous en souvenir, utilisez un élément pour vous rafraîchir la mémoire, tel qu'une affiche, une chanson, un poème, une blague, *mais ne l'inscrivez nulle part*.
- Si vous utilisez PGPdisk chez vous et que vous partagez votre ordinateur avec d'autres personnes, ces dernières pourront visualiser vos fichiers PGPdisk. Si vous démontez les volumes PGPdisk après les avoir utilisés, aucune autre personne ne pourra lire leur contenu.
- Si un autre utilisateur dispose d'un accès physique à votre ordinateur, il peut supprimer vos fichiers PGPdisk, ainsi que tout autre fichier ou volume. Dans ce cas, tentez de sauvegarder vos fichiers PGPdisk ou de les conserver sur un périphérique externe sur lequel vous avez un contrôle physique exclusif.
- Soyez également attentif au fait que les copies de votre volume PGPdisk utilisent la même clé secrète que l'original. Si vous échangez une copie de votre volume avec un autre utilisateur et modifiez tous les deux votre mot de passe maître, chacun d'entre vous continue à utiliser la même clé pour crypter des données. Quoique difficile, la récupération de la clé n'est pas une tâche insurmontable.

Gestion de réseau privé virtuel PGPnet

8

Ce chapitre décrit non seulement PGPnet et ses fonctions, mais fournit également des instructions quant à son mode d'utilisation. Il présente, en outre, le concept de réseaux privés virtuels.

La technologie actuelle a considérablement modifié notre espace de travail. Tous les mémos et les rapports établis entre les différents bureaux étaient généralement placés dans une boîte à lettres et reçus quelques jours plus tard. Ils sont désormais envoyés de manière électronique et reçus en quelques secondes. Aujourd'hui, les salariés travaillant à domicile ou effectuant un voyage d'affaires peuvent passer un appel téléphonique pour transférer des données en provenance ou à destination de leur bureau local ou personnel.

Ces avancées technologiques présentent cependant deux inconvénients : la sécurité des données transmises via les lignes téléphoniques est compromise et le coût des services téléphoniques a considérablement augmenté. Les entreprises ont considéré Internet comme la solution face à l'augmentation des coûts, mais la sécurité reste une préoccupation majeure.

Heureusement, la technologie la plus récente fournit également une solution à ces problèmes. Les *réseaux privés virtuels (VPN)* permettent aux entreprises de transmettre des données de manière sécurisée via Internet, tout en renforçant la sécurité de ces données transmises et en diminuant le coût des services téléphoniques.

Qu'est-ce qu'un réseau privé virtuel (VPN) ?

Un VPN permet à une entreprise d'offrir un accès sécurisé à ses applications et données à tous ses salariés et filiales, quel que soit le pays où ils se trouvent et ce, tant qu'ils disposent d'un accès à Internet. Les VPN permettent l'établissement de connexions sécurisées entre deux ordinateurs, un ordinateur et un sous-réseau ou entre deux sous-réseaux.

Exemple. L'entreprise A, située à Boston, a des filiales en Californie, au Texas et en Floride. Chacune d'elles envoie des comptes rendus commerciaux hebdomadaires au siège social. Avant que l'entreprise A n'installe un VPN, chacune des filiales composait un numéro d'entreprise pour transmettre les comptes rendus au siège. Une fois le VPN de l'entreprise A installé, les filiales pouvaient se connecter à Internet, via leur *fournisseur de services Internet (ISP)* local, à l'intranet du siège social en passant par Internet, et pouvaient également utiliser le VPN pour la transmission des données. Un appel longue distance coûteux est désormais devenu un appel local et, avantages non

négligeables, les niveaux de sécurité et de confidentialité ont été renforcés. Les données transmises de l'expéditeur vers le destinataire sont protégées via le fournisseur de services Internet, l'Internet lui-même et via tout routeur ou passerelle. Un VPN offre aux utilisateurs la confidentialité des données, leur intégrité et l'authentification de leur origine.

Les entreprises disposant de réseaux privés virtuels peuvent également les utiliser pour rendre leurs données internes accessibles aux entreprises et correspondants fiables (par exemple, leurs fournisseurs et consultants). Ainsi, chaque partie bénéficie d'un gain de temps, des économies d'argent et d'autres ressources. Outre la possibilité offerte à tous les utilisateurs autorisés d'envoyer et de recevoir des données de manière sécurisée, un VPN utilisé conjointement avec un pare-feu protège votre intranet contre tout utilisateur non autorisé. Un *pare-feu* contrôle les ordinateurs visibles par un hôte externe sur l'intranet d'une entreprise, ainsi que les services accessibles à cet hôte. Un pare-feu contrôle également les ordinateurs visibles par un hôte sur l'intranet d'une entreprise, ainsi que les services accessibles à cet hôte.

Outre les avantages que constituent une sécurité renforcée et des coûts réduits, les VPN empêchent également les fournisseurs de services Internet (ISP) de lire tout message de texte en claire (à savoir, les messages non cryptés) et vous offrent un niveau de sécurité accru supplémentaire contre les attaques internes.

Comment fonctionne un VPN ?

Un VPN étend *l'intranet* d'une entreprise (à savoir, son réseau interne) à l'Internet via la création d'un *tunnel* privé sécurisé. Fonctionnement Pour ce faire, il utilise un protocole d'encapsualtion (par exemple, Sécurité de protocole Internet (IPSec)) et recourt au cryptage pour la protection des données du moment où elles sont envoyées jusqu'au moment où elles sont réceptionnées par le destinataire désigné.

Quelles informations devez-vous protéger ?

Il est impératif de protéger un large éventail d'informations stockées sur vos ordinateurs ou transmises vers d'autres entités (par exemple, les banques, les clients, les partenaires commerciaux et les organismes fiscaux locaux ou nationaux). Ces informations sont les suivantes :

- Archives des salariés
- Archives de la paie
- Mots de passe et comptes utilisateur
- Archives des ventes client

- Fichiers de recherche et de développement de produits
- Fichiers de code source

La sécurité est également menacée par le fait que les pirates peuvent accéder à votre intranet et mener les types d'attaques suivantes :

- Suppression ou téléchargement de fichiers importants
- Lecture des messages électroniques
- Erreur fatale sur les ordinateurs
- Interdiction de l'accès aux ordinateurs (refus d'attaque du service)
- Ecoute d'une ligne à la recherche de paquets afin d'obtenir les mots de passe utilisateur et d'autres informations

La sécurité de vos données, ordinateurs et réseaux étant essentielle, PGP a été conçu pour éliminer un nombre important de menaces qui pèsent sur vos réseaux.

Fonctions de PGPnet

Le programme PGPnet comporte les fonctions suivantes :

- Un assistant de configuration vous permettant de configurer des hôtes, passerelles et sous-réseaux via lesquels vous pouvez communiquer de manière sécurisée.
- Des communications poste à poste sécurisées. Aucune passerelle intermédiaire n'est requise.
- Une interface utilisateur simple.
- Une liste sommaire de toutes les associations de sécurité PGPnet actives. Une *Association de sécurité (AS)* contient des informations permettant d'identifier le mode de communication de deux ordinateurs entre eux.
- Une initialisation et une négociation automatiques de l'expiration des associations de sécurité.
- Un mode expert permettant aux utilisateurs avertis de ne pas avoir à recourir à l'Assistant de configuration.
- Les informations relatives à l'historique, utilisées à des fins de diagnostic, apparaissent sous un format facile à lire. Il n'est pas nécessaire d'effectuer une recherche parmi les fichiers d'historique.

Définition de PGPnet

PGPnet, un *réseau privé virtuel (VPN)*, constitue une application de cryptage facile à utiliser, permettant d'établir des communications sécurisées et économiques avec d'autres utilisateurs de PGPnet. Ce produit est basé sur les protocoles IETF IPSec et IETF IKE (Echange de clés via Internet), et étend le protocole IKE afin de prendre en charge l'authentification des clés PGP.

PGPnet assure la confidentialité, l'intégrité et l'authenticité des informations envoyées à partir d'un hôte PGPnet vers un sous-réseau, une passerelle ou un hôte sécurisé.

- Un *hôte sécurisé* est un ordinateur exécutant PGPnet ou un autre logiciel client de communication port à port compatible IPSec (c'est-à-dire, un logiciel qui permet aux hôtes de communiquer directement entre eux).
- Une *passerelle sécurisée* est un pare-feu ou un autre type de passerelle qui encapsule les paquets à destination d'un utilisateur autorisé. Dans ce cas, le terme « autorisé » signifie que le certificat ou le mot de passe complexe partagé du logiciel client est configuré comme acceptable sur la passerelle. Lorsque vous utilisez PGPnet, vous pouvez choisir de communiquer avec un hôte à l'aide de votre clé PGP, d'un certificat X.509 ou d'un mot de passe complexe partagé.
- Un *sous-réseau sécurisé* est un sous-réseau comprenant jusqu'à 254 ordinateurs exécutant généralement PGPnet ou un logiciel client compatible. La spécification du sous-réseau sécurisé vous permet à vous ou à votre administrateur d'identifier plusieurs ordinateurs dans une plage d'adresses IP compatibles IPsec. Notez que les sous-réseaux sécurisés ne doivent pas être protégés par des passerelles.

ASTUCE : Si un sous-réseau comporte de nombreux hôtes sécurisés et un nombre limité d'hôtes non sécurisés, configurez-le en tant que sous-réseau sécurisé, puis ajoutez des hôtes non sécurisés pour chaque exception.

Vous pouvez communiquer en toute sécurité avec des utilisateurs de PGPnet sur l'intranet de votre entreprise, et avec d'autres utilisateurs de PGPnet dans le monde entier. Vous pouvez communiquer via des passerelles, des sous-réseaux et des hôtes que vous-même (ou votre administrateur PGPnet, le cas échéant) avez identifiés comme étant sécurisés. PGPnet permet l'envoi sécurisé de données via Internet et d'autres réseaux non fiables.

Définition d'une association de sécurité

Lors de la première communication d'un ordinateur local avec un ordinateur distant, PGPnet effectue une négociation d'échange de clés via Internet (IKE), puis crée une association de sécurité.

- Lors de la *négociation IKE*, les deux ordinateurs définissent leur mode de communication (par exemple, le type de cryptage, la durée de l'association de sécurité et la méthode d'authentification).
- L'*association de sécurité (AS)* obtenue comporte des informations permettant d'identifier le mode de communication des deux ordinateurs.

PGPnet enregistre, puis surveille toutes les AS mises en place par votre ordinateur et par d'autres ordinateurs avec le vôtre. Lorsqu'une AS initiée par votre ordinateur arrive quasiment à expiration, PGPnet met en place une autre AS avec l'hôte distant. Vous pouvez visualiser toutes les AS actives sur le panneau **Etat** de PGPnet. Pour plus d'informations sur le panneau **Etat** panel, reportez-vous à la section « Affichage du panneau Etat » à la page 161.

Les deux modes de PGPnet : Tunnel et Transport

PGPnet utilise respectivement le mode Tunnel et le mode Transport pour les communications avec des hôtes ou des sous-réseaux protégés par une passerelle sécurisée et pour les communications port à port entre deux hôtes sécurisés non reliés par une passerelle.

Définition du mode Tunnel

La transmission est réalisée via un tunnel lorsque l'ordinateur exécutant PGPnet envoie des paquets via une passerelle sécurisée vers un hôte ou un sous-réseau protégé par cette passerelle. Dans la fenêtre Hôtes de PGPnet, le sous-réseau ou l'hôte de destination est situé en retrait sous la passerelle. Les paquets sont envoyés vers de tels hôtes via un *tunnel*. L'ensemble du paquet envoyé est d'abord physiquement placé dans un autre paquet, puis il est crypté et enfin envoyé vers la passerelle.

Définition du mode Transport

PGPnet peut établir des communications sécurisées port à port. Deux ordinateurs exécutant PGPnet peuvent communiquer de manière sécurisée, quel que soit leur emplacement sur Internet. Une passerelle sécurisée ne s'avère pas nécessaire. Ce type de communication est appelé *mode Transport*. Les passerelles et les pare-feux ne sont pas sécurisés. Aussi les paquets sont-ils transmis de manière sécurisée à partir de l'ordinateur source vers l'ordinateur de destination. En mode Transport, les paquets sont cryptés, puis authentifiés.

Mode de communication de PGPnet avec des hôtes sécurisés et non sécurisés

Les paragraphes suivants présentent le mode de communication de PGPnet avec différents hôtes :

Hôte sécurisé sans passerelle sécurisée entre les hôtes. Les paquets de PGPnet sont cryptés, puis authentifiés (mode Transport).

Hôte sécurisé protégé par une passerelle sécurisée. PGPnet crypte chaque paquet, puis le transmet via un tunnel vers la passerelle. Cette fonction élimine tout risque d'utilisation de la passerelle comme point d'écoutes indiscrètes (mode Tunnel).

Hôte non sécurisé protégé par une passerelle sécurisée. PGPnet transmet des paquets via un tunnel vers la passerelle qui les transfère vers leur destination finale (mode Tunnel).

Utilisation de PGPnet

Si vous disposez d'un administrateur PGPnet, PGPnet peut être configuré lors de son installation.

Si vous ne disposez pas d'un administrateur PGPnet ou si PGPnet n'est pas préconfiguré, installez-le, sélectionnez votre clé ou votre certificat d'authentification (ou les deux), puis configurez des hôtes, des passerelles et des sous-réseaux via l'Assistant d'ajout d'hôtes.

Lorsque PGPnet est configuré, il est lancé en arrière-plan. Chaque fois que vous essayez d'établir une communication avec un autre ordinateur (par exemple, via un e-mail ou un navigateur Web), PGPnet vérifie s'il existe une AS entre cet ordinateur et le vôtre.

- S'il existe une AS entre votre ordinateur et l'ordinateur de destination, PGPnet transmet votre communication selon les termes de cette AS.
- S'il n'existe aucune AS entre votre ordinateur et l'ordinateur de destination et si l'ordinateur est sécurisé, PGPnet lance une négociation IKE afin d'établir une AS, puis transmet votre communication.

- S'il n'existe aucune AS pour l'ordinateur de destination et si ce dernier n'est pas sécurisé, PGPnet traite la communication en fonction des paramètres de sécurité définis dans le panneau Général (**Affichage—>Options—>Général**). Ainsi, si les deux cases **Exiger des communications sécurisées avec tous les hôtes** et **Autoriser des communications avec des hôtes non configurés** sont cochées, PGPnet autorise l'ordinateur à communiquer de manière sécurisée.

REMARQUE : Ceci peut s'avérer dangereux dans la mesure où vous ne pouvez pas communiquer avec les serveurs DNS, DHCP ou WINS, sauf si ces derniers lancent PGPnet ou sont explicitement désignés comme hôtes non sécurisés.

Prenez en compte les remarques suivantes :

- Toutes les AS sont interrompues lors du redémarrage de votre ordinateur ou lors de sa mise en mode veille. Par conséquent, tout ordinateur avec lequel vous n'avez pas communiqué depuis que vous avez redémarré votre propre ordinateur requiert une nouvelle négociation IKE.
- Si vous vous déconnectez de PGPnet, les AS sont susceptibles d'arriver à expiration, et la génération par PGP d'une nouvelle association peut s'avérer impossible jusqu'à la prochaine connexion.
- PGPnet écoute toujours les requêtes d'AS des autres ordinateurs.

Modification des paramètres du panneau de configuration réseau

PGPnet sécurise l'adaptateur réseau spécifique auquel il est connecté. Par conséquent, si vous modifiez les paramètres de votre panneau de configuration réseau, PGPnet effectue automatiquement un contrôle des associations et vous invite à redémarrer votre système. Pour garantir un fonctionnement correct de PGP, redémarrez le système.

Lancement du programme PGPnet

Pour lancer PGPnet

1. Sélectionnez **Démarrer—>Programmes—>PGP—>PGPnet**.

   Ou

   Lancez PGPnet à partir de PGPtray dans la barre des tâches Windows (**PGPtray—> PGPnet—>Etat, Historique** ou **Hôtes**).

Ces deux opérations permettent d'ouvrir la fenêtre PGPnet (voir Figure 8-1).

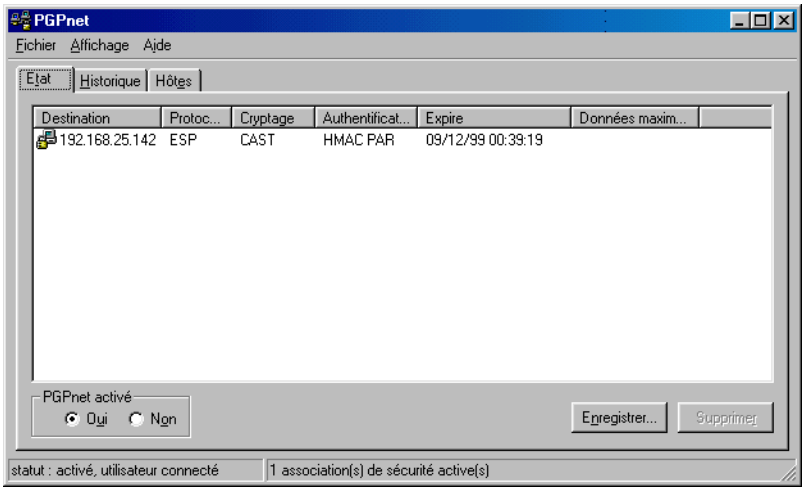


Figure 8-1. fenêtre PGPnet

PGPnet est activé par défaut. Pour activer ou désactiver PGPnet, utilisez les boutons radio situés dans le coin inférieur gauche de la fenêtre. Toutefois, si PGPnet est désactivé et si vous redémarrez votre ordinateur, PGPnet sera désactivé. Pour plus d'informations, reportez-vous aux sections « Désactivation de PGPnet » à la page 160 et « Activation de PGPnet » à la page 160.

Sélection d'une clé ou d'un certificat d'authentification

La première procédure à effectuer préalablement à l'utilisation de PGPnet consiste à sélectionner la clé et / ou le certificat X.509 que vous utiliserez à des fins d'authentification. Si vous ne disposez pas d'une clé ou d'un certicat X.509, consultez la section « Création et échange de clés » à la page 23.

Pour sélectionner votre clé et/ou certificat d'authentification

1. Dans le menu **Affichage** de la fenêtre PGPnet, cliquez sur **Options** (ou sélectionnez PGPnet, **dans PGPtray,** puis sélectionnez **Options)**.
2. Cliquez sur l'onglet **Authentification** (voir Figure 8-2 à la page 157).
3. Sélectionnez la clé et / ou le certificat à utiliser pour l'authentification (cliquez sur **Sélectionner la clé** ou **Sélectionner le certificat**). Notez que la clé ou le certificat doit appartenir à une paire de clés et que vous devez disposer de la clé privée. PGPnet affiche le certificat ou la clé sélectionné(e) dans la zone **Authentication PGP**ou **Authentication X.509**.

4. Cliquez sur **OK**. Une boîte de dialogue vous invite à entrer le mot de passe complexe de la clé sélectionnée.

5. Entrez le mot de passe complexe de la clé, puis cliquez sur **OK**.

IMPORTANT : Si vous créez une connexion VPN avec un autre hôte PGPnet et si vous utilisez PGPkeys pour l'authentification, utilisez le même type de clé PGP. Si un côté de la connexion utilise une clé RSA et si l'autre côté utilise une clé Diffie-Hellman, la négociation d'une AS s'avère impossible.

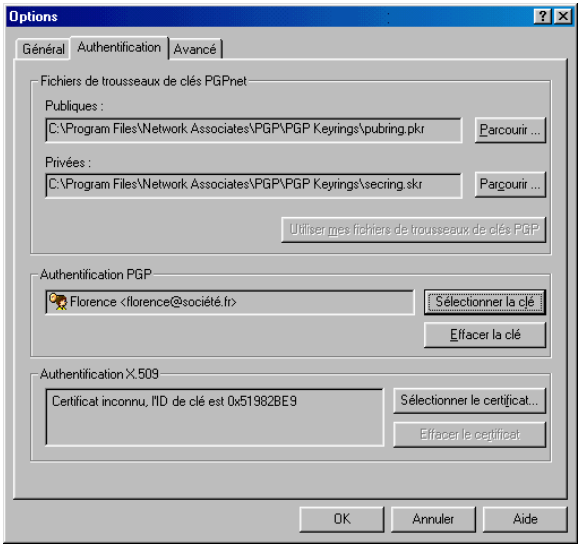


Figure 8-2. Panneau Authentification

Aperçu de la fenêtre PGPnet

La fenêtre PGPnet comporte trois menus :

- **Fichier** (**Quitter**)
- **Affichage** (**Etat**, **Historique**, **Hôtes** et **Options**)
- **Aide** (**Sommaire de l'aide** et **A propos de**)

La fenêtre PGPnet comporte trois panneaux :

- Le panneau **Etat** permet de contrôler l'état des AS existantes (reportez-vous à la section « Affichage du panneau Etat » à la page 161).

- Le panneau **Historique** permet de contrôler les entrées de l'historique à des fins de diagnostic (reportez-vous à la section « Affichage du panneau Historique » à la page 163).
- Le panneau **Hôtes** permet d'ajouter, de modifier ou de supprimer des entrées sur la liste d'hôtes PGPnet, d'établir et d'interrompre des AS (reportez-vous à la section « Utilisation du panneau Hôtes » à la page 164).

PGPnet est activé par défaut. Pour activer ou désactiver PGPnet, utilisez les boutons radio situés dans le coin inférieur gauche de la fenêtre.

La ligne inférieure de la fenêtre, la barre d'état, affiche à gauche les messages relatifs à l'état de PGPnet et, à droite, le nombre d'AS actives. Les messages suivants peuvent apparaître dans la barre d'état :

Tableau 8-1. Messages d'état

Message	Description
état : activé, l'utilisateur est connecté	PGPnet est activé, l'utilisateur est connecté.
état : activé, l'utilisateur est déconnecté	PGPnet est activé, l'utilisateur est déconnecté.
état : aucune connexion n'est requise	Ce message apparaît lorsque aucune clé d'authentification n'est définie.
état : désactivé	L'utilisateur a désactivé PGPnet.
pilote non installé	Le pilote PGPnet ne répond pas. Redémarrez votre système. Si le pilote ne répond toujours pas, réinstallez PGPnet. Si le problème persiste, contactez le support technique de NAI.
le service ne fonctionne pas	Le service PGPnet ne fonctionne pas. Redémarrez votre système. Si ce message apparaît à nouveau, réinstallez PGPnet. Si le problème persiste, contactez le support technique de NAI.
le service ne répond pas	Le service PGPnet fonctionne, mais il ne répond pas aux messages de l'application. Redémarrez votre système. Si ce message apparaît à nouveau, réinstallez PGPnet. Si le problème persiste, contactez le support technique de NAI.

Utilisation de PGPnet à partir de PGPtray

Le sous-menu de PGPnet, accessible via l'icône PGPtray de la barre des tâches Windows, vous permet d'effectuer les opérations suivantes :

Pour...	Procédez comme suit...
Afficher le panneau Historique	Cliquez sur l'icône PGPtray, sélectionnez PGPnet, puis cliquez sur **Historique**.
Afficher le panneau Etat	Cliquez sur l'icône PGPtray, sélectionnez PGPnet, puis cliquez sur **Etat**.
Afficher le panneau Hôtes	Cliquez sur l'icône PGPtray, sélectionnez PGPnet, puis cliquez sur **Hôtes**.
Afficher la fenêtre Options	Cliquez sur l'icône PGPtray, sélectionnez PGPnet, puis cliquez sur **Options**.
Vous connecter à PGPnet	Cliquez sur l'icône PGPtray, sélectionnez PGPnet, puis cliquez sur **Connecter**. Cette option apparaît en grisé si aucune clé d'authentification n'est sélectionnée.
Vous déconnecter de PGPnet	Cliquez sur l'icône PGPtray, sélectionnez PGPnet, puis cliquez sur **Déconnecter**. Cette option apparaît en grisé si aucune clé d'authentification n'est sélectionnée.
Quitter	Cliquez sur l'icône PGPtray, puis cliquez sur **Quitter**.

Icône PGPtray

L'icône PGPtray vous indique si PGPnet est désactivé ou non installé (verrou gris), installé et activé (verrou jaune sur un réseau), ou installé mais désactivé (verrou jaune sur un réseau accompagné d'un rond jaune et d'un point d'exclamation). Lorsque vous placez le pointeur de la souris sur l'icône **PGPtray**, une info-bulle affiche l'état de PGPnet, ainsi qu'une description des messages d'erreurs, tels que « le service n'est pas installé ».

Désactivation de PGPnet

Vous devez parfois désactiver PGPnet, par exemple, à des fins de diagnostic. Lorsque PGPnet est désactivé, toutes les communications entre tous les ordinateurs sont effectuées sans modification, ni sécurisation.

Pour désactiver PGPnet, cliquez sur **Désactivé** dans la fenêtre PGPnet (voir Figure 8-3 à la page 160).

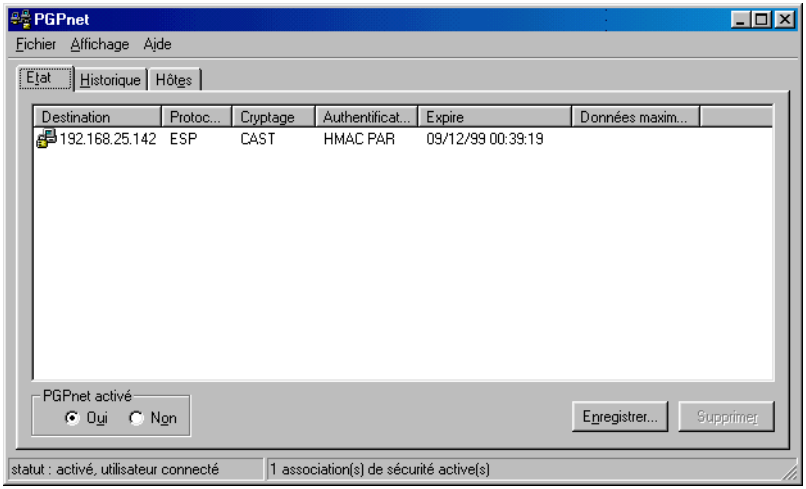


Figure 8-3. Fenêtre PGPnet

Activation de PGPnet

Pour activer PGPnet, cliquez sur **Activé** dans la fenêtre PGPnet (voir Figure 8-3 à la page 160).

Fermeture de PGPnet

Sélectionnez **Quitter** dans le menu Fichier de la fenêtre PGPnet, cliquez sur le **X** dans le coin supérieur droit de la fenêtre PGPnet ou cliquez sur l'icône de la barre des tâches, puis sur **Quitter**.

Notez que la fermeture de PGPnet n'entraîne ni la désactivation du service PGPnet, ni l'interruption des AS.

Utilisation de PGPnet

Lorsque PGPnet est activé, il est lancé en arrière-plan. Pour communiquer avec un ordinateur, utilisez votre logiciel (par exemple, e-mail ou navigateur Web) de manière habituelle. PGPnet évalue chaque communication, procède au cryptage, puis l'encapsulation comme requis.

Affichage du panneau Etat

Le panneau **Etat** situé dans la fenêtre PGPnet répertorie les AS actives et, le cas échéant, leur date d'expiration (voir Figure 8-4 à la page 162). Une AS peut être interrompue lorsque sa capacité atteint une certaine limite (par exemple, 4 Mo de données sont transmises via l'AS) ou après un laps de temps défini. La longueur d'une AS est négociée lors de sa mise en place. Lorsque PGPnet négocie l'AS, il définit une valeur d'expiration, puis crée automatiquement une nouvelle AS lorsque cette valeur est atteinte. Les utilisateurs peuvent configurer cette valeur d'expiration de l'AS. Pour plus d'informations, reportez-vous à la section « Définition des valeurs d'expiration » à la page 186.

- Si votre ordinateur a initié une AS et que celle-ci est sur le point d'expirer, PGPnet lance automatiquement la négociation d'une nouvelle AS de remplacement. Par conséquent, le panneau **Etat** peut parfois afficher automatiquement deux AS pour le même ordinateur.
- Lorsque vous établissez une AS avec un autre hôte, PGPnet utilise les valeurs d'expiration les plus restrictives parmi celles définies par l'un ou l'autre de ces deux hôtes. Par conséquent, une AS est susceptible d'arriver à expiration avant que la valeur maximale d'expiration ne soit atteinte.

Le tableau suivant décrit les informations que le panneau **Etat** de PGPnet affiche pour chaque AS :

Colonne	Description
Destination	Adresse IP de l'hôte ou de la passerelle cible.
Protocole	Type de protocole négocié, par exemple, AH, ESP ou IPCOMP.
Cryptage	Type d'algorithme de cryptage négocié. Lorsqu'il s'agit d'une AS d'authentification uniquement, cette colonne peut être vide. Les types de cryptage incluent DES triple ou CAST.

Colonne	Description
Authentification	Type d'algorithme d'authentification négocié. Cette colonne peut être vide ou peut contenir l'une des entrées suivantes : HMAC RM5 ou HMAC SHA. En cas d'utilisation des deux protocoles ESP et AH, cette colonne peut comporter deux entrées.
Expire	Date et heure d'expiration de l'AS (mm/jj/aa hh:mm:ss AM ou PM). Lorsque l'expiration de l'AS dépend uniquement du volume des données, cette colonne affiche « Jamais ».
Données maximales	Nombre maximal de Mo de données transportées par l'AS avant expiration.

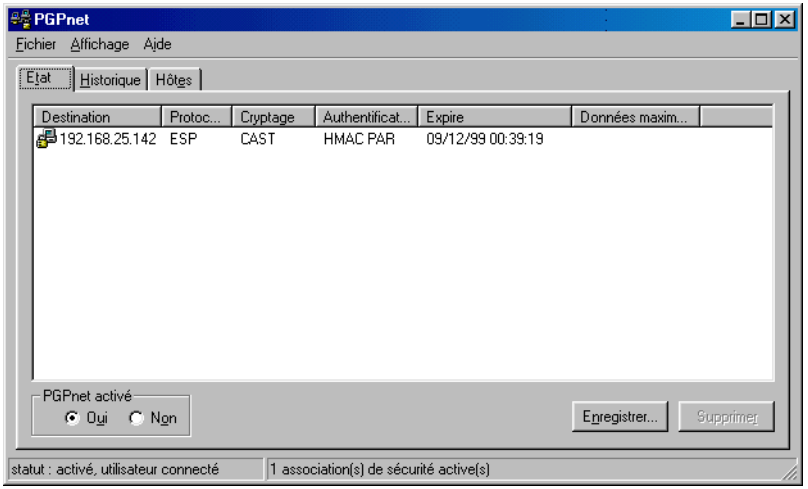


Figure 8-4. Panneau Etat

Pour sauvegarder, à des fins de diagnostic, une liste des AS actives, utilisez la fonction **Enregistrer**. Pour sauvegarder la liste des AS sous un fichier texte séparé par des tabulations, cliquez sur **Enregistrer**.

Pour supprimer une AS, utilisez la fonction **Supprimer**. Vous pouvez le faire lorsque vous pensez qu'une AS a été compromise, lorsque vous êtes certain que l'hôte cible est en panne ou lorsque vous estimez que la connexion doit être interrompue.

Pour activer ou désactiver PGPnet, cliquez sur **Activé** ou **Désactivé**.

Pour afficher les dernières entrées d'historique, cliquez sur l'onglet **Historique**.

Affichage du panneau Historique

Le panneau **Historique** affiche les erreurs système et de service, la date et l'heure à laquelle elles sont survenues, ainsi que leur description. Utilisez ces informations afin de résoudre les problèmes susceptibles de se produire (voir Figure 8-5 à la page 163).

Pour sélectionner les types d'événements à afficher, à savoir Service, IKE, IPSec, PGP et / ou Système, cochez les cases **Afficher les événements** correspondantes. Pour afficher un type d'événement spécifique, cochez la case correspondante.

Pour sauvegarder les informations de l'historique actuel dans un fichier texte, cliquez sur **Enregistrer**.

Pour supprimer les informations de l'historique actuel à la fois dans le fichier d'historique et à l'écran, cliquez sur **Effacer**.

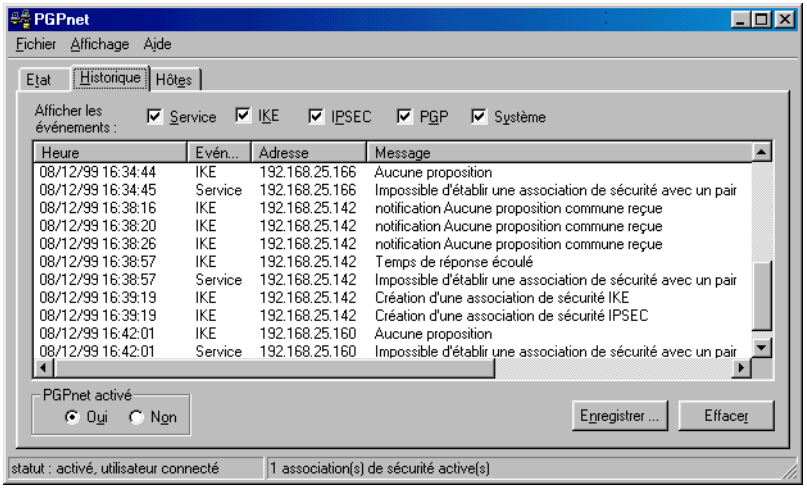


Figure 8-5. Panneau Historique

Le tableau suivant décrit les informations affichées pour chaque entrée d'historique :

Colonne	Description
Heure	La date et l'heure, au format mm/jj/aa hh:mm:ss AM ou PM, auxquelles l'erreur est survenue.
Evénement	Type d'événement, Service, IKE, IPSec, PGP ou erreur système.
Adresse	Adresse IP de l'hôte distant.
Message	Texte décrivant le type d'erreur (par exemple, Impossible d'établir une association de sécurité avec un pair).

Utilisation du panneau Hôtes

Le panneau **Hôtes** affiche les passerelles, sous-réseaux et hôtes sécurisés. Si un signe plus (+) apparaît à gauche d'un élément, cliquez sur ce signe pour agrandir l'affichage et faire apparaître d'autres entrées associées à cet élément (voir Figure 8-7 à la page 169).

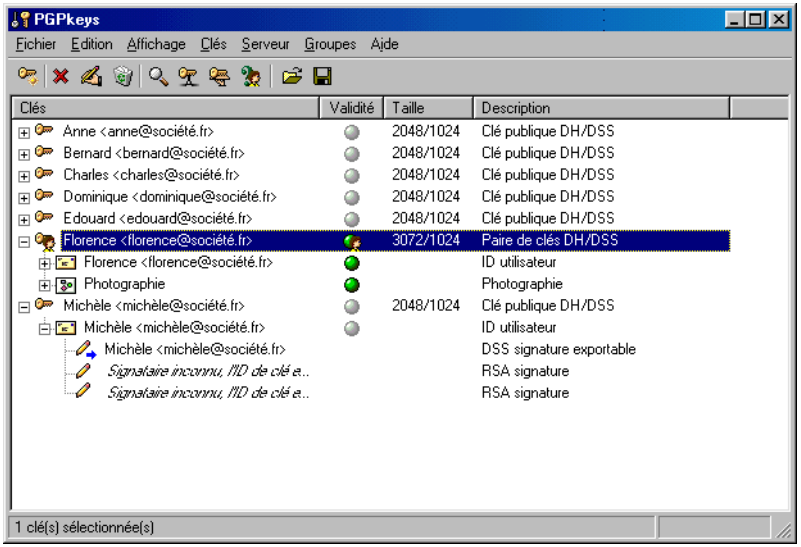


Figure 8-6. Panneau Hôtes

Le tableau suivant décrit les informations affichées pour chaque entité.

Colonne	Description
Nom	Nom descriptif de l'entrée d'hôte, de sous-réseau ou de passerelle.
Adresse	Adresse IP de l'hôte, du sous-réseau ou de la passerelle.
Sous-réseau	Lorsque l'entrée d'hôte représente un sous-réseau, cette zone affiche son masque. Dans le cas contraire, cette zone n'est pas renseignée.
Authentification	Une icône indique le type d'authentification utilisé pour l'entrée d'hôte. • Une icône représentant une clé indique l'authentification de cryptographie de clés publiques. • Une icône représentant un certificat indique l'authentification par certificat X.509. • Une icône représentant une oreille indique une authentification de secret partagé. • Aucune icône n'indique que l'entrée d'hôte configurée n'est pas sécurisée.
AS	Affiche un point vert lorsqu'une AS existe pour cet hôte. Dans le cas contraire, la colonne n'est pas renseignée.

Le tableau suivant décrit les boutons du panneau **Hôtes**.

Bouton	Description
Editer	Affiche les valeurs de l'élément sélectionné dans la boîte de dialogue Hôte/Passerelle.
Supprimer	Supprime l'entrée d'hôte sélectionnée.
Ajouter	Active l'Assistant d'ajout d'hôtes/de passerelles (si vous êtes en mode expert, ce bouton active la boîte de dialogue Hôte/Passerelle).
Connecter/ Déconnecter	Le bouton Connecter établit une AS alors que le bouton Déconnecter l'interrompt.

Boutons Connecter et Déconnecter

Pour établir une AS avec un hôte configuré, utilisez le bouton **Connecter**. Sélectionnez l'hôte, puis cliquez sur **Connecter**. Ce bouton est désactivé lorsque vous sélectionnez une entrée d'hôte inappropriée (par exemple, un sous-réseau sécurisé ou un hôte non sécurisé qui n'est pas protégé par une passerelle).

Pour interrompre une AS avec un hôte configuré, utilisez le bouton **Déconnecter**. Sélectionnez l'hôte, puis cliquez sur **Déconnecter**.

Pour plus d'informations sur l'établissement d'une AS, reportez-vous à la section « Etablissement d'une AS » à la page 166.

Etablissement d'une AS

Etablissement d'une AS à l'aide des clés d'authentification de PGP

Effectuez les étapes décrites ci-dessous afin d'établir une AS avec un autre hôte à l'aide des clés d'authentification de PGP.

Pour établir une AS avec un autre hôte à l'aide des clés d'authentification de PGP

1. Vérifiez que les systèmes sont reliés par une connexion réseau.
2. Installez PGPnet sur les deux systèmes.

   Lors de l'installation, sélectionnez l'adaptateur réseau approprié pour PGPnet. Par exemple, si la connexion réseau est effectuée via Ethernet, PGPnet doit être relié à l'adaptateur correspondant. Il en va de même en cas de connexion réseau via un modem (l'adaptateur correspondant est également appelé encapsulateur de réseau étendu à accès distant ou carte d'accès distant).
3. Après avoir installé PGPnet, redémarrez les deux systèmes.
4. Pour chaque système, vérifiez qu'une clé d'authentification a été définie dans la section **Authentification PGP** du panneau **Authentification** (**Affichage—>Options—>Authentification**).
5. Echangez, signez, puis validez les clés publiques utilisées par chaque système pour l'authentification. Pour plus d'informations, reportez-vous à la section Chapitre 2, « Utilisation de PGP ».

> **ASTUCE :** Pour une meilleure compatibilité, utilisez une partie tierce de confiance ou une CA.

6. Il est nécessaire qu'au moins un utilisateur crée une entrée dans la liste d'hôtes PGPnet pour l'autre système. Vous devez connaître l'adresse IP ou le nom d'hôte de ce système. Vérifiez que l'entrée identifie l'hôte comme sécurisé (si tel est le cas, l'icône située en regard de l'entrée d'hôte dans le panneau **Hôtes** représente un ordinateur avec un verrou).

7. Sélectionnez l'entrée de l'hôte dans le panneau **Hôtes**, puis cliquez sur **Connecter**. Si la connexion est établie, un point vert apparaît dans la colonne AS.

Etablissement d'une AS à l'aide des certificats d'authentification X.509

Effectuez les étapes décrites ci-dessous afin d'établir une AS avec un autre hôte à l'aide d'un certificat d'authentification X.509.

Pour établir une AS avec un autre hôte à l'aide d'un certificat d'authentification X.509

1. Vérifiez que chaque système dispose d'une connexion réseau.

2. Installez PGPnet sur les deux systèmes.

   Lors de l'installation, sélectionnez l'adaptateur réseau approprié pour PGPnet. Par exemple, si la connexion réseau est effectuée via Ethernet, PGPnet doit être relié à l'adaptateur correspondant. Il en va de même en cas de connexion réseau via un modem (l'adaptateur correspondant est également appelé encapsulateur de réseau étendu à accès distant ou carte d'accès distant).

3. Après avoir installé PGPnet, redémarrez les deux systèmes.

4. Vérifiez que chaque système dispose d'un certificat d'authentification dans la section **Authentification X.509** située dans le panneau **Authentification** (**Affichage—>Options—>Authentification**).

5. Vérifiez qu'il existe une CA par défaut pour le certificat X.509, qu'elle est signée et considérée comme entièrement fiable sur les deux systèmes. Les deux systèmes doivent disposer de la même CA par défaut.

6. Il est nécessaire qu'au moins un utilisateur crée une entrée dans la liste d'hôtes PGPnet pour l'autre système. Vous devez connaître l'adresse IP ou le nom d'hôte de ce système. Vérifiez que l'entrée identifie l'hôte comme sécurisé. Si l'hôte est sécurisé, l'icône située en regard de son entrée dans le panneau **Hôtes** représente un ordinateur avec un verrou.

7. Sélectionnez l'entrée de l'hôte dans le panneau **Hôtes**, puis cliquez sur **Connecter**. Si la connexion est établie, un point vert apparaît dans la colonne AS.

Etablissement d'une AS à l'aide de l'authentification par mot de passe complexe secret partagé

Effectuez les étapes décrites ci-dessous afin d'établir une AS avec un autre hôte à l'aide de l'authentification par mot de passe complexe secret partagé.

Pour établir une AS avec un autre hôte à l'aide de l'authentification par secret partagé

> **AVERTISSEMENT :** Contrairement aux mots de passe complexes PGP traditionnels, les mots de passe complexes secrets partagés sont stockés sur votre ordinateur sous forme non cryptée. Ceci présente un risque potentiel qu'il est cependant facile de prévenir via l'utilisation de clés ou de certificats.

1. Vérifiez que chaque système dispose d'une connexion réseau.
2. Installez PGPnet sur les deux systèmes.

   Lors de l'installation, sélectionnez l'adaptateur réseau approprié pour PGPnet. Par exemple, si la connexion réseau est effectuée via Ethernet, PGPnet doit être relié à l'adaptateur correspondant. Il en va de même en cas de connexion réseau via un modem (l'adaptateur correspondant est également appelé encapsulateur de réseau étendu à accès distant ou carte d'accès distant).
3. Après avoir installé PGPnet, redémarrez les deux systèmes.
4. Les deux utilisateurs doivent créer une entrée dans la liste d'hôtes PGPnet pour l'autre système.

   Vous devez connaître l'adresse IP ou le nom d'hôte de l'autre système, puis convenir d'un mot de passe complexe secret partagé.

   Pour plus d'informations sur la configuration d'un hôte sécurisé, reportez-vous à la section « Ajout d'un hôte, d'un sous-réseau ou d'une passerelle » à la page 169.
5. Sélectionnez l'entrée de l'hôte dans le panneau **Hôtes**, puis cliquez sur **Connecter**. Si la connexion est établie, un point vert apparaît dans la colonne AS.

Ajout d'un hôte, d'un sous-réseau ou d'une passerelle

REMARQUE : Si vous êtes un utilisateur averti, reportez-vous à la section « Mode expert : ajout d'hôtes, de passerelles et de sous-réseaux sans utiliser l'Assistant » à la page 180.

Si votre entreprise dispose d'un administrateur PGPnet, il a probablement préconfiguré la plupart des hôtes, sous-réseaux et passerelles via lesquels vous communiquez. Chaque hôte, sous-réseau ou passerelle préconfiguré(e) représente une entrée dans la liste d'hôtes PGPnet. Pour ajouter des entrées supplémentaires à cette liste, utilisez l'Assistant d'**ajout d'hôtes** PGPnet ou la boîte de dialogue **Hôte/Passerelle**.

Si vous ne disposez pas d'un administrateur PGPnet ou si les hôtes, sous-réseaux ou passerelles ne sont pas configurés lors de l'installation de PGPnet, l'Assistant d'**ajout d'hôtes** est lancé automatiquement lors du premier démarrage de PGPnet. Cet Assistant vous permet d'ajouter les hôtes, sous-réseaux et passerelles nécessaires.

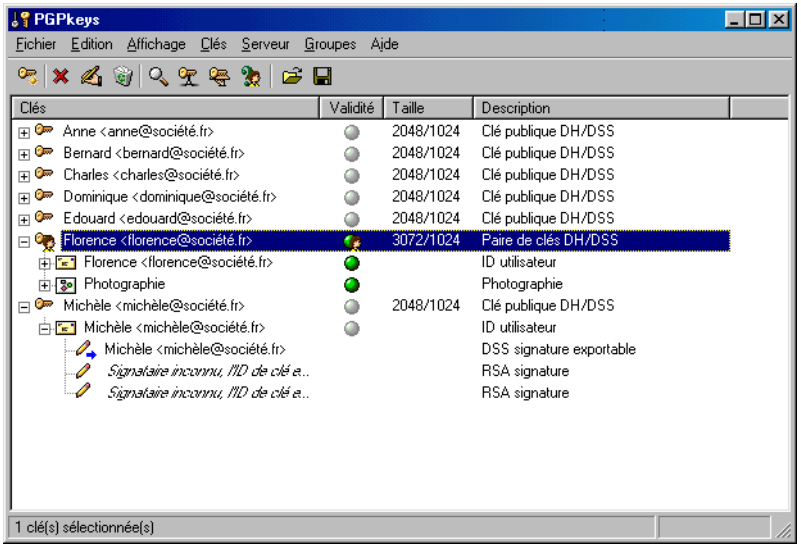


Figure 8-7. Panneau Hôtes

Informations à connaître

Les paragraphes suivants indiquent les informations nécessaires pour ajouter un hôte, un sous-réseau ou une passerelle.

Tableau 8-1. Informations à connaître pour ajouter des hôtes, des passerelles et des sous-réseaux

Pour :	Vous devez connaître :
Ajouter un hôte sécurisé	Le nom de domaine ou l'adresse IP de l'hôte
Ajouter un sous-réseau	L'adresse IP et le masque de sous-réseau
Ajouter une passerelle	Le nom de domaine ou l'adresse IP de l'hôte
Ajouter un hôte protégé par une passerelle configurée	Le nom de domaine ou l'adresse IP de l'hôte
Ajouter un sous-réseau protégé par une passerelle configurée	L'adresse IP et le masque de sous-réseau

Tableau 8-2. Pages traitant de l'ajout d'hôtes, de sous-réseaux et de passerelles

Pour :	Voir...
Ajouter un hôte	page 170
Ajouter un sous-réseau	page 172
Ajouter une passerelle	page 174
Ajouter un hôte protégé par une passerelle configurée	page 175
Ajouter un sous-réseau protégé par une passerelle configurée	page 176

Ajout d'un hôte

REMARQUE : Pour ajouter un hôte protégé par une passerelle configurée existante, reportez-vous à la section « Ajout d'un hôte protégé par une passerelle sécurisée » à la page 175.

Pour ajouter une entrée d'hôte à la liste, utilisez l'Assistant d'**ajout d'hôtes** de PGPnet.

1. Dans la fenêtre principale de PGPnet, cliquez sur l'onglet **Hôtes**.
2. Cliquez sur **Ajouter** (ou Alt-A). L'Assistant d'**ajout d'hôtes** apparaît. Lisez le contenu du premier écran, puis cliquez sur **Suivant**.
3. L'Assistant demande si vous souhaitez ajouter un hôte, un sous-réseau ou une passerelle. Cliquez sur **Hôte**, puis sur **Suivant**.
4. Vous pouvez appliquer des communications sécurisées ou autoriser des communications non sécurisées. Cliquez sur le bouton radio situé en regard de votre sélection, puis sur **Suivant**.
5. Entrez un nom descriptif pour l'ordinateur avec lequel vous souhaitez communiquer, puis cliquez sur **Suivant**.
6. Entrez soit le nom de domaine d'hôte, soit son adresse IP, puis cliquez sur **Suivant**. L'Assistant lance ensuite une recherche sur votre entrée. Si elle s'avère introuvable, cliquez sur **Précédent** pour revenir à l'écran précédent, puis entrez à nouveau le nom ou l'adresse IP.

Pour appliquer des communications sécurisées, effectuez les étapes suivantes :

7. Sélectionnez le mode de communication à établir avec cet ordinateur : la sécurité cryptographique de clés publiques ou la sécurité de secret partagé (basée sur le mot de passe complexe). Cliquez sur **Suivant**. Si vous avez sélectionné la sécurité de secret partagé, entrez le mot de passe complexe. Notez que les deux hôtes doivent configurer le même mot de passe complexe secret partagé. Cliquez sur **Suivant**.

AVERTISSEMENT : Contrairement aux mots de passe complexes PGP traditionnels, les mots de passe complexes secrets partagés sont stockés sur votre ordinateur sous forme non cryptée, ce qui représente un risque potentiel.

Si vous n'avez pas sélectionné de clé ou de certificat d'authentification, l'Assistant vous y invite maintenant.

- Si vous avez sélectionné la sécurité de secret partagé, passez directement à l'etape 8.
- Si vous avez sélectionné la sécurité cryptographique de clés publiques, passez directement à l'etape 9.

8. Sélectionnez votre mode d'identification à l'ordinateur distant (uniquement en cas d'utilisation de l'authentification de secret partagé) : adresse IP, nom de domaine d'hôte, nom de domaine utilisateur ou nom explicite.

   Adresse IP : identification via l'adresse IP de cet ordinateur [nnn.nnn.nnn.nnn]

   Nom de domaine d'hôte : identification via le nom de domaine d'hôte de cet ordinateur [nomordinateur.nomduréseau]

   Nom de domaine utilisateur : identification via le nom de domaine d'hôte et le nom de domaine utilisateur définis [par exemple, nomutilisateur@nomordinateur.nomduréseau]

   Nom explicite : identification via une chaîne de texte définie, par exemple, « CN=« Paul Blanc »,_C=FR,_O=« Acme,_Inc. » »

   Cliquez sur **Suivant**. Si vous sélectionnez Nom de domaine utilisateur ou Nom explicite, entrez le nom, puis cliquez sur **Suivant**.

9. L'Assistant ajoute l'entrée à votre liste d'hôtes. Pour quitter l'Assistant, cliquez sur **Terminer**.

Ajout d'un sous-réseau

REMARQUE : Pour ajouter un sous-réseau protégé par une passerelle configurée existante, reportez-vous à la section « Ajout d'un sous-réseau protégé par une passerelle configurée » à la page 176.

Pour ajouter une entrée de sous-réseau à la liste d'hôtes, utilisez l'Assistant d'**ajout d'hôtes** de PGPnet.

1. Dans la fenêtre principale de PGPnet, cliquez sur l'onglet **Hôtes**.
2. Cliquez sur **Ajouter** (ou Alt-A). L'Assistant d'**ajout d'hôtes** apparaît. Lisez le contenu du premier écran, puis cliquez sur **Suivant**.
3. L'Assistant demande si vous souhaitez ajouter un hôte, un sous-réseau ou une passerelle. Cliquez sur **Sous-réseau**, puis sur **Suivant**.
4. Vous pouvez appliquer des communications sécurisées ou autoriser des communications non sécurisées. Cliquez sur le bouton radio situé en regard de votre sélection, puis sur **Suivant**.
5. Entrez un nom descriptif pour le sous-réseau avec lequel vous souhaitez communiquer, puis cliquez sur **Suivant**.

6. Entrez le masque et l'adresse IP du sous-réseau. Cliquez sur **Suivant**.

REMARQUE : Si vous configurez un sous-réseau avec un mot de passe complexe secret partagé, tous les ordinateurs de ce sous-réseau doivent être configurés avec le même mot de passe complexe secret partagé.

Pour appliquer des communications sécurisées, effectuez les étapes suivantes :

7. Sélectionnez le mode de communication à utiliser avec ce sous-réseau : la sécurité cryptographique de clés publiques ou la sécurité de secret partagé (basée sur le mot de passe complexe). Cliquez sur **Suivant**. Si vous avez sélectionné la sécurité de secret partagé, entrez le mot de passe complexe. Dans ce cas, chaque ordinateur situé sur ce sous-réseau doit également être configuré avec le même mot de passe complexe de secret partagé. Cliquez sur **Suivant**.

AVERTISSEMENT : Contrairement aux mots de passe complexes PGP traditionnels, les mots de passe complexes secrets partagés sont stockés sur votre ordinateur sous forme non cryptée, ce qui représente unrisque potentiel.

---

8. Sélectionnez votre mode d'identification à l'ordinateur distant (uniquement en cas d'utilisation de l'authentification de secret partagé) : adresse IP, nom de domaine d'hôte, nom de domaine utilisateur ou nom explicite.

   Adresse IP : identification via l'adresse IP de cet ordinateur [nnn.nnn.nnn.nnn]

   Nom de domaine d'hôte : identification via le nom de domaine d'hôte de cet ordinateur [nomordinateur.nomduréseau]

   Nom de domaine utilisateur : identification via le nom de domaine d'hôte et le nom de domaine utilisateur définis [par exemple, nomutilisateur@nomordinateur.nomduréseau]

   Nom explicite : identification via une chaîne de texte définie, par exemple, « CN=« Paul Blanc »,_C=FR,_O=« Acme,_Inc. » »

   Cliquez sur **Suivant**. Si vous sélectionnez Nom de domaine utilisateur ou Nom explicite, entrez le nom, puis cliquez sur **Suivant**.

9. L'Assistant ajoute l'entrée à votre liste d'hôtes. Cliquez sur **Terminer**.

Ajout d'une passerelle

Pour ajouter une entrée de passerelle sécurisée à la liste d'hôtes, utilisez l'Assistant d'**ajout d'hôtes** de PGPnet.

1. Dans la fenêtre principale de PGPnet, cliquez sur l'onglet **Hôtes**.
2. Cliquez sur **Ajouter** (ou Alt-A). L'Assistant d'**ajout d'hôtes** apparaît. Lisez le contenu du premier écran, puis cliquez sur **Suivant**.
3. L'Assistant demande si vous souhaitez ajouter un hôte, un sous-réseau ou une passerelle. Cliquez sur le bouton radio **Passerelle**, puis sur **Suivant**.
4. Entrez un nom descriptif pour la passerelle avec laquelle vous souhaitez communiquer de manière sécurisée, puis cliquez sur **Suivant**.
5. Entrez soit le nom de domaine d'hôte, soit l'adresse IP de la passerelle, puis cliquez sur **Suivant**. L'Assistant lance ensuite une recherche sur votre entrée. Si elle s'avère introuvable, cliquez sur **Précédent** pour revenir à l'écran précédent, puis entrez à nouveau le nom ou l'adresse IP. Après avoir entré l'adresse IP appropriée, cliquez sur **Suivant**.
6. Sélectionnez le mode de communication à utiliser avec cet ordinateur : la sécurité cryptographique des clés publiques ou la sécurité de secret partagé (basée sur le mot de passe complexe). Cliquez sur **Suivant**. Si vous avez sélectionné la sécurité de secret partagé, entrez le mot de passe complexe. Cliquez sur **Suivant**.

AVERTISSEMENT : Contrairement aux mots de passe complexes PGP traditionnels, les mots de passe complexes secrets partagés sont stockés sur votre ordinateur sous forme non cryptée, ce qui représente un risque potentiel.

- Si vous avez sélectionné la sécurité de secret partagé, passez directement à l'etape 7.
- Dans le cas contraire, passez directement à l'etape 8.

7. Sélectionnez votre mode d'identification à l'ordinateur distant (uniquement en cas d'utilisation de l'authentification de secret partagé) : adresse IP, nom de domaine d'hôte, nom de domaine utilisateur ou nom explicite.

   Adresse IP : identification via l'adresse IP de cet ordinateur [nnn.nnn.nnn.nnn]

   Nom de domaine d'hôte : identification via le nom de domaine d'hôte de cet ordinateur [nomordinateur.nomduréseau]

   Nom de domaine utilisateur : identification via le nom de domaine d'hôte et le nom de domaine utilisateur définis [par exemple, nomutilisateur@nomordinateur.nomduréseau]

   Nom explicite : identification via une chaîne de texte définie, par exemple, « CN=« Paul Blanc »,_C=FR,_O=« Acme,_Inc. » »

   Cliquez sur **Suivant**. Si vous sélectionnez Nom de domaine utilisateur ou Nom explicite, entrez le nom, puis cliquez sur **Suivant**.

8. L'Assistant ajoute l'entrée de passerelle sécurisée à votre liste d'hôtes.

   A cet instant de la procédure, vous pouvez créer un nouvel hôte ou un nouveau sous-réseau associé à cette passerelle. Pour ce faire, cliquez sur le bouton radio **Oui**. Si vous ne souhaitez pas créer un nouveau sous-réseau ou un nouvel hôte, cliquez sur le bouton radio **Non**, puis sur **Suivant**.

   - Pour créer un nouvel hôte, passez directement à l'Etape 2 à la page 171.
   - Pour créer un nouveau sous-réseau, passez directement à l'Etape 2 à la page 172.
   - Si vous ne souhaitez pas créer un hôte ou un sous-réseau maintenant, cliquez sur **Terminer**.

Ajout d'un hôte protégé par une passerelle sécurisée

Pour ajouter un hôte sécurisé protégé par une passerelle configurée à la liste d'hôtes, utilisez l'Assistant d'**ajout d'hôtes** de PGPnet.

1. Dans la fenêtre principale de PGPnet, cliquez sur l'onglet **Hôtes**.
2. Sélectionnez la passerelle configurée, puis cliquez sur **Ajouter**. L'Assistant d'**ajout d'hôtes** apparaît. Lisez le contenu du premier écran, puis cliquez sur **Suivant**.
3. L'Assistant demande si vous souhaitez créer une nouvelle entrée d'hôte pour un ordinateur ou un sous-réseau accessible via la passerelle sélectionnée. Pour ce faire, sélectionnez **Oui**, puis cliquez sur **Suivant**.

4. L'Assistant vous demande de sélectionner le type de communication à configurer. Sélectionnez **Hôte**, puis cliquez sur **Suivant**. Pour ajouter un hôte sécurisé, reportez-vous à la section « Ajout d'un hôte » à la page 170. Pour ajouter un hôte non sécurisé, passez directement à l'étape 5.

5. L'Assistant demande si vous souhaitez ajouter un hôte sécurisé ou non sécurisé. Sélectionnez **Autoriser des communications non sécurisées**, puis cliquez sur **Suivant**.

6. Entrez un nom descriptif pour l'ordinateur avec lequel vous souhaitez communiquer, puis cliquez sur **Suivant**.

7. Entrez soit le nom de domaine d'hôte, soit son adresse IP, puis cliquez sur **Suivant**. L'Assistant lance ensuite une recherche sur votre entrée. Si elle s'avère introuvable, cliquez sur **Précédent** pour revenir à l'écran précédent, puis entrez à nouveau le nom ou l'adresse IP.

8. L'Assistant ajoute l'entrée à votre liste d'hôtes. Pour quitter l'Assistant, cliquez sur **Terminer**.

Ajout d'un sous-réseau protégé par une passerelle configurée

REMARQUE : Pour ajouter un sous-réseau qui n'est pas protégé par une passerelle configurée existante, reportez-vous à la section « Ajout d'un sous-réseau » à la page 172.

Pour ajouter un sous-réseau protégé par une passerelle configurée à la liste d'hôtes, utilisez l'Assistant d'**ajout d'hôtes** de PGPnet.

1. Dans la fenêtre principale de PGPnet, cliquez sur l'onglet **Hôtes**.

2. Sélectionnez la passerelle configurée, puis cliquez sur **Ajouter**. L'Assistant d'**ajout d'hôtes** apparaît. Lisez le contenu du premier écran, puis cliquez sur **Suivant**.

3. L'Assistant demande si vous souhaitez créer une nouvelle entrée d'hôte pour un ordinateur ou un sous-réseau accessible via la passerelle sélectionnée. Pour ce faire, sélectionnez **Oui**, puis cliquez sur **Suivant**.

4. L'Assistant vous demande de sélectionner le type de communication à configurer. Sélectionnez **Sous-réseau**, puis cliquez sur **Suivant**. Pour ajouter un sous-réseau sécurisé, reportez-vous à la section « Ajout d'un sous-réseau » à la page 172**.** Pour ajouter un sous-réseau non sécurisé, passez directement à l'etape 5.

5. L'Assistant demande si vous souhaitez ajouter un sous-réseau sécurisé ou non sécurisé. Sélectionnez **Autoriser des communications non sécurisées**, puis cliquez sur **Suivant**.

6. Entrez un nom descriptif pour le sous-réseau avec lequel vous souhaitez communiquer, puis cliquez sur **Suivant**.
7. Entrez l'adresse IP et le masque du sous-réseau avec lequel vous souhaitez communiquer, puis cliquez sur **Suivant**.
8. L'Assistant ajoute l'entrée de sous-réseau à votre liste d'hôtes. Pour quitter l'Assistant, cliquez sur **Terminer**.

Modification d'une entrée d'hôte, de sous-réseau ou de passerelle

Vous devez parfois modifier la configuration d'un hôte, d'un sous-réseau ou d'une passerelle, par exemple, lorsqu'une adresse IP, un masque de sous-réseau ou un nom de domaine d'hôte est modifié(e). Pour modifier cette configuration, procédez comme suit :

1. Cliquez sur l'onglet **Hôtes**.
2. Sélectionnez l'hôte, le sous-réseau ou la passerelle à modifier.
3. Cliquez sur **Editer**.

   Raccourci : cliquez deux fois directement sur l'hôte dans la liste.
4. Apportez les modifications nécessaires.
5. Cliquez sur **OK**.

La base de données PGPnet est mise à jour immédiatement. Cette mise à jour n'est toutefois pas effectuée en cas de fonctionnement anormal du service ou du pilote PGPnet. Un redémarrage de l'ordinateur peut s'avérer nécessaire.

Suppression d'une entrée d'hôte, de sous-réseau ou de passerelle

Vous devez parfois supprimer un hôte, un sous-réseau ou une passerelle configuré(e), par exemple, lorsque vous pensez que cette entité n'est plus sécurisée. Pour supprimer un hôte, un sous-réseau ou une passerelle, procédez comme suit :

1. Cliquez sur l'onglet **Hôtes**.
2. Sélectionnez l'hôte, le sous-réseau ou la passerelle à supprimer.
3. Cliquez sur **Supprimer**.

Demande de présentation d'une clé ou d'un certificat spécifique

Vous pouvez demander à un hôte de présenter une clé ou un certificat spécifique lorsqu'il tente d'établir une AS. S'il ne le fait pas, le certificat ou la clé approprié(e), la communication sera impossible.

Pour demander à un hôte de présenter une clé ou un certificat spécifique

1. Si vous ne l'avez pas encore fait, ajoutez l'hôte, le sous-réseau ou la passerelle dans PGPnet (pour plus d'informations, reportez-vous à la section « Ajout d'un hôte, d'un sous-réseau ou d'une passerelle » à la page 169). PGPnet ajoute une entrée correspondante à la liste d'hôtes dans le panneau **Hôtes**.

2. Sélectionnez l'entrée dans le panneau **Hôtes**, puis cliquez sur **Editer**. La boîte de dialogue **Hôte/Passerelle** apparaît. La section **Authentification distante** apparaît dans la partie inférieure de cette boîte de dialogue.

3. Vous pouvez demander à l'hôte, au sous-réseau ou à la passerelle de présenter une clé PGP spécifique ou un certificat X.509 d'authentification.

   - Pour demander une clé PGP spécifique, cliquez sur le bouton radio **Clé PGP**. La boîte de dialogue Sélectionner la clé apparaît. Cliquez sur la clé appropriée, puis sur **OK**. La clé apparaît dans la zone **Authentification distante**. Pour fermer la boîte de dialogue Hôte / Passerelle, cliquez sur **OK**.

   - Pour demander un certificat X.509 spécifique, cliquez sur le bouton radio correspondant. La boîte de dialogue **Sélection d'un certificat X.509**apparaît. Cliquez sur le certificat approprié, puis sur **OK**. Ce certificat apparaît dans la zone **Authentification distante**. Boîte de dialogue Hôte / Passerelle Pour fermer la boîte de dialogue Hôte / Passerelle, cliquez sur **OK**.

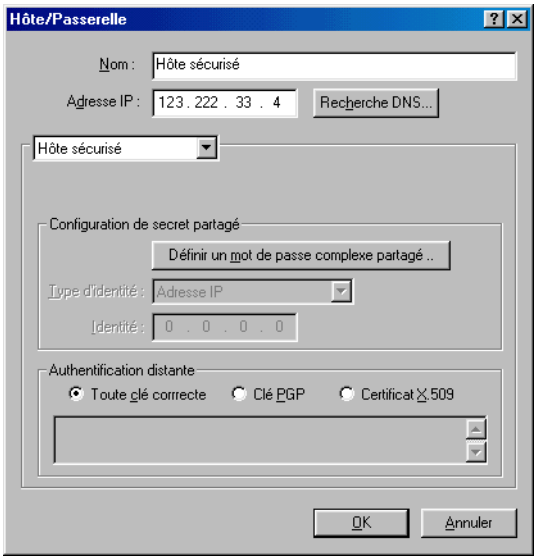


Figure 8-8. Hôte/Passerelle

Affichage du panneau Général

Pour afficher le panneau **Général**, sélectionnez Options dans le menu Affichage de la fenêtre PGPnet.

Utilisez le panneau **Général** pour effectuer les opérations suivantes :

- Activation / désactivation du mode expert
- Contrôle du niveau de sécurité des communications avec les hôtes
- Mémorisation des mots de passe complexes entre les connexions
- Demande clé d'authentification valides à tous les hôtes
- Définition de valeurs d'expiration pour les clés de configuration (IKE) et les clés principales (IPSEC) permettant d'établir des associations de sécurité avec d'autres hôtes configurés

Mode expert : ajout d'hôtes, de passerelles et de sous-réseaux sans utiliser l'Assistant

Si vous maîtrisez PGPnet, utilisez le **mode expert** (**Affichage—>Options—>Général**) afin d'ajouter et de modifier rapidement des hôtes, des passerelles et des sous-réseaux. Contrairement à l'Assistant qui vous guide étape par étape au cours du processus d'ajout, le **mode expert** de PGPnet ne vous présente qu'un seul formulaire pour l'ajout d'une nouvelle entrée.

REMARQUE : En mode expert, pensez à sélectionner, si vous ne l'avez pas encore fait, une clé ou un certificat d'authentification (**Affichage—>Options—> Authentication**).

Pour activer et utiliser le mode expert

1. Pour afficher le panneau **Général**, sélectionnez **Options** dans le menu **Affichage**.
2. Cliquez sur **Mode expert** (une coche apparaît).
3. Cliquez sur **OK**.
4. Cliquez sur l'onglet **Hôtes**. Pour afficher la boîte de dialogue **Hôte/Passerelle**, cliquez sur **Ajouter**.

Recherche DNS : adresse IP d'un hôte

Le mode expert de PGPnet comporte une fonction de recherche DNS permettant d'identifier l'adresse IP d'un hôte.

Pour utiliser la fonction de recherche DNS

1. Cliquez sur **Recherche DNS**. La boîte de dialogue correspondante apparaît.
2. Entrez le nom d'hôte du système dans la zone **Nom d'hôte à rechercher**, puis cliquez sur **Rechercher**. PGPnet recherche l'adresse IP du nom d'hôte entré.
    - Lorsque PGPnet trouve l'adresse IP, celle-ci apparaît à l'écran. Pour indiquer l'adresse IP dans le formulaire de modification d'hôte et de passerelle, cliquez sur **Utiliser**.

- Lorsque l'adresse IP de cet hôte s'avère introuvable, vous en êtes informé.

ASTUCE : Entrez le nom d'hôte du système dans la zone Nom de la boîte de dialogue Hôte / Passerelle, puis cliquez sur **Recherche DNS**. La fenêtre correspondante apparaît. Pour trouver l'adresse IP du nom d'hôte défini, cliquez sur **Rechercher**.

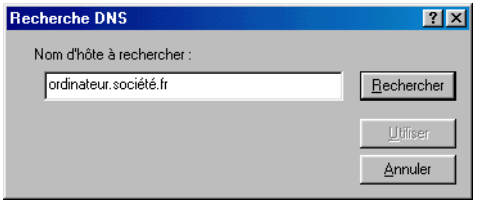


Figure 8-9. Boîte de dialogue Recherche DNS

Authentification distante

Les commandes situées dans la section **Authentification distante** de la boîte de dialogue **Hôte/Passerelle** vous permettent de demander à l'hôte distant de présenter une clé PGP ou un certificat X.509 spécifique lors de chaque tentative d'établissement d'une AS avec votre hôte. Une tentative de connexion sans présentation du certificat ou de la clé spécifié(e) sera rejetée par votre ordinateur. Le paramètre par défaut est **Toute clé corrrecte**.

IMPORTANT : Si vous sélectionnez une clé PGP spécifique ou un certificat X.509 pour une entrée de sous-réseau sécurisé, tous les utilisateurs de ce sous-réseau doivent utiliser la même clé d'authentification.

Pour identifier une clé d'authentification PGP spécifique à présenter par l'hôte distant

1. Cliquez sur **Clé PGP**.
2. Sélectionnez l'une des clés affichées dans la boîte de dialogue contextuelle, puis cliquez sur **OK**. La clé apparaît dans la section **Authentification distante** de la boîte de dialogue **Hôte/Passerelle**.
3. Cliquez sur **OK**.

Pour identifier un certificat d'authentification X.509 spécifique à présenter par l'hôte distant

1. Cliquez sur Certificat X.509.
2. Sélectionnez l'un des certificats affichés dans la boîte de dialogue contextuelle, puis cliquez sur **OK**. La clé apparaît dans la section **Authentification distante** de la boîte de dialogue **Hôte/Passerelle**.
3. Cliquez sur **OK**.

Désactivation du mode expert

Pour désactiver le mode expert

1. Pour afficher le panneau **Général**, sélectionnez **Options** dans le menu **Affichage**.
2. Cliquez sur **Mode expert** (une coche apparaît).
3. Cliquez sur **OK**.

Contrôle du niveau de sécurité des communications avec les hôtes

Vous utiliserez PGPnet principalement pour établir des communications sécurisées avec d'autres hôtes. Ses fonctions (cryptage, authentification et encapsulation) permettent la transmission sécurisée de vos données via Internet ou d'autres réseaux publics ou privés en toute sécurité. Vos données sont protégées lors de leur transfert via des réseaux et des ordinateurs qui ne sont pas sous le contrôle de votre entreprise. Toute tentative d'interception, de déchiffrement ou de modification des données effectuée par un pirate est impossible. Vos données sont intactes lorsqu'elles arrivent à leur destination finale.

PGPnet comporte des fonctions vous permettant de communiquer avec des hôtes non configurés (à savoir, des hôtes qui n'ont pas été ajoutés à la liste d'hôtes de PGPnet) et d'exiger des communications sécurisées avec tous les hôtes.

Options Autoriser des communications avec des hôtes non configurés et Exiger des communications sécurisées avec tous les hôtes

Ces deux options vous permettent de contrôler les ordinateurs avec lesquels vous communiquez et de minimiser le nombre de systèmes à ajouter à la liste d'hôtes.

Si la plupart des systèmes avec lesquels vous communiquez n'exécutent pas PGPnet, utilisez l'Assistant pour ajouter les hôtes sécurisés à la liste, puis cochez la case **Autoriser des communications avec des hôtes non configurés**. Vous pourrez ainsi communiquer à la fois avec les hôtes sécurisés identifiés dans la liste d'hôtes et avec tous les autres hôtes.

Si la plupart des systèmes avec lesquels vous communiquez exécutent PGPnet, utilisez l'Assistant pour ajouter les hôtes non sécurisés à la liste, puis cochez la case **Exiger des communications sécurisées avec tous les hôtes**. Vous pourrez ainsi communiquer à la fois avec les hôtes non sécurisés identifiés dans la liste d'hôtes et avec tous les autres hôtes compatibles IPSec.

Autoriser des communications avec des hôtes non configurés

Pour échanger des données ni confidentielles, ni sensibles avec des hôtes non configurés dans PGPnet, utilisez cette fonction (**Affichage—>Options—>Général**). Vous pouvez, par exemple, utiliser cette fonction si vous surfez régulièrement sur le Web. Ce paramètre est activé par défaut.

- Pour autoriser des communications avec des hôtes non configurés, cochez cette case.
- Pour interdire des communications avec des hôtes non configurés, décochez-la.

Exiger des communications sécurisées avec tous les hôtes

Pour exiger des communications sécurisées avec tous les hôtes, utilisez cette fonction (**Affichage—>Options—>Général**). Par exemple, si tous les systèmes de votre entreprise sont configurés avec PGPnet, utilisez cette fonction pour ne plus avoir à identifier chaque hôte.

Lorsque cette case est cochée, PGPnet négocie une AS avec chaque ordinateur cible avant d'autoriser toute communication. Ce paramètre est désactivé par défaut (la case n'est pas cochée).

- Pour demander à PGPnet de négocier des communications sécurisées avec tous les hôtes, cochez cette case.

- Pour autoriser des communications non sécurisées avec tous les hôtes, décochez-la.

REMARQUE : Si cette fonction est activée, la communication entre deux ordinateurs définis comme hôtes non sécurisés est toujours possible.

AVERTISSEMENT : Cette fonction de sécurité est conçue pour des environnements dans lesquels tous les ordinateurs sont configurés avec PGPnet. Lorsque cette fonction est activée (la case est cochée), la communication avec tout ordinateur non configuré avec PGPnet est impossible. Par conséquent, si vous êtes dans un evironnement qui n'est pas configuré avec PGPnet et que vous activez cette fonction, vous risquez de perdre le volume de données de votre trafic réseau.

Exiger une clé d'authentification correcte

Pour vérifier que les clés présentées par les hôtes distants sont correctes sur le trousseau de clés local, utilisez cette fonction (**Affichage—>Options—>Général**).

- Pour demander à PGPnet de vérifier que les clés présentées par les hôtes distants sont correctes sur le trousseau de clés local, activez ce paramètre (cochez la case correspondante). Utilisez-le si vous communiquez uniquement avec des hôtes utilisant des clés et des certificats corrects sur votre trousseau de clés.
- Pour demander à PGPnet d'accepter une clé, quelle que soit sa validité, désactivez ce paramètre (décochez la case correspondante). Utilisez-le lorsque vous exécutez PGPnet sur des serveurs (par exemple, serveurs de messagerie ou serveurs Web) autorisant la connectivité avec tout hôte client. Le serveur utilise la clé correcte pour s'identifier sur l'hôte client, mais il accepte toute clé présentée par cet hôte client. Dans ce cas, ce paramètre est désactivé (la case est décochée) pour le serveur, et activé (la case est cochée) pour l'hôte client. Pour que ce scénario fonctionne, l'hôte client doit disposer de la clé d'authentification fiable du serveur.

IMPORTANT : Lorsque cette fonction est désactivée (la case est décochée), elle prime sur le paramètre **Toute clé corrrecte** situé dans la section **Authentification** de la boîte de dialogue **Hôte/Passerelle**. Dans ce cas, le serveur accepte toutes les clés même si elles ne sont pas correctes. Pour exiger un certificat ou une clé spécifique pour chaque hôte, vous pouvez toujours utiliser la boîte de dialogue **Hôte/Passerelle**. Pour plus d'informations, reportez-vous à la section « Demande de présentation d'une clé ou d'un certificat spécifique » à la page 178.

REMARQUE : Toutes les authentifications effectuées au moyen de clés apparaissent dans le panneau **Historique**, et chaque entrée affiche l'ID de clé.

REMARQUE : Lorsque cette fonction est activée (la case est cochée) et qu'une clé PGP est sélectionnée comme mode d'**Authentification distante**, (boîte de dialogue **Hôte/Passerelle**) les deux exigences sont appliquées (l'ordinateur doit présenter la clé appropriée qui doit également être correcte).

Mémorisation des mots de passe complexes entre les connexions

Pour demander à PGPnet de mémoriser les mots de passe complexes entre les connexions, utilisez cette fonction (**Affichage—>Options—>Général**).

- Lorsque cette fonction est activée (la case est cochée), PGPnet conserve les mots de passe complexes entrés. Si vous quittez Windows, puis vous connectez à nouveau, vous n'aurez pas à ressaisir vos mots de passe complexes.
- Lorsque cette fonction est désactivée (la case est décochée) et que vous quittez Windows, les mots de passe complexes sont supprimés. Vous devrez les saisir à nouveau lors de votre prochaine connexion.

REMARQUE : Ceci s'applique uniquement en cas de connexion et de déconnexion de Windows. Lorsque cette fonction est activée et que vous quittez Windows, puis vous connectez à nouveau sous un autre nom d'utilisateur, vous n'aurez pas à ressaisir les mots de passe complexes. Ceci ne s'applique pas aux connexions et déconnexions de PGPnet.

L'utilisation d'une clé sans mot de passe complexe vous évite d'avoir à le mettre en mémoire. Vous pouvez procéder ainsi si votre ordinateur est automatisé, par exemple, un serveur.

- Pour demander à PGPnet de mémoriser des mots de passe complexes entre les connexions, cochez cette case.
- Dans le cas contraire, décochez-la.

Définition des valeurs d'expiration

Vous pouvez définir les valeurs d'expiration des clés de configuration (IKE) et des clés principales (IPSec). Ces clés permettent la création de vos associations de sécurité. Vous pouvez définir les valeurs en heure (**Durée**) ou en taille (**Méga-octets**).

La **Durée** est affichée sous le format suivant :

2j, 08h, 04m (la clé expire dans 2 jours, 8 heures et 4 minutes)

Les **Méga-octets** sont affichés sous le format suivant :

99 (la clé expire une fois que 99 méga-octets de données ont été transférés)

Notez que lorsque vous établissez une AS avec un autre hôte, PGPnet utilise les valeurs d'expiration les plus restrictives de l'un ou l'autre de ces deux hôtes. Par conséquent, une AS est susceptible d'arriver à expiration avant que la valeur maximale d'expiration que vous avez définie ne soit atteinte.

AVERTISSEMENT : Le fait de réduire la valeur par défaut pour les méga-octets peut entraîner plusieurs initialisations et négociations lors de la transmission de fichiers volumineux et, par conséquent, une interruption temporaire du fonctionnement réseau normal.

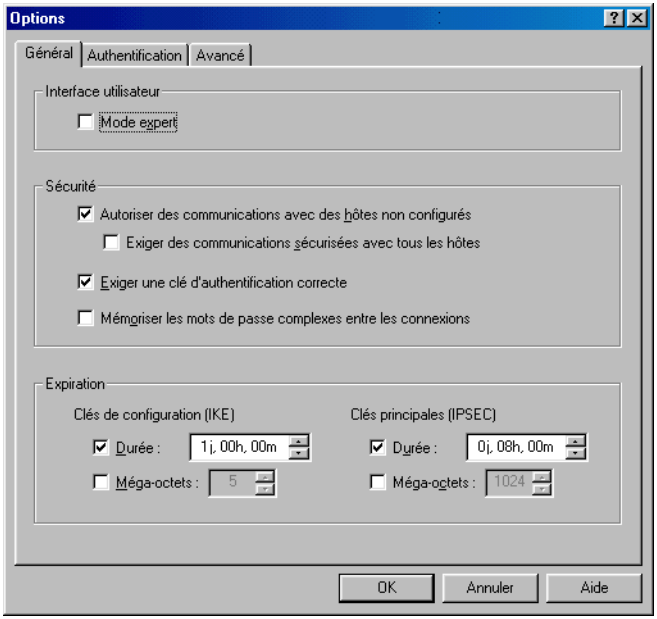


Figure 8-10. Panneau Général

Pour définir les valeurs d'expiration des clés de configuration (IKE)

1. Accédez au panneau **Général** (**Affichage—>Options**). Les informations d'**Expiration** apparaissent dans la section inférieure de ce panneau.
2. Pour définir la durée des clés de configuration, cochez la case **Durée**, puis utilisez les flèches Haut et Bas situées en regard de la zone correspondante ou entrez une valeur numérique pour les champs j, h et m.
3. Pour définir un nombre de **Méga-octets** pour les clés de configuration, cliquez sur **Méga-octets**, puis utilisez les flèches Haut et Bas ou entrez une valeur numérique.
4. Cliquez sur **OK**.

Pour définir les valeurs d'expiration des clés principales (IPSec)

1. Accédez au panneau **Général** (**Affichage—>Options**). Les informations d'**Expiration** apparaissent dans la section inférieure de ce panneau.
2. Pour définir la durée des clés principales, cliquez sur **Durée**. Utilisez les flèches Haut et Bas situées en regard de la zone **Durée** ou entrez une valeur numérique pour les champs j, h et m.
3. Pour définir un nombre de **Méga-octets** pour les clés principales, cochez la case **Méga-octets**, puis utilisez les flèches Haut et Bas ou entrez une valeur numérique.
4. Cliquez sur **OK**.

Authentification d'une connexion

Les commandes du panneau **Authentification** vous permettent d'effectuer les opérations suivantes :

- Sélectionnez vos fichiers de trousseaux de clés publiques et privées PGPnet comme trousseaux d'authentification actifs (**Fichiers de trousseaux de clés PGPnet**). Cette fonction vous permet de définir des fichiers de trousseaux de clés PGPnet indépendants.

  Les zones **Publiques** et **Privées** affichent initialement le trousseau de clés publiques de la personne ayant installé PGPnet (il s'agit généralement de l'administrateur). Pour sélectionner d'autres fichiers de trousseaux de clés, cliquez sur **Parcourir**.

Si vous ne disposez pas de fichiers de trousseaux de clés PGPnet, cliquez sur **Utiliser mes fichiers de trousseaux de clés PGP** pour indiquer à PGPnet d'utiliser les vôtres. Notez que lorsque vous cliquez sur ce bouton, PGPnet utilise les fichiers de trousseaux de clés PGP de l'utilisateur actuellement connecté à votre système. Lorsque vous cliquez sur **Utiliser mes fichiers de trousseaux de clés PGP**, les fichiers de trousseaux de clés publiques et privées sont réinitialisés en fonction de vos trousseaux de clés PGP.

- Pour authentifier votre ordinateur local, sélectionnez une clé PGP (**Authentification PGP**).
- Pour authentifier votre ordinateur local, sélectionnez un certificat X.509 (**Authentification X.509**).
- Une fois que vous avez cliqué sur **OK**, vous devez entrer le mot de passe complexe du certificat ou de la clé d'authentification sélectionné(e). Entrez-le, puis cliquez sur **OK**. Vous devez entrer ce mot de passe complexe lors de chaque connexion à PGPnet, sauf si la fonction **Mémoriser les mots de passe complexes entre les connexions** située dans le panneau **Général** est activée (la case est cochée).

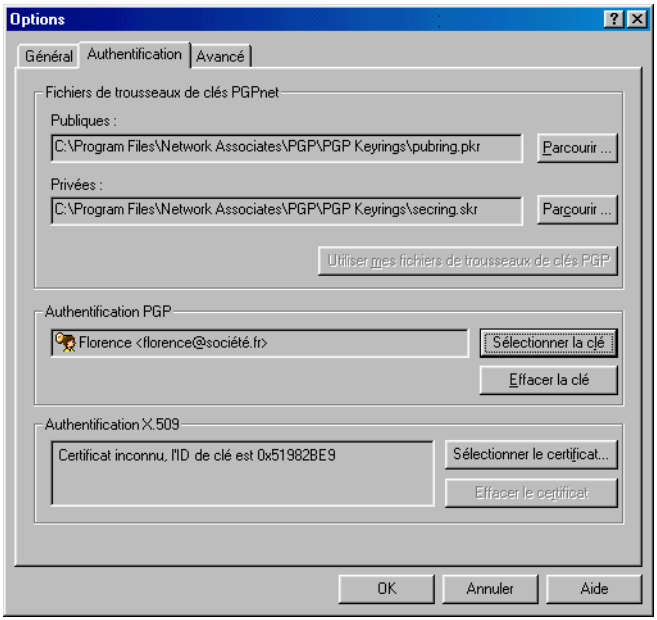


Figure 8-11. Panneau Authentification

Le tableau suivant décrit les boutons du panneau **Authentification**.

Bouton	Description
Bouton Parcourir	Affiche les boîtes de dialogue Sélection de fichiers de trousseaux de clés publiques et Sélection de fichiers de trousseaux de clés privées. Utilisez ces boîtes de dialogue pour sélectionner vos fichiers de trousseaux de clés PGPnet publiques et privées comme trousseau d'authentification actif.
Utiliser mes fichiers de trousseaux de clés PGP	Indique à PGPnet d'utiliser vos fichiers de trousseaux de clés PGP comme trousseau d'authentification actif.
Sélectionner la clé	Affiche la boîte de dialogue de sélection d'une clé PGP. Utilisez cette boîte de dialogue pour sélectionner une paire de clés permettant d'authentifier votre ordinateur. Entrez ensuite le mot de passe complexe de la clé sélectionnée.
Effacer la clé	Efface la clé PGP sélectionnée.
Sélectionner un certificat	Affiche la boîte de dialogue de sélection d'un certificat. Utilisez cette boîte de dialogue pour sélectionner un certificat X.509 permettant d'authentifier votre ordinateur. Entrez ensuite le mot de passe complexe de la clé à laquelle le certificat est associé.
Effacer le certificat	Efface le certificat X.509 sélectionné.

Panneau Avancé

AVERTISSEMENT : Les paramètres par défaut de ce panneau vous permettent de communiquer avec les utilisateurs de PGPnet ou de GVPN. Modifiez ces paramètres uniquement si vous êtes un utilisateur IPSec averti.

Le panneau **Avancé** (**Affichage—>Options**) affiche les **Propositions distantes autorisées** et les **Propositions** IKE et IPSec.

- La section **Propositions distantes autorisées** indique à PGPnet d'accepter toute proposition de la part d'autres utilisateurs et comportant tout élément coché (autorisé) dans ces zones, à l'exception des éléments Aucun relatifs à Chiffrement et Hachages. Les éléments Aucun doivent être cochés une fois toutes les précautions prises. Si vous cochez la case Aucun pour Chiffrements (cryptage), PGPnet accepte les propositions n'incluant pas de cryptage. Si vous cochez la case Aucun pour Hachages (authentification), PGPnet accepte les propositions n'incluant pas d'authentification.

- Les sections **Propositions** IKE et IPSec permettent d'identifier les propositions faites aux autres utilisateurs. Ils doivent accepter exactement les paramètres définis dans, au moins, l'une de vos propositions IKE ou IPSec.

Propositions distantes autorisées

La section **Propositions distantes autorisées** de ce panneau permet d'identifier les types de chiffrements, de hachages et de clés Diffie-Hellman autorisés par PGPnet. Seuls les utilisateurs IPSec avertis doivent apporter des modifications aux paramètres de ce panneau.

Les *chiffrements* sont des algorithmes utilisés pour le cryptage et le décryptage. Pour autoriser un type de chiffrement spécifique (CAST ou DES triple), cochez la case correspondante. Cochez la case Aucun après avoir pris toutes les précautions nécessaires, car elle indique à PGP d'accepter les propositions n'incluant pas de cryptage de la part d'autres utilisateurs.

Une *fonction de hachage* convertit une chaîne d'entrée de taille variable, puis la convertit en chaîne de sortie de taille fixe. Pour autoriser un type de hachage spécifique (SHA-1 ou RM5), cochez la case située à gauche du type correspondant. Cochez la case Aucun après avoir pris toutes les précautions nécessaires, car elle indique à PGP d'accepter les propositions n'incluant pas d'authentification de la part d'autres utilisateurs.

Une *fonction de compression* convertit une entrée de taille fixe en sortie de taille fixe. Il existe deux types de compression : LZS et Compresser. Pour autoriser un type de compression spécifique, cochez la case correspondante.

REMARQUE : Les fonctions LZS et Compresser optimisent les performances des communications à vitesse réduite, via des modems et RNIS, par exemple. Toutefois, elles diminuent les performances des communications à grande vitesse (par exemple, le modem câble, DSL, T-1 et T-3) en raison de la surcharge des routines de compression.

Diffie-Hellman est un protocole d'accord de clé. Pour autoriser une taille de clé spécifique (1 024 ou 1 536 bits), cochez la case correspondante.

Terme	Description
Chiffrements	Algorithme utilisé pour le cryptage et le décryptage. Types : CAST DES triple Lorsque la case Aucun est cochée, PGPnet accepte les propositions ne comportant pas d'authentification de la part d'autres utilisateurs.
Hachages	Une fonction de hachage convertir une chaîne d'entrée de taille variable en chaîne de sortie de taille fixe. Types : SHA-1 (algorithme de hachage sûr) RM5 (algorithme de résumé de message) Lorsque la case Aucun est cochée, PGPnet accepte les propositions ne comportant pas d'authentification de la part d'autres utilisateurs.
Diffie-Hellman	Protocole d'accord de clé. Tailles : 1 024 bits 1 536 bits
Compression	Crée une sortie de taille fixe comprimée à partir d'une entrée de taille fixe. Types : LZS Compresser REMARQUE : Les fonctions LZS et Compresser optimisent les performances des communications à vitesse réduite, via des modems et RNIS, par exemple. Toutefois, elles diminuent les performances des communications à grande vitesse (par exemple, le modem câble, DSL, T-1 et T-3) en raison du temps système pris par les routines de compression.

Pour ajouter un élément aux propositions distantes autorisées

1. Accédez à la fenêtre **Options** (**Affichage—>Options**).
2. Cliquez sur l'onglet **Avancé**.
3. Cliquez sur la case située à gauche de l'élément. Une coche apparaît.
4. Cliquez sur **OK**.

Pour supprimer un élément des propositions distantes autorisées

1. Accédez à la fenêtre **Options** (**Affichage—>Options**).
2. Cliquez sur l'onglet **Avancé**.
3. Cliquez sur la case située à gauche de l'élément. La coche est supprimée.
4. Cliquez sur **OK**.

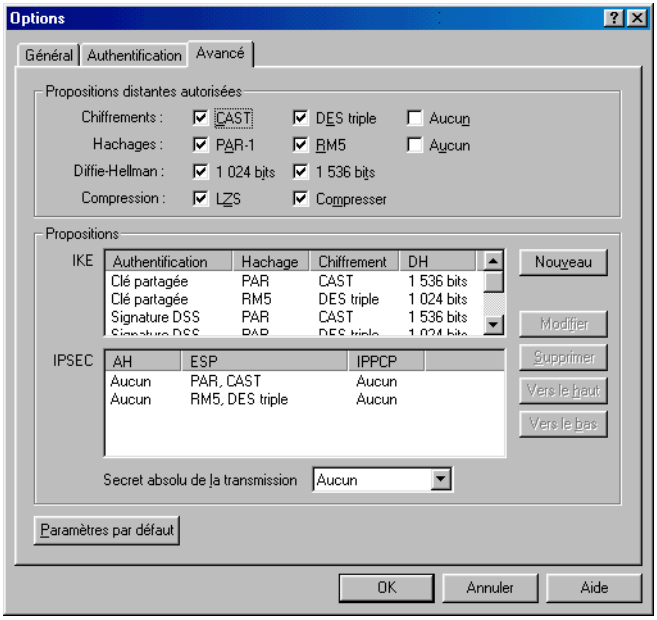


Figure 8-12. Panneau Avancé

Propositions

Pour ajouter, modifier, supprimer ou réorganiser vos propositions existantes, utilisez la section **Propositions** du panneau **Avancé**. Encore une fois, seuls les utilisateurs IPSec avertis doivent apporter des modifications à ce panneau. Les propositions IKE et IPSec indiquent à PGPnet les propositions à faire aux autres utilisateurs. Elles doivent être acceptées exactement telles que définies. Notez que PGPnet autorise au moins une proposition et, au plus, 16 propositions pour IKE et IPSec à la fois.

❑ **REMARQUE :** Les fonctions LZS et Compresser optimisent les performances des communications à vitesse réduite, via des modems et RNIS, par exemple. Toutefois, elles diminuent les performances des communications à grande vitesse (par exemple, le modem câble, DSL, T-1 et T-3) en raison du temps système pris par les routines de compression.

Le tableau suivant permet d'identifier les types d'authentifications, de hachages et de chiffrements, ainsi que les protocoles Diffie-Hellman utilisés dans les propositions IKE.

Terme	Description
Authentification	Moyen permettant de vérifier des informations, telles que l'identité. Types : Clé partagée (une clé secrète est partagée par plusieurs utilisateurs) Signature DSS (standard de signature numérique) Signature RSA
Hachage	Une fonction de hachage convertit une chaîne d'entrée de taille variable en chaîne de sortie de taille fixe. Types : SHA (algorithme de hachage sûr) RM5 (algorithme de résumé de message)
Chiffrement	Algorithme utilisé pour le cryptage et le décryptage. Types : CAST DES triple
DH (Diffie-Hellman)	Protocole d'accord de clé. Tailles : 1 024 bits 1 536 bits

Le tableau suivant identifie les types de AH, ESP et IPPCP utilisés dans les propositions IPSec.

Terme	Description
AH	En-tête d'authentification, un sous-protocole IPSec permettant la gestion de l'authentification uniquement. En outre, il authentifie divers éléments de l'en-tête IP. Ce sous-protocole est utile lorsque le cryptage ne s'avère pas nécessaire, par exemple, lorsqu'une communication est encapsulée via une passerelle à l'aide de l'AH. Types : SHA et RM5.
ESP	Sécurité par encapsulation de la charge utile, un sous-protocole IPSec permettant la gestion du cryptage et de l'authentification. Types de hachage : Aucun, SHA et RM5. Types de chiffrement : Aucun, CAST et DES triple.
IPPCP	Protocole de compression de la charge utile IP. Types : Compresser et LZS. REMARQUE : Les fonctions LZS et Compresser optimisent les performances des communications à vitesse réduite, via des modems et RNIS, par exemple. Toutefois, elles diminuent les performances des communications à grande vitesse (par exemple, le modem câble, DSL, T-1 et T-3) en raison du temps système pris par les routines de compression.

Secret absolu de la transmission

Toutes les propositions IPSec utilisent le même paramètre Diffie-Hellman : Aucun, 1 024 ou 1 536 bits.

Ajout d'une proposition IKE ou IPSec

Pour ajouter une proposition IKE ou IPSec

1. Accédez à la fenêtre **Options** (**Affichage—>Options**).
2. Cliquez sur l'onglet **Avancé**.
3. Cliquez sur **Nouveau**, puis sélectionnez IKE ou IPSec.
4. Effectuez les sélections appropriées dans la fenêtre contextuelle Proposition IKE ou IPSec.

5. Cliquez sur **OK**.
6. Si vous ajoutez une proposition IPSec, sélectionnez le paramètre Diffie-Hellman approprié (Aucun, 1 024 et 1 536) pour **Secret absolu de la transmission**. Toutes les propositions IPSec utilisent le même paramètre Diffie-Hellman.
7. Cliquez sur **OK**.

Modification d'une proposition IKE ou IPSec

Pour modifier une proposition IKE ou IPSec

1. Accédez à la fenêtre Options (**Affichage—>Options**).
2. Cliquez sur l'onglet **Avancé**.
3. Sélectionnez la proposition.
4. Cliquez sur **Editer**.
5. Apportez les modifications nécessaires dans la fenêtre contextuelle Proposition IKE ou IPSec.
6. Cliquez sur **OK** dans la fenêtre contextuelle.
7. Vérifiez le paramètre affiché dans la zone **Secret absolu de la transmission**. Notez que toutes les propositions IPSec utilisent le même paramètre Diffie-Hellman. Modifiez-le, le cas échéant.
8. Cliquez sur **OK** dans le panneau **Avancé**.

Figure 8-13. Boîte de dialogue Proposition IKE

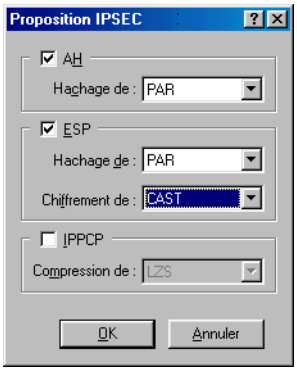


Figure 8-14. Boîte de dialogue IPSec

Suppression d'une proposition IKE ou IPSec

Pour supprimer une proposition IKE ou IPSec

1. Accédez à la fenêtre **Options** (**Affichage—>Options**).
2. Cliquez sur l'onglet **Avancé**.
3. Cliquez sur la proposition.
4. Cliquez sur **Supprimer**.
5. Cliquez sur **OK**.

Réorganisation des propositions IKE ou IPSec

Pour réorganiser des propositions IKE ou IPSec

1. Accédez à la fenêtre **Options** (**Affichage—>Options**).
2. Cliquez sur l'onglet **Avancé**.
3. Sélectionnez la proposition.
4. Pour déplacer la proposition vers le haut, cliquez sur **Déplacer vers le haut**. Pour déplacer la proposition vers le bas, cliquez sur **Déplacer vers le bas**.
5. Cliquez sur **OK**.

Bouton Paramètres par défaut

Utilisez ce bouton pour restaurer les paramètres par défaut de toutes les zones apparaissant à l'écran. Dans la plupart des cas, ces paramètres par défaut suffiront à établir les AS et à utiliser PGPnet.

Sélection de l'adaptateur réseau : modification de votre interface réseau sécurisée

Lors de l'installation de PGPnet, sélectionnez l'interface réseau à sécuriser sur votre ordinateur. Votre interface réseau est généralement une carte Ethernet, un encapsulateur de réseau étendu à accès distant ou une carte d'accès distant (représentant votre modem).

Utilisez le module de sélection de l'adaptateur de PGPnet (**Démarrer—>Programmes—>PGP—>Sélection de l'adaptateur réseau**) dans les cas suivants :

- Lorsque vous souhaitez sécuriser une interface réseau différente.
- Lorsque votre ordinateur vérifie votre protocole réseau et vos connexions d'adaptateur. Dans ce cas, PGPnet vous conseille de redémarrer votre système et de lancer la sélection de l'adaptateur réseau de PGPnet afin de sécuriser à nouveau une interface réseau.

Pour sécuriser une interface réseau différente (Windows 95/98)

1. Choisissez Sélection de l'adaptateur réseau dans le menu **Démarrer** (**Démarrer—>Programmes—> PGP—>Sélection de l'adaptateur réseau**). La boîte de dialogue correspondante apparaît et répertorie tous les autres adaptateurs.
2. Sélectionnez l'interface réseau appropriée, puis cliquez sur **OK**. PGP vous invite à redémarrer votre ordinateur.

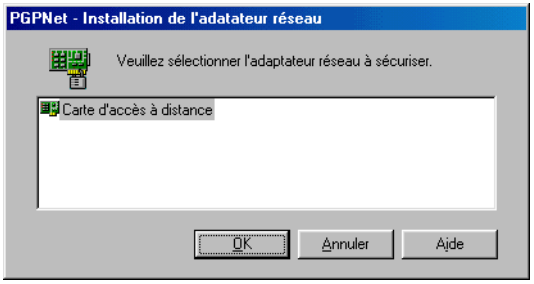


Figure 8-15. Boîte de dialogue Sélection de l'adaptateur réseau

3. Redémarrez votre ordinateur (vous devez le faire pour pouvoir exécuter les fonctions liées au réseau).

Pour sécuriser une interface réseau différente (Windows NT)

1. Choisissez Sélection de l'adaptateur réseau dans le menu **Démarrer** (**Démarrer—>Programmes—> PGP—>Sélection de l'adaptateur réseau**). La boîte de dialogue correspondante apparaît. Lisez le texte qu'elle contient.
2. Pour sécuriser une interface réseau différente, cliquez sur **OK**. PGP vérifie les connexions de votre ordinateur, puis se déconnecte de l'adaptateur auquel il était connecté.

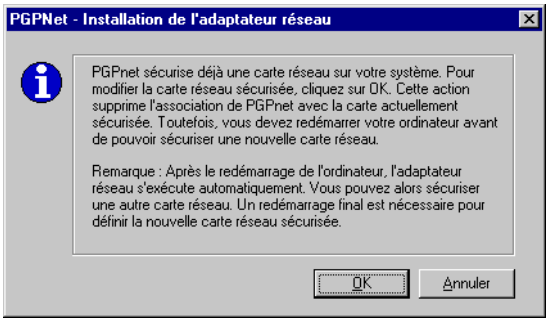


Figure 8-16. Boîte de dialogue Sélection de l'adaptateur réseau

3. Redémarrez votre ordinateur lorsque vous y êtes invité.
4. Lors du redémarrage, le module de sélection de l'adaptateur réseau est automatiquement lancé et vous invite à sélectionner un adaptateur réseau pour PGPnet.
5. Sélectionnez l'interface réseau appropriée. PGP vérifie les connexions de votre ordinateur, puis vous invite à le redémarrer.

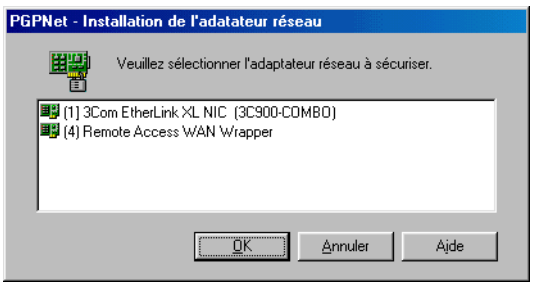


Figure 8-17. Boîte de dialogue Sélection de l'adaptateur réseau

6. Redémarrez votre ordinateur (vous devez le faire pour pouvoir exécuter les fonctions liées au réseau).

Pour sécuriser à nouveau une interface réseau après vérification des connexions (Windows NT)

1. Redémarrez votre ordinateur lorsque vous y êtes invité.
2. Lors du redémarrage, le module de sélection de l'adaptateur réseau est automatiquement lancé et vous invite à sélectionner un adaptateur réseau pour PGPnet.
3. Sélectionnez l'interface réseau appropriée. PGP vérifie les connexions de votre ordinateur, puis vous invite à le redémarrer.

Redémarrez votre ordinateur (vous devez le faire pour pouvoir exécuter les fonctions liées au réseau).

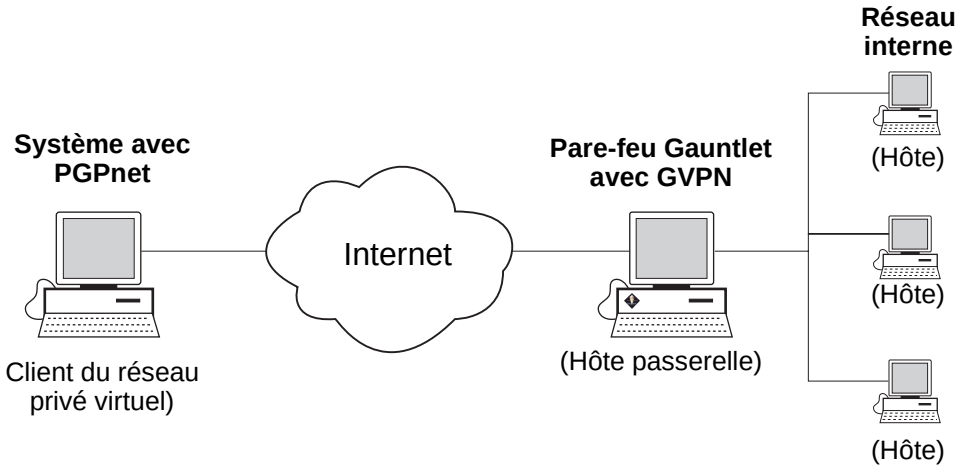
Création d'un réseau privé virtuel avec PGPnet 9

Ce chapitre décrit comment mettre en place un réseau privé virtuel à l'aide de PGPnet et de la fonction GVPN d'un pare-feu Gauntlet.

Pour l'exemple illustré dans ce chapitre, nous envisageons de créer un lien fiable entre les deux périphériques à l'aide du mode Client IKE et de l'authentification par certificat. Ce type de configuration d'un réseau privé virtuel est approprié dans le cas où un salarié d'entreprise accède au réseau d'entreprise protégé par un pare-feu via Internet et un fournisseur de services Internet ou s'il obtient son adresse IP de manière dynamique, via DHCP, par exemple.

Topologie

La topologie de ce réseau privé virtuel correspond à la structure suivante :



Terminologie relative aux pare-feux

Il est important de connaître certains termes spécifiques lors de la mise en place d'un réseau privé virtuel avec un pare-feu Gauntlet :

- **Secret pré-partagé et authentification par certificat** : les pare-feux Gauntlet prennent en charge deux méthodes d'authentification : le secret pré-partagé, où la ou les personnes configurant le lien utilisent un mot de passe complexe validé lors de l'authentification, et une authentification par certificat, où les deux périphériques du lien échangent des certificats lors de l'authentification.

- **Liens fiables et privés** : avec un lien fiable, les données provenant du client du réseau privé virtuel ignorent les serveurs proxy du pare-feu et parviennent directement à la destination concernée. Ignorez les fonctionnalités de sécurité du pare-feu uniquement si le client du réseau privé virtuel est parfaitement fiable, par exemple, s'il s'agit d'un membre de votre entreprise. Lors d'un lien privé, les serveurs proxy ne sont pas contournés. Le client du réseau privé virtuel doit alors s'authentifier au pare-feu pour accéder à la destination appropriée.

- **Interfaces internes et externes** : il s'agit de pare-feux dotés de deux interfaces physiques : une interface pour Internet (externe) et l'autre pour le réseau interne. Chaque interface possède sa propre adresse IP. L'interface utilisée pour la connexion à Internet est appelée interface externe et celle utilisée pour la connexion au réseau interne est appelée interface interne. Dans la plupart des cas, le pare-feu protège le réseau interne des données provenant de l'interface externe.

- **IKE Client et IPSec avec les modes IKE** : les pare-feux Gauntlet gèrent deux types de connexion : le mode IKE Client, fonctionnant uniquement avec l'authentification par certificat, mais prenant en charge les clients du réseau privé virtuel qui acquièrent leur adresse IP à l'aide de DHCP (c'est à dire qu'ils ne possèdent pas d'adresse IP fixe, mais une adresse différente leur est attribuée à chaque connexion) et le mode IPSec avec IKE qui prend en charge l'authentification par certificat ou du secret pré-partagé mais requiert que tous les hôtes ou sous-réseaux possèdent des adresses IP fixes (c'est-à-dire que le protocole DHCP n'est pas supporté).

  Le mode IKE Client est généralement mieux adapté aux configurations client / passerelle du réseau privé virtuel (PGPnet au pare-feu, par exemple). Cependant, le mode IPSec avec IKE convient davantage aux configurations passerelle / passerelle (pare-feu à pare-feu).

Mise en place du réseau privé virtuel

Pour mettre en oeuvre un réseau privé virtuel entre le système doté de PGPnet et le pare-feu Gauntlet à l'aide du mode Client IKE et de l'authentification par certificat, vous devez :

- Définir l'authentification par certificat
- Configurer le pare-feu Gauntlet
- Configurer PGPnet
- Mettre en place le réseau privé virtuel à l'aide de PGPnet

Tous ces éléments sont décrits dans les sections suivantes.

Définition de l'authentification par certificat

Dans le cadre de l'établissement d'un réseau privé virtuel, la première étape consiste à configurer les deux périphériques, en vue d'utiliser l'authentification par certificat. La validité des certificats est impérative pour garantir la fiabilité du lien entre les deux périphériques du réseau privé virtuel.

Pour plus d'informations sur l'obtention de certificats X.509 valides pour le pare-feu Gauntlet, reportez-vous au manuel Gauntlet Firewall Global Virtual Private Network User's Guide pour Windows NT ou UNIX (selon la version du pare-feu Gauntlet utilisée). Les documents sont livrés au format papier avec le pare-feu. Ils sont également disponibles sous la forme de fichiers PDF sur le CD d'installation.

Pour obtenir un certificat X.509 valide pour PGPnet (le client du réseau privé virtuel), vous devez récupérer le certificat CA par défaut auprès de l'autorité de certification (CA), considérée comme fiable par les deux périphériques sur le réseau privé virtuel (dans ce cas, votre CA d'entreprise). Ajoutez ensuite ce certificat à votre trousseau de clés, demandez un certificat pour PGPnet à la CA, puis récupérez-le pour PGPnet une fois émis. PGPkeys vous permet d'utiliser toutes ces fonctions.

Pour obtenir un certificat X.509 valide pour PGPnet (le client du réseau privé virtuel) :

1. Ouvrez votre navigateur Web et connectez-vous au site d'inscription de la CA.

   Par exemple, si votre entreprise utilise le serveur PKI Net Tools comme autorité de certification, le format de l'URL sera comparable à : **https://10.0.1.54**

   Si vous ne connaissez pas l'URL de ce site, contactez votre administrateur PGP ou PKI.

2. Recherchez et consultez le certificat CA par défaut.

   Par exemple, si votre entreprise utilise le serveur PKI Net Tools, cliquez sur le lien de téléchargement des certificats CA, puis consultez le certificat CA par défaut.

3. Copiez le bloc de clé (y compris pour le « -- Certificat désigné -- » et les extensions) pour le certificat CA par défaut, puis collez-le dans votre fenêtre PGPkeys.

   La boîte de dialogue d'importation de clés apparaît et importe le certificat CA par défaut sur votre trousseau de clés.

4. Validez le certificat CA par défaut en le signant avec votre clé.

   Vous souhaitez peut-être définir le certificat CA par défaut en tant que gestionnaire en chef de la sécurité, afin de considérer automatiquement comme fiables les certificats signés par son intermédiaire.

5. Affichez ses propriétés, puis définissez-le comme **Fiable**.

6. Choisissez **Options** dans le menu Edition de PGPkeys, puis cliquez sur l'onglet **CA**.

   L'onglet correspondant apparaît.

7. Dans la zone de texte **URL de l'autorité de certification**, entrez l'URL de la CA par défaut.

   Il s'agit de la même URL que celle utilisée dans l'étape 1.

   S'il s'agit d'une URL distincte pour la CA de révocation, entrez-la dans la zone de texte correspondante. Si vous ne connaissez pas l'URL de la CA de révocation, laissez ce champ vierge ou consultez l'administrateur PGP ou PKI de votre entreprise.

8. Dans la zone **Type**, sélectionnez le type de serveur PKI utilisé par votre entreprise : Serveur Net Tools PKI, VeriSign OnSite ou Entrust.

9. Cliquez sur Sélectionner le certificat, puis choisissez le certificat CA par défaut.

10. Cliquez sur **OK**.

11. Dans l'écran PGPkeys, sélectionnez votre paire de clés (ou clé privée). Choisissez **Ajouter**, puis **Certificat** dans le menu Clés.

    La boîte de dialogue Attributs du certificat apparaît.

12. Vérifiez les attributs et utilisez les boutons Ajouter, Editer et Supprimer pour effectuer toute modification nécessaire.

13. Cliquez sur **OK**.

    La boîte de dialogue PGP - Saisie d'un mot de passe complexe apparaît.

14. Entrez le mot de passe complexe pour votre paire de clés, puis cliquez sur **OK**.

    La demande de certificat est envoyée au serveur CA. Celui-ci s'authentifie alors auprès de votre ordinateur et accepte votre demande.

    A ce stade, l'administrateur PKI ou PGP de votre entreprise vérifie les informations de votre demande. Les informations d'identification et la clé publique sont rassemblées, puis signées numériquement avec le certificat de la CA. L'élément signé obtenu est votre nouveau certificat.

    L'administrateur vous envoie un message électronique (à l'aide de l'adresse e-mail fournie sur votre paire de clés), indiquant que votre certificat peut à présent être rapatrié.

15. Pour récupérer votre certificat et l'ajouter à votre paire de clés, ouvrez PGPnet, (le cas échéant), puis sélectionnez la clé PGP pour laquelle vous avez demandé un certificat.

16. Choisissez **Récupérer le certificat** dans le menu Serveur.

    PGP contacte le serveur CA, récupère automatiquement votre nouveau certificat X.509, puis l'ajoute à votre clé PGP.

Configuration du pare-feu Gauntlet

Pour mettre en place un réseau privé virtuel entre un système doté de PGPnet et d'un pare-feu Gauntlet, l'étape suivante consiste à configurer le pare-feu de manière appropriée.

REMARQUE : Cette procédure suppose qu'un pare-feu Gauntlet est installé. Pour plus d'informations, veuillez vous reporter à la documentation livrée avec le pare-peu.

IMPORTANT : Afin qu'un réseau privé virtuel constitué de PGPnet et de Gauntlet Firewall version 5.0, fonctionne correctement, le pare-feu doit correspondre à la passerelle par défaut pour les hôtes situés sur le sous-réseau sécurisé. Si les passerelles par défaut et sécurisée diffèrent (lorsque la passerelle par défaut est un routeur, par exemple), des problèmes peuvent survenir lors de l'acheminement du trafic en retour sur un réseau local Ethernet.

Cette procédure s'applique aux pare-feux Gauntlet Windows et UNIX. Les principales différences entre les deux sont notées dans le texte.

Pour configurer un pare-feu Gauntlet pour un réseau privé virtuel :

1. A l'aide du Gauntlet Firewall Manager, cliquez sur l'onglet VPN.

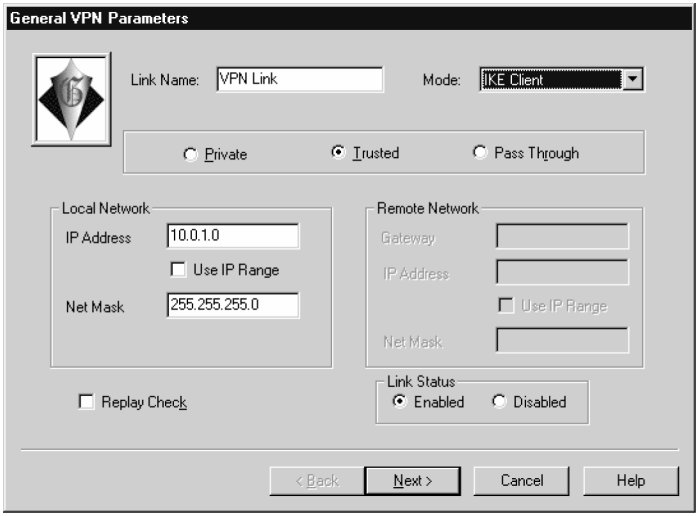
   L'écran correspondant apparaît.

   Sous UNIX, sélectionnez le répertoire **VPNs**, puis cliquez sur **Links**.

2. Cliquez sur **Add**.

   L'écran General VPN Parameters apparaît.

   Sous UNIX, cet écran est appelé Add GVPN Link Configuration.



3. Ajoutez un lien pour le réseau privé virtuel avec les paramètres suivants :

   Link Name : Entrez un nom descriptif

   Mode : IKE Client

   Link Type : Trusted

   IP Address : Entrez l'adresse IP de l'hôte ou du sous-réseau protégé par le pare-feu à utiliser dans le réseau privé virtuel (généralement, vous devez configurer un sous-réseau, afin que l'accès ne soit pas limité à un ordinateur)

   Use IP Range : Non coché

   Net Mask : Entrez le masque du sous-réseau entré dans le champ IP Address ou 255.255.255.255 si l'adresse IP dans le champ IP Address est un hôte et non un sous-réseau.

REMARQUE : Les informations relatives à l'adresse IP et au masque de sous-réseau entrées pour l'hôte ou le sous-réseau que vous êtres en train de configurer doivent êtres également entrées dans PGPnet.

   Replay Check : Non coché

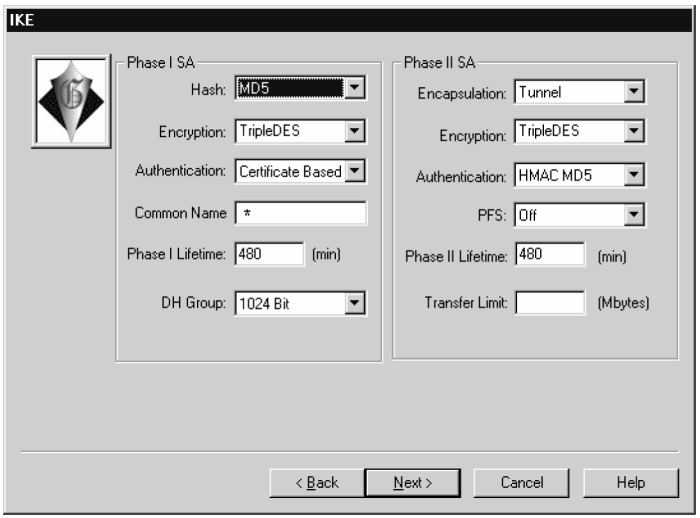
   Link Status : Activé

4. Pour passer à l'écran suivant, cliquez sur **Next**.

   Sous UNIX, cliquez sur **Link Details**.

   L'écran IKE apparaît.

Cet écran est appelé Edit IKE Configuration sous UNIX.



Utilisez les paramètres suivants :

Phase I SA

Hash : MD5

Encryption : TripleDES

Authentication : Certificate Based

Common Name : * (Sous UNIX, laissez ce champ vierge)

Phase I Lifetime : 480

DH Group : 1024 Bit

Phase II SA

Encapsulation : Tunnel

Encryption : TripleDES

Authentication : HMAC MD5

PFS : Off

Phase II Lifetime : 480

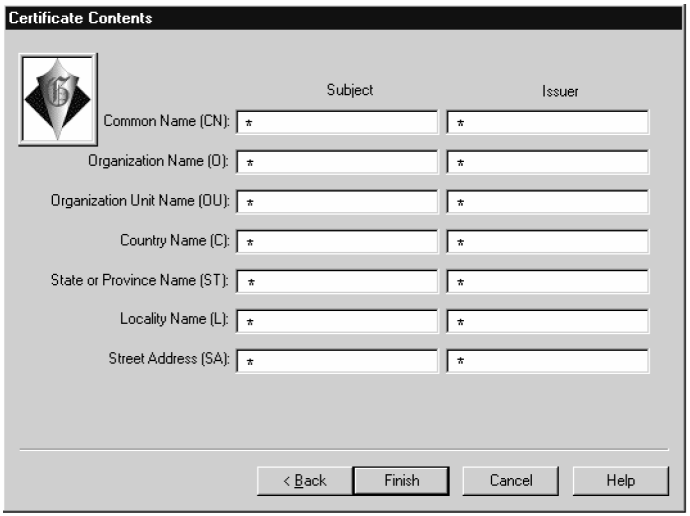
Transfer Limit : Laissez ce champ vierge

5. Pour passer à l'écran suivant, cliquez sur **Next**.

   Sous UNIX, cliquez sur **Certificate Contents**.

L'écran correspondant apparaît. Chaque champ doit comporter un astérisque (*).

Cet écran est appelé Client Certificate Configuration sous UNIX. Tous les champs doivent rester vierges, n'entrez pas d'astérisques.



6. Cliquez sur **Finish**, puis appliquez les modifications apportées au pare-feu.

   Sous UNIX, cliquez sur **OK**, puis appliquez les modifications apportées au pare-feu.

Configuration de PGPnet

Pour mettre en place un réseau privé virtuel entre un système constitué de PGPnet et d'un pare-feu Gauntlet, l'étape suivante consiste à configurer PGPnet de manière appropriée.

REMARQUE : Cette procédure suppose que PGP version 5.5 ou ultérieure est déjà installé, ainsi que le composant PGPnet.

Dans cet exemple, nous allons procéder à la configuration des communications sur un hôte ou un sous-réseau non sécurisé protégé par une passerelle sécurisée.

REMARQUE : La communication avec un hôte sécurisé protégé par une passerelle sécurisée requiert l'installation de la version 5.0 ou ultérieure de Gauntlet Firewall for UNIX ou la version 5.5 ou ultérieure de Gauntlet Firewall for Windows NT.

Pour configurer PGPnet pour le réseau privé virtuel à l'aide de l'Assistant d'ajout d'hôtes :

1. Ouvrez PGPnet, puis cliquez sur l'onglet **Hôtes**.
2. Dans l'onglet Hôtes, cliquez sur **Ajouter**.

   L'Assistant d'ajout d'hôtes apparaît.
3. Lisez le texte à l'écran, puis cliquez sur **Suivant**.
4. Sélectionnez **Passerelle** pour le type d'hôte, puis cliquez sur **Suivant**.

   Si vous souhaitez communiquer avec un hôte protégé par un pare-feu, vous devez d'abord configurer l'hôte de passerelle (le pare-feu), puis l'hôte situé derrière le pare-feu.
5. Entrez un nom descriptif pour l'hôte, puis cliquez sur **Suivant**.
6. Entrez l'adresse IP de l'hôte (à savoir l'adresse IP de l'interface externe du pare-feu), puis cliquez sur **Suivant**.
7. Cochez la case **Utiliser uniquement la sécurité cryptographique de clés publiques**, puis cliquez sur **Suivant**.

   Il vous est à présent demandé si vous souhaitez ajouter un hôte ou un sous-réseau.
8. Cochez **Oui**, puis cliquez sur **Suivant**.
9. Effectuez les sélections appropriées (Hôte ou Sous-réseau), puis cliquez sur **Suivant**.

   Il s'agit de l'hôte ou du sous-réseau protégé par le pare-feu avec lequel vous souhaitez communiquer.

IMPORTANT : Dans PGPnet, vous devez conserver la même configuration, Hôte ou Sous-réseau, que celle du pare-feu Gauntlet. Ainsi, si vous avez entré l'adresse IP et le masque d'un sous-réseau dans l'étape 3 de la procédure pour configurer le pare-feu Gauntlet, vous devez entrer l'adresse IP et le masque du même sous-réseau dans PGPnet.

10. Cochez la case **Autoriser des communications non sécurisées**, puis cliquez sur **Suivant**.
11. Attribuez un nom descriptif à l'hôte ou au sous-réseau ajouté, puis cliquez sur **Suivant**.

12. Entrez l'adresse IP de l'hôte ou du sous-réseau (et le masque de sous-réseau, le cas échéant), puis cliquez sur **Suivant**.

    Les informations relatives à l'adresse IP ***doivent*** être identiques à celles entrées dans l'étape 3 de la procédure pour configurer le pare-feu Gauntlet.

13. Continuez d'ajouter les hôtes et/ou les sous-réseaux requis pour votre configuration. Une fois terminé, sélectionnez Non, puis cliquez sur **Suivant**.

14. Si aucune clé n'a été définie pour l'authentification, un écran vous invitant à en sélectionner une apparaît. Cliquez sur **Sélectionner le certificat**. Choisissez ensuite le certificat X.509 ajouté, puis cliquez sur **Suivant**.

15. Cliquez sur **Terminer**.

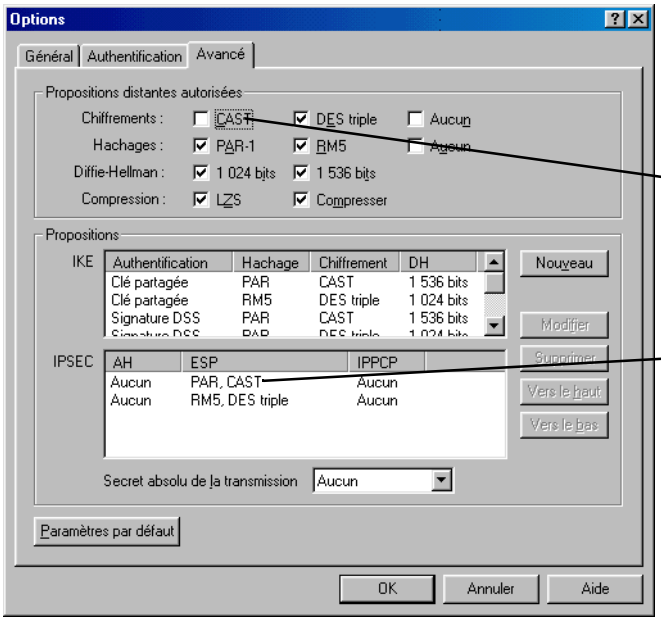
16. Si vous avez spécifié une clé d'authentification, vous êtes invité à entrer votre mot de passe complexe. Entrez-le, puis cliquez sur **OK**.

    L'onglet Hôtes apparaît.

17. Utilisez les paramètres par défaut de PGPnet, sauf si vous souhaitez définir les valeurs d'expiration de l'association de sécurité (dans l'onglet Général de l'écran Options).

IMPORTANT : Si vous mettez en place un réseau privé virtuel avec un hôte ou un sous-réseau protégé par Gauntlet Firewall for Windows NT version 5.0, vous devez désélectionner CAST dans la liste Propositions distantes autorisées. Pour ce faire, choisissez Options dans le menu Affichage de PGPnet. Cliquez sur l'onglet Avancé, puis décochez l'option CAST.

Si vous mettez en place un réseau privé virtuel avec un hôte ou un sous-réseau protégé par Gauntlet Firewall for UNIX version 5.0, vous devez déplacer en haut de la liste des propositions IPSec la proposition IPSec utilisé (dans cet exemple, RM5, DES triple). Pour ce faire : choisissez Options dans le menu Affichage de PGPnet. Cliquez ensuite sur l'onglet Avancé et recherchez les propositions IPSec. Dans la colonne ESP, cliquez sur RM5, DES triple, puis sur Déplacer vers le haut jusqu'à ce RM5, DES triple se trouve en haut de la liste, puis cliquez sur OK.



Pour un réseau privé virtuel avec Gauntlet Firewall for Windows NT 5.0, CAST doit être désélectionné.

Pour un réseau privé virtuel avec Gauntlet Firewall for UNIX 5.0, la proposition IPSec utilisée (dans cet exemple, RM5, DES triple) doit se trouver en haut de la liste des propositions IPSec.

Mise en place d'un réseau privé virtuel à l'aide de PGPnet

Pour mettre en oeuvre un réseau privé virtuel entre un système avec PGPnet et un pare-feu Gauntlet, l'étape finale consiste à mettre en place le réseau privé virtuel (appelé association de sécurité dans la terminologie PGPnet) à l'aide de PGPnet.

Pour mettre en place un réseau privé virtuel à l'aide de PGPnet :

1. Ouvrez PGPnet, puis cliquez sur l'onglet **Hôtes**.
2. Cliquez sur le nom de l'hôte (le pare-feu) configuré.
3. Si votre certificat X.509 a déjà été défini comme votre clé d'authentification, passez à l'étape 10. Si ce n'est pas le cas ou si vous n'en êtes pas sûr, passez à l'étape 4.
4. Choisissez **Options** dans le menu Affichage.

   L'écran correspondant apparaît.
5. Cliquez sur l'onglet **Authentification**.
6. Dans l'onglet Authentification, cliquez sur **Sélectionner le certificat**.

   La liste des certificats X.509 situés sur votre trousseau de clés apparaît.

7. Cliquez sur le nom du certificat à utiliser pour vous authentifier, puis cliquez sur **OK**.
8. Pour fermer l'écran Options, cliquez à nouveau sur **OK**.

   Une boîte de dialogue vous invite à entrer le mot de passe complexe de la clé sélectionnée.
9. Entrez-le, puis cliquez sur **OK**.

   L'écran Hôtes apparaît.
10. Cliquez sur le signe (+) situé en regard de l'hôte (le pare-feu) configuré.

    Une liste des entrées d'hôtes (hôtes ou sous-réseaux protégés par la passerelle) apparaît.
11. Pour commencer à communiquer avec un hôte ou un sous-réseau non sécurisé, cliquez sur l'hôte auquel vous souhaitez vous connecter, puis sur **Connecter**.

    Si votre configuration est correcte, les protocoles IPSec établissent une association de sécurité entre le client du réseau privé virtuel (PGPnet) et le pare-feu Gauntlet.

    Une fois l'association de sécurité créée, un point vert apparaît à droite de l'hôte dans la colonne AS.
12. Cliquez sur l'onglet **Etat**.

    L'association de sécurité est répertoriée.
13. Dans le cas contraire, cliquez sur l'onglet **Journal** pour connaître la raison du problème.

REMARQUE : Pour plus d'informations sur l'établissement d'une association de sécurité, sur les erreurs notées dans le journal, ainsi que sur la configuration de PGPnet, reportez-vous au chapitre PGPnet.

Dépannage de PGP A

Vous trouverez dans cette annexe des informations relatives aux problèmes ayant pu survenir lors de l'utilisation de PGP, ainsi que des solutions.

Erreur	Cause	Solution
Authentification rejetée par la connexion SKEP distante	L'utilisateur situé sur le côté distant de la connexion de fichier de partage réseau a rejeté la clé que vous avez fournie pour authentification.	Utilisez une autre clé pour authentifier la connexion de fichier de partage réseau ou contactez l'utilisateur distant pour lui assurer que la clé que vous utilisez est valide.
Cette clé est déjà signée par la clé de signature spécifiée.	Une clé déjà signée ne peut pas l'être une seconde fois.	Vous avez peut-être sélectionné la mauvaise clé. Dans ce cas, sélectionnez une autre clé à signer.
Des parties de clé ne peuvent être combinées.	Vous avez cherché à combiner la même partie de clé à deux reprises.	Si les parties de clé reçues proviennent d'un fichier de parties de clé, essayez de sélectionner un autre fichier. Si les parties reçues proviennent du réseau, il est possible que vous deviez contacter l'utilisateur situé sur un système distant pour lui demander d'envoyer une autre série de parties.
Données aléatoires disponibles insuffisantes.	Le générateur de nombres aléatoires nécessite davantage d'entrées pour générer des nombres aléatoires corrects.	Lorsque vous y serez invité, déplacez votre pointeur ou appuyez sur des touches de façon aléatoire pour générer des entrées.
Erreur dans le système de noms de domaines	L'adresse de destination fournie est incorrecte ou votre connexion réseau est mal configurée.	Vérifiez que l'adresse de destination fournie est correcte. Si cela est le cas, vérifiez votre connexion réseau.
Erreur survenue lors de l'écriture du trousseau de clés ou du fichier exporté.	L'écriture de données dans un fichier a échoué.	Votre disque dur est peut-être saturé ou, si le fichier est placé sur une disquette, celle-ci n'est pas insérée dans le lecteur correspondant.
Erreur survenue lors de l'ouverture ou de l'écriture du trousseau de clés ou du fichier de sortie.	Un fichier requis n'a pas pu être ouvert.	Assurez-vous que vos options PGP sont correctement paramétrées. Si vous avez récemment supprimé des fichiers dans le répertoire où PGP est installé, celui-ci doit éventuellement être à nouveau installé.

Erreur	Cause	Solution
Impossible de crypter vers la clé spécifiée, car elle est en signature seule.	La clé sélectionnée peut être utilisée uniquement pour la signature.	Sélectionnez une autre clé ou générez une nouvelle clé pouvant crypter des données.
Impossible de signer avec la clé spécifiée, car elle est en cryptage seul.	La clé sélectionnée peut être utilisée uniquement pour le cryptage.	Sélectionnez une autre clé ou générez une nouvelle clé pouvant signer des données.
Impossible de trouver des clés secrètes dans votre trousseau de clés.	Votre trousseau ne comporte aucune clé privée.	Générez votre propre paire de clés dans PGPkeys.
Impossible de trouver la clé spécifiée dans votre trousseau de clés.	La clé nécessaire au décryptage du message en cours n'est pas sur votre trousseau.	Demandez à l'expéditeur du message de le renvoyer en veillant à le crypter vers votre clé publique.
Impossible d'effectuer l'action en raison d'une opération incorrecte sur des fichiers.	La lecture ou l'écriture de données dans un fichier a échoué.	Le fichier est probablement altéré. Si possible, essayez de modifier vos préférences PGP afin d'utiliser un autre fichier.
Impossible d'exécuter cette opération, car ce fichier est en lecture seule ou protégé. Si vous stockez vos fichiers de trousseaux de clés sur un support amovible, celui-ci n'est peut-être pas inséré dans le lecteur.	Un fichier requis est paramétré en lecture seule ou est en cours d'utilisation par un autre programme.	Fermez les programmes susceptibles d'accéder aux mêmes fichiers que ceux utilisés par le programme en cours. Si vous conservez vos fichiers de trousseaux de clés sur disquette, assurez-vous que celle-ci est insérée dans le lecteur.
Impossible d'exécuter l'opération demandée car la mémoire tampon de sortie est de taille insuffisante.	La sortie est trop grande par rapport à la capacité de traitement des tampons internes.	Si vous cryptez ou signez, il est possible que vous deviez découper le message en petits éléments et crypter/signer chacun d'entre eux successivement. Si vous décryptez ou procédez à une vérification, demandez à l'expéditeur de crypter/signer des éléments plus petits et de vous les renvoyer.
Le fichier de préférences administratives est introuvable	Le fichier de préférences configuré par votre administrateur PGP, généralement le personnel informatique, est manquant.	Réinstallez PGP sur votre ordinateur. Si, toutefois, ce message continue à apparaître, informez-en votre administrateur PGP. Il devra vous fournir un nouveau programme d'installation PGP.

Erreur	Cause	Solution
Le fichier de trousseaux de clés est altéré.	La lecture ou l'écriture de données dans un fichier a échoué.	Un fichier est probablement altéré ou manquant. Il peut s'agir du fichier de trousseaux de clés. Si possible, essayez d'utiliser un autre nom de fichier ou un autre chemin.
Le fichier d'entrée spécifié n'existe pas.	Le nom de fichier entré n'existe pas.	Recherchez le nom et le chemin exacts du fichier souhaité.
Le message ou les données contiennent une signature séparée.	La signature du message/fichier est située dans un fichier séparé.	Cliquez deux fois sur le fichier de signature séparé en premier lieu.
Le mot de passe complexe entré ne correspond pas à celui affecté à la clé.	Le mot de passe complexe entré est incorrect.	Il est possible que la touche des majuscules soit enfoncée ou que vous ayez mal saisi le mot de passe complexe. Veuillez réessayer.
Le temps d'évaluation pour le cryptage et la signature PGP est expiré. Opération annulée.	Le temps d'évaluation du produit a expiré.	Téléchargez la version gratuite ou achetez la version commercialisée du produit.
Le trousseau de clés contient un paquet PGP erroné (altéré).	Le message PGP sur lequel vous travaillez ou votre trousseau de clés est altéré.	S'il s'agit d'un message que vous utilisez, demandez à l'expéditeur de vous le renvoyer. Si votre trousseau est en cause, essayez de le restaurer à partir de sa copie de sauvegarde.
L'ID utilisateur spécifié n'a pas été ajouté, car il existe déjà dans la clé sélectionnée.	Il est impossible d'ajouter un ID utilisateur à une clé si celle-ci en comporte déjà un identique.	Essayez d'ajouter un autre ID utilisateur ou supprimez d'abord celui qui est identique.
Mémoire insuffisante de la bibliothèque de PGP.	Mémoire insuffisante du système d'exploitation.	Fermez tous les programmes activés. En cas d'échec, cela signifie que votre ordinateur requiert davantage de mémoire.
Prise non connectée.	La connexion réseau au serveur de certificats PGP ou celle du fichier de parties de clé a été coupée.	Essayez de rétablir la connexion en répétant la procédure employée pour l'établir. En cas d'échec, vérifiez votre connexion réseau.

Transfert de fichiers entre Mac OS et Windows

B

Le transfert de fichiers avec Mac OS est un problème classique lors de l'utilisation de tout type de logiciel d'échange de données, tel que les applications de messagerie, FTP, les utilitaires de compression et PGP. Cette annexe a pour objectif d'expliquer comment ce problème a été résolu de manière définitive avec la version 5.5.x de PGP et d'examiner le mode de communication avec les versions précédentes de PGP.

Mac OS conserve les fichiers différemment des autres systèmes d'exploitation. Le format du fichier texte sous Mac OS est également différent. Les fichiers Mac OS sont en réalité deux fichiers distincts, comprenant un segment de données et un segment de ressources. Pour envoyer un fichier de Mac OS vers Windows sans perdre aucune donnée, les deux segments doivent fusionner pour ne plus en former qu'un seul. La méthode classique de conversion d'un fichier Mac OS en un seul fichier, afin de le transférer sur un autre Macintosh ou PC sans perdre aucune de ses parties, est appelée MacBinary.

Le problème est que, sans logiciel adapté, Windows et les autres plates-formes ne peuvent pas comprendre le format MacBinary de manière inhérente. Dans le cas où un fichier au format MacBinary n'a pas pu être converti en un fichier Windows, le fichier obtenu est inutilisable. Des utilitaires tiers Windows permettent de convertir ce fichier pour pouvoir l'utiliser, mais recourir à cette méthode peut s'avérer peu pratique.

Les versions précédentes de PGP et la plupart des utilitaires disponibles de nos jours sur le marché tentent généralement d'ignorer ce problème autant que possible et donnent libre cours à l'utilisateur quant au choix de conversion d'un fichier sous MacBinary lors de l'envoi à partir d'un système Mac OS. Ainsi, le choix d'envoyer le fichier avec MacBinary sans risquer de perdre aucune donnée ou sans MacBinary, en espérant qu'aucune donnée importante ne sera perdue, dépend de l'utilisateur, qui bien souvent ne sait pas quelle est la bonne décision à prendre. Cette décision dépend en fait de la destination du fichier : Windows ou Mac OS. Que se passe-t'il si vous envoyez ce fichier sur les deux plates-formes à la fois ? Aucune solution n'est envisageable pour résoudre ce problème avec les anciennes versions de PGP et de nombreux autres utilitaires. Ce problème a causé une grande confusion et un grand désagrément auprès des utilisateurs.

Le processus inverse, consistant à envoyer un fichier de Windows vers Mac OS, a également été considéré comme un problème majeur. Windows utilise les extensions des noms de fichiers, comme .doc, pour identifier le type d'un fichier. Mac OS ne reconnaît pas ces extensions. Ces fichiers sont envoyés sur un Macintosh sans aucune information relative au créateur ou au type du fichier. Pour rendre les fichiers utilisables à leur réception, il est nécessaire d'effectuer des opérations obscures dans la boîte de dialogue d'ouverture du créateur. Dans la plupart des cas, il est également nécessaire que l'utilisateur comprenne manuellement les codes de créateur et de type Mac OS en les définissant dans un utilitaire tiers.

Heureusement, les dernières versions de PGP (versions 5.5 à 6.5) permettent de résoudre ce problème. Si tous les utilisateurs PGP disposent des dernières versions de ce logiciel, plus personne n'aura à se soucier de l'envoi de fichiers de Mac OS vers Windows et inversement.

Transfert de Mac OS vers Windows

Lors du cryptage ou de la signature d'un fichier, trois options sont disponibles sous Mac OS :

- **MacBinary : Oui.** Cette option est recommandée pour tous les cryptages de fichiers à l'intention d'un autre utilisateur possédant la version 5.5 ou ultérieure de PGP sur tout type de plate-forme. Ainsi, les utilisateurs Mac OS recevront le fichier souhaité et la version Windows décodera automatiquement le fichier au format MacBinary, qui sera doté d'une extension .doc pour Microsoft Word ou .ppt pour Microsoft PowerPoint. PGP comprend des informations sur la plupart des extensions de nom de fichier et des codes de créateur Macintosh des applications les plus courantes. Dans les cas où le fichier est de type inconnu ou qu'il peut être utilisé uniquement sous Mac OS, telle qu'une application Mac OS, le fichier est conservé au format MacBinary, pour lui permettre ensuite d'être transmis sur un Macintosh sans aucune perte de données.

- **MacBinary : Non.** Si vous communiquez avec des utilisateurs qui disposent d'une ancienne version de PGP, la décision d'utiliser ou non le format MacBinary revient généralement à l'expéditeur, comme pour la plupart des autres programmes et des versions précédentes de PGP pour Mac OS. Lorsque vous envoyez un fichier sur un PC avec une ancienne version, si vous savez que le fichier peut être lu par les applications Windows sans utiliser MacBinary, sélectionnez cette option. Il s'agit de la plupart des fichiers qui sont généralement multi plates-formes, tels que ceux créés par les applications Microsoft Office, les fichiers graphiques, les fichiers compressés, etc. L'expéditeur ou le destinataire doit attribuer manuellement un nouveau nom au fichier reçu pour obtenir l'extension de nom de fichier correcte sous Windows. Cette action est nécessaire, car le destinataire Windows ne dispose pas des informations relatives au créateur généralement converties au format MacBinary.
- **MacBinary : Intelligent.** Dans certains cas, cette option s'avère utile lors de la communication avec des utilisateurs de versions antérieures de PGP. Cette option vous permet de choisir d'utiliser ou non MacBinary en fonction d'une analyse des données réelles du fichier. Si le fichier correspond à l'un des types figurant dans la liste suivante, le format MacBinary ne sera pas utilisé. Ainsi, il sera lisible sur tout PC disposant d'une version quelconque de PGP :
  - Fichier compressé PKzip
  - Fichier compressé Lempel-Ziv
  - Fichier au format MIDI
  - Fichier compressé PackIt
  - Fichier graphique GIF
  - Fichier compressé StuffIt
  - Fichier compressé Compactor
  - Fichier compressé Arc
  - Fichier graphique JPEG

Comme vous pouvez le constater, seul un nombre limité de fichiers pourront être lus par les anciennes versions de PGP sur d'autres plates-formes à l'aide de l'option Intelligent. Tout autre type de fichier reçu sur un PC doté d'une ancienne version de PGP sera illisible sans la suppression du codage MacBinary à l'aide d'un utilitaire tiers. D'autre part, sur PC, l'extension du fichier ne sera pas non plus correcte, sauf si cette extension a été ajoutée manuellement par l'expéditeur. Lors de l'utilisation du mode Intelligent, le fichier obtenu peut ne pas correspondre à l'original lors de son envoi sur un Macintosh, car les codes de créateur et de type de fichier risque d'être perdus. Ce mode a été conservé principalement du fait qu'il était présent dans la version 5.0 de PGP et que certains utilisateurs peuvent avoir uniquement besoin d'envoyer des fichiers de ce type. Cette option est déconseillée dans la plupart des cas.

En résumé, si vos destinataires disposent des versions 6.x uniquement, sélectionnez toujours MacBinary : Oui (par défaut). Ainsi, vous n'aurez plus à vous soucier si votre environnement utilise la version 6.x de PGP uniquement. Lors de l'envoi de fichiers à des utilisateurs disposant d'anciennes versions, vous devez sélectionner MacBinary : Non pour les types de fichiers multi plates-formes et MacBinary : Oui pour les fichiers ne pouvant pas être lus par les utilisateurs PC (comme une application Mac OS, par exemple).

REMARQUE : PGP version 5.0 ne dispose pas d'une option MacBinary : Non. Pour envoyer des types de fichiers sans MacBinary, qui ne figurent pas dans la liste MacBinary : Intelligent, vers un PC utilisant la version 5.0, le fichier doit être défini manuellement sur l'un des codes de créateur et de type de fichier dans la liste Intelligent avant d'être envoyé.

Réception de fichiers Windows sous Mac OS

Lors du décryptage, les versions 5.5.x et ultérieures de PGP tentent de convertir automatiquement les extensions de nom pour les fichiers qui ne sont pas au format MacBinary en informations relatives au type et au créateur Mac OS. Par exemple, si un utilisateur Windows vous envoie un fichier portant l'extension .doc, ce fichier sera enregistré sous la forme d'un document Microsoft Word. La même liste d'applications utilisées lors de l'ajout d'extensions lors de la réception d'un fichier MacBinary sous Windows est utilisée pour l'opération inverse. Dans la plupart des cas, vous pouvez lire directement les fichiers obtenus en cliquant deux fois dessus sous Mac OS.

Les versions précédentes de PGP pour Mac OS ne disposent pas de cette fonction. L'utilisateur devra déterminer manuellement si le fichier appelé « rapport.doc » est bien un fichier Microsoft Word. Après avoir déterminé son créateur, dans le cas de Microsoft Word, il vous suffit de sélectionner Fichier, Ouvrir, puis de choisir Tous les fichiers dans le menu. De nombreuses applications disposent de cette fonction, mais pas la totalité. Si le document ne peut pas être ouvert à partir de l'application, l'utilisateur devra déterminer les codes de type et de créateur Macintosh appropriés pour le fichier et les définir manuellement à l'aide d'un utilitaire tiers, dont la plupart sont gratuits. Dans ce cas, l'installation de la version 6.x représente probablement la meilleure solution, éliminant ainsi le problème.

Applications prises en charge

La liste suivante répertorie les principales applications dont les documents sont automatiquement reconnus par PGP lors d'un transfert de Windows vers Mac OS et inversement. Vous pouvez ajouter des éléments à cette liste en modifiant le fichier PGPMacBinaryMappings.txt situé dans le répertoire \WINDOWS. Pour Mac, supprimez le suffixe .txt du nom de fichier—PGPMacBinaryMappings se situe dans Dossier Système / Préférences / Pretty Good Preferences.

- 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 (texte, RTF, modèles)
- PGP
- Microsoft PowerPoint
- StuffIt
- QuickTime
- Corel WordPerfect
- Microsoft Excel (de nombreux types de fichiers)
- Quark XPress

Les extensions de noms de fichiers suivantes sont également converties :

.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	.hai	.lzh	.Z	.exe
.mpg	.dvi	.tex	.aif	.zip	.au
.mod	.svx	.wav	.tar	.pct	.pic
.pit	.txt	.mdi	.pak	.tif	.eps

Phil Zimmermann à propos de PGP

C

Ce chapitre comporte des données de base à la fois sur la cryptographie et sur PGP, telles que fournies par Phil Zimmermann.

Pourquoi ai-je créé PGP ?

« Quoi que vous fassiez, cela sera de peu d'importance, mais il est fondamental que vous le réalisiez. » —Mahatma Gandhi.

C'est personnel et privé. Et cela ne regarde personne d'autre que vous. Vous pouvez être en train de préparer une campagne politique, de parler de vos impôts ou de vivre une idylle secrète. Vous pouvez également être en relation avec un dissident politique victime des méthodes répressives de son pays. Quel que soit le sujet, vous ne souhaitez pas que vos messages électroniques personnels (e-mail) ou que vos documents confidentiels soient lus par quiconque. Vous avez le droit de vouloir protéger votre vie privée. C'est aussi simple que la Constitution américaine.

Le droit de protéger sa vie privée est énoncé implicitement dans l'ensemble de la Déclaration des droits des citoyens. Cependant, lors de l'élaboration de la Constitution américaine, les Pères fondateurs n'ont pas jugé nécessaire de formuler explicitement le droit d'avoir une conversation privée. Cela aurait été ridicule, car, il y a deux cents ans, toutes les conversations pouvaient se dérouler en privé. Si une personne était à proximité, il suffisait d'aller derrière la grange, puis de continuer à converser. Personne ne pouvait vous écouter à votre insu. Le droit d'avoir une conversation confidentielle relevait des droits naturels, pas uniquement au sens philosophique du terme mais aussi au sens physique en raison du niveau de technologie de l'époque.

L'invention du téléphone, qui a marqué le début de l'ère de l'information, a tout révolutionné. Aujourd'hui, la plupart de nos conversations sont véhiculées électroniquement. Aussi, les plus intimes peuvent être écoutées sans que nous le sachions. Un téléphone portable peut être contrôlé par quiconque dispose d'une radio. Les messages électroniques envoyés via Internet ne sont pas plus sécurisés que les appels passés par téléphone portable. Aujourd'hui, l'e-mail remplace de plus en plus le courrier postal et, à mesure qu'il perd de son aspect novateur, il devient la norme d'échange d'informations utilisée par tous. L'e-mail peut être régulièrement et automatiquement analysé à grande échelle dans le but de rechercher des mots clés intéressants sans que cela soit détecté. Cela ressemble à la pêche aux filets dérivants.

Vous pensez peut-être que le cryptage de vos e-mails ne se justifie pas. Si vous êtes réellement un citoyen respectueux de la loi et n'ayant rien à cacher, pourquoi ne pas envoyer systématiquement votre courrier écrit sur carte postale ? Pourquoi ne pas se soumettre à des contrôles anti–dopage sur demande ? Pourquoi exiger un mandat de perquisition à la police se présentant chez vous ? Cherchez-vous à cacher quelque chose ? Si vous dissimulez votre courrier dans des enveloppes, cela signifie-t-il que vous êtes un esprit subversif, un trafiquant de drogue ou même un paranoïaque ? Les citoyens respectueux des lois doivent–ils crypter leurs e-mails ?

Que se passerait-il si nous pensions tous que les citoyens en règle devaient utiliser des cartes postales pour leur courrier ? Si une personne non conformiste faisait valoir le droit à la protection de la vie privée en utilisant une enveloppe pour son courrier, cela éveillerait les soupçons. Les autorités pourraient ouvrir son courrier afin de découvrir ce qu'elle cherche à dissimuler. Heureusement, nous ne vivons pas dans ce type d'univers et nous cachons presque toutes nos missives à l'aide d'enveloppes. Aussi, personne n'attire de soupçons en protégeant sa vie privée de cette manière. C'est la vérité du plus grand nombre. De la même manière, il serait bien commode que chacun prenne l'habitude de crypter l'ensemble de ses e-mails, innocents ou non, car le recours à une telle pratique n'éveillerait pas les soupçons. Vous pouvez considérer cette démarche comme une forme de solidarité.

Jusqu'à présent, si le gouvernement souhaitait violer la vie privée de citoyens lambda, il devait consacrer beaucoup d'argent et d'efforts pour intercepter, ouvrir à la vapeur, puis lire une lettre. Il devait également écouter et éventuellement transcrire des conversations téléphoniques, du moins jusqu'à l'apparition de la technologie de reconnaissance vocale. Ce type de contrôle laborieux était peu commode à grande échelle. Il était utilisé uniquement lorsque c'était jugé nécessaire.

Le projet de loi sénatoriale américaine 266 datant de 1991 et ayant pour objet de lutter contre toutes les formes d'infractions comportait une mesure troublante. Si cette résolution non impérative était entrée en vigueur, elle aurait contraint les fabricants d'équipements de communications sécurisés à insérer dans leurs produits des « trappes » spéciales de manière à ce que le gouvernement puisse lire les messages cryptés de tout un chacun. Elle stipule que « Le Congrès a pour intention de demander aux prestataires et aux fabricants d'équipements de services de communication électronique de garantir que les systèmes de communication permettent au gouvernement d'obtenir le texte en clair du contenu des communications vocales, de données et autres, lorsque la loi l'autorise. » C'est ce projet de loi qui m'a incité, cette année-là, à proposer la publication électronique gratuite de PGP, peu de temps avant que cette mesure législative ne soit abandonnée suite aux vigoureuses protestations des groupes industriels et des défenseurs des libertés individuelles.

La loi américaine sur la téléphonie numérique votée en 1994 (Digital Telephony bill) a imposé l'installation par les opérateurs de ports d'écoute téléphonique distants dans leurs commutateurs numériques, créant par là même une nouvelle infrastructure technologique pour l'écoute téléphonique « pointer-et-cliquer ». Ainsi, les agents fédéraux ne sont plus obligés de sortir pour fixer des pinces crocodiles aux lignes téléphoniques. Ils peuvent désormais écouter vos appels téléphoniques à partir de leur quartier général à Washington. Naturellement, la loi exige toujours un mandat pour procéder à une écoute. Cependant, alors que les infrastructures technologiques peuvent rester en l'état pendant des décennies, les lois et les politiques peuvent changer du jour au lendemain. Lorsqu'une infrastructure de communications optimisée pour la surveillance est solidement établie, une modification du paysage politique peut aboutir à des abus. L'élection d'un nouveau gouvernement ou, cas extrême, le bombardement d'un bâtiment du gouvernement fédéral, peut modifier le contexte politique.

Un an après le vote, en 1994, de la loi sur la téléphonie numérique, le FBI a rendu public le projet visant à demander aux opérateurs téléphoniques d'intégrer dans leur infrastructure la capacité de capter simultanément 1 pour cent des conversations téléphoniques dans les principales villes des Etats-Unis. Cela équivaut à la multiplication par plus de 1 000 du nombre de mises sur écoute. Auparavant, seuls quelque mille écoutes téléphoniques par an étaient effectuées sur mandat aux Etats-Unis, à la fois aux niveaux local, fédéral et étatique. Il est non seulement difficile d'imaginer comment le gouvernement pourrait employer suffisamment de juges pour signer le nombre de mandats permettant de procéder à l'écoute de 1 pour cent des appels téléphoniques des Américains, mais il est encore plus difficile de concevoir comment il pourrait recruter assez d'agents fédéraux pour rester assis à les écouter en temps réel. La seule manière plausible de traiter ces appels requerrait une application digne d'Orwell de la technologie de reconnaissance vocale automatique pour passer au crible toutes les conversations à la recherche de mots clés intéressants ou de voix particulières. Si le gouvernement ne détecte pas sa cible parmi ce premier échantillon, les écoutes peuvent être effectuées sur un autre échantillon de la même taille jusqu'à ce que la recherche soit fructueuse ou encore jusqu'à ce que chaque ligne téléphonique ait été contrôlée pour circulation d'informations subversives. Le FBI a déclaré qu'une telle procédure serait nécessaire dans le futur. Ce projet provoqua une telle indignation qu'il fut rejeté par le Congrès, en tous les cas cette fois-ci, en 1995. Néanmoins, une telle demande du FBI pour obtenir de plus larges pouvoirs est révélatrice de ses intentions futures. L'échec de ce projet n'est pas particulièrement rassurant lorsque l'on pense que la loi sur la téléphonie numérique de 1994 avait été rejetée lors de sa première présentation en 1993.

Les progrès réalisés dans le domaine de la technologie ne permettront pas le maintien du statu quo en matière de confidentialité. Ce statu quo est instable. Si nous n'agissons pas, les nouvelles technologies fourniront au gouvernement de nouvelles possibilités de surveillance automatique auxquelles Staline n'aurait même pas pu rêver. Le recours à la cryptographie invulnérable constitue la seule manière de protéger la confidentialité des lignes téléphoniques en pleine ère de l'information.

Ce recours à la cryptographie ne doit pas être motivé par une méfiance vis-à-vis du gouvernement. Votre société peut être mise sur écoute par vos concurrents, par le grand banditisme ou par des gouvernements étrangers. Ainsi, plusieurs gouvernements étrangers reconnaissent faire appel à leurs services de renseignements pour l'espionnage des sociétés étrangères afin de fournir à leurs propres entreprises un avantage concurrentiel. Ironie du sort, les restrictions imposées par le gouvernement américain en matière de cryptographie ont affaibli le système de défense des entreprises américaines contre les services de renseignements étrangers et le grand banditisme.

Le gouvernement est conscient du rôle clé que la cryptographie jouera dans ses relations avec la population. En avril 1993, l'administration de Clinton a rendu public une toute nouvelle initiative de politique de cryptage étudiée par l'agence de sécurité nationale américaine (NSA) depuis l'arrivée de Bush à la présidence. La pièce maîtresse de cette initiative consistait en un système de cryptage conçu par les autorités, appelé la puce Clipper, contenant un nouvel algorithme de cryptage NSA classifié. Le gouvernement a essayé d'encourager l'industrie du secteur privé à l'intégrer dans l'ensemble de ses produits de communication sécurisés, tels que les téléphones et télécopieurs sécurisés, etc. AT&T a incorporé le système Clipper dans ses produits sécurisés impliquant l'usage de la voix. Voici ce qui se cache derrière ce système : pendant tout le processus de fabrication, chaque puce Clipper est chargée avec sa propre et unique clé dont le gouvernement obtient une copie placée en dépôt. Cependant, ne soyez pas inquiets, le gouvernement a promis qu'il utiliserait ces clés pour lire vos conversations uniquement « lorsque dûment habilité par la loi ». Naturellement, pour donner au système Clipper toute son efficacité, une mesure consistant à proscrire toute autre forme de cryptographie doit s'ensuivre.

Le gouvernement a commencé par déclarer que le recours au système Clipper serait volontaire et non imposé, contrairement à d'autres types de cryptographie. Cependant, la réaction de la population contre l'usage de cette puce a été plus forte que ne l'auraient imaginée les autorités. L'industrie informatique a unanimement exprimé son opposition à l'utilisation du système Clipper. Le Directeur du FBI, Louis Freeh, a affirmé au cours d'une conférence de presse en 1994 que si ce système ne parvenait pas à obtenir le soutien du public et que si les services d'écoute du FBI perdaient leur raison d'être en raison d'une cryptographie contrôlée par le gouvernement, ses services auraient comme dernier recours d'ester en justice pour réclamer des dommages et inté-

rêts. Suite à la tragédie d'Oklahoma City, M. Freeh a déclaré au cours de son témoignage devant le Comité judiciaire du Sénat que le gouvernement se devait de limiter les possibilités de recours parmi la population à la cryptographie invulnérable (bien que personne n'ait suggéré que les terroristes l'aient utilisée).

Le centre américain d'informations luttant pour les libertés individuelles sur les réseaux informatiques (The Electronic Privacy Information Center - EPIC) a eu connaissance de documents révélateurs dans le cadre de la loi sur la liberté d'information (Freedom of Information Act). Dans un document intitulé « Cryptage : menaces, applications et solutions éventuelles » envoyé au Conseil américain de la sécurité nationale en février 1993, au FBI, à la NSA et au Département de la justice (Department of justice - DOJ), il est conclu que « les solutions techniques, telles qu'elles se présentent actuellement, sont exploitables uniquement si elles sont intégrées à l'ensemble des produits de cryptage. Pour ce faire, il est nécessaire d'élaborer un texte législatif requérant l'utilisation de produits de cryptage agréés par le gouvernement ou respectant les exigences gouvernementales en matière de cryptage. »

Les antécédents du gouvernement quant au respect total des libertés individuelles des citoyens n'inspirent pas confiance. Le programme COINTELPRO du FBI visait des groupes d'opposants à la politique gouvernementale. Le FBI a espionné les mouvements pacifistes et ceux défendant les droits des citoyens. Il a mis sur écoute téléphonique Martin Luther King Jr. ; Nixon tenait une liste de ses ennemis. Sur ces entrefaites, le scandale du Watergate éclata. Le Congrès semble aujourd'hui résolu à voter des lois réduisant nos libertés individuelles sur Internet. Jamais depuis le début du siècle la méfiance de la population vis-à-vis du gouvernement n'avait à ce point envahi le monde politique, toutes tendances confondues.

L'une des manières de lutter contre la tendance inquiétante du gouvernement à considérer la cryptographie comme illicite consiste à employer cette technique autant que possible tant qu'elle reste légale. Une fois l'utilisation récurrente de la cryptographie invulnérable entrée dans les mœurs, il deviendra plus difficile pour les autorités de la réprimander. C'est pourquoi l'utilisation de PGP sert la démocratie.

Si la protection de la vie privée devient illégale, seuls les hors-la-loi pourront bénéficier d'intimité. Les organismes de renseignements disposent de technologies de cryptage de haut niveau, au même titre que les grands trafiquants de drogue et d'armes. Toutefois, de nos jours le citoyen lambda et les organisations politiques de base n'ont généralement pas accès à la technologie cryptographique de clés publiques bon marché de « standard militaire ».
Mais demain…

PGP donne à chacun le pouvoir de prendre en main sa vie privée. Je l'ai créé pour répondre au besoin ressenti par une grande partie de la société.

Les algorithmes symétriques de PGP

PGP propose une sélection de plusieurs algorithmes de clés secrètes afin de crypter le message réel. Par algorithme de clé secrète, nous désignons un chiffrement par bloc conventionnel ou symétrique utilisant la même clé pour le cryptage et le décryptage. Les trois chiffrements par bloc symétriques offerts par PGP sont CAST, DES triple et IDEA. Il ne s'agit pas d'algorithmes « faits maison », mais tous ont été développés par des équipes d'éminents cryptographes.

Pour ceux s'intéressant de près à la cryptographie, qu'ils sachent que les trois chiffrements fonctionnent sur des blocs de texte en clair et chiffré de 64 bits. La taille des clés CAST et IDEA atteint 128 bits et celle de DES triple, 168 bits. A l'instar de DES (norme de cryptage de données), un de ces chiffrements peut être utilisé en mode de renvoi de chiffrement (CFB) et de chaînage de blocs de chiffrement (CBC). Sur PGP, ils fonctionnent en mode CFB 64 bits.

J'ai inclus l'algorithme de cryptage de CAST dans PGP, car ce chiffrement par bloc présente l'avantage de comporter une clé de 128 bits, d'être rapide et gratuit. Son nom est composé des initiales de ses inventeurs, à savoir Carlisle Adams et Stafford Tavares de Northern Telecom (Nortel). Nortel a présenté une demande de brevet pour CAST, mais s'est engagé par écrit à fournir CAST à quiconque sans versement de droits. CAST semble avoir été particulièrement bien conçu par des personnes jouissant d'une bonne réputation dans ce domaine. La conception repose sur un ensemble d'affirmations pouvant être formellement démontrées et laissant à penser qu'un nombre impressionnant de clés est nécessaire pour casser sa clé de 128 bits. CAST ne comporte aucune clé faible ou semi-faible. De nombreux éléments tangibles tendent à montrer l'immunité totale de CAST contre la cryptanalyse linéaire et différentielle, les formes de cryptanalyse les plus performantes répertoriées dans la littérature disponible dans le domaine et qui ont été à même de casser DES. CAST est trop récent pour qu'un dossier d'antécédents exhaustif soit constitué, mais sa conception formelle et la bonne réputation de ses inventeurs attireront indubitablement l'attention et les critiques du reste de la communauté cryptographique académique. J'éprouve quasiment le même sentiment de confiance vis-à-vis de CAST que d'IDEA, le chiffrement que j'avais sélectionné pour des versions plus récentes de PGP il y a quelques années. A cette époque, IDEA était également trop récent pour constituer un dossier d'antécédents, mais il a fait son chemin.

Le chiffrement par bloc IDEA (International Data Encryption Algorithm – Algorithme de cryptage de données international) est basé sur la conception consistant à « associer des opérations de différents groupes algébriques ». Il a été développé à ETH à Zurich par James L. Massey et Xuejia Lai, puis édité en 1990. Dans des publications antérieures, cet algorithme était nommé IPES (Improved Proposed Encryption Standard – Norme de cryptage proposée améliorée), mais il a pris par la suite le nom de IDEA. Jusqu'ici, IDEA a bien mieux résisté aux attaques que d'autres chiffrements par bloc, tels que FEAL, REDOC-II, LOKI, Snefru et Khafre. Il est également plus résistant que DES vis-à-vis des attaques différentielles très puissantes que constituent Biham et

Shamir, ainsi que des attaques provenant de cryptanalyse linéaire. Alors que le chiffrement continue de s'attirer les critiques des zones les plus importantes du monde cryptanalytique, la confiance en IDEA ne cesse de croître. Malheureusement, la détention du brevet pour la conception d'IDEA par Ascom Systec constitue l'obstacle majeur au passage de cet algorithme au stade de norme et, contrairement à DES et CAST, IDEA n'a pas été rendu accessible au public sans versement de droits.

PGP inclut, en guise de protection, trois clés DES triple dans son répertoire de chiffrements par bloc disponibles. DES a été développé par IBM au milieu des années 1970. Bien qu'étant bien conçue, sa clé de 56 bits est de taille insuffisante par rapport aux normes actuelles. DES triple est particulièrement invulnérable et résulte d'une étude approfondie menée sur plusieurs années. Par conséquent, il est probablement plus sûr que les nouveaux chiffrements par bloc, tels que CAST et IDEA. DES triple correspond au DES appliqué trois fois au même bloc de données, à l'aide de trois clés différentes, à l'exception près que la seconde opération DES est exécutée en arrière en mode de décryptage. DES triple est beaucoup plus lent que CAST ou IDEA, mais la rapidité importe généralement peu dans les applications e-mail. Bien que la taille de sa clé atteigne 168 bits, DES triple semble bénéficier d'une puissance de clé supérieure ou égale à 112 bits contre un pirate disposant d'une énorme capacité de stockage de données. Selon un article écrit par Michael Weiner à Crypto96, toute capacité distante potentielle de stockage de données à la disposition d'un pirate lui permettrait de lancer une attaque nécessitant quasiment autant d'efforts que pour casser une clé de 129 bits. DES triple n'est lié à aucun brevet.

Les clés publiques de PGP générées par la version 5.0, ou version ultérieure de PGP, renferment des informations indiquant au logiciel d'un expéditeur les chiffrements par bloc supportés par le logiciel du destinataire, de telle sorte qu'il sache quels chiffrements utiliser pour procéder au cryptage. Les clés publiques Diffie-Hellman / DSS acceptent CAST, IDEA ou DES triple en tant que chiffrement par bloc, CAST étant sélectionné par défaut. Pour des raisons de compatibilité, les clés RSA ne sont actuellement pas dotées de cette fonction. Seul l'algorithme IDEA est utilisé par PGP pour envoyer des messages aux clés RSA, car les versions antérieures de PGP prendraient uniquement en charge RSA et IDEA.

A propos des routines de compression de données PGP

PGP compresse habituellement le texte en clair préalablement à son cryptage. En effet il est impossible de compresser des données cryptées. Cette compression des données permet de réduire le temps de transmission du modem, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique. La plupart des techniques de cryptanalyse consistent à exploiter les

redondances trouvées dans le texte en clair pour casser le chiffrement. La compression des données réduit cette redondance dans le texte en clair, améliorant ainsi considérablement la résistance à la cryptanalyse. Cette compression du texte clair prend du temps, mais la démarche en vaut la peine sur le plan de la sécurité.

Les fichiers trop courts pour la compression ou qui ne se compressent pas correctement ne sont pas compressés par PGP. En outre, le programme reconnaît les fichiers produits par les programmes de compression les plus connus, comme PKZIP, et ne tente pas de compresser un fichier déjà compressé.

Pour ceux qui s'intéressent à la technique, le programme recourt aux routines de compression du logiciel gratuit ZIP créé par Jean-Loup Gailly, Mark Adler et Richard B. Wales. Ce logiciel utilise des algorithmes de compression fonctionnant de manière équivalente à ceux utilisés par le programme PKZIP 2.x. du logiciel PKW. Sa rapidité et son ratio de compression très performant constituent les principales raisons de la sélection du logiciel de compression ZIP pour PGP.

A propos des nombres aléatoires utilisés comme clés de session

PGP crée des clés de session temporaires à l'aide d'un générateur de nombres pseudo-aléatoires cryptographiquement invulnérable. Si ce fichier de valeurs initiales aléatoires n'existe pas, il est automatiquement créé, puis affecté de nombres véritablement aléatoires dérivés de vos événements aléatoires collectés par le programme PGP à partir de la synchronisation de vos frappes clavier et des mouvements de votre pointeur.

Ce générateur crée à nouveau le fichier de valeurs initiales aléatoires lors de chaque utilisation en y ajoutant de nouvelles données partiellement dérivées de l'heure et d'autres sources véritablement aléatoires. L'algorithme de cryptage conventionnel fait office de moteur pour le générateur de nombres aléatoires. Le fichier de valeurs initiales aléatoires contient des données et des clés aléatoires utilisées pour verrouiller le moteur de cryptage conventionnel du générateur aléatoire.

Pour diminuer les risques qu'un pirate ne dérive vos clés de la session suivante ou précédente, ce fichier doit être protégé contre toute divulgation. Le pirate aurait toutes les peines du monde à obtenir toute information utile du fichier de valeurs initiales aléatoires, car il est nettoyé cryptographiquement avant et après chaque utilisation. Néanmoins, il semble plus prudent de ne pas le mettre entre toutes les mains. Si possible, rendez ce fichier lisible par vous uniquement. Sinon, ne laissez pas n'importe qui effectuer des copies sur votre ordinateur.

A propos du résumé de message

Le résumé de message constitue un « distillat » compact (160 ou 128 bits) de la somme de contrôle de votre message ou fichier. Vous pouvez également le considérer comme une « empreinte digitale » de votre message ou fichier. Le résumé de message « représente » votre message de sorte qu'en cas d'altération du message, un autre calcul de résumé en découlerait. Cela permet de détecter toute modification apportée au message par un faussaire. Un résumé de message est calculé à l'aide d'une fonction de hachage à sens unique cryptographiquement invulnérable. D'un point de vue informatique, un pirate ne peut pas concevoir un message de substitution qui donnerait lieu à un résumé de message identique. A cet égard, un résumé de message présente plus d'avantages qu'une somme de contrôle, car il est facile de concevoir un autre message produisant la même somme de contrôle. Toutefois, ni la somme de contrôle, ni le message d'origine ne peut être dérivé(e) du résumé.

L'algorithme de résumé de message désormais utilisé par PGP (Version 5.0 et ultérieure) est nommé SHA, acronyme correspondant aux mots Secure Hash Algorithm (Algorithme de hachage sécurisé), et a été conçu par la NSA à l'attention de l'Agence gouvernementale de normes et de technologie (NIST). SHA constitue un algorithme de hachage de 160 bits. Certaines personnes éprouvent de la méfiance vis-à-vis de tout ce qui émane de la NSA, car celle-ci est chargée d'intercepter les communications et de casser les codes. N'oubliez pas que la NSA n'a aucun intérêt à falsifier des signatures et que le gouvernement bénéficierait d'une norme de signature numérique non falsifiable empêchant qui que ce soit de nier sa signature. Ceci présente des avantages divers pour l'application de la loi et la collecte de renseignements. Par ailleurs, SHA a été publié pour le grand public et a été revu dans le détail par la plupart des meilleurs cryptographes au monde spécialisés dans les fonctions de hachage. Tous reconnaissent que SHA est extrêmement bien conçu. Il comporte certaines innovations permettant de surmonter l'ensemble des faiblesses constatées dans les précédents algorithmes de résumés de message publiés par des cryptographes académiques. Toutes les nouvelles versions de PGP prennent en charge l'algorithme de résumé de message SHA grâce auquel des signatures peuvent être créées à l'aide des nouvelles clés DSS conformes au standard de signature magnétique de la NIST. Pour des raisons de compatibilité avec les anciennes versions de PGP, les nouvelles versions de PGP prennent-elles aussi en charge RM5 pour les signatures RSA.

Le RM5, un algorithme de hachage de 128 bits, constitue l'algorithme de résumé de message utilisé par les précédentes versions de PGP. Il a été placé dans le domaine public par RSA Data Security, Inc. RM5 a failli être cassé en 1996 par le cryptographe allemand Hans Dobbertin. Cependant, bien que n'ayant pas été cassé, RM5 a révélé de telles faiblesses qu'il est déconseillé de s'en servir pour générer des signatures. En s'attelant à la tâche, il est probable qu'il puisse être entièrement cassé, permettant ainsi de falsifier des signatures. Si vous souhaitez éviter de découvrir un jour votre signature numérique PGP apposée sur une fausse déclaration, vous feriez mieux d'adopter les clés DSS de PGP comme méthode favorite pour générer des signatures numériques, car DSS utilise SHA en tant qu'algorithme de hachage sûr.

Comment protéger les clés publiques contre la falsification ?

Il n'est pas nécessaire de cacher les clés d'un système de cryptographie de clés publiques. Il est même préférable de les diffuser aussi largement que possible. Toutefois, il est important de les protéger contre la falsification afin d'être certain qu'elles appartiennent réellement aux personnes en étant à priori les détenteurs. Il peut s'agir là de la plus grande vulnérabilité affectant un système de cryptographie de clés publiques. Dans un premier temps, nous examinerons un cas de catastrophe potentielle, puis nous décrirons comment l'éviter via PGP.

Supposons que vous souhaitiez envoyer un message privé à Alice. Vous téléchargez le certificat de clé publique d'Alice à partir d'un BBS (tableau d'affichage électronique). A l'aide de cette clé, vous cryptez votre lettre pour Alice, puis lui envoyez via l'e–mail du BBS.

Malheureusement, à votre insu à tous les deux, un autre utilisateur prénommé Charlie s'est infiltré dans le BBS et a généré sa propre clé publique en y associant l'ID utilisateur d'Alice. En cachette, il remplace la vraie clé publique d'Alice par sa clé erronée. Vous utilisez involontairement la fausse clé de Charlie au lieu de la clé publique d'Alice. Cette fausse clé étant associée à l'ID utilisateur d'Alice, vous ne remarquez rien d'anormal. Charlie peut, à présent, déchiffrer le message rédigé à l'attention d'Alice puisqu'il détient la clé privée correspondante. Il peut même crypter à nouveau le message déchiffré à l'aide de la vraie clé publique d'Alice et lui renvoyer, de manière à ce qu'aucune infraction ne soit suspectée. Il peut également signer à la place d'Alice avec cette clé privée puisque les signatures d'Alice seront toutes vérifiées via la fausse clé.

Le seul moyen d'éviter un problème de ce type consiste à empêcher quiconque de falsifier des clés publiques. Si Alice vous envoie directement sa clé publique, vous êtes à l'abri de toute mésaventure. Cette opération peut toutefois être difficile à réaliser si Alice se situe à des milliers de kilomètres de vous ou si vous n'arrivez pas à la joindre.

Vous pourriez vous procurer la clé publique d'Alice auprès d'un ami commun, David, qui est sûr de détenir une copie correcte de cette clé. David peut signer la clé publique d'Alice afin de garantir son authenticité. Il peut créer cette signature à l'aide de sa propre clé privée.

Ceci entraînerait la création d'un certificat de clé publique signé indiquant que la clé d'Alice n'a pas été falsifiée. Pour vérifier la signature de David, vous devez disposer d'une copie conforme à sa clé publique. Autre solution : David pourrait également fournir à Alice une copie signée de votre clé publique, servant ainsi de « correspondant » entre Alice et vous.

Ce certificat de clé publique signé destiné à Alice pourrait être téléchargé par elle ou par David sur le BBS, d'où vous pourriez ensuite vous-même le télécharger. Vous vérifieriez alors cette signature via la clé publique de David afin de vous assurer qu'il s'agit réellement de la clé publique d'Alice. Aucun imposteur ne peut vous tromper en vous communiquant sa fausse clé comme étant celle d'Alice puisque personne d'autre ne peut falsifier les signatures de David.

Quelqu'un ayant la confiance de nombreuses personnes pourrait remplir les fonctions de « correspondant » d'utilisateurs en fournissant des signatures pour leurs certificats de clés publiques. Cette personne aurait le statut d'« Autorité de certification ». Tout certificat de clé publique comportant la signature de cette Autorité serait fiable et considéré comme appartenant véritablement à la personne censée en être le détenteur. Seule une copie correcte de la clé publique de l'Autorité de certification serait nécessaire aux utilisateurs souhaitant participer, afin de pouvoir vérifier les signatures de l'Autorité. Dans certains cas, l'Autorité de certification peut également remplir la fonction de serveur de clés, permettant ainsi aux utilisateurs d'un réseau de rechercher des clés publiques par son intermédiaire. Toutefois, rien ne justifie la nécessité qu'un tel serveur certifie des clés.

Une Autorité de certification centralisée de confiance est particulièrement adaptée aux grandes sociétés impersonnelles ou aux institutions gouvernementales. Certaines institutions instaurent des hiérarchies d'Autorités de certification.

Dans les milieux moins centralisés, il est probablement plus judicieux que chaque utilisateur agisse en tant que correspondant fiable auprès de ses amis plutôt que de recourir à une Autorité de certification de clé centralisée.

L'un des atouts majeurs de PGP est de fonctionner aussi bien dans un milieu centralisé à l'aide d'une Autorité de certification que dans un milieu décentralisé où les personnes s'échangent leurs clés personnelles.

Cette lutte laborieuse contre la falsification des clés publiques constitue le seul problème difficile à résoudre dans les applications de clés publiques. C'est le « talon d'Achille » de la cryptographie de clé publique qui est à lui seul à l'origine de nombreuses solutions logicielles complexes.

Utilisez une clé publique uniquement lorsque vous êtes certain qu'elle est correcte, non falsifiée et qu'elle appartient réellement à la personne supposée y être associée. Si vous avez obtenu le certificat de clé publique directement de son détenteur ou s'il porte la signature d'une personne en qui vous avez confiance, par exemple vous ayant auparavant fourni une clé publique correcte, alors toutes les garanties sont réunies. En outre, l'ID utilisateur doit porter le nom complet du détenteur de la clé, pas uniquement son prénom.

Aussi tentant cela soit-il, ne vous fiez *jamais* à une clé publique téléchargée à partir d'un BBS, à moins qu'elle ne soit signée par une personne de confiance. Cette clé non certifiée pourrait avoir été falsifiée par n'importe qui, voire par l'administrateur système du BBS.

Si vous devez signer le certificat de clé publique d'un tiers, assurez-vous qu'il appartient réellement à la personne désignée dans l'ID utilisateur du certificat. En effet, en signant ce certificat, vous vous engagez personnellement sur le fait que la clé appartient réellement à la personne concernée. Quiconque se fiant à vous acceptera cette clé publique parce que votre signature y est apposée. Il peut être dangereux de croire aux « on-dit » : signez une clé publique uniquement si vous avez appris par vous-même qui la détient réellement. L'idéal consiste à ne la signer qu'après l'avoir obtenue directement de son détenteur.

Il est plus important d'être sûr du détenteur d'une clé lorsque vous la signez que lorsque vous souhaitez simplement l'utiliser pour crypter un message. Des signatures de certification apposées par des correspondants de confiance suffisent pour garantir la validité d'une clé. En revanche, avant de signer une clé, renseignez-vous en personne sur l'identité de son détenteur. Vous pouvez éventuellement téléphoner à cette personne et lui lire l'empreinte digitale de la clé afin d'être sûr que la clé lui appartient réellement. Vérifiez que vous vous adressez bien à la bonne personne.

N'oubliez pas que l'apposition de votre signature sur un certificat de clé publique ne garantit pas l'intégrité de son détenteur mais uniquement celle de la clé (c'est à dire de sa détention). Votre crédibilité n'est pas mise en jeu par le fait de signer la clé publique d'un psychopathe alors que vous êtes absolument certain qu'il en est le détenteur. Des tiers accepteraient cette clé comme lui appartenant parce que vous l'avez signée (en partant du principe qu'ils se fient à vous), mais ils ne feraient pas confiance au détenteur. Se fier à une clé et faire confiance à son détenteur sont deux attitudes différentes.

Conservez à portée de main votre clé publique à laquelle sont associées plusieurs signatures de certification de divers « correspondants » garantissant la validité de votre clé. Il reste à espérer que la plupart des gens se fieront à au moins l'un d'entre eux. Vous pouvez placer votre clé et l'ensemble de ces signatures de certification associées sur plusieurs BBS. Lorsque vous signez une clé publique, renvoyez-la à son détenteur de manière à ce qu'il puisse ajouter votre signature à l'ensemble des références qu'il a réunies pour sa clé publique.

Prenez les précautions nécessaires afin que personne ne puisse falsifier votre trousseau de clés publiques. La vérification d'un certificat de clé publique venant d'être signé doit finalement dépendre de l'intégrité des clés publiques fiables placées sur votre trousseau de clés publiques. Exercez un contrôle physique sur votre trousseau de clés publiques, de préférence à partir de votre

ordinateur personnel plutôt qu'à partir d'un système distant exploité en temps partagé, ainsi que vous le feriez pour votre clé privée. De cette manière, vous le protégez contre la falsification, mais pas contre la divulgation. Conservez une copie de sauvegarde fiable de votre trousseau de clés publiques et de votre clé privée sur un support protégé en écriture.

Votre clé publique étant utilisée en tant qu'ultime autorité pour certifier directement ou indirectement toutes les autres clés de votre trousseau, il est fondamental de protéger celle-ci en premier lieu contre la falsification. Vous pouvez conserver une copie de sauvegarde sur une disquette protégée en écriture.

PGP part généralement du principe que vous veillez physiquement à la sécurité de votre système et de vos trousseaux de clés, ainsi qu'à celle de votre copie de PGP. Si un intrus peut falsifier votre disque, il peut théoriquement falsifier le programme et, du même coup, affaiblir les systèmes de sécurité du programme permettant de détecter la falsification de clés.

Une façon quelque peu complexe de protéger l'ensemble de votre trousseau de clés contre de telles tentatives consiste à le signer dans son intégralité à l'aide de votre clé privée. Pour ce faire, constituez un certificat de signature séparée de votre trousseau.

Comment PGP localise-t-il les clés correctes ?

Avant de lire cette section, lisez la précédente intitulée « Comment protéger les clés publiques contre la falsification ? »

PGP localise sur votre trousseau les clés correctement certifiées par des signatures de correspondants en qui vous avez confiance. Il vous suffit d'indiquer à PGP les personnes que vous avez désignées comme correspondants et de certifier leurs clés vous-même à l'aide de la plus fiable de vos clés. PGP peut la sélectionner à cet endroit, validant ainsi automatiquement l'ensemble des autres clés signées par vos correspondants désignés. Naturellement, vous pouvez directement signer davantage de clés.

Il existe deux types de critères très différents utilisés par PGP pour juger de l'utilité d'une clé publique. Ne les confondez pas :

1. La clé appartient–elle réellement à la personne censée en être le détenteur ? En d'autres termes, a-t-elle été certifiée par une signature fiable ?

2. Appartient-elle à une personne suffisamment fiable pour certifier d'autres clés ?

PGP peut calculer la réponse à la première question. Quant à la seconde, vous devez répondre de façon explicite à PGP. Une fois cette seconde réponse donnée, PGP est en mesure de calculer celle de la question 1 pour d'autres clés signées par le correspondant déclaré fiable.

Les clés certifiées par un tel correspondant sont estimées correctes par PGP. Les clés détenues par des correspondants fiables doivent elles-mêmes être certifiées par vous-même ou par d'autres correspondants fiables.

PGP offre également la possibilité d'affecter plusieurs niveaux de fiabilité aux personnes désignées comme correspondants. La confiance que vous avez en un détenteur de clé pour qu'il agisse en tant que correspondant ne reflète pas uniquement l'estime que vous avez pour son intégrité, mais aussi pour sa capacité à comprendre la gestion des clés et à faire preuve de discernement lors de la signature de clés. Vous pouvez désigner une personne comme étant non fiable, à fiabilité marginale ou complète en matière de certification d'autres clés publiques. Ces informations relatives à la fiabilité sont stockées avec la clé sur votre trousseau, sauf si vous indiquez à PGP de copier une clé en dehors de votre trousseau de clés. En effet, vos opinions personnelles sur la fiabilité sont confidentielles.

Lorsque PGP calcule la validité d'une clé publique, il examine le niveau de fiabilité de l'ensemble des signatures de certification associées. Il calcule un résultat pondéré. Par exemple, deux signatures à fiabilité marginale sont jugées aussi dignes de foi qu'une seule signature à fiabilité complète. Le scepticisme du programme est réglable. Par exemple, vous pouvez demander à PGP d'exiger deux signatures à fiabilité complète ou trois signatures à fiabilité marginale pour considérer une clé correcte.

Votre propre clé est « implicitement » correcte selon PGP, aucune signature de correspondant n'étant nécessaire pour prouver sa validité. Pour reconnaître vos clés publiques, PGP recherche les clés privées correspondantes sur la clé privée. PGP est également fondé sur le principe que vous vous accordez une confiance totale pour la certification d'autres clés.

Au fil du temps, vous accumulez des clés appartenant à des personnes que vous souhaitez désigner comme correspondants fiables. Toute autre personne choisira ses propres correspondants fiables et accumulera progressivement un ensemble de signatures de certification qu'il distribuera avec sa clé, en supposant que ces destinataires se fieront à au moins une ou deux de ces signatures. Il en résultera une fiabilité du Web décentralisée, tolérant les pannes pour l'ensemble des clés publiques.

Cette approche de base unique dans son genre contraste vivement avec les systèmes de gestion des clés publiques standard élaborés par le gouvernement et autres institutions monolithiques, comme la messagerie étendue de confidentialité (PEM), et qui reposent sur la centralisation du contrôle et de la confiance obligatoire. Ces systèmes standard sont fondés sur une hiérarchie d'Autorités

de certification vous imposant les personnes à qui vous fier. La méthode décentralisée probabiliste du programme permettant de déterminer la légitimité de la clé publique constitue la pièce maîtresse de son architecture de gestion des clés. PGP vous laisse choisir qui bon vous semble, et vous place à la tête de votre propre pyramide de certification privée. PGP s'adresse à ceux pensant ne pas être aussi bien servis que par eux-mêmes.

Le fait que l'accent soit mis ici sur cette approche de base décentralisée ne signifie pas que le fonctionnement de PGP soit moins performant dans un système de gestion des clés publiques plus hiérarchisé et centralisé. Par exemple, des utilisateurs appartenant à de grandes entreprises souhaiteront probablement qu'une seule et même personne signe l'ensemble des clés des employés. PGP appréhende ce scénario centralisé comme un cas particulier de dégénérescence du modèle de fiabilité PGP plus répandu.

Comment protéger les clés privées contre la divulgation ?

Protégez très soigneusement votre clé privée et votre mot de passe complexe. Si votre clé privée est compromise, faites-le savoir rapidement à l'ensemble des parties intéressées avant que quiconque ne l'utilise pour signer en votre nom. Par exemple, quelqu'un pourrait l'utiliser pour signer des certificats de clés publiques erronées, ce qui pourrait être très dommageable, surtout si de nombreuses personnes se fient à votre signature. En outre, la compromission de votre clé privée peut s'étendre aux messages vous étant adressés.

La première mesure à prendre pour protéger votre clé privée consiste à toujours en conserver le contrôle physique. Enregistrez-la sur votre ordinateur personnel, chez vous, ou sur votre ordinateur portable. Si, au bureau, vous travaillez sur un ordinateur sur lequel vous n'exercez pas toujours un contrôle physique, conservez vos trousseaux de clés publiques et privées sur une disquette protégée en écriture et prenez-la avec vous en partant. Il serait peu prudent de laisser votre clé privée sur un ordinateur distant exploité en temps partagé, tel qu'un système UNIX à accès distant. Une personne piratant votre ligne modem pourrait s'emparer de votre mot de passe complexe et se procurer votre clé privée à partir du système distant. Utilisez votre clé privée à partir d'un ordinateur placé sous votre contrôle physique.

Ne stockez pas votre mot de passe complexe sur l'ordinateur comportant votre fichier de clés privées. Il est aussi dangereux de stocker à la fois la clé privée et le mot de passe complexe sur le même ordinateur que de conserver son code bancaire et sa carte bleue dans le même portefeuille. Vous ne souhaitez certainement pas que quelqu'un mette la main sur la disquette comportant à la fois votre mot de passe complexe et votre fichier de clés privées. Le mieux est de mémoriser votre mot de passe complexe sans le stocker où que ce soit. Si vous avez besoin d'écrire votre mot de passe complexe sur une feuille, conservez-la en lieu sûr, plus encore que le fichier de clés privées.

Conservez des copies de sauvegarde de clé privée. N'oubliez pas que vous disposez de l'unique copie de votre clé privée et que si vous l'égarez, l'ensemble des copies de votre clé publique distribuées deviendrait inutile.

L'approche décentralisée et non institutionnalisée prise en charge par PGP pour la gestion des clés publiques présente des avantages, mais elle implique également que vous ne pouvez pas compter sur une seule liste centralisée des clés compromises. Cela complique la tâche consistant à limiter les dommages entraînés par la compromission de votre clé privée. Le plus simple consiste à faire fonctionner le bouche à oreille et à espérer que tout le monde sera tenu au courant.

Dans le pire des cas, à savoir la compromission de votre clé privée et de votre mot de passe complexe (en espérant que vous vous en aperceviez), vous devez émettre un certificat de « révocation de clé ». Ce type de certificat sert à signaler à chacun qu'il doit cesser d'utiliser votre clé publique. Vous pouvez créer un tel certificat à l'aide de PGP via la commande Révoquer dans le menu PGPkeys ou en demandant à votre autorité de révocation désignée de le générer à votre place. Envoyez-le vers le serveur de certificats, de manière à ce que chacun en prenne connaissance. Les logiciels PGP installent ce certificat de révocation de clé sur les trousseaux de clés publiques et empêchent automatiquement l'utilisation accidentelle de votre clé. Vous devez générer une nouvelle paire de clés publiques / privées, puis publier la nouvelle clé publique. Vous pouvez envoyer un seul fichier contenant à la fois votre nouvelle clé publique et le certificat de révocation de clé relatif à votre ancienne clé.

En cas de perte de votre clé privée

En règle générale, lorsque vous souhaitez révoquer votre propre clé privée, vous pouvez utiliser la commande Révoquer du menu PGPkeys afin d'émettre un certificat de révocation, signé avec votre clé privée personnelle.

Mais que faire si votre clé privée est perdue ou endommagée ? Il vous est alors impossible de la révoquer vous-même, car vous avez besoin de cette clé privée que vous venez de perdre. Si votre clé ne dispose d'aucune autorité de révocation désignée, c'est-à-dire d'une personne définie dans PGP comme autorisée à révoquer cette clé en votre nom, vous devez alors demander à chaque utilisateur ayant signé votre clé de retirer sa certification. Ainsi, toute personne tentant d'utiliser votre clé, car elle fait confiance à l'un de vos correspondants, saura qu'elle ne peut pas considérer votre clé publique comme fiable.

Pour plus d'informations sur les autorités de révocation désignées, reportez-vous à la section « Pour désigner une autorité de révocation » du Chapitre 6.

Attention aux remèdes de charlatans

Lors de l'évaluation d'un logiciel cryptographique, la question de sa fiabilité se pose toujours. Même si vous pouvez vérifier personnellement le code source, vous ne possédez peut-être pas l'expérience nécessaire pour juger de sa sécurité. Et même si vous étiez un cryptographe expérimenté, certains points faibles des algorithmes pourraient encore vous échapper.

Lorsque j'étais encore étudiant, au début des années soixante-dix, j'ai conçu un système de cryptage que j'estimais particulièrement astucieux. Une simple série de nombres pseudo-aléatoires était ajoutée au texte en clair afin de générer le texte chiffré. Selon toute apparence, ce procédé empêchait une analyse fréquentielle du texte chiffré et s'avérait inviolable, même pour les services de renseignement gouvernementaux disposant de ressources inépuisables. J'étais si fier de mon invention.

Des années plus tard, j'ai découvert ce même système décrit dans plusieurs introductions à la cryptographie et dans divers comptes rendus de séminaires. Formidable ! D'autres cryptographes avaient élaboré le même procédé. Hélas, il était présenté comme un simple exercice d'application aux techniques élémentaires de cryptanalyse et le jeu consistait à casser son code. C'en était fini de mon idée brillante.

De cette expérience humiliante, j'ai appris combien il était facile de se donner l'illusion de la sécurité lors de l'élaboration d'un algorithme de cryptage. La plupart des personnes ne réalisent pas les efforts nécessaires à la conception d'un algorithme de cryptage soumis aux attaques prolongées et déterminées de la part d'un opposant ingénieux. De nombreux ingénieurs informatiques ont développé des systèmes de cryptage plus ou moins naïfs (souvent pratiquement identiques) qui ont parfois été incorporés à des logiciels de cryptage et commercialisés, de manière lucrative, à des utilisateurs peu méfiants.

Cela revient à vendre des ceintures de sécurité automobiles qui semblent parfaites, mais qui ne se verrouillent pas même lors d'un test de collision à basse vitesse. Se fier à leur fiabilité peut s'avérer pire que de ne pas mettre sa ceinture. Tant qu'un accident n'est pas arrivé, personne ne peut douter de leur fiabilité. Un logiciel cryptographique vulnérable peut vous amener à mettre involontairement des informations confidentielles en péril, alors que vous auriez su comment les protéger si vous n'aviez pas disposé d'un tel outil. De plus, il est même possible que vous ne découvriez jamais que vos données ont été exposées.

Certains logiciels du commerce ont parfois recours à la norme de cryptage de données fédérale (DES), un algorithme conventionnel assez performant, recommandé par le gouvernement pour un usage commercial (et non pour les renseignements classifiés, ce qui peut paraître plutôt bizarre). DES peut utiliser divers « modes de fonctionnement », certains meilleurs que d'autres.

Le gouvernement recommande expressément d'éviter le mode le plus élémentaire et le plus vulnérable pour les messages, c'est-à-dire le mode ECB (dictionnaire de code électronique). En revanche, il conseille vivement les modes CFB (renvoi de chiffrement) et CBC (chaînage de blocs de chiffrement) qui sont plus évolués et plus performants face aux attaques.

Malheureusement, la plupart des modules de cryptage du commerce que j'ai pu examiner utilisent le mode ECB. Au cours de discussions avec les auteurs de certaines de ces implémentations, ils m'ont avoué n'avoir jamais entendu parler des modes CBC et CFB et ignorer tout des points faibles du mode ECB. Le simple fait que leurs connaissances en cryptographie soient insuffisantes pour être au courant de ces concepts élémentaires n'est pas très rassurant. En outre, leurs clés DES sont souvent conçues d'une manière inappropriée et peu sûre. Mais, plus grave encore, ces mêmes modules logiciels incluent parfois un second algorithme de cryptage plus rapide pouvant être utilisé au lieu du DES qui est considéré comme plus lent. La plupart du temps, l'auteur de ce module est persuadé que son algorithme propriétaire est aussi sécurisé que l'algorithme DES. Cependant, après quelques questions, je découvre généralement qu'il s'agit en fait d'une variante du procédé brillant que j'avais inventé alors que j'étais étudiant. Ou bien, il refusera peut-être de me révéler le secret de son algorithme, tout en m'assurant de son ingéniosité et de sa fiabilité. Il est sûrement sincère, mais comment le croire sans jeter un coup d'œil au code ?

En toute impartialité, je dois souligner que ces produits aussi peu performants sont souvent élaborés par des entreprises non spécialisées dans les techniques de cryptographie.

Cependant, même les excellents logiciels qui utilisent l'algorithme DES selon le mode de fonctionnement approprié, présentent également des problèmes. La norme de cryptage DES emploie une clé de 56 bits qui, selon les standards actuels, est trop petite et peut désormais facilement être forcée par des recherches exhaustives sur des calculateurs particulièrement rapides. En effet, la norme DES a atteint les limites de sa durée de vie utile, et il en est de même des logiciels basés sur cette norme.

Il existe une entreprise, appelée AccessData (http://www.accessdata.com) qui vend un module à prix modéré permettant de casser certains procédés de cryptage intégrés, tels que ceux utilisés par les applications WordPerfect, Lotus 1-2-3, Microsoft Excel, Symphony, Quattro Pro, Paradox, MS Word et PKZIP. Non seulement ce module permet de deviner les mots de passe, mais il autorise également une véritable analyse de cryptographie. Certaines personnes s'en servent lorsqu'elles ont oublié le mot de passe de leurs fichiers. Les fonctionnaires chargés de l'application de la loi l'utilisent également pour consulter les fichiers saisis. Après avoir discuté avec Eric Thompson, son auteur, j'ai appris qu'il ne fallait pas plus d'une fraction de seconde à son logiciel pour violer un code, mais qu'il lui avait ajouté une boucle de temporisation afin de ralentir son exécution et donner ainsi l'illusion à l'utilisateur d'une difficulté à résoudre.

Dans le domaine de la téléphonie sécurisée, le choix proposé est plutôt désolant. Le principal produit concurrent est le STU-III (unité téléphonique sécurisée), commercialisé par Motorola et AT&T pour une somme comprise entre 2 000 et 3 000 dollars et utilisé par le gouvernement des Etats-Unis pour ses applications classifiées. Son algorithme de cryptographie est assez complexe, mais une autorisation spéciale du gouvernement est requise pour faire l'acquisition de cette version évoluée. Il existe également, dans le commerce, une version du STU-III qui a été édulcorée à la demande de la NSA, ainsi qu'une version vouée à l'export qui a été rendue encore plus vulnérable. Ensuite, vous pouvez également acquérir Surity 3600 d'AT&T pour la modique somme de 1 200 dollars. Ce produit utilise pour le cryptage la fameuse puce Clipper du gouvernement américain, avec dépôts de clés pour faciliter les écoutes téléphoniques. Enfin, vous pouvez bien sûr commander dans les catalogues, soi-disant spécialisés dans les accessoires d'espionnage, des brouilleurs de voix analogiques (non numériques), qui ne sont ni plus ni moins que des gadgets inutiles pour ce qui est de la cryptographie, mais qui sont commercialisés comme produits de communications « sécurisés » à des utilisateurs crédules.

D'une certaine façon, l'éthique dans le domaine de la cryptographie est la même que dans l'industrie pharmaceutique. L'intégrité est une règle cruciale. Il est difficile de distinguer des ampoules de pénicilline de bonne ou de mauvaise qualité. Il est facile d'évaluer un tableur, mais comment savoir si un module de cryptographie est vulnérable ? Rien ne différencie un texte chiffré généré par un algorithme de cryptage défaillant d'un texte chiffré créé par un algorithme performant. Le commerce propose beaucoup de remèdes de charlatan et de médicaments miracle. Mais contrairement aux camelots de l'ancien temps, ces concepteurs logiciels ne savent généralement pas que leur portion n'est que de la poudre de perlimpinpin. Il s'agit sans aucun doute d'ingénieurs informatiques remarquables, mais ils n'ont sûrement jamais lu aucun des ouvrages académiques traitant de la cryptographie. Pourtant, ils restent persuadés qu'ils sont capables de développer un logiciel de cryptage performant. Et pourquoi pas ? A première vue, cela paraît plutôt intuitif. Et leur logiciel semble fonctionner correctement.

Toute personne croyant avoir conçu un procédé de cryptage inviolable est soit un génie hors du commun, soit un grand naïf totalement inexpérimenté. Hélas, j'ai eu souvent affaire à des apprentis cryptographes qui souhaitaient apporter des « améliorations » à PGP en ajoutant des algorithmes de cryptage de leur cru.

Je me souviens d'une conversation avec Brian Snow, un cryptographe éminent de la NSA. Il me déclara qu'il ne pourrait jamais se fier à un algorithme de cryptage, élaboré par quelqu'un qui n'avait pas d'abord gagné ses galons en cassant du code. Cela semblait tomber sous le sens. J'observai alors que pratiquement personne dans le monde commercial de la cryptographie ne répondait à ce critère. « Oui », me répondit-il avec un sourire plein d'assurance,

« Et, c'est ce qui rend notre travail à la NSA si facile ». J'en eus froid dans le dos. Je ne possédais pas non plus toutes les compétences requises.

Le gouvernement a également colporté des boniments. Après la deuxième guerre mondiale, les Etats-Unis ont vendu à des gouvernements du tiers-monde des équipements allemands de chiffrement utilisant le code Enigma. Mais, bien sûr, il omirent de préciser que les alliés avaient déjà cassé ce code pendant la guerre, un fait qui demeura classé défense pendant de nombreuses années. Aujourd'hui encore, de nombreux systèmes UNIX, de par le monde, utilisent la méthode de chiffrement Enigma pour le cryptage des fichiers, en partie car le gouvernement a créé de nombreux obstacles légaux contre l'implémentation de meilleurs algorithmes. En 1977, l'état a même été jusqu'à tenter d'empêcher la publication initiale de l'algorithme RSA et, pendant de longues années, il a littéralement étouffé tout effort commercial pour développer, à l'attention du grand public, des téléphones réellement sécurisés.

La tâche principale de l'agence de sécurité nationale du gouvernement des Etats-Unis consiste à rassembler des renseignements, essentiellement par des écoutes clandestines des communications privées de la population (reportez-vous à l'ouvrage de James Bamford, intitulé *The Puzzle Palace*). La NSA a accumulé des compétences et des ressources considérables dans l'art du piratage de codes. Lorsque la population est dans l'impossibilité de se protéger au moyen d'un système cryptographique efficace, le travail de la NSA s'en trouve ainsi facilité. De plus, l'agence de sécurité nationale du gouvernement des Etats-Unis est également chargée d'approuver et de recommander les algorithmes de cryptage. Certaines critiques font valoir qu'il y a conflit d'intérêt. Autant demander au renard de garder le poulailler ! Dans les années quatre-vingt, la NSA a préconisé l'utilisation d'un algorithme de cryptage qui avait été créé par ses employés (le programme d'approbation COMSEC), tout en refusant de dévoiler ses rouages sous le prétexte qu'il était classé défense. L'agence souhaitait simplement que tout le monde l'adopte les yeux fermés. Néanmoins, tous les cryptographes vous diront qu'un algorithme correctement conçu n'a pas besoin d'être classé défense pour rester sécurisé. Seules les clés doivent être protégées. Et puis, comment être parfaitement sûr qu'un algorithme classé défense par la NSA est réellement sécurisé ? Si personne ne peut vérifier leur algorithme, cela serait vraiment un jeu d'enfant pour la NSA d'élaborer un code de cryptage qu'ils seraient les seuls à pouvoir casser.

Trois facteurs déterminants sont à l'origine de la qualité médiocre des logiciels de cryptographie commercialisés aux Etats-Unis.

- Le premier réside dans le manque de compétences quasiment généralisé des concepteurs de logiciels de cryptage du commerce (bien que cela soit en train de changer depuis la publication de PGP). Tous les ingénieurs informatiques ont tendance à se prendre pour des cryptographes, ce qui a conduit à une prolifération de logiciels de cryptographie d'un niveau désastreux.

- Le deuxième facteur est dû à la volonté délibérée et systématique de la NSA d'éliminer toute technologie de cryptage valable, par des intimidations juridiques et des pressions économiques. Une partie de ces pressions a été exercée par des contrôles sévères sur l'exportation des logiciels de cryptage dont l'effet immédiat, en raison des lois économiques du marketing, a été d'anéantir la production nationale.

- Le troisième principe à la base de cette méthode d'élimination a consisté à n'accorder des brevets logiciels pour tous les algorithmes de cryptage de clés publiques qu'à une seule et unique entreprise, créant ainsi un goulet d'étranglement afin d'empêcher toute propagation de cette technologie (quoique ce cartel se soit disloqué à l'automne 1995).

Le résultat direct de ces efforts est qu'avant la publication de PGP, il n'existait, aux Etats-Unis, pratiquement aucun logiciel de cryptage polyvalent hautement sécurisé.

Aujourd'hui, je ne suis pas aussi certain de la sécurité de PGP que je ne l'étais jadis lors de mes exploits universitaires. Dans le cas contraire, cela serait vraiment un mauvais signe. Mais, je ne pense pas que PGP présente des défaillances évidentes (bien que je sois à peu près sûr qu'il contienne des bogues). J'ai sélectionné les meilleurs algorithmes dans les publications universitaires traitant de la cryptologie et non destinées à la défense. Pour la plupart, ces algorithmes ont fait l'objet individuellement d'un examen minutieux de la part de mes homologues. Je connais dans le monde de nombreux cryptographes de renom et j'ai discuté avec certain d'entre eux des algorithmes et des protocoles utilisés dans PGP. Ce produit a fait l'objet de recherches exhaustives et sa conception a pris de nombreuses années. Et, le plus important, je ne travaille pas pour la NSA. Toutefois, je ne vous demande pas de me croire sur parole lorsque je vous parle de l'intégrité de PGP, car son code source est disponible afin de faciliter son évaluation.

Il existe enfin une dernière preuve de mon engagement à garantir la qualité de PGP. Depuis les premiers balbutiements de PGP et sa distribution gratuite en 1991, j'ai fait l'objet, pendant trois ans, d'une enquête par les services de douane américains en raison de la diffusion à l'étranger de PGP, avec le risque de poursuites criminelles et de plusieurs années d'emprisonnement. D'ailleurs, auparavant aucun logiciel de cryptographie n'avait jamais autant dérangé le gouvernement (c'est bien PGP qui déclenche toutes ces foudres). Est-ce que cela ne vous en dit pas plus sur la force de PGP ? Toute ma réputation repose sur l'intégrité cryptographique de mes produits. Je ne renierai pas mon engagement à défendre votre droit à la confidentialité pour lequel j'ai risqué ma liberté. Je ne suis pas prêt à apposer mon nom sur un produit qui pourrait comporter un passage secret.

Vulnérabilités

« Si tous les ordinateurs du monde (260 millions) travaillaient ensemble, il leur faudrait tout de même, en moyenne, 12 millions de fois l'âge de l'univers pour casser un seul message crypté par PGP ».

--William Crowell, Directeur adjoint, Agence de sécurité nationale du gouvernement des Etats-Unis, 20 mars 1997.

Aucun système de sécurité de données n'est impénétrable. PGP peut être mis en échec de diverses manières. Dans tout système de sécurité de données, vous devez d'abord vous poser la question si les informations que vous tentez de protéger présentent aux yeux des pirates informatiques une valeur plus importante que le coût de l'attaque elle-même. Cette stratégie devrait vous amener à vous prémunir contre les attaques les moins coûteuses et à ne pas vous tracasser pour les plus onéreuses. Il est possible que le débat qui va suivre vous paraisse exagérément paranoïaque, mais une telle attitude est parfaitement appropriée lorsque le sujet de la vulnérabilité est abordé.

Sécurité du mot de passe complexe et de la clé privée

L'attaque la plus simple dont vous pouvez faire l'objet peut probablement survenir si vous notez quelque part le mot de passe complexe de votre clé privée. Si quelqu'un arrive à l'obtenir et accède également au fichier de votre clé privée, il pourra alors lire vos messages et effectuer des signatures en votre nom.

Voici quelques recommandations qui vous aideront à protéger votre mot de passe complexe :

1. N'utilisez pas de mots de passe complexes évidents, pouvant facilement être devinés, tels que les noms de vos enfants ou de votre conjoint.

2. Ajoutez à votre mot de passe complexe des espaces, ainsi qu'une combinaison de chiffres et de lettres. Si votre mot de passe complexe est constitué d'un seul mot, il pourra facilement être trouvé par une recherche informatique de tous les mots du dictionnaire. C'est la raison pour laquelle un mot de passe complexe est préférable à un simple mot de passe. Toutefois, un pirate sophistiqué peut parcourir à l'aide de son ordinateur un recueil de citations célèbres afin de deviner votre mot de passe complexe.

3. Faites preuve d'imagination. Utilisez un mot de passe complexe dont vous vous souviendrez facilement, quoique difficile à deviner. Vous pouvez, par exemple, inventer de toutes pièces une phrase absurde ou recourir à une citation littéraire tirée d'un ouvrage d'un auteur obscur.

Falsification de clé publique

Le risque principal de vulnérabilité réside dans la falsification des clés publiques. Ce point faible du système de cryptographie de clé publique est d'une importance cruciale, en partie, car la plupart des novices ne reconnaissent pas immédiatement cette contrefaçon.

En deux mots, lorsque vous utilisez la clé publique de quelqu'un d'autre, assurez-vous qu'elle n'a pas été falsifiée. Vous ne devez vous fier à une clé publique provenant d'un tiers uniquement si vous l'avez obtenue directement de son détenteur ou si elle a été signée par une personne à qui vous faites confiance. Prenez les précautions nécessaires afin que personne ne puisse falsifier votre trousseau de clés publiques. Gardez un œil sur vos trousseaux de clés publiques et privées. Il est préférable de les stocker sur votre ordinateur personnel, plutôt que sur un système partagé distant. Conservez une copie de sauvegarde de vos deux trousseaux de clés.

Suppression de fichiers incomplète

Une des autres menaces pesant sur la sécurité est due au système de suppression des fichiers de la plupart des systèmes d'exploitation. Lorsque vous cryptez un fichier, puis supprimez le texte en clair d'origine, en réalité le système d'exploitation n'efface pas physiquement les données. Il désigne simplement ces blocs disque comme supprimés, autorisant ainsi leur réutilisation ultérieure. Cela revient un peu à jeter des dossiers confidentiels dans la corbeille de recyclage, au lieu d'utiliser le broyeur à documents. Les blocs disque contiennent encore les informations sensibles que vous souhaitiez effacer et seront probablement écrasés par de nouvelles données à un moment ou un autre. Si un pirate informatique lit ces blocs disque effacés immédiatement après leur libération, il pourra alors récupérer votre texte non crypté.

En fait, cette récupération de données résiduelles peut également survenir accidentellement, par exemple, si votre disque ou certains fichiers étaient involontairement effacés ou altérés. Dans un tel cas, il est possible de lancer un programme de réparation afin de tenter de récupérer les fichiers endommagés. Cependant, il arrive alors souvent que des fichiers effacés ressuscitent. Vos fichiers confidentiels que vous croyiez éliminés à tout jamais peuvent ainsi réapparaître, puis être consultés par la personne intervenant sur votre disque. De plus, lors de la création de votre message d'origine à l'aide d'un traitement ou d'un éditeur de texte, cette application génère automatiquement une multitude de copies temporaires de votre texte sur le disque. A la fermeture de votre fichier, ces copies temporaires sont supprimées, mais ces fragments sensibles peuvent demeurer quelque part sur votre disque.

La seule manière d'empêcher la réapparition du texte en clair est de provoquer d'une façon ou d'une autre son écrasement. A moins d'être sûr et certain que tous les blocs disque effacés seront rapidement réutilisés, vous devez prendre des mesures concrètes afin d'écraser le texte en clair, ainsi que tout fragment pouvant avoir été abandonné par votre traitement de texte sur votre disque. Pour effacer toute trace de votre texte confidentiel, utilisez les fonctionnalités d'effacement sécurisé et d'effacement de l'espace libre de PGP.

Virus et chevaux de Troie

Une autre attaque pourrait être occasionnée par un virus informatique hostile qui infecterait PGP ou votre système d'exploitation. Ce virus éventuel serait spécialement conçu pour s'emparer de votre mot de passe complexe, de votre clé privée ou de vos messages cryptés et pour enregistrer clandestinement ces informations volées sur un fichier, transmis ultérieurement via le réseau au détenteur du virus. Il pourrait également altérer le comportement de PGP afin que les signatures ne soient pas correctement vérifiées. Ces attaques sont moins onéreuses que des agressions par cryptanalyse.

La protection contre ce type d'attaque relève du domaine général de la défense contre les infections virales. Il existe dans le commerce des produits antivirus assez performants et il convient de respecter certaines précautions afin de réduire considérablement le risque de propagation d'un virus. Une description exhaustive des mesures antivirales dépasse le cadre de notre présentation. PGP n'est pas protégé contre les virus, car votre ordinateur personnel est supposé fonctionner dans un environnement sûr. Si un tel virus venait à naître, il faut espérer que la nouvelle finirait par se répandre.

Une attaque similaire consiste à créer une imitation astucieuse de PGP, présentant un comportement pratiquement identique à l'original, mais ne fonctionnant pas comme prévu. Par exemple, il est possible d'altérer délibérément l'application afin que les signatures ne soient pas vérifiées correctement, autorisant ainsi la validation de faux certificats de clés. Pour un pirate informatique, il est facile de créer un tel *cheval de Troie*, car le code source de PGP est accessible à tous. Il est donc à la portée de tout informaticien de modifier ce code source, puis d'engendrer un zombie lobotomisé de PGP qui paraît authentique, mais qui suit les ordres de son maître satanique. Ce cheval de Troie pourrait ensuite être diffusé à grande échelle, sous la fausse allégation d'être d'une origine légitime. N'est-ce pas insidieux ?

Cela vaut peut-être la peine de se procurer une copie directement auprès de Network Associates, Inc.

Il existe d'autres moyens de vérifier la non falsification de PGP, notamment avec les signatures numériques. Pour vérifier une signature sur une version suspecte de PGP, vous pouvez recourir à une version sûre de PGP. Cependant, cette méthode ne sera d'aucune utilité si votre système d'exploitation est infecté ou si votre original de l'exécutable pgp.exe a été altéré intentionnellement de façon à compromettre sa capacité à contrôler les signatures. Ce test suppose que vous possédez une copie fiable de la clé publique utilisée pour vérifier la signature sur l'exécutable de PGP.

Fichiers d'échange ou mémoire virtuelle

A l'origine, PGP a été développé pour MS-DOS, un système d'exploitation archaïque selon les standards actuels. Lors de son portage sur des systèmes d'exploitation plus évolués, tels que Microsoft Windows et le Mac OS, un nouveau point faible a émergé. Cette vulnérabilité découle du fait que ces systèmes d'exploitation sophistiqués recourent à une technique appelée la *mémoire virtuelle*.

La mémoire virtuelle vous permet d'exécuter des applications volumineuses qui exigent davantage de mémoire que l'espace disponible sur les circuits intégrés à semi-conducteur de votre ordinateur. Ce procédé est pratique car les logiciels sont de plus en plus gourmands en mémoire depuis que les interfaces graphiques sont devenues la norme et que les utilisateurs ont pris l'habitude d'exécuter simultanément plusieurs applications volumineuses. En règle générale, le système d'exploitation utilise le disque dur pour le stockage des portions de logiciel temporairement non utilisées. Le système d'exploitation peut ainsi, sans que vous ne le sachiez, écrire sur le disque des informations, telles que des clés, des mots de passe complexes et du texte en clair décrypté, censées être conservées uniquement dans la mémoire centrale. PGP ne conserve pas ces données sensibles en mémoire plus longtemps que nécessaire, mais le risque que le système d'exploitation inscrive ces informations sur le disque dur n'est pas exclu.

Ces données sont enregistrées dans une zone de mémoire auxiliaire du disque, connue sous le nom de *fichier d'échange*. Dès que nécessaire, ces informations peuvent être récupérées pour lecture à partir du fichier d'échange, afin de ne stocker dans la mémoire physique qu'une portion de votre application ou de vos données. L'ensemble de cette activité est transparente pour l'utilisateur qui perçoit uniquement les sonorités caractéristiques d'un disque en cours de traitement. Microsoft Windows permute les segments de mémoire, appelés *pages*, à l'aide de l'algorithme de remplacement de page LRU (Least Recently Used). Autrement dit, les pages pour lesquelles l'accès est le moins récent seront les premières à être permutées sur le disque. Selon cette approche, il est probable que le risque de basculer des données confidentielles sur le disque est plutôt réduit, car PGP ne les conserve pas longtemps en mémoire. Toutefois, il est impossible d'apporter une garantie formelle.

En outre, toute personne pouvant accéder physiquement à votre ordinateur peut consulter ce fichier d'échange. Si ce problème vous inquiète, vous pouvez y remédier en vous procurant un logiciel spécifique permettant d'écraser votre fichier d'échange. Une autre solution consiste également à désactiver la mémoire virtuelle. Microsoft Windows et Mac OS possèdent cette fonctionnalité. Toutefois, si vous désactivez la mémoire virtuelle il est possible que vous ayez besoin d'installer des barrettes de mémoire supplémentaires, afin de pouvoir stocker l'ensemble de vos informations sur la mémoire vive.

Violation de la sécurité physique

Une violation de la sécurité peut autoriser un individu à obtenir physiquement vos textes en clair ou les impressions de vos messages. Un adversaire déterminé ne reculera ni devant le cambriolage, la fouille de vos ordures, des enquêtes ou des saisies au-delà du raisonnable, la corruption, le chantage, ni même l'infiltration de votre personnel. Certaines de ces attaques ne paraissent pas si invraisemblables lorsqu'il s'agit d'infiltrer des organisations politiques de masse qui dépendent de nombreux volontaires.

Ne vous laissez pas aller à un sentiment de sécurité trompeur pour la seule raison que vous possédez un outil cryptographique. Ces techniques protègent vos données uniquement lorsqu'elles sont cryptées. Une fuite au niveau de la sécurité peut toujours exposer vos données en clair ou, même, vos informations écrites ou parlées.

Ces attaques sont moins onéreuses que des agressions par cryptanalyse de PGP.

Attaques Tempest

Certains adversaires, particulièrement bien équipés, ont eu recours à la détection à distance des signaux électromagnétiques émis par votre ordinateur. Ce piratage coûteux en termes de technologie et de main-d'œuvre demeure tout de même moins onéreux qu'une attaque par cryptanalyse. Dans ce type de scénario, une camionnette équipée de manière appropriée se gare à proximité de vos bureaux, puis intercepte vos séquences de touches, ainsi que les messages affichés sur l'écran vidéo de votre ordinateur. Tous vos mots de passe, messages, etc. sont ainsi mis en péril. Il est possible de contrecarrer ce type d'attaque par un blindage approprié de votre matériel informatique et de votre câblage réseau afin d'éliminer toute émission de signaux. Cette technologie de blindage électronique, connue sous l'appellation « Tempest », est utilisée par certaines agences gouvernementales et par une partie de l'industrie militaire. Vous pouvez vous procurer ce type de blindage auprès de certains revendeurs de matériel informatique.

Certaines versions de PGP (versions 6.0 et ultérieures) permettent d'afficher le texte en clair décrypté à l'aide d'une police spécifique présentant des niveaux réduits d'émissions radio-électriques à partir de l'écran vidéo de votre ordinateur. La détection à distance des signaux est ainsi plus difficile à réaliser. Cette police spéciale est disponible dans certaines versions de PGP prenant en charge la fonction « Affichage sécurisé ».

Protection contre les horodatages erronés

Un des points vulnérables de PGP quelque peu ignoré consiste pour des utilisateurs malhonnêtes à falsifier les horodatages de leurs certificats et signatures de leur clé publique. Vous pouvez ne pas prendre connaissance de cette section si vous n'êtes pas un utilisateur expérimenté de PGP ou si vous n'êtes pas parfaitement au fait des protocoles de clés publiques.

Rien ne peut empêcher un utilisateur indélicat de modifier le réglage de la date et de l'heure de son horloge système et de générer des certificats et des signatures de clé publique qui paraîtront avoir été créés à un autre moment. Il peut ainsi faire croire que sa signature a été apposée ou que sa paire de clés publique / privée a été créée avant ou après la date réelle. Cet acte peut présenter pour lui certains avantages légaux ou financiers s'il souhaite, par exemple, se ménager une porte de sortie afin de pouvoir répudier une signature.

A mon avis, ce problème de falsification des horodatages des signatures numériques existe déjà pour les signatures manuscrites. N'importe quelle date peut être ajoutée à une signature manuscrite d'un contrat et personne ne semble s'en inquiéter outre mesure. Et même, dans certains cas, une date « incorrecte » sur une signature manuscrite peut ne pas être considérée comme une pratique frauduleuse. Un horodatage peut attester de la date réelle de la signature d'un document ou de la date à laquelle le signataire souhaite que sa signature soit effective.

Dans des situations où il est primordial de pouvoir s'assurer qu'une signature comporte une date correcte et non falsifiée, il suffit de faire appel à un notaire pour certifier et dater la signature. Une méthode analogue peut être appliquée aux signatures numériques. Dans ce cas, il sera demandé à un tiers en qui l'on a toute confiance de contresigner un certificat de signature et d'y apposer un horodatage fiable. Inutile de mettre en place des protocoles excessivement compliqués. Les attestations de signature ont toujours été reconnues comme une manière légitime d'établir la date exacte de la signature d'un document.

Une autorité de certification digne de confiance ou un notaire pourrait créer des signatures certifiées conformes, avec un horodatage authentifié. Ce système ne nécessiterait pas obligatoirement l'intervention d'une administration centralisée. Un correspondant fiable ou une tierce partie désintéressée pourrait même jouer ce rôle, de la même manière que les notaires de nos provinces le font. Lorsqu'un notaire contresigne la signature d'autres personnes, il crée ainsi un certificat de signature d'un autre certificat de signature. Pour les signatures numériques, sa tâche serait pratiquement identique à celle qu'il remplit déjà pour attester des signatures manuscrites. Il lui suffirait ensuite

d'entrer le certificat de la signature (séparé du document signé) dans un registre notarié spécifique. Toute personne pourrait avoir accès à ce registre. La signature du notaire comporterait alors un horodatage certifié conforme qui, du point de vue de la crédibilité et au sens légal le plus strict, serait plus fiable que l'horodatage de la signature d'origine.

Dans son article, paru en 1983 dans IEEE Computer, Denning a déjà traité ce sujet de manière approfondie. Dans des versions ultérieures de PGP, des fonctionnalités facilitant l'attestation des signatures par notaire, avec des horodatages certifiés conformes, pourraient être ajoutées.

Exposition sur des systèmes multi-utilisateurs

A l'origine, PGP a été conçu pour un PC mono-utilisateur, avec contrôle physique direct. Si vous utilisez PGP à votre domicile sur votre ordinateur personnel, vos fichiers cryptés ne risquent pratiquement rien, à moins que quelqu'un ne s'introduise dans votre maison, dérobe votre ordinateur, puis vous persuade de lui indiquer votre mot de passe complexe (ou que celui-ci soit suffisamment simple à deviner).

PGP n'est pas conçu pour protéger vos données sous forme non-cryptées lorsqu'elles sont situées sur un système exposé. De plus, rien ne peut empêcher un intrus d'employer des méthodes sophistiquées pour lire votre clé privée lorsque vous l'utilisez. Vous devez donc tenir compte de ces risques sur les systèmes multi-utilisateurs et adapter vos attentes et votre comportement en conséquence. Dans votre situation particulière, vous devrez peut-être utiliser PGP uniquement sur un système isolé mono-utilisateur directement sous votre contrôle physique.

Analyse du trafic

Même si le pirate est dans l'incapacité de lire le contenu de vos messages cryptés, il peut déduire certaines informations d'importance à partir de la provenance et de la destination de ces messages, de leur taille et de leur heure d'envoi. Cette pratique ressemble à la consultation frauduleuse de votre facture de téléphone quant à vos appels longue distance, pour en déduire quels sont vos correspondants, à quelles dates vous les contactez et la durée de vos conversations, même si elle ne permet pas de connaître la nature de vos appels. Cette technique est appelée l'analyse du trafic. PGP seul ne vous fournit pas de protection contre ce type d'analyse. Pour résoudre ce problème, il convient d'utiliser des protocoles de communication spécialisés, conçus pour réduire les risques d'analyse du trafic dans votre environnement de communication, en y associant, si possible, une aide cryptographique.

Cryptanalyse

Quoique très onéreuse, une attaque extraordinaire basée sur l'analyse cryptographique pourrait être déployée par un individu disposant d'énormes ressources informatiques, telle une agence gouvernementale. Cet individu serait alors en mesure de casser le cryptage de votre clé publique à l'aide d'une quelconque nouvelle technique mathématique secrète. Toutefois, la défense civile n'a cessé d'attaquer la cryptographie des clés publiques, et ce sans succès depuis 1978.

Le gouvernement américain dispose certainement de méthodes secrètes pour casser les algorithmes de cryptage conventionnels utilisés dans PGP. Il s'agit là du pire cauchemar de tout cryptographe. Il n'existe aucune sécurité absolue garantissant la mise en pratique de la cryptographie.

Il n'en demeure pas moins qu'un certain optimisme se justifie. Les algorithmes de clés publiques, de résumés de messages et le chiffrement par bloc utilisés dans PGP ont été développés par certains des meilleurs cryptographes au monde. Les algorithmes de PGP ont subi des analyses de sécurité et des révisions croisées intensives, menées par certains des meilleurs cryptanalystes ne dépendant pas de l'armée.

Par ailleurs, bien que le chiffrement par bloc utilisé dans PGP comporte quelques faiblesses mineures, PGP compresse le texte d'origine avant le cryptage, ce qui permet d'atténuer sensiblement ces faiblesses. Le travail informatique nécessaire au piratage devient alors bien plus onéreux que la valeur intrinsèque du message.

Si votre situation justifie vos craintes quant à des attaques de ce type, il est alors recommandé de contacter un consultant spécialisé dans la sécurité des données, afin de mettre en place des solutions personnalisées adaptées à vos besoins spécifiques.

En résumé, sans une bonne protection cryptographique de vos communications de données, tout pirate peut pratiquement sans effort intercepter vos messages, parfois même avec une certaine routine, et spécialement s'ils ont été envoyés par modem ou système de messagerie. Si vous utilisez PGP et suivez des mesures de précaution raisonnables, le pirate devra redoubler d'efforts et de moyens pour violer votre intimité.

De plus, si vous vous protégez contre les attaques les plus simples et restez confiant quant à la possibilité d'attaques menées par un pirate déterminé et plein de ressources, PGP vous garantira une sécurité presque parfaite.

Listes de mots biométriques

Par Philip Zimmermann et Patrick Juola

PGP utilise une liste de mots spécifique pour transférer les informations binaires de manière authentifiée sur un canal vocal, tel qu'un téléphone, via des signatures biométriques. La voix humaine prononçant ces mots, si elle est reconnue par l'auditeur, sert à l'authentification biométrique des données transportées par ces mots. La finalité de cette liste de mots est identique à celle de l'alphabet militaire : elle permet l'acheminement des lettres sur un canal vocal radio parasité. Cependant, l'alphabet militaire comporte 26 mots, chacun représentant une lettre. Notre liste, quant à elle, comporte 256 mots phonétiquement distincts soigneusement sélectionnés, représentant les 256 valeurs de type octet possibles comprises entre 0 et 255.

Nous avons créé une liste de mots pour la lecture des informations binaires par téléphone, chaque mot représentant une valeur de type octet différente. Nous avons tenté de concevoir une liste de mots pour diverses applications. La première application envisagée consistait à lire les empreintes digitales des clés publiques de PGP par téléphone, afin de les authentifier. Dans ce cas, l'empreinte digitale est d'une longueur de 20 octets, nécessitant la lecture de 20 mots à voix haute. Il s'est avéré que la lecture de tant d'octets en hexadécimal était fastidieuse et pouvait entraîner des erreurs. Il est donc préférable d'utiliser une liste de mots, où chaque mot représente un octet.

Certaines applications peuvent nécessiter la transmission de séquences d'octets encore plus longues par téléphone, par exemple, des clés et des signatures entières, ce qui peut impliquer la lecture de plus d'une centaine d'octets. L'utilisation de mots plutôt que d'octets hexadécimaux semble encore plus justifiée dans ce cas.

Des erreurs peuvent se glisser lors de la lecture à voix haute de longues séquences d'octets. Les types de syndromes d'erreurs générées par les données lues par l'homme diffèrent de ceux générés lors de la transmission des données via un modem. Les erreurs de modem impliquent généralement des bits permutés à cause du parasitage de la ligne. Les méthodes de détection d'erreurs pour les modems entraînent généralement l'ajout de codes CRC, optimisés pour la détection des séquences de bruit de la ligne. Cependant, les séquences aléatoires de mots prononcés par l'homme entraînent généralement l'un des trois types d'erreurs suivants : 1) transposition de deux mots consécutifs, 2) duplication de mots ou 3) omission de mots. Si nous devions concevoir un schéma de détection des erreurs pour ce type de canal de transmission des données, il serait nécessaire qu'il prenne en compte ces trois types d'erreurs. Zhahai Stewart a proposé un schéma satisfaisant (lors d'une conversation privée en 1991) pour détecter ces erreurs.

Le schéma de Stewart concernant la détection des erreurs lors de la lecture à voix haute de longues séquences d'octets via une liste de mots implique l'utilisation non pas d'une liste de mots, mais de deux. Chaque liste contient 256 mots phonétiquement distincts, chaque mot représentant une valeur de type octet différente comprise entre 0 et 255. Les deux listes sont utilisées à tour de rôle pour les octets de décalage pair et impair dans la séquence d'octets.

Par exemple, le premier octet (décalage 0 dans la séquence) est utilisé pour sélectionner un mot dans la liste paire. L'octet au décalage 1 est utilisé pour sélectionner un octet dans la liste impaire. L'octet au décalage 2 permet de sélectionner à nouveau un mot dans la liste paire et celui au décalage 3 permet de sélectionner à nouveau un mot dans la liste impaire. Chaque valeur de type octet est en réalité représentée par deux mots différents, en fonction de la présence de l'octet au décalage pair ou impair depuis le début de la séquence d'octets. Prenons l'exemple des mots « adult » et « amulet », chacun apparaissant à la même position dans les deux listes de mots, à savoir la position 5. La séquence de 3 octets de répétition 05 05 05 est alors représentée par la séquence des trois mots « adult, amulet, adult ».

Cette approche facilite la détection des trois types d'erreurs communes contenues dans les flux de données prononcées : transposition, duplication et omission. Une transposition produit deux mots consécutifs de la liste paire, suivis de deux mots consécutifs de la liste impaire (ou inversement). Une duplication est reconnaissable par deux mots en double consécutifs, situation ne pouvant se produire dans une séquence classique. Une omission est repérée par deux mots consécutifs provenant de la même liste.

Pour que l'être humain puisse détecter facilement et immédiatement l'un des trois syndromes d'erreurs décrits ci-dessus, sans utiliser d'ordinateur, nous avons créé une propriété clairement différente pour chacune des deux listes : la liste paire contient uniquement des mots à deux syllabes et la liste impaire des mots à trois syllabes. Cette suggestion provient de Patrick Juola, linguiste informatique.

PGPfone est l'application qui a permis d'accélérer la mise en place réelle de la liste de mots de Juola et Zimmermann. Cette application transforme votre ordinateur en téléphone sécurisé. Nous l'avons utilisée pour authentifier l'échange de la clé Diffie-Hellman d'origine de PGPfone sans employer de signatures numériques, ni d'infrastructures de clé publique. Nous savions que nous finirions par utiliser PGPfone pour authentifier les empreintes digitales des clés lorsque nous l'avons appliquée, plus tard, à PGP.

L'idée se profilant derrière la création de listes de mots était l'élaboration d'une unité métrique servant à mesurer la distance phonétique entre deux mots, puis son utilisation comme une mesure absolue dans le but de créer une liste complète. Grady Ward a répertorié un grand nombre de mots avec leurs prononciations et Patrick Juola a élaboré le meilleur sous-ensemble de la liste de Ward à l'aide d'algorithmes génétiques. En fait, il a créé une population d'hypothèses nombreuse, qu'il a laissé se « reproduire » en échangeant des mots avec d'autres hypothèses et, à l'instar de l'évolution biologique, les meilleures hypothèses ont survécu jusqu'à la génération suivante. Après 200 générations environ, la liste s'est stabilisée pour devenir la meilleure hypothèse, avec une distance phonétique beaucoup plus importante entre les mots que dans les premières listes.

Le développement de l'unité métrique a représenté un obstacle majeur. Les linguistes ont étudié la production et la perception des sons pendant des décennies. Une série de caractéristiques standard est à présent utilisée pour décrire les sons dans la langue anglaise. Vous pouvez, par exemple, prononcer les termes « pun », « fun », « dun » et « gun » (faites-le) et remarquer le mouvement de votre langue lors de la prononciation de chaque terme. Les linguistes l'appellent le « point d'articulation ». Les bruits très différents dans cette caractéristique ont une sonorité différente pour les anglophones. La combinaison de toutes les caractéristiques sonores d'un seul mot nous donne une représentation de la sonorité globale du mot. Il est alors possible de calculer la distance phonétique entre deux mots.

En fait, cette étude n'a pas été si simple, les diverses caractéristiques étant difficiles à déterminer. Certaines caractéristiques liées au mot, telles que les accents, étaient difficiles à représenter et l'analyse reposant sur les caractéristiques est tout simplement impossible pour certains sons. D'autres critères plus subtils étaient également à prendre en considération. Ainsi, nous souhaitions que les mots soient suffisamment communs pour être reconnus universellement, sans toutefois tomber dans l'ennui. Nous ne voulions pas de mots prêtant à confusion, tels que « repeat », « begin » ou « error ». Certaines caractéristiques sonores sont moins perceptibles pour les anglophones non natifs. Ainsi, certains Japonais peuvent entendre et prononcer le « r » et le « l » de la même manière. Si les mots étaient suffisamment courts, nous pourrions en afficher un nombre suffisant sur un petit écran à cristaux liquides. Les groupes consonantiques importants (« corkscrew » comporte cinq consonances d'affilée) sont parfois difficiles à prononcer, surtout pour les non anglophones. D'une façon ou d'une autre, nous avons tenté d'intégrer tous ces critères dans un filtre situé dans la liste du dictionnaire d'origine ou dans l'unité métrique de distance elle-même.

Une fois la liste calculée par l'ordinateur, nous l'avons étudiée. Les mots étaient bel et bien distincts. Cependant, la plupart d'entre eux semblaient avoir été choisis plutôt par un ordinateur que par un être humain. Beaucoup étaient stupides, d'autres laids, voir ennuyeux et trop simples. Nous avons donc ajouté de la « substance » à cette liste. Certains mots ont été supprimés, puis remplacés par des mots choisis par l'homme. L'ordinateur a ensuite testé les nouveaux mots contenus dans la liste pour déterminer s'ils étaient phonétiquement distants du reste de la liste. Nous avons également essayé de ne pas sélectionner des mots phonétiquement trop rapprochés des autres mots du dictionnaire, pour ne pas les confondre avec des mots ne figurant pas dans la liste.

Juola a utilisé plusieurs critères de sélection dans ses algorithmes. Il a publié un article plus détaillé à ce sujet. Il s'agit d'une brève présentation du mode de création de notre liste.

Je ne suis pas pleinement satisfait de cette liste de mots. J'aurais aimé qu'elle contienne des mots plus d'actualité et moins ennuyeux. Les termes comme « Aztec » et « Capricorn » et ceux de l'alphabet militaire classique me satisfont. Bien que nous souhaitions nous réserver le droit de réviser cette liste dans le futur, il est peu probable que nous puissions le faire, étant donné les problèmes juridiques qui seront occasionnés par cette version d'origine. La dernière modification de la version de la liste remonte à septembre 1998.

Si vous avez des suggestions concernant l'ajout ou la suppression de certains mots, envoyez-les à l'adresse pgpfone-bugs@mit.edu et, par la même occasion, à Patrick Juola à juola@mathcs.duq.edu. Les listes de mots complètes, paires et impaires, sont répertoriées ci-dessous.

Liste de mots à deux syllabes

aardvark	absurd	accrue	acme	adrift
adult	afflict	ahead	aimless	Algol
allow	alone	ammo	ancient	apple
artist	assume	Athens	atlas	Aztec
baboon	backfield	backward	banjo	beaming
bedlamp	beehive	beeswax	befriend	Belfast
berserk	billiard	bison	blackjack	blockade
blowtorch	bluebird	bombast	bookshelf	brackish
breadline	breakup	brickyard	briefcase	Burbank
button	buzzard	cement	chairlift	chatter
checkup	chisel	choking	chopper	Christmas
clamshell	classic	classroom	cleanup	clockwork
cobra	commence	concert	cowbell	crackdown
cranky	crowfoot	crucial	crumpled	crusade
cubic	dashboard	deadbolt	deckhand	dogsled
dragnet	drainage	dreadful	drifter	dropper
drumbeat	drunken	Dupont	dwelling	eating
edict	egghead	eightball	endorse	endow
enlist	erase	escape	exceed	eyeglass
eyetooth	facial	fallout	flagpole	flatfoot
flytrap	fracture	framework	freedom	frighten
gazelle	Geiger	glitter	glucose	goggles
goldfish	gremlin	guidance	hamlet	highchair
hockey	indoors	indulge	inverse	involve
island	jawbone	keyboard	kickoff	kiwi
klaxon	locale	lockup	merit	minnow
miser	Mohawk	mural	music	necklace
Neptune	newborn	nightbird	Oakland	obtuse
offload	optic	orca	payday	peachy
pheasant	physique	playhouse	Pluto	preclude
prefer	preshrunk	printer	prowler	pupil
puppy	python	quadrant	quiver	quota
ragtime	ratchet	rebirth	reform	regain
reindeer	rematch	repay	retouch	revenge
reward	rhythm	ribcage	ringbolt	robust
rocker	ruffled	sailboat	sawdust	scallion
scenic	scorecard	Scotland	seabird	select
sentence	shadow	shamrock	showgirl	skullcap
skydive	slingshot	slowdown	snapline	snapshot
snowcap	snowslide	solo	southward	soybean
spaniel	spearhead	spellbind	spheroid	spigot
spindle	spyglass	stagehand	stagnate	stairway
standard	stapler	steamship	sterling	stockman
stopwatch	stormy	sugar	surmount	suspense
sweatband	swelter	tactics	talon	tapeworm
tempest	tiger	tissue	tonic	topmost
tracker	transit	trauma	treadmill	Trojan
trouble	tumor	tunnel	tycoon	uncut
unearth	unwind	uproot	upset	upshot
vapor	village	virus	Vulcan	waffle
wallet	watchword	wayside	willow	woodlark
Zulu				

Liste de mots à trois syllabes

adroitness	adviser	aftermath	aggregate	alkali
almighty	amulet	amusement	antenna	applicant
Apollo	armistice	article	asteroid	Atlantic
atmosphere	autopsy	Babylon	backwater	barbecue
belowground	bifocals	bodyguard	bookseller	borderline
bottomless	Bradbury	bravado	Brazilian	breakaway
Burlington	businessman	butterfat	Camelot	candidate
cannonball	Capricorn	caravan	caretaker	celebrate
cellulose	certify	chambermaid	Cherokee	Chicago
clergyman	coherence	combustion	commando	company
component	concurrent	confidence	conformist	congregate
consensus	consulting	corporate	corrosion	councilman
crossover	crucifix	cumbersome	customer	Dakota
decadence	December	decimal	designing	detector
detergent	determine	dictator	dinosaur	direction
disable	disbelief	disruptive	distortion	document
embezzle	enchanting	enrollment	enterprise	equation
equipment	escapade	Eskimo	everyday	examine
existence	exodus	fascinate	filament	finicky
forever	fortitude	frequency	gadgetry	Galveston
getaway	glossary	gossamer	graduate	gravity
guitarist	hamburger	Hamilton	handiwork	hazardous
headwaters	hemisphere	hesitate	hideaway	holiness
hurricane	hydraulic	impartial	impetus	inception
indigo	inertia	infancy	inferno	informant
insincere	insurgent	integrate	intention	inventive
Istanbul	Jamaica	Jupiter	leprosy	letterhead
liberty	maritime	matchmaker	maverick	Medusa
megaton	microscope	microwave	midsummer	millionaire
miracle	misnomer	molasses	molecule	Montana
monument	mosquito	narrative	nebula	newsletter
Norwegian	October	Ohio	onlooker	opulent
Orlando	outfielder	Pacific	pandemic	Pandora
paperweight	paragon	paragraph	paramount	passenger
pedigree	Pegasus	penetrate	perceptive	performance
pharmacy	phonetic	photograph	pioneer	pocketful
politeness	positive	potato	processor	provincial
proximate	puberty	publisher	pyramid	quantity
racketeer	rebellion	recipe	recover	repellent
replica	reproduce	resistor	responsive	retraction
retrieval	retrospect	revenue	revival	revolver
sandalwood	sardonic	Saturday	savagery	scavenger
sensation	sociable	souvenir	specialist	speculate
stethoscope	stupendous	supportive	surrender	suspicious
sympathy	tambourine	telephone	therapist	tobacco
tolerance	tomorrow	torpedo	tradition	travesty
trombonist	truncated	typewriter	ultimate	undaunted
underfoot	unicorn	unify	universe	unravel
upcoming	vacancy	vagabond	vertigo	Virginia
visitor	vocalist	voyager	warranty	Waterloo
whimsical	Wichita	Wilmington	Wyoming	yesteryear
Yucatan				

Glossaire

AES (norme de cryptage avancée)	Normes agréées NIST (Agence générale de normes et de technologie) et généralement utilisées au cours des 20 ou 30 prochaines années.
Algorithme (cryptage)	Ensemble de règles mathématiques (logiques) utilisées au cours des processus de cryptage et de décryptage.
Algorithme (hachage)	Ensemble de règles mathématiques (logiques) utilisées au cours des processus de création du résumé de message et de la génération de la clé / signature.
Algorithme symétrique	Egalement appelé algorithmes de clé unique, de clé secrète et conventionnel. Les clés de cryptage et de décryptage sont soit identiques, soit calculées l'une à partir de l'autre. Il existe deux sous-catégories : Bloc et Flux.
Anonymat	Dissimulation de l'identification d'une entité d'origine ou de qualité d'auteur inconnue ou non déclarée.
ANSI (Institut national américain de normalisation)	Elabore des normes via divers comités de normalisation accrédités (ASC). Le comité X9 met l'accent sur les normes de sécurité relatives à l'industrie des services financiers.
Attaque « au dictionnaire »	Attaque de force brutale calculée visant à deviner un mot de passe en essayant des combinaisons de mots évidentes et logiques.
Authentification	Définition de l'origine des informations cryptées via la vérification de la signature numérique ou de la clé publique d'un utilisateur grâce au contrôle de son empreinte digitale unique.
Autorisation	Confère à une entité une sanction officielle, ainsi que des droits d'accès ou des compétences juridiques.
Autorité de certification	Un ou plusieurs utilisateurs fiables ayant la responsabilité de la certification de l'origine des clés et leur ajout à une base de données commune.
CA (autorité de certification)	Partie tierce de confiance (PTC) créant des certificats constitués d'affirmations quant à divers attributs et les liant à une entité et / ou une clé publique.

Canal sécurisé — Méthode de transfert des informations d'une entité à une autre, de sorte que la réorganisation, la suppression, l'insertion ou la lecture par un pirate soit impossible (SSL, IPSec ou transmission des informations par chuchotement).

CAPI (API de cryptographie) — API de cryptographie de Microsoft pour les systèmes d'exploitation et applications Windows.

CAST — Chiffrement par bloc de 64 bits utilisant une clé de 64 bits, six boîtes de brouillage avec 8 bits en entrée et 32 bits en sortie. Système développé au Canada par Carlisle Adams et Stafford Tavares.

Certificat (numérique) — Document électronique associé à une clé publique par une partie tierce de confiance fournissant la preuve que la clé publique appartient à un détenteur légitime et n'a pas été compromise.

Certificat d'autorisation — Document électronique permettant à un utilisateur de prouver ses droits d'accès ou son identité.

Certification — Approbation des informations par une entité fiable.

Certifier — Signer la clé publique d'un autre utilisateur.

Chiffrement par bloc — Chiffrement symétrique opérant sur des blocs de texte en clair et de texte chiffré comprenant généralement 64 bits.

Clé — Code numérique utilisé pour le cryptage, la signature, le décryptage et la vérification des messages et des fichiers. Les clés sont réparties par paires et stockées sur des trousseaux.

Clé auto-signée — Clé publique signée par la clé privée correspondante pour preuve de son origine.

Clé de session — Clé secrète (symétrique) utilisée pour le cryptage de chaque ensemble de données sur une base de transaction. Une clé de session différente est utilisée pour chaque session de communication.

Clé privée — Partie secrète d'une paire de clés utilisée pour la signature et le décryptage des informations. La clé privée d'un utilisateur doit être connue uniquement par ce dernier.

Clé publique

L'une des deux clés d'une paire de clés est utilisée pour le cryptage des informations et la vérification des signatures. La clé publique d'un utilisateur peut être mise à la disposition de collègues de travail ou d'autres utilisateurs. La connaissance de la clé publique d'un utilisateur ne permet pas de découvrir la clé privée correspondante.

Clés asymétriques

Paire de clés utilisateur distincte, mais intégrée comprenant une clé publique et une clé privée. Chaque clé est à sens unique : si elle est utilisée pour le cryptage des informations, elle ne peut pas l'être pour le décryptage de ces mêmes données.

Clés de signature d'entreprise

Clé publique conçue par l'agent de sécurité d'une entreprise en tant que clé commune à l'ensemble du système et considérée comme fiable par tous les utilisateurs de l'entreprise pour la signature d'autres clés.

Correspondant

Utilisateur ou entreprise autorisé(e) à répondre de l'authenticité de la clé publique d'un utilisateur. Vous désignez un correspondant en signant sa clé publique.

Correspondant fiable

Utilisateurs auxquels vous faites confiance pour vous fournir des clés correctes. Lorsqu'un correspondant fiable signe la clé d'un autre utilisateur, vous considérez qu'elle est valide et ne jugez pas nécessaire de la vérifier avant de l'utiliser.

Cryptage

Méthode de brouillage des informations permettant de les rendre illisibles à tous les utilisateurs, à l'exception du destinataire concerné. Toutefois, ce dernier doit préalablement décrypter ces informations.

Cryptage conventionnel

Cryptage reposant sur un mot de passe complexe commun plutôt que sur la cryptographie d'une clé publique. Le fichier est crypté à l'aide d'une clé de session permettant le cryptage via un mot de passe complexe à définir.

Cryptanalyse

L'art ou la science de transformer le texte chiffré en texte en clair sans connaissance initiale de la clé utilisée pour le cryptage du texte en clair.

Cryptographie

L'art et la science de créer des messages à caractère privé pouvant être signés, protégés contre toute modification avec non répudiation.

Cryptographie de clé publique

Cryptographie dans laquelle une paire de clés publiques et privées est utilisée et où le canal ne doit pas nécessairement être sécurisé.

CRYPTOKI

Voir PKCS n°11.

Découpage de clé ou « partage d'un secret »

Processus de division d'une clé privée en plusieurs parties et de partage de ces parties parmi un groupe d'utilisateurs. Un nombre défini d'utilisateurs doivent rassembler les différentes parties de leur clé afin de l'utiliser.

Décryptage

Méthode de décodage des données cryptées afin de les rendre à nouveau lisibles. La clé privée du destinataire est utilisée pour ce décryptage.

Dépôt/reprise de clé

Pratique selon laquelle l'utilisateur d'un système de cryptage de clé publique soumet sa clé privée à un tiers, lui permettant ainsi de surveiller les communications cryptées.

DES (norme de cryptage de données)

Chiffrement par bloc de 64 bits, algorithme symétrique également appelé algorithme de cryptage des données (DEA) par l'ANSI et DEA-1 par l'ISO. Ce système est largement répandu depuis plus de 20 ans. Il a été adopté comme norme fédérale pour le traitement de l'information (FIPS 46) en 1976.

DES triple

Configuration de cryptage dans laquelle l'algorithme DES est utilisé trois fois avec trois clés différentes.

Diffie-Hellman

Premier algorithme de clé publique, inventé en 1976, utilisant des logarithmes discrets dans un champ fini.

DSA (Algorithme de signature numérique)

Algorithme de signature numérique de clé publique proposé par NIST (l'agence gouvernementale de normes et de technologie) pour l'utilisation dans DSS (standard de signature numérique).

DSS (Standard de signature numérique)

Standard proposé (FIPS) par NIST pour les signatures numériques à l'aide de DSA.

ECC (Système cryptographique de courbe elliptique)

Méthode unique permettant la création d'algorithmes de clés publiques en fonction des courbes mathématiques sur des champs finis ou via des nombres premiers importants.

Echange de clés

Schéma permettant à plusieurs nœuds de transférer une clé de session secrète sur un canal non sécurisé.

EES (standard de cryptage à dépôts)

Standard proposé par le gouvernement américain pour le cryptage à dépôts des clés privées.

Empreinte digitale

Chaîne de nombres et de caractères utilisée pour l'authentification des clés publiques. Il s'agit de la principale procédure de contrôle de l'authenticité d'une clé. Voir *Empreinte digitale de la clé*.

Empreinte digitale de la clé — Chaîne de nombres et de caractères utilisée pour l'authentification des clés publiques. Par exemple, vous pouvez téléphoner au détenteur d'une clé publique et lui faire lire l'empreinte digitale associée à sa clé de façon à pouvoir la comparer à celle située sur votre copie de sa clé publique et voir si elles coïncident. Si l'empreinte digitale ne coïncide pas, vous savez que vous disposez d'une clé erronée.

Fiabilité directe — Etablissement d'une confiance port à port.

Fiabilité du Web — Modèle de fiabilité largement répandu et utilisé par PGP pour valider la provenance d'une clé publique lorsque son niveau de fiabilité est cumulé en fonction de la connaissance individuelle des « correspondants ».

Fiabilité hiérarchique — Série progressive d'entités répartissant la fiabilité dans une structure organisée, généralement utilisée dans les autorités émettant les certificats ANSI X.509.

Fiabilité implicite — Réservée pour les paires de clés situées sur votre trousseau de clés local. Si la partie privée d'une paire de clés est trouvée sur votre trousseau de clés, PGP vous considère comme détenteur de cette paire de clés et suppose que vous vous faites implicitement confiance.

Fiable — Une clé publique est considérée comme fiable si elle a été validée par vous-même ou par un autre utilisateur désigné en tant que correspondant.

FIPS (Norme fédérale pour le traitement de l'information) — Norme gouvernementale américaine publiée par la NIST (agence gouvernementale de normes et de technologie).

Fonction de hachage — Fonction de hachage à sens unique générant un résumé de message qui ne peut être converti afin d'obtenir l'original.

Gestion des clés — Procédure de stockage et de distribution sécurisés de clés cryptographiques précises. Processus global de génération et de distribution sécurisées d'une clé cryptographique vers des destinataires autorisés.

Gestionnaire en chef de la sécurité — Correspondant fiable de correspondants fiables.

Hachage à sens unique — Fonction d'une chaîne de variable permettant de créer une valeur de longueur fixe et représentant l'image d'origine, également appelée résumé de message, empreinte digitale ou contrôle d'intégrité du message (MIC).

Hexadécimal

Hexadécimal désigne un système de numérotation à 16 chiffres. Il décrit un système de numérotation contenant 16 numéros de séquence comme unités de base (y compris 0) préalablement à l'ajout d'une nouvelle position pour le numéro suivant. Notez que nous utilisons « 16 » dans le cas présent comme nombre décimal pour définir un nombre égal à « 10 » au format hexadécimal. Les nombres hexadécimaux vont de 0 à 9, puis comprennent les lettres A à F.

Horodatage

Enregistrement de l'heure de création ou d'existence des informations.

HTTP (Protocole de transfert de documents hypertextuels)

Protocole commun utilisé pour le transfert de documents entre différents serveurs ou d'un serveur vers un client.

ID de clé

Code lisible permettant d'identifier une paire de clés. Deux paires de clés peuvent disposer d'un ID utilisateur identique, mais elles sont dotées d'ID de clé différente.

ID utilisateur

Texte permettant d'identifier une paire de clés. Le format habituel d'un ID utilisateur est, par exemple, le nom et l'adresse e-mail du détenteur. L'ID utilisateur permet aux utilisateurs (le détenteur et ses collègues) d'identifier le détenteur de la paire de clés.

IDEA (Norme internationale de cryptage de données)

Chiffrement symétrique de bloc de 64 bits utilisant des clés de 128 bits basées sur une combinaison d'opérations de différents groupes algébriques. Algorithme considéré comme l'un des plus complexes.

IKE (Echange de clés via Internet)

Méthode sécurisée d'échange de clés via Internet. IKE est également candidat à l'architecture de sécurité de IPsec.

Integrité

Garantie selon laquelle les données ne sont pas modifiées (par des utilisateurs non autorisés) lors du stockage ou du transfert.

Intégrité des données

Méthode garantissant que les informations n'ont pas été modifiées par des moyens illicites ou inconnus.

IPSec

Schéma de cryptage de couche TCP/IP en cours d'étude dans l'IETF (groupe de travail Internet).

ISO (Organisation internationale de normalisation)

Responsable d'un nombre important de normes, telles que le modèle OSI (interconnexion des systèmes ouverts) et les relations internationales avec l'ANSI quant à X.509.

LDAP (Protocole d'accès aux petits clients)

Protocole simple prenant en charge les opérations d'accès et de recherche sur des répertoires contenant des informations telles que des noms, numéros de téléphone et adresses sur d'autres systèmes incompatibles via Internet.

Longueur de clé

Nombre de bits correspondant à la taille de la clé. Plus la clé est longue, plus elle est complexe.

MIC (contrôle d'intégrité du message)

Défini à l'origine dans PEM (messagerie étendue de confidentialité) pour l'authentification via RM2 ou RM5. Micalg (calcul de l'intégrité du message) est utilisé dans des implémentations MIME sécurisées.

MIME (extensions de messagerie Internet multi-usages)

Ensemble disponible de spécifications offrant la possibilité d'interchanger du texte dans des langues comprenant des jeux de caractères différents et des e-mails multimédia au sein de systèmes informatiques différents utilisant des normes de messagerie Internet.

Monnaie électronique

Argent électronique stocké et transféré via plusieurs protocoles complexes.

Mot de passe

Séquence de caractères ou mot soumis par un sujet à un système à des fins d'authentification, de validation ou de vérification.

Mot de passe complexe

Mot de passe facile à retenir permettant d'améliorer la sécurité par rapport à un mot de passe simple. Le broyage d'une clé permet de la convertir en clé aléatoire.

Nombre aléatoire

Aspect important de nombreux systèmes de cryptographie et élément nécessaire à la génération d'une(de) clé(s) unique(s) ne pouvant être découverte(s) par un adversaire. Généralement, les nombres réellement aléatoires sont dérivés de sources analogiques et impliquent l'utilisation d'un matériel spécifique.

Non répudiation

Vise à empêcher la répudiation des engagements ou actions précédent(e)s.

Paire de clés

Elle est composée d'une clé publique et de sa clé privée complémentaire. Dans les systèmes de cryptographie tels que le programme PGP, chaque utilisateur dispose au minimum d'une paire de clés.

Pare-feu

Combinaison matérielle et logicielle permettant de protéger le périmètre du réseau public / privé contre des attaques spécifiques et ce, afin de garantir un certain degré de sécurité.

Partage d'un secret

voir *Découpage de clé*.

PGP/MIME	Norme IETF (RFC 2015) offrant confidentialité et authentification à l'aide des types de contenu de sécurité MIME (extensions de messagerie Internet multi-usages) décrits dans la demande de commentaire RFC1847, actuellement disponible dans les versions PGP 5.0 et ultérieures.
PKCS (Normes de cryptographie des clés publiques)	Ensemble de normes de facto pour la cryptographie de clés publiques développé conjointement avec un groupement informel d'entreprises (Apple, DEC, Lotus, Microsoft, MIT, RSA et Sun) comprenant des normes d'implémentation spécifiques aux algorithmes spécifiques et indépendantes des algorithmes. Spécifications définissant la syntaxe du message et d'autres protocoles contrôlés par RSA Data Security Inc.
PKI (Infrastructure de clé publique)	Système de certification largement disponible et accessible permettant, avec un niveau de fiabilité plus ou moins élevé, d'obtenir la clé publique d'une entité et de vous assurer qu'elle n'a pas été révoquée.
Résumé de message	Condensé de votre message ou somme de contrôle de votre fichier. Il représente votre message. Si celui-ci a été modifié de quelque manière que ce soit, un résumé de message différent est généré.
Révocation	Reprise de la certification ou de l'autorisation.
RFC (demande de commentaire)	Document IETF, soit des sous-séries RFC FYI (à titre informatif) correspondant à des présentations et à des introductions, soit des sous-séries RFC STD permettant d'identifier et de définir des normes Internet. Chaque demande de commentaire est indexée par un numéro, facilitant sa récupération (www.ietf.org).
RSA	Diminutif de RSA Data Security, Inc., se rapportant à Ron Rivest, Adi Shamir et Len Adleman ou à l'algorithme qu'ils ont inventé. L'algorithme RSA est utilisé dans la cryptographie de clés publiques et repose sur le fait qu'il est facile de multiplier deux nombres premiers importants, mais difficile de les factoriser à partir du produit.
S/MIME (extension de messagerie Internet multi-usages)	Norme proposée développée par le logiciel Deming et RSA Data Security pour le cryptage et/ou l'authentification des données MIME. S/MIME définit un format pour les données MIME, les algorithmes devant être utilisés pour l'interopérabilité (RSA, RC2, SHA-1) et les questions opérationnelles supplémentaires, telles que les certificats ANSI X.509 et le transfert via Internet.

Schéma Elgamal

Utilisé à la fois pour les signatures numériques et le cryptage en fonction de logarithmes discrets dans un champ fini. Ce schéma peut être utilisé avec la fonction DSA.

Signature

Code numérique créé à l'aide d'une clé privée. Les signatures permettent d'authentifier les informations via le processus de vérification des signatures. Lors de la signature d'un message ou d'un fichier, le programme PGP utilise votre clé privée pour créer un code numérique spécifique à la fois au contenu du message et à la clé privée. Tout utilisateur peut avoir recours à votre clé publique pour la vérification de votre signature.

Signature aveugle

Capacité à signer un document sans connaissance de son contenu, comme pour un notaire.

Signature numérique

Voir *signature*.

Signer

Appliquer une signature.

Sous-clé

Une sous-clé est une clé de cryptage Diffie-Hellman ajoutée comme un sous-ensemble à votre clé maître. Une fois créée, vous pouvez faire expirer ou révoquer une sous-clé sans affecter votre clé maître ou les signatures qui y sont collectées.

SSL (Couche socket sécurisée)

Développée par Netscape pour offrir une sécurité et une confidentialité via Internet. Prend en charge l'authentification du client et du serveur et assure la sécurité et l'intégrité du canal de transmission. Fonctionne sur la couche de transport et imite la « bibliothèque des sockets », ce qui lui permet de ne pas dépendre de l'application. Crypte l'intégralité du canal de communication et ne prend pas en charge les signatures numériques au niveau du message.

Système de cryptographie

Système composé d'algorithmes cryptographiques, de tout texte en clair, texte chiffré et de toute clé.

Texte

Texte ASCII de 7 bits standard et imprimable.

Texte au format ASCII protégé

Informations binaires, codées à l'aide d'un jeu de caractères ASCII de 7 bits standard et imprimables, permettant de faciliter le transfert des informations via les systèmes de communication. Dans le programme PGP, une extension par défaut est affectée aux fichiers texte au format ASCII protégé. En outre, ils sont codés, puis décodés au format ASCII radix-64.

Texte chiffré

Texte en clair ayant subi un algorithme de cryptage. Une clé de cryptage permet de déverrouiller le texte en clair d'origine à partir du texte chiffré.

Texte en clair	Caractères lisibles par l'homme ou bits lisibles par l'ordinateur.
Texte en clair	Texte normal, lisible, non crypté et non signé.
TLS (Sécurité de la couche de transport)	Un avant-projet IETF de la version 1 se fonde sur le protocole SSL version 3 et fournit la confidentialité des communications sur Internet.
TLSP (Protocole de sécurité de la couche de transport)	Projet de norme internationale ISO 10736.
Trousseau de clés	Jeu de clés. Chaque utilisateur dispose de deux types de trousseaux de clés : un trousseau de clés privées et un trousseau de clés publiques.
Trousseau de clés privées	Ensemble d'une ou de plusieurs clés privées appartenant au détenteur de ce trousseau.
Trousseau de clés publiques	Jeu de clés publiques. Votre trousseau de clés publiques comporte votre(vos) propre(s) clé(s) publique(s).
Validité	Indique le niveau de confiance quant à l'appartenance de la clé à son détenteur supposé.
Vérification	Processus consistant à comparer une signature créée à l'aide d'une clé privée à sa clé publique. La vérification permet de garantir que les informations ont réellement été envoyées par le signataire et que le message n'a pas été modifié ultérieurement par un autre utilisateur.
VPN (Réseau privé virtuel)	Permet aux réseaux privés d'effectuer une liaison à partir de l'utilisateur final, sur un réseau public (Internet) directement vers la passerelle d'accueil de votre choix, telle que l'intranet de votre entreprise.
X.509	Certificat numérique UIT-T correspondant à un document électronique reconnu au niveau international, permettant de prouver l'identité et l'appartenance de la clé publique au sein d'un réseau de communication. Il comporte le nom de l'émetteur, les informations d'identification de l'utilisateur, la signature numérique de l'émetteur, ainsi que d'autres extensions éventuelles.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

X

Z