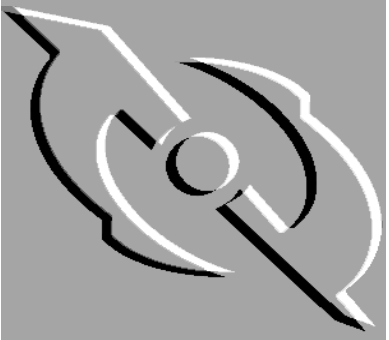

PGP Command Line

Guide de l'utilisateur

Version Internationale 6.5.

GARANTIE LIMITEE

Garantie limitée. Network Associates garantit, pour une période de (60) soixante jours à partir de la date d'achat d'origine, les supports (par exemple, disquettes) contenant le logiciel contre tout défaut de matériau et de fabrication.

Recours du client. La responsabilité de Network Associates 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) au remplacement des supports défectueux contenant le logiciel avec une copie sur les supports non défectueux. Les supports défectueux doivent être renvoyés à Network Associates aux frais du client avec une copie du reçu. Cette garantie limitée n'est plus valable si le défaut a été provoqué par un accident, une utilisation abusive ou une mauvaise utilisation. Tout support de remplacement sera soumis à la période de garantie d'origine. Ce recours est limité aux Etats-Unis, car Network Associates est sujet à des restrictions régies par les lois et les décrets relatifs au contrôle des exportations aux Etats-Unis.

Limites de responsabilité. Dans les limites permises par la loi, à l'exception de la garantie limitée du présent document, LE LOGICIEL EST FOURNI “ TEL QUEL ” SANS GARANTIE, EXPRESSE OU IMPLICITE. SANS LIMITATION DES DISPOSITIONS SUSMENTIONNEES, LE CLIENT EST TENU RESPONSABLE DE LA SELECTION DU LOGICIEL POUR OBTENIR DES RESULTATS ATTENDUS ET POUR L'INSTALLATION, L'UTILISATION ET LES RESULTATS OBTENUS GRACE AU LOGICIEL. SANS LIMITATION DES DISPOSITIONS SUSMENTIONNEES, NETWORK ASSOCIATES N'OFFRE AUCUNE GARANTIE INDIQUANT QUE L'EXECUTION DU LOGICIEL SERA EXEMPTE D'ERREURS OU D'AUTRES DEFAUTS ET NE SERA PAS INTERROMPUE, OU QUE LE LOGICIEL REPONDE A DES BESOINS SPECIFIQUES. DANS LES LIMITES PERMISES PAR LA LOI, NETWORK ASSOCIATES DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, COMPRENANT MAIS NON LIMITEE AUX GARANTIES IMPLICITES DE VENTE, ADAPTATION A UN USAGE PARTICULIER ET NON RESPECT CONFORMEMENT AU LOGICIEL ET A LA DOCUMENTATION CORRESPONDANTE. CERTAINS ETATS ET JURIDICTIONS N'AUTORISENT PAS LA LIMITATION DES GARANTIES IMPLICITES. DANS DE TELS CAS, LA LIMITATION CI-DESSUS PEUT ËTRE LIMITEE DANS SON APPLICATION. Les spécifications mentionnées sont applicables dans les limites permises par la loi.

ACCORD DE LICENCE

A l'attention de tous les utilisateurs : VOUS TROUVEREZ LES TERMES SPECIFIQUES DE LA LICENCE D'UTILISATION DU LOGICIEL DECRIT DANS CETTE DOCUMENTATION DANS LES FICHIERS README.1ST, LICENSE.TXT OU DANS TOUT AUTRE DOCUMENT DE LICENCE FOURNI AVEC VOTRE LOGICIEL SOIT SOUS FORME DE FICHIER TEXTE, SOIT COMME ELEMENT DE L'EMBALLAGE DU LOGICIEL. SI VOUS N'ACCEPTEZ PAS TOUS LES TERMES QUI Y SONT ENONCES, N'INSTALLEZ PAS LE LOGICIEL. LE CAS ECHEANT, VOUS POUVEZ RENVOYER LE PRODUIT A SON LIEU D'ACHAT AFIN DE VOUS FAIRE REMBOURSER EN INTEGRALITE.

L'exportation de ce logiciel et de la documentation 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. +31(20)5866100
Gatwickstraat 25
1043 GL Amsterdam
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.

Table des matières

Préface ix
Organisation du présent guide ix
Conventions utilisées dans ce guide ix
Pour contacter Network Associates x
Service clientèle x
Support technique x
Compatibilité An 2000 xi
Formation de Network Associates xi
Commentaires xi
Lectures recommandées xii

Chapitre 1. Présentation de PGP 1
Utilisation de PGP 1
Présentation rapide 1
Etapes de base pour l'utilisation de PGP 2

Chapitre 2. Introduction 5
Lancement de PGP 5
Emplacement des fichiers PGP 5
PGPPATH : définit le nom du chemin d'accès de PGP 6
Compatibilité de PGP avec PGP 2.6.2 6
Création et échange de clés 7
Concepts relatifs aux clés 7
Création d'une paire de clés 8
Protection des clés 10
Distribution d'une clé publique 11
Résumé des commandes de serveur de clés 11
Création d'un mot de passe complexe facile à mémoriser 12
Options de la ligne de commande de PGP 13
Saisie des paramètres de configuration de PGP sur la ligne de commande 15

Fonctions de PGP courantes 15
Création, désactivation, réactivation et révocation d'une clé 15
Cryptage et décryptage de messages 16
Effacement du disque 17
Signature de messages 17
Spécification de types de fichiers 18
Commandes de maintenance de clé 18
Création de certificats de signature 20
Résumé des commandes 20
Annulation d'une opération 20

Chapitre 3. Rubriques avancées 21
Identification de votre répertoire principal : HOME 21
Utilisation de PGP en mode non interactif à partir de scripts shell UNIX ou de fichiers batch MSDOS 21
Suppression des questions non essentielles : BATCHMODE 21
Suppression des questions de confirmation : FORCE 22
Compréhension des codes d'état de sortie de PGP 22
Utilisation de PGP comme filtre de type UNIX 22
Cryptage et transmission de données binaires 23
Envoi de fichiers de données binaires au format ASCII protégé sans cryptage ni signature 24
Décryptage de messages au format ASCII protégé 24
Envoi d'une clé publique au format ASCII protégé 24
Envoi de fichiers texte ASCII vers différents environnements système 25
Gestion des certificats de signature 26
Création d'un certificat de signature et de fichiers texte séparés 26
Réception d'un certificat de signature et de fichiers texte séparés . . .26
Commandes de gestion des fichiers 27
Décryptage d'un message et affichage du texte de sortie en clair 27
Décryptage d'un message et attribution d'un nouveau nom au fichier de texte de sortie en clair. 27
Décryptage d'un message et récupération du nom de fichier de texte en clair d'origine 27
Suppression d'une clé du serveur de clés 27

Cryptage d'un texte pouvant être affiché uniquement par son destinataire 28
Stockage de fichiers signés : signature d'un fichier sans cryptage . . .28
Effacement du disque 28
Commandes de gestion des clés 29
Modification de votre ID utilisateur ou de votre mot de passe complexe ou création de votre clé de signature par défaut à partir d'une clé existante 29
Modification des paramètres de fiabilité d'une clé publique 30
Vérification du contenu d'un trousseau de clés publiques 30
Vérification d'une clé publique par téléphone 31
Sélection de clés à l'aide de l'ID de clé 31
PGPPASS : stocke votre mot de passe complexe 32
PGPPASSFD 32

Chapitre 4. Fichier de configuration de PGP 33
A propos du fichier de configuration de PGP : pgp.cfg 33
ARMOR : sortie au format ASCII protégé 34
ARMORLINES : taille des fichiers à plusieurs entrées au format ASCII protégé 35
CERT_DEPTH : profondeur des correspondants à imbriquer 35
CLEARSIG : message signé lisible à l'œil nu 35
COMMENT : commentaire au format ASCII protégé 36
COMPATIBLE : active la compatibilité de l'interface utilisateur avec PGP 2.6.2 37
COMPLETES_NEEDED : nombre de correspondants entièrement fiables nécessaires 37
COMPRESS : compression avant cryptage 37
CIPHERNUM 37
ENCRYPTTOSELF : cryptage automatique 38
FASTKEYGEN : génération de clés rapide 38
HASHNUM 38
INTERACTIVE : confirmation d'ajouts de clés 38
KEYSERVER_URL 38
MARGINALS_NEEDED : nombre de correspondants fiables de manière marginale nécessaires 39
MYNAME : ID d'utilisateur par défaut pour les signatures 39

PAGER : commande shell permettant d'afficher du texte de sortie en clair 39
PGP_MIME 39
PGP_MIMEPARSE 40
PUBRING : nom de fichier de votre trousseau de clés publiques 40
RANDOMDEVICE 40
RANDSEED : nom de fichier pour la valeur initiale de nombres aléatoires 40
SECRING : nom du fichier de votre trousseau de clés secrètes 41
SHOWPASS : renvoi du mot de passe complexe à l'utilisateur 41
TMP : nom du chemin d'accès au répertoire des fichiers temporaires 41
TEXTMODE : suppose que le texte en clair est un fichier texte 42
TZFIX : ajustement des zones horaires 42
VERBOSE : messages sans détails, normaux ou détaillés 43

Annexe A. Codes de sortie et d'erreur 45

Index 47

Préface

Organisation du présent guide

Ce guide se compose des chapitres suivants :

- Le chapitre 1, « Présentation de PGP »,, présente l'utilisation du logiciel permettant d'implémenter les lignes de commande de PGP.
- Le chapitre 2, « Introduction », décrit comment lancer et quitter PGP, comment créer et échanger des clés, et enfin comment exécuter les fonctions courantes de PGP sur la ligne de commande.
- Le chapitre 3, « Rubriques avancées », décrit l'utilisation de PGP en mode non interactif dans les scripts shell UNIX et les fichiers batch MSDOS, son utilisation comme filtre de type UNIX, ainsi que le cryptage et la transmission de données binaires.
- Le chapitre 4, « Fichier de configuration de PGP », présente le fichier de configuration de PGP, ainsi que les paramètres de configuration figurant dans ce fichier.

Conventions utilisées dans ce guide

Les conventions suivantes sont utilisées dans ce guide.

Gras	Les menus, les champs, les options et les boutons sont indiqués en gras. Exemple : Choisissez la commande **Effacer** dans le menu **Modifier**.
`Police Sans Serif`	La police Sans Serif s'applique aux noms de chemin d'accès, aux noms de fichiers, au texte apparaissant à l'écran et à certaines touches du clavier.
`Séquences de touches`	La police Sans Serif gras s'applique aux séquences de touches que vous devez saisir.
`Variables`	La police Sans Serif italique indique un texte de ligne de commande nécessitant une valeur.

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) 5866100 ou écrivez à l'adresse suivante :

Network Associates International BV.
Gatwickstraat 25
NL-1043 GL Amsterdam

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 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 à l'écran ou apparaissant dans un fichier d'historique (les produits ne génèrent pas tous des historiques).
- Logiciel de messagerie et version correspondante (si le problème implique l'utilisation de PGP avec un produit de messagerie électronique, 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.

Formation de 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 Line », *MIT Press* ; 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 » *Scribner* ; 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 & Sons* ; 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.

Présentation de PGP 1

Bienvenue dans PGP. Ce logiciel vous permet de crypter vos données pour protéger leur confidentialité, facilement et de manière sécurisée. Ainsi, seuls les destinataires souhaités de ces données peuvent les lire. PGP vous permet également de signer numériquement des informations et assurer ainsi leur authenticité.

Utilisation de PGP

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.

- Une institution financière peut avoir recours à PGP pour transférer, en toute sécurité, des fichiers de l'un de ses services à l'autre. Les fichiers sont cryptés vers la clé du serveur de destination et envoyés via FTP dans un répertoire installé sur un serveur distant. Le serveur distant examine périodiquement son répertoire de réception et dès qu'il détecte l'arrivée de nouveaux fichiers, il les décrypte, puis les envoie vers leur destination finale.
- Les développeurs UNIX et Windows peuvent utiliser ce produit afin de sécuriser les transactions financières des internautes. Par exemple, si vous vendez des produits sur votre site Web, vous pouvez intégrer PGP dans vos scripts pour crypter automatiquement les informations relatives à la commande et de la carte de crédit d'un client, en vue de les stocker ou de les transférer vers un ordinateur sécurisé. Le terme *fichier batch MSDOS* fait référence à une invite de commandes de Windows NT.

Le terme *MSDOS* fait référence à la fenêtre d'invite de commandes de Windows NT.

Présentation rapide

PGP repose sur une technologie de cryptage largement reconnue, appelée *cryptographie de clé publique*, qui met en jeu deux clés complémentaires, c'est-à-dire une paire de clés, dont le rôle est d'assurer la sécurité des communications. Cette paire est constituée d'une *clé privée* à laquelle vous seul avez accès, et d'une *clé publique*, que vous pouvez échanger librement avec d'autres utilisateurs de PGP. Ces deux types de clés sont stockés dans des fichiers de trousseaux de clés.

Vous trouverez une présentation complète de la technique de cryptage de PGP dans le manuel *Introduction à la cryptographie* fourni avec le produit.

Etapes de base pour l'utilisation de PGP

Cette section présente rapidement les procédures à suivre lors de l'utilisation de PGP. Pour en savoir plus sur chacune de ces procédures, reportez-vous aux chapitres correspondants de ce manuel.

1. Installez PGP sur votre ordinateur. Pour obtenir des instructions complètes sur l'installation, reportez-vous à la documentation fournie avec PGP.

2. Créez une paire de clés publiques et privées.

   Avant de commencer à utiliser PGP, vous devez générer 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 diffuser librement à tout correspondant.

   Dès que vous avez terminé la procédure d'installation de PGP, vous pouvez créer une nouvelle paire de clés.

   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 8.

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 cela, vous devez disposer d'une copie de leur clé publique, et réciproquement. Votre clé publique n'étant rien de plus qu'un bloc de texte, il est donc facile 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 un serveur d'entreprise à partir duquel toute personne peut obtenir une copie si elle le souhaite.

   Pour plus d'informations sur l'échange de clés publiques, reportez-vous à la section « Création et échange de clés » à la page 7, ainsi qu'à la section « Distribution d'une clé publique » à la page 11.

4. Validez des clés publiques

   Une fois 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 figurant sur votre copie de la clé publique d'un utilisateur avec celle de la clé originale de cet utilisateur.

La présence de la signature d'un correspondant fiable sur une clé vous permet de supposer que cette dernière est valide. En général, les utilisateurs PGP demandent à d'autres correspondants fiables de signer signent leurs clés publiques pour attester de leur authenticité. Par exemple, vous pouvez demander une copie de votre clé publique à un collègue fiable en lui demandant de la certifier et de la renvoyer, de façon à pouvoir inclure sa signature lorsque vous placez votre clé sur un serveur de clés publiques. 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 offre le moyen d'établir ce niveau de validité pour chacune des clés publiques ajoutées à votre trousseau de clés publiques. 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.

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.

Lorsque vous êtes certain de disposer d'une clé publique valide, signez-la pour indiquer que vous pensez que son utilisation est sûre. Par ailleurs, vous pouvez accorder au détenteur d'une clé un niveau de fiabilité reflétant la confiance que vous lui accordez pour répondre de l'authenticité de la clé publique d'un utilisateur.

5. Cryptez et signez des 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.

6. Décryptez et vérifiez des messages et fichiers électroniques.

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

7. Effacez des fichiers.

   Pour supprimer définitivement un fichier, vous pouvez utiliser la commande d'effacement pour être certain qu'il sera impossible de récupérer ce fichier. Celui-ci est immédiatement écrasé de sorte que sa récupération à l'aide de logiciels de récupération de disque est impossible.

Introduction 2

Ce chapitre aborde les thèmes suivants :

- Lancement et sortie de PGP
- Création et échange de paires de clés
- Exécution des fonctions de PGP courantes à partir de la ligne de commande
- Affichage du Guide de l'utilisateur en ligne de PGP

Lancement de PGP

Pour lancer PGP, entrez la séquence suivante sur la ligne de commande :

pgp

Vous pouvez effectuer toutes les fonctions de PGP à partir de la ligne de commande.

Emplacement des fichiers PGP

Sous UNIX :

Lors du premier lancement de PGP, le logiciel vérifie que la variable d'environnement PGPPATH est définie. Si cette variable est définie, le logiciel place les fichiers de préférences PGP, de trousseaux de clés, pgp.cfg, ainsi que le fichier des valeurs initiales aléatoires dans le répertoire %PGPPATH%.

Si la variable PGPPATH n'est pas définie, le logiciel vérifie que la variable d'environnement USERPROFILE est définie. Si cette variable est définie, le logiciel place les fichiers dans le répertoire %USERPROFILE%\Application Data\pgp.

Si la variable USERPROFILE n'est pas définie, le logiciel place les fichiers dans le répertoire %SYSTEMROOT%\pgp.

Sous Windows NT :

Lors du premier lancement de PGP, le logiciel vérifie que la variable d'environnement PGPPATH est bien définie. Si cette variable est définie, le logiciel place le fichier pgp.cfg dans le répertoire %PGPPATH%.

Si la variable PGPPATH n'est pas définie, le logiciel vérifie que la variable USERPROFILE est définie. Si cette variable est définie, le logiciel place le fichier pgp.cfg dans le répertoire %USERPROFILE%\Application Data\pgp.

Si la variable USERPROFILE n'est pas définie, le logiciel place le fichier pgp.cfg dans le répertoire %SYSTEMROOT%\pgp.

Le fichier des préférences est placé dans le répertoire %USERPROFILE%\Application Data\pgp. Il identifie l'emplacement par défaut des trousseaux de clés (normalement, ils sont stockés dans le même répertoire, %USERPROFILE%\Application Data\pgp).

Le fichier des valeurs initiales aléatoires est toujours placé dans le répertoire %SYSTEMROOT%.

PGPPATH : définit le nom du chemin d'accès de PGP

Ce paramètre identifie l'emplacement de fichiers PGP spécifiques :

SET PGPPATH=<PGPpathname>

Par exemple :

SET PGPPATH=C:\PGP

Il est nécessaire que PGP connaisse l'emplacement des fichiers suivants :

- Vos fichiers de trousseaux de clés pubring.pkr et secring.skr
- Le fichier de valeur initiale de nombre aléatoire randseed.rnd
- Le fichier de configuration de PGP pgp.cfg (ou .pgprc)

Ces fichiers peuvent être stockés dans un répertoire quelconque. Le paramètre PGPPATH vous permet d'identifier leur emplacement.

Compatibilité de PGP avec PGP 2.6.2

Cette version de PGP comprend une option permettant de rendre l'interface utilisateur compatible avec PGP 2.6.2. Cette fonction peut s'avérer nécessaire pour l'interaction avec des scripts analysant les données de sortie ou, en cas d'impossibilité, pour communiquer avec les boîtes de dialogue de PGP.

Pour activer cette fonction, ajoutez la ligne suivante au fichier de configuration pgp.cfg :

```
COMPATIBLE=on
```

Vous avez également la possibilité d'entrer la séquence +COMPATIBLE sur la ligne de commande.

Création et échange de clés

Cette section décrit la génération des paires de clés publiques et privées permettant de correspondre avec d'autres utilisateurs de PGP. La transmission de votre clé publique et la récupération de clés publiques 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 2-1. Ce système vous permet, ainsi qu'aux utilisateurs PGP, de générer une paire de clés, constituée d'une clé publique et d'une clé privée. 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. Vous 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 leur signatures numériques.

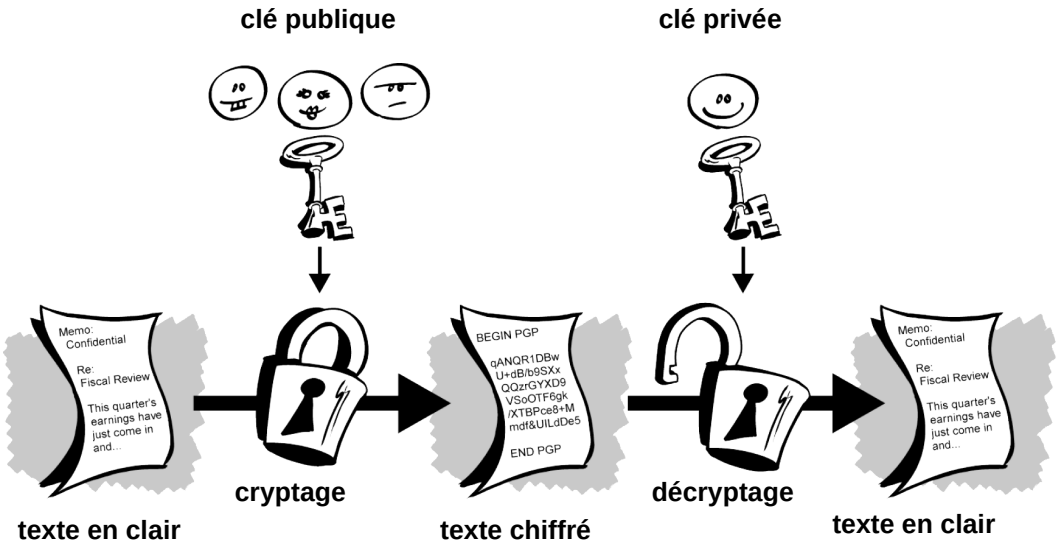

Figure 2-1. Diagramme de cryptographie de clé publique

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 transmettez librement à vos futurs correspondants. Vous pouvez utiliser la ligne de commande PGP pour générer une nouvelle paire de clés.

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 futurs correspondants. Dans ce cas, vous n'avez pas besoin de créer une nouvelle paire de clés (comme le décrit la section suivante). Identifiez, à l'aide de la variable d'environnement PGPPATH, l'emplacement de vos trousseaux de clés existants. Pour plus d'informations, reportez-vous à la section « PGPPATH : définit le nom du chemin d'accès de PGP » à la page 6.

Pour créer une nouvelle paire de clés

1. Entrez la séquence suivante sur la ligne de commande :

   pgp -kg

2. Pour la version gérant DSS / DH, passez à l'etape 4.

   Pour les versions gérant RSA, choisissez le type de clé :

   a. DSS / DH

   b. RSA

   Passez à l'etape 4.

3. Pour les versions gérant DSS / DH, sélectionnez une nouvelle clé de signature ou ajoutez une nouvelle sous-clé de cryptage à une clé DSS existante.

4. Sélectionnez la taille de clé à générer. La durée de génération d'une clé de grande taille dépendra de la vitesse de l'ordinateur utilisé.

   La taille de la clé correspond au nombre de bits utilisés pour constituer votre clé numérique. Une clé de grande taille est moins vulnérable. Cependant, l'utilisation d'une grande clé augmente les temps de cryptage et de décryptage. 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. Une clé de 1 024 bits est suffisamment sûre.

5. Entrez votre ID utilisateur. 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. Par exemple :

   Paul Blanc <pb@xyzentr.com>

   Si vous ne disposez pas d'adresse e-mail, utilisez votre numéro de téléphone ou tout autre type d'informations permettant de garantir que votre ID utilisateur est unique.

6. Pour les versions activées RSA, passez à l'etape 7.

   Si vous avez sélectionné une nouvelle clé de signature, entrez **y** pour créer une clé de cryptage, puis sélectionnez la taille souhaitée.

   Si vous ne souhaitez pas créer de clé de cryptage, entrez **n** pour générer uniquement une nouvelle clé de signature.

7. Entrez un mot de passe complexe, constitué d'une chaîne de caractères ou de mots, vous garantissant l'accès exclusif à votre clé privée. Pour plus d'informations, reportez-vous à la section « Création d'un mot de passe complexe facile à mémoriser » à la page 12.

   ☐ **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.

   ---

8. Le logiciel vous demande d'entrer un texte aléatoire lui facilitant l'accumulation de quelques bits aléatoires dans le but de créer des clés. Entrez une séquence de touches suffisamment aléatoires dans la durée.

9. La paire de clés générée est placée dans vos trousseaux de clés publiques et secrètes.

   Pour transmettre votre nouvelle clé publique à vos amis, utilisez l'option de commande -kx pour copier cette clé à partir de votre trousseau de clés publiques, puis la placer dans un fichier de clés publiques distinct. Vous pouvez envoyer ce fichier à vos amis, qui pourront ensuite l'ajouter à leurs trousseaux de clés publiques. Pour plus d'informations, reportez-vous à la section « Distribution d'une clé publique » à la page 11.

Protection des clés

Après avoir généré une paire de clés, il est préférable d'en conserver une copie dans un endroit sûr.

Vos clés privées et publiques sont stockées dans des fichiers de trousseaux de clés séparés, que vous pouvez copiez 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 répertoire identifié par la variable d'environnement PGPPATH, mais vous pouvez enregistrer vos copies de sauvegarde où vous le souhaitez. Pour plus d'informations, reportez-vous à la section « PGPPATH : définit le nom du chemin d'accès de PGP » à la page 6.

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 votre ordinateur 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 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.

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 manière différentes :

- Mise à disposition de votre clé publique via un serveur de clés publiques
- Insertion de votre clé publique dans un message électronique
- Exportation ou copie de votre clé publique dans un fichier texte

Votre clé publique se compose principalement d'un bloc de texte. Sa mise à disposition sur un serveur de clés publiques, 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.

Résumé des commandes de serveur de clés

Pour extraire une clé de votre trousseau, puis l'envoyer vers le serveur de clés :

pgp -kx <userid> <keyfile> <URL>

Pour obtenir une clé du serveur de clés et la placer dans votre trousseau de clés (deux commandes sont nécessaires) :

pgp -kx <userid> <keyfile> <URL>

pgp -ka <keyfile>

Pour supprimer une clé de votre trousseau ou du serveur de clés :

pgp -kr <userid> <URL>

Pour afficher des clés correspondant à un ID utilisateur spécifique sur le serveur de clés :

pgp -kv <userid> <URL>

Notez que la variable d'environnement KEYSERVER_URL identifie l'URL du serveur de clés par défaut, par exemple, ldap://certserveur.pgp.com.

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 alphabétiques 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.

Options de la ligne de commande de PGP

Le tableau suivant identifie et décrit les options de ligne de commande de PGP permettant de crypter, de décrypter et de gérer les fichiers et les clés. La section suivante, « Fonctions de PGP courantes » à la page 15, vous informe sur l'utilisation de ces options à partir de la ligne de commande.

Option	Description
-a	Convertit un fichier en fichier au format ASCII protégé (en créant un fichier .asc), lorsqu'elle est utilisée avec d'autres options, telles que le cryptage ou la signature.
-c	Procède à un cryptage conventionnel.
-e	Crypte via le cryptage de clé publique.
-f	Utilise le mode filtre de type UNIX pour lire des données d'entrée standard ou écrire des données de sortie standard.
-g	Affiche l'aide sur les options relatives aux groupes. Le tableau ci-après présente les combinaisons -g.
-h	Affiche le résumé des commandes.
-k	Affiche l'aide sur les options relatives aux clés. Le tableau ci-après présente les combinaisons -k.
-m	Affiche la sortie sous forme de texte en clair.
-o	Définit le nom du fichier de sortie, lorsqu'elle est utilisée avec d'autres options, telles que le cryptage, le décryptage, la vérification de signatures et le mode filtre.
-p	Récupère le nom de fichier du texte en clair original.
-s	Procède à la signature.
-t	Identifie le fichier d'entrée comme fichier de texte.
-u	Identifie la clé à utiliser pour effectuer une signature.
-w	Spécifie l'effacement du fichier.
-z	Identifie le mot de passe complexe sur la ligne de commande.

L'option -k affiche l'aide sur les options relatives aux clés. Elle est également utilisée en combinaison avec d'autres options. Le tableau suivant répertorie et décrit ces combinaisons.

Option	Description
-k	Affiche l'aide sur les options relatives aux clés.
-kg	Génère une clé.
-ka	Ajoute des clés au trousseau.
-kc	Vérifie les signatures.
-ke	Modifie l'ID utilisateur ou le mot de passe complexe de votre clé secrète ou crée une clé de signature par défaut à partir d'une clé existante.
-kr	Supprime des clés du trousseau ou du serveur de clés.
-krs	Supprime des signatures associées à des clés du trousseau.
-ks	Signe des clés du trousseau.
-kd	Révoque ou désactive des clés du trousseau.
-kds	Révoque des signatures associées à des clés du trousseau.
-kx	Extrait des clés du trousseau, puis les envoie vers le serveur de clés.
-kv	Affiche des clés du trousseau.
-kvc	Affiche les empreintes digitales d'un jeu de clés.
-kw	Affiche les clés et les signatures du trousseau de clés.

L'option -g est toujours utilisée en combinaison avec une autre option. Le tableau suivant répertorie ces combinaisons et décrit leur utilisation.

Option	Description
-g	Affiche l'aide sur les options relatives aux groupes.
-ga	Ajoute des éléments à un groupe.
-gr	Supprime des éléments d'un groupe.
-gv	Affiche un groupe.
-gvv	Affiche un groupe et les clés qu'il contient. L'affichage de tous les groupes et des clés qu'ils contiennent constitue l'option par défaut.

Saisie des paramètres de configuration de PGP sur la ligne de commande

Notez que vous pouvez entrer chacun des paramètres de configuration de PGP décrit dans le Chapitre 4, « Fichier de configuration de PGP » sous forme d'une option longue sur la ligne de commande (par exemple, +fastkeygen ou +passthrough).

Fonctions de PGP courantes

Cette section décrit les fonctions de PGP courantes, réparties dans les catégories suivantes :

- Création, désactivation, réactivation et révocation d'une clé
- Cryptage et décryptage de messages
- Effacement de texte
- Signature de messages
- Spécification de types de fichiers
- Commandes de maintenance de clé

Notez que les [crochets] indiquent un champ facultatif ; ne les saisissez pas.

Création, désactivation, réactivation et révocation d'une clé

Création d'une paire de clés

Pour créer vos propres paires de clés secrètes et publiques uniques, entrez la séquence suivante sur la ligne de commande :

```
pgp -kg
```

Révocation d'une clé

Pour révoquer définitivement votre propre clé, émettez un certificat de révocation de clé :

```
pgp -kd <your_userid>
```

Désactivation ou réactivation d'une clé

Pour désactiver ou réactiver une clé publique de votre propre trousseau de clés publiques :

```
pgp -kd <userid>
```

Cryptage et décryptage de messages

Décryptage d'un message ou vérification de l'intégrité de la signature d'un fichier signé

pgp <ciphertext_filename> [-o plaintext_filename]

Décryptage d'un message et récupération du nom de fichier de texte en clair original

pgp -p <ciphertext_filename>

Pour plus d'informations, reportez-vous à la section « Décryptage d'un message et récupération du nom de fichier de texte en clair d'origine » à la page 27.

Décryptage d'un message et affichage du texte en clair de sortie

pgp -m <ciphertext_filename>

Le résultat est similaire à la commande de type UNIX « more ». Les données de sortie ne sont pas écrites dans un fichier. Pour plus d'informations, reportez-vous à la section « Décryptage d'un message et affichage du texte de sortie en clair » à la page 27.

Décryptage d'un message au format ASCII protégé

pgp <ASCII-armored_message>

Cette commande permet de décrypter un message au format ASCII protégé. PGP convertit le message en données binaires, générant ainsi un fichier de texte chiffré « PGP » sous forme binaire, puis créée le fichier de sortie sous forme de texte en clair. Pour plus d'informations, reportez-vous à la section « Décryptage de messages au format ASCII protégé » à la page 24.

Décryptage d'un message, lecture à partir d'une entrée standard et écriture dans une sortie standard

pgp -feast <recipients_userid> <<input_filename> ><output_filename>

Pour plus d'informations, reportez-vous à la section « Utilisation de PGP comme filtre de type UNIX » à la page 22.

Cryptage d'un texte en clair par cryptographie conventionnelle uniquement

pgp -c <plaintext_filename>

Cryptage d'un fichier de texte en clair avec la clé publique du destinataire

pgp -e <plaintext_filename> <recipients_userid>

Cryptage d'un message pour plusieurs destinataires

pgp -e <textfile-filename> <userid1> <userid2> <userid3>

Cryptage d'un message pouvant être affiché uniquement par les destinataires

Utilisez cette commande pour indiquer que seuls les destinataires du texte en clair décrypté doivent être en mesure de visualiser ce texte et qu'il ne doit pas pouvoir être enregistré sur un disque.

pgp -sem <message.txt> <recipients_userid>

Pour plus d'informations,
reportez-vous à la section « Cryptage d'un texte pouvant être affiché uniquement par son destinataire » à la page 28.

Effacement du disque

Effacement du fichier de texte en clair original

pgp -ew <message.txt> <recipients_userid>

Après avoir généré le fichier de texte chiffré, PGP efface le fichier de texte en clair.

- Ajoutez l'option -w (effacement) au cours du cryptage.
- Ajoutez l'option -m (plus) au cours du décryptage.

Pour plus d'informations, reportez-vous à la section « Effacement du disque » à la page 28.

Signature de messages

Signature d'un fichier de texte en clair avec la clé secrète et cryptage de ce fichier avec la clé publique du destinataire

pgp -es <plaintext filename> <recipients_userid> [-u your_userid]

Signature d'un fichier de texte en clair avec une clé secrète

pgp -s <plaintext_filename> [-u your_userid]

Signature d'un fichier de texte en clair ASCII

pgp -sta <plaintext_filename> [-u your_userid]

PGP signe un fichier de texte en clair ASCII avec votre clé secrète, générant ainsi un message de texte en clair signé pouvant être utilisé comme message électronique.

Spécification de types de fichiers

Création d'un fichier de texte chiffré au format ASCII protégé 64

pgp -sea <plaintext_filename> <recipients_userid>

ou

pgp -kxa <userid> <keyfile> [keyring]

Vous pouvez télécharger le fichier généré vers un éditeur de texte via des canaux à 7 bits, afin de le transmettre comme un message électronique classique.

Ajoutez l'option -a au cours du cryptage, de la signature d'un message ou de l'extraction d'une clé. Pour plus d'informations, reportez-vous à la section « Cryptage et transmission de données binaires » à la page 23.

Création d'un fichier de texte en clair ASCII

pgp -seat <message.txt> <recipients_userid>

Le fichier est converti selon les conventions locales du destinataire relatives aux lignes de texte.

Ajoutez l'option -t (texte) aux autres options.

Commandes de maintenance de clé

Ajout du contenu d'un fichier de clés publiques ou secrètes ou d'un trousseau de clés publiques ou secrètes.

pgp -ka <keyfile> [keyring]

Copie d'une clé à partir d'un trousseau de clés publiques ou secrètes

pgp -kx <userid> <keyfile> [keyring]

ou :

pgp -kxa <userid> <keyfile> [keyring]

Obtention d'une clé à partir du serveur et ajout de cette clé dans un trousseau de clés (deux commandes sont nécessaires)

pgp -kx <userid> <keyfile> <URL>

pgp -ka <keyfile>

Exemple d'URL : ldap://certserver.pgp.com

Affichage du contenu d'un trousseau de clés publiques

pgp -kv[v] [userid] [keyring]

Affichage de toutes les signatures de certification associées à chaque clé

pgp -kvv [userid] [keyring]

Affichage de l'empreinte digitale d'une clé publique

pgp -kvc [userid] [keyring]

PGP affiche l'« empreinte digitale » d'une clé publique, afin de faciliter sa vérification par téléphone avec le détenteur de la clé. Pour plus d'informations sur les empreintes digitales, reportez-vous à la section « Vérification d'une clé publique par téléphone » à la page 31.

Affichage du contenu d'un trousseau de clés publiques et vérification des signatures de certification

pgp -kc [your_userid] [keyring]

Pour en savoir plus, reportez-vous à la section « Vérification du contenu d'un trousseau de clés publiques » à la page 30.

Affichage de toutes les clés d'un fichier de trousseaux de clés spécifique

pgp <keyring_filename>

PGP affiche toutes les clés dans un fichier de trousseaux de clés spécifique. Lorsque vous utilisez cette commande, PGP répertorie toutes les clés dans le fichier keyfile.pgp, puis tente de les ajouter à votre trousseau de clés, si elles ne sont pas déjà présentes.

Modification de l'ID utilisateur ou du mot de passe complexe d'une clé secrète ou création d'une clé de signature par défaut à partir d'une clé existante

pgp -ke <userid> [keyring]

Modification des paramètres de fiabilité d'une clé publique

pgp -ke <userid> [keyring]

Pour en savoir plus, reportez-vous à la section « Modification des paramètres de fiabilité d'une clé publique » à la page 30.

Suppression d'une clé ou d'un ID utilisateur d'un trousseau de clés publiques

pgp -kr <userid> [keyring]

Si vous spécifiez un fichier de trousseaux de clés, PGP tente d'ouvrir ce fichier, ainsi que le fichier de trousseaux de clés publiques ou privées correspondant. Si l'ID utilisateur à supprimer se rapporte à un trousseau contenant une clé publique et privée, PGP vous demande si vous souhaitez également supprimer la clé privée. Si vous répondez non, PGP ne supprime aucun élément.

Suppression des signatures sélectionnées à partir d'un ID utilisateur sur un trousseau de clés

pgp -krs <userid> [keyring]

Signature et certification de la clé publique d'un autre utilisateur appartenant à votre trousseau de clés publiques

pgp -ks <recipients_userid> [-u your_userid] [keyring]

Création de certificats de signature

Création d'un certificat de signature séparé du document

pgp -sb <plaintext_filename> [-u your_userid]

Pour plus d'informations, reportez-vous à la section « Création d'un certificat de signature et de fichiers texte séparés » à la page 26.

Résumé des commandes

Pour afficher un résumé rapide sur l'utilisation des commandes de PGP, entrez la séquence suivante sur la ligne de commande :

pgp -h

Annulation d'une opération

Pour annuler l'opération en cours, entrez CTRL - C à une invite quelconque.

Pour annuler une opération à long terme, entrez CTRL - C à tout moment.

Rubriques avancées 3

Ce chapitre décrit les rubriques et les commandes avancées de PGP :

- Identification de votre répertoire principal
- Utilisation de PGP en mode non interactif à partir de scripts shell UNIX ou de fichiers batch MSDOS
- Utilisation de PGP comme filtre de type UNIX
- Cryptage et transmission de données binaires
- Envoi de fichiers ASCII vers différents environnements système

Identification de votre répertoire principal : HOME

UNIX uniquement. Cette variable d'environnement identifie le répertoire principal des utilisateurs.

Utilisation de PGP en mode non interactif à partir de scripts shell UNIX ou de fichiers batch MSDOS

« MSDOS » fait référence à l'invite de commandes de Windows NT.

Suppression des questions non essentielles : BATCHMODE

Lorsque le paramètre BATCHMODE est activé sur la ligne de commande, PGP ne pose aucune question inutile ou ne vous invite pas à saisir d'autres noms de fichiers :

```
pgp +batchmode <ciphertext_filename>
```

Utilisez cette variable lorsque vous lancez PGP à partir de scripts shell ou de fichiers batch. Lorsque que le paramètre BATCHMODE est défini sur on (activé), certaines commandes de gestion des clés nécessitent l'interaction de l'utilisateur. Dans ce cas, les scripts shell seront dans l'obligation d'éviter ces commandes.

Vous pouvez également activer ce paramètre pour vérifier la validité d'une signature dans un fichier :

- Si le fichier ne contient aucune signature, le code de sortie est 1.
- Si le fichier contient une signature correcte, le code de sortie est 0.

Suppression des questions de confirmation : FORCE

Lorsque vous indiquez à PGP d'écraser un fichier existant ou de supprimer une clé d'un trousseau (commande –kr), vous devez confirmer cette action.

Pour lancer PGP en mode non interactif à partir d'un script shell UNIX ou d'un fichier batch MSDOS, utilisez l'option FORCE. Ainsi, à chaque demande de confirmation, la réponse « oui » est sous-entendue.

pgp +force <ciphertext_filename>

ou :

pgp -kr +force <your_userid>

Compréhension des codes d'état de sortie de PGP

Lorsque vous lancez PGP en mode « batch » (par exemple, à partir d'un fichier « .bat » MSDOS ou à partir d'un script shell UNIX), PGP renvoie une erreur d'état de sortie vers le shell.

- Un code d'état de sortie égal à zéro signifie une sortie normale.
- Un code d'état de sortie différent de zéro vous indique qu'une erreur est survenue. Les codes d'état de sortie renvoyés au shell dépendent des différentes conditions d'erreur.

Utilisation de PGP comme filtre de type UNIX

UNIX permet à deux applications d'interagir via des canaux de communication. Les données de sortie d'une application peuvent être directement transmises via un canal de communication à une autre application. Pour ce faire, les applications doivent être en mesure de lire les données brutes d'une « entrée standard » et de produire une « sortie standard ».

Pour utiliser le mode de filtre de type UNIX de PGP, à savoir la lecture à partir d'une entrée standard et l'écriture dans une sortie standard, ajoutez l'option -f :

pgp -feast <recipients_userid> <<input_filename> ><output_filename>

Cette fonction facilite l'utilisation de PGP avec des applications de messagerie.

Si vous utilisez le mode filtre de PGP pour décrypter un fichier de texte chiffré, la variable d'environnement PGPPASS peut s'avérer utile. Cette variable permet de conserver votre mot de passe complexe et vous évite d'avoir à le saisir. Pour plus d'informations, reportez-vous à la section « PGPPASS : stocke votre mot de passe complexe » à la page 32.

Cryptage et transmission de données binaires

Plusieurs systèmes de messagerie autorisent uniquement l'envoi de messages contenant du texte ASCII. Par conséquent, PGP prend en charge un format ASCII protégé pour les messages de texte chiffré (semblable à MIME).

Le format ASCII protégé, qui représente les données binaires uniquement par des caractères ASCII imprimables, vous permet de transmettre ou d'envoyer des données binaires cryptées via des canaux à 7 bits comme du texte de messages électroniques classique. Ce format protège les messages contre toute corruption lors de leur transfert via des passerelles intersystèmes sur Internet. PGP ajoute également un code CRC pour détecter les erreurs de transmission.

Le format ASCII protégé convertit le texte en clair en développant des groupes de 3 octets binaires de 8 bits en 4 caractères ASCII imprimables. Ainsi, la taille du fichier augmente de 33 % environ. Cependant, cette augmentation est compensée par la compression ayant eu lieu avant le cryptage.

Pour générer un fichier au format ASCII protégé, entrez la commande suivante :

pgp -ea <plaintext_filename> <recipients_userid>

Cette commande indique à PGP de générer un fichier de texte chiffré au format ASCII protégé, appelé message.asc. Ce fichier contient des données au format ASCII protégé de type MIME. Vous pouvez charger le fichier dans un éditeur de texte via des canaux à 7 bits, puis le transmettre comme un message électronique classique.

La plupart des applications de messagerie ne permettent pas l'envoi de messages d'une taille supérieure à 50 000 ou 65 000 octets. Les messages volumineux sont découpés en fichiers de plus petite taille. Si vous souhaitez appliquer le format ASCII protégé à un fichier volumineux, PGP découpe le fichier en fichiers de plus petite taille, portant les extensions « .as1 », « .as2 », « .as3 », etc.

Envoi de fichiers de données binaires au format ASCII protégé sans cryptage ni signature

L'option -a de PGP vous permet de convertir un fichier au format ASCII protégé. L'expéditeur et le destinataire ne requièrent pas de clé, car ils n'ont pas à effectuer de cryptage ou de signature. Si vous utilisez l'option -a, PGP découpe les fichiers volumineux en fichiers de plus petite taille afin d'être envoyés par e-mail. Il tente ensuite de compresser les données avant de les convertir au format ASCII protégé, puis ajoute un code de détection d'erreur CRC à chacun des fichiers de plus petite taille. Utilisez la commande suivante :

pgp -a <binary_filename>

Cette commande indique à PGP de générer un fichier au format ASCII protégé, appelé « filename.asc ». Le destinataire utilise l'option -p pour ôter la protection du message, puis restaurer le nom de fichier d'origine de l'expéditeur.

Décryptage de messages au format ASCII protégé

Pour décrypter un message au format ASCII protégé, entrez la commande suivante :

pgp <ASCII-armored_filename>

PGP reconnaît que le fichier est au format ASCII protégé, il le reconvertit au format binaire (en créant un fichier de texte chiffré .pgp de type binaire), puis crée un fichier de sortie sous forme de texte chiffré classique.

Si le message d'origine est volumineux et qu'il est envoyé sous forme de fichiers de plus petite taille, vous devez les concaténer dans l'ordre dans un seul fichier avant le décryptage du message. Lorsque PGP décrypte le message, il ignore le texte parasite figurant dans les en-têtes qui ne sont pas compris dans les blocs de message au format ASCII protégé.

Envoi d'une clé publique au format ASCII protégé

Si vous souhaitez envoyer une clé publique au format ASCII protégé à une autre personne, ajoutez l'option -a lors de l'extraction de cette clé de votre trousseau.

Si vous avez omis d'utiliser cette option lors de la création d'un fichier de texte chiffré ou de l'extraction d'une clé, vous pouvez convertir le fichier binaire au format ASCII protégé à l'aide de l'option -a (sans spécifier le cryptage). PGP convertit le fichier en fichier « .asc ».

Envoi de fichiers texte ASCII vers différents environnements système

PGP crypte tous les fichiers de texte chiffré, les données binaires de 8 bits ou les textes ASCII. Il est utilisé principalement pour les messages électroniques qui contiennent du texte ASCII.

Le texte ASCII n'est pas représenté de la même manière sur tous les ordinateurs. Par exemple, sur un système MSDOS, toutes les lignes de texte ASCII se terminent par un retour chariot, suivi d'un saut de ligne. Sur un système UNIX, toutes les lignes se terminent simplement par un saut de ligne. Sur un Macintosh, elles se terminent par un retour chariot.

Les messages de texte ASCII classiques non cryptés sont généralement traduits automatiquement dans une forme « canonique » classique lors de leur transmission d'un ordinateur à un autre. Le texte canonique comporte un retour chariot et un saut à la ligne à la fin de chaque ligne de texte.

Un texte crypté ne peut pas être converti automatiquement par un protocole de communication, car le texte en clair est masqué par le chiffrement. Pour remédier à ce problème, l'option « t » de PGP vous permet de spécifier de traiter le texte en clair comme du texte ASCII et de le convertir en texte canonique avant le cryptage. Une fois le message reçu, le texte en clair décrypté est converti automatiquement sous forme de texte adapté à l'environnement local.

Pour utiliser cette fonction, entrez l'option « t » lors du cryptage ou de la signature d'un message :

pgp -et <plaintext_filename> <recipients_userid>

Si PGP détecte des données binaires sans texte dans le fichier de texte en clair, PGP ignore l'option « t ».

PGP comprend une variable d'environnement correspondant à l'option « t », TEXTMODE. Si vous recevez systématiquement des fichiers de texte en clair plutôt que des données binaires, définissez TEXTMODE=ON.

Gestion des certificats de signature

Création d'un certificat de signature et de fichiers texte séparés

Dans la plupart des cas, les certificats de signature sont joints physiquement au texte signé, ce qui facilite la vérification des signatures. Toutefois, vous pouvez créer un fichier de certificat de signature séparé, puis envoyer les deux fichiers (le fichier de texte et le fichier de certificat de signature) au destinataire. Cette fonction s'avère utile lorsque plusieurs personnes doivent signer un document, tel qu'un contrat juridique, sans imbriquer de signatures. La signature de chaque personne est indépendante.

Pour créer un fichier de certificat de signature séparé, combinez l'option « b » avec l'option « s ». Entrez la commande suivante :

pgp -sb <plaintext_filename> [-u <your_userid>]

Cette commande indique à PGP de générer un certificat de signature séparé dans un fichier appelé letter.sig. Le contenu de ce fichier n'est pas ajouté au fichier <letter.txt>.

Réception d'un certificat de signature et de fichiers texte séparés

Si vous tentez de traiter un fichier de certificat de signature, PGP vous invite à identifier le fichier texte correspondant. Une fois le fichier texte identifié, PGP vérifie l'intégrité de la signature.

Si vous savez qu'une signature est séparée d'un fichier texte, vous pouvez spécifier les deux noms de fichier sur la ligne de commande.

pgp <letter.sig> <letter.txt>

ou

pgp <letter> <letter.txt>

Commandes de gestion des fichiers

Décryptage d'un message et affichage du texte de sortie en clair

Pour afficher le texte de sortie en clair décrypté (comme vous le feriez avec la commande de type UNIX « more »), sans l'écrire dans un fichier, utilisez l'option -m lors du décryptage :

pgp -m <ciphertext_filename>

Cette commande indique à PGP d'afficher le texte en clair décrypté sur un écran à la fois.

Décryptage d'un message et attribution d'un nouveau nom au fichier de texte de sortie en clair

Lorsque PGP crypte un fichier de texte en clair, il enregistre le nom de fichier d'origine et le joint au texte en clair avant de le compresser et de le crypter. Lorsque PGP décrypte le fichier de texte chiffré, il attribue un nom au fichier de texte de sortie en clair identique au nom de fichier de texte chiffré d'entrée, mais supprime l'extension.

L'option -o sur la ligne de commande vous permet de spécifier un nom de fichier de sortie de texte en clair plus significatif.

pgp -o <ciphertext_filename> <new_plaintext_filename>

Décryptage d'un message et récupération du nom de fichier de texte en clair d'origine

Comme indiqué à la section précédente, lorsque PGP crypte un fichier de texte en clair, il enregistre le nom de fichier d'origine, puis le joint au texte en clair avant de le compresser et de le crypter. Pour indiquer à PGP de conserver le nom de fichier de texte en clair d'origine, puis de l'utiliser comme nom du fichier de texte de sortie en clair décrypté, utilisez l'option « -p ».

pgp -p <ciphertext_filename>

Suppression d'une clé du serveur de clés

pgp -kr <userid> <URL>

Exemple d'URL : ldap://certserver.pgp.com.

Cryptage d'un texte pouvant être affiché uniquement par son destinataire

Pour spécifier que seul le destinataire du texte en clair décrypté doit être en mesure de visualiser ce texte et que ce dernier ne doit pas pouvoir être enregistré sur le disque, ajoutez l'option -m :

pgp -sem <message.txt> <recipients_userid>

Lorsque le destinataire décrypte le texte chiffré à l'aide de sa clé secrète et de son mot de passe complexe, le texte en clair s'affiche sur son écran, mais n'est pas enregistré sur le disque. Le texte apparaît, comme avec la commande de type UNIX « more », un écran à la fois. Si le destinataire souhaite lire à nouveau le message, le texte chiffré doit être décrypté une seconde fois.

Cette fonction est le moyen le plus sûr d'éviter que vos messages confidentiels soient conservés par inadvertance sur le disque du destinataire.

Notez que cette fonction n'empêche pas une personne sensée et déterminée d'enregistrer, par un moyen quelconque, le texte en clair décrypté sur un disque. Elle est conçue pour empêcher qu'un utilisateur occasionnel n'effectue cet enregistrement par inadvertance.

Stockage de fichiers signés : signature d'un fichier sans cryptage

Si vous souhaitez signer un fichier de texte en clair sans spécifier de cryptage, PGP compresse le fichier après que l'avoir signé. Ainsi, ce fichier ne peut pas être lu par un utilisateur occasionnel. Cette méthode vous permet de stocker des fichiers signés dans des applications d'archive.

Effacement du disque

Après la génération d'un fichier de texte chiffré par PGP, vous pouvez demander à PGP d'écraser et de supprimer automatiquement le fichier de texte en clair, afin d'effacer toute trace de ce texte sur le disque. Lorsqu'un fichier de texte en clair contient des informations confidentielles, utilisez l'option « w » pour éviter que quiconque ne puisse récupérer le fichier à l'aide d'un utilitaire d'analyse de bloc du disque.

Utilisez l'option « w » lors du cryptage et de la signature d'un message :

pgp -ew <message.txt> <recipients_userid>

Cette commande indique à PGP de créer un fichier de texte chiffré « message.pgp », puis de supprimer le fichier de texte en clair « message.txt ».

Notez que cette option n'effacera pas tous les fragments du texte en clair que votre traitement de texte a pu créer sur le disque lors de l'édition du message avant le lancement de PGP. La plupart des traitements de texte créent des fichiers de sauvegarde, des fichiers de travail ou les deux.

PGP écrase le fichier à 26 reprises.

Commandes de gestion des clés

Modification de votre ID utilisateur ou de votre mot de passe complexe ou création de votre clé de signature par défaut à partir d'une clé existante

Vous pouvez avoir besoin de modifier votre mot de passe complexe, par exemple lorsqu'une personne a pu le découvrir en regardant par-dessus votre épaule lorsque vous le saisissez. Vous devez éventuellement modifier votre ID utilisateur si vous avez modifié votre nom et votre adresse e-mail. Vous pouvez ajouter un deuxième ou un troisième ID utilisateur à votre clé si vous possédez plusieurs noms, adresses e-mail ou fonctions. PGP vous permet d'associer plusieurs ID utilisateur à votre clé, chacun d'entre eux pouvant être utilisé pour la recherche de votre clé sur le trousseau. Vous serez peut être également amené à créer votre clé de signature par défaut à partir d'une clé existante.

Pour modifier votre ID utilisateur ou votre mot de passe complexe pour une clé secrète ou pour créer une clé de signature par défaut à partir d'une clé existante, utilisez la commande suivante :

pgp -ke <your_userid> [keyring]

PGP vous invite à entrer un nouvel ID utilisateur ou un nouveau mot de passe complexe.

Si vous modifiez votre ID utilisateur, PGP ajoute en réalité un nouvel ID utilisateur sans supprimer l'ancien. Pour supprimer l'ancien ID utilisateur, vous devez effectuer une autre opération.

Si vous choisissez d'utiliser la clé en tant que correspondant à fiabilité ultime, vous pouvez créer votre clé de signature par défaut à partir de cette clé.

Si vous spécifiez le paramètre facultatif [trousseau], celui-ci doit correspondre à un trousseau de clés publiques et non à un trousseau de clés secrètes. Le champ ID utilisateur doit être reconnu par PGP comme votre propre ID utilisateur, car il apparaît à la fois sur votre trousseau de clés publiques et secrètes. Ces deux trousseaux sont mis à jour même si vous avez spécifié uniquement le trousseau de clés publiques.

Vous pouvez également utiliser la commande -ke pour modifier les paramètres de fiabilité d'une clé publique. Pour plus d'informations, reportez-vous à la section « Modification des paramètres de fiabilité d'une clé publique » à la page 30.

Modification des paramètres de fiabilité d'une clé publique

Pour modifier les paramètres de fiabilité d'une clé publique de votre trousseau de clés publiques, entrez la commande suivante :

pgp -ke <userid> [keyring]

Si vous spécifiez le paramètre facultatif [trousseau], celui-ci doit correspondre à un trousseau de clés publiques et non à un trousseau de clés secrètes.

Vérification du contenu d'un trousseau de clés publiques

PGP vérifie automatiquement toutes les nouvelles clés ou signatures sur votre trousseau de clés publiques et met à jour l'ensemble des paramètres de fiabilité, ainsi que des scores de validité. Il met à jour, théoriquement, toutes les informations sur l'état de validité des clés au fur et à mesure de l'ajout et de la suppression d'éléments sur votre trousseau de clés publiques.

Cependant, il se peut que vous souhaitiez de manière explicite que PGP exécute une analyse complète de votre trousseau de clés publiques, en vérifiant toutes les signatures de certification, les paramètres de fiabilité, en mettant à jour tous les scores de validité et en comparant votre propre correspondant à fiabilité ultime à une copie de sauvegarde conservée sur une disquette protégée en écriture. Il est conseillé d'effectuer cette maintenance de manière périodique pour s'assurer du bon état général de votre trousseau de clés publiques.

Pour forcer l'analyse complète de votre trousseau de clés publiques, utilisez la commande -kr (vérification du trousseau de clés).

pgp -kc

Pour que PGP vérifie toutes les signatures d'une seule clé publique sélectionnée, vous pouvez également utiliser la commande suivante :

pgp -kc <your_userid> [keyring]

Pour plus d'informations sur le mode de vérification de la copie de sauvegarde de votre clé, reportez-vous à la section « CERT_DEPTH : profondeur des correspondants à imbriquer » à la page 35.

Vérification d'une clé publique par téléphone

Si une personne vous fait parvenir une clé publique qui n'a pas été certifiée par une personne de confiance, comment savoir que vous êtes en possession de la bonne clé ? Si vous connaissez le détenteur de cette clé et que vous reconnaissez sa voix au téléphone, téléphonez-lui, puis vérifiez l'empreinte digitale de la clé par téléphone. Pour ce faire, vous devez, ainsi que le détenteur de la clé, utiliser la commande –kvd pour afficher l'empreinte digitale de la clé :

pgp -kvc <userid> [keyring]

Cette commande indique à PGP d'afficher la clé avec le résumé de 32 caractères des composants de clé publique (les clés Diffie-Hellman ont des empreintes digitales de 40 caractères). Lisez l'empreinte digitale au détenteur de la clé pour vérifier si les empreintes digitales correspondent.

Cette procédure vous permet à vous, ainsi qu'à votre correspondant de vérifier et de signer chacune de vos clés en toute confiance. Il s'agit d'une méthode sûre et pratique pour introduire vos amis dans un réseau de confiance.

Notez que l'envoi par messagerie électronique de l'empreinte digitale d'une clé n'est pas la meilleure méthode de vérification de la clé, car votre message peut être intercepté et modifié. Il est préférable d'utiliser un canal différent de celui utilisé pour l'envoi de la clé elle-même. La meilleure solution est d'envoyer la clé via e-mail et de communiquer son empreinte digitale au cours d'une conversation téléphonique. Certaines personnes distribuent l'empreinte digitale de leur clé sur leurs cartes de visite.

Sélection de clés à l'aide de l'ID de clé

Dans la plupart des cas, vous sélectionnez une clé en entrant un ID utilisateur ou un fragment d'ID utilisateur. Cependant, vous pouvez utiliser l'ID de clé hexadécimal pour sélectionner une clé. Pour ce faire, entrez l'ID de clé doté du préfixe « 0x », plutôt que l'ID utilisateur :

pgp -kv 0x67F796C2

Cette commande indique à PGP d'afficher toutes les clés possédant la valeur 67F796C2 dans leurs ID de clé.

Cette fonction s'avère particulièrement utile si une personne possède deux clés différentes avec le même ID utilisateur. Vous pouvez choisir la bonne clé en spécifiant l'ID de clé spécifique.

PGPPASS : stocke votre mot de passe complexe

Lorsqu'un mot de passe complexe est requis pour déverrouiller une clé secrète, PGP vous invite à le saisir. Pour stocker votre mot de passe complexe, saisissez la variable d'environnement PGPPASS sur la ligne de commande. Si PGP requiert un mot de passe complexe, il tente d'utiliser le mot de passe complexe stocké. Si ce dernier est incorrect, PGP vous invite à entrer le mot de passe complexe correct.

SET PGPPASS=zaphod beeblebrox au président

L'exemple ci-dessus supprime l'invite de saisie du mot de passe complexe si ce dernier est « zaphod beeblebrox au président ».

Cette fonction s'avère utile si vous recevez régulièrement un grand nombre de messages entrants adressés à votre clé secrète. Ce qui évite d'avoir à saisir votre mot de passe complexe plusieurs fois.

La méthode la plus sûre pour utiliser cette fonction est d'entrer la commande à chaque démarrage du système et de l'effacer ou d'éteindre votre ordinateur une fois terminé. N'utilisez pas cette fonction dans un environnement où une autre personne peut accéder à votre ordinateur.

Transmission de votre mot de passe complexe à partir d'une autre application

L'option de ligne de commande –z de PGP vous permet de transmettre votre mot de passe complexe à PGP à partir d'une autre application. Cette option est conçue principalement pour lancer PGP à partir d'une application de messagerie.

Le mot de passe complexe suit l'option –z sur la ligne de commande. Utilisez cette fonction avec précaution.

PGPPASSFD

Cette variable d'environnement correspond au descripteur de fichier du mot de passe complexe. Si elle est définie sur zéro (0), PGP utilise la première ligne de texte à partir de stdin comme mot de passe complexe.

Fichier de configuration de PGP 4

A propos du fichier de configuration de PGP : pgp.cfg

PGP stocke plusieurs paramètres définis par l'utilisateur dans le fichier de configuration au format texte, pgp.cfg. Un fichier de configuration vous permet en fait de définir des indicateurs et des paramètres (également appelés variables d'environnement) pour PGP, ce qui vous évite de les configurer sur la ligne de commande de PGP.

Utilisez des paramètres de configuration pour effectuer, entre autres, les opérations suivantes :

- Contrôle de l'emplacement de stockage des fichiers de travail temporaires de PGP.
- Définition du niveau de scepticisme de PGP lors de l'évaluation de la validité d'une clé en fonction de son nombre de signatures de certification.

Les paramètres de configuration peuvent être définis sous forme de nombres entiers, de chaînes de caractères ou de valeurs booléennes on / off (activées / désactivées). Ces dernières des types de paramètres. PGP inclut un exemple de fichier de configuration que vous pouvez consulter.

Les règles suivantes s'appliquent au fichier de configuration :

- Les lignes vierges sont ignorées.
- Tout caractère situé après la marque de commentaire # est ignoré.
- Les mots-clés ne sont pas sensibles à la casse.

Un extrait de fichier de configuration type est présenté ci-après :

```
# TMP est le répertoire des fichiers de travail de PGP, tels qu'un
disque en mémoire vive.
TMP = "e:\" # Ce paramètre peut être remplacé par la variable
d'environnement TMP.
ARMOR=ON # Utiliser l'indicateur -a pour la protection ASCII, le
cas échéant.
# CERT_DEPTH correspond au niveau d'imbrication des correspon-
dants.
cert_depth = 3
```

Dans les situations suivantes, PGP utilise des valeurs par défaut pour les paramètres de configuration :

- Les paramètres de configuration ne sont pas définis.
- Le fichier de configuration n'existe pas.
- PGP ne trouve pas le fichier de configuration.

Remarquez qu'il est également possible de définir ces mêmes paramètres de configuration directement à partir de la ligne de commande PGP en les faisant précéder du caractère « + » (plus). Par exemple, les deux commandes PGP suivantes ont des effets identiques :

pgp -e +armor=on message.txt smith

pgp -ea message.txt smith

Pour plus d'informations sur l'emplacement du fichier pgp.cfg, reportez-vous à la section « Emplacement des fichiers PGP » à la page 5.

Vous trouverez ci-après un récapitulatif des paramètres de configuration de PGP par ordre alphabétique.

ARMOR : sortie au format ASCII protégé

Paramètre par défaut : ARMOR=OFF

Le paramètre de configuration ARMOR est équivalent à l'option de ligne de commande -a. Lorsque ce paramètre est activé, PGP émet du texte chiffré ou des clés au format ASCII protégé, pour le transport via les canaux de messagerie. Les fichiers de sortie portent l'extension « .asc ».

Activez ce paramètre (ARMOR=ON), si vous souhaitez utiliser PGP principalement pour vos messages électroniques.

ARMORLINES : taille des fichiers à plusieurs entrées au format ASCII protégé

Paramètre par défaut : ARMORLINES=0

La plupart des applications de messagerie ne permettent pas l'envoi de messages d'une taille supérieure à 50 000 ou 65 000 octets. Par conséquent, PGP limite le nombre de lignes d'un fichier à 720. Lorsque PGP crée un fichier au format ASCII protégé « .asc » volumineux, celui-ci est découpé en fichiers à plusieurs entrées de plus petites tailles, afin d'être envoyé via des applications de messagerie. Ces fichiers portent les extensions « .as1 », « .as2», « .as3», etc.

Le paramètre de configuration ARMORLINES définit le nombre maximal de lignes autorisé dans chaque fichier d'une suite de fichiers « .asc » à plusieurs entrées. Si vous définissez ARMORLINES sur zéro, PGP ne découpe pas votre fichier en plusieurs parties.

CERT_DEPTH : profondeur des correspondants à imbriquer

Paramètre par défaut : CERT_DEPTH=4

Le paramètre de configuration CERT_DEPTH identifie le nombre autorisé de niveaux d'imbrication de vos correspondants pour certifier d'autres correspondants, dont le rôle est de certifier les clés publiques de votre trousseau.

Par exemple, si la valeur du paramètre CERT_DEPTH est définie sur 1, une seule couche de correspondants est située au-dessous de votre clé la plus fiable. Dans ce cas, vous devez directement certifier les clés publiques de tous les correspondants fiables sur votre trousseau. Si la valeur du paramètre CERT_DEPTH est définie sur 0, vous pouvez n'avoir aucun correspondant. Vous devez alors certifier directement chacune des clés publiques de votre trousseau afin de les utiliser. Les valeurs minimale et maximale du paramètre CERT_DEPTH sont respectivement égales à 0 et 8.

CLEARSIG : message signé lisible à l'œil nu

Paramètre par défaut : CLEARSIG=ON

Pour générer un message signé lisible à l'œil nu sans l'aide de PGP, utilisez le paramètre CLEARSIG. Cependant, pour vérifier la signature, le destinataire doit toujours utiliser PGP.

Un certificat de signature sous forme binaire est ajouté en préfixe aux messages signés PGP non cryptés. Le message signé est compressé, ce qui le rend illisible à l'œil nu, même s'il n'est pas crypté.

Pour envoyer ces données binaires via un canal de messagerie à 7 bits, PGP applique le format ASCII protégé (voir le paramètre ARMOR). Ce format rend le message illisible à l'œil nu, même s'il n'a pas été compressé par PGP. Le destinataire doit d'abord supprimer la protection du message à l'aide de PGP, puis décompresser ce message avant de le lire.

Si le message en clair est sous forme de texte, et non pas sous forme binaire, utilisez le paramètre CLEARSIG pour envoyer un message signé via un canal de messagerie. Le message signé n'est pas compressé et le format ASCII protégé est appliqué au certificat de signature binaire, non pas au message en clair. Le paramètre CLEARSIG permet la génération d'un message signé lisible à l'œil nu, sans l'aide de PGP (encore une fois, pour vérifier la signature, le destinataire devra utiliser PGP).

Par défaut, le paramètre CLEARSIG est défini sur « on ». Pour permettre le fonctionnement optimal de CLEARSIG, les paramètres ARMOR et TEXTMODE doivent également être activés. Choisissez ARMOR=ON (ou utilisez l'option -a) et TEXTMODE=ON (ou utilisez l'option -t). Si CLEARSIG est défini sur « off » dans votre fichier de configuration, activez-le à nouveau directement sur la ligne de commande :

pgp -sta +clearsig=on message.txt.

Puisque cette méthode applique le format ASCII protégé uniquement au certificat de signature binaire, et non pas au texte du message, un message non protégé est susceptible d'être altéré lors de son acheminement. Ce risque survient lorsque le message est transféré via une passerelle de messagerie effectuant des conversions de jeux de caractères ou lorsque des espaces supplémentaires sont ajoutés ou supprimés en fin de ligne. Dans ce cas, la vérification de la signature n'est pas effectuée, ce qui peut laisser croire à tort que le message a été altéré intentionnellement.

Lorsque PGP calcule la signature du texte en mode CLEARSIG, les espaces parasites sur chaque ligne sont ignorés.

COMMENT : commentaire au format ASCII protégé

Le commentaire au format ASCII protégé apparaît dans toutes les sorties au format ASCII protégé comme un en-tête de commentaire, situé sous l'en-tête de version.

COMPATIBLE : active la compatibilité de l'interface utilisateur avec PGP 2.6.2

Paramètre par défaut : COMPATIBLE=OFF

Le paramètre de configuration COMPATIBLE active la compatibilité de l'interface utilisateur avec PGP 2.6.2. Cette fonction peut s'avérer nécessaire pour l'interaction avec des scripts analysant les données de sortie ou, en cas d'impossibilité, communiquant avec les boîtes de dialogue de PGP.

Pour activer cette fonction, ajoutez la ligne suivante au fichier de configuration pgp.cfg :

```
COMPATIBLE=OFF
```

COMPLETES_NEEDED : nombre de correspondants entièrement fiables nécessaires

Paramètre par défaut : COMPLETES_NEEDED=1

Le paramètre de configuration COMPLETES_NEEDED identifie le nombre minimal de correspondants entièrement fiables nécessaires à la certification complète d'une clé publique de votre trousseau.

COMPRESS : compression avant cryptage

Paramètre par défaut : COMPRESS=ON

Le paramètre de configuration COMPRESS active ou désactive la compression des données préalablement au cryptage. Il est utilisé principalement pour le débogage de PGP. Dans PGP, la règle veut généralement que le texte en clair soit compressé avant d'être crypté. Ne modifiez pas ce paramètre.

CIPHERNUM

Ce paramètre permet de spécifier le chiffrement à utiliser. Les valeurs possibles sont les suivantes :

kPGPCipherAlgorithm_IDEA = 1

kPGPCipherAlgorithm_3DES = 2

kPGPCipherAlgorithm_CAST5 = 3

Grâce à ce paramètre, l'application n'a pas besoin de connaître les valeurs codées dans le kit de développement logiciel. D'autres algorithmes pourront être ajoutés dans les versions ultérieures.

ENCRYPTTOSELF : cryptage automatique

Paramètre par défaut : ENCRYPTTOSELF=PFF

Utilisez cette variable pour indiquer à PGP d'ajouter le paramètre MYNAME aux destinataires.

FASTKEYGEN : génération de clés rapide

Paramètre par défaut : FASTKEYGEN=ON

Utilisez ce paramètre pour activer la génération de clés rapide.

HASHNUM

Numéro décrivant l'algorithme de hachage utilisé. Les valeurs possibles sont de type PGPHashAlgorithm :

kPGPHashAlgorithm_MD5 = 1

kPGPHashAlgorithm_SHA = 2

kPGPHashAlgorithm_RIPEMD160 = 3

Grâce à ce paramètre, l'application n'a pas besoin de connaître les valeurs codées dans le kit de développement logiciel. D'autres algorithmes pourront être ajoutés dans les versions ultérieures.

INTERACTIVE : confirmation d'ajouts de clés

Paramètre par défaut : INTERACTIVE=OFF

Cette variable permet de configurer PGP afin qu'une confirmation vous soit demandée lorsque vous ajoutez un fichier avec plusieurs clés sur votre trousseau. Lorsque cette variable est activée, vous devez valider l'ajout de chaque clé au trousseau.

KEYSERVER_URL

Paramètre par défaut : KEYSERVER_URL=""

Identifie l'URL du serveur de clés par défaut, par exemple, ldap://certserver.pgp.com.

MARGINALS_NEEDED : nombre de correspondants fiables de manière marginale nécessaires

Paramètre par défaut : MARGINALS_NEEDED=2

Le paramètre de configuration MARGINALS_NEEDED identifie le nombre minimal de correspondants fiables de manière marginale nécessaires à la certification complète d'une clé publique de votre trousseau.

MYNAME : ID d'utilisateur par défaut pour les signatures

Paramètre par défaut : MYNAME= ""

Le paramètre de configuration MYNAME définit l'ID d'utilisateur par défaut à utiliser pour la sélection de la clé secrète de signature. Si le paramètre MYNAME n'est pas défini, PGP utilise la clé secrète la plus récente de votre trousseau de clés secrètes. Vous pouvez passer outre ce réglage en utilisant l'option –u qui permet de définir un ID d'utilisateur sur la ligne de commande de PGP.

PAGER : commande shell permettant d'afficher du texte de sortie en clair

Paramètre par défaut : PAGER= ""

L'option –m de PGP vous permet d'afficher, écran par écran, une sortie au format texte en clair décrypté, sans avoir à écrire cette sortie dans un fichier.

PGP dispose d'un utilitaire d'affichage de pages intégré. Si vous préférez utiliser un autre utilitaire, identifiez-le à l'aide du paramètre PAGER. Ce paramètre spécifie la commande shell utilisée par PGP pour afficher un fichier.

Notez que si l'expéditeur a spécifié qu'un fichier était accessible uniquement en lecture seule, PGP utilise toujours sa fonction d'affichage intégrée.

Pour plus d'informations, reportez-vous à la section « Décryptage d'un message et affichage du texte de sortie en clair » à la page 27.

PGP_MIME

Paramètre par défaut : PGP_MIME=OFF

Utilisez ce paramètre pour définir la compatibilité avec PGP-MIME.

PGP_MIMEPARSE

Paramètre par défaut : PGP_MIMEPARSE=OFF

Ce paramètre permet de configurer PGP afin qu'une tentative d'analyse des parties MIME du corps du texte soit effectuée.

PUBRING : nom de fichier de votre trousseau de clés publiques

Paramètre par défaut : PUBRING = "%PGPPATH%/pubring.pkr" sous UNIX

%USERPROFILE%\Application Data\pgp\pubring.pkr sous NT

Vous pouvez conserver votre trousseau de clés publiques dans un répertoire différent de votre fichier de configuration PGP (à savoir, le répertoire défini par votre variable d'environnement PGPPATH). Pour connaître le chemin d'accès et le nom de fichier complets de votre trousseau de clés publiques, utilisez le paramètre PUBRING.

Utilisez également cette fonction sur la ligne de commande pour spécifier un autre trousseau de clés.

RANDOMDEVICE

Paramètre par défaut : RANDOMDEVICE = /dev/random sous UNIX

UNIX uniquement. Identifie le pool d'entropie du système, /dev/random. PGP tente alors de pénétrer ce périphérique par une acquisition d'entropie. En cas d'échec, une autre tentative est effectuée à partir des séquences de touches de l'utilisateur. Ce paramètre n'est pas pris en charge sous Windows NT.

RANDSEED : nom de fichier pour la valeur initiale de nombres aléatoires

Paramètre par défaut : RANDSEED = "%PGPPATH%/randseed.rnd" sous UNIX

"%SYSTEMROOT% /randseed.rnd" sous Windows NT

Le fichier de valeurs initiales de nombre aléatoires, randseed.rnd, est utilisé pour la génération des clés de session. Vous pouvez conserver ce fichier dans un répertoire ou sur un périphérique plus sécurisé (ce fichier est généralement situé dans le répertoire défini par votre variable d'environnement PGPPATH). Pour connaître le chemin d'accès et le nom complets de votre fichier de valeurs initiales de nombres aléatoires, utilisez le paramètre RANDSEED.

SECRING : nom du fichier de votre trousseau de clés secrètes

Paramètre par défaut : SECRING = "%PGPPATH%/secring.pgp"

Vous pouvez conserver votre trousseau de clés secrètes dans un répertoire différent de celui de votre fichier de configuration PGP (à savoir, le répertoire défini par votre variable d'environnement PGPPATH). Pour connaître le chemin d'accès et le nom de fichier complets de votre trousseau de clés secrètes, utilisez le paramètre PUBRING.

SHOWPASS : renvoi du mot de passe complexe à l'utilisateur

Paramètre par défaut : SHOWPASS=OFF

Votre mot de passe complexe n'apparaît pas lorsque vous le saisissez, ce qui évite qu'une personne en prenne connaissance en regardant par-dessus votre épaule. Toutefois, vous pouvez rencontrer des difficultés lors de la saisie de votre mot de passe complexe, les caractères saisis n'apparaissant pas à l'écran. Par ailleurs, il vous est possible d'effectuer cette saisie dans l'intimité de votre propre domicile.

Le paramètre de configuration SHOWPASS autorise un contrôle par écho lors de la saisie de votre mot de passe complexe.

TMP : nom du chemin d'accès au répertoire des fichiers temporaires

Paramètre par défaut : TMP = ""

Le paramètre de configuration TMP définit le répertoire utilisé par PGP pour le stockage des fichiers de travail temporaires. Si TMP n'est pas défini, les fichiers temporaires sont écrits dans le répertoire en cours. Si la variable d'environnement shell TMP est définie, PGP stocke les fichiers temporaires dans le répertoire désigné.

TEXTMODE : suppose que le texte en clair est un fichier texte

Paramètre par défaut : TEXTMODE=OFF

Le paramètre de configuration TEXTMODE est équivalent à l'option de ligne de commande -t. S'il est activé, ce paramètre permet à PGP de considérer que le texte en clair est un fichier texte, non pas un fichier binaire, puis de le convertir en « texte canonique » préalablement à son cryptage. Le texte canonique comporte un retour chariot et un saut à la ligne à la fin de chaque ligne de texte.

Ce paramètre est automatiquement désactivé lorsque PGP détecte que le fichier de texte en clair contient des données binaires sans texte. Activez ce paramètre (TEXTMODE=ON), si vous souhaitez utiliser PGP principalement pour des envois de messages électroniques.

Pour plus d'informations, reportez-vous à la section « Envoi de fichiers texte ASCII vers différents environnements système » à la page 25.

TZFIX : ajustement des zones horaires

Paramètre par défaut : TZFIX=0

UNIX uniquement. Dans PGP, l'horodatage des clés et des certificats de signature est effectué en temps moyen de Greenwich (GMT). Lorsque PGP demande l'heure au système, elle est indiquée en GMT. Toutefois, sur certains systèmes, l'heure est indiquée en heure du Pacifique, plus huit heures.

Le paramètre de configuration TZFIX indique le nombre d'heures à ajouter à la fonction d'heure système pour obtenir le temps moyen de Greenwich. Si votre système d'exploitation n'indique pas l'heure GMT, utilisez TZFIX pour régler l'heure système en temps GMT.

Pour Los Angeles :	SET TZ=PST8PDT
Pour Denver :	SET TZ=MST7MDT
Pour l'Arizona :	SET TZ=MST7

L'heure d'été n'existe pas en Arizona.

Pour Chicago :	SET TZ=CST6CDT
Pour New York :	SET TZ=EST5EDT
Pour Londres :	SET TZ=GMT0BST
Pour Amsterdam :	SET TZ=MET-1DST
Pour Moscou :	SET TZ=MSK-3MSD
Pour Auckland :	SET TZ=NZT-13

VERBOSE : messages sans détails, normaux ou détaillés

Paramètre par défaut : VERBOSE = 1

La variable VERBOSE contrôle le niveau de détails des messages de diagnostic de PGP. Les paramètres sont les suivants :

0 – Seules les requêtes et les erreurs sont affichées (c'est-à-dire que l'utilisateur est invité à procéder à la saisie et les erreurs sont affichées, le cas échéant).

1 – Paramètre par défaut normal. Affiche un niveau raisonnable de détails dans les messages de diagnostic ou d'avertissement.

2 – Affiche un maximum d'informations, généralement pour diagnostiquer les problèmes relatifs à PGP. Ce paramètre n'est pas recommandé en cas d'utilisation normale.

Codes de sortie et d'erreur A

Cette annexe répertorie les codes de sortie et d'erreur de PGP.

Erreurs d'ordre général

Erreur	Explication
0	Sortie sans erreur
1	fichier incorrect
2	fichier introuvable
3	fichier inconnu
4	mode batch erroné
5	argument incorrect
6	interruption du processus
7	mémoire insuffisante

Erreurs liées aux trousseaux de clés

Erreur	Code
10	erreur de génération de clés
11	clé inexistante
12	erreur d'ajout au trousseau de clés
13	erreur d'extraction du trousseau de clés
14	erreur de modification de trousseau de clés
15	erreur d'affichage du trousseau de clés
16	erreur de suppression du trousseau de clés
17	erreur de vérification du trousseau de clés
18	erreur de signature de clé
19	erreur de suppression de signature de clé

Erreurs liées aux trousseaux de clés

Erreur	Code
KEY_SIGNATURE_ERROR	erreur de signature de clé

Erreurs de codage

Erreur	Code
20	erreur de signature
21	erreur de cryptage de clé publique
22	erreur de cryptage
23	erreur de compression

Erreurs de décodage

Erreur	Description
30	erreur de vérification de signature
31	erreur de décryptage de clé publique
32	erreur de décryptage
33	erreur de décompression

Index

A

-a, 13
Affichage d'un groupe, 14
Affichage d'un groupe et des clés qu'il contient, 14
Affichage de clés du trousseau de clés, 14
Affichage de l'empreinte digitale d'une clé publique, 19
Affichage de la sortie sous forme de texte en clair, 13
Affichage de toutes les clés d'un fichier de trousseaux de clés spécifique, 19
Affichage de toutes les signatures de certification associées à chaque clé, 19
Affichage des clés et des signatures du trousseau de clés, 14
Affichage des empreintes digitales d'un jeu de clés, 14
Affichage du contenu d'un trousseau de clés publiques, 19
Affichage du contenu d'un trousseau de clés publiques et vérification des signatures de certification, 19
Aide sur les options relatives aux clés., 13
Aide sur les options relatives aux groupes, 13
Ajout d'éléments à un groupe, 14
Ajout de clés au trousseau, 14
Ajout du contenu d'un fichier de clés publiques ou secrètes ou d'un trousseau de clés publiques ou secrètes., 18
ARMOR, 34
ARMORLINES, 35
Assistant PGPkeys
    création d'une paire de clés, 8

B

BATCHMODE, 21

C

-c, 13
CERT_DEPTH, 35
Certification
    clés publiques, 3
Certificats de signature, 26
CIPHERNUM, 37
Clé de signature par défaut, 29
CLEARSIG, 35
Clés
    copie de sauvegarde, 10
    distribution, 11
    enregistrement, 10
    présentation, 7
    protection, 10
Clés privées
    création
        paires de clés, 2
    présentation, 1
    protection, 10
    stockage, 10
Clés publiques
    certification, 3
    création
        paires de clés, 2
    diffusion à d'autres utilisateurs, 2
    distribution, 11
    échange avec d'autres utilisateurs, 2
    protection, 10
    stockage, 10
    validation, 2
Codes d'erreur, 45
Codes d'état de sortie de PGP, 22
Codes de sortie, 45
Commande -kx, 10
Commande shell permettant d'afficher du texte de sortie en clair, 39
Commandes de gestion des clés, 29
Commandes de gestion des fichiers, 27
COMMENT, 36
Commentaire au format ASCII protégé, 36

COMPATIBLE, 6
COMPLETES_NEEDED, 37
COMPRESS, 37
Compression avant cryptage, 37
Confirmation d'ajouts de clés, 38
Copie d'une clé à partir d'un trousseau de clés publiques ou secrètes, 18
Correspondant à fiabilité ultime, 29
Création
    paire de clés, 8
    paires de clés, 8
Création d'un certificat de signature et de fichiers texte séparés, 26
Création d'un certificat de signature séparé du document, 20
Création d'un fichier de texte chiffré au format ASCII protégé 64, 18
Création d'un fichier de texte en clair ASCII, 18
Création d'une clé de signature par défaut à partir d'une clé existante, 29
Création d'une paire de clés, 15
Cryptage
    message électronique, 3
Cryptage automatique, 38
Cryptage conventionnel, 13
Cryptage d'un fichier de texte en clair avec la clé publique du destinataire, 16
Cryptage d'un message pour plusieurs destinataires, 17
Cryptage d'un message pouvant être affiché uniquement par les destinataires, 17
Cryptage d'un texte en clair par cryptographie conventionnelle uniquement, 16
Cryptage de données binaires, 23
Cryptage via le cryptage de clé publique, 13

D

Décryptage
    message électronique, 3
Décryptage d'un message, 16
Décryptage d'un message au format ASCII protégé, 16
Décryptage d'un message et affichage du texte de sortie en clair, 27
Décryptage d'un message et affichage du texte en clair de sortie, 16
Décryptage d'un message et récupération du nom de fichier de texte en clair original, 16
Décryptage d'un message, lecture à partir d'une entrée standard et écriture dans une sortie standard, 16
Décryptage de messages au format ASCII protégé, 24
Définition du nom du chemin d'accès de PGP, 6
Désactivation d'une clé, 15
Distribution
    clés publiques, 2, 11

E

-e, 13
Echange de clés publiques
    clés publiques, 2
Effacement, 13
Effacement du disque, 28
Effacement du fichier de texte en clair original, 17
ENCRYPTTOSELF, 38
Enregistrement
    clés, 10
Envoi d'une clé publique au format ASCII protégé, 24
Envoi de fichiers de données binaires au format ASCII protégé sans cryptage ni signature, 24
Envoi de fichiers texte ASCII vers différents environnements système, 25
Extraction de clés du trousseau, 14

F

-f, 13
Falsification
    protection des clés, 10
FASTKEYGEN, 38
Fenêtres PGPkeys
    création de paires de clés, 8
Fichier .asc, 13
Fichiers de données binaires, 24

Filtrage, 22
Filtre de type UNIX, 22
FORCE, 22
Format ASCII protégé, 13, 23
Formation sur les produits Network Associates, xi
    programme, xi

G

-g, 13 á 14
Génération
    paires de clés, 8
Génération d'une clé, 14
Génération de clés rapide, 38
Gestion des certificats de signature, 26

H

-h, 13
HASHNUM, 38
HOME, 21

I

ID d'utilisateur par défaut pour les signatures, 39
INTERACTIVE, 38

K

-k, 13 á 14
KEYSERVER_URL, 38

L

Lancement de PGP, 5

M

-m, 13
MARGINALS_NEEDED, 39
Message électronique
    cryptage, 3
    décryptage, 3
    signature, 3
    vérification, 3
Message signé lisible à l'œil nu, 35
Mode filtre de type UNIX, 13
Modification d'un jeu de clés, 14
Modification de l'ID utilisateur ou mot de passe complexe correspondant à votre clé secrète, 19
Modification de votre ID utilisateur ou de votre mot de passe complexe, 29
Modification des paramètres de fiabilité d'une clé publique, 19, 30
Mot de passe complexe
    suggestions, 9
MYNAME, 39

N

Network Associates
    contact
        Etats-Unis, x
        support aux clients, x
    formation, xi
Nom de fichier de votre trousseau de clés publiques, 40
Nom de fichier pour la valeur initiale de nombres aléatoires, 40
Nom du chemin d'accès au répertoire des fichiers temporaires, 41
Nom du fichier de votre trousseau de clés secrètes, 41
nombre de correspondants entièrement fiables nécessaires, 37
Nombre de correspondants fiables de manière marginale nécessaires, 39

O

-o, 13
Obtention d'une clé à partir du serveur et ajout de cette clé dans un trousseau de clés (deux commandes sont nécessaires), 18

P

-p, 13
PAGER, 39
Paire de clés publiques et privées

création, 2
Paires de clés
création, 2, 8
description, 8
génération, 8
PGP 2.6.2, 6
pgp -h, 20
pgp -kd, 15
pgp -kg, 8, 15
pgp.cfg, 33
PGP_MIME, 39
PGP_MIMEPARSE, 40
PGPPASS, 32
PGPPASSFD, 32
PGPPATH, 6
Pirates
protection, 10
Présentations
clés privées, 1
concepts relatifs aux clés, 7
trousseaux de clés, 1
Profondeur des correspondants à imbriquer, 35
Protection
clés, 10
PUBRING, 40
pubring.pkr, 10

R

RANDOMDEVICE, 40
RANDSEED, 40
Réactivation d'une clé, 15
Réception d'un certificat de signature et de fichiers texte séparés, 26
Renvoi du mot de passe complexe à l'utilisateur, 41
Résumé des commandes, 20
Révocation d'une clé, 15
Révocation de signatures associées à des clés du trousseau, 14
Révocation ou désactivation de clés du trousseau, 14

S

-s, 13
SECRING, 41
secring.skr, 10
Sélection de clés à l'aide de l'ID de clé, 31
SHOWPASS, 41
Signature, 13
message électronique, 3
Signature d'un fichier de texte en clair ASCII, 17
Signature d'un fichier de texte en clair avec la clé secrète et cryptage de ce fichier avec la clé publique du destinataire, 17
Signature d'un fichier de texte en clair avec une clé secrète, 17
Signature d'un fichier sans cryptage, 28
Signature de clés du trousseau, 14
Signature et certification de la clé publique d'un autre utilisateur appartenant à votre trousseau de clés publiques, 20
Sortie au format ASCII protégé, 34
Stockage
clés, 10
Stockage de fichiers signés, 28
Stockage de votre mot de passe complexe, 32
Support aux clients
contact, x
Support technique
adresse électronique, x
en ligne, x
informations à fournir par l'utilisateur, x á xi
Supposition que le texte en clair est un fichier texte, 42
Suppression d'éléments d'un groupe, 14
Suppression d'une clé ou d'un ID utilisateur d'un trousseau de clés publiques, 20
Suppression de clés du trousseau, 14
Suppression de signatures associées à des clés du trousseau, 14
Suppression des questions de confirmation, 22
Suppression des questions non essentielles, 21

Suppression des signatures sélectionnées à partir d'un ID utilisateur sur un trousseau de clés, 20

T

-t, 13
Taille des fichiers à plusieurs entrées au format ASCII protégé, 35
TEXTMODE, 42
TMP, 41
Transmission de données binaires, 23
Transmission de votre mot de passe complexe à partir d'une autre application, 32
Trousseaux de clés
    présentation, 1
    présentations, 1

U

-u, 13

V

Validation
    clés publiques, 2
VERBOSE, 43
Vérification
    message électronique, 3
Vérification d'une clé publique par téléphone, 31
Vérification de l'intégrité d'un fichier signé, 16
Vérification de signatures, 14
Vérification du contenu d'un trousseau de clés publiques, 30

W

-w, 13

Z

-z, 13