



Présentation de PGP Desktop

PGP Desktop garantit une sécurité complète pour les ordinateurs de bureau et les portables, permettant ainsi aux entreprises, aux groupes de travail et aux individus de protéger leurs informations sensibles sans modifier leur infrastructure informatique ni interrompre leurs processus de travail. Cette solution primée facile à utiliser chiffre les messages électroniques, les fichiers, les volumes virtuels et les disques entiers grâce à une application bureautique unique.

La famille d'applications PGP Desktop se combine en plusieurs offres groupées.

- **PGP Desktop Professional** comprend PGP Desktop Email et PGP Whole Disk Encryption.
- **PGP Whole Disk Encryption** comprend PGP Whole Disk Encryption.

PGP Desktop Email

Grâce à PGP Desktop Email, vous pouvez chiffrer, signer, déchiffrer et vérifier les messages électroniques de façon automatique et transparente conformément à des stratégies qui ont été définies pour vous par des administrateurs ou des stratégies que vous configurez si vous ne vous trouvez pas dans un environnement géré par PGP Universal Server.

PGP Whole Disk Encryption

Vous pouvez avoir recours à PGP Whole Disk Encryption (PGP WDE) pour verrouiller l'intégralité du contenu de votre système ou d'un lecteur externe ou USB Flash de votre choix.

PGP Desktop vous permet par ailleurs d'effectuer les opérations suivantes :

- utiliser une partie de l'espace de votre disque dur en tant que lecteur virtuel chiffré possédant sa propre lettre ;
- créer des archives Zip protégées ;
- détruire complètement les fichiers et les dossiers de sorte qu'il soit impossible de récupérer leurs données.

Table des matières

- *Présentation de PGP Desktop* (page 1)
- *Vous venez d'acheter PGP Desktop ?* (page 1)
- *Notions de base* (page 1)
- *Éléments installés* (page 2)
- *Configuration requise* (page 2)
- *Installation de PGP Desktop* (page 2)
- *Démarrage de PGP Desktop* (page 3)
- *Écran principal de PGP Desktop* (page 3)
- *Utilisation de PGP Desktop Email* (page 4)
- *Utilisation de la Visionneuse PGP* (page 5)
- *Chiffrement d'un lecteur à l'aide de PGP WDE* (page 7)
- *Création de volumes PGP Virtual Disk* (page 13)
- *Création d'une archive PGP Zip* (page 10)
- *Décomposition de fichiers à l'aide de PGP Shred* (page 11)
- *Assistance* (page 12)

Vous venez d'acheter PGP Desktop ?

Consultez ce guide détaillé pour vous familiariser avec le logiciel. Vous verrez qu'avec PGP Desktop, protéger vos données devient aussi facile que tourner la clé dans une serrure.

- Ce *guide de démarrage rapide* vous explique comment installer PGP Desktop et commencer à l'utiliser.
- Vous trouverez des informations plus détaillées sur PGP Desktop dans le *Guide de l'utilisateur de PGP Desktop*. Ce manuel vous présente les paires de clés, vous explique pourquoi il peut être utile d'en créer et décrit les procédures de création d'une clé et d'échange de clés avec des tiers en vue de chiffrer vos données et de les partager en toute sécurité.

Remarque : une licence PGP Desktop vous donne accès à un ensemble donné de fonctionnalités PGP Desktop. Certaines fonctionnalités spéciales de PGP Desktop peuvent requérir une licence supplémentaire. Pour plus d'informations, reportez-vous à la section relative aux licences du *Guide de l'utilisateur de PGP Desktop*.

- Pour obtenir des informations sur le déploiement, la gestion et l'application des stratégies pour PGP Desktop, consultez le manuel *Guide de l'administrateur de PGP Universal Server*.

Après l'installation, PGP Desktop vous invite à créer une paire de clés PGP. Une paire de clés est constituée d'une clé privée et d'une clé publique.

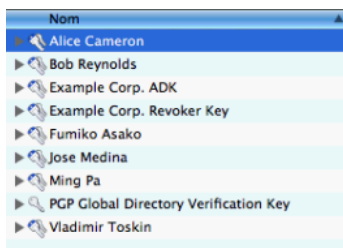
- Comme son nom le suggère, la *clé privée* doit rester

confidentielle, de même la phrase secrète associée. Si une personne prend possession de votre clé privée et de sa phrase secrète, elle pourra lire vos messages et emprunter votre identité pour communiquer avec des tiers. Votre clé privée est employée pour déchiffrer les messages chiffrés entrants et signer les messages sortants.

- En ce qui concerne votre *clé publique*, vous pouvez la communiquer à tous. Aucune phrase secrète ne lui est associée. Elle sert à chiffrer les messages qui ne pourront être déchiffrés qu'avec votre clé privée et à vérifier les messages signés.

Dans votre trousseau de clés sont stockées aussi bien vos paires de clés que les clés publiques de tiers ; vous utilisez ces dernières pour envoyer des messages chiffrés à leurs détenteurs. Pour afficher les clés de votre trousseau, cliquez sur le panneau de contrôle Clés PGP :

1. L'icône pour une paire de clés PGP représente deux clés (qui symbolisent la clé privée et la clé publique). Par exemple, dans l'illustration ci-dessous, Alice Cameron dispose d'une paire de clés PGP.
2. Sur les icônes des clés publiques des autres utilisateurs figure une seule clé. Par exemple, la clé publique de Ming Pa a été ajoutée au trousseau de clés illustré ici.



Éléments installés

PGP Desktop utilise des licences pour octroyer l'accès aux fonctionnalités incluses dans le logiciel. Selon le type de licence dont vous disposez, une partie ou l'intégralité des applications de la gamme PGP Desktop est active.

Ce document contient des instructions relatives à l'affichage des fonctionnalités activées par votre licence.

PGP Desktop Email fait partie de la gamme PGP Desktop. PGP Desktop Email vous permet de chiffrer, signer, déchiffrer et vérifier les messages électroniques de façon automatique et transparente, conformément aux stratégies que vous configurez. Il vous permet également de chiffrer vos sessions de messagerie instantanée, notamment avec les clients AIM et iChat. Les utilisateurs discutant par messagerie instantanée doivent tous deux avoir activé PGP Desktop Email.

PGP Whole Disk Encryption (PGP WDE) fait partie de la gamme PGP Desktop. Vous pouvez avoir recours à cette application pour verrouiller l'intégralité du contenu de votre système ou d'un lecteur externe ou USB Flash de votre choix. Les secteurs de démarrage, fichiers système et fichiers d'échange sont tous chiffrés. Lorsque vous appliquez la fonctionnalité de chiffrement complet du disque à votre lecteur de démarrage, vous n'avez pas à vous préoccuper de

l'éventualité de la perte ou du vol de votre ordinateur : en effet, sans la phrase secrète appropriée, aucun pirate ne pourra accéder à vos données.

Volumes PGP Virtual Disk : fonctionnalité du logiciel permettant d'utiliser une partie de l'espace de votre disque dur en tant que lecteur virtuel chiffré possédant sa propre lettre. Un PGP Virtual Disk représente l'endroit idéal pour stocker vos fichiers sensibles. Cela revient à les placer dans un coffre. Lorsque la porte du coffre est ouverte (quand le volume est monté), vous pouvez modifier les fichiers qu'il contient, en sortir ou en ajouter de nouveaux. Autrement (lorsque le volume est démonté), toutes les données sont protégées.

Avec **PGP Zip**, vous pouvez regrouper différents fichiers et dossiers dans une même archive chiffrée, compressée et portable. Pour que vous puissiez créer ou ouvrir une archive PGP Zip, PGP Desktop doit être installé sur votre système. PGP Zip est un outil grâce auquel vous pouvez archiver en toute sécurité vos données sensibles, que ce soit pour les distribuer à des tiers ou bien les sauvegarder.

PGP Shredder détruit définitivement des fichiers et dossiers pour qu'ils ne puissent pas être récupérés, même à l'aide d'un logiciel de récupération de fichiers. Lorsque vous supprimez un fichier en le plaçant dans la corbeille (sous Windows ou Mac OS X), celui-ci n'est pas véritablement éliminé ; il demeure sur votre lecteur et finira par être écrasé. Jusqu'alors, pour un pirate, le récupérer est un jeu d'enfant. PGP Shredder, au contraire, remplace immédiatement les fichiers, à plusieurs reprises. Cette opération est très efficace, sachant que les fichiers ne peuvent pas être récupérés, même à l'aide d'un logiciel de récupération de disque élaboré. Cette fonctionnalité permet en outre de nettoyer en profondeur l'espace libre sur vos lecteurs pour empêcher la récupération des données que vous avez supprimées.

Avec la **gestion des clés**, vous pouvez gérer les clés PGP, qu'il s'agisse de vos propres paires de clés ou des clés publiques de tiers. Vous utilisez votre clé privée pour déchiffrer les messages que vous recevez et qui ont été chiffrés avec votre clé publique, et pour sécuriser vos volumes PGP Virtual Disk. Vos clés publiques, quant à elles, vous servent à chiffrer les messages que vous envoyez ou à ajouter des utilisateurs aux volumes PGP Virtual Disk.

Configuration requise

Pour installer PGP Desktop sur votre système Mac OS X, vous devez disposer de la configuration système minimale suivante :

- Apple Mac OS X
- 512 Mo de RAM
- 64 Mo d'espace disque dur

Installation de PGP Desktop

PGP Corporation vous recommande de fermer toutes les applications ouvertes avant de lancer l'installation. Ce

processus peut nécessiter un redémarrage du système.

Remarque : pour pouvoir installer la mise à jour, vous devez disposer de droits d'administration sur votre système.

Le programme d'installation de PGP Desktop vous guide tout au long de la procédure d'installation du logiciel.

➤ **Pour installer PGP Desktop sur votre système Mac OS X**

1. Fermez toutes les autres applications.
2. Montez l'image DiskCopy PGP.
3. Cliquez deux fois sur PGP.pkg.
4. Suivez les instructions affichées à l'écran.
5. Si vous y êtes invité, redémarrez le système.

Remarque : si votre ordinateur se trouve dans un domaine protégé par un PGP Universal Server, votre administrateur PGP aura peut-être prédéfini des fonctions ou paramètres du programme d'installation de PGP Desktop. En outre, si votre administrateur PGP a configuré une inscription automatisée, votre mot de passe de domaine Windows sera utilisé pour toutes les conditions requises de phrase secrète dans PGP Desktop. Si la stratégie le spécifie, PGP Whole Disk Encryption peut démarrer automatiquement pour chiffrer le contenu de votre disque au moment où votre mot de passe Windows est saisi.

Gestion des licences

Pour connaître les fonctionnalités prises en charge par votre licence, ouvrez PGP Desktop et sélectionnez **PGP > Licence**. Cliquez sur **Détails**. Les détails relatifs à votre licence sont alors affichés.

Démarrage de PGP Desktop

- Quatre modes d'accès sont proposés :
- Écran principal de PGP Desktop
 - Utilisation de l'icône PGP Desktop dans la barre de menus
 - Utilisation de l'icône PGP Dock
 - Utilisation du Finder sous Mac OS X

Écran principal de PGP Desktop

L'écran principal de PGP Desktop représente votre premier mode d'interaction avec le produit.



L'écran principal de PGP Desktop comporte les éléments suivants :

- 1 Le champ de recherche :** vous pouvez y rechercher des clés figurant dans le trousseau de clés local. Il vous suffit de saisir les caractères à trouver pour que les noms et adresses de courrier électronique du trousseau de clés local qui comportent ces caractères s'affichent. Pour utiliser d'autres critères de recherche, cliquez sur **Recherche avancée**.
 - 2 La zone de travail de PGP Desktop :** cette zone contient des informations sur l'élément sélectionné ainsi que sur les actions que vous pouvez lui appliquer.
 - 3 La barre d'outils :** cette barre permet d'accéder aux fonctions fréquemment utilisées. Vous pouvez effectuer les tâches suivantes :
 - créer une archive PGP Zip ;
 - créer un volume PGP Virtual Disk ;
 - monter un volume PGP Virtual Disk existant ;
 - synchroniser des clés ;
 - décomposer des fichiers.
 - 4 L'élément Clés :** cet élément vous permet de contrôler les clés PGP que PGP Desktop gère pour vous.
 - 5 L'élément PGP Disk :** cet élément vous permet d'afficher et de gérer les volumes PGP Virtual Disk. Vous pouvez également l'utiliser pour créer d'autres volumes de ce type, ainsi que pour chiffrer un disque entier ou gérer le chiffrement de disques amovibles à l'aide de la fonction PGP Whole Disk Encryption.
 - 6 L'élément Messagerie PGP :** cet élément vous permet de gérer les services de messagerie PGP. Il sert en outre à créer des services et stratégies et à gérer ceux existant.
 - 7 L'élément Serveurs de clés :** cet élément vous permet d'afficher et de gérer les serveurs de clés.
- (non visible)* **L'élément PGP Zip :** cet élément vous permet d'afficher et de gérer les archives PGP Zip.

Utilisation de PGP Desktop Email

PGP Desktop Email chiffre et signe les messages sortants, et déchiffre et vérifie les messages entrants, tout cela de manière totalement automatique et transparente. Continuez à envoyer et recevoir votre courrier électronique comme à l'accoutumée ; PGP Desktop Email s'occupe du reste.

Envoi de courriers électroniques chiffrés

Après l'installation, PGP Desktop Email se positionne entre votre client de messagerie et votre serveur de messagerie électronique et surveille le trafic de courrier électronique.

Lorsque des messages *entrants* arrivent, PGP Desktop les intercepte avant qu'ils n'atteignent votre boîte de réception et essaie automatiquement de les déchiffrer et de les vérifier ; il utilise vos clés privées pour le déchiffrement et les clés publiques de tiers pour la vérification. Après avoir traité les messages, il les place dans votre boîte de réception.

Le plus souvent, vous n'avez rien à faire ; les messages entrants déchiffrés sont affichés dans votre boîte de réception exactement comme les autres.

Lorsque vous envoyez du courrier électronique, PGP Desktop Email intercepte ces messages *sortants* lors de leur transfert vers votre serveur de messagerie électronique et essaie automatiquement de les chiffrer et de les signer, conformément aux stratégies configurées.

Là encore, vous n'avez rien à faire ; lorsque vous créez un message à l'aide de votre client de messagerie, puis l'envoyez, PGP Desktop Email se charge de tout.

Pour savoir en détail comment PGP Desktop Email gère vos messages entrants et sortants en toute transparence, reportez-vous aux sections ci-après.

Messages entrants

PGP Desktop gère les messages électroniques entrants en fonction de leur contenu. Ces scénarios supposent une utilisation autonome de PGP Desktop, et non pas dans un domaine protégé par un PGP Universal Server (dans ce cas, les stratégies de messagerie définies par votre administrateur PGP Universal Server s'appliquent) :

- **Message ni chiffré, ni signé.** PGP Desktop transfère le message à votre client de messagerie sans effectuer la moindre action sur le contenu du message.
- **Message chiffré mais non signé.** Lorsque PGP Desktop détecte un message entrant chiffré, il tente de le déchiffrer pour vous. Pour cela, PGP Desktop recherche dans le trousseau de clés local la clé privée capable de déchiffrer le message. Si la clé privée ne se trouve pas dans le trousseau de clés local, PGP Desktop ne pourra pas procéder au déchiffrement du message. Ce dernier sera alors transféré à votre client de messagerie sans être déchiffré. Si la clé privée se trouve dans le trousseau de clés local, PGP Desktop déchiffre aussitôt le message, à condition que la phrase secrète de la clé privée se trouve en mémoire (en cache). Si ce n'est pas le cas, PGP Desktop vous invite à saisir la phrase secrète et, si elle est

correcte, déchiffre le message. Une fois le message déchiffré, PGP Desktop le transfère à votre client de messagerie.

Si le proxy de messagerie de PGP Desktop est désactivé, PGP Desktop ne peut pas déchiffrer les messages entrants chiffrés. Il les transfère alors à votre client de messagerie tels quels. Il est conseillé de laisser votre proxy de messagerie activé en permanence si vous prévoyez d'envoyer et de recevoir des messages chiffrés. Par défaut, il est activé.

- **Message signé mais non chiffré.** PGP Desktop recherche dans le trousseau de clés local la clé publique qui permet de vérifier la signature. Si PGP Desktop ne parvient pas à trouver la clé publique adéquate dans le trousseau de clés local, il recherche alors un serveur de clés dans `keys.domain` (où **domain** correspond au domaine de l'expéditeur du message), puis dans le *PGP Global Directory* (<https://keyserver.pgp.com>), et enfin dans tout autre serveur de clés configuré. Si PGP Desktop parvient à trouver la clé publique appropriée à l'un de ces emplacements, il vérifie la signature et transfère le message à votre client de messagerie, avec en annotation les informations relatives à la signature. (Ces informations sont également consignées dans le journal de PGP.) Si PGP Desktop ne parvient pas à trouver la clé publique adéquate, il transfère le message à votre client de messagerie sans le vérifier.
- **Message chiffré et signé.** PGP Desktop effectue les deux processus décrits ci-dessus : il commence par rechercher la clé privée afin de déchiffrer le message, puis il recherche la clé publique pour en vérifier la signature. Il est cependant à noter que si un message ne peut pas être déchiffré, il ne peut pas être vérifié.

Si PGP Desktop ne parvient pas à déchiffrer ou vérifier un message, il peut être utile de contacter l'expéditeur du message. Si le message n'a pas pu être déchiffré, assurez-vous que l'expéditeur a utilisé votre clé publique correcte. Si le message n'a pas pu être vérifié, demandez à l'expéditeur de publier sa clé sur le PGP Global Directory (les anciennes versions de PGP ou les autres produits OpenPGP peuvent accéder à la version en ligne de cet annuaire à l'adresse *PGP Global Directory* (<https://keyserver.pgp.com>)) ou de vous l'envoyer directement par message électronique.

Remarque : Par défaut, PGP Desktop ne chiffre les messages qu'avec des clés dont la validité est certifiée. Si vous n'avez pas obtenu de clé depuis le PGP Global Directory, vérifiez son empreinte digitale avec le propriétaire et signez-la pour pouvoir l'utiliser.

Messages sortants

Les messages électroniques que vous envoyez peuvent être chiffrés, signés, les deux ou ni l'un ni l'autre. Puisque vous avez probablement des combinaisons différentes pour les destinataires ou les domaines de messagerie, vous devez créer des stratégies pour vos différentes possibilités de message électronique sortant. Une fois les stratégies correctes mises en œuvre, vos messages électroniques sont

protégés de manière automatique et transparente.

Si votre ordinateur se trouve dans un environnement géré par un PGP Universal Server, vos stratégies PGP Desktop sont contrôlées par les stratégies définies par votre administrateur PGP Universal Server. Celui-ci peut également avoir défini le mode de gestion des messages électroniques sortants en cas d'indisponibilité du PGP Universal Server. Ces stratégies sont appelées « stratégies hors connexion » (ou locales).

Stratégies par défaut

PGP Desktop Email inclut quatre stratégies par défaut :

- **Demandes administrateur de liste de publipo** : les demandes administratives de listes de publipo sont envoyées en clair, c'est-à-dire ni chiffrées, ni signées.
- **Envois de listes de publipo** : les envois de listes de publipo sont transférés signés, à des fins d'authentification, mais pas chiffrés.
- **Demande le chiffrement : confidentiel [PGP]** : tout message marqué comme confidentiel dans votre client de messagerie ou contenant le texte « [PGP] » en objet doit être chiffré à l'aide de la clé publique valide du destinataire, sans quoi il ne sera pas envoyé. Cette stratégie représente un moyen de gérer facilement les messages qui *doivent* être envoyés sous forme chiffrée ou ne seront pas envoyés du tout.
- **Chiffrement opportuniste** : indique que tout message pour lequel aucune clé de chiffrement n'a pu être trouvée doit être envoyé en clair (sans chiffrement). Placer cette stratégie en dernier dans la liste des stratégies permet de vous assurer que le message sera effectivement envoyé (sauf si vous le marquez comme étant confidentiel), même si c'est en clair, y compris si la clé de chiffrement du destinataire est introuvable.

Création de stratégies

PGP Desktop Email offre la possibilité de créer et d'utiliser d'autres stratégies que les quatre stratégies par défaut. Vous pouvez créer des stratégies sur la base d'un large choix de critères. Si vous utilisez PGP Desktop Email dans un environnement géré par un PGP Universal Server, vos stratégies de messagerie ainsi que d'autres paramètres peuvent être contrôlés par l'administrateur PGP de l'entreprise.

Pour obtenir des informations exhaustives à propos de la création et de la mise en œuvre des stratégies de messagerie, reportez-vous au manuel *Guide de l'utilisateur de PGP Desktop*.

Mon message a-t-il été chiffré ?

Dans la mesure où PGP Desktop Email agit de façon automatique et transparente, vous pouvez parfois être amené à vous demander si vos messages sont vraiment envoyés sous forme chiffrée. C'est probablement le cas, mais vous pouvez vous en assurer.

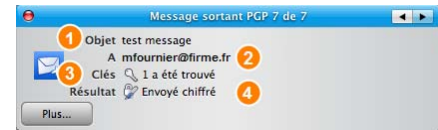
Alertes du Notificateur

Les alertes du Notificateur PGP Desktop vous signalent les événements liés à votre système de messagerie et vous

permettent de les contrôler.

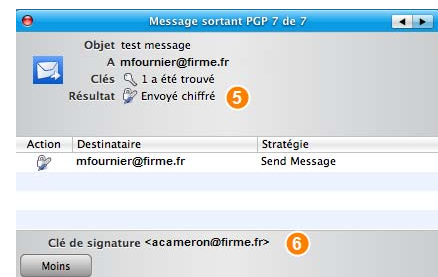
Par exemple, lorsque vous envoyez un message chiffré, l'alerte de Notificateur correspondante apparaît dans le coin inférieur droit de l'écran. Elle comprend les éléments suivants :

1. Objet de l'alerte
2. Nom du destinataire
3. Clés trouvées pour ce dernier
4. État du message



Si vous souhaitez davantage d'informations concernant le message envoyé, cliquez sur **Plus**. Des informations supplémentaires s'affichent :

5. Opérations que PGP Desktop Email a effectuées sur le message
6. Nom du signataire du message



Pour plus d'informations sur les notifications, consultez le *Guide de l'utilisateur de PGP Desktop*.

Journal de PGP

Le journal de PGP répertorie diverses mesures prises par PGP Desktop dans le but de sécuriser votre messagerie.

Par exemple, le message pour lequel les alertes de Notificateur ci-dessus sont affichées a généré dans le journal de PGP une entrée comprenant les éléments suivants :

1. l'indication qu'un message sortant a été envoyé, accompagnée du nom de l'expéditeur et de l'objet du message.
2. L'heure du chiffrement, l'adresse de courrier électronique utilisée pour le chiffrement et l'adresse de courrier électronique de l'expéditeur.

1 Envoyer par courrier électronique Info Traitement du message sortant de gtatou@example.com, dont l'objet est : weekly Status Report
09:31:49 Envoyer par courrier électronique Info chiffrement du message PGP/MIME à gtatou@example.com avec la ou les clés :
2 09:31:49 Envoyer par courrier électronique Info 'gtatou <gtatou@example.com>' <gtatou@example.com> (0x2F542CF1:0x951F3B46)
09:31:49 Envoyer par courrier électronique Info Signature du message PGP/MIME avec la clé 'gtatou <gtatou@example.com>' (0x2F542CF1)

Utilisation de la Visionneuse PGP

En temps normal, PGP Desktop joue le rôle d'intermédiaire entre votre client de messagerie (Mozilla Thunderbird, par exemple) et votre serveur de messagerie électronique, chiffrant et signant les messages sortants, d'une part, et

déchiffrant et vérifiant les messages entrants, d'autre part. Il se trouve alors dans ce que l'on appelle le « flux de messagerie ».

La Visionneuse PGP vous permet de déchiffrer, de vérifier et d'afficher les messages *en dehors* du flux de messagerie.

Ouverture d'un message électronique ou d'un fichier chiffré

Utilisez la Visionneuse PGP pour ouvrir (déchiffrer, vérifier et afficher) les fichiers de messages chiffrés des types suivants :

- **.pgp** : créé par une application PGP.
- **.eml** : créé par Outlook Express ou Thunderbird.
- **.emlx** : créé par le programme Mail.app d'Apple sur les systèmes Mac OS X.
- **.msg** : créé par Microsoft Outlook.

Lorsque la Visionneuse PGP ouvre un message chiffré, elle n'écrase *pas* le texte chiffré. Le message d'origine reste intact.

➤ Pour déchiffrer, vérifier et afficher un message chiffré issu d'un fichier

1. Ouvrez PGP Desktop et sélectionnez l'onglet Visionneuse PGP.
2. Cliquez sur **Ouvrir le fichier dans la Visionneuse PGP** ou sélectionnez **Visionneuse > Ouvrir le fichier dans la Visionneuse PGP**.
3. Dans la boîte de dialogue **Ouvrir le fichier du message**, accédez au fichier à ouvrir, sélectionnez-le et cliquez sur **Ouvrir**. La Visionneuse PGP déchiffre, vérifie et affiche le message dans une fenêtre séparée.

Remarque : vous pouvez faire glisser le fichier à déchiffrer vers la partie de la fenêtre de la Visionneuse PGP qui présente l'intitulé : **Faites glisser les messages ou les fichiers ici**. La Visionneuse PGP ouvre le fichier, le déchiffre et le vérifie, puis affiche le message.

4. Pour ouvrir un autre message, cliquez sur **Ouvrir le message** dans la barre d'outils, accédez au fichier voulu, sélectionnez-le, puis cliquez sur **Ouvrir**. La Visionneuse PGP déchiffre, vérifie et affiche le message.
5. Cliquez sur **Plus petit** pour réduire la taille du texte ou sur **Plus grand** pour l'augmenter.
6. Cliquez sur **Texte riche** pour afficher le message ou le fichier au format RTF ou sur **Texte brut** pour l'afficher en clair.
7. Cliquez sur **Imprimer** pour imprimer le message ou le fichier.

Copie de messages électroniques dans votre boîte de réception

Utilisez la Visionneuse PGP pour copier, dans la boîte de réception de votre client de messagerie, des versions en texte brut des messages déchiffrés.

➤ Pour copier un message dans la boîte de

réception de votre client de messagerie

1. Lorsque le message voulu est affiché dans la fenêtre de la Visionneuse PGP, cliquez sur **Copier vers la boîte de réception**.

La boîte de dialogue de confirmation **Copier vers la boîte de réception** s'affiche. Pour que cette boîte de dialogue de confirmation ne s'affiche plus, cochez la case **Ne plus afficher ce message**.

La boîte de dialogue de confirmation **Copier vers la boîte de réception** contient le nom du client de messagerie vers lequel le message va être copié. Pour modifier ce paramètre, reportez-vous aux préférences de la Visionneuse PGP.

2. Cliquez sur **OK** pour continuer.

Si vous copiez un message vers le client de messagerie Mozilla Thunderbird pour la première fois, une boîte de dialogue vous informant que vous devez installer un module complémentaire s'affiche.

3. Si vous décidez d'installer ce module, cliquez sur **Oui** et suivez les instructions à l'écran ; dans le cas contraire, cliquez sur **Non**. Vous devez utiliser Thunderbird version 2.0 ou ultérieure pour pouvoir installer le module complémentaire.

La Visionneuse PGP ouvre votre client de messagerie et copie une version en texte brut du message dans la boîte de réception.

Exportation de messages électroniques

Pour exporter un message déchiffré vers un fichier, utilisez la Visionneuse PGP.

➤ Pour exporter un message depuis la Visionneuse PGP vers un fichier

1. Lorsque le message est affiché dans la fenêtre de la Visionneuse PGP, cliquez sur **Exporter**.
2. Dans la boîte de dialogue **Exporter le message**, indiquez le nom, l'emplacement et le format du fichier, puis cliquez sur **Exporter**.
La Visionneuse PGP enregistre le fichier à l'emplacement choisi.

Indication d'options supplémentaires

Pour spécifier plusieurs fonctionnalités de la Visionneuse PGP, dans la barre d'outils de cette dernière (située à l'extrême droite), cliquez sur le bouton Outils :

- **Codage du texte** : cette option permet de préciser le format de codage du texte pour le message affiché dans la Visionneuse PGP.
- **Afficher les images distantes** : cette option permet d'afficher les ressources externes (images, feuilles de style CSS, contenu iframe, etc.) pour le message présenté dans la Visionneuse. Vous pouvez configurer la Visionneuse de sorte qu'elle affiche automatiquement les ressources externes dans les préférences.
- **Afficher la source du message** : cette option permet de visualiser la source du message affiché dans la

Visionneuse PGP. Ainsi, vous pourrez obtenir davantage d'informations concernant le message.

- **Préférences** : cette option permet d'ouvrir la boîte de dialogue des préférences de la Visionneuse PGP.

Chiffrement d'un lecteur à l'aide de PGP WDE

Utilisez la fonction PGP WDE pour chiffrer intégralement le disque d'amorçage (ordinateurs Macintosh avec processeur Intel uniquement) et les disques externes sur les systèmes Mac OS X. Cette fonction permet également de chiffrer intégralement les disques externes formatés Windows.

Avant de chiffrer votre disque, assurez-vous de sauvegarder son contenu afin de ne perdre aucune donnée en cas de perte ou de vol de l'ordinateur ou d'incapacité à déchiffrer le disque.

Le logiciel de sauvegarde fonctionne normalement avec PGP WDE ; les fichiers qu'il sauvegarde sont déchiffrés *avant* d'être sauvegardés.

1. Ouvrez PGP Desktop et cliquez sur l'élément PGP Disk. L'écran PGP Disk s'affiche.



2. Cliquez sur **Chiffrer un disque**. L'écran Chiffrer le disque complet apparaît et présente la liste des disques de votre système pouvant être protégés.
3. Dans la liste **Sélectionnez un disque, sélectionnez le disque à protéger**.
4. Dans la section **Sécuriser avec**, précisez la méthode d'accès au disque protégé. Sélectionnez l'utilisateur **Clé publique** ou **Phrase secrète**.

Remarque : si vous chiffrez un disque de démarrage, vous pouvez uniquement utiliser l'authentification par phrase secrète. PGP Desktop sélectionne donc **Utilisateur de phrase secrète** pour vous et passe directement à l'écran Ajout d'un utilisateur de PGP Whole Disk.

- Pour protéger votre disque avec une clé publique, sélectionnez **Clé publique**, puis cliquez sur **Continuer**. L'écran Ajout d'un utilisateur de PGP Whole Disk s'affiche. Sélectionnez une clé dans la liste fournie et cliquez sur **Continuer**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche. Tapez la phrase secrète de la clé sélectionnée, puis cliquez sur **OK**. L'écran Récapitulatif de PGP Whole Disk Encryption apparaît, présentant un récapitulatif de la façon dont le disque sera chiffré. Cette option est disponible uniquement si vous chiffrez un disque

amovible.

- Pour protéger votre disque avec une phrase secrète, sélectionnez **Phrase secrète**, puis cliquez sur **Continuer**. L'écran Ajout d'un utilisateur de PGP Whole Disk s'affiche. Complétez le champ **Nom** (ou acceptez le nom par défaut), puis saisissez la phrase secrète souhaitée dans le champ **Saisissez votre phrase secrète**, puis tapez-la à nouveau dans le champ **Confirmez votre phrase secrète**. **Pour que la phrase secrète s'affiche à mesure que vous saisissez les caractères, sélectionnez Afficher les frappes**. Cliquez sur **Continuer**. L'écran Récapitulatif de PGP Whole Disk Encryption apparaît, présentant un récapitulatif de la façon dont le disque sera chiffré.

L'indicateur de qualité de la phrase secrète fournit une indication de base sur la force de la phrase secrète que vous créez en comparant le degré d'entropie de cette phrase par rapport à une véritable chaîne aléatoire 128 bits (même degré d'entropie que dans une clé AES128). Pour plus d'informations, reportez-vous à la section Indicateur de qualité de la phrase secrète (du *Guide de l'utilisateur de PGP Desktop pour Mac OS X*).

5. Vérifiez les informations, puis cliquez sur **Chiffrer**. Le processus de chiffrement commence et l'écran Progression du chiffrement apparaît.
6. Cliquez sur **Fermer**. La fenêtre de l'application PGP Desktop s'affiche tandis que le processus de chiffrement se poursuit en arrière-plan. Une barre indique l'avancée du processus de chiffrement.

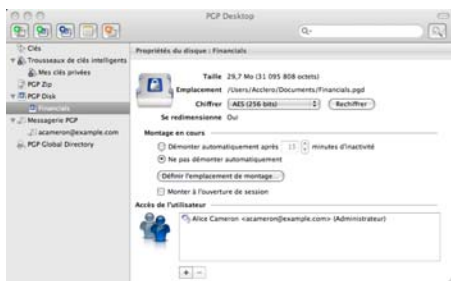
Remarque : le processus de chiffrement continue même si vous fermez l'écran Progression du chiffrement. Vous ne pouvez cependant pas voir la barre de progression tant que vous ne fermez pas cet écran.

7. Au cours du processus de chiffrement, vous pouvez effectuer les opérations suivantes :

- Pour interrompre temporairement le processus de chiffrement, cliquez sur **Arrêter**. La boîte de dialogue Chiffrement non terminé s'affiche.
- Cliquez sur **Pause** pour interrompre le processus de chiffrement, sur **Déchiffrer** pour déchiffrer la partie du disque déjà chiffrée ou sur **Annuler** pour fermer la boîte de dialogue et poursuivre le processus de chiffrement.

Remarque : si le processus s'interrompt pour signaler une erreur de lecture/écriture du disque, cela signifie que PGP Desktop a identifié des secteurs défectueux sur le disque au cours du chiffrement. Inversez immédiatement le processus de chiffrement en *déchiffrant* la partie du disque déjà chiffrée. Utilisez ensuite les outils de vérification de disque pour déterminer et résoudre le problème.

Lorsque le processus de chiffrement est terminé, les propriétés du disque chiffré s'affichent.



Meilleures pratiques avec PGP WDE

Avant de chiffrer votre disque, vous devez effectuer certaines tâches afin de garantir un chiffrement initial correct.

- **Déterminer si le disque concerné est pris en charge** : pour plus de détails concernant les types de disques pris en charge, reportez-vous à la section « Types de disques pris en charge » du *Guide de l'utilisateur de PGP Desktop*.
- **Vérifier que les caractères que vous avez utilisés pour votre phrase secrète sont tous pris en charge** : pour connaître la liste des caractères acceptés pour les phrases secrètes, reportez-vous à la section « Caractères pris en charge » du *Guide de l'utilisateur de PGP Desktop*.
- **Vérifier le bon fonctionnement du disque avant de commencer son chiffrement** : si PGP WDE rencontre des erreurs sur le disque lors du chiffrement, le processus sera interrompu afin que vous puissiez les corriger. Il est cependant plus efficace de les résoudre avant de commencer le chiffrement. Reportez-vous à la section *Vérification du bon fonctionnement du disque avant le chiffrement* (à la page 8).
- **Effectuer une sauvegarde du disque avant le chiffrement** : avant de chiffrer votre disque, assurez-vous de sauvegarder son contenu afin de ne perdre aucune donnée en cas de perte ou de vol de l'ordinateur, ou d'incapacité à déchiffrer le disque. Pensez également à effectuer des sauvegardes régulières.
- **Évaluer le temps nécessaire pour chiffrer le disque** et se préparer en conséquence. Reportez-vous à la section *Calcul de la durée du chiffrement* (à la page 8).
- **Effectuer un test pilote afin de vérifier la compatibilité du logiciel** : pour plus de sécurité, PGP Corporation conseille de tester PGP WDE sur quelques ordinateurs afin de vérifier qu'il n'existe aucun conflit avec d'autres logiciels installés avant un déploiement sur un grand nombre d'ordinateurs. Ce test peut s'avérer particulièrement utile dans les environnements utilisant une image COE (Corporate Operating Environment) standardisée. Certains logiciels de protection des disques sont incompatibles avec PGP WDE et peuvent causer de graves problèmes, tels que la perte de données. Reportez-vous à la section *Effectuer un test pilote afin de vérifier la compatibilité du logiciel* (à la page 9), qui répertorie les problèmes d'interopérabilité connus, ainsi que les *Notes de publication de PGP Desktop* contenant

les mises à jour apportées à cette liste.

- **Vérifier que le mode veille a été désactivé**. PGP Desktop n'est pas compatible avec le mode mise en veille prolongée des systèmes Mac OS X.
- **Utilisation d'Apple Boot Camp**. Si vous utilisez Apple Boot Camp, PGP Corporation vous recommande d'effectuer toutes les opérations de chiffrement et de déchiffrement à partir de la partition Mac OS X. Assurez-vous que vous avez installé PGP Desktop sur les partitions Mac OS X et Windows avant d'effectuer les opérations de chiffrement et de déchiffrement à partir de la partition Mac OS X.

Vérification du bon fonctionnement du disque avant le chiffrement

PGP Corporation adopte délibérément une attitude prudente lors du chiffrement des disques afin d'éviter la perte de données. Il n'est pas rare que des erreurs de contrôle de redondance cyclique (CRC) se produisent au cours du processus. Si PGP WDE rencontre un disque dur comportant des secteurs défectueux, il interrompt, par défaut, le processus de chiffrement. Vous pouvez ainsi résoudre le problème avant de reprendre le chiffrement afin d'éliminer le risque que des données soient endommagées ou perdues.

Pour éviter toute interruption lors du chiffrement, PGP Corporation vous recommande de corriger les erreurs du disque avant de commencer le processus.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, les secteurs défectueux identifiés lors du chiffrement sont consignés dans le PGP Universal Server et le processus se poursuit.

Recommandations

Avant d'utiliser PGP WDE, il est recommandé d'exécuter un utilitaire tiers d'analyse du disque capable d'effectuer une vérification de base de l'intégrité des données et de corriger les incohérences pouvant engendrer des erreurs de contrôle de redondance cyclique (CRC). Ces applications sont capables de corriger les erreurs susceptibles d'affecter le chiffrement.

Attention : Il est vivement conseillé de défragmenter les disques présentant une fragmentation importante avant de les chiffrer.

Calcul de la durée du chiffrement

Le chiffrement est un processus long et très consommateur en CPU. La durée du processus de chiffrement est fonction de la taille du disque. Prenez ce facteur en compte lorsque vous planifiez le chiffrement initial du disque.

Facteurs ayant une incidence sur la vitesse du chiffrement :

- taille du disque ;
- nombre de processeurs et leur vitesse ;
- nombre de processus système exécutés sur l'ordinateur ;
- nombre d'applications exécutées sur le système ;
- quantité du temps processeur requise par ces

applications.

Sur un système moyen, le chiffrement d'un disque de démarrage de 80 Go nécessite environ trois heures avec PGP Whole Disk Encryption (lorsque aucune autre application n'est exécutée). Un système très rapide, en revanche, peut facilement chiffrer ce disque en moins d'une heure.

Vous pouvez, sans problème, utiliser votre système lors du chiffrement. Au cours du processus de chiffrement, vous pouvez utiliser le système, mais son fonctionnement est ralenti.

PGP Desktop ralentit automatiquement le processus de chiffrement si vous utilisez le système. Le processus est plus rapide si vous ne vous servez pas de l'ordinateur au cours du chiffrement initial. Le système fonctionne de nouveau normalement une fois le chiffrement terminé.

L'exécution d'autres applications au cours du chiffrement sera légèrement moins rapide jusqu'à la fin du processus.

Effectuer un test pilote afin de vérifier la compatibilité du logiciel

Pour plus de sécurité, PGP Corporation conseille de tester PGP WDE sur quelques ordinateurs afin de vérifier qu'il n'existe aucun conflit avec d'autres logiciels installés avant un déploiement sur un grand nombre d'ordinateurs.

Création de volumes PGP Virtual Disk

La fonction relative aux volumes PGP Virtual Disk utilise une partie de l'espace de votre disque dur en tant que volume de disque virtuel chiffré. Vous pouvez créer des utilisateurs supplémentaires pour un volume, afin de permettre aux personnes que vous choisissez d'y accéder.

1. Dans PGP Desktop, sélectionnez l'élément PGP Disk, puis cliquez sur **Nouveau PGP Virtual Disk**.



2. Dans le champ **Veillez saisir la taille souhaitée pour le volume PGP Disk**, indiquez la quantité d'espace à réserver au nouveau volume PGP Virtual Disk. Utilisez des nombres entiers, pas des nombres décimaux. Vous pouvez augmenter ou diminuer le chiffre affiché dans le champ à l'aide des flèches. Dans le menu, sélectionnez **Ko** (kilo-octets), **Mo** (méga-octets) ou **Go** (giga-octets).
3. Précisez le type d'authentification à mettre en place pour l'utilisateur principal de ce volume PGP Virtual Disk :

- Pour protéger le volume avec votre paire de clés, sélectionnez **Clé publique**.
 - Pour le protéger avec une phrase secrète, sélectionnez **Utilisateur de phrase secrète**.
4. Pour afficher ou modifier les options avancées, cochez la case **Options avancées**. Les options **Chiffrer** et **Formater** s'affichent.

Attention : les paramètres **Options avancées** par défaut conviennent à la plupart des utilisateurs. Évitez de les modifier si elles ne vous sont pas familières.

- Dans le menu **Chiffrer**, sélectionnez l'algorithme de chiffrement à employer pour protéger le volume PGP Virtual Disk : **AES 256 (256 bits)** ou **CAST5 (128 bits)**. Pour plus d'informations sur ces algorithmes de chiffrement, reportez-vous à la section Algorithmes de chiffrement des volumes PGP Virtual Disk du *Guide de l'utilisateur de PGP Desktop pour Mac OS X*.
- Dans le menu **Formater**, choisissez le format de disque à appliquer au volume PGP Virtual Disk.

MS-DOS : optez pour ce format si vous envisagez de partager ce volume avec un autre utilisateur de PGP Desktop 10.0 pour Windows.

Mac OS étendu : il s'agit du format par défaut (utilisé par ailleurs dans le système de fichiers Mac OS moderne) ; il prend en charge les gros volumes PGP Virtual Disk. La taille minimale est de 4 Mo. Le format Mac OS étendu est aussi nommé HFS+.

Mac OS étendu (journalisé) : optez pour ce format si la journalisation est activée sur votre système. (Avec la journalisation, une copie de tous les éléments enregistrés sur le disque est placée dans une zone privée du système de fichiers, ce qui facilite la récupération du disque en cas de besoin.)

Mac OS étendu (respecte la casse, journalisé) : optez pour ce format si la journalisation avec distinction des majuscules et minuscules est activée sur votre système.

Mac OS standard : ce format garantit une compatibilité ascendante avec les systèmes d'exploitation Mac OS plus anciens. La taille minimale du volume doit être de 512 Ko.

Système de fichiers UNIX : optez pour ce format si vous avez l'intention de partager le volume PGP Virtual Disk avec une personne utilisant un système de fichiers UNIX. La taille minimale du volume doit être de 128 Ko.

Pour connaître le format d'un lecteur Mac OS X existant, sélectionnez-le, puis, dans le menu Fichier, choisissez Obtenir des infos.

5. Cliquez sur **Continuer**.
6. L'étape suivante est différente selon que vous avez choisi une authentification avec clé publique ou phrase secrète.

- Dans le cas d'un accès à l'aide d'une clé publique, l'écran Sélectionnez une clé publique pour sécuriser votre PGP Disk apparaît ; il comporte les clés publiques grâce auxquelles vous pouvez vous authentifier pour accéder au volume PGP Virtual Disk que vous créez.

Sélectionnez une clé dans la liste fournie et cliquez sur **Continuer**. Vous devez alors saisir la phrase secrète rattachée à la clé choisie (sauf si cette phrase est déjà en cache, auquel cas vous n'avez rien à faire).

Indiquez la phrase secrète, puis cliquez sur **OK**. La boîte de dialogue Enregistrer sous s'affiche. Passez à l'étape suivante.

- Dans le cas d'un accès à l'aide d'une phrase secrète, l'écran Définir une phrase secrète principale pour votre PGP Disk apparaît.

Dans le champ **Nom**, saisissez le nom que vous souhaitez attribuer à l'utilisateur principal (ou administrateur) du volume PGP Virtual Disk.

Dans le champ **Saisissez votre phrase secrète**, tapez la phrase secrète que vous voulez utiliser. L'indicateur **Qualité de la phrase secrète** indique le niveau de sécurité de la phrase secrète saisie. Si vous souhaitez voir les caractères tapés et si vous êtes sûr que personne ne peut être témoin de la saisie, cochez la case **Afficher les frappes**.

Dans le champ **Confirmez votre phrase secrète**, saisissez à nouveau la phrase secrète à utiliser. Cliquez sur **Continuer**. La boîte de dialogue Enregistrer sous s'affiche. Passez à l'étape suivante.

7. Saisissez un nom de fichier et un emplacement pour le volume PGP Virtual Disk, puis cliquez sur **Enregistrer**.
8. Vérifiez les informations figurant dans l'écran Récapitulatif de la création de PGP Disk. Lorsque vous avez terminé, cliquez sur **Créer**.
9. L'écran Création de votre volume PGP Virtual Disk est affiché ; il indique l'état d'avancement de la création du volume. Lorsque le disque a été créé, l'écran Félicitations apparaît. Cliquez sur **Terminer**.
10. Votre nouveau volume PGP Virtual Disk est monté automatiquement, et les informations afférentes sont affichées dans une fenêtre du Finder. Le nom du disque est en outre fourni sous l'élément **PGP Disk**.

Création d'une archive PGP Zip

Avec les archives PGP Zip, vous pouvez regrouper différents fichiers et dossiers dans une même archive compressée et portable. Il existe trois types d'archives PGP Zip :

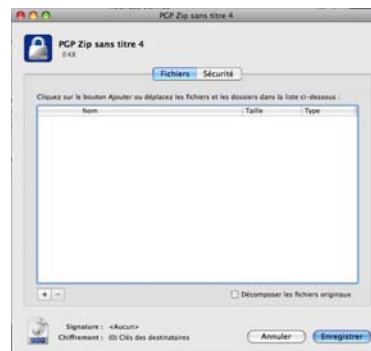
- **Clés des destinataires** : permet de chiffrer l'archive avec des clés publiques. Seul le détenteur des clés privées correspondantes peut ouvrir l'archive. Il s'agit du type d'archive PGP Zip le plus sécurisé. Les destinataires

doivent également utiliser le logiciel PGP (pour Windows ou Mac OS X).

- **Phrase secrète** : permet de chiffrer l'archive avec une phrase secrète, qui doit être transmise aux destinataires. Les destinataires doivent également utiliser le logiciel PGP (pour Windows ou Mac OS X).
- **Signer uniquement** : permet de signer l'archive sans la chiffrer, simplement pour prouver que vous êtes bien l'expéditeur. Les destinataires doivent également utiliser le logiciel PGP (pour Windows ou Mac OS X) pour pouvoir ouvrir et vérifier l'archive.

Les types d'archive PGP Zip Phrase secrète et Signer uniquement sont décrits brièvement dans le présent document, mais de manière plus détaillée dans le *Guide de l'utilisateur de PGP Desktop*.

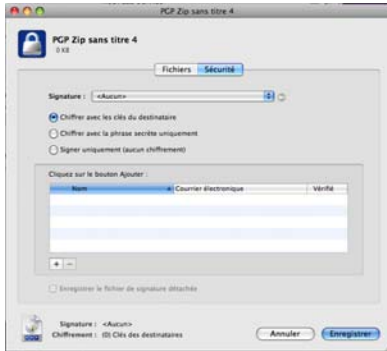
1. Ouvrez PGP Desktop et sélectionnez l'élément PGP Zip. La boîte de dialogue PGP Zip s'affiche.
2. Cliquez sur **Créer un PGP Zip**. La boîte de dialogue PGP Zip sans titre apparaît.



3. Sous l'onglet **Fichiers**, précisez les fichiers ou dossiers à inclure dans l'archive PGP Zip que vous créez. Procédez comme suit :
 - Faites glisser les fichiers et dossiers vers la liste.
 - Cliquez sur le signe « plus » situé sous la liste, puis, dans la boîte de dialogue qui s'ouvre, sélectionnez les fichiers ou dossiers à inclure dans l'archive PGP Zip. Cliquez ensuite sur **Ajouter** afin d'ajouter les fichiers ou dossiers à la liste.

Si vous ajoutez un fichier ou un dossier et vous apercevez par la suite que vous n'en avez plus besoin, sélectionnez-le dans la liste et cliquez sur le signe « moins » situé au-dessous. Le fichier ou dossier est alors supprimé de la liste.
4. Pour supprimer en toute sécurité de votre système les fichiers ou dossiers que vous placez dans l'archive PGP Zip, choisissez l'option **Décomposer les fichiers originaux**.

5. Lorsque vous avez précisé les fichiers ou dossiers à inclure dans l'archive, cliquez sur l'onglet **Sécurité**.



6. Si vous le souhaitez, spécifiez la clé privée de votre trousseau de clés à utiliser pour doter l'archive PGP Zip en cours de création d'une **signature**.

Cette clé servira à signer numériquement l'archive. Le ou les destinataires peuvent vérifier qui a envoyé l'archive en vérifiant la signature numérique avec la clé publique correspondante.

Pour consulter les propriétés de la clé de signature sélectionnée, cliquez sur l'icône de clé située à droite de l'ID utilisateur associé à la clé. Lorsque vous avez terminé, fermez la boîte de dialogue Infos sur la clé.

7. Sélectionnez le type de chiffrement à employer :

- **Chiffrer avec les clés du destinataire** : cette option permet de chiffrer l'archive PGP Zip avec les clés publiques du ou des destinataires. Ainsi, seules ces personnes peuvent l'ouvrir.

Si vous optez pour un chiffrement par clé publique, faites glisser les clés publiques des destinataires sur la liste, ou cliquez sur le signe « plus » et sélectionnez les clés publiques des destinataires souhaités.
- **Chiffrer avec la phrase secrète uniquement** : cette option permet de chiffrer l'archive PGP Zip à l'aide d'une phrase secrète que vous fournissez lors de l'enregistrement de l'archive. Seules les personnes qui connaissent la phrase secrète peuvent ouvrir l'archive. N'oubliez pas de communiquer cette phrase secrète aux personnes auxquelles vous voulez donner accès à l'archive.

Saisissez-la dans le champ **Phrase secrète**, puis retapez-la dans le champ **Confirmer**. Pour que la phrase secrète s'affiche à mesure que vous saisissez les caractères, sélectionnez **Afficher les frappes**.
- **Signer uniquement (aucun chiffrement)** : cette option permet de créer une archive PGP Zip non chiffrée. Néanmoins, étant donné que vous ne chiffrez pas l'archive, vous devez spécifier une clé de signature dans le champ **Signature**.

8. Si votre archive PGP Zip ne contient qu'un seul fichier et que vous signiez le fichier, mais ne le chiffriez pas, vous devez créer un fichier de signature détachée ; pour cela, cochez la case **Enregistrer le fichier de signature**

détachée.

Si vous souhaitez créer ce type de fichier, vous ne pouvez inclure dans l'archive qu'*un seul* fichier, vous devez choisir une clé de signature et vous pouvez pas chiffrer l'archive.

9. Cliquez sur **Enregistrer**.
10. Indiquez un nom de fichier et un emplacement pour l'archive PGP Zip, puis cliquez sur **Enregistrer**. Si vous avez indiqué une clé de signature dans le champ **Signature**, vous êtes invité à saisir la phrase secrète associée (si celle-ci n'est pas en cache).
11. Saisissez la phrase secrète, puis cliquez sur **OK**. L'archive PGP Zip est créée à l'emplacement indiqué.

Décomposition de fichiers à l'aide de PGP Shred

La fonctionnalité PGP Shredder détruit totalement les fichiers et dossiers, de sorte que même un logiciel de récupération de fichiers élaboré n'est pas en mesure de les récupérer. Lorsque l'icône de PGP Shredder et la Corbeille (sur les systèmes Windows et Mac OS X) apparaissent toutes deux sur votre bureau, seul PGP Shredder écrase immédiatement les fichiers indiqués de sorte qu'ils ne soient pas récupérables.

Pour décomposer des fichiers, utilisez l'un des éléments suivants :

- l'icône PGP Shredder ;
- la barre d'outils de PGP ;
- l'option de menu Décomposer dans PGP Desktop ;
- le Finder.

Décomposition de fichiers à l'aide de l'icône de PGP Shredder

➤ Pour décomposer un fichier ou un dossier à l'aide de l'icône de PGP Shredder

1. Recherchez le fichier ou le dossier à supprimer en toute sécurité.
2. Faites glisser son icône sur celle de PGP Shredder. Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers ou les dossiers indiqués.
3. Cliquez sur **OK**. Le fichier ou le dossier est supprimé de votre système en toute sécurité.

Conseil : Créez un alias de l'icône de PGP Shredder sur votre bureau, ainsi vous n'aurez pas besoin de rechercher l'icône de PGP Shredder dans le dossier /Applications pour décomposer les fichiers. Déplacez ensuite l'alias sur le Bureau (ou Dock).

Décomposition de fichiers à l'aide de l'icône Décomposer les fichiers dans la barre d'outils PGP Desktop

➤ Pour décomposer un fichier ou un dossier à l'aide de la barre d'outils PGP Desktop

1. Cliquez sur l'icône **Décomposer les fichiers** dans la barre d'outils.
2. Recherchez le fichier ou le dossier à décomposer, puis cliquez sur **Décomposer**. Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers ou les dossiers indiqués.
3. Cliquez sur **OK**. Le fichier ou le dossier est supprimé de votre système en toute sécurité.

Décomposition de fichiers à l'aide de la fonction Décomposer du menu Fichier

➤ Pour décomposer un fichier ou un dossier à l'aide de la fonction Décomposer

1. Sélectionnez **Fichier > Décomposer**.
2. Accédez au fichier ou au dossier à décomposer, puis cliquez sur **Décomposer**. Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers ou les dossiers indiqués.
3. Cliquez sur **OK**. Le fichier ou le dossier est supprimé de votre système en toute sécurité.

Décomposition de fichier dans le Finder

➤ Pour décomposer un fichier ou un dossier dans le Finder

1. Dans le Finder, recherchez le fichier ou le dossier à décomposer.
2. Maintenez la touche Ctrl enfoncée et cliquez sur le fichier ou le dossier (ou cliquez avec le bouton droit sur le fichier ou le dossier si votre souris possède deux boutons), puis sélectionnez **PGP > Décomposer**. Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers ou les dossiers indiqués.
3. Cliquez sur **OK**. Le fichier ou le dossier est supprimé de votre système en toute sécurité.

Assistance

Coordonnées

Prise de contact avec le support technique

- Pour connaître les différentes options de support offertes par PGP et savoir comment contacter le support technique, accédez à la *page d'accueil du support de PGP Corporation* (<https://support.pgp.com>).
- Pour consulter la base de connaissances du support PGP ou entrer en relation avec le support technique, accédez au *portail du support PGP* (<https://support.pgp.com>).
Remarque : il vous est possible de consulter certaines parties de la base de connaissances du support PGP même si vous ne bénéficiez pas d'un contrat de support technique, mais vous devez avoir souscrit à ce type de contrat pour pouvoir faire appel au support technique.
- Pour accéder aux forums de support PGP, visitez le *support de PGP* (<http://forum.pgp.com>). Vous pourrez alors participer aux forums de communautés d'utilisateurs hébergés par PGP Corporation.

Prise de contact avec le service clientèle

- Pour obtenir de l'aide à propos des commandes, des téléchargements et de la gestion des licences, consultez le *service clientèle de PGP Corporation* (<https://pgp.custhelp.com/app/cshome>).

Prise de contact avec les autres services

- Pour contacter d'autres personnes de PGP Corporation, consultez la *page des contacts PGP* (http://www.pgp.com/about_pgp_corporation/contact/index.html).
- Pour des informations générales sur PGP Corporation, visitez le *site Web de PGP* (<http://www.pgp.com>).

Documentation disponible

Avant l'installation, vous pouvez consulter la documentation complète relative au produit sur le *portail du support de PGP Corporation* (<https://support.pgp.com>).

Sauf indication contraire, l'aide en ligne est installée et accessible à partir de PGP Desktop. Des notes de publication sont également disponibles ; elles présentent les informations de dernière minute qui n'ont pas pu être incluses dans la documentation du produit. Les guides de l'utilisateur et les guides de démarrage rapide, fournis sous la forme de fichiers PDF, sont disponibles sur le *portail du support de PGP Corporation* (<https://support.pgp.com>).

Une fois que PGP Desktop est commercialisé, des informations complémentaires sont intégrées à la base de connaissances en ligne disponible sur la *base de connaissances du support de PGP* (<https://support.pgp.com/?faq=589>).

Copyright et marques

Copyright © 1991-2009 PGP Corporation. Tous droits réservés. PGP, Pretty Good Privacy et le logo de PGP sont des marques déposées, et PGP Universal est une marque de commerce de PGP Corporation aux États-Unis et dans d'autres pays. Toutes les autres marques, déposées ou non, mentionnées dans ce document appartiennent exclusivement à leur propriétaire respectif.