PGP® Desktop pour Windows

Guide de l'utilisateur

Informations de version

Guide de l'utilisateur de PGP Desktop pour Windows. PGP Desktop Version 10.0.0. Sortie en Décembre 2009.

Informations de copyright

Marques

Licences et brevets

Le chiffrement cryptographique IDEA décrit dans le brevet américain n°5 214 703 est fourni sous licence par Ascom Tech AG. L'algorithme de chiffrement CAST-128, mis en œuvre conformément à la RFC 2144, est disponible dans le monde entier hors droits pour usages commercial et non commercial. PGP Corporation a assorti d'une licence les droits de propriété industrielle inclus dans la demande de brevet portant le numéro de série 10/655,563, déposée par le conseil The Regents (les régents) de l'Université de Californie et intitulée « Block Cipher Mode of Operation for Constructing a Wide-blocksize block Cipher from a Conventional Block Cipher » (Fonctionnement du chiffrement par blocs pour la mise en place d'un chiffrement par blocs volumineux à partir d'un chiffrement par blocs conventionnel). Certains logiciels tiers intégrés au PGP Universal Server sont fournis dans le cadre de la licence GNU-GPL. Le PGP Universal Server n'est pas, globalement, régi par cette licence. Si vous souhaitez obtenir une copie du code source du logiciel GPL inclus dans le PGP Universal Server, contactez le *support de PGP* (https://support.pgp.com). PGP Corporation peut être détenteur de brevets et/ou de demandes de brevet traitant d'un ou de plusieurs sujets abordés dans ce logiciel ou cette documentation ; la mise à disposition du logiciel et de la documentation ne vous apporte aucun droit concernant lesdits brevets.

Notifications

Éléments inclus ou pouvant être inclus dans ce produit :

● Code de compression Zip et ZLib, créé par Mark Adler et Jean-Loup Gailly, issu de la mise en œuvre Info-ZIP développée par zlib (http://www.zlib.net), pouvant être employé après autorisation. ● Libxml2, analyseur C XML et boîte à outils créés pour le projet Gnome, distribués et protégés par copyright dans le cadre de la licence MIT figurant à la page suivante : http://www.opensource.org/licenses/mit-license.html. Copyright © 2007 - Open Source Initiative. ● Programme de compression de données ultra performant bzip2 1.0, disponible gratuitement, fourni sous copyright par Julian Seward, © 1996-2005. ● Serveur d'applications (http://jakarta.apache.org/), serveur Web (http://www.apache.org/), Jakarta Commons (http://jakarta.apache.org/commons/license.html) et log4j, une bibliothèque Java utilisée pour l'analyse HTML, mis au point par l'Apache Software Foundation (Fondation Apache). La licence est disponible à la page www.apache.org/licenses/LICENSE-2.0.txt. ● Castor, structure de liaison de données open source permettant de déplacer des données XML vers des objets du langage de programmation Java et des objets Java vers des bases de données, commercialisée par l'ExoLab Group dans le cadre d'une licence de type Apache 2.0 disponible sur http://www.castor.org/license.html. ● Xalan, bibliothèque de logiciels open source proposée par la Fondation Apache (qui applique le langage de transformation XML XSLT et le langage d'interrogation XML XPath), commercialisée dans le cadre de la licence Apache Software License, version 1.1 (disponible à la page http://xml.apache.org/xalan-j/#license1.1). ● Apache Axis, mise en œuvre du protocole SOAP (« Simple Object Access Protocol ») employée pour les communications entre différents produits PGP et fournie dans le cadre de la licence Apache disponible à la page http://www.apache.org/licenses/LICENSE-2.0.txt. ● mx4j, mise en œuvre open source des API JMX (Java Management eXtension), commercialisée dans le cadre d'une licence de type Apache, disponible à la page http://mx4j.sourceforge.net/docs/ch01s06.html. ● jpeglib version 6a, basé partiellement sur le travail effectué par l'Independent JPEG Group (http://www.ijg.org/). ● Bibliothèque C XSLT libxslt développée pour le projet GNOME, utilisée pour les transformations XML et distribuée dans le cadre de la licence MIT (http://www.opensource.org/licenses/mit-license.html). ● Programme de compilation d'expressions régulières Perl PCRE version 4.5, protégé par copyright et distribué par l'Université de Cambridge. ©1997-2006. Le contrat de licence figure à la page http://www.pcre.org/license.txt. ● Protocoles BIND Balanced Binary Tree Library et DNS (Domain Name System, système de noms de domaine) mis au point et protégés par copyright par Internet Systems Consortium, Inc. (http://www.isc.org). ● Mise en œuvre gratuite de démon sur BSD, proposée par le projet FreeBSD, © 1994-2006. ● Bibliothèque SNMP (Simple Network Management Protocol, protocole d'administration de réseau simple), développée et protégée par copyright par la Carnegie Mellon University © (1989, 1991, 1992), Networks Associates Technology, Inc, © (2001-2003), Cambridge Broadband Ltd. © (2001-2003), Sun Microsystems, Inc., © (2003), Sparta, Inc, © (2003-2006), Cisco, Inc et Information Network Center of Beijing University of Posts and Telecommunications, © (2004). Le contrat de licence afférent est disponible à la page http://net-snmp.sourceforge.net/about/license.html. ● Protocole NTP version 4.2, mis au point par Network Time Protocol et fourni sous copyright à divers contributeurs. ● Protocole LDAP (Lightweight Directory Access Protocol), mis au point et protégé par copyright par The OpenLDAP Foundation. OpenLDAP est une mise en œuvre open source du protocole LDAP. Copyright © 1999-2003, The OpenLDAP Foundation. Le contrat de licence figure à la page http://www.openldap.org/software/release/license.html. Secure Shell OpenSSH version 4.2.1, créé via le projet OpenBSD et commercialisé par le même biais dans le cadre d'une licence de type BSD, disponible à la page http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD. ● PC/SC Lite, mise en œuvre gratuite de PC/SC ; une spécification pour l'intégration SmartCard est commercialisée dans le cadre de la licence BSD. ● Postfix, agent de transfert de messages open source, commercialisé dans le cadre de la licence IBM Public License 1.0, disponible à la page http://www.opensource.org/licenses/ibmpl.php. ● PostgreSQL, système de gestion de base de données relationnelles (SGBDR) pour objets logiciels gratuit, commercialisé dans le cadre d'une licence de type BSD figurant à la page http://www.postgresql.org/about/licence. ● Pilote JDBC PostgreSQL, programme Java gratuit permettant la connexion à une base de données PostgreSQL à l'aide d'un code Java standard indépendant de la base de données (c) (1997-2005, PostgreSQL Global Development Group) et commercialisé dans le cadre d'une licence de type BSD disponible à la page http://jdbc.postgresql.org/license.html. ● PostgreSQL Regular Expression Library, SGBDR pour objets logiciels gratuit, commercialisé dans le cadre d'une licence de type BSD disponible à la page http://www.postgresql.org/about/licence. ● 21.vixie-cron, version de cron, un démon UNIX standard exécutant des programmes donnés selon une planification établie, créée par Vixie. Copyright © 1993-1994, Paul Vixie ; utilisation soumise à autorisation. ● JacORB, objet Java employé pour faciliter la communication entre les processus écrits en langage Java et la couche de données, fourni dans le cadre de la licence open source GNU-LGPL

(Library General Public License, devenue depuis Lesser General Public License) disponible à la page http://www.jacorb.org/lgpl.html. Copyright © 2006, The JacORB Project. ● TAO (ACE ORB), mise en œuvre open source d'un CORBA (Common Object Request Broker Architecture) permettant d'établir la communication entre les processus écrits en langages C/C++ et la couche de données. Copyright © 1993-2006, Douglas C. Schmidt et son groupe de recherche à l'Université de Washington, l'Université de Californie (Irvine) et l'Université Vanderbilt. La licence du logiciel open source est disponible à la page http://www.cs.wustl.edu/~schmidt/ACE-copying.html. ● libcURL, bibliothèque de téléchargement de fichiers via des services de réseau communs, qui est aussi un logiciel open source fourni dans le cadre d'une licence dérivée MIT/X figurant à la page http://curl.haxx.se/docs/copyright.html. Copyright (c) - 1996-2007, Daniel Stenberg. ● libuuid, bibliothèque servant à générer des identifiants uniques et commercialisée dans le cadre d'une licence de type BSD disponible à l'adresse http://thunk.org/hg/e2fsprogs/?file/fe55db3e508c/lib/uuid/COPYING. Copyright © 1996-1997, Theodore Ts'o. ● libpopt, bibliothèque d'analyse des options de ligne de commande, commercialisée dans le cadre de la licence de documentation libre GNU disponible à la page http://directory.fsf.org/libs/COPYING.DOC. Copyright © 2000-2003, Free Software Foundation, Inc. ● gSOAP, outil de développement destiné aux clients Windows, leur permettant de communiquer avec le chipset AMT d'Intel Corporation sur une carte mère, distribué dans le cadre de la licence GNU-GPL disponible à la page http://www.cs.fsu.edu/~engelen/soaplicense.html. ● Windows Template Library (WTL), utilisé pour mettre au point les composants de l'interface utilisateur et distribué dans le cadre de la licence Common Public License v1.0 figurant à la page http://opensource.org/licenses/cpl1.0.php. ● Kit Perl, comprenant plusieurs utilitaires distincts qui permettent d'automatiser des fonctions de maintenance variées, fourni dans le cadre de la licence artistique Perl figurant à la page http://www.perl.com/pub/a/language/misc/Artistic.html. ● rEFIt - libeg, qui apporte une bibliothèque d'interfaces graphiques pour l'échange de formulaires informatisé, notamment le rendu d'image, le rendu de texte et l'alpha blending, et qui est distribué dans le cadre de la licence disponible à la page http://refit.svn.sourceforge.net/viewvc/*checkout*/refit/trunk/refit/LICENSE.txt?revision=288. Copyright © 2006, Christoph Pfisterer. Tous droits réservés. ● Java Radius Client, utilisé pour authentifier les utilisateurs de PGP Universal Web Messenger via Radius et distribué dans le cadre de la licence GNU-LGPL (Lesser General Public License, anciennement Library General Public License) disponible à la page http://www.gnu.org/licenses/lgpl.html. ● Yahoo! Interface utilisateur (YUI) version de bibliothèque 2.5.2, bibliothèque d'interface utilisateur Web pour AJAX. Copyright (c) 2009, Yahoo! Inc. Tous droits réservés. Distribué dans le cadre d'une licence de type BSD, disponible à la page http://developer.yahoo.com/yui/license.html. ● JSON-lib version 2.2.1, bibliothèque Java utilisée pour la conversion d'objets Java en objects JSON (JavaScript Object Notation) pour AJAX. Distribué dans le cadre de la licence Apache 2.0, disponible à la page http://json-lib.sourceforge.net/license.html. ● EZMorph, utilisé par JSON-lib et distribué dans le cadre de la licence Apache 2.0, disponible à la page http://ezmorph.sourceforge.net/license.html. ● Apache Commons Lang, utilisé par JSON-lib et distribué dans le cadre de la licence Apache 2.0, disponible à la page http://commons.apache.org/license.html. ● Apache Commons BeanUtils, utilisé par JSON-lib et distribué dans le cadre de la licence Apache 2.0, disponible à la page http://commons.apache.org/license.html.

Informations concernant l'exportation

L'exportation du logiciel et de la documentation peut être régie par les principes et réglementations énoncés de façon ponctuelle par le Bureau of Export Administration du Département du Commerce américain, qui est chargé de limiter les exportations et ré-exportations de certains produits et de certaines données techniques.

Restrictions

Le logiciel accompagnant la présente documentation vous est fourni sous licence, pour votre usage personnel, dans le cadre du contrat de licence pour utilisateur final associé. Les informations figurant dans ce document peuvent être modifiées sans préavis. PGP Corporation ne saurait garantir que celles-ci répondent à vos besoins ou sont exemptes d'erreurs. Des inexactitudes techniques ou erreurs typographiques peuvent être présentes. Des modifications peuvent toutefois être apportées et incorporées dans les éventuelles versions ultérieures du document au moment de la rédaction de ces dernières.

Table des matières

Utilisation des PGP Virtual Disks 211

Création de données mobiles et accès à celles-ci à l'aide de PGP Portable 233

Utilisation de PGP NetShare 241

1 À propos de PGP Desktop 10.0 pour Windows

PGP Desktop est un outil de sécurité faisant appel au chiffrement pour protéger les données des accès non autorisés.

Il sécurise vos données durant leur transfert par courrier électronique ou messagerie instantanée. Il vous permet de chiffrer l'intégralité de votre disque dur ou de votre partition de disque dur (sous Windows), afin de garantir une protection continue, ou bien une partie du disque dur, via un disque virtuel sur lequel vous pouvez stocker vos données essentielles en toute sécurité. Vous pouvez aussi utiliser l'application pour partager vos fichiers et dossiers de façon sécurisée avec d'autres utilisateurs du même réseau. Il vous est possible de regrouper divers fichiers et dossiers au sein d'un module compressé chiffré pour une distribution ou une sauvegarde simple. PGP Desktop vous permet enfin de décomposer (supprimer en toute sécurité) vos fichiers sensibles, afin que personne ne puisse les récupérer, ainsi que de décomposer l'espace libre de votre disque dur afin qu'il ne reste aucune trace non sécurisée de vos fichiers.

Grâce à ce logiciel, vous pouvez créer des paires de clés PGP et gérer à la fois vos paires de clés personnelles et les clés publiques de tiers.

Pour pouvoir utiliser PGP Desktop de façon optimale, vous devez vous familiariser avec les termes présentés dans la section *Terminologie afférente à PGP Desktop* (à la page 13). Vous devez également connaître la cryptographie conventionnelle et le chiffrement par clé publique, décrits dans la section *Cryptographie conventionnelle et chiffrement par clé publique* (à la page 16).

Contenu du chapitre

Nouveautés de PGP Desktop pour Windows version 10.0

Reposant sur la technologie éprouvée de PGP Corporation, PGP Desktop 10.0 pour Windows intègre de nombreuses améliorations, ainsi que des fonctions nouvellement développées ou corrigées.

Nouveautés de PGP Desktop version 10.0

Généralités

- **Prise en charge de nouveaux systèmes d'exploitation**. PGP Desktop pour Windows peut désormais être installé sous Windows 7.
- **Nouvelles versions localisées**. PGP Desktop a été localisé et peut maintenant être installé en français (France) et en espagnol (Amérique latine).
- **Prise en charge de nouvelles cartes à puce**. Pour le prédémarrage et le postdémarrage dans PGP Desktop pour Windows :
  - Carte à puce Axalto Cyberflex Access 32K V2
  - Cartes individuelles de vérification d'identité Giesecke and Devrient Sm@rtCafe Expert 3.2
  - Cartes individuelles de vérification d'identité Oberthur ID-One Cosmo V5.2D
  - Jeton USB SafeNet iKey 2032
  - Cartes T-Systems Telesec NetKey 3.0 et TCOS 3.0 IEI
- **Interface repensée**. La fenêtre principale de l'application utilisateur PGP Desktop pour Windows a été repensée.
- **Connectivité de PGP Universal Server**. Résilience accrue de PGP Desktop lorsque la connectivité à PGP Universal Server dépend d'une connexion de réseau privé virtuel ou est intermittente.

Clés PGP

- **Clés du mode clé de serveur (SKM) améliorées**. Les clés SKM incluent désormais toute la clé sur votre trousseau. En outre, vous pouvez également utiliser les clés SKM pour des fonctions de chiffrement, par exemple, le chiffrement et le déchiffrement du disque et des fichiers, ainsi que le déchiffrement de messages électroniques MAPI lorsque vous êtes déconnecté.
- **Emplacement du trousseau**. Dans PGP Desktop pour Windows, vous avez la possibilité d'utiliser les variables d'environnement pour indiquer l'emplacement de vos trousseaux.

- **Indicateurs d'utilisation des clés**. Chaque sous-clé possède désormais ses propres propriétés de clé. Ainsi, une sous-clé peut être utilisée uniquement pour PGP WDE et une autre, pour toutes les autres fonctions de PGP Desktop. Définissez l'utilisation d'une clé particulière lorsque vous souhaitez utiliser une clé uniquement pour le chiffrement du disque mais que vous ne souhaitez pas recevoir de message électronique chiffré utilisant cette clé.
- **Recherche de la clé USP (Universal Server Protocol)**. Le protocole des services de PGP Universal (USP) est un protocole SOAP qui fonctionne sur les ports HTTP/HTTPS standard. Il s'agit du mécanisme de recherche de clé par défaut. Si vous vous trouvez dans un environnement géré par un PGP Universal Server, toutes les demandes de recherche de clé, ainsi que les autres communications entre PGP Universal Server et PGP Desktop, utilisent le protocole PGP USP.

Messagerie PGP

- **Visionneuse PGP**. La visionneuse PGP vous permet de déchiffrer et d'afficher les messages IMAP/POP/SMTP hérités.
- **Lotus Notes**. PGP Desktop offre maintenant la possibilité de chiffrer les messages électroniques à l'aide du chiffrement natif Lotus Notes si PGP Desktop est configuré pour cela et que le destinataire est un utilisateur Notes interne.
- **Lotus Notes**. PGP Desktop offre désormais la possibilité de chiffrer des messages électroniques Lotus Notes RTF à l'aide des formats PGP/MIME, S/MIME ou PGP partitionné.
- **Lotus Notes**. Les annotations PGP dans les messages respectent les paramètres régionaux d'horodatage.
- **Boutons Microsoft Outlook supplémentaires**. Des boutons vous permettent d'ajouter un chiffrement et/ou votre signature numérique à vos messages Outlook. Cette nouvelle fonctionnalité permet de respecter les lois relatives à la signature numérique qui stipulent que l'intention de signer doit être claire.
- **Amélioration des stratégies hors connexion**. Dans un environnement géré, la stratégie relative aux messages électroniques et désormais appliquée même si vous êtes hors ligne et déconnecté de PGP Universal Server, ou si le serveur lui-même est hors ligne.

PGP Portable.

- Cette option précédemment autonome est maintenant incluse dans PGP Desktop. Il est possible de créer des disques PGP Portable sur les systèmes Windows. Cette fonctionnalité demande une licence distincte.

PGP Whole Disk Encryption

- **Compatibilité de cartes à puce supplémentaire**. Les nouvelles cartes à puce ajoutées pour l'authentification du prédémarrage dans PGP Whole Disk Encryption pour Windows sont les suivantes : Axalto Cyberflex Access 32K V2, , jeton USB Marx CrypToken, jeton USB SafeNet iKey 2032 et carte à puce T-Systems T-Telesec NetKey.
- **Prise en charge des cartes individuelles de vérification d'identité**. Prise en charge dans PGP Whole Disk Encryption pour Windows des cartes individuelles de vérification d'identité Giesecke and Devrient Sm@rtCafe Expert 3.2 et Oberthur ID-One Cosmo V5.2D.
- **Nouveaux claviers compatibles (Windows)** : 50 claviers internationaux peuvent être utilisés pour vous connecter à PGP BootGuard. Pour connaître les claviers compatibles, reportez-vous au guide de l'utilisateur de PGP Desktop pour Windows ou à l'aide en ligne.
- **Prise en charge intégrale du chiffrement de disque sous Linux**. PGP WDE pour Linux propose un chiffrement intégral de disque avec authentification de prédémarrage sous Ubuntu et Red Hat. Pour plus d'informations, reportez-vous au guide PGP Whole Disk Encryption pour Linux Command Line.
- **Autorécupération en local**. PGP Desktop pour Windows vous permet maintenant d'accéder à votre disque chiffré à partir de l'écran PGP BootGuard si vous avez oublié votre phrase secrète. Lorsque cette fonctionnalité est configurée, vous n'avez pas besoin de l'aide de votre administrateur.
- **Améliorations multi-utilisateurs**. Dans un environnement dans lequel plusieurs utilisateurs ont accès à un groupe d'ordinateurs, l'administrateur PGP Universal Server peut mettre en place un mot de passe administrateur PGP WDE. Lorsque vous entrez ce mot de passe dans l'écran PGP BootGuard sur un système PGP Desktop pour Windows, vous devez entrer votre phrase secrète Windows et le disque est déchiffré.
- **Amélioration du chiffrement forcé**. Lorsque l'administrateur PGP Universal Server change de stratégie et exige que tous les disques soient chiffrés, au téléchargement suivant de la stratégie sur votre système, l'assistant PGP WDE s'affiche et vous permet de lancer le chiffrement du disque.
- **Prise en charge supplémentaire des jetons pour PGP BootGuard**. Vous pouvez maintenant utiliser le jeton USB Marx CrypToken sur PGP BootGuard pour PGP Desktop pour Windows.
- **Prise en charge des caractères ASCII étendus**. Il est désormais possible d'utiliser les caractères ASCII étendus lors de la création d'utilisateurs PGP WDE.
- **Caractères Kanji**. Les caractères Kanji s'affichent maintenant correctement sur l'écran PGP BootGuard.

- **Systèmes d'exploitation Windows Server**. Vous pouvez désormais installer PGP WDE sur les systèmes d'exploitation Windows Server (Windows Server 2003 et Windows Server 2008). Pour plus d'informations sur la configuration système requise et sur les meilleures pratiques relatives à l'utilisation de PGP WDE sur les systèmes Windows Server, consultez l'*article 1737 de la base de connaissances de PGP* (http://support.pgp.com/?faq=1737).

Utilisation de ce manuel

Le présent manuel comporte des informations concernant la configuration et l'utilisation des composants de PGP Desktop. Chaque chapitre est consacré à un composant particulier.

Utilisateurs gérés/non gérés

Il est possible d'avoir recours à un PGP Universal Server afin de contrôler les stratégies et les paramètres employés par les composants de PGP Desktop. Les entreprises disposant du logiciel PGP optent souvent pour cette solution. Les utilisateurs de PGP Desktop choisissant cette configuration sont appelés des utilisateurs *gérés*, car les paramètres et stratégies disponibles dans leur application PGP Desktop sont prédéfinis par un administrateur PGP et gérés par le biais d'un PGP Universal Server. Si vous travaillez dans un environnement géré, il se peut que votre entreprise ait mis en place des conditions d'utilisation spécifiques. Par exemple, les utilisateurs gérés peuvent ou non être autorisés à envoyer des messages au format texte brut, ou bien être obligés de chiffrer leur disque avec PGP Whole Disk Encryption.

Les utilisateurs non soumis au contrôle d'un PGP Universal Server sont dits *non gérés* ou *autonomes*.

Ce document explique le fonctionnement de PGP Desktop dans les deux cas mentionnés ; cependant, il peut arriver que certains des paramètres qui y sont décrits ne soient pas disponibles pour les utilisateurs gérés dans leur environnement. Pour plus d'informations, reportez-vous à la section *Utilisation de PGP Desktop avec un PGP Universal Server* (à la page 341).

Remarque : les références aux environnements gérés avec un PGP Universal Server ne concernent pas les produits PGP Virtual Disk et PGP Virtual Disk Professional.

Fonctionnalités personnalisées par l'administrateur de PGP Universal Server

Si vous utilisez PGP Desktop en tant qu'utilisateur « géré » dans un environnement géré par un PGP Universal Server, certains paramètres peuvent être spécifiés par votre administrateur. Ces paramètres peuvent changer la façon dont les fonctionnalités s'affichent dans PGP Desktop.

- **Fonctionnalités désactivées** : l'administrateur de PGP Universal Server peut activer ou désactiver des fonctionnalités spécifiques. Par exemple, il peut empêcher la création d'archives PGP Zip ou celle de dossiers protégés PGP NEtShare (sous Windows).

  Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas et le menu de cette fonctionnalité n'est pas disponible. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Votre interface de PGP Desktop peut être différente si votre administrateur a personnalisé les fonctionnalités disponibles.

- **BootGuard personnalisé**. Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, l'administrateur PGP peut avoir personnalisé l'écran PGP Whole Disk Encryption BootGuard pour inclure du texte supplémentaire ou une image personnalisée, telle que le logo de votre entreprise. Les graphiques inclus dans ce guide illustrent l'installation par défaut. Votre écran d'ouverture de session peut être différent si l'administrateur l'a personnalisé.

Conventions employées dans ce manuel

Les mentions Remarque, Attention et Avertissement sont utilisées comme suit.

Remarque : les remarques sont des informations complémentaires, mais essentielles. Elles visent à attirer votre attention sur des aspects importants du produit. Lisez-les pour pouvoir exploiter le produit au mieux.

Attention : les mentions Attention signalent la possibilité d'une perte de données ou d'une violation mineure de la sécurité. Elles vous indiquent une situation dans laquelle des problèmes peuvent survenir si aucune mesure n'est prise. Vous devez y prendre garde.

Avertissement : les avertissements signalent la possibilité d'une perte de données conséquente ou d'une violation majeure de la sécurité. Ils font état de l'apparition de graves problèmes en l'absence d'action appropriée. Prenez-les très au sérieux.

À qui est destiné ce document

Ce document est destiné à toute personne utilisant le logiciel PGP Desktop pour Windows pour protéger ses données.

Remarque : Si vous êtes novice dans le domaine de la cryptographie, pour connaître la terminologie et les concepts utilisés dans PGP Desktop, consultez le document intitulé *Introduction à la cryptographie*, qui a été installé sur votre ordinateur lors de l'installation de PGP Desktop.

À propos des licences PGP Desktop

Une licence est octroyée aux utilisateurs du logiciel PGP pour leur permettre d'exploiter ses fonctionnalités ; elle définit par ailleurs la date d'expiration du logiciel. Selon le type de licence dont vous disposez, une partie ou l'intégralité des applications de la gamme PGP Desktop est active. Une fois que vous avez saisi votre numéro de licence, vous devez procéder à l'enregistrement de votre logiciel auprès de PGP Corporation, manuellement ou en ligne.

Il existe trois types de licences :

- **Évaluation** : ce type de licence est limité dans le temps et n'inclut probablement pas toute la fonctionnalité de PGP Desktop.
- **Abonnement** : ce type de licence est en général valable pour une durée d'abonnement d'un an. Au cours de la durée d'abonnement, vous recevez la version en cours du logiciel PGP, ainsi que toutes les mises à niveau et mises à jour publiées au cours de cette période.
- **Définitive** : ce type de licence vous permet d'utiliser PGP Desktop indéfiniment. Avec la police d'assurance annuelle, qui doit être renouvelée tous les ans, vous recevez toutes les mises à jour et mises à niveau publiées durant la période d'application de la police.

Gestion des licences de PGP Desktop pour Windows

Pour définir une licence pour PGP Desktop Effectuez l'une des opérations suivantes :

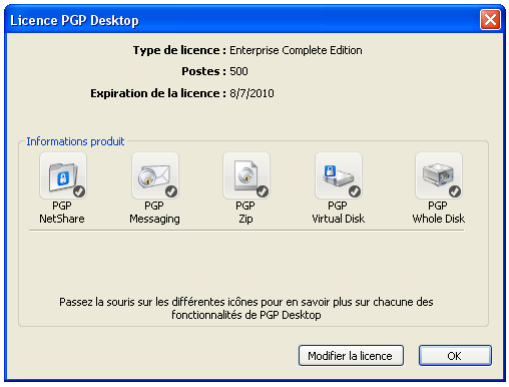
- Si vous êtes un utilisateur géré, vous utilisez probablement déjà une copie sous licence de PGP Desktop. Reportez-vous à la section *Consultation des détails de la licence* (à la page 7) pour consulter les détails de votre licence. Si vous avez des questions, contactez votre administrateur PGP.
- Si vous êtes un utilisateur non géré ou un administrateur PGP, reportez-vous à la section *Consultation des détails de la licence* (à la page 7) pour consulter les détails de votre licence. Si vous devez enregistrer votre copie de PGP Desktop, suivez la procédure décrite dans la section *Enregistrement de PGP Desktop pour Windows* (à la page 8).

Consultation des détails de la licence

Pour afficher les détails de votre licence PGP Desktop

1 Dans la zone de notification, double-cliquez sur l'icône PGP Desktop.

2 Sélectionnez **Aide > Licence**. La boîte de dialogue contenant la licence PGP Desktop apparaît.



Elle indique les détails suivants :

Élément	Description
Type de licence	Nom du produit sous licence.
Postes	Nombre de postes sur lesquels peut être installée la licence.
Expiration de la licence	Date d'expiration de la licence.
Informations produit	Composants actifs en fonction de la licence. Positionnez le curseur sur le nom du produit pour afficher des informations sur celui-ci et savoir si vous disposez d'une licence vous permettant de l'utiliser.

Remarque : si vous n'autorisez pas votre copie de PGP Desktop, vous n'aurez accès qu'à quelques fonctionnalités limitées (PGP Zip et Clés).

Enregistrement de PGP Desktop pour Windows

Si vous devez changer de numéro de licence ou si vous n'avez pas procédé à l'autorisation de la licence au moment de la configuration du logiciel, suivez les instructions ci-dessous pour enregistrer votre produit.

Remarque : assurez-vous que votre connexion Internet est active avant de continuer. Si vous ne disposez pas d'un accès à Internet, il vous faut soumettre une demande d'autorisation manuelle.

Avant de commencer

Si vous avez acheté PGP Desktop, vous avez dû recevoir un message de confirmation de commande avec un fichier .PDF joint.

1. Notez le nom, la société et le numéro de licence qui y figurent. Vous les trouverez dans la section intitulée **Important Note** (Note importante) du fichier .PDF. Vous aurez besoin de ces informations au cours du processus de définition de la licence.

   Lors de la configuration du logiciel PGP Desktop, saisissez le nom, la société, l'adresse de courrier électronique et le numéro de licence pour enregistrer votre copie de PGP Desktop sur le serveur d'autorisation de PGP Corporation.

   Remarque : le numéro de licence figure également dans la page de téléchargement du produit PGP.

   Dans la zone de notification, double-cliquez sur l'icône PGP Desktop.

2. Sélectionnez **Aide** > **Licence**. La boîte de dialogue contenant la licence PGP Desktop apparaît.
3. Cliquez sur **Modifier la licence**. La boîte de dialogue Assistant de gestion des licences PGP s'affiche.
4. Dans les champs prévus à cet effet, indiquez le **nom** et la **société** exactement tels qu'ils apparaissent dans le fichier .PDF joint au message de confirmation de commande du produit PGP. Vous les trouverez dans la section intitulée **Important Note** (Note importante) du fichier .PDF. Si ce dernier ne comporte pas de section avec ce nom**, le nom et la société entrés lors de la première tentative d'autorisation seront utilisés de manière permanente.**
5. Saisissez l'adresse de courrier électronique à associer à la licence du produit.
6. Tapez-la une seconde fois pour confirmation.

   Remarque : si vous avez déjà autorisé ce numéro de licence, vous devez entrer le nom, la société et l'adresse de courrier électronique que vous aviez fournis la fois précédente. Si vous indiquez des informations différentes, le processus d'autorisation n'aboutira pas.

7. Cliquez sur **Suivant**.
8. Effectuez l'une des opérations suivantes :

   - Tapez votre numéro de licence à 28 caractères dans les champs correspondants (par exemple, DEMO1-DEMO2-DEMO3-DEMO4-DEMO5-ABC).

   Remarque : pour éviter des erreurs de saisie et faciliter le processus d'autorisation, copiez intégralement le numéro de licence, placez le curseur dans le premier champ Numéro de licence, puis collez le contenu du Presse-papiers. Le numéro sera alors automatiquement inclus dans les six champs Numéro de licence.

- Pour demander une version d'évaluation unique, valable 30 jours, de PGP Desktop, sélectionnez **Demander un essai unique de 30 jours de PGP Desktop**. Lorsque vous achetez une licence, vous pouvez entrer son numéro à tout moment jusqu'à la fin de la période d'évaluation de 30 jours. Si vous n'indiquez pas de licence valide, PGP Desktop rétablira le mode sans licence à l'issue des 30 jours.
- Pour acheter une licence de PGP Desktop, choisissez **Acheter un numéro de licence maintenant**. La page Web du magasin PGP Store en ligne s'ouvre dans votre navigateur.
- Pour utiliser PGP Desktop sans licence, sélectionnez **Utiliser sans licence et désactiver la plupart des fonctionnalités**. Les seules fonctions de PGP Desktop que vous pouvez utiliser sans licence sont PGP Zip et les clés PGP.

9 Cliquez sur **Suivant** pour procéder à l'autorisation.

10 Une fois que le produit PGP a été autorisé, les fonctions activées par la licence sont affichées. Cliquez sur **Suivant**, puis sur **Terminer** pour achever la procédure.

Résolution des erreurs d'autorisation de licence

Si vous recevez un message d'erreur durant le processus d'enregistrement du logiciel, suivez la procédure de dépannage adéquate. Reportez-vous à la section *HOWTO: License PGP Desktop 9.x* **(Procédure : autorisation de licence pour PGP Desktop 9.x)** du *portail du support de PGP* (https://support.pgp.com) pour obtenir des suggestions.

Si votre licence est arrivée à expiration

Si votre licence de PGP Desktop est arrivée à expiration, vous recevez un message Expiration de la licence PGP lorsque vous lancez PGP Desktop. Consultez les sections suivantes pour obtenir des informations sur la façon dont une licence arrivée à expiration affecte le fonctionnement de PGP Desktop.

PGP Desktop Email

- Les messages électroniques sortants ne sont plus envoyés sous forme chiffrée.

PGP NetShare

- Les dossiers protégés PGP NetShare sont accessibles, bien que les fichiers protégés restent chiffrés. (Pour afficher les fichiers chiffrés, déchiffrez manuellement les dossiers et fichiers.)
- Il n'est plus possible de créer des dossiers protégés PGP NetShare.

- Les fichiers placés dans un dossier protégé ne sont pas chiffrés.
- Il n'est plus possible d'ajouter des clés dans un dossier protégé PGP NetShare ou d'en retirer.

PGP Virtual Disk

- Les PGP Virtual Disks sont toujours accessibles en mode lecture seule. Ce mode permet de copier des données à partir d'un PGP Virtual Disk, mais pas d'en copier vers un PGP Virtual Disk.

PGP Whole Disk Encryption

- Tous les disques fixes qui ont été chiffrés avec PGP Desktop sont automatiquement déchiffrés 90 jours après la date d'expiration de la licence.

Assistance

Pour accéder à des ressources supplémentaires, consultez les sections ci-dessous.

Obtention d'informations sur le produit

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).

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).

2 Présentation de base de PGP Desktop

Cette section décrit la terminologie afférente à PGP Desktop et apporte quelques données conceptuelles de haut niveau en matière de cryptographie.

Contenu du chapitre

Terminologie afférente à PGP Desktop

Pour utiliser pleinement PGP Desktop, vous devez vous familiariser avec les termes des sections suivantes.

Composants du produit PGP

PGP Desktop et ses composants sont décrits dans la liste qui suit. Il est possible que vous ne disposiez pas de toutes les fonctionnalités du produit ; cela dépend de votre licence. Pour plus d'informations, reportez-vous à la section *À propos des licences PGP Desktop* (cf. "Gestion des licences de PGP Desktop pour Windows" à la page 7).

- **PGP Desktop** : logiciel utilisant la cryptographie pour empêcher les accès non autorisés à vos données. PGP Desktop est disponible en versions Mac OS X et Windows.
  - **Messagerie PGP** : fonction de PGP Desktop qui prend en charge tous vos clients de messagerie, de façon automatique et transparente, par le biais de stratégies que vous pouvez contrôler. Pour ce faire, PGP Desktop a recours à une nouvelle technologie de proxy (l'ancienne technologie avec plug-in demeure disponible). Le service de messagerie PGP permet en outre de protéger plusieurs clients de messagerie instantanée, tels qu'AIM et iChat (sous réserve que les utilisateurs aient activé ce service).

- **PGP Whole Disk Encryption** : Whole Disk Encryption est une fonction de PGP Desktop qui vous permet de chiffrer votre disque dur complet ou seulement une partition (sous Windows), y compris l'enregistrement d'amorçage, garantissant ainsi la protection de tous les fichiers que vous n'utilisez pas. Vous pouvez combiner, sur un même système, des volumes PGP Whole Disk Encryption et PGP Virtual Disk. Pour une sécurité améliorée sur les systèmes Windows, vous avez la possibilité de protéger les lecteurs chiffrés du disque à l'aide d'une phrase secrète ou d'une paire de clés sur un jeton USB.
- **PGP NetShare** : fonction de PGP Desktop pour Windows grâce à laquelle vous pouvez paramétrer le partage de fichiers et de dossiers entre plusieurs utilisateurs de votre choix, et ce en toute sécurité et transparence. Les utilisateurs de PGP NetShare peuvent protéger leurs fichiers et dossiers simplement en les plaçant dans un dossier de protection spécial.
- **Clés PGP** : fonction de PGP Desktop offrant un contrôle total aussi bien de vos propres clés PGP que de celles des personnes avec lesquelles vous échangez des messages électroniques sécurisés.
- **Volumes PGP Virtual Disk** : les volumes PGP Virtual Disk représentent une fonction de PGP Desktop qui vous permet d'utiliser une partie de l'espace disponible sur votre disque dur en tant que disque virtuel chiffré. Vous pouvez protéger un volume PGP Virtual Disk avec une clé ou une phrase secrète. Vous pouvez même créer des utilisateurs supplémentaires pour un volume, de sorte que celui-ci puisse aussi être utilisé par les personnes auxquelles vous le permettez. La fonction PGP Virtual Disk est particulièrement utile sur les ordinateurs portables, puisque, si vous perdez votre ordinateur ou vous le faites dérober, les données sensibles stockées sur le volume PGP Virtual Disk sont protégées contre les accès non autorisés.
- **PGP Shred** : fonction de PGP Desktop vous permettant de supprimer en toute sécurité des données de votre système. PGP Shred remplace les fichiers ; ainsi, ceux-ci ne peuvent pas être récupérés, même à l'aide d'un logiciel de récupération de fichiers.
- **Visionneuse PGP** : la Visionneuse PGP vous permet de déchiffrer, de vérifier et d'afficher les messages *en dehors* du flux de messagerie.
- **PGP Zip** : fonction de PGP Desktop grâce à laquelle vous pouvez regrouper différents fichiers et dossiers dans un module compressé chiffré unique qui pourra facilement être transporté ou sauvegardé. Vous pouvez chiffrer une archive PGP Zip avec une clé PGP ou une phrase secrète.

- **PGP Universal** : outil destiné aux entreprises souhaitant sécuriser le système de messagerie utilisé par leurs employés, de façon automatique et transparente. Si vous utilisez PGP Desktop 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.

- **PGP Global Directory** : serveur de clés publiques d'accès gratuit hébergé par PGP Corporation. Ce serveur fournit un accès rapide et simple à l'univers des clés PGP. Il fait appel à une technologie de serveur de clés d'avant-garde, qui permet de rechercher l'adresse de courrier électronique dans une clé (afin de vérifier que son propriétaire veut effectivement publier la clé qu'il détient) et d'offrir aux utilisateurs la possibilité de gérer leurs propres clés. Si vous avez recours au serveur PGP Global Directory, vous avez de plus grandes chances de trouver une clé publique valide pour le destinataire de vos messages sécurisés. PGP Desktop s'intègre parfaitement dans l'environnement de ce serveur.

Terminologie utilisée dans PGP Desktop

Avant de commencer à utiliser PGP Desktop, il est conseillé de vous familiariser avec les termes suivants :

- **Déchiffrement :** processus consistant à transformer des données chiffrées (brouillées) en données à nouveau compréhensibles. Lorsque vous recevez des données qui ont été chiffrées par un tiers à l'aide de votre clé publique, servez-vous de votre clé privée pour les déchiffrer.
- **Chiffrement :** processus de brouillage de données visant à éviter que les personnes non autorisées qui ont pu accéder auxdites données ne puissent les exploiter. Les données sont tellement brouillées qu'elles n'ont pas de sens.
- **Signature :** processus consistant à appliquer une signature numérique aux données en utilisant votre clé privée. Dans la mesure où les données signées à l'aide de votre clé privée peuvent uniquement être vérifiées à l'aide de votre clé publique, la faculté d'effectuer cette opération est la preuve que vous avez utilisé votre clé privée pour signer les données et, par conséquent, vous identifie en tant qu'expéditeur de ces dernières.
- **Vérification :** processus permettant de démontrer, grâce à l'utilisation de la clé publique de la personne concernée, que sa clé privée a servi à appliquer une signature numérique aux données. Les données signées à l'aide d'une clé privée peuvent uniquement être vérifiées avec la clé publique correspondante, c'est pourquoi, s'il est possible de vérifier des données signées avec une clé publique spécifique, cela implique que le signataire est le détenteur de la clé privée associée.
- **Paire de clés :** combinaison de clé privée et de clé publique. Lorsque vous créez une « clé » PGP, vous générez en fait une paire de clés. Votre paire de clés comporte, hormis vos clés privée et publique, votre nom et votre adresse de courrier électronique, et s'assimile donc davantage à un ID numérique (permettant de vous identifier dans le monde numérique tout comme votre permis de conduire ou votre passeport permettent de vous identifier dans le monde réel).

- **Clé privée :** clé totalement confidentielle. Votre clé privée représente le seul moyen de déchiffrer les données qui ont été chiffrées avec votre clé publique. De même, elle seule permet de créer une signature numérique pouvant être vérifiée à l'aide de votre clé publique.

  Attention : ne communiquez à personne votre clé privée ou la phrase secrète rattachée ! Et conservez votre clé privée en lieu sûr.

- **Clé publique :** clé que vous distribuez aux tiers pour qu'ils puissent vous envoyer des messages sécurisés (pouvant être déchiffrés uniquement par votre clé privée) et vérifier votre signature numérique. Les clés publiques peuvent être largement distribuées.

  Vos clés publique et privée sont liées par une relation mathématique, mais quelqu'un disposant de votre clé publique n'a aucunement la possibilité de découvrir votre clé privée.

- **Serveur de clés :** référentiel de clés. Certaines entreprises hébergent des serveurs de clés stockant les clés publiques de leurs employés, pour permettre à d'autres employés de trouver ces clés et d'envoyer des messages sécurisés à ces derniers. Le serveur *PGP Global Directory* (https://keyserver.pgp.com) est un serveur de clés d'accès gratuit et public, hébergé par PGP Corporation.

- **Cartes à puce et jetons :** les cartes à puce et les jetons sont des dispositifs mobiles sur lesquels vous pouvez créer ou copier votre paire de clés PGP. En créant votre paire de clés PGP sur une carte à puce ou un jeton, vous améliorez la sécurité du processus, puisque toute personne souhaitant chiffrer, signer, déchiffrer ou vérifier des données doit posséder cette carte ou ce jeton. De cette manière, même si une personne non autorisée parvient à accéder à votre ordinateur, vos données chiffrées demeurent protégées, car la carte à puce ou le jeton contenant votre paire de clés PGP ne vous a pas quitté. Par ailleurs, si vous copiez votre paire de clés PGP sur une carte à puce ou un jeton, cela vous permet de l'utiliser en dehors de votre système principal, de la sauvegarder et de distribuer votre clé publique. Les cartes à puce et les jetons ne sont pas disponibles pour le stockage de clé lorsqu'ils sont utilisés avec PGP Desktop pour Mac OS X.

Cryptographie conventionnelle et chiffrement par clé publique

La **cryptographie conventionnelle** utilise la même phrase secrète pour chiffrer et déchiffrer les données. Elle est parfaite pour les données qui ne se déplacent pas, en raison de sa rapidité. Cependant, elle n'est pas adaptée à l'envoi de données chiffrées à un tiers, en particulier s'il s'agit d'une personne que vous ne connaissez pas.

Le **chiffrement par clé publique** utilise deux clés (ou paire de clés) pour le chiffrement et le déchiffrement. L'une de ces deux clés est votre clé privée. Comme son nom l'indique, cette clé doit rester privée. Totalement privée. La deuxième clé est votre clé publique. Contrairement à l'autre, vous pouvez la partager avec des tiers. En réalité, ce partage est indispensable.

Le chiffrement par clé publique fonctionne de la façon suivante : supposons que vous souhaitiez échanger des messages privés avec votre cousine qui vit dans une autre ville que vous. Vous possédez tous les deux PGP Desktop. Pour commencer, vous devez tous deux créer votre paire de clés : une clé privée et une clé publique. Vous gardez votre clé privée secrète et vous envoyez votre clé publique à un serveur de clés publiques tel que le PGP Global Directory (keyserver.pgp.com), service public de distribution de clés publiques. (Certaines entreprises possèdent leurs propres serveurs de clés privées.)

Une fois les clés publiques créées dans le serveur de clés, vous pouvez accéder à ce serveur et récupérer la clé publique de votre cousine, tandis que celle-ci peut faire la même chose de son côté. (Il existe d'autres façons d'échanger des clés publiques ; pour plus d'informations, reportez-vous à la section *Utilisation des clés PGP* (à la page 43).) Ceci est important car pour envoyer un message électronique chiffré que seule votre cousine peut déchiffrer, vous devez utiliser la clé publique de votre cousine. Le système fonctionne en ce sens que seule la clé privée de votre cousine peut déchiffrer un message chiffré à l'aide de sa clé publique. Même vous, qui disposez de sa clé publique, ne pouvez déchiffrer le message une fois qu'il a été chiffré avec cette dernière. **La clé privée représente le seul moyen de déchiffrer les données qui ont été chiffrées avec la clé publique correspondante.**

Vos clés publique et privée sont liées par une relation mathématique, mais il n'est pas possible de découvrir la clé privée de quelqu'un en possédant sa clé publique.

Pour en savoir plus à propos de la cryptographie

Pour plus d'informations sur la cryptographie, reportez-vous au document *Introduction à la cryptographie*, installé sur votre système en même temps que PGP Desktop. Vous pouvez y accéder depuis le menu Démarrer.

Première utilisation de PGP Desktop

PGP Corporation recommande de suivre la procédure ci-dessous lorsque vous utilisez PGP Desktop pour la première fois :

1 **Installez PGP Desktop sur votre ordinateur.**

Si vous prévoyez d'utiliser le logiciel dans le cadre de votre travail, votre administrateur PGP a peut-être fourni des instructions d'installation spécifiques ou prédéfini certains paramètres dans le programme d'installation de PGP. Quoi qu'il en soit, cette première étape est indispensable.

2 Laissez-vous guider par l'assistant d'installation.

Cet assistant apparaît une fois que vous avez installé PGP Desktop et redémarré l'ordinateur. Il vous aide à effectuer les opérations suivantes :

- Définition d'une licence pour PGP Desktop
- Création d'une paire de clés (avec ou sans sous-clés) si vous n'en possédez pas encore
- Publication de votre clé publique sur le serveur PGP Global Directory
- Activation de la messagerie PGP
- Consultation rapide des autres fonctions disponibles

Si le programme d'installation de PGP Desktop a été configuré par un administrateur PGP, il se peut que vous puissiez exécuter d'autres tâches par l'intermédiaire de l'assistant d'installation.

3 Procédez à des échanges de clés publiques.

Une fois que vous avez créé une paire de clés, vous pouvez commencer à envoyer des messages sécurisés à d'autres utilisateurs de PGP Desktop et à recevoir les leurs (vous devez avoir échangé au préalable vos clés publiques respectives). Vous pouvez également avoir recours aux fonctions de protection de disque de PGP Desktop.

L'échange de clés publiques est une étape cruciale. Pour pouvoir envoyer un message sécurisé à un destinataire, vous devez disposer d'une copie de sa clé publique. De même, pour que le destinataire soit en mesure de vous renvoyer lui aussi un message sécurisé, il doit disposer d'une copie de votre clé publique. Si vous n'avez pas chargé celle-ci sur le serveur PGP Global Directory via l'assistant d'installation, faites-le maintenant. Si vous ne possédez pas la clé publique des personnes auxquelles vous voulez envoyer des messages, commencez par la rechercher sur le serveur PGP Global Directory. PGP Desktop effectue cette opération pour vous (lorsque vous envoyez un message, il recherche et vérifie automatiquement les clés des autres utilisateurs du produit). Il chiffre ensuite votre message à l'aide de la clé publique du destinataire et le lui envoie.

4 Procédez à la validation des clés publiques provenant de serveurs de clés non approuvés.

Lorsque vous recevez une clé publique en provenance d'un serveur de clés non approuvé, vérifiez dans la mesure du possible que celle-ci n'a pas été falsifiée et appartient véritablement à la personne désignée. Pour cela, comparez, à l'aide de PGP Desktop, l'empreinte unique figurant sur votre copie de la clé publique de cette personne et celle figurant sur la clé d'origine (vous pouvez par exemple téléphoner au propriétaire de la clé et lui demander de vous lire les données de l'empreinte). Les clés provenant de serveurs de clés approuvés, comme le serveur PGP Global Directory, ont déjà été vérifiées.

5 **Commencez à sécuriser votre courrier électronique, vos fichiers et vos sessions de messagerie instantanée.**

Après avoir généré votre paire de clés et procédé à un échange de clés publiques, vous pouvez commencer à chiffrer, déchiffrer, signer et vérifier les messages électroniques et les fichiers. La fonction de session de messagerie instantanée sécurisée génère automatiquement ses propres clés ; par conséquent, vous pouvez l'employer avant même d'avoir créé votre paire de clés. La seule condition pour que la session soit sécurisée est que vous dialoguiez avec une personne qui utilise également PGP Desktop.

6 **Lisez les notes informatives de la fonction de notification de PGP Desktop qui s'affichent**.

Lors de l'envoi ou de la réception de messages, ou de l'exécution d'une autre fonction PGP Desktop, la fonction de notification affiche des notes informatives, dans le coin de l'écran de votre choix. Ces notes vous indiquent l'opération que PGP Desktop a effectuée ou va effectuer. Une fois que vous avez pris l'habitude d'envoyer et de recevoir des messages, vous pouvez modifier les options associées à la fonction de notification de PGP ou désactiver celle-ci.

7 **Après l'envoi ou la réception de messages, consultez les journaux pour vous assurer que le fonctionnement est normal.**

Si vous souhaitez obtenir d'autres informations que celles fournies par la fonction de notification, reportez-vous au journal de PGP ; vous y trouverez des détails concernant l'ensemble des opérations de messagerie.

8 **Au besoin, modifiez vos stratégies de messagerie.**

Si ces stratégies sont correctement configurées dans PGP Desktop, les messages électroniques sont envoyés et reçus automatiquement, en toute transparence. Si le destinataire de votre message possède une clé stockée sur le serveur PGP Global Directory, les stratégies PGP Desktop par défaut procurent un chiffrement *opportuniste*. Ce type de chiffrement implique que, si PGP Desktop dispose de tous les éléments requis (tels que la clé publique **vérifiée** du destinataire) pour chiffrer le message de manière automatique, il le fait. Dans le cas contraire, il envoie le message sous forme de *texte en clair* (non chiffré). Les stratégies PGP Desktop par défaut fournissent en outre un chiffrement *forcé* en option. En d'autres termes, si vous incluez le texte « [PGP] » dans la ligne d'objet d'un message, ce message **doit** être envoyé de façon sécurisée. Si aucune clé vérifiée ne peut être trouvée, il n'est pas envoyé et une note informative s'affiche.

9 Commencez à utiliser les autres fonctions de PGP Desktop.

Parallèlement aux fonctions de messagerie, PGP Desktop propose des fonctions permettant de sécuriser vos disques de travail :

- Vous pouvez utiliser **PGP Whole Disk Encryption** pour chiffrer un disque de démarrage, une partition de disque (sur les systèmes Windows), un disque externe ou une clé USB. Tous les fichiers se trouvant sur le disque ou dans la partition sont alors sécurisés, puisqu'ils sont chiffrés et déchiffrés « à la volée » à chacune de leurs utilisations. Pour vous, le processus est totalement transparent.
- **PGP Virtual Disk** permet de créer un « disque dur virtuel » sécurisé. Ce disque dur virtuel agit comme une chambre forte pour vos fichiers. Pour le démonter et le verrouiller, servez-vous de PGP Desktop ou de l'Explorateur Windows (ou bien du Finder sous Mac OS X). Vos fichiers seront ainsi sécurisés, et ce même si le reste de votre ordinateur est déverrouillé.
- Vous pouvez utiliser **PGP Zip** pour créer des archives PGP Zip compressées et chiffrées. Celles-ci constituent un bon mode de transport ou de stockage sécurisé de fichiers.
- Vous pouvez utiliser **PGP Shredder** pour supprimer des fichiers sensibles devenus superflus. Cette fonction a pour effet de supprimer définitivement les fichiers, qui seront irrémédiablement perdus.
- Utilisez **PGP NetShare** pour partager des fichiers et des dossiers en toute sécurité et simplicité avec le nombre de personnes de votre choix, tout en disposant d'un contrôle d'accès maximal.

3 Installation de PGP Desktop

Cette section décrit la procédure d'installation de PGP Desktop sur votre ordinateur et vous explique comment commencer à utiliser le logiciel.

Contenu du chapitre

Conditions requises pour l'installation

Vous trouverez dans cette section la configuration système minimale requise pour l'installation de PGP Desktop sur un ordinateur Windows.

Configuration requise

Avant de procéder à l'installation, vérifiez que vous disposez de la configuration système minimale suivante :

- Microsoft Windows 2000 (Service Pack 4),

  Remarque : les systèmes d'exploitation ci-dessus sont pris en charge uniquement lorsque tous les correctifs logiciels et de sécurité les plus récents fournis par Microsoft ont été appliqués.

  PGP Whole Disk Encryption (WDE) est pris en charge sur toutes les versions client ci-dessus, ainsi que sur les versions de Windows Server suivantes :

  - Windows Server 2003 SP 2 (éditions 32 et 64 bits)
  - Windows Server 2008 SP 1 et 2 (éditions 32 et 64 bits)
  - Windows Server 2008 R2 (éditions 32 et 64 bits)

Pour plus d'informations sur la configuration système requise et sur les meilleures pratiques relatives à l'utilisation de PGP WDE sur les systèmes Windows Server, consultez l'*article 1737 de la base de connaissances de PGP* (http://support.pgp.com/?faq=1737).

- 512 Mo de RAM
- 64 Mo d'espace disque dur

Pour obtenir des informations sur les logiciels de messagerie, de messagerie instantanée et anti-virus pris en charge, consultez les *notes de publication PGP Desktop10.0 pour Windows*.

Compatibilité avec Citrix et les services de terminal

PGP Desktop pour Windows a été testé avec les services de terminal suivants :

- Citrix Presentation Server 4.0
- Citrix Metaframe XP
- les services Terminal Server Windows 2003.

Dans ces environnements sont disponibles les fonctions de PGP Desktop pour Windows ci-après :

- Le chiffrement des messages électroniques est totalement pris en charge.
- La fonctionnalité PGP Zip est totalement prise en charge.
- La fonctionnalité PGP Shred est totalement prise en charge.
- PGP NetShare est totalement pris en charge.
- Les disques PGP Virtual Disk ne peuvent pas être montés au niveau d'une lettre de lecteur sur Citrix/TS, mais peuvent l'être au niveau de points de montage de répertoire sur des volumes NTFS.
- PGP Whole Disk Encryption n'est pas pris en charge.
- Les cartes à puce ne sont pas compatibles.

Pour obtenir des informations relatives à l'installation de PGP Desktop sur un serveur Citrix, consultez l'*article 832 de la base de connaissances du support de PGP* (https://support.pgp.com/?faq=832).

Installation et configuration de PGP Desktop

Cette section comprend des informations relatives à l'installation ou la mise à niveau de PGP Desktop, et à l'assistant d'installation.

Installation du logiciel

Remarque : pour pouvoir installer PGP Desktop, vous devez disposer des droits d'administration sur votre système.

Pour installer PGP Desktop sur votre système Windows

1. Localisez le programme d'installation de PGP Desktop. Il se présente sous la forme d'un fichier .MSI, que votre administrateur PGP peut vous avoir transmis par le biais de l'outil Déploiement SMS de Microsoft.
2. Double-cliquez sur le fichier exécutable du programme d'installation de PGP Desktop.
3. Suivez les instructions affichées à l'écran.
4. 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 et/ou paramètres du programme d'installation de PGP Desktop. En outre, si votre administrateur PGP a configuré une inscription silencieuse, vous devez entrer votre mot de passe de domaine Windows chaque fois que votre phrase secrète est requise dans PGP Desktop. Si la stratégie le spécifie, PGP Whole Disk Encryption peut démarrer automatiquement pour chiffrer votre disque lorsque vous entrez votre mot de passe Windows.

Mise à niveau du logiciel

Remarque : PGP Desktop pour Windows et PGP Universal Satellite pour Windows ne peuvent pas être installés conjointement sur un même système. Les programmes d'installation de ces deux produits sont capables de détecter la présence de l'autre programme et, si ce dernier est déjà installé, le processus est interrompu.

Vous pouvez mettre à niveau une version antérieure des produits ci-après vers PGP Desktop pour Windows :

- PGP Desktop pour Windows
- PGP Universal Satellite pour Windows

Si le système d'exploitation de votre ordinateur est Microsoft Windows XP, vous pouvez uniquement mettre à niveau PGP Desktop 8.x vers PGP Desktop 9.6 ou une version ultérieure. Si votre système d'exploitation est Microsoft Windows 2000, les mises à niveau des versions 6.x, 7.x et 8.x de PGP Desktop sont possibles.

Remarque importante : si vous mettez votre ordinateur à niveau vers une nouvelle version du système d'exploitation et souhaitez utiliser cette version de PGP Desktop, veillez à désinstaller les versions précédentes avant d'effectuer la mise à niveau du système d'exploitation et l'installation de PGP Desktop. Pensez à sauvegarder vos clés et vos trousseaux de clés avant la désinstallation. Et n'oubliez pas que, si vous avez utilisé PGP Whole Disk Encryption, vous devrez déchiffrer le contenu de votre disque pour pouvoir désinstaller PGP Desktop.

Mise à niveau de PGP Desktop

Effectuez l'une des opérations suivantes :

- **À partir de PGP Desktop 8.x pour Windows :** suivez la procédure d'installation standard pour PGP Desktop 10.0 pour Windows.

  PGP Desktop 8.x pour Windows est automatiquement désinstallé et PGP Desktop 10.0 pour Windows est installé. Les trousseaux de clés et fichiers PGP Virtual Disk existants peuvent être utilisés dans la version plus récente.

- **À partir d'une version de PGP Desktop pour Windows** *antérieure* **à la version 8.0 :** si vous disposez d'une version de PGP Desktop antérieure à la version 8.0, désinstallez-la manuellement avant de commencer l'installation de PGP Desktop 10.0 pour Windows. Les trousseaux de clés et fichiers PGP Virtual Disk existants peuvent être utilisés dans la version plus récente.

Mise à niveau à partir de PGP Universal Satellite

Effectuez l'une des opérations suivantes :

- **À partir de PGP Universal Satellite 1.2 pour Windows (ou d'une version antérieure) :** suivez la procédure d'installation pour PGP Desktop 10.0 pour Windows.

  Les versions existantes de PGP Universal Satellite pour Windows sont automatiquement désinstallées et PGP Desktop 10.0 pour Windows est installé. Les anciens paramètres sont conservés.

  Attention : il est impossible d'installer une version de PGP Universal Satellite conjointement avec PGP Desktop 10.0 pour Windows. Aucun des deux programmes ne fonctionnerait correctement. En cas d'installation conjointe, désinstallez les deux programmes, puis réinstallez seulement PGP Desktop.

- **À partir de PGP Desktop pour Windows (version 8.x) et de PGP Universal Satellite :** suivez la procédure d'installation pour PGP Desktop 10.0 pour Windows.

PGP Desktop et PGP Universal Satellite pour Windows sont automatiquement désinstallés et PGP Desktop 10.0 pour Windows est installé. Les trousseaux de clés et fichiers PGP Virtual Disk existants peuvent être utilisés dans la version plus récente.

Recherche des mises à jour

Lorsque cette case est cochée, PGP Desktop recherche les mises à jour logicielles automatiquement, selon l'intervalle spécifié. La valeur par défaut est un jour. Si une version plus récente de PGP Desktop est disponible, un écran de notification s'affiche et vous permet de la télécharger. Lorsque cette case est désactivée, PGP Desktop ne recherche pas automatiquement les mises à jour logicielles. Pour plus d'informations, reportez-vous à la section *Options générales* (cf. "Options de l'onglet Général" à la page 314).

Une fois la mise à jour téléchargée, suivez les invites pour l'installer.

Cette option nécessite une connexion Internet active.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, cette option peut être requise. PGP Desktop recherche alors des mises à jour sur le PGP Universal Server associé.

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

Mise à niveau d'installations autonomes vers des installations gérées de PGP Desktop

Si vous utilisez PGP Desktop en mode autonome et que vous souhaitiez dorénavant que votre environnement soit géré par un PGP Universal Server, vous devez installer une version liée et estampillée de PGP Desktop par-dessus votre installation autonome existante. Vous devez également effectuer le processus d'inscription associé. Votre administrateur PGP vous fournira un fichier d'installation afin que vous puissiez installer une version liée et estampillée.

Mise à niveau du logiciel du système d'exploitation

Si vous mettez à niveau votre ordinateur vers une nouvelle version du système d'exploitation (par exemple, un système Windows vers Windows Vista ou un système Mac OS X vers les versions 10.4.x à 10.5.x), veillez à procéder comme suit :

1. Sauvegardez vos clés et vos trousseaux de clés avant la désinstallation.
2. Si vous avez utilisé la fonctionnalité PGP Whole Disk Encryption, déchiffrez le contenu de votre disque avant de désinstaller PGP Desktop.
3. Désinstallez les versions précédentes de PGP Desktop *avant* d'effectuer la mise à niveau vers la nouvelle version du système d'exploitation.

4 Une fois le système d'exploitation mis à niveau, réinstallez PGP Desktop. Importez vos clés/votre trousseau de clés et, si nécessaire, chiffrez ensuite le contenu de votre disque.

Définition d'une licence pour PGP Desktop

Pour des informations sur les licences de cette version, consultez les *Notes de publication de PGP Desktop*.

Exécution de l'assistant d'installation

À l'issue de l'installation de PGP Desktop, vous êtes invité à redémarrer l'ordinateur. Au redémarrage, dès que le Bureau Windows s'affiche, l'assistant d'installation de PGP Desktop est automatiquement lancé. Cet assistant vous présente une série d'écrans dans lesquels des questions vous sont posées, puis configure PGP Desktop en fonction de vos réponses.

Il comporte uniquement les écrans qui sont appropriés pour votre installation, en prenant en compte un certain nombre de facteurs.

Il ne définit pas tous les paramètres de PGP Desktop. Lorsque vous en avez terminé avec l'assistant d'installation, vous pouvez définir d'autres paramètres en dehors de celui-ci.

Désinstallation de PGP Desktop

Pour désinstaller PGP Desktop, vous pouvez avoir recours soit au programme de désinstallation de PGP Desktop, soit à la fonction d'**ajout/suppression de programmes** de Windows. La procédure ci-dessous décrit une désinstallation via le programme de désinstallation de PGP Desktop.

Si vous effectuez une mise à niveau de PGP Desktop 8.x (ou d'une version ultérieure), il n'est **pas** nécessaire de désinstaller PGP Desktop au préalable. Pour plus d'informations, reportez-vous à la section *Mise à niveau du logiciel* (à la page 23).

Pour désinstaller PGP Desktop

1 Cliquez sur le menu **Démarrer** et sélectionnez **Programmes > PGP > Désinstaller PGP Desktop.** Une boîte de dialogue de confirmation apparaît.

2 Cliquez sur **Oui** pour continuer la procédure de désinstallation. Le logiciel PGP Desktop est alors supprimé de votre système.

Les trousseaux de clés, PGP Virtual Disk et les fichiers PGP Zip (`.pgp`) ne sont *pas* supprimés, en vue d'une réinstallation future de PGP Desktop.

3 Si vous y êtes invité, redémarrez l'ordinateur pour finaliser la désinstallation.

Remarque : au lieu de désinstaller PGP Desktop, vous pouvez vous contenter d'arrêter les services PGP Desktop exécutés en arrière-plan. Si vous préférez cette option, PGP Desktop ne protégera plus vos messages électroniques et instantanés, mais les volumes et disques PGP Virtual Disk ou les partitions protégées par la fonction PGP Whole Disk Encryption resteront accessibles. Si vous souhaitez seulement désactiver les proxys de messagerie électronique ou de messagerie instantanée PGP Desktop, utilisez la boîte de dialogue Options de PGP (sélectionnez **Outils > Options**, cliquez sur l'onglet Messagerie, puis désélectionnez les options inutiles).

Transfert d'une installation PGP Desktop sur un autre ordinateur

Le transfert d'une installation PGP Desktop vers un autre ordinateur est un processus relativement simple, mais quelques étapes essentielles doivent néanmoins être franchies. Ce processus se décompose en plusieurs étapes :

Pour transférer votre installation PGP Desktop sur un autre ordinateur

1. Désinstallez PGP Desktop. Pour ce faire, sélectionnez **Démarrer > Programmes > PGP > Désinstaller PGP Desktop**. Vous pouvez également employer la fonctionnalité d'ajout/suppression de programmes du Panneau de configuration de Windows. Celle-ci constitue le seul moyen de supprimer PGP Desktop si vous exécutez une ancienne version du programme.

   Notez que les fichiers des trousseaux de clés ne sont pas supprimés lors de l'opération.

2. Transférez les trousseaux de clés. Pour cela, enregistrez les fichiers correspondants (`pubring.pkr` et `secring.skr`) qui se trouvent sur l'ancien ordinateur sur une disquette ou un autre support amovible, puis copiez le contenu du support sur le nouvel ordinateur. Par défaut, les fichiers des trousseaux de clés sont stockés dans le dossier C:\Documents and Settings\<utilisateur>\Mes documents\PGP\.

   Si PGP Desktop n'a encore jamais été installé sur le nouvel ordinateur, vous devez créer ce dossier avant de copier les fichiers des trousseaux de clés.

3. Installez PGP Desktop sur le nouvel ordinateur. Pour télécharger le logiciel, cliquez sur le lien de téléchargement qui figure dans le message initial de confirmation de commande de PGP Corporation.

4. Au cours de l'installation, procédez comme suit :

   - Durant l'exécution de l'assistant d'installation de PGP Desktop sur le nouvel ordinateur, sélectionnez l'option **Non, je dispose déjà de trousseaux de clés** et précisez dans quel dossier vous avez copié les fichiers des trousseaux de clés.

- Utilisez les mêmes nom, société et numéro de licence que lors de l'autorisation initiale de PGP Desktop.

4 Interface utilisateur de PGP Desktop

Cette section décrit l'interface utilisateur de PGP Desktop.

Contenu du chapitre

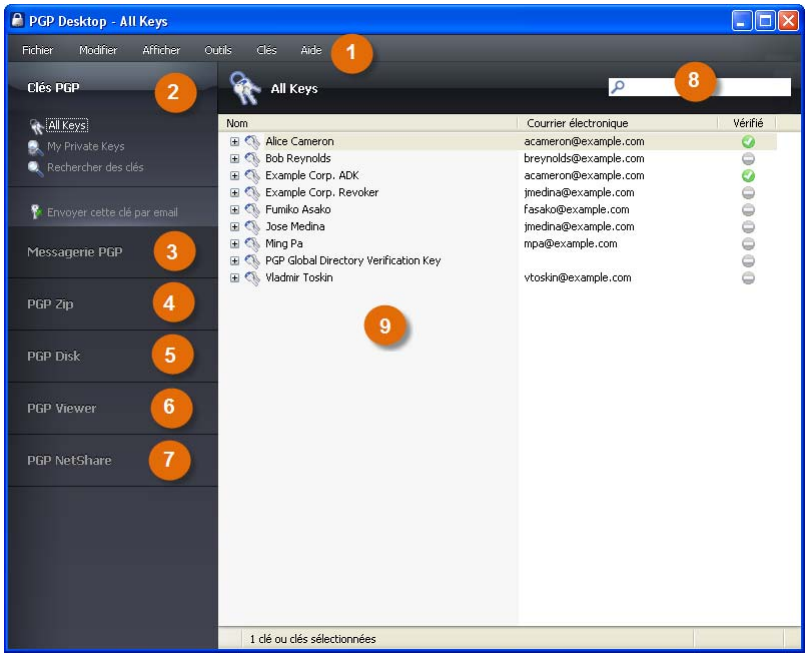
Accès aux fonctions de PGP Desktop

Quatre modes d'accès sont proposés :

- *La fenêtre principale de PGP Desktop* (cf. "Écran principal de PGP Desktop" à la page 30)
- *L'icône de la zone de notification PGP* (cf. "Utilisation de l'icône de la zone de notification PGP" à la page 31)
- *Les menus contextuels de l'Explorateur Windows* (cf. "Utilisation des menus contextuels de l'Explorateur Windows" à la page 33)
- *Le menu Démarrer* (cf. "Utilisation du menu Démarrer" à la page 35)

Écran principal de PGP Desktop

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



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

1	**La barre de menus** : cette barre vous permet d'accéder aux commandes de PGP Desktop. Les menus qu'elle contient sont différents suivant le panneau de contrôle sélectionné.
2	**Le panneau de contrôle Clés PGP** : ce panneau vous permet de contrôler les clés PGP.
3	**Le panneau de contrôle Messagerie PGP** : ce panneau vous permet de contrôler le service de messagerie PGP.
4	**Le panneau de contrôle PGP Zip** : ce panneau vous permet de contrôler PGP Zip, ainsi que l'assistant de PGP Zip, grâce auquel vous pouvez créer des archives PGP Zip.
5	**Le panneau de contrôle PGP Disk** : ce panneau vous permet de contrôler PGP Disk.
6	**Le panneau de contrôle Visionneuse PGP**. Permet de déchiffrer, de vérifier et d'afficher les messages *en dehors* du flux de messagerie.
7	**Le panneau de contrôle PGP NetShare** : ce panneau vous permet de contrôler PGP NetShare.

8	**La zone de travail de PGP Desktop** : cette zone contient des informations sur le panneau de contrôle sélectionné, ainsi que sur les actions que vous pouvez lui appliquer.
9	**La zone de recherche de clés PGP** : cette zone sert à rechercher des clés spécifiques dans votre trousseau de clés. Au fur et à mesure de votre saisie, PGP Desktop affiche les résultats de la recherche en fonction du critère que vous avez indiqué (nom ou adresse de courrier électronique).

Vous pouvez développer chacun des panneaux de contrôle afin de visualiser les options disponibles ou les réduire dans un souci de gain d'espace (dans ce cas, seul le bandeau du panneau de contrôle est visible). Pour développer un panneau de contrôle, cliquez sur son bandeau.

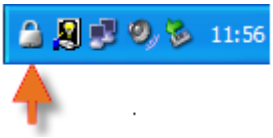
Lorsqu'une boîte de contrôle est développée, son contenu varie selon ce sur quoi vous travaillez ou selon les éléments sélectionnés. Par exemple, lorsqu'une clé publique est sélectionnée et que vous ouvrez la boîte de contrôle Clés PGP, les options **Envoyer un courrier électronique à ce destinataire** et **Envoyer cette clé par courrier électronique** figurent au bas de la boîte de contrôle. Seule l'option **Envoyer cette clé par courrier électronique** est disponible si la clé sélectionnée est privée. Si aucune clé n'est sélectionnée, aucune des deux options n'apparaît.

Utilisez la touche Tab pour parcourir l'écran principal de PGP Desktop, puis la touche d'espacement ou la touche Entrée pour sélectionner une option.

Remarque : pour ouvrir le client de messagerie par défaut du système et créer un courrier électronique en utilisant l'adresse de la clé sélectionnée, cliquez sur **Envoyer un courrier électronique à ce destinataire**. Cette méthode permet d'envoyer facilement un message à une personne dont l'adresse est incluse dans votre trousseau de clés. Pour ouvrir le client de messagerie par défaut du système et créer un courrier électronique en utilisant la clé publique sélectionnée jointe (le message n'est pas transmis), cliquez sur **Envoyer cette clé par courrier électronique**. Cette option est particulièrement utile si vous souhaitez envoyer votre clé publique ou une autre clé publique faisant partie de votre trousseau à quelqu'un qui n'en dispose pas encore.

Utilisation de l'icône de la zone de notification PGP

La plupart des fonctionnalités de PGP Desktop sont accessibles par l'intermédiaire de l'icône de la zone de notification PGP.



Conseil : vous pouvez ouvrir PGP Desktop en double-cliquant sur cette icône.

L'icône de la zone de notification PGP peut prendre quatre formes différentes :

- **Fonctionnement normal** () : cette icône signifie que PGP Desktop fonctionne normalement : aucune phrase secrète n'a été mise en cache, l'envoi de messages par serveur proxy est activé et aucune autre opération PGP n'est en cours.
- **Phrase secrète mise en cache** () : cette icône signifie que PGP Desktop fonctionne normalement ; en outre, au moins une phrase secrète pour clé privée a été mise en cache. La mise en cache des phrases secrètes est une fonctionnalité facultative qui apporte un gain de temps, dans la mesure où, si une phrase secrète est en cache, vous n'avez pas besoin de la saisir pour signer une clé, par exemple. Toutefois, elle constitue un risque en termes de sécurité, puisque quiconque ayant la possibilité d'accéder à votre système pourra utiliser PGP Desktop sans avoir à taper la phrase secrète appropriée.
- **Envoi de messages par serveur proxy désactivé** () : cette icône signifie que l'envoi de messages électroniques par serveur proxy a été désactivé ; les messages chiffrés entrants ne seront ni déchiffrés ni vérifiés et les messages sortants ne seront ni chiffrés ni signés. Vous pouvez réactiver l'envoi de messages par proxy par le biais du menu de la zone de notification PGP ou des options PGP.
- **Occupé** () : cette icône signifie qu'une opération, par exemple le chiffrement d'un disque, est en cours dans PGP Desktop. À l'issue de celle-ci, l'icône reprend la forme qui convient.

Lorsque vous cliquez avec le bouton droit ou gauche de la souris sur l'icône de la zone de notification PGP, un menu vous donnant accès à diverses options apparaît. Remarque : selon que vous vous trouviez dans un environnement autonome ou géré, certaines options peuvent ne pas être disponibles.

- **Quitter les services PGP** : cette option permet d'interrompre les services PGP Desktop sur l'ordinateur. Utilisez cette commande avec prudence, car elle mettra fin au chiffrement et au déchiffrement automatiques du courrier électronique et des sessions de messagerie instantanée.

  Si vous avez arrêté les services PGP et souhaitez par la suite les relancer, redémarrez l'ordinateur ou sélectionnez PGP Desktop dans le menu Démarrer (cliquez sur **Démarrer > Programmes > PGP > PGP Desktop**).
- **À propos de PGP Desktop** : cette option permet d'afficher des informations sur la version de PGP Desktop que vous avez installée, notamment sur la licence.
- **Rechercher les mises à jour** : cette option permet de se connecter au serveur de mise à jour PGP Corporation pour déterminer si une version plus récente de PGP Desktop peut être téléchargée. Elle est disponible uniquement pour les installations autonomes.
- **Aide** : cette option permet d'ouvrir l'aide en ligne intégrée à PGP Desktop.
- **Options** : cette option permet d'ouvrir la boîte de dialogue Options de PGP Desktop.

- **Afficher le notificateur** : cette option permet d'afficher les dernières notifications relatives aux messages entrants et sortants.
- **Afficher le journal de PGP** : cette option permet d'afficher le journal de PGP Desktop. Ce journal répertorie les mesures prises par PGP Desktop pour sécuriser vos données.
- **Ouvrir la Visionneuse PGP** : cette option permet d'ouvrir la Visionneuse PGP dans le but de déchiffrer le courrier électronique en dehors du flux de messagerie.
- **Ouvrir PGP Desktop** : cette option permet d'ouvrir la fenêtre principale de PGP Desktop. Pour ouvrir PGP Desktop, vous pouvez également *double-cliquer* sur l'icône de la zone de notification PGP Desktop.
- **Mettre à jour la stratégie** : cette option permet de télécharger manuellement la stratégie à partir du serveur PGP Universal Server. Elle est disponible uniquement pour les installations gérées.
- **Effacer les caches** : cette option permet de supprimer les informations mises en cache, telles que les phrases secrètes et les clés publiques.

  Remarque : une phrase secrète mise en cache n'est pas effacée si vous avez utilisé une carte à puce ou un jeton pour accéder à un dossier protégé par PGP NetShare, puis supprimé cette carte ou ce jeton. Pour effacer une phrase secrète en cache, il vous faut créer un raccourci clavier. Pour plus d'informations, reportez-vous à la section *Options avancées* (à la page 332).
- **Démonter les PGP Virtual Disks** : cette option permet de démonter tous les volumes PGP Virtual Disk montés.
- **Fenêtre en cours** : cette option permet d'appliquer une fonctionnalité PGP Desktop (Déchiffrer et vérifier, Chiffrer et signer, Signer, Chiffrer) au contenu de la fenêtre active.
- **Presse-papiers** : cette option permet d'appliquer une fonctionnalité PGP Desktop (Déchiffrer et vérifier, Chiffrer et signer, Signer, Chiffrer) au contenu du Presse-papiers. Elle sert aussi à effacer ou modifier celui-ci.

Utilisation des menus contextuels de l'Explorateur Windows

Vous pouvez également accéder aux fonctions de PGP Desktop par l'intermédiaire des menus contextuels de l'Explorateur Windows. Ouvrez l'Explorateur Windows, cliquez avec le bouton droit sur l'élément que vous souhaitez utiliser, puis, dans le menu contextuel, sélectionnez **PGP Desktop**.

L'Explorateur vous donne accès aux fonctions de PGP Desktop disponibles pour l'élément choisi :

- **Un lecteur** : si vous cliquez avec le bouton droit sur un lecteur de votre système dans l'Explorateur Windows, puis sélectionnez PGP Desktop dans le menu contextuel, vous pouvez effectuer l'opération suivante sur le lecteur :
  - Décomposer de l'espace libre par PGP
- **Un lecteur PGP Virtual Disk** : si vous cliquez avec le bouton droit sur un lecteur PGP Virtual Disk monté de votre système dans l'Explorateur Windows, puis sélectionnez PGP Desktop dans le menu contextuel, vous pouvez effectuer les opérations suivantes sur le lecteur :
  - Le démonter
  - Rechercher le fichier PGP Virtual Disk (.pgd) dans l'Explorateur Windows
  - Modifier ses propriétés

  Si vous cliquez avec le bouton droit sur le fichier PGP Virtual Disk (.pgd) correspondant à un disque non monté dans l'Explorateur Windows, puis sélectionnez PGP Desktop dans le menu contextuel, vous pouvez également réaliser les actions suivantes :
  - Compacter l'espace inutilisé
  - Utiliser PGP Shred pour supprimer en toute sécurité le disque PGP Virtual Disk (dans ce cas, toutes les données qu'il contient sont supprimées)
  - Chiffrer à nouveau le disque PGP Virtual Disk
- **Un dossier** : si vous cliquez avec le bouton droit sur un dossier de l'Explorateur Windows, puis sélectionnez PGP Desktop dans le menu contextuel, vous pouvez effectuer les opérations suivantes sur le dossier :
  - L'ajouter à une nouvelle archive PGP Zip
  - Créer une archive à auto-déchiffrement pour y placer le contenu du dossier
  - Le sécuriser avec une clé ou une phrase secrète
  - Le déchiffrer et le vérifier
  - L'ajouter à PGP NetShare
  - Le décomposer
- **Un fichier** : si vous cliquez avec le bouton droit sur un fichier de l'Explorateur Windows, puis sélectionnez PGP Desktop dans le menu contextuel, les opérations ci-après sont possibles, suivant le type du fichier :
  - Si vous sélectionnez un fichier non chiffré, vous pouvez le sécuriser à l'aide d'une clé ou d'une phrase secrète, le signer, le décomposer ou créer une archive à auto-déchiffrement.
  - Si vous sélectionnez un fichier chiffré, vous pouvez le déchiffrer et le vérifier, ou le décomposer.

- Si vous sélectionnez un volume PGP Virtual Disk non monté (`.pgd`), vous pouvez le monter ou le modifier ; si vous sélectionnez un volume monté, vous pouvez le démonter.
- Si vous sélectionnez un fichier PGP Zip (.PGP), vous pouvez le déchiffrer et le vérifier, l'afficher ou le décomposer.
- Si vous sélectionnez un fichier de clé PGP (`.asc`), vous pouvez le déchiffrer et le vérifier, ou le décomposer. Si vous choisissez de le déchiffrer et de le vérifier, vous avez la possibilité de l'importer.
- Si vous sélectionnez un fichier de trousseau de clés publiques ou privées PGP (fichiers PKR et SKR, respectivement), vous pouvez inclure les clés qu'il contient dans votre trousseau ou le décomposer.

Utilisation du menu Démarrer

Vous pouvez ouvrir PGP Desktop par le biais du menu Démarrer de Windows. Pour ce faire, sélectionnez **Démarrer > Programmes > PGP**.

Le menu Démarrer vous donne accès :

- à la documentation PGP Desktop en anglais et dans d'autres langues prises en charge ;
- à l'application PGP Desktop ;
- à la procédure de désinstallation de PGP Desktop.

Alertes du notificateur PGP Desktop

Le notificateur PGP Desktop affiche de petites notes informatives concernant le statut des messages électroniques entrants et sortants, ainsi que des sessions de messagerie instantanée.

Remarque : cette fonction de PGP Desktop indique également le statut des fonctions PGP Whole Disk Encryption et PGP NetShare sur votre ordinateur. Pour plus d'informations, reportez-vous à la section *Fonctionnalités du notificateur PGP Desktop pour disque* (à la page 38).

Notificateur PGP Desktop pour la messagerie

Le notificateur PGP Desktop pour la messagerie vous permet d'effectuer les tâches suivantes :

- Vérifier si un message électronique entrant est correctement déchiffré et/ou signé.

- Vérifier si un message électronique sortant est correctement chiffré et/ou signé.
- Interrompre l'envoi d'un message électronique si les options de chiffrement ne vous conviennent pas.
- Afficher un court résumé de l'expéditeur, de l'objet et de la clé de chiffrement d'un message électronique.
- Vérifier à tout moment l'état des messages entrants ou sortants précédents pour la session Windows en cours.
- Vérifier que la session de discussion en ligne avec un autre utilisateur PGP Desktop est sécurisée.

Le notificateur PGP Desktop vous permet de surveiller tous les messages électroniques entrants, ou une partie de ceux-ci, et de garder un contrôle précis sur tout ou partie des messages sortants. Le choix vous appartient. Vous pouvez configurer un très grand nombre d'options dans le notificateur ou désactiver complètement le notificateur PGP Desktop, si vous préférez.

Autres caractéristiques du notificateur PGP Desktop :

- Pour la notification des messages, utilisez les flèches gauche et droite situées dans l'angle supérieur droit de la fenêtre du notificateur pour faire défiler les messages vers le haut ou vers le bas. De cette manière, vous pouvez consulter les messages reçus avant ou après celui que vous êtes en train de lire.
- Lorsqu'elles sont affichées pour la première fois, les boîtes de message de notificateur sont partiellement transparentes afin d'éviter qu'elles masquent le moindre élément de votre écran. Elles deviennent opaques lorsque vous placez le curseur dessus et redeviennent transparentes lorsque vous en éloignez le curseur.
- Les messages du notificateur restent affichés pendant quatre secondes avant de disparaître, sauf si vous placez le curseur dessus (vous pouvez modifier ce paramètre par défaut dans les options). Si vous avez besoin de plus de temps pour lire un notificateur, placez le curseur dessus : le notificateur reste affiché à l'écran.
- Si vous n'avez pas lu un notificateur ou si vous voulez relire d'anciens notificateurs, procédez comme suit :
  - Sous Windows, sélectionnez **Afficher le notificateur** dans l'icône de PGP dans la zone de notification.
  - Sous Mac OS X, sélectionnez **Afficher le notificateur** dans l'icône PGP Desktop de la barre de menus.
- Pour fermer un message de notificateur, cliquez sur la croix **X** qui se trouve dans l'angle supérieur droit du message sous Windows et dans l'angle supérieur gauche sous Mac OS X.

Pour plus d'informations sur la configuration des options du notificateur PGP Desktop, reportez-vous à *Options du notificateur* (à la page 330).

Notificateur PGP Desktop - Messages entrants

Les notifications de message électronique entrant vous permettent de savoir si le message a été déchiffré et vérifié, ou déchiffré et signé par une clé inconnue ou non vérifiée.

Notificateur PGP Desktop - Messages sortants

Pour une simple notification, configurez le Notificateur PGP Desktop de sorte qu'il apparaisse momentanément lors de l'envoi du message électronique (pour tous les messages ou pour certains messages répondant à des critères particuliers).

Vous pouvez aussi configurer PGP Desktop de manière à inclure les boutons **Bloquer** et **Envoyer** dans la fenêtre du Notificateur.

Pour gérer le courrier électronique sortant avec le Notificateur

1. Dans la fenêtre du Notificateur de message sortant PGP, procédez comme suit :
   - Pour interrompre l'envoi du message électronique, cliquez sur **Bloquer**. Seul ce message est bloqué. Les messages électroniques suivants pour ce destinataire pourront être envoyés.
   - Pour envoyer ce message, même si la clé du destinataire est introuvable, cliquez sur **Envoyer**.
   - Pour poursuivre la suspension du traitement du message, laissez le curseur sur la fenêtre du Notificateur. Dès que vous éloignez le curseur de la fenêtre, le message est traité conformément à la règle par défaut.
   - Le paramètre **Différer les messages sortants pour** dans les options du Notificateur permet de fixer la durée, en secondes, qui s'écoule avant que le Notificateur envoie le message électronique sans intervention de votre part. Le Notificateur indique le temps restant avant l'envoi du message.
2. Pous afficher des informations supplémentaires, y compris l'action, le destinataire, la stratégie et la clé de signature, cliquez sur **Plus**.

   La consultation de ces informations supplémentaires est facultative. Pour les masquer à nouveau, cliquez sur **Moins**.

Messages sortants du Notificateur PGP Desktop pour la stratégie hors connexion

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur peut avoir spécifié les actions à effectuer sur les messages sortants lorsque le PGP Universal Server n'est pas disponible. Le message sortant du Notificateur est l'un des éléments suivants :

- Votre PGP Universal Server n'est pas disponible et la stratégie est définie pour bloquer tous les messages. Les messages électroniques restent dans votre boîte d'envoi et seront envoyés lorsque le PGP Universal Server pourra être contacté.
- Votre PGP Universal Server n'est pas disponible et la stratégie est définie pour envoyer tous les messages en texte en clair.
- Votre PGP Universal Server n'est pas disponible et la stratégie est définie pour permettre à votre stratégie locale de prendre la priorité.

Dans les deux derniers cas, vous pouvez choisir d'envoyer ou de bloquer le message sortant comme vous le feriez avec tout autre message sortant.

Notificateur PGP pour la messagerie instantanée

Si PGP Desktop est installé sur votre ordinateur et que vous définissiez la réception de notifications pour la messagerie instantanée (sous l'onglet **Notifications** dans les préférences de PGP Desktop), vous recevez une alerte lorsque les sessions AIM (AOL Instant Messenger) initiées avec d'autres utilisateurs de PGP Desktop sont sécurisées.

Lorsque vous utilisez la fonctionnalité de messagerie instantanée sécurisée, une notification s'affiche au moment de la connexion au programme de messagerie instantanée pour vous informer que la communication est sécurisée. Une icône représentant un cadenas apparaît en regard de votre nom d'utilisateur dans la plupart des clients de messagerie instantanée compatibles avec AIM.

Lorsque vous vous déconnectez du programme de messagerie instantanée, une notification annonce la fin de la session sécurisée.

Pour plus d'informations sur la configuration et l'utilisation de la fonctionnalité de communication sécurisée par messagerie instantanée, reportez-vous à la section Sécurité des messages instantanés.

Fonctionnalités du notificateur PGP Desktop pour disque

Le notificateur PGP Desktop pour disque vous permet de rester informé lorsque vous utilisez les composants PGP NetShare et PGP Whole Disk Encryption.

Remarque : Le notificateur PGP Desktop affiche également sur votre ordinateur le statut des messages électroniques entrants et sortants. Pour plus d'informations, reportez-vous à *Notificateur PGP Desktop pour la messagerie* (à la page 35).

PGP NetShare

Utilisé conjointement avec PGP NetShare, le Notificateur PGP Desktop vous informe des éléments suivants :

- Action effectuée sur un dossier partagé

- Emplacement du dossier concerné
- Nom du dossier concerné
- Auteur de l'action

PGP Whole Disk Encryption

Utilisé conjointement avec PGP Whole Disk Encryption, le Notificateur PGP Desktop vous informe des éléments suivants :

- Disque en cours de chiffrement
- Taille et type du disque
- État du processus de chiffrement

Activation ou désactivation des messages de notification

Pour activer ou désactiver des messages de notification

1. Ouvrez PGP Desktop et sélectionnez **Outils > Options de PGP**.
2. Cliquez sur l'onglet Notificateur.
3. Sous **Utilisation**, indiquez si vous souhaitez **Utiliser le notificateur PGP** et, le cas échéant, son emplacement. Les notification de PGP Desktop peuvent être affichées dans n'importe quel angle de l'écran (**En bas à droite**, **En bas à gauche**, **En haut à droite** ou **En haut à gauche**). Choisissez celui dans lequel vous souhaitez les voir apparaître. La position par défaut est **En bas à droite**.
4. Si vous utilisez la messagerie de PGP Desktop et que vous souhaitez que des messages de notification PGP Desktop s'affichent pour vous informer de l'état du chiffrement ou de la signature lorsque vous envoyez des courriers électroniques, cochez la case **M'avertir du traitement des messages sortants**. Désactivez-la pour arrêter l'affichage de ces notifications.
5. PGP Desktop recherche une clé publique pour chaque destinataire des messages envoyés. Par défaut, s'il ne trouve pas de clé publique, il envoie le message en clair (sans chiffrement). Sélectionnez **Me demander confirmation avant l'envoi d'un courrier électronique lorsque la clé du destinataire est introuvable** si vous voulez être averti lorsqu'une clé est introuvable afin de pouvoir bloquer le message et que celui-ci ne soit pas envoyé. Spécifiez ensuite les options suivantes :

- **Toujours me demander confirmation avant l'envoi d'un courrier électronique :** : cochez cette case si vous souhaitez confirmer l'envoi de chaque courrier électronique. Vous pouvez consulter l'état du chiffrement dans le Notificateur et choisir d'envoyer ou de bloquer le message.
- **Différer les messages sortants pendant n seconde(s) pour confirmer** (où *n* est un nombre entre 1 et 30 ; la valeur par défaut est de 4 secondes) : pour modifier le temps d'attente avant l'envoi des messages sortants et l'affichage des notifications PGP Desktop, cliquez sur les flèches haut et bas. Cette période vous permet de consulter le message du Notificateur PGP Desktop.

(Pour plus d'informations sur les paramètres de stratégie par défaut de PGP Desktop, reportez-vous à la section *Services et stratégies* (à la page 100).)

6 Pour les courriers électroniques entrants, indiquez comment vous voulez être averti de leur état. Sélectionnez l'une des possibilités suivantes pour l'option **Afficher des notifications pour les messages entrants** :

- **À la réception de messages sécurisés** : un message de notification apparaît chaque fois que vous recevez un courrier électronique sécurisé. Elle indique l'expéditeur et l'objet du message, l'état de chiffrement et de vérification, ainsi que l'adresse de courrier électronique de l'expéditeur.
- **Uniquement en cas d'échec de vérification du message** : un message de notification s'affiche uniquement lorsque PGP Desktop ne parvient pas à vérifier la signature du message entrant.
- **Jamais** : si vous ne souhaitez pas voir de message de notification lors de la réception de courriers électroniques, sélectionnez cette option. Cela n'a aucune incidence sur les messages de notification relatifs aux messages sortants.

7 Si vous voulez qu'un message de notification PGP Desktop s'affiche brièvement au début et à la fin d'une conversation sécurisée de messagerie instantanée, cochez la case **M'avertir de l'état des sessions de messagerie instantanée chiffrées PGP**.

Affichage du journal de PGP

Ce journal répertorie les mesures prises par PGP Desktop pour sécuriser vos données.

Pour afficher le journal de PGP

1 Pour afficher les journaux, vous devez activer la journalisation. Pour cela, dans PGP Desktop, sélectionnez **Outils > Activer la journalisation**.

2 Effectuez l'une des opérations suivantes :

- Cliquez sur l'icône de la zone de notification de PGP Desktop et sélectionnez **Afficher le journal de PGP** dans le menu contextuel. Le journal de PGP s'ouvre dans une nouvelle fenêtre.
- Dans PGP Desktop, sélectionnez **Outils > Afficher le journal**. Le journal de PGP s'ouvre dans une nouvelle fenêtre.
- Dans le panneau de contrôle Messagerie PGP, cliquez sur **Journal de PGP**. Le journal de PGP s'affiche dans la fenêtre de l'application.

3 Pour modifier les options d'affichage ou filtrer certaines informations de journalisation, procédez comme suit :

- Cliquez sur la flèche à droite du champ **Afficher le journal de** pour sélectionner les jours pour lesquels vous souhaitez consulter les journaux.
- Cliquez sur la flèche à droite du champ **Afficher la rubrique** pour sélectionner les types des journaux que vous souhaitez consulter. Les rubriques disponibles sont : **Tous**, **PGP**, **Courrier électronique**, **MI**, **Disque complet**, **NetShare**, **Zip/SDA** et **Virtual Disk**.
- Cliquez sur la flèche à droite du champ **Afficher le niveau** pour sélectionner le niveau de gravité minimal des entrées du journal à afficher. Les niveaux disponibles sont : **Erreur**, **Avertir, Info** et **Informations détaillées**.

  Pour que les journaux **Informations détaillées** puissent être affichés, la fenêtre d'affichage Journal de PGP doit rester ouverte. Lorsque vous la fermez, le niveau de journalisation par défaut, à savoir **Info**, est rétabli. Remarque : la journalisation **Informations détaillées** peut générer des fichiers journaux volumineux.

4 Une fois la consultation du journal terminée :

- Pour enregistrer une copie du journal de PGP, cliquez sur **Enregistrer**.
- Pour effacer les entrées du journal, cliquez sur **Décomposer**.
- Pour quitter la fenêtre Journal de PGP, cliquez sur **Fermer**.

5 Utilisation des clés PGP

La fonctionnalité des clés PGP de PGP Desktop est celle que vous utilisez pour la création et la maintenance de votre ou de vos paires de clés et les clés publiques d'autres utilisateurs de PGP Desktop.

Cette section décrit l'affichage des clés, la création d'une paire de clés, la distribution de votre clé publique, l'obtention des clés publiques d'autres personnes, et l'utilisation de serveurs de clés.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

Affichage des clés

Pour afficher les clés sur le trousseau de clés local, ouvrez PGP Desktop et cliquez sur la boîte de contrôle Clés PGP. Cliquez ensuite sur :

- **Toutes les clés**. Affiche toutes les clés PGP de vos trousseaux de clés.
- **Mes clés privées**. Affiche uniquement les clés privées de vos trousseaux de clés.
- **Rechercher des clés**. Vous permet de chercher des clés dans vos trousseaux de clés selon les critères que vous spécifiez.

- **Clés de carte à puce**. Si une carte à puce est connectée à votre système, cette option est aussi présente.

Certaines des tâches les plus communes que vous voudrez peut-être effectuer sont disponibles à partir de la boîte de contrôle Clés PGP ou de la zone de travail des clés PGP. Ces tâches sont les suivantes :

- Si une clé publique est sélectionnée dans une des vues des clés PGP de vos trousseaux de clés, l'option pour **Envoyer un courrier électronique à ce destinataire** est disponible dans la boîte de contrôle Clés PGP.
- Si vous sélectionnez une clé publique trouvée dans les résultats d'une recherche mais absente de vos trousseaux de clés locaux, l'option **Ajouter à mon trousseau de clés** est disponible dans la boîte de contrôle Clés PGP.
- Pour voir les propriétés de n'importe quelle clé affichée dans la zone de travail, double-cliquez simplement sur une partie quelconque de la clé pour afficher la boîte de dialogue Propriétés de la clé correspondante.

Quand vous effectuez une recherche, l'option **Enregistrer cette recherche de clé** est disponible dans la boîte de contrôle Clés PGP : vous pouvez ainsi enregistrer les résultats pour y accéder ultérieurement.

Création d'une paire de clés

Vous avez probablement déjà créé une paire de clés PGP par le biais de l'assistant d'installation de PGP Desktop ou dans une version antérieure du logiciel, mais, si ce n'est pas le cas, faites-le maintenant. Vous en aurez besoin pour pouvoir effectuer la plupart des actions proposées dans PGP Desktop.

Attention : il est déconseillé de créer des clés trop souvent. Une paire de clés PGP est semblable à un passeport ou permis de conduire numérique ; si vous créez de nombreuses paires, vous vous y perdrez, et les personnes qui souhaitent vous envoyer des messages chiffrés ne s'y retrouveront pas non plus. Il est préférable de regrouper toutes les adresses de courrier électronique que vous utilisez au sein d'une seule clé. Le serveur PGP Global Directory publiera une seule clé par adresse de courrier électronique.

Si PGP Desktop est exécuté dans un environnement géré par un PGP Universal Server, la création de paires de clés peut être désactivée.

Pour créer une paire de clés PGP

1. Assurez-vous que la boîte de contrôle Clés PGP est sélectionnée.
2. Sélectionnez **Fichier > Nouvelle clé PGP** ou appuyez sur la combinaison de touches Ctrl+N. Le premier écran de l'assistant de génération de clé PGP s'affiche.
3. Lisez les informations de cet écran.

4 Si vous voulez générer votre nouvelle paire de clés PGP sur un jeton ou une carte à puce, assurez-vous que le jeton ou la carte à puce est connectée au système puis sélectionnez la case **Générer une clé sur le jeton : [nom de la carte à puce ou du jeton sur le système]**. Pour plus d'informations sur les cartes à puce et les jetons, reportez-vous à la section *Stockage de clés sur des cartes à puce et des jetons* (cf. "Stockage des clés sur des cartes à puce et jetons" à la page 299).

5 Cliquez sur **Suivant**. L'écran Nom et affectation de messagerie s'affiche.

6 Saisissez votre vrai nom dans le champ **Nom complet** et votre adresse de courrier électronique correcte dans le champ **Adresse de courrier électronique principale**. Il n'est pas absolument nécessaire de saisir votre vrai nom ou même votre adresse de courrier électronique. Cependant, les autres personnes vous identifieront plus facilement en tant propriétaire de la clé publique si vous utilisez votre vrai nom. De plus, quand vous téléchargez votre clé publique vers PGP Global Directory et la rendez ainsi facilement accessible aux autres utilisateurs de PGP Desktop, vous devez indiquer votre adresse de courrier électronique correcte.

7 Si vous souhaitez ajouter des adresses de courrier électronique supplémentaires à la clé que vous créez, cliquez sur **Plus** et saisissez-les dans les champs qui s'affichent.

8 Pour spécifier des paramètres avancés pour la clé que vous créez, cliquez sur **Avancé**. La boîte de dialogue Paramètres de clé avancés s'affiche. Utilisez cette boîte de dialogue pour spécifier le type et la taille de la clé, son expiration, et d'autres paramètres.

9 Sélectionnez les paramètres des éléments suivants :

- **Type de clé**. Choisissez entre Diffie-Hellman/DSS et RSA.
- **Générer une sous-clé de signature distincte**. Sélectionnez cette case si vous devez signer avec une sous-clé distincte. Un sous-clé de signature distincte est créée en même temps que la nouvelle paire de clés. Vous pouvez aussi créer des sous-clés de signature ou de chiffrement supplémentaires à tout moment une fois la nouvelle clé créée. Pour plus d'informations sur les sous-clés de signature et de chiffrement distinctes, reportez-vous à la section *Utilisation des sous-clés* (à la page 72).
- **Taille de clé**. Saisissez de 1024 bits à 4096 bits. Plus grande est la clé, plus sécurisée est-elle mais plus il faudra de temps pour la générer. Certains jetons et cartes à puce limitent la taille de la clé à 1024 bits.
- **Expiration**. Sélectionnez **Jamais** ou spécifiez une date d'expiration pour la paire de clés que vous créez.
- **Chiffrements autorisés**. Désélectionnez tout chiffrement que la paire de clés que vous créez ne doit pas prendre en charge.
- **Chiffrement par défaut**. Sélectionnez le chiffrement à utiliser quand aucun algorithme n'est spécifié. Seul un chiffrement autorisé peut être sélectionné comme chiffrement par défaut.

- **Hachages autorisés**. Désélectionnez tout hachage que la paire de clés que vous créez ne doit pas prendre en charge.
- **Hachage par défaut**. Sélectionnez le hachage à utiliser quand aucun hachage n'est spécifié. Seul un hachage autorisé peut être sélectionné comme hachage par défaut.

10 Cliquez sur **OK** pour fermer la boîte de dialogue Paramètres de clé avancés.

11 Cliquez sur **Suivant**.

12 Si vous faites partie d'un environnement géré par un PGP-Universal Server, il est possible que vous voyiez l'écran Paramètres de l'entreprise. Cet écran affiche les clés que votre administrateur PGP a configurées pour être ajoutées à votre copie de PGP Desktop, par exemple la clé de déchiffrement supplémentaire (ADK) de votre entreprise ou la clé d'entreprise.

L'écran Affectation de la phrase secrète s'affiche.

13 Saisissez la phrase secrète que vous voulez utiliser pour maintenir l'accès exclusif à la clé privée de la paire de clés créée.

14 Pour confirmer la saisie, appuyez sur la touche **Tabulation** pour accéder au champ Confirmation et y entrer de nouveau la même phrase secrète. Pour les informations sur l'indicateur de qualité de la phrase secrète, reportez-vous à la section *Indicateur de qualité de la phrase secrète* (à la page 336).

Remarque : normalement, afin de renforcer le niveau de sécurité, les caractères que vous saisissez pour la phrase secrète ne sont pas visibles à l'écran. Cependant, si vous êtes certain que personne ne vous voit, vous pouvez afficher les caractères saisis pour la phrase secrète en cochant la case **Afficher les frappes**.

Avertissement : sauf si votre administrateur PGP a implémenté une stratégie de reconstruction de clé PGP pour votre société, rien ni personne, y compris PGP Corporation, ne peut récupérer une clé dont la phrase secrète a été oubliée.

15 Cliquez sur **Suivant** pour lancer le processus de génération de clé. PGP Desktop génère votre nouvelle paire de clés.

Ce processus peut durer plusieurs minutes.

16 Quand le processus de génération de clé indique qu'il a terminé, cliquez sur **Suivant**. Vous êtes invité à ajouter à PGP Global Directory la partie de clé publique de la clé que vous venez de créer.

17 Lisez le texte à l'écran et cliquez sur **Suivant** pour ajouter votre nouvelle clé au PGP Global Directory (recommandé). Cliquez sur **Ignorer** si vous voulez empêcher que la clé publique soit postée dans PGP Global Directory.

18 Cliquez sur **Terminer**. Votre nouvelle paire de clés PGP a été générée. Elle devrait être visible dans la zone de travail des clés PGP. Si elle n'apparaît pas dans la liste, assurez-vous que **Toutes les clés** ou **Mes clés privées** est sélectionné dans la boîte de contrôle Clés PGP.

Attention : à ce stade, il est recommandé de conserver une copie de sauvegarde de la clé privée dans un emplacement sûr. Votre clé privée est très importante. Sa perte peut avoir des conséquences catastrophiques une fois qu'elle a servi à chiffrer des données. Reportez-vous à la section *Protection de votre clé privée* (à la page 48).

Mots de passe et phrases secrètes

Se retrouver dans l'incapacité de déchiffrer un fichier après l'avoir soi-même chiffré est une manière douloureuse d'apprendre à choisir une phrase secrète dont vous vous souviendrez.

La plupart des applications exigent un mot de passe d'une longueur entre trois et huit lettres. D'une manière générale, l'utilisation d'une phrase secrète d'un seul mot est fortement déconseillé. Un mot de passe d'un seul de mot est vulnérable à une attaque par dictionnaire, à savoir l'essai par un ordinateur de tous les mots du dictionnaire jusqu'à la découverte de votre mot de passe. Vous pouvez aisément imaginer des attaques par dictionnaire un peu améliorées qui permettent de trouver d'importantes collections de mots de passe, même si ceux-ci sont légèrement modifiés par rapport aux termes du dictionnaire.

Pour se protéger contre ce type d'attaques, il est fortement recommandé de créer un mot de passe qui comprend une combinaison de lettres minuscules et majuscules, de chiffres, de signes de ponctuation et d'espaces. Il en résulte un mot de passe plus fort mais obscur, dont vous risquez de ne pas vous rappeler facilement.

L'insertion arbitraire de nombreux caractères non alphabétiques dans une phrase secrète dans le but de contrecarrer une attaque par dictionnaire rend la phrase secrète trop facile à oublier ; elle pourrait entraîner une perte d'informations désastreuse si vous ne pouvez pas déchiffrer vos propres fichiers. Une phrase secrète de plusieurs mots est moins vulnérable à une attaque par dictionnaire. Cependant, à moins que la phrase secrète choisie ne soit facilement stockée en mémoire à long terme, il est peu probable que vous la reteniez textuellement.

Le choix improvisé d'une phrase entraînera probablement son oubli total. Choisissez une phrase qui est déjà présente dans votre mémoire à long terme. Ne choisissez pas une phrase que vous avez récemment répétée à d'autres personnes, ni une citation célèbre : vous voulez qu'un pirate ingénieux ait des difficultés à la découvrir. Si elle est déjà profondément ancrée dans votre mémoire à long terme, vous ne l'oublierez probablement pas. Bien sûr, si vous êtes assez imprudent pour écrire votre phrase secrète sur un papier collé à votre ordinateur ou rangé dans un tiroir de votre bureau, ce que vous choisissez n'aura aucune importance.

Pour plus d'informations, reportez-vous à la section *Utilisation des mots de passe et phrases secrètes* (à la page 335).

Protection de votre clé privée

PGP Corporation recommande de prendre ces mesures immédiatement après la création de votre paire de clés :

Attention : l'absence de ces mesures pourrait entraîner par la suite des pertes de données dévastatrices.

- Sauvegardez une copie de votre fichier de clé privée dans un emplacement différent et sûr, au cas où votre copie principale soit un jour endommagée ou perdue. Reportez-vous à la section *Sauvegarde de votre clé privée* (à la page 49).
- Réfléchissez à la phrase secrète que vous choisissez afin de vous assurer d'en choisir une que vous n'oublierez pas. Si vous avez quelque inquiétude quant à votre capacité à retenir la phrase secrète choisie pendant le processus de création de clé, changez-la TOUT DE SUITE pour une autre que vous n'oublierez pas. Pour en savoir plus sur la modification de votre phrase secrète, reportez-vous à la section *Modification de votre phrase secrète* (à la page 65).

Votre fichier de clé privée est très important parce qu'une fois que vous avez chiffré des données avec votre clé publique, seule la clé privée correspondante peut les déchiffrer. C'est aussi vrai pour votre phrase secrète ; la perte de votre clé privée ou de la phrase secrète implique l'impossibilité de déchiffrer les données chiffrées avec la clé publique correspondante. Quand vous chiffrez des informations, elles sont chiffrées avec votre phrase secrète et votre clé privée. Vous avez besoin des deux pour déchiffrer les données chiffrées. Une fois les données chiffrées, rien ni personne, pas même PGP Corporation, ne peut déchiffrer les données en l'absence de votre fichier de clé privée et de votre phrase secrète.

Pensez à une situation où vous avez d'importantes données chiffrées, et que vous oubliez votre phrase secrète ou perdez votre clé privée. Les données chiffrées seraient inaccessibles, inutilisables et irrécupérables.

Protection des clés et des trousseaux de clés

En plus d'effectuer des copies de sauvegarde de vos clés, vous devez faire particulièrement attention à l'emplacement de stockage de votre clé privée. Même si votre clé privée est protégée par une phrase secrète que vous seul devriez connaître, quelqu'un pourrait découvrir votre phrase secrète, puis utiliser votre clé privée pour déchiffrer votre courrier électronique ou contrefaire votre signature numérique. Par exemple, quelqu'un peut regarder les touches que vous tapez par-dessus votre épaule ou les intercepter sur le réseau voire sur Internet.

Pour empêcher quiconque qui aurait pu intercepter votre phrase secrète d'utiliser votre clé privée, ne stockez votre clé privée que sur votre propre ordinateur. Si votre ordinateur est relié à un réseau, assurez-vous que vos fichiers ne sont pas automatiquement inclus dans une sauvegarde système où d'autres utilisateurs pourraient avoir accès à votre clé privée. Étant donnée la facilité d'accès aux ordinateurs par les réseaux, si vous manipulez des informations extrêmement sensibles, il est préférable que vous conserviez votre clé privée sur une disquette que vous pouvez insérer comme les clés traditionnelles quand vous voulez lire ou signer des informations privées.

Comme précaution de sécurité supplémentaire, pensez à affecter un nom distinct à votre fichier de trousseau de clés privées et à le stocker dans un emplacement différent que celui par défaut. Utilisez l'onglet Clés de la boîte de dialogue Options pour attribuer un nom et un emplacement à vos fichiers de trousseau de clés privées et publiques.

Vos clés privées et publiques sont stockées dans des fichiers de trousseau de clés distincts. Vous pouvez les copier dans un autre emplacement sur votre disque dur ou sur une disquette. Par défaut, le trousseau de clés privées (`secring.skr`) et le trousseau de clés publiques (`pubring.pkr`) sont stockés avec les autres fichiers du programme dans votre dossier « PGP » ; vous pouvez enregistrer vos sauvegardes dans un emplacement de votre choix.

Les clés générées sur une carte à puce ne peuvent pas être sauvegardées, car la partie privée de votre paire de clés n'est pas exportable. (Il est possible de générer des clés sur une carte à puce uniquement sur le systèmes Windows.)

Vous pouvez configurer PGP Desktop pour sauvegarder automatiquement vos trousseaux de clés après sa fermeture. Définissez les options de sauvegarde de vos trousseaux de clés dans l'onglet Clés de la boîte de dialogue Options (pour les systèmes Windows) ou de la boîte de dialogue Préférences (pour les systèmes Mac OS X).

Sauvegarde de votre clé privée

Pour sauvegarder votre clé privée

1. Dans le panneau de contrôle Clés PGP, cliquez sur **Mes clés privées**.
2. Cliquez sur l'icône qui représente votre paire de clés.
3. Sélectionnez **Fichier > Exporter**.
4. Saisissez un nom pour le fichier.
5. Cochez la case **Inclure la ou les clés privées**. Cette opération est importante ; si vous ne l'exécutez pas, seule votre clé publique sera exportée.
6. Cliquez sur **Enregistrer**.

7 Copiez le fichier dont l'extension est .asc à un emplacement sécurisé. Ce peut être un CD que vous archivez soigneusement, un autre PC ou un lecteur USB Flash que vous gardez en lieu sûr. Rappelez-vous de ne pas distribuer ce fichier à quiconque : il contient vos deux clés, privée et publique.

Remarque : si votre ordinateur se trouve dans un environnement géré par un PGP Universal Server et que votre mode clé soit SKM, vous ne pouvez pas exporter votre clé à l'aide de cette méthode. Pour exporter votre paire de clés, demandez à votre administrateur PGP Universal Server d'effectuer l'opération à partir de la console de gestion. Pour identifier le mode clé utilisé, reportez-vous à la section *Modes clé* (à la page 133).

Que faire si vous avez perdu votre clé ?

Si vous avez perdu votre clé et que vous n'avez pas de copie de sauvegarde pour la restaurer, vous ne pourrez plus jamais déchiffrer les informations chiffrées avec cette clé. Toutefois, vous pouvez reconstruire votre clé si votre administrateur PGP a implémenté une stratégie de restauration de clé pour votre entreprise. Pour plus d'informations, consultez la section *Reconstruction de clé PGP* (cf. "Reconstruction de clés avec PGP Universal Server" à la page 86, "Perte de votre clé ou phrase secrète" à la page 86) et contactez votre administrateur PGP.

Distribution de votre clé publique

Après la création de votre paire de clés PGP Desktop, vous devez communiquer votre clé publique aux personnes avec lesquelles vous voulez échanger des messages chiffrés.

Vous rendez votre clé publique accessible aux autres afin qu'ils puissent vous envoyer des informations chiffrées et vérifier votre signature numérique ; et vous avez besoin de leur clé publique pour leur envoyer des messages chiffrés.

Vous pouvez distribuer votre clé publique de plusieurs façons :

- *Publication de votre clé sur le serveur PGP Global Directory* (cf. "Mise de votre clé publique sur un serveur de clés" à la page 51).

  Généralement, les autres méthodes sont inutiles une fois que votre clé est publiée dans cet annuaire.

- *Inclusion de votre clé publique dans un message électronique* (à la page 52).

- *Export de votre clé publique ou copie dans un fichier texte* (cf. "Exportation de votre clé publique dans un fichier" à la page 53).

Sur les systèmes Windows, vous pouvez aussi :

- *Copier directement d'une carte à puce vers le trousseau de clés de quelqu'un* (cf. "Copie directe d'une carte à puce vers le trousseau de clés de quelqu'un" à la page 53).

Mise de votre clé publique sur un serveur de clés

La meilleure méthode pour rendre votre clé publique accessible est de la mettre sur un serveur de clés publiques, une grande base de données de clés à laquelle chacun peut accéder. Ainsi, toute personne peut vous envoyer un courrier électronique chiffré sans avoir à vous demander expressément une copie de votre clé. La maintenance d'un grand nombre de clés publiques rarement utilisées vous est évitée, à vous ainsi qu'aux autres.

Un certain nombre de serveurs de clés existent dans le monde, y compris PGP Global Directory, où vous pouvez rendre votre clé accessible à quiconque. Si vous utilisez PGP Desktop dans un domaine protégé par le PGP Universal Server, votre administrateur PGP aura préconfiguré PGP Desktop avec les paramètres appropriés.

Quand vous utilisez un serveur de clés publiques, gardez ceci à l'esprit avant d'envoyer votre clé :

- Est-ce bien la clé que vous voulez utiliser ? Des personnes qui tentent de communiquer avec vous pourraient s'en servir pour chiffrer des informations importantes. Pour cette raison, nous vous recommandons fortement de ne mettre sur un serveur de clés que les clés destinées à être utilisées par d'autres personnes.
- Vous rappellerez-vous la phrase secrète qui correspond à cette clé pour récupérer les données chiffrées avec ladite clé ou, si vous ne voulez pas utiliser cette clé, pour la révoquer ?
- En dehors de PGP Global Directory, une fois qu'une clé est publiée, il n'est pas possible de revenir en arrière. Certains serveurs de clés publiques ont une politique contre la suppression de clés. D'autres possèdent des fonctionnalités de réplication qui copient les clés d'un serveur de clés à l'autre : même si vous pouvez supprimer votre clé d'un serveur, elle pourrait réapparaître ultérieurement.

La plupart des gens postent leur clé publique dans l'annuaire PGP Global Directory immédiatement après avoir créé leur paire de clés. Si vous avez déjà posté votre clé dans PGP Global Directory, il est inutile de recommencer. Dans la plupart des cas, il n'est pas utile de publier votre clé sur un autre serveur de clés quel qu'il soit. Remarque : il est possible que d'autres serveurs de clés ne vérifient pas les clés. Ainsi, les clés trouvées sur d'autre serveurs de clés peuvent exiger des efforts supplémentaires de votre part pour contacter le propriétaire de la clé à des fins de vérification d'empreinte digitale.

Pour envoyer manuellement votre clé publique à un serveur de clés

1 Ouvrez PGP Desktop.

2 Assurez-vous que la boîte de contrôle Clés PGP est sélectionnée.

3 Cliquez avec le bouton droit sur la paire de clés dont vous voulez envoyer la clé publique au serveur de clés.

4 Sélectionnez **Envoyer vers**, puis choisissez dans la liste le serveur de clés auquel vous voulez envoyer la clé publique. Si le serveur de clés auquel vous voulez envoyer votre clé publique ne figure pas dans la liste, reportez-vous à la section *Utilisation des serveurs de clés* (à la page 56). Une fois la clé publique copiée sur le serveur de clés, PGP Desktop vous en informe.

Dès que vous placez une copie de votre clé publique sur un serveur de clés, celle-ci peut-être utilisée par les personnes qui veulent vous envoyer des données chiffrées ou vérifier votre signature numérique. Même si vous n'indiquez pas explicitement où se trouve votre clé publique, vos interlocuteurs peuvent s'en procurer une copie grâce à votre nom ou à votre adresse de courrier électronique.

De nombreuses personnes indiquent l'adresse Web de leur clé publique à la fin de leurs messages électroniques. Dans la plupart des cas, il suffit au destinataire de double-cliquer sur cette adresse pour accéder à une copie de cette clé sur le serveur. Certaines personnes indiquent même leur empreinte numérique PGP sur leurs cartes de visite professionnelles.

Inclusion de votre clé publique dans un message électronique

Une autre méthode pratique pour communiquer votre clé publique à quelqu'un est de l'inclure dans un message électronique.

Quand vous envoyez votre clé publique à quelqu'un, assurez-vous de signer le message électronique. Ainsi, le destinataire peut vérifier votre signature et s'assurer que personne n'a falsifié les informations entre temps. Bien sûr, si votre clé n'a pas encore a été signée par un introducteur approuvé, les destinataires de votre signature ne peuvent véritablement s'assurer que la signature est de vous qu'en vérifiant l'empreinte digitale sur votre clé.

Pour inclure votre clé publique dans un message électronique

1 Dans PGP Desktop, assurez-vous que la boîte de contrôle Clés PGP est sélectionnée.

2 Cliquez avec le bouton droit sur la paire de clés dont vous voulez inclure la clé publique dans un message électronique.

3 Sélectionnez **Envoyer vers**, puis **Destinataire du message**. Votre application de messagerie électronique s'ouvre. Elle contient déjà vos informations de clé.

4 Adressez le message et envoyez-le.

Si cette méthode ne fonctionne pas pour vous, vous pouvez ouvrir PGP Desktop, sélectionner votre paire de clés, choisir **Edition > Copier**, ouvrir un message électronique, puis coller la clé publique dans le corps du message. Avec certaines applications de messagerie, il vous suffit de faire glisser votre clé depuis PGP Desktop vers le texte de votre message électronique pour transférer les informations liées à votre clé publique.

Exportation de votre clé publique dans un fichier

Une autre méthode de distribution de votre clé publique est de l'exporter vers un fichier puis de mettre ce fichier à disposition de la personne avec qui vous voulez communiquer de manière sécurisée.

Il y a trois façons d'exporter ou d'enregistrer votre clé publique dans un fichier :

- Sélectionnez votre paire de clés, puis **Fichier > Exporter**. Saisissez un nom et un emplacement de fichier, puis cliquez sur **Enregistrer**. Assurez-vous de *ne pas* inclure votre clé privée avec votre clé publique si vous prévoyez de donner ce fichier à d'autres personnes.
- Ctrl+cliquez sur la clé que vous voulez enregistrer dans un fichier, sélectionnez **Exporter** dans la liste, saisissez un nom et un emplacement de fichier, puis cliquez sur **Enregistrer**. Assurez-vous de *ne pas* inclure votre clé privée avec votre clé publique si vous prévoyez de donner ce fichier à d'autres personnes.
- Sélectionnez votre paire de clés, puis **Modifier > Copier**. Ouvrez un éditeur de texte et sélectionnez **Coller** pour insérer les informations sur la clé dans le fichier texte, puis enregistrez le fichier. Vous pouvez ensuite envoyer ce fichier par courrier électronique ou le donner à qui vous voulez. Le destinataire doit utiliser PGP Desktop sur son système afin de récupérer la partie de clé publique.

Copie directe d'une carte à puce vers le trousseau de clés de quelqu'un

Si votre clé publique est stockée sur une carte à puce, une autre méthode de distribution est de la copier de la carte à puce directement dans le trousseau de clés de quelqu'un.

Pour plus d'informations sur la manière de le faire, reportez-vous à la section *Copie de la clé publique d'une carte à puce sur un trousseau de clés* (cf. "Copie de votre clé publique d'une carte à puce sur un trousseau de clés" à la page 306).

Obtention de clés publiques d'autres personnes

Tout comme vous devez distribuer votre clé publique à ceux qui veulent vous envoyer du courrier chiffré ou vérifier votre signature numérique, vous devez obtenir les clés publiques des autres pour leur envoyer du courrier chiffré ou vérifier leurs signatures numériques.

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

- Récupération automatique de la clé vérifiée dans le PGP Global Directory
- Recherche manuelle de la clé sur un serveur de clés publiques
- Ajout automatique de la clé publique à votre trousseau de clés directement à partir d'un message électronique
- Importation de la clé publique à partir d'un fichier exporté
- Obtention de la clé dans le serveur PGP Universal Server de votre société

Les clés publiques sont de simples blocs de texte. Elles sont donc faciles à ajouter à votre trousseau de clés soit en les important d'un fichier, soit en les copiant d'un message électronique puis en les collant dans votre trousseau de clés publiques dans PGP Desktop.

Obtention de clés publiques sur un serveur de clés

Si la personne à qui vous voulez envoyer du courrier chiffré est un utilisateur expérimenté de PGP Desktop, une copie de sa clé publique se trouve probablement dans PGP Global Directory ou dans un autre serveur de clés publiques. Il vous est donc très aisé d'obtenir une copie de sa clé la plus récente quand vous voulez lui envoyer un message électronique. De plus, cela vous évite de devoir stocker un grand nombre de clés publiques sur votre trousseau de clés publiques.

Il existe un certain nombre de serveurs de clés publiques, comme PGP Global Directory dont la maintenance est assurée par PGP Corporation, où vous pouvez localiser les clés de la plupart des utilisateurs de PGP. Si le destinataire ne vous a pas indiqué d'adresse Web où trouver sa clé publique, vous pouvez accéder à n'importe quel serveur de clés et lancer une recherche sur le nom de l'utilisateur ou son adresse électronique. Il est possible que vous n'obteniez pas de résultat puisque tous les serveurs de clés publiques ne sont pas régulièrement mis à jour avec les données des clés stockées sur l'ensemble des autres serveurs.

Si votre ordinateur se trouve dans un domaine protégé par un PGP Universal Server, votre administrateur PGP peut vous demander d'utiliser le serveur de clés intégré au PGP Universal Server. Dans ce cas, votre logiciel PGP Desktop est probablement déjà configuré pour accéder au PGP Universal Server approprié.

De même, le PGP Universal Server est configuré par défaut pour communiquer avec le PGP Global Directory. De cette façon, l'écosystème PGP distribue la charge de la recherche et de la vérification des clés.

Pour récupérer la clé publique d'un tiers à partir d'un serveur de clés

1. Ouvrez PGP Desktop et activez la boîte de contrôle Clés PGP.
2. Choisissez **Rechercher des clés** dans le panneau de contrôle Clés PGP. L'écran Rechercher des clés s'affiche dans la zone de travail.
3. Indiquez vos critères de recherche, puis cliquez sur **Rechercher**. Si vous voulez limiter la recherche à un serveur de clés spécifique, cliquez dans le champ **Rechercher** et sélectionnez le serveur de clés approprié. Si le serveur de clés souhaité ne figure pas dans la liste, choisissez **Modifier la liste des serveurs de clés** et ajoutez-le.

   Vous pouvez rechercher des clés dans un serveur de clés en spécifiant des valeurs pour plusieurs caractéristiques de clé. L'inverse de la plupart des opérations est également possible. Vous pouvez ainsi utiliser le critère « L'ID d'utilisateur n'est pas Charles ».

   Les résultats de la recherche s'affichent.
4. Si vous avez trouvé une clé publique à ajouter à votre trousseau de clés, cliquez sur **Ajouter à mon trousseau de clés** dans le panneau de contrôle Clés PGP. La clé sélectionnée est ajoutée à votre trousseau.

Conseil : si votre critère de recherche correspond à un prénom très courant (par exemple, Nom, contient, Jean), seule la première correspondance trouvée est retournée. Ceci permet d'éviter le hameçonnage (ou la récolte des clés d'un serveur de clés). Pour les noms ou les domaines courants, vous aurez peut-être à indiquer le nom complet ou l'adresse de courrier électronique afin de trouver la bonne clé.

Obtention de clés publiques par message électronique

Une autre moyen simple d'obtenir une copie de la clé publique d'une personne est de lui demander de la joindre à un message électronique.

Pour ajouter une clé publique jointe à un message électronique

1. Ouvrez le message électronique.
2. Double-cliquez sur le fichier `.asc` qui inclut la clé publique. PGP Desktop reconnaît le format du fichier et ouvre la boîte de dialogue Sélectionner une ou des clés.
3. Si vous y êtes invité, choisissez d'ouvrir le fichier.
4. Sélectionnez la ou les clés publiques que vous voulez ajouter à votre trousseau de clés puis cliquez sur **Importer**.

Utilisation des serveurs de clés

PGP Desktop reconnaît les types de serveurs de clés suivants :

- **Serveurs de clés PGP Universal** : Si vous utilisez PGP Desktop dans un domaine protégé par un PGP Universal Server, PGP Desktop est préconfiguré pour communiquer uniquement avec le serveur de clés intégré au PGP Universal Server avec lequel il a un lien. Pour PGP Desktop, il s'agit d'un serveur de clés approuvé. PGP Desktop approuve automatiquement toute clé trouvée sur ce serveur de clés à moins que le PGP Universal Server ne lui indique que la clé n'est pas approuvée, ce qui peut par exemple arriver lors de la vérification de signatures de clés distantes.

  L'adresse de votre serveur de clés PGP Universal peut ressembler à : https://serveurcles.exemple.com.

- **PGP Global Directory** : Si vous utilisez PGP Desktop à l'extérieur d'un domaine protégé par un PGP Universal Server, PGP Desktop est préconfiguré pour communiquer avec *PGP Global Directory* (https://keyserver.pgp.com).

  PGP Global Directory est un serveur de clés publiques gratuit hébergé par PGP Corporation. Il offre un accès rapide et facile à l'ensemble des clés PGP. Il utilise la technologie de serveur de clé nouvelle génération qui vérifie la clé associée à chaque adresse de courrier électronique (de façon que le serveur de clés soit pas engorgé par des clés inutilisées, plusieurs clés par adresse électronique, des clés contrefaites, et d'autres problèmes dont les anciens serveurs de clés souffraient), et vous permet de gérer vos propres clés, y compris de remplacer votre clé, de la supprimer et d'y ajouter des adresses électroniques. L'utilisation de PGP Global Directory améliore significativement vos chances de trouver la clé publique d'une personne avec qui vous voulez échanger des messages sécurisés.

  Pour PGP Desktop, PGP Global Directory est un serveur de clés approuvé, PGP Desktop approuvera automatiquement toute clé qu'il y trouve. Pendant la connexion initiale à PGP Global Directory, la clé de vérification de PGP Global Directory est téléchargée, signée et approuvée par la clé que vous publiez dans l'annuaire. La clé PGP Global Directory est aussi ajoutée à votre trousseau de clés. Toutes les clés vérifiées par PGP Global Directory sont ainsi considérées comme valides par PGP Desktop.

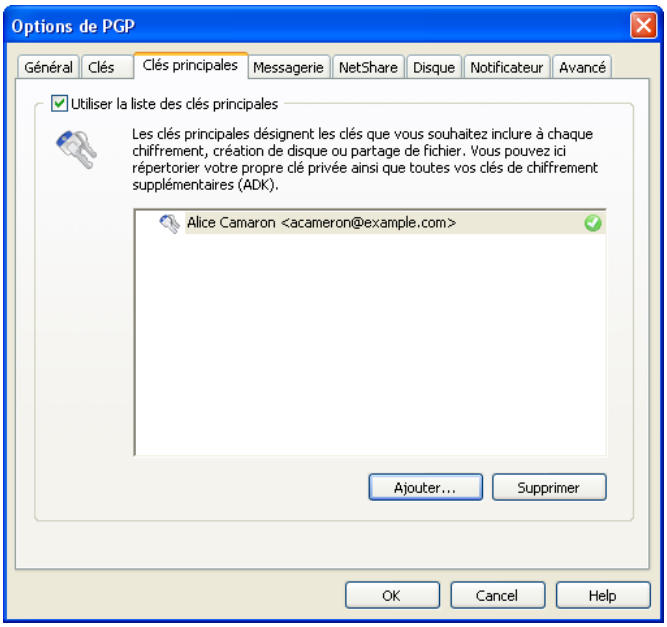
  Protocole des services de PGP Universal : Le protocole des services de PGP Universal (USP) est un protocole SOAP qui fonctionne sur les ports HTTP/HTTPS standard. Il s'agit du mécanisme de recherche de clé par défaut. Si vous vous trouvez dans un environnement géré par un PGP Universal Server, toutes les demandes de recherche de clé, ainsi que les autres communications entre le PGP Universal Server et PGP Desktop, utilisent le protocole PGP USP.

- **Autre serveurs de clés** : dans la plupart des cas, les autres serveurs de clés sont aussi des serveurs de clés publiques. Cependant, vous pouvez avoir accès, par votre entreprise ou quelque autre moyen, à un serveur de clés privées.

Pour plus d'informations sur l'utilisation des serveurs de clés, reportez-vous à la section *Options des clés* (cf. "Options de l'onglet Clés" à la page 316).

Utilisation de clés principales

La liste des clés principales est un ensemble de clés que vous souhaitez voir ajoutées par défaut chaque fois que vous choisissez des clés pour la messagerie, le chiffrement de disque, PGP NetShare et PGP Zip. Elle vous permet de ne pas avoir à faire glisser dans le champ **Destinataires** les clés que vous utilisez régulièrement.



Remarque : si vous avez généré votre clé à l'aide de l'assistant d'installation, celle-ci est automatiquement ajoutée à la liste des clés principales. Si, en revanche, vous avez importé votre clé dans PGP Desktop, elle n'est pas automatiquement ajoutée à la liste.

Ajout de clés à la liste des clés principales

▸ **Pour ajouter des clés à la liste des clés principales**

1. Dans PGP Desktop, sélectionnez **Outils > Options**.
2. Cliquez sur l'onglet Clés principales.

3 Pour utiliser la liste des clés principales, cochez la case **Utiliser la liste des clés principales**. Vous ne pouvez pas ajouter de clés à cette liste, ou en supprimer, si vous n'avez pas coché cette case.

4 Cliquez sur **Ajouter**. La boîte de dialogue Sélectionner des clés principales s'affiche.

5 Dans la liste **Source de clé** à gauche, cliquez pour sélectionner les clés à utiliser. Pour sélectionner plusieurs clés, cliquez sur leur nom tout en maintenant la touche Maj ou Ctrl enfoncée.

6 Une fois que vous avez sélectionné les clés de votre choix, cliquez sur **Ajouter**.

Conseil : si vous ne voulez pas inclure certaines clés de la liste **Clés à ajouter** à droite, sélectionnez-les et cliquez sur **Supprimer**.

7 Lorsque vous avez terminé de sélectionner des clés, cliquez sur **OK**. Les clés que vous avez sélectionnées apparaissent dans la liste des clés principales.

Suppression de clés de la liste des clés principales

▸ **Pour supprimer des clés de la liste des clés principales**

1 Dans PGP Desktop, sélectionnez **Outils > Options**.

2 Cliquez sur l'onglet Clés principales.

3 Pour utiliser la liste des clés principales, cochez la case **Utiliser la liste des clés principales**. Vous ne pouvez pas ajouter de clés à cette liste, ou en supprimer, si vous n'avez pas coché cette case.

4 Sélectionnez la ou les clés à supprimer. Pour sélectionner plusieurs clés, vous pouvez cliquer sur leur nom tout en maintenant la touche Maj ou Ctrl enfoncée.

5 Cliquez sur **Supprimer**. La ou les clés sont supprimées.

6 Gestion des clés PGP

Cette section décrit le mode de gestion des clés avec PGP Desktop.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

Examen et paramétrage des propriétés de la clé

La zone de travail des clés PGP peut contenir les détails importants ci-dessous sur vos clés :

- Nom
- Adresse de courrier électronique
- Validité
- Taille
- ID de clé
- Confiance
- Date de création
- Date d'expiration
- Clé de déchiffrement supplémentaire (ADK)
- État
- Description de clé
- Utilisation de la clé

Vous pouvez choisir la quantité de détails présentés en cliquant sur l'élément **Clés**, puis en sélectionnant **Afficher > Colonnes** afin de décider des colonnes à afficher.

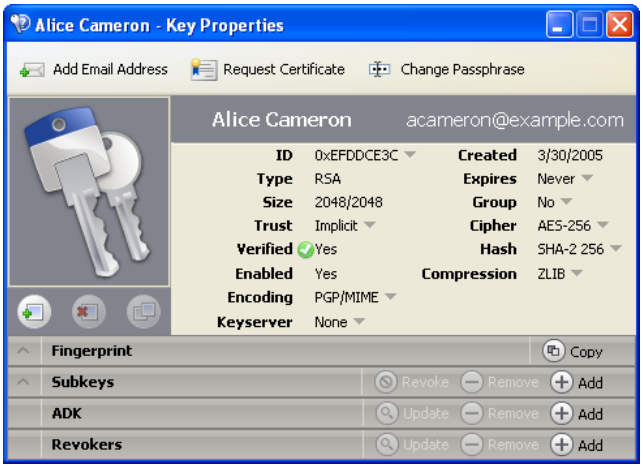
Vous pouvez accéder à des informations supplémentaires sur une clé et modifier certaines informations dans les propriétés de la clé.

Remarque : si votre ordinateur se trouve dans un environnement géré par un PGP Universal Server et que votre mode clé soit SKM, vous ne pouvez pas modifier votre clé. En outre, les clés SKM sont configurées pour ne jamais expirer. Pour identifier le mode clé utilisé, reportez-vous à la section *Modes clé* (à la page 133).

Pour afficher les propriétés d'une clé

1 Ouvrez PGP Desktop, cliquez sur le panneau de contrôle Clés PGP, puis sélectionnez **Toutes les clés**. Toutes les clés de votre trousseau s'affichent.

2 Double-cliquez sur la clé dont vous voulez afficher les propriétés. La boîte de dialogue Propriétés de la clé pour la clé choisie s'affiche.



Utilisation d'ID photographiques

Vous pouvez inclure un ID photographique sur vos clés Diffie-Hellman/DSS et RSA.

Pour ajouter votre photographie à la clé

1 Ouvrez PGP Desktop, cliquez sur le panneau de contrôle Clés PGP, puis sélectionnez **Mes clés privées**.

2 Dans la zone de travail des clés PGP, double-cliquez sur la clé privée à laquelle ajouter l'ID photo. La boîte de dialogue Propriétés de la clé de la clé sélectionnée s'affiche.

3 Cliquez avec le bouton droit sur l'icône des silhouettes de clés et sélectionnez **Ajouter un ID Photo**. La boîte de dialogue Ajouter un ID Photo s'affiche.

4 Faites glisser ou coller votre photographie dans la boîte de dialogue Ajouter photo ou parcourez les fichiers en cliquant sur **Sélectionner fichier**.

5 Cliquez sur **OK**. La boîte de dialogue Phrase secrète s'ouvre.

6 Saisissez la phrase secrète de la clé que vous modifiez, puis cliquez sur **OK**. Votre ID photo est ajouté à votre clé publique.

Pour supprimer un ID photo

- Cliquez avec le bouton droit sur la photo actuelle dans la boîte de dialogue Propriétés de la clé et sélectionnez **Supprimer l'ID photo**. La photo est supprimée de la clé.

Pour copier un ID photo

- Cliquez avec le bouton droit sur la photo actuelle dans la boîte de dialogue Propriétés de la clé et sélectionnez **Copier l'ID photo**. Vous pouvez ensuite coller la photo dans une autre clé ou dans un programme graphique.

Gestion des noms d'utilisateur et des adresses de courrier électronique d'une clé

PGP Desktop prend en charge plusieurs noms et adresses de courrier électronique sur votre paire de clés. Ces noms et adresses de courrier électronique aident les autres à trouver votre clé pour vous envoyer des messages chiffrés.

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

1. Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP, puis sélectionnez **Mes clés privées**.
2. Dans la zone de travail Clés PGP, double-cliquez sur la clé privée à laquelle vous voulez ajouter un nom d'utilisateur ou une adresse de courrier électronique. La boîte de dialogue Propriétés de la clé de la clé choisie s'affiche.
3. Cliquez sur **Ajouter une adresse de courrier électronique**. La boîte de dialogue Nom nouvel utilisateur PGP apparaît.
4. Tapez le nouveau nom et la nouvelle adresse de courrier électronique dans les champs appropriés, puis cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète de la clé PGP s'affiche.
5. Saisissez la phrase secrète de clé privée de la clé que vous êtes en train de modifier, puis cliquez sur **OK**.
6. Pour définir le nouveau nom d'utilisateur et la nouvelle adresse en tant qu'identificateur principal de la clé, cliquez sur le nom du détenteur de clé principal actuel dans la boîte de dialogue Propriétés de la clé, puis sélectionnez l'utilisateur que vous venez d'ajouter.
7. Quittez la boîte de dialogue Propriétés de la clé. Dans la liste de clés de PGP Desktop, le nouveau nom est ajouté à la fin de la liste des noms d'utilisateurs associée à la clé.

Pour changer le nom principal associé à votre clé

1. Effectuez l'une des opérations ci-dessous :

- Dans la boîte de dialogue Propriétés de la clé, cliquez sur le nom du détenteur principal actuel et sélectionnez le nom de l'utilisateur dans la liste qui s'affiche.
- Dans PGP Desktop, développez votre clé dans la liste, cliquez avec le bouton droit sur le nom de l'utilisateur à définir en tant qu'identificateur principal, puis choisissez **Définir en tant que nom primaire** dans le menu contextuel.

Pour supprimer un nom ou une adresse de courrier électronique de votre paire de clés

1. Dans la liste des clés, cliquez sur le signe plus situé à gauche du nom de la clé à développer.
2. Sélectionnez l'ID d'utilisateur à supprimer.
3. Appuyez sur la touche Supprimer de votre clavier. Une boîte de dialogue de confirmation apparaît.

   Conseil : vous pouvez également sélectionner **Edition > Supprimer** (sous Windows) ou **Edition > Effacer** (sous Mac OS X).
4. Cliquez sur **Supprimer**. L'ID d'utilisateur est supprimé.

Importation de clés et certificats X.509

Vous pouvez importer des clés publiques PGP et des certificats X.509 et PKCS-12 (un format de certificat numérique utilisé par la plupart des navigateurs) dans votre trousseau de clés PGP Desktop, ainsi que des certificats X.509 publics PKCS-7. Vous pouvez aussi importer les certificats X.509 au format de messagerie avec confidentialité renforcée (PEM) de votre navigateur en effectuant un copié-collé vers votre trousseau de clés publiques.

Il y a de nombreuses façons d'importer la clé publique PGP d'une personne et de l'ajouter à votre trousseau de clés. Ces méthodes comprennent :

- Double-cliquer sur le fichier dans votre système. Si PGP Desktop reconnaît le format du fichier, il l'ouvrira et vous demandera si vous voulez importer la ou les clés dans le fichier.
- Importer le fichier de clé dans PGP Desktop.
- Faire glisser le fichier contenant la clé publique dans la fenêtre Clés PGP.

L'assistant d'importation de certificat de PGP Desktop vous aidera dans cette tâche. Pour plus d'informations, reportez-vous à la section *Utilisation de l'assistant d'importation de certificat* (à la page 64).

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server et que vous avez importé un certificat X.509 sur un jeton au cours de l'inscription (en choisissant d'importer le certificat en tant que clé PGP), vous devez activer manuellement l'option **Synchroniser le trousseau de clés avec les jetons et les cartes à puce**. Pour ce faire, dans PGP Desktop, sélectionnez **Outils > Options**, puis cliquez sur l'onglet Clés. Cette étape est indispensable pour que la clé fonctionne correctement avec PGP Whole Disk Encryption.

Utilisation de l'assistant d'importation de certificat

Les certificats X. 509 peuvent être importés dans PGP Desktop à partir de fichiers, de la banque de certificats personnels Windows ou de cartes à puce. Il est même possible d'importer les certificats basés sur une carte à puce et qui sont affichés dans votre banque de certificats personnels Windows. L'assistant d'importation de certificat vous guide tout au long du processus d'importation.

Lors de l'importation de certificats à partir de fichiers, le certificat ne peut être importé que d'un fichier dont l'extension est PEM, PFX, P7b ou P12.

Remarque : lorsque vous utilisez des certificats de la banque de certificats personnels Windows, ce dernier peut vous inviter à entrer le mot de passe de votre certificat ou votre code confidentiel (si vous utilisez une carte à puce basée sur les certificats personnels Windows l'invite vient alors du logiciel tiers de la carte à puce).

Certaines opérations, comme la modification du mot de passe du certificat, ne sont pas autorisées à partir de PGP Desktop lorsque les certificats de la banque de certificats personnels Windows sont utilisés. Utilisez le logiciel Windows (ou de la carte à puce) pour effectuer telles opérations.

Pour importer un certificat avec de l'assistant d'importation de certificat

Avant de commencer : Assurez-vous que vous connaissez la phrase secrète pour le certificat que vous importez.

1. Démarrez l'assistant :
   - Sélectionnez **Fichier > Ouvrir**.
   - Sélectionnez **Fichier > Importer certificats personnels**.
   - Faites glisser le fichier contenant la clé publique dans la fenêtre Clés PGP.
2. Si vous utilisez PGP Desktop dans un environnement géré par le PGP Universal Server et que votre administrateur a défini que vous pouviez choisir la méthode d'importation du certificat, sélectionnez :
   - **Sur une clé existante** — le certificat est ajouté à une clé qui se trouve déjà dans votre trousseau de clés.

- **En tant que nouvelle ou nouvelles clés PGP** — une nouvelle clé PGP est créée avec le certificat importé.
- **En tant que clé(s) wrapper PGP X.509** — une nouvelle clé PGP est créée avec le certificat importé. PGP Desktop traite la nouvelle clé comme un certificat X.509.

3 Une fois votre sélection faite, cliquez sur **Suivant**. L'écran Saisie de la phrase secrète du Certificat ou la boîte de dialogue Saisissez la phrase secrète PGP s'affiche.

4 Saisissez le mot de passe du certificat, puis cliquez sur **Suivant**.

- Si vous importez le certificat avec l'option **Sur une clé existante**, l'écran **Sélectionner une clé** s'affiche. Rendez-vous à la prochaine étape.
- Si vous importez le certificat avec l'option **En tant que nouvelle ou nouvelles clés PGP**, la clé est générée. Cliquez sur **Terminer**. Le processus est terminé.
- Si vous importez le certificat avec l'option **En tant que clé(s) wrapper PGP X.509**, la boîte de dialogue Sélectionner une ou des clés s'affiche. Cliquez pour sélectionner la clé, cliquez sur Importer et la clé wrapper PGP X.509 est générée. Le processus est terminé.

5 Pour terminer l'importation du certificat avec l'option **Sur une clé existante**, dans la boîte de dialogue **Sélectionner une clé, sélectionnez la clé dans laquelle vous souhaitez importer le certificat puis saisissez le mot de passe pour la clé. Cliquez sur Suivant**.

6 La boîte de dialogue Progression de la génération de clé s'affiche alors que le certificat est importé sur la clé.

7 Cliquez sur **Terminer**. Le processus est terminé.

Modification de votre phrase secrète

Il est conseillé de modifier régulièrement la phrase secrète, par exemple tous les trois mois. Il est encore plus important de modifier votre phrase secrète dès que vous pensez qu'elle a été interceptée, par exemple par quelqu'un qui regardait par-dessus votre épaule lorsque vous la saisissiez sur le clavier.

Pour modifier la phrase secrète pour une clé scindée, vous devez d'abord réassembler celle-ci.

Conseil : lorsque vous modifiez votre phrase secrète sur votre clé, cette dernière n'est pas modifiée sur les copies de la clé (comme les sauvegardes que vous pourriez avoir faites). Si vous pensez que votre clé a été compromise, PGP Corporation recommande de décomposer toute copie de sauvegarde précédemment effectuée et de procéder à de nouvelles copies de sauvegarde de la clé.

Si votre ordinateur se trouve dans un environnement géré par un PGP Universal Server et que votre mode clé soit SKM, vous ne pouvez pas modifier la phrase secrète associée à votre clé. Les clés SKM sont protégées par une phrase secrète générée de façon aléatoire (qui est elle-même protégée) et vous n'êtes jamais invité à saisir une phrase secrète pour ce type de clé. Pour identifier le mode clé utilisé, reportez-vous à la section *Modes clé* (à la page 133).

Pour changer votre phrase secrète de clé privée

1. Ouvrez PGP Desktop, cliquez sur le panneau de contrôle Clés PGP, puis sélectionnez **Mes clés privées**.
2. Dans la zone de travail Clés PGP, double-cliquez sur la clé privée dont vous voulez changer la phrase secrète. La boîte de dialogue Propriétés de la clé s'affiche.
3. Cliquez sur **Modifier la phrase secrète**. L'assistant de phrase secrète PGP apparaît.
4. Saisissez la phrase secrète actuelle de la clé privée, puis cliquez sur **Suivant.** La boîte de dialogue Créer une phrase secrète s'affiche.
5. Indiquez votre nouvelle phrase secrète dans le premier champ de texte, puis saisissez-la une deuxième fois dans le champ **Confirmer la phrase secrète** de façon à la confirmer.

   Pour visualiser ce que vous tapez, cochez la case **Afficher les frappes**.

   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* (à la page 336).
6. Cliquez sur **Terminer.** Votre phrase secrète a été changée.

Suppression de clés, d'ID d'utilisateur et de signatures

PGP Desktop vous permet de contrôler les clés de vos trousseaux de clés, ainsi que les ID d'utilisateurs et les signatures sur ces clés.

Avec les clés publiques sur vos trousseaux de clés, vous pouvez supprimer des clés entières, n'importe quel ID d'utilisateur d'une clé, et n'importe quelle signature ou toutes les signatures d'une clé.

Avec vos paires de clés, vous pouvez supprimer des paires de clés entières, ou n'importe quelle signature ou toutes les signatures ; ainsi que supprimer les ID d'utilisateurs d'une paire de clés tant qu'il ne s'agit pas du seul ID d'utilisateur de la paire de clés.

Remarque : vous ne pouvez cependant pas effacer un ID d'utilisateur d'une clé s'il s'agit du seul ID d'utilisateur, et vous ne pouvez pas supprimer les auto-signatures des clés.

Pour supprimer une clé, un ID d'utilisateur ou une signature de votre trousseau de clés PGP

1. Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP, puis sélectionnez **Toutes les clés** dans le panneau de contrôle. Toutes les clés de votre trousseau s'affichent.
2. Effectuez l'une des opérations ci-dessous :
   - Pour supprimer une clé, cliquez avec le bouton droit sur cette clé, sélectionnez **Supprimer** dans la liste de commandes qui s'affiche, puis cliquez sur **OK** dans la boîte de dialogue Confirmation. La clé est supprimée de votre trousseau.
   - Pour supprimer un ID d'utilisateur (d'une clé publique) ou une signature, cliquez sur le signe plus situé à gauche de la clé pour afficher les ID d'utilisateurs et signatures. Cliquez avec le bouton droit sur l'ID d'utilisateur ou la signature à supprimer, sélectionnez **Supprimer** dans la liste de commandes qui s'affiche, puis cliquez sur **OK** dans la boîte de dialogue Confirmation. L'ID d'utilisateur ou la signature est supprimé.

Désactivation et activation des clés publiques

Parfois, vous pouvez souhaiter désactiver temporairement une clé publique de votre trousseau de clés. Cela peut s'avérer utile si vous souhaitez garder une clé publique pour une utilisation ultérieure, mais que vous ne vouliez pas qu'elle encombre la liste de vos destinataires à chaque fois que vous envoyez un courrier électronique.

Vous ne pouvez pas désactiver une paire de clés « implicitement approuvée ». Pour désactiver une clé définie comme implicitement approuvée, vous devez d'abord changer son état de confiance en **Aucun**.

Pour désactiver ou activer une clé publique

1. Ouvrez PGP Desktop, cliquez sur le panneau de contrôle Clés PGP, puis sélectionnez **Toutes les clés**. Toutes les clés de votre trousseau s'affichent.
2. Double-cliquez sur la clé publique que vous voulez désactiver. La boîte de dialogue Propriétés de la clé pour la clé choisie s'affiche.
3. Localisez le champ **Activé** dans les propriétés de la clé.

- Si le paramètre actuel du champ **Activé** est **Oui**, la clé est activée. Pour désactiver la clé, cliquez une fois sur **Oui**. Le champ **Activé** prend alors la valeur **Non** et la clé est désactivée.
- Si le paramètre actuel du champ **Activé** est **Non**, la clé est désactivée. Pour activer la clé, cliquez une fois sur **Non**. Le champ **Activé** prend alors la valeur **Oui** et la clé est activée.

Une clé désactivée ne peut pas être utilisée pour chiffrer ou signer. Néanmoins, elle peut l'être pour déchiffrer ou vérifier.

Conseil : vous pouvez également synchroniser des clés de votre trousseau avec le PGP Universal Server. Cette option permet essentiellement d'activer ou de désactiver des clés publiques de votre trousseau. Pour ce faire, cliquez avec le bouton droit sur une clé et sélectionnez **Synchroniser**.

Vérification d'une clé publique

Il est difficile de savoir à coup sûr si une clé publique appartient à une personne en particulier sauf si cette personne vous remet la clé en mains propres sur un support amovible ou si vous la trouvez dans PGP Global Directory. L'échange de clés sur les supports amovibles médias n'est généralement pas pratique, surtout pour les utilisateurs qui se trouvent à des kilomètres les uns des autres.

La question reste entière : comment s'assurer que la clé publique obtenue d'un serveur de clés publiques (et non de PGP Global Directory) est vraiment la clé publique de la personne indiquée sur la clé ? La réponse est : vous devez vérifier l'empreinte digitale de la clé.

Il y a plusieurs façons de vérifier l'empreinte digitale d'une clé, mais la plus sûre est d'appeler la personne et de lui demander de vous lire l'empreinte digitale par téléphone. Sauf si cette personne est la cible d'une attaque, la probabilité que cet appel puisse être intercepté et la personne imitée est extrêmement basse. Vous pouvez aussi comparer l'empreinte digitale sur votre copie de la clé publique de quelqu'un à celle trouvée sur sa clé originale stockée dans un serveur public.

Il y a deux façons de voir l'empreinte digitale : dans une liste unique de mots ou dans un format hexadécimal.

Pour consulter l'empreinte numérique d'une clé publique

1. Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP, puis sélectionnez **Toutes les clés** dans le panneau de contrôle.

   Toutes les clés de votre trousseau s'affichent.

2. Double-cliquez sur la clé publique dont vous voulez consulter l'empreinte numérique. La boîte de dialogue Propriétés de la clé pour la clé choisie s'affiche.

L'empreinte numérique de la clé apparaît sous le nom et l'adresse de courrier électronique, au format hexadécimal (10 ensembles de quatre caractères) ou au format de listes de mots (quatre colonnes de cinq mots uniques).

3 Comparez l'empreinte de la clé à l'empreinte d'origine. Si les deux empreintes sont identiques, il s'agit de la véritable clé. Sinon, il ne s'agit *pas* de la véritable clé.

La liste de mots est constituée de mots d'authentification spéciaux utilisés par PGP Desktop, qui sont soigneusement sélectionnés en fonction de leur distinction phonétique et de la facilité de leur compréhension sans ambiguïté phonétique.

La liste de mots a un objectif similaire à l'alphabet militaire, qui permet aux pilotes de transmettre des informations de façon distincte par le biais d'un canal radio bruyant.

4 Si vous possédez une clé contrefaite, supprimez-la.

5 Ouvrez votre navigateur Web, accédez au *PGP Global Directory* (https://keyserver.pgp.com) et recherchez la véritable clé publique.

Signature d'une clé publique

Quand vous créez une paire de clés, les clés sont automatiquement signées. De même, une fois que vous êtes sûr qu'une clé appartient à la bonne personne, vous pouvez signer la clé publique de cette personne et indiquer ainsi que vous avez vérifié la clé. Quand vous signez la clé publique de quelqu'un, une icône de signature et votre nom d'utilisateur apparaissent sur cette clé.

Si vous importez une paire de clés d'une sauvegarde ou d'un ordinateur différent, il est possible que cette paire de clés doive aussi être signée.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, la fonctionnalité de signature de clé peut être désactivée.

Pour signer la clé d'un tiers

1 Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP, puis sélectionnez **Toutes les clés** dans le panneau de contrôle. Toutes les clés de votre trousseau s'affichent.

2 Effectuez l'une des opérations ci-dessous :

- Dans le menu **Clés**, sélectionnez **Signer**.
- Cliquez avec le bouton droit sur la clé à signer et sélectionnez **Signer** dans la liste de commandes qui s'affiche.

La boîte de dialogue Clé de signature PGP s'affiche. Elle contient le nom d'utilisateur/l'adresse de courrier électronique, ainsi que l'empreinte hexadécimale.

3 Cochez la case **Autoriser l'exportation de la signature** pour permettre l'exportation de votre signature avec la clé.

Une signature exportable est une signature qui peut être envoyée à des serveurs et qui se déplace avec la clé à chaque exportation. Elle peut ainsi être glissée jusqu'à un message électronique. Cette case constitue un moyen rapide d'indiquer que vous voulez exporter votre signature afin que d'autres personnes puissent avoir confiance en celle-ci et donc en vos clés.

4 Cliquez sur **Plus de choix** pour configurer des options telles que le type de signature et la date d'expiration.

5 Choisissez un type de signature pour signer la clé publique. Les options disponibles sont les suivantes :

- **Non exportable** : utilisez cette signature lorsque vous pensez que la clé est valide, mais que vous ne voulez pas que des tiers dépendent de votre certification. Ce type de signature ne peut pas être exporté ni envoyé à un serveur de clés avec la clé associée.
- **Exportable** : utilisez des signatures exportables lorsque votre signature est envoyée avec la clé au serveur de clés, afin que d'autres personnes puissent avoir confiance en votre signature et donc en vos clés. Cette option donne le même résultat que l'activation de la case **Autoriser l'exportation de la signature** dans le menu des clés de signature.
- **Méta-introducteur non exportable** : cette option certifie que cette clé et toutes les clés signées à l'aide de celle-ci avec une assertion de validité d'introducteur approuvé sont des introducteurs de toute confiance. Ce type de signature est non exportable.
- **L'introducteur approuvé est exportable** : utilisez cette signature lorsque vous certifiez que cette clé est valide et que le propriétaire de la clé doit être entièrement approuvé pour pouvoir attester d'autres clés. Ce type de signature est exportable. Vous pouvez limiter les capacités de validation de l'introducteur approuvé à un domaine de messagerie spécifique.

6 L'option **Niveau de confiance maximal** vous permet d'identifier le nombre de niveaux d'imbrication des introducteurs approuvés. Ainsi, si vous la définissez sur 1, il ne peut y avoir qu'un seul niveau d'introducteurs en dessous de la clé de l'introducteur méta.

7 Si vous voulez limiter les capacités de validation de clé de l'introducteur approuvé à un seul domaine, tapez le nom de ce domaine dans la zone de texte **Restriction de domaine**.

8 Dans le champ **Expiration**, sélectionnez **Jamais** si vous ne voulez pas que cette signature possède une date d'expiration, ou sélectionnez une date d'expiration.

9 Cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète de la clé PGP s'affiche.

10 Sélectionnez la clé avec laquelle vous voulez signer dans la liste, puis tapez la phrase secrète de la clé de signature, le cas échéant. (Si la phrase secrète est déjà mise en cache, vous n'avez pas besoin de la saisir à nouveau.)

11 Cliquez sur **OK**. La clé est signée.

Révocation de votre signature à partir d'une clé publique

Il se peut que vous vouliez, ou ayez besoin de, révoquer votre signature à partir d'une clé de votre trousseau.

Pour révoquer votre signature

1 Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP, puis sélectionnez **Toutes les clés** dans le panneau de contrôle. Toutes les clés de votre trousseau s'affichent.

2 Développez la clé à partir de laquelle vous voulez révoquer votre signature jusqu'à ce que votre clé de signature s'affiche.

3 Cliquez avec le bouton droit sur votre clé de signature, plus sélectionnez **Révoquer** dans la liste d'options affichée. La boîte de dialogue Révoquer la signature s'affiche.

4 Vérifiez que l'ID et le nom de clé correspondent à la clé correcte (à partir de laquelle vous souhaitez révoquer la signature) et cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète de la clé PGP s'affiche.

5 Saisissez votre phrase secrète, puis cliquez sur **OK**. Votre signature est révoquée à partir de la clé.

Remarque : si votre signature était exportable et que vous avez distribué la clé avec celle-ci, vous devez distribuer la clé à l'aide de la clé révoquée pour que les autres utilisateurs puissent voir la révocation.

Attribution de confiance pour les validations de clés

En plus de certifier qu'une clé appartient à quelqu'un, vous pouvez assigner un niveau de confiance au propriétaire des clés, et indiquer ainsi le degré de confiance que vous lui accordez en tant qu'introducteur d'autres personnes dont les clés vous seront peut-être fournies ultérieurement.

Ceci signifie que si jamais vous obtenez une clé d'une personne signée par quelqu'un que vous avez désigné comme digne de confiance, la clé est considérée valide bien que vous n'ayez pas effectué le contrôle vous-même.

Vous devez signer une clé avant de pouvoir lui assigner un niveau de confiance.

Le niveau de confiance des clés publiques peut être **Aucun**, **Marginal** ou **Approuvé**. Celui de vos paires de clés peut être **Aucun** ou **Implicite** (ce qui signifie qu'il s'agit de votre propre clé et que vous avez donc entièrement confiance). Vous ne devriez pas avoir les paires de clés de qui que ce soit d'autre.

Pour plus d'informations sur l'approbation des clés, reportez-vous à la section *Introduction à la cryptographie*.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, la possibilité d'accorder de la confiance à des clés peut être désactivée.

Pour accorder de la confiance à une clé

1. Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP, puis sélectionnez **Toutes les clés** dans le panneau de contrôle. Toutes les clés de votre trousseau s'affichent.
2. Double-cliquez sur la clé à laquelle vous voulez accorder de la confiance. La boîte de dialogue Propriétés de la clé pour la clé choisie s'affiche.
3. Recherchez le champ **Confiance**.
4. Cliquez sur le paramètre actuel et sélectionnez le paramètre de votre choix dans la liste.
   - Si vous accordez de la confiance à une clé publique, vous pouvez sélectionner **Aucun**, **Marginal** ou **Approuvé**. L'option Aucun signifie que vous ne faites pas confiance au propriétaire pour agir comme un introducteur. L'option Marginal signifie que vous lui accordez une confiance partielle et l'option Approuvé indique que vous lui faites entièrement confiance.
   - Si vous accordez de la confiance à une paire de clés, vous pouvez sélectionner **Aucun** ou **Implicite**. Seules les paires de clés que vous importez à partir d'une sauvegarde ou d'un autre de vos ordinateurs doivent être définies sur Implicite. Lorsque vous créez une paire de clé, elle est automatiquement définie sur Implicite.

Utilisation des sous-clés

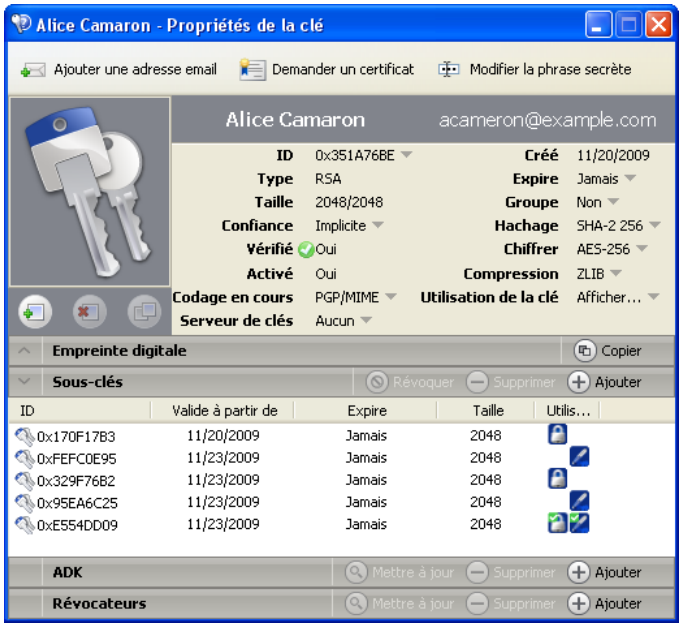
Une paire de clés PGP Desktop est composée des éléments suivants :

- la **clé principale**, utilisée uniquement pour la signature ;
- une **Sous-clé** obligatoire pour le chiffrement ;
- une ou plusieurs *sous-clés distinctes* **en option** pour la signature, le chiffrement ou la combinaison signature/chiffrement.

Lors du processus de signature, c'est la clé principale qui est utilisée par défaut, alors que lors du chiffrement, il s'agit d'une sous-clé. La sécurité d'une paire de clés PGP Desktop peut en être améliorée : une sous-clé de chiffrement distincte peut être révoquée, supprimée ou ajoutée à la paire de clés PGP Desktop sans que la Clé principale ni les signatures qu'elle porte ne soient affectées.

En plus de la Clé principale et de la sous-clé de chiffrement obligatoire, vous avez la possibilité de créer une ou plusieurs sous-clés supplémentaires pour votre paire de clés PGP Desktop. Vous pouvez créer n'importe quelle combinaison de sous-clés à n'utiliser que pour le chiffrement, que pour la signature, ou pour le chiffrement et la signature.

Vous pouvez afficher les sous-clés d'une paire de clés dans la boîte de dialogue Propriétés de la clé. La colonne Utilisation indique la fonction exécutée par la sous-clé :



Clé	Description
	Les sous-clés de chiffrement sont représentées par un cadenas bleu.
	Les sous-clés de signature sont représentées par un crayon bleu.
	Enfin, les sous-clés qui servent au chiffrement et à la signature affichent les deux symboles.
	La sous-clé de chiffrement par défaut affiche une petite coche verte dans le coin supérieur gauche.
	La sous-clé de signature par défaut affiche une petite coche verte dans le coin supérieur gauche.

Utilisation de sous-clés distinctes

Voici quelques exemples de l'utilité de sous-clés distinctes supplémentaires :

- **Plusieurs sous-clés de chiffrement** valides à différentes périodes de la durée de vie de la paire de clés peuvent augmenter la sécurité. Vous pouvez créer des sous-clés de chiffrement avec des date de début et d'expiration réglées de manière qu'une seule sous-clé de chiffrement à la fois n'est valide. Par exemple, vous pourriez créer plusieurs sous-clés de chiffrement valides uniquement pour une année future (assurez-vous de spécifier des dates correctes). La sous-clé de chiffrement en service changera alors avec la nouvelle année. Cette mesure de sécurité peut s'avérer utile car elle permet de changer automatiquement de clé de chiffrement à intervalles réguliers sans avoir à recréer et redistribuer une nouvelle clé publique. Les sous-clés arrivées à expiration affichent une horloge rouge sur l'icône de clé.
- **Plusieurs sous-clés de signature** sont nécessaires dans les régions où la loi exige des sous-clés de signature distinctes pour les signatures numériques contractuelles.

Les sous-clés distinctes que vous pouvez créer dépendent du type de paire de clés que vous utilisez :

- Pour les paires de clés RSA, vous pouvez créer des sous-clés pour le chiffrement, la signature, et le chiffrement/signature.
- Pour les paires de clés Diffie-Hellman/DSS, vous pouvez créer des sous-clés de chiffrement ou de signature, mais vous ne pouvez pas créer de sous-clés de chiffrement et de signature.
- Pour les paires de clés héritées PGP plus anciennes, les sous-clés ne sont pas prises en charge.

Affichage des sous-clés

Vous pouvez afficher et modifier les informations des sous-clés dans vos propres paires de clés. Les informations des sous-clés dans les paires de clés publiques de votre trousseau de clés peuvent être affichées mais non modifiées.

Pour afficher les sous-clés et les propriétés des sous-clés

1. Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP puis sur **Toutes les clés**.

   Toutes les clés de votre trousseau de clés s'affichent.

2 Vous pouvez afficher les propriétés d'une clé en suivant l'une des procédures suivantes :

- Double-cliquez sur la clé que vous voulez afficher.
- Cliquez avec le bouton droit sur la clé, puis sélectionnez **Propriétés de la clé** dans le menu contextuel.
- Cliquez sur la clé dans le trousseau de clés pour la sélectionner, puis sélectionnez **Clés > Propriétés de la clé**.

La boîte de dialogue Propriétés de la clé pour la clé choisie s'affiche.

3 Cliquez sur l'en-tête **Sous-clés** dans la boîte de dialogue Propriétés de la clé. Les sous-clés de cette clé s'affichent.

4 Pour afficher les propriétés d'une sous-clé, cliquez avec le bouton droit sur la sous-clé que vous voulez afficher puis sélectionnez **Propriétés de la sous-clé** dans le menu contextuel.

Création de sous-clés

Vous créerez très probablement vos sous-clés de la manière décrite dans cette section. Cependant, vous pouvez aussi créer des sous-clés avec l'assistant de nouvelle clé lors de l'installation de PGP Desktop. Pour plus d'informations, reportez-vous à la section *Première utilisation de PGP Desktop* (à la page 17).

Pour créer des sous-clés

1 Dans la section Sous-clés de la boîte de dialogue Propriétés de la clé, cliquez sur le bouton **Ajouter**. La boîte de dialogue Nouvelle sous-clé s'affiche.

2 Dans la zone **Utilisez cette sous-clé pour :**, sélectionnez **Chiffrement**, **Signature ou Chiffrement et signature** selon l'usage auquel vous destinez cette nouvelle sous-clé.

3 Dans le champ **Taille de clé**, choisissez une taille de clé comprise entre 1024 et 4096 bits ou saisissez une taille de clé personnalisée dans la même fourchette.

4 Dans le champ **Date de début**, saisissez une date d'entrée en vigueur pour la sous-clé que vous créez ou choisissez une date dans le calendrier.

5 Dans la zone **Expiration**, sélectionnez **Jamais**, ou sélectionnez **Date**, puis spécifiez une date ou choisissez-en une dans le calendrier. Ces informations définissent la date d'expiration de la sous-clé.

6 Cliquez sur **OK.** La boîte de dialogue Phrase secrète s'affiche.

7 Saisissez votre phrase secrète, puis cliquez sur **OK.** La sous-clé est alors créée.

Pour préciser l'utilisation de cette sous-clé (avec la messagerie PGP uniquement, par exemple), reportez-vous à la section *Définition de l'utilisation des clés pour les sous-clés* (à la page 76).

Définition de l'utilisation des clés pour les sous-clés

À chaque sous-clé peuvent être associées des propriétés d'utilisation de clé distinctes. Par exemple, une sous-clé peut être utilisée uniquement pour PGP WDE et une autre, pour toutes les autres fonctions de PGP Desktop.

Si vous souhaitez utiliser une clé seulement pour le chiffrement de disque, mais que vous ne vouliez pas recevoir de messages chiffrés, vous pouvez décider de définir l'utilisation de la clé. Si vous distribuez votre clé publique n'autorisant pas la messagerie PGP, les messages électroniques envoyés par un autre utilisateur ne seront pas chiffrés à l'aide de votre clé publique.

Remarque : si vous vous trouvez dans un environnement géré par un PGP Universal Server et que votre mode clé soit SKM, vous ne pouvez pas modifier les indicateurs d'utilisation des clés. Pour identifier le mode clé utilisé, reportez-vous à la section *Modes clé* (à la page 133).

Pour spécifier l'utilisation d'une clé

1. Ouvrez PGP Desktop, cliquez sur le panneau de contrôle Clés PGP, puis sur **Toutes les clés**.

   Toutes les clés de votre trousseau de clés s'affichent.

2. Pour visualiser les propriétés d'une clé, suivez l'une des procédures ci-après :

   - Double-cliquez sur la clé que vous voulez afficher.
   - Cliquez avec le bouton droit sur la clé, puis sélectionnez **Propriétés de la clé** dans le menu contextuel.
   - Cliquez sur la clé dans le trousseau de clés pour la sélectionner, puis choisissez **Clés > Propriétés de la clé**.

   La boîte de dialogue Propriétés de la clé pour la clé choisie s'affiche.

3. Dans celle-ci, cliquez sur l'en-tête **Sous-clés**. Les sous-clés de cette clé s'affichent.

4 Pour afficher les propriétés d'une sous-clé, cliquez avec le bouton droit sur la sous-clé concernée, puis sélectionnez **Propriétés de la sous-clé** dans le menu contextuel.

5 Dans la section Utilisation de la clé, choisissez les fonctions de PGP Desktop avec lesquelles la clé peut être employée. Une coche apparaît alors en regard des fonctions sélectionnées.

6 Cliquez sur **Fermer**. Les propriétés des sous-clés sont enregistrées.

Révocation de sous-clés

Pour révoquer une sous-clé

1 Dans la zone **Sous-clés** de la boîte de dialogue Propriétés de la clé, sélectionnez la sous-clé à révoquer, puis cliquez sur **Révoquer** (au-dessus de la liste des sous-clés). Une boîte de dialogue **Avertissement PGP s'affiche et vous informe qu'une fois que la sous-clé aura été révoquée, les autres utilisateurs ne pourront plus chiffrer de données avec celle-ci.**

2 Cliquez sur **Oui** pour révoquer la sous-clé ou sur **Non** pour annuler. La boîte de dialogue Phrase secrète s'affiche.

3 Saisissez votre phrase secrète, puis cliquez sur **OK**. La sous-clé est révoquée et l'icône est modifiée.

Suppression de sous-clés

Pour supprimer une sous-clé

1. Dans la zone **Sous-clés** de la boîte de dialogue Propriétés de la clé, **sélectionnez la sous-clé à supprimer, puis cliquez sur Supprimer** (au-dessus de la liste des sous-clés). Une boîte de dialogue **Avertissement PGP** s'affiche et vous informe qu'une fois que la sous-clé aura été supprimée, vous ne pourrez plus déchiffrer les données qui avaient été chiffrées avec celle-ci.
2. Cliquez sur **Oui** pour supprimer la sous-clé ou sur **Non** pour annuler. La sous-clé est alors supprimée.

Utilisation des clés de déchiffrement supplémentaire (ADK)

Une clé de déchiffrement supplémentaire (ADK) est une clé généralement utilisée par les responsables de la sécurité d'une entreprise afin de déchiffrer les messages que les employés reçoivent ou envoient au sein de l'entreprise.

Les messages chiffrés par une clé qui comporte une clé de déchiffrement supplémentaire (ADK) sont chiffrés avec la clé publique du destinataire et la clé de déchiffrement supplémentaire : le détenteur de cette clé peut donc aussi déchiffrer le message.

Ces clés sont rarement utilisées ou nécessaires en dehors d'un environnement géré par un PGP Universal Server. Bien que l'administrateur PGP n'ait normalement pas à utiliser les clés de déchiffrement supplémentaires, il arrive qu'il soit nécessaire de récupérer le message électronique de quelqu'un. Ce peut être le cas lorsque quelqu'un est blessé et absent du travail pour quelques temps ou que les enregistrements de messages électroniques sont réquisitionnés par un tribunal et que la société a à déchiffrer ces messages pour qu'ils constituent une preuve dans une affaire.

Vous ne pouvez modifier que les clés de déchiffrement supplémentaires de vos paires de clés.

Ajout d'une clé de déchiffrement supplémentaire (ADK) à une paire de clés

Pour ajouter une clé de déchiffrement supplémentaire (ADK)

1. Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP puis sur **Mes clés privées** dans la boîte de contrôle. Les clés privées de votre trousseau de clés s'affichent.

2 Double-cliquez sur la clé à laquelle vous ajoutez une clé de déchiffrement supplémentaire (ADK). La boîte de dialogue Propriétés de la clé pour la clé choisie s'affiche.

3 Cliquez sur la flèche vers le haut à la gauche de **Clé de déchiffrement supplémentaire (ADK)**, le cas échéant (seules les clés qui ont déjà au moins une clé de déchiffrement supplémentaire afficheront une flèche vers le haut). Les informations sur la clé de déchiffrement supplémentaire (ADK) de cette clé sont affichées, si les paramètres sont configurés.

4 Cliquez sur l'icône du signe plus (+) à droite de la zone Clé de déchiffrement supplémentaire (ADK). La boîte de dialogue Sélectionner une ou des clés s'affiche.

5 Sélectionnez la clé que vous voulez utiliser comme clé de déchiffrement supplémentaire (ADK), puis cliquez sur **OK.** Une boîte de dialogue Avertissement PGP s'affiche et vous êtes invité à confirmer que vous souhaitez ajouter la clé sélectionnée comme clé de déchiffrement supplémentaire (ADK).

6 Cliquez sur **Oui**. La boîte de dialogue Saisissez la phrase secrète de la clé PGP s'affiche.

7 Saisissez la phrase secrète pour la clé à laquelle vous ajoutez la clé de déchiffrement supplémentaire (ADK), puis cliquez sur **OK**. Une boîte de dialogue Informations PGP s'affiche et vous indique que la clé de déchiffrement supplémentaire (ADK) a été ajoutée à la clé.

8 Cliquez sur **OK**.

Remarque : si vous ajoutez une clé de déchiffrement supplémentaire (ADK) à votre clé, alors les personnes qui vous envoient des courriers électroniques chiffrés doivent pouvoir accéder à la partie de clé publique de la clé de déchiffrement supplémentaire.

Mise à jour d'une clé de déchiffrement supplémentaire

▸ **Pour mettre à jour une clé de déchiffrement supplémentaire**

1 Dans la liste des clés de chiffrement supplémentaires, sélectionnez la ou les clés à mettre à jour : Les clés sélectionnées sont alors mises en surbrillance.

2 Cliquez sur la flèche vers le bas. La clé est alors mise à jour.

Suppression d'une clé de déchiffrement supplémentaire

Pour supprimer une clé de déchiffrement supplémentaire

1. Dans la liste des clés de déchiffrement supplémentaires, sélectionnez la ou les clés à supprimer. Les clés sélectionnées sont alors mises en surbrillance.
2. Cliquez sur le signe moins. Une boîte de dialogue Avertissement PGP vous invite à confirmer la suppression de cette clé de chiffrement supplémentaire.
3. Cliquez sur **OK** pour supprimer la clé. La clé de déchiffrement supplémentaire est supprimée.

Utilisation des révocateurs

Vous pourriez un jour oublier votre phrase secrète ou perdre votre paire de clés (par exemple, à la suite du vol de votre ordinateur portable ou d'une défaillance du disque dur).

Sauf si vous utilisez aussi la reconstruction de la clé et que vous pouvez reconstruire votre clé privée, vous ne pourriez plus utiliser votre clé, et vous n'auriez aucun moyen de la révoquer et d'indiquer aux autres de ne plus l'utiliser pour chiffrer. Pour vous protéger de cette éventualité, vous pouvez désigner une tierce personne comme révocateur de clé. Le tiers que vous désignez a alors la capacité de révoquer votre clé comme si vous la révoquiez vous-même.

Cette fonctionnalité est disponible pour les deux clés Diffie-Hellman/DSS et RSA.

Vous ne pouvez modifier les informations du révocateur que sur vos paires de clés. Si une clé publique de votre trousseau de clés a un révocateur, vous pouvez voir ces informations mais pas les modifier.

Désignation d'un révocateur désigné

Pour ajouter un révocateur désigné à votre clé

1. Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP puis sur **Mes clés privées** dans la boîte de contrôle. Les clés privées de votre trousseau de clés s'affichent.
2. Double-cliquez sur la clé à laquelle vous ajoutez un révocateur. La boîte de dialogue Propriétés de la clé pour la clé choisie s'affiche.

3 Cliquez sur le signe plus (+) à la gauche de **Révocateurs**, le cas échéant (seules les clés qui ont déjà au moins un révocateur configuré afficheront le signe plus). Les informations sur les révocateurs sont affichées, si les paramètres sont configurés.

4 Cliquez sur l'icône du signe plus (+) à droite de la zone Révocateurs. La boîte de dialogue Sélectionner une ou des clés s'affiche.

5 Sélectionnez la clé que vous voulez utiliser comme clé du révocateur, puis cliquez sur **OK**.

Une boîte de dialogue Avertissement PGP s'affiche et vous demande de confirmer que vous souhaitez accorder les privilèges de révocateur à la ou aux clés sélectionnées.

6 Cliquez sur **Oui** pour continuer ou sur **Non** pour annuler. La boîte de dialogue Saisissez la phrase secrète de la clé PGP s'affiche.

7 Saisissez la phrase secrète pour la paire de clés à laquelle vous ajoutez le révocateur, puis cliquez sur **OK.** Une boîte de dialogue Informations PGP s'affiche.

8 Cliquez sur **OK.** La ou les clés sélectionnées sont dorénavant autorisées à révoquer votre clé. Pour une gestion efficace des clés, distribuez une copie actuelle de votre clé au ou aux révocateurs ou téléchargez votre clé sur le serveur de clés.

Révocation d'une clé

Si jamais il arrive que vous n'ayez plus confiance en votre paire de clés personnelle, vous pouvez révoquer votre clé, ce qui indique à tout le monde d'arrêter d'utiliser votre clé publique.

La meilleure façon de propager une clé révoquée est de la placer sur un serveur de clés publiques.

Pour révoquer une clé

1 Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP puis sur **Mes clés privées** dans la boîte de contrôle. Les clés privées de votre trousseau de clés s'affichent.

2 Cliquez avec le bouton droit sur la clé que vous voulez révoquer, puis sélectionnez **Révoquer** dans la liste des commandes affichées. Une boîte de dialogue Avertissement PGP s'affiche et vous êtes invité à confirmer que vous voulez révoquer cette clé.

3 Cliquez sur **Oui** pour confirmer que vous souhaitez révoquer la clé sélectionnée ou sur **Non** pour annuler. La boîte de dialogue Saisissez la phrase secrète de la clé PGP s'affiche.

4 Saisissez la phrase secrète de la paire de clés que vous révoquez, puis cliquez sur **OK.** Quand vous révoquez une clé, elle apparaît alors marquée d'une croix rouge (X) pour indiquer qu'elle n'est plus valide.

5 Synchronisez la clé révoquée afin que tout le monde sache que cette clé publique est dorénavant révoquée et ne doit plus être utilisée.

Scission et réassemblage de clé

Toute clé privée peut être scindée en parts réparties entre plusieurs « actionnaires » par un processus de chiffrement appelé scission de clé Blakely-Shamir. Cette technique est recommandée pour les clés de très haute sécurité.

Par exemple, PGP Corporation scinde une clé d'entreprise entre plusieurs personnes. Dès qu'il faut signer avec cette clé, les parts de la clé sont temporairement réassemblées.

Création d'une clé scindée

Quand vous scindez une clé, les parts sont enregistrées comme des fichiers soit chiffrés avec la clé publique d'un actionnaire, soit chiffrés de façon conventionnelle si l'actionnaire n'a pas de clé publique. Après la scission de la clé, toute tentative de signature ou de déchiffrement avec elle entraînera automatiquement une tentative de réassemblage de la clé.

Pour créer une clé scindée avec plusieurs parts

1 Ouvrez PGP Desktop, cliquez sur la boîte de contrôle Clés PGP puis sur **Mes clés privées** dans la boîte de contrôle. Les clés privées de votre trousseau de clés s'affichent.

2 Cliquez sur la paire de clés que vous voulez scinder. La paire de clés sélectionnée est alors mise en surbrillance.

3 Sélectionnez **Clés >Partager la clé > Partager.** La boîte de dialogue Clé PGP partagée s'affiche.

4 Ajoutez des actionnaires pour la clé scindée en glissant et déplaçant leurs clés dans la liste **Actionnaires**.

Pour ajouter un actionnaire sans clé publique, cliquez sur **Ajouter**, saisissez le nom de la personne, puis laissez-la saisir sa phrase secrète. (L'actionnaire doit être physiquement présent pour saisir sa propre phrase secrète).

5 Quand tous les actionnaires sont répertoriés, vous pouvez spécifier le nombre de parts de clé qui sont nécessaires au déchiffrement ou à la signature avec cette clé.

Par défaut, chaque actionnaire est responsable d'une part. Pour augmenter le nombre de parts qu'un actionnaire contrôle, cliquez sur son nom dans la liste des actionnaires puis utilisez les flèches pour rectifier le nombre de parts.

6 Cliquez sur **Scinder la clé.** Vous êtes invité à sélectionner un répertoire où stocker les parts.

7 Sélectionnez un emplacement où stocker les parts de clé, puis cliquez sur **OK.** L'écran Phrase secrète s'affiche.

8 Saisissez la phrase secrète de la clé que vous voulez scinder, puis cliquez sur **OK**. Une boîte de dialogue de confirmation apparaît.

9 Cliquez sur **Oui** pour scinder la clé. La clé est scindée et les parts sont enregistrées à l'emplacement que vous avez spécifié. Chaque part de clé est enregistrée avec le nom de l'actionnaire pour nom de fichier, suivi d'une extension SHF.

10 Distribuez les parts de clé aux propriétaires, puis supprimez les copies locales des parts.

Une fois une clé scindée entre plusieurs actionnaires, toute tentative de signature ou de déchiffrement avec elle entraînera automatiquement une tentative de réassemblage de la clé par PGP Desktop.

Veillez à conserver la clé d'origine qui a été scindée. Vous devez disposer de cette clé pour pouvoir réassembler la clé scindée pour toute fonction de déchiffrement.

Réassemblage de clés scindées

Une fois une clé scindée entre plusieurs actionnaires, toute tentative de signature ou de déchiffrement avec elle entraîne automatiquement une tentative de réassemblage de la clé par PGP Desktop. Le réassemblage de la clé peut s'effectuer de deux façons : localement et à distance.

Le réassemblage local de parts de clé exige la présence de l'actionnaire auprès de l'ordinateur de réassemblage. Chaque actionnaire devra obligatoirement saisir la phrase secrète pour sa part de clé.

Le réassemblage de parts de clé à distance exige des actionnaires distants qu'ils s'authentifient et déchiffrent leurs clés avant de les envoyer sur le réseau. L'implémentation du protocole TLS (Transport Layer Security) dans PGP Desktop fournit un lien sécurisé pour la transmission de parts de clé, et permet à plusieurs personnes distantes de signer ou déchiffrer avec leur part de clé de manière sécurisée.

Attention : avant que recevoir les parts de clé par le réseau, vous devriez vérifier l'empreinte digitale de chaque actionnaire et signer leur clé publique pour vous assurer que leur clé d'authentification est légitime.

Avant de commencer, vérifiez que la clé d'origine qui a été scindée se trouve bien sur l'ordinateur de réassemblage.

Pour réassembler une clé scindée

1 Contactez chaque actionnaire de la clé scindée. Pour réassembler des parts de clé localement, les actionnaires de la clé doivent être présents.

Pour collecter des parts de clé sur le réseau, assurez-vous que les actionnaires distants ont bien installé PGP Desktop et qu'ils sont prêts à envoyer leur fichier de partage de clé. Les actionnaires distants doivent posséder :

- leurs fichiers de partage de clé et mots de passe ;
- une paire de clés (pour l'authentification auprès de l'ordinateur collectant les parts de clé) ;
- une connexion réseau ;
- l'adresse IP ou le nom de domaine complet de l'ordinateur collectant les parts de clé.

2 Effectuez l'une des opérations suivantes :

- Pour réassembler la clé de façon temporaire, sur l'ordinateur de réassemblage, utilisez l'Explorateur Windows pour sélectionner le ou les fichiers à signer ou déchiffrer à l'aide de la clé scindée.

  Cliquez avec le bouton droit sur le ou les fichiers et sélectionnez **Signer ou déchiffrer** dans le menu contextuel PGP. L'écran **Saisissez la phrase secrète de la clé sélectionnée PGP** s'affiche et la clé scindée est sélectionnée.

  Cliquez sur **OK** pour reconstituer la clé sélectionnée. L'écran Collecte des parts de clé s'affiche.

- Pour réassembler la clé de façon permanente, cliquez avec le bouton droit sur la clé scindée et sélectionnez **Propriétés de la clé** dans le menu qui apparaît.

  Dans la boîte de dialogue Propriétés de la clé, cliquez sur **Joindre la clé** (ce bouton s'intitule **Modifier la phrase secrète** pour les clés non scindées).

La boîte de dialogue Phrase secrète s'affiche.

3 Effectuez l'une des opérations suivantes :

- Si vous collectez les parts de clé localement, cliquez sur **Sélectionner un fichier de partage**, puis recherchez les fichiers de partage associés à la clé scindée. Les fichiers de partage peuvent être collectés sur le disque dur, une disquette ou un lecteur monté. Passez à l'étape suivante.

- Si vous collectez les parts de clé sur le réseau, cliquez sur **Démarrer le réseau**. L'utilisateur distant doit démarrer PGP Desktop et sélectionner **Clés > Partager la clé > Envoyer la part de clé**. Commence alors le processus de sélection du fichier de partage, de déchiffrement de ce fichier, de sélection d'une clé d'autorisation, de déverrouillage de cette clé et de saisie du nom d'hôte ou de l'adresse IP de l'ordinateur de réassemblage.

Dans le champ Clé de signature, sélectionnez la paire de clés à utiliser pour l'authentification auprès du système distant et saisissez la phrase secrète.

Cliquez sur **OK** pour préparer l'ordinateur à recevoir les parts de clé.

L'état de la transaction s'affiche dans la zone Parts réseau. Lorsque l'état devient « Écoute en cours », l'application PGP est prête à recevoir les parts de clé.

C'est à ce moment que les actionnaires doivent envoyer leurs parts de clé.

Lorsqu'une part est reçue, la boîte de dialogue Authentification à distance s'affiche. Si vous n'avez pas signé la clé utilisée pour authentifier le système distant, celle-ci est considérée comme non valide. Bien que vous puissiez réassembler la clé scindée avec une clé d'authentification non valide, cela n'est pas conseillé. Vous devez vérifier l'empreinte numérique de tous les actionnaires et signer la clé publique de chacun d'entre eux pour vous assurer que la clé d'authentification est légitime.

4. Cliquez sur **Confirmer** pour accepter le fichier de partage.
5. Continuez à collecter des parts de clé jusqu'à ce que la valeur Nombre total de parts collectées corresponde à la valeur de Nombre total de parts nécessaires sur l'écran Collecte des parts de clé.
6. Cliquez sur **OK.**

- Si vous avez choisi de réassembler la clé de façon temporaire afin d'effectuer une opération de déchiffrement ou de signature, le fichier est signé ou déchiffré avec la clé scindée et la clé réassemblée est abandonnée.
- Si vous avez décidé de réassembler la clé de façon permanente, celle-ci est enregistrée en tant que clé entièrement réassemblée (et n'est plus scindée).

Perte de votre clé ou phrase secrète

Si vous avez perdu votre clé, vous pouvez la reconstruire de façon à continuer de chiffrer et déchiffrer des données. La façon dont vous devez procéder dépend de l'environnement d'utilisation de PGP Desktop : autonome ou géré par un PGP Universal Server.

Si vous avez oublié votre phrase secrète, vous pouvez la réinitialiser. Pour cela, vous devez répondre correctement à trois des cinq questions de sécurité auxquelles vous avez répondu lorsque vous avez configuré votre clé ou créé vos questions de sécurité.

Reconstruction de clés avec PGP Universal Server

Cette section ne s'applique qu'aux utilisateurs PGP Desktop dans un environnement géré par le PGP Universal Server, et dont l'administrateur PGP a configuré la prise en charge de la reconstruction de clé pour leur copie de PGP Desktop.

En cas de perte de votre clé ou d'oubli de votre phrase secrète, si vous n'avez pas de copie de sauvegarde pour restaurer votre clé, vous ne pourrez plus jamais déchiffrer les informations chiffrées avec cette clé. Vous pouvez cependant reconstruire votre clé si votre administrateur PGP a implémenté pour vous une stratégie de reconstruction de clé PGP, stratégie qui consiste à chiffrer et stocker votre clé sur un PGP Universal Server de telle façon que vous seul pouvez la récupérer.

Le PGP Universal Server qui conserve les données de reconstruction de clé stocke votre clé de telle façon que vous seul pouvez y accéder. Pas même l'administrateur PGP n'a la capacité de déchiffrer votre clé.

Si votre administrateur PGP a configuré la prise en charge de la reconstruction de clé, vous serez invité à saisir des informations « secrètes » supplémentaires lors de l'installation de PGP Desktop ou de la création de vos questions de sécurité.

Une fois votre clé sur le serveur, vous pouvez la restaurer à tout moment en sélectionnant **Clés > J'ai perdu ma clé** ou **Clés > J'ai oublié ma phrase secrète** dans PGP Desktop pour Windows, ou **Clés > Reconstruire** dans PGP Desktop pour Mac OS X.

Conseil : si vous n'avez pas été invité à créer vos questions PGP durant l'installation de PGP Desktop et que votre administrateur PGP Universal Server autorise la reconstruction de clé locale, vous pouvez créer ces questions manuellement. Pour plus d'informations, reportez-vous à la section *Création de vos questions de sécurité* (à la page 87).

Création des données de reconstruction de clé

Lorsque vous répondez aux questions relatives à la sécurité PGP, vous créez des données de reconstruction de clé. Dans un environnement autonome, ces informations sont stockées dans un fichier .krb sur votre disque local. Dans un environnement géré, vous envoyez les données de reconstruction de clé au PGP Universal Server de votre entreprise quand vous installez PGP Desktop ou que vous créez et répondez à vos questions de sécurité.

Choisissez des questions personnelles et complexes dont vous ne risquez pas d'oublier les réponses. Vos questions peuvent comporter jusqu'à 95 caractères. « Qui m'a emmené à la plage » ? ou « Pourquoi Fred est-il parti ?» sont par exemple de bonnes questions. « Quel est le nom de jeune fille de ma mère » ? ou « À quel lycée suis-je allé ?» sont par exemple de mauvaises questions.

Une fois que vous avez créé les cinq questions PGP et que vous y avez répondu, votre clé privée est scindée en cinq parties à l'aide de la scission de clé Blakely-Shamir. Trois des cinq parties sont nécessaires pour reconstruire la clé. Chaque partie est alors chiffrée avec le hachage, ou numéro d'identification unique, d'une réponse. Si vous connaissez trois des réponses, vous pouvez reconstruire la clé entière.

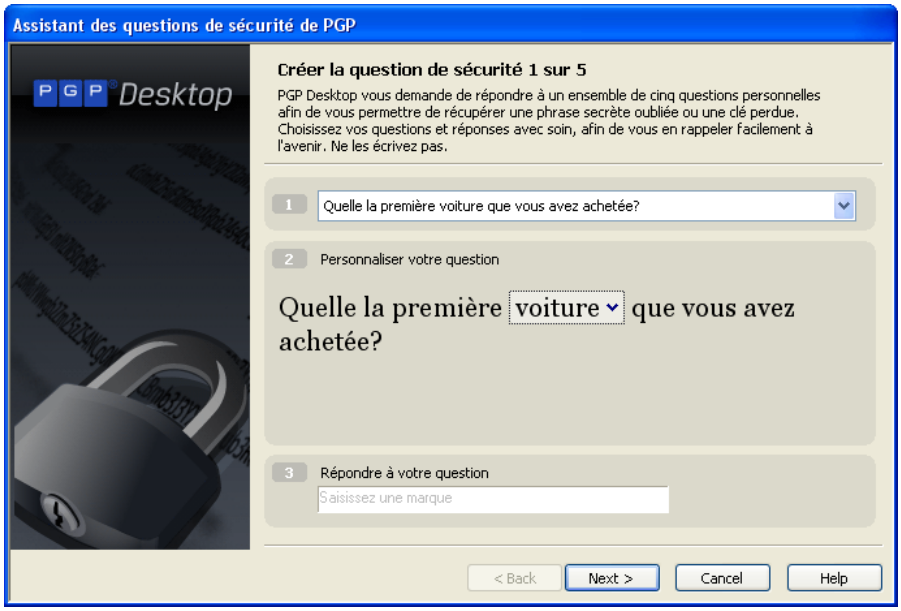
Création de vos questions de sécurité

Pour pouvoir reconstruire votre clé ou générer une nouvelle phrase secrète suite à l'oubli de la précédente, vous devez créer vos questions de sécurité. Vous pouvez personnaliser les cinq questions de sécurité de sorte que vous soyez le seul à connaître leurs réponses.

Pour créer vos questions de sécurité

1. Dans PGP Desktop, cliquez sur le panneau de contrôle Clés PGP et sélectionnez votre clé.
2. Sélectionnez **Clés > Créer Mes questions PGP**. L'assistant des questions de sécurité de PGP apparaît.

3 Tapez la phrase secrète de votre clé, puis cliquez sur **Suivant**. La boîte de dialogue Créer la question de sécurité 1 sur 5 s'affiche.



4 Dans le premier écran Créer la question de sécurité, cliquez sur la flèche du premier champ pour sélectionner la question à utiliser. Vous pourrez personnaliser des parties de la question au cours de l'étape suivante.

Si vous souhaitez personnaliser l'ensemble de la question afin de créer votre propre question, sélectionnez **Saisir ma propre question**.

5 Pour l'option **Personnaliser votre question**, cliquez sur les flèches situées en regard du texte à personnaliser. Par exemple, si vous avez choisi la première question, vous pouvez la personnaliser en remplaçant « ami » par « garçon » et « sur qui vous avez flashé » par « à qui vous avez tenu la main ».

Si vous décidez de créer votre propre question, indiquez-la dans ce champ. Veillez à saisir une question dont vous êtes le seul à connaître la réponse.

6 Pour l'option **Répondre à votre question**, saisissez la réponse à cette question de sécurité. Vous pouvez taper votre réponse en majuscules et en minuscules, uniquement en majuscules ou uniquement en minuscules. Aucune distinction ne sera faite à ce niveau lorsque vous répondrez à la question.

Un conseil s'affiche dans ce champ et disparaît dès que vous commencez à taper une réponse. Par exemple, pour répondre à la question « Quel a été le premier garçon à qui vous avez tenu la main ? », le conseil est « Saisir les nom et prénom ».

7 Une fois que vous avez défini votre question et saisi sa réponse, cliquez sur **Suivant** pour continuer. La boîte de dialogue Créer la question de sécurité 2 sur 5 s'affiche.

8 Vous êtes invité à créer un total de cinq questions et réponses de sécurité. Reprenez les étapes ci-dessus pour sélectionner des questions, les personnaliser et y répondre.

Une fois que vous avez entré les cinq questions et réponses, l'écran Fin de l'assistant des questions de sécurité de PGP s'affiche. Cliquez sur **Terminer** pour quitter l'assistant.

Vous avez à présent défini les cinq questions de sécurité. Si vous avez perdu votre clé ou oublié votre phrase secrète, vous pouvez reconstruire la clé ou réinitialiser la phrase en répondant à trois de ces cinq questions.

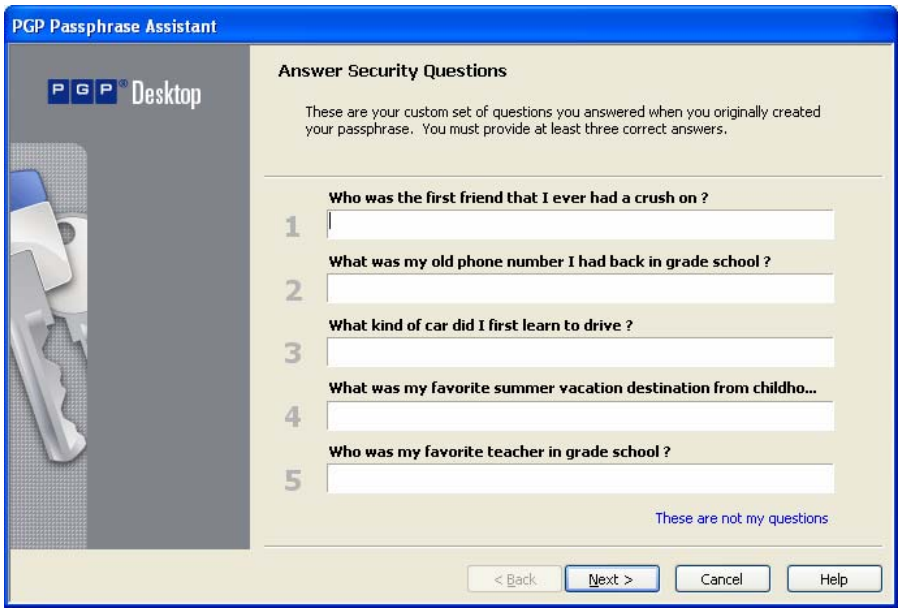
Reconstruction de votre clé en cas de perte de celle-ci ou de la phrase secrète

Si vous avez perdu votre clé ou oublié votre phrase secrète, vous devez reconstruire la clé. Pour cela, vous devez au préalable avoir créé un ensemble de questions de sécurité auxquelles vous êtes le seul à savoir répondre. Pour plus d'informations, reportez-vous à la section *Création de vos questions de sécurité* (à la page 87).

Pour reconstruire votre clé

1 Dans PGP Desktop, cliquez sur le panneau de contrôle Clés PGP et sélectionnez votre clé.

2 Sélectionnez **Clés > J'ai perdu ma clé**. La boîte de dialogue Assistant de phrase secrète PGP : Répondre aux questions de sécurité s'affiche.



Conseil : si les questions qui apparaissent ne sont pas vos questions, cliquez sur le lien Ce ne sont pas mes questions. La boîte de dialogue Assistant de phrase secrète PGP : Sélectionner une clé à reconstruire s'affiche. Sélectionnez l'ID de la clé à reconstruire et cliquez sur **Suivant**.

3. Répondez correctement à trois des cinq questions de sécurité et cliquez sur **Suivant**. L'écran Assistant de phrase secrète PGP : Réussite s'affiche.
4. Cliquez sur **Suivant** pour poursuivre la création d'une phrase secrète. La boîte de dialogue Assistant de phrase secrète PGP : Créer une phrase secrète s'affiche.
5. Tapez, puis confirmez votre phrase secrète.

   Cochez la case **Afficher les frappes** si vous souhaitez voir les caractères saisis. Assurez-vous que personne ne regarde ce que vous tapez.

   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* (à la page 336).
6. Cliquez sur **Terminer**. Votre clé a été reconstruite.

Protection de vos clés

En plus d'effectuer des copies de sauvegarde de vos clés, vous devez faire particulièrement attention à l'emplacement de stockage de votre clé privée. Même si votre clé privée est protégée par une phrase secrète que vous seul devriez connaître, quelqu'un pourrait découvrir votre phrase secrète, puis utiliser votre clé privée pour déchiffrer votre courrier électronique ou contrefaire votre signature numérique. Par exemple, quelqu'un peut regarder les touches que vous saisissez par-dessus votre épaule ou les intercepter sur le réseau voire sur Internet.

Pour empêcher quiconque qui aurait pu intercepter votre phrase secrète d'utiliser votre clé privée, ne stockez votre clé privée que sur votre propre ordinateur. Si votre ordinateur est relié à un réseau, assurez-vous que vos fichiers ne sont pas automatiquement inclus dans une sauvegarde système où d'autres utilisateurs pourraient avoir accès à votre clé privée. Étant donnée la facilité d'accès aux ordinateurs par les réseaux, si vous manipulez des informations extrêmement sensibles, vous voudrez peut-être conserver votre clé privée sur un lecteur flash que vous pouvez insérer comme les clés traditionnelles quand vous voulez lire ou signer des informations privées.

Comme précaution de sécurité supplémentaire, pensez à affecter un nom distinct à votre fichier de trousseau de clés privées et à le stocker dans un emplacement différent que celui par défaut.

Vos clés privées et publiques sont stockées dans des fichiers de trousseau de clés distincts. Vous pouvez les copier dans un autre emplacement sur votre disque dur ou sur une disquette. Par défaut, le trousseau de clés privées (`secring.skr`) et le trousseau de clés publiques (`pubring.pkr`) sont stockés avec les autres fichiers du programme dans votre dossier « PGP » ; vous pouvez enregistrer vos sauvegardes dans un emplacement de votre choix.

Vous pouvez configurer PGP Desktop pour sauvegarder automatiquement vos trousseaux de clés après sa fermeture. Vous pouvez définir les options de sauvegarde de vos trousseaux de clés dans l'onglet Clés de la boîte de dialogue Options (pour les systèmes Windows) ou la boîte de dialogue Préférences (pour les systèmes Mac OS X).

Conseil : la modification votre phrase secrète sur votre clé ne la modifie pas sur les copies de la clé (par exemple, les sauvegardes que vous pourriez avoir faites). Si vous pensez que votre clé a été compromise, PGP Corporation recommande de décomposer toute copie de sauvegarde précédemment effectuée et de procéder à de nouvelles copies de sauvegarde de la clé.

7 Sécurisation des messages électroniques

Cette section décrit l'utilisation de PGP Desktop pour sécuriser automatiquement et en toute transparence vos messages électroniques.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

Processus PGP Desktop de sécurisation des messages électroniques

Lorsque l'envoi sécurisé des messages est activé, PGP Desktop surveille le trafic des messages électroniques entre votre client et votre serveur de messagerie. Selon les circonstances, PGP Desktop agira en votre nom pour chiffrer, signer, déchiffrer ou vérifier les messages.

Une fois configuré, et il est très probable que PGP Desktop puisse le faire automatiquement à votre place, vous n'avez plus rien à faire pour chiffrer et/ou signer des messages sortants, ou déchiffrer et/ou vérifier des messages entrants. Le proxy de messagerie de PGP Desktop effectue toutes ces actions pour vous.

La méthode employée diffère selon qu'il s'agisse de messages entrants ou sortants.

Dans le cas de messages entrants, PGP Desktop évalue automatiquement tous les messages électroniques entrants et prend les mesures appropriées (voir la section suivante).

Dans le cas de messages sortants, PGP Desktop peut prendre diverses mesures à votre place en fonction des stratégies configurées. Une stratégie est un ensemble d'instructions (du type « Dans telle circonstance, faire ceci ») qui indique à PGP Desktop ce qu'il doit faire dans des situations particulières. En combinant ces instructions, il est possible d'élaborer des stratégies qui satisfont toutes vos exigences en matière de sécurité des messages électroniques. PGP Desktop inclut un jeu de stratégies adaptées aux besoins de la grande majorité des utilisateurs. Vous avez néanmoins la possibilité de modifier ces stratégies en fonction de vos exigences.

Par défaut, lorsque vous utilisez PGP Desktop de manière autonome et que vous envoyez un message, PGP Desktop recherche une clé approuvée pour chiffrer le message. Il recherche d'abord la clé publique du destinataire dans le trousseau de clés par défaut (appelé Toutes les clés sous Windows) ou dans le trousseau de clés local (appelé Clés sous Mac OS X). S'il ne la trouve pas, il recherche alors, ici encore par défaut, une clé approuvée pour le destinataire dans le PGP Global Directory. S'il ne trouve aucune clé approuvée dans ce répertoire, le message est envoyé en clair, c'est-à-dire non chiffré. Ce comportement par défaut, appelé *chiffrement opportuniste*, permet de trouver le juste milieu entre la protection des messages sortants et l'assurance de leur envoi.

La création de stratégies est traitée en détail dans la section *Création d'une stratégie de sécurité* (à la page 112).

Si votre ordinateur se trouve dans un domaine protégé par un PGP Universal Server, vos stratégies PGP Desktop locales déterminent la méthode et le moment du chiffrement de vos messages. Pour plus d'informations, adressez-vous à l'administrateur PGP Universal Server de votre entreprise.

Remarque : PGP Desktop vérifie uniquement le trousseau de clés par défaut. Pour envoyer des courriers électroniques chiffrés à un destinataire dont la clé figure dans votre trousseau de clés local, veillez à importer cette clé vers votre trousseau par défaut.

Si vous possédez plusieurs trousseaux de clés, le trousseau par défaut est le premier indiqué dans le panneau de contrôle Clés PGP. Pour spécifier un autre trousseau de clés par défaut, cliquez avec le bouton droit sur le trousseau dans le panneau de contrôle Clés PGP, choisissez Propriétés et cochez la case **Trousseau de clés par défaut**.

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

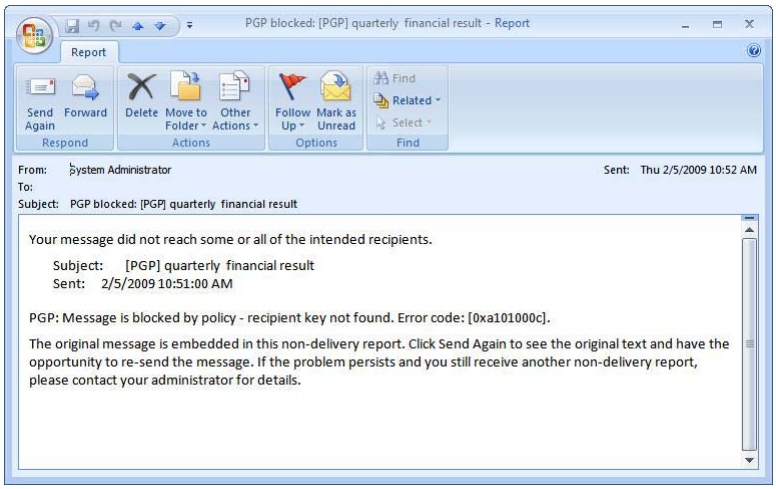
Les messages électroniques que vous envoyez peuvent être chiffrés, signés, les deux ou ni l'un ni l'autre. Puisque vous avez probablement des combinaisons différentes pour les destinataires ou les domaines de messagerie, vous devez créer des stratégies pour vos différentes possibilités de message électronique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

Envoi de courriers électroniques MAPI avec Microsoft Outlook

PGP Desktop version 9.10 permet désormais de mettre en attente les messages sortants afin que vous puissiez continuer à travailler dans un courrier électronique sans avoir à attendre que le message du Notificateur PGP disparaisse.

Lorsqu'une clé est introuvable, au lieu d'afficher le message sous forme de notification PGP, puis d'afficher le message sortant (afin que vous puissiez le modifier pour supprimer son destinataire, par exemple), un rapport de non-remise « clé introuvable » est généré et envoyé. Ce rapport a le format d'un message électronique entrant et est envoyé par l'« administrateur système ». Il contient des informations sur la raison pour laquelle le message n'a pas été reçu par un ou plusieurs destinataires.



Les messages les plus courants contenus dans les rapports de non-remise sont les suivants :

- PGP : le message est bloqué par la stratégie : serveur inaccessible.
- PGP : le message est bloqué : impossible de trouver la clé de déchiffrement supplémentaire.
- PGP : le message est bloqué : impossible de déverrouiller la clé de signature.
- PGP : le message est bloqué : impossible de trouver l'ID clé par clé.
- PGP : le message est bloqué par la notification.
- PGP : le message est bloqué par la stratégie : impossible de trouver la clé du destinataire.
- PGP : le message est bloqué par la stratégie.

Contactez votre administrateur PGP Universal Server pour obtenir de l'aide sur ces problèmes de stratégie.

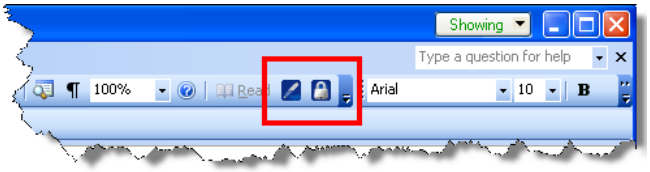
Utilisation des boutons Signer et Chiffrer dans Microsoft Outlook

PGP Desktop pour Windows 10.0 propose une nouvelle fonctionnalité pour Microsoft Outlook 2002 SP3, 2003 (XP) SP3 et 2007 lorsque ce système est associé à des comptes de messagerie électronique Microsoft Exchange (MAPI) et SMTP. Cette fonctionnalité fournit des boutons permettant de signer, chiffrer, ou signer et chiffrer de manière explicite un message électronique. Elle assure la conformité avec les réglementations relatives aux signatures, notamment la réglementation européenne, qui requièrent que les utilisateurs valident leurs messages électroniques en les signant.

Les boutons **Signer** et **Chiffrer** sont disponibles aussi bien pour les installations autonomes que gérées de PGP Desktop.

- Dans les environnements autonomes, les boutons Signer et Chiffrer peuvent être activés ou désactivés dans la boîte de dialogue Options. Pour activer ou désactiver l'un de ces boutons, sélectionnez **Outils > Options**, cliquez sur l'onglet Messagerie, puis activez (ou désactivez) l'option **Activer les boutons de chiffrement et de signature PGP dans Outlook**. Par défaut, les boutons sont désactivés.
- Si vous utilisez PGP Desktop dans un environnement géré, l'administrateur de votre serveur PGP Universal Server aura tranché sur la disponibilité de cette fonctionnalité et l'aura peut-être désactivée à l'aide d'une stratégie.

Lorsque la fonctionnalité est activée dans Microsoft Outlook 2002/2003, les deux boutons apparaissent dans la barre d'outils de l'application.



Lorsqu'elle est activée dans Microsoft Outlook 2007, les deux boutons apparaissent dans le ruban de message :

la stratégie de messagerie sortante détermine le mode d'envoi du message électronique. Trois nouvelles stratégies par défaut pour la prise en charge de ces boutons sont incluses dans les nouvelles installations de PGP Desktop. Pour les installations existantes, il est nécessaire de créer ces trois stratégies. Pour plus d'informations sur les paramètres applicables aux stratégies, reportez-vous à la section *Informations sur les stratégies de sécurité et exemples* (à la page 119).

Les boutons **Signer** et **Chiffrer** constituent une fonctionnalité supplémentaire, grâce à laquelle vous êtes en mesure de contrôler les messages à chiffrer et/ou signer. Ils ne remplacent pas le proxy de messagerie utilisé dans PGP Desktop.

Remarque : si vous répondez à, ou transférez, un message électronique et que vous souhaitiez chiffrer et/ou signer le message ainsi obtenu, veillez à sélectionner les boutons appropriés. Les transferts et les réponses sont traités comme des nouveaux messages, et vous devez, pour sécuriser le message, sélectionner clairement les options de votre choix.

Lors de la création ou du transfert d'un message électronique ou de la réponse à un message, suivez la procédure ci-dessous.

Pour signer, chiffrer, ou signer et chiffrer un message électronique

1. Commencez par créer votre message électronique.
2. Effectuez l'une des opérations suivantes :
   - Pour seulement signer le message, cliquez sur **Signer** (). Si vous optez pour cette méthode, le message est envoyé en texte en clair.
   - Pour seulement chiffrer le message, cliquez sur **Chiffrer** ().
   - Pour signer *et* chiffrer le message électronique, cliquez sur **Signer** et **Chiffrer** ().

   Conseil : si vous avez cliqué sur l'un des boutons, ou les deux, puis enregistrez le message électronique en tant que brouillon, les boutons restent activés tant que vous n'avez pas terminé de créer le message.
3. Lorsque vous avez fini, envoyez le message. Le Notificateur PGP Desktop affiche le résultat des processus de signature et/ou chiffrement (pour plus d'informations sur le Notificateur, reportez-vous à la section *Messages sortants du Notificateur PGP Desktop* (cf. "Notificateur PGP Desktop - Messages sortants" à la page 37)).

Utilisation de la stratégie hors connexion

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, la stratégie hors connexion relative aux messages électroniques est définie par l'administrateur de votre PGP Universal Server. Cette stratégie détermine ce que deviennent les messages lorsque le PGP Universal Server est hors connexion ou ne peut pas être contacté par PGP Desktop.

- **Bloquer les messages sortants** : vos messages sortants ne sont pas envoyés. Si les messages peuvent être mis en file d'attente par votre client de messagerie, ils restent dans la file d'attente jusqu'à ce que le PGP Universal Server soit disponible. S'ils ne peuvent pas être placés en file d'attente, ils sont bloqués.
- **Envoyer les messages sortants en texte en clair** : vous devez décider si vous voulez envoyer le message électronique de façon non sécurisée. Si vous choisissez de l'envoyer, le message est envoyé en texte en clair. Si vous décidez de ne pas l'envoyer, le message est bloqué.
- **Suivre la stratégie autonome** : PGP Desktop se base sur la stratégie autonome pour gérer vos messages sortants. Pour plus d'informations, reportez-vous à la section *Affichage des services et stratégies* (à la page 102).

Pour plus d'informations sur les notifications que vous recevez dans les cas présentés ci-dessus, reportez-vous à la section *Messages sortants du Notificateur PGP Desktop pour la stratégie hors connexion* (à la page 37).

L'administrateur de votre serveur PGP Universal Server peut préciser la fréquence de téléchargement de vos stratégies de messagerie dans PGP Desktop. En mode hors ligne, la dernière stratégie de messagerie hors connexion téléchargée reste applicable pour le traitement de vos messages électroniques sortants. Si vous restez déconnecté sur une période plus longue que le délai de grâce autorisé pour l'application de la stratégie de messagerie autonome hors connexion, votre administrateur peut avoir indiqué également la méthode de traitement du courrier électronique sortant. Le cas échéant, selon la stratégie choisie par l'administrateur, PGP Desktop peut commencer à bloquer vos messages sortants ou bien à les traiter à l'aide de la même stratégie de messagerie autonome hors connexion.

Si vous êtes resté déconnecté pendant un certain temps, vous pouvez, lorsque vous vous reconnectez, demander manuellement à télécharger la stratégie du PGP Universal Server. Pour cela, une fois reconnecté, cliquez sur l'icône de PGP Desktop dans la zone de notification et sélectionnez **Mettre à jour la stratégie**. Les stratégies les plus récentes sont téléchargées depuis le serveur PGP Universal Server et les journaux Client sont chargés vers celui-ci. L'option permettant de mettre à jour manuellement une stratégie est uniquement proposée aux utilisateurs gérés.

Si votre administrateur PGP Universal Server vous autorise à utiliser des stratégies autonomes, reportez-vous à la section *Création d'une stratégie de sécurité* (à la page 112).

Services et stratégies

Pour bien comprendre comment utiliser PGP Desktop pour protéger vos messages sortants de manière automatique et en toute transparence, vous devez connaître la définition de ces deux termes : service et stratégie.

- **Service** : Informations sur un compte de messagerie électronique de votre système et les stratégies relatives à ce compte. Dans la plupart des cas, PGP Desktop crée et configure automatiquement un service pour chaque compte de messagerie de votre système. Dans certains cas, il se peut que vous souhaitiez créer et configurer un service manuellement.
- **Stratégie** : Ensemble d'instructions indiquant les actions que PGP Desktop doit réaliser dans des situations particulières. Les stratégies sont généralement associées à plusieurs services (une stratégie peut être utilisée par des services différents). De même, un service peut posséder, et c'est généralement le cas, plusieurs stratégies.

Lorsque PGP Desktop décide de la méthode à suivre pour gérer un message électronique sortant particulier, il vérifie les stratégies configurées pour le service les unes après les autres, en suivant l'ordre des stratégies dans la liste. Lorsqu'il trouve une stratégie applicable, il interrompt la recherche de stratégie et applique la stratégie trouvée.

Tous les nouveaux services sont créés avec les stratégies par défaut suivantes :

- **Boutons Chiffrer et Signer** : Lorsque vous sélectionnez les boutons **Chiffrer** et **Signer** dans Microsoft Outlook 2002, 2003 ou 2007, le message électronique est à la fois signé et chiffré. Cette stratégie n'est applicable que sur PGP Desktop pour Windows.
- **Bouton Signer** : Lorsque vous sélectionnez le bouton **Signer** dans Microsoft Outlook 2002, 2003 ou 2007, le message électronique est signé. Cette stratégie n'est applicable que sur PGP Desktop pour Windows.
- **Bouton Chiffrer** : Lorsque vous sélectionnez le bouton **Chiffrer** dans Microsoft Outlook 2002, 2003 ou 2007, le message électronique est chiffré. Cette stratégie n'est applicable que sur PGP Desktop pour Windows.
- **Demandes administrateur de liste de publipostage** : Indique que les demandes administratives de listes de publipostage sont envoyées en clair, c'est-à-dire ni chiffrées, ni signées.
- **Envois de listes de publipostage** : Indique que les envois de listes de publipostage sont transférés signés, à des fins d'authentification, mais pas chiffrés.
- **Demander le chiffrement : confidentiel [PGP]** : Indique que 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. Sinon, le message ne peut pas être envoyé.
- **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 bien envoyé, bien qu'en clair, même si la clé de chiffrement du destinataire est introuvable.

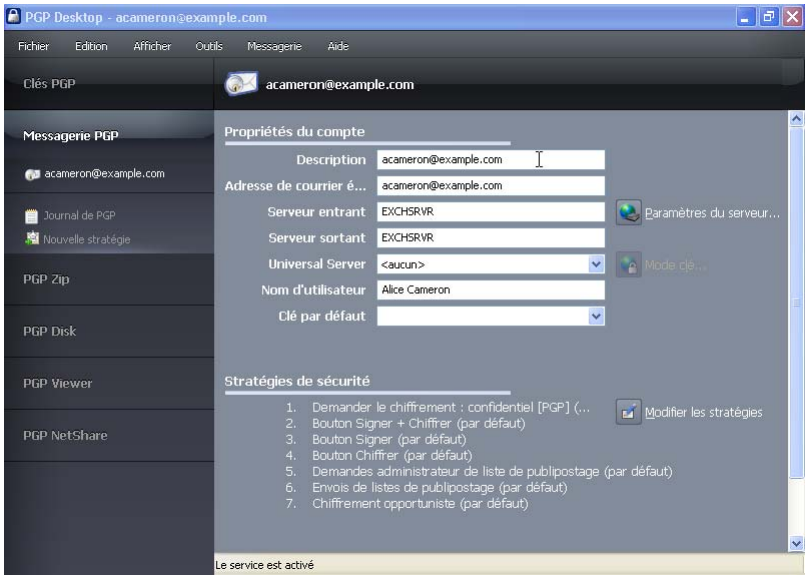
Ne placez pas la stratégie Chiffrement opportuniste en premier dans la liste des stratégies, ni même à un emplacement autre qu'en dernier, car lorsque PGP Desktop trouve une stratégie applicable, et le chiffrement opportuniste est toujours applicable, il interrompt la recherche et applique la stratégie trouvée. Ainsi, si une stratégie plus pertinente pour votre message est placée dans la liste après le chiffrement opportuniste, elle ne sera jamais appliquée.

Remarque : Vous pouvez modifier les stratégies par défaut, mais vous ne pouvez pas les supprimer. Vous pouvez également les désactiver et en changer l'ordre dans la liste des stratégies.

Affichage des services et stratégies

Pour afficher les services et stratégies

1. Ouvrez PGP Desktop.
2. Cliquez sur le panneau de contrôle Messagerie PGP. Le panneau de contrôle est mis en surbrillance. Tous les services actuellement configurés sont répertoriés dans la partie supérieure du panneau.
3. Cliquez sur un service pour consulter les propriétés du compte et les stratégies de sécurité qui y sont associées. Cette section fournit des informations sur la stratégie de sécurité appliquée. Si votre ordinateur se trouve dans un environnement géré par un PGP Universal Server, les stratégies de sécurité sont définies par votre administrateur.



Si vous utilisez PGP Desktop dans ce type d'environnement, différents messages et/ou options peuvent être affichés au-dessus de la liste des stratégies, suivant la configuration choisie pour la stratégie.

Si la configuration choisie pour la stratégie PGP Universal Server est la suivante :	Le message affiché dans PGP Desktop au-dessus de la liste des stratégies indique :
Stratégie hors connexion de blocage	« Les messages sont bloqués lorsque le serveur est inaccessible. »
Stratégie hors connexion d'envoi en clair	« Les messages sont envoyés en clair lorsque le serveur est inaccessible. »
Stratégie hors connexion : autonome	« Les stratégies autonomes s'appliquent lorsque le serveur est inaccessible. » Vous pouvez utiliser la case à cocher **Afficher les stratégies autonomes**.
Stratégie : autonome	« Les stratégies autonomes suivantes sont appliquées. »

Dans tous les cas, si votre administrateur a indiqué que la stratégie pouvait être remplacée, la case à cocher **Remplacer les stratégies du serveur par des stratégies locales** est disponible.

Création d'un service de messagerie

Un service regroupe des informations relatives à un compte de messagerie électronique et des stratégies de sécurité correspondantes qui doivent être appliquées aux messages sortants.

Important : dans la plupart des cas, PGP Desktop crée les services pour vous, à mesure que vous utilisez votre compte de messagerie électronique pour envoyer et recevoir des messages. Si vous avez besoin de créer un service vous-même, veillez à lire et bien comprendre les présentes instructions. Une mauvaise configuration du service peut engendrer des problèmes lors de l'envoi ou de la réception des messages électroniques.

Pour créer un service

1. Ouvrez PGP Desktop et cliquez sur le panneau de contrôle Messagerie PGP. Le panneau de contrôle est mis en surbrillance.
2. Dans celui-ci, cliquez sur **Nouveau service de messagerie**. Vous pouvez également sélectionner **Messagerie > Créer un service.**

   Dans la zone de travail de la messagerie PGP, les éléments suivants s'affichent : l'intitulé « Nouveau service » en haut de la fenêtre, les champs des propriétés du compte, vides, et les stratégies de sécurité par défaut, dans la section Stratégies de sécurité.
3. Dans le champ **Description** de la section Propriétés du compte, saisissez le nom du service.

4 Dans le champ **Adresse de courrier électronique**, saisissez votre adresse de courrier électronique.

5 Tapez le nom de vos serveurs de messagerie électronique entrant et sortant ou cliquez sur **Paramètres du serveur** pour définir des options avancées. Si vous décidez de définir des options avancées, la boîte de dialogue Paramètres du serveur s'affiche.

6 Sélectionnez le type de serveur utilisé par le nouveau service dans le champ **Type de serveur** :

- **Messagerie sur Internet**, pour les utilisateurs de PGP Desktop autonomes disposant d'une connexion de messagerie POP ou IMAP.
- **PGP Universal**, pour les utilisateurs de PGP Desktop dont l'ordinateur se trouve dans un environnement géré par un PGP Universal Server. Pour plus d'informations sur les paramètres à utiliser, contactez votre administrateur PGP Universal Server.
- **MAPI/Exchange**, pour les utilisateurs de PGP Desktop qui emploient Microsoft Outlook comme client de messagerie sur un serveur Microsoft Exchange/MAPI. Pour plus d'informations sur les paramètres à utiliser, contactez votre administrateur de messagerie électronique.
- **Lotus Notes**, pour les utilisateurs de PGP Desktop qui emploient Lotus Notes comme client de messagerie avec un serveur Lotus Domino. Pour plus d'informations sur les paramètres à utiliser, contactez votre administrateur de messagerie.

Certains champs de la boîte de dialogue Paramètres du serveur varient en fonction du type de serveur que vous avez sélectionné.

Remarque : si vous établissez une connexion manuelle à un serveur PGP Universal Server, reportez-vous à la section *Liaison manuelle à un PGP Universal Server* (à la page 343).

7 Dans la section **Serveur de messagerie entrant**, saisissez les informations suivantes :

- **Nom** : saisissez le nom du serveur de messagerie qui gère les messages entrants.
- **Protocole** : sélectionnez le protocole utilisé pour récupérer les messages sur le serveur de messagerie entrant.

  Le paramètre **Automatique** (disponible pour les types de serveur **Messagerie sur Internet** et **PGP Universal**) permet de détecter automatiquement les connexions POP ou IMAP.
- **Port** : conservez la valeur par défaut Automatique ou indiquez le port de connexion au serveur de messagerie entrant pour récupérer les messages (dans le cas où vous avez sélectionné le type de serveur **Messagerie sur Internet** ou **PGP Universal** et le protocole **POP** ou **IMAP**, pas **Automatique**).

- **SSL/TLS** : indiquez le mode d'interaction de PGP Desktop avec votre serveur de messagerie électronique. Sélectionnez l'une des options suivantes :
  - **Automatique :** PGP fera tout son possible pour fournir la protection SSL/TLS. Il tentera d'abord d'utiliser le deuxième port indiqué, puis d'exécuter la commande STARTTLS (si elle est prise en charge par le serveur) et, si les méthodes précédentes ont échoué, il se connectera au serveur de manière non sécurisée.
  - **STARTTLS requis :** PGP Desktop requiert que le serveur réponde favorablement à la commande STARTTLS.
  - **SSL requis :** PGP Desktop requiert l'acceptation par le serveur des connexions protégées par SSL à l'autre port spécifié.
  - **Aucune tentative :** PGP Desktop ne tente pas de protéger par SSL/TLS la connexion au serveur de messagerie.
- **M'avertir si le client de messagerie fait une tentative de connexion SSL/TLS :** lorsque cette option est sélectionnée, PGP Desktop affiche une boîte de dialogue si le client de messagerie fait une tentative de connexion SSL/TLS, car cette condition est incompatible avec l'envoi de vos messages électroniques par serveur proxy à l'aide de PGP Desktop. (Cette option est sélectionnée par défaut.)

Attention : vous ne devez sélectionner cette option que si vous êtes sûr que votre serveur de messagerie prend en charge le protocole SSL. Cela permet de vous assurer que les messages ne seront pas transférés entre PGP Desktop et le serveur de messagerie via une connexion non sécurisée si, par exemple, un problème survient lors de la négociation de la protection SSL pour la connexion. **Si vous activez cette option alors que votre serveur de messagerie ne prend pas en charge le protocole SSL, PGP Desktop n'enverra ni ne recevra aucun message.**

Serveur de messagerie sortant (SMTP)

- **Nom** : saisissez le nom du serveur de messagerie qui gère les messages sortants.
- **Port** : conservez **Automatique (465, 25)** ou spécifiez un autre port de connexion au serveur de messagerie sortant pour l'envoi de messages.

  Cette option est uniquement disponible pour le serveur de messagerie sortant si vos paramètres vous ont permis de la choisir pour le serveur de messagerie entrant.
- **SSL/TLS** : indiquez le mode d'interaction de PGP Desktop avec votre serveur de messagerie électronique. Sélectionnez l'une des options suivantes :

- **Automatique :** PGP Desktop fera tout son possible pour fournir la protection SSL/TLS. Il tentera d'abord d'utiliser le deuxième port indiqué, puis d'exécuter la commande STARTTLS (si elle est prise en charge par le serveur) et, si les méthodes précédentes ont échoué, il se connectera au serveur de manière non sécurisée.
- **STARTTLS requis :** PGP Desktop requiert que le serveur réponde favorablement à la commande STARTTLS.
- **SSL requis :** PGP Desktop requiert l'acceptation par le serveur des connexions protégées par SSL à l'autre port spécifié.
- **Aucune tentative :** PGP Desktop ne tente pas de protéger par SSL/TLS la connexion au serveur de messagerie.

- **M'avertir si le client de messagerie fait une tentative de connexion SSL/TLS :** lorsque cette option est sélectionnée, PGP Desktop affiche une boîte de dialogue si le client de messagerie fait une tentative de connexion SSL/TLS, car cette condition est incompatible avec l'envoi de vos messages électroniques par serveur proxy à l'aide de PGP Desktop. (Cette option est sélectionnée par défaut.)

Attention : vous ne devez sélectionner cette option que si vous êtes sûr que votre serveur de messagerie prend en charge le protocole SSL. Cela permet de vous assurer que les messages ne seront pas transférés entre PGP Desktop et le serveur de messagerie via une connexion non sécurisée si, par exemple, un problème survient lors de la négociation de la protection SSL pour la connexion. **Si vous activez cette option alors que votre serveur de messagerie ne prend pas en charge le protocole SSL, PGP Desktop n'enverra ni ne recevra aucun message.**

8. Cliquez sur **OK** lorsque vous avez terminé.
9. Dans le champ **Universal Server, sélectionnez le nom du PGP Universal Server qui protège le domaine de messagerie dans lequel vous vous trouvez. <Aucun>** s'affiche si votre ordinateur ne fait pas partie d'un domaine de messagerie protégé par un PGP Universal Server. Si votre domaine est protégé par un PGP Universal Server, mais que celui-ci ne soit pas répertorié dans la liste, sélectionnez **<créer>** pour saisir le nom de votre PGP Universal Server. Pour plus d'informations, contactez votre administrateur PGP Universal Server.
10. Cliquez sur **Mode clé**. La boîte de dialogue du mode de gestion des clés apparaît ; elle précise votre mode clé actuel. Si nécessaire, cliquez sur **Réinitialiser la clé** pour lancer l'assistant d'installation de clé.
11. Cliquez sur **OK**.
12. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur associé au compte de messagerie électronique.
13. Dans le champ **Clé par défaut** est affichée la clé actuelle.

- Si vous utilisez PGP Desktop de manière autonome, vous pouvez conserver la clé par défaut ou en sélectionner une autre dans le menu (si une autre clé est disponible).
- En revanche, si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, la clé par défaut s'affiche et vous ne pouvez pas en changer. Si vous devez changer la clé, cliquez sur Mode clé et suivez la procédure de réinitialisation de clé sur un PGP Universal Server.

14 Cochez la case **Mettre en cache la phrase secrète de cette clé lorsque j'ouvre une session** si vous souhaitez mettre en cache la phrase secrète de la paire de clés que vous venez de sélectionner lorsque vous ouvrez une session.

Si vous ne mettez pas en cache la phrase secrète de la clé, vous êtes invité à la saisir lorsque vous envoyez des messages signés ou recevez des messages chiffrés.

15 Dans la section **Stratégies de sécurité fournies par [nom du serveur]**, les stratégies actuelles applicables sont affichées. Vous pouvez conserver les stratégies de sécurité par défaut, les désactiver ou créer des stratégies si vous utilisez PGP Desktop de manière autonome. Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, les options à votre disposition seront probablement différentes, selon la configuraiton choisie par votre administrateur PGP Universal Server.

16 Si vous avez modifié des stratégies, vous devez cliquer sur **Terminé** lorsque vous avez terminé. Dès que vous en avez terminé avec la configuration des stratégies de sécurité, le compte est prêt à être utilisé. Il n'est pas nécessaire de cliquer sur un bouton quelconque pour enregistrer les informations. Elles sont enregistrées dès que vous les saisissez.

Modification des propriétés du service de messagerie

Attention : avant de modifier un service de messagerie existant, assurez-vous d'avoir fermé votre client de messagerie.

Pour modifier les propriétés du compte d'un service existant

1 Ouvrez PGP Desktop et cliquez sur la boîte de contrôle Messagerie PGP. La boîte de contrôle Messagerie PGP est mise en surbrillance.

2 Cliquez sur le nom du service dont vous voulez modifier les propriétés de compte. Les paramètres du service sélectionné s'affichent dans la zone de travail de la messagerie PGP.

3 Modifiez les propriétés du compte du service, si nécessaire. Pour plus d'informations, reportez-vous à la section *Création d'un service de messagerie* (à la page 103).

Désactivation ou activation d'un service

Si vous ne souhaitez plus utiliser un service, mais que vous ne voulez pas le supprimer car vous pourriez en avoir à nouveau besoin, vous avez la possibilité de le désactiver. Ceci s'avère particulièrement utile si vous souhaitez que PGP Desktop traite uniquement les messages électroniques de certains comptes. Si vous êtes sûr que vous n'aurez plus besoin du service, vous pouvez le supprimer.

Pour désactiver ou activer un service existant

1. Dans la boîte de contrôle Messagerie PGP, cliquez sur le nom du service que vous souhaitez désactiver. Les paramètres du service s'affichent dans la zone de travail de la messagerie PGP.
2. Effectuez l'une des opérations ci-dessous :
   - Pour désactiver le service, sélectionnez **Messagerie > Désactiver le service**. Le service est désactivé.
   - Pour activer le service, sélectionnez **Messagerie > Activer le service**. Le service est activé.

   PGP Desktop vous informe que la modification ne sera prise en compte qu'après avoir redémarré votre client de messagerie.

Conseil : Vous pouvez désactiver, activer et supprimer des services en cliquant avec le bouton droit de la souris sur le nom du service dans la boîte de contrôle Messagerie PGP et en sélectionnant la commande qui vous intéresse.

Suppression d'un service

Si vous êtes certain de ne plus jamais avoir besoin d'un service de messagerie, vous pouvez le supprimer de PGP Desktop.

Pour supprimer un service

1. Cliquez sur le nom du service à supprimer. Les paramètres du service s'affichent dans la zone de travail de la messagerie PGP.
2. Sélectionnez **Messagerie > Supprimer le service**. Le service est supprimé.

Conseil : vous pouvez supprimer un service en cliquant sur son nom avec le bouton droit dans le panneau de contrôle Messagerie PGP, puis en sélectionnant la commande appropriée.

Services multiples

Certains services de messagerie électronique et fournisseurs de services Internet utilisent à tour de rôle plusieurs serveurs de messagerie pour un seul nom de DNS. Dans ce cas, PGP Desktop crée différents services de messagerie pour le même compte de messagerie électronique, car il considère chaque serveur de messagerie comme étant distinct et nécessitant son propre service de messagerie.

PGP Desktop prend en charge le caractère de remplacement pour les services de messagerie électronique les plus courants, par exemple *.yahoo.com et *.me.com (ou *.mac.com). Cependant, si vous utilisez un service de messagerie moins courant ou si les services modifient la configuration de leurs serveurs de messagerie, vous risquez de rencontrer ce problème.

Si vous vous apercevez que PGP Desktop crée plusieurs services pour un même compte de messagerie électronique et que vous constatez, en vérifiant les paramètres, que ceux-ci sont identiques, si ce n'est que le serveur de messagerie du premier service est du type **courrier1.exemple.com, celui du deuxième service du type** `courrier2.exemple.com`, celui du troisième service du type `courrier3.exemple.com`, etc., vous pouvez modifier manuellement l'un de ces services.

La meilleure solution consiste à modifier manuellement l'un des services afin que le nom du serveur de messagerie pour le service en question puisse prendre en charge plusieurs serveurs de messagerie utilisés à tour de rôle. Dans l'exemple ci-dessus, vous pouvez remplacer dans la boîte de dialogue Paramètres du serveur le nom du serveur de l'un des services par `mail*.example.com` et supprimer les autres services.

Certaines configurations de ce type peuvent générer des noms de serveur plus complexes et nécessiter une solution légèrement différente. Par exemple, si PGP Desktop crée des services dont les serveurs de messagerie sont pop.frodon.exemple.com, smtp.bilbon.exemple.com et courrier.exemple.com, la meilleure solution consiste à utiliser le caractère de remplacement de la manière suivante : ***.exemple.com.**

Dépannage des services de messagerie PGP

Par défaut, PGP Desktop détermine automatiquement vos paramètres de compte de messagerie électronique et crée un service de messagerie PGP qui envoit les messages électroniques via un serveur proxy pour ce compte de messagerie.

En raison du grand nombre possible de paramètres du compte de messagerie électronique et de configurations du serveur de messagerie, il peut arriver à l'occasion qu'un service de messagerie créé automatiquement par PGP Desktop ne fonctionne pas correctement.

Si PGP Desktop a créé un service de messagerie qui ne fonctionne pas correctement, l'une ou plusieurs des actions suivantes peuvent corriger le problème :

- Vérifiez que vous pouvez vous connecter à Internet et envoyer et recevoir des messages électroniques lorsque les services PGP sont arrêtés. Pour ce faire :
  - Sous Windows, cliquez avec le bouton droit de la souris sur l'icône de PGP Desktop dans la zone de notification et sélectionnez **Quitter les services PGP** dans la liste des commandes.
  - Sous Mac OS X, maintenez enfoncée la touche Option et sélectionnez **Quitter** dans l'icône PGP Desktop de la barre de menus.

  Remarque : Vous devez toujours redémarrer votre client de messagerie après avoir arrêté ou démarré les services PGP.
- Vérifiez dans les notes de publication PGP Desktop relatives à la version de PGP Desktop que vous utilisez s'il s'agit d'un problème connu.
- Vérifiez que l'authentification SMTP est activée pour le compte de messagerie électronique (dans votre client de messagerie). Ceci est recommandé pour que PGP Desktop puisse envoyer vos messages par serveur proxy. Si vous disposez d'un seul compte de messagerie électronique et que vous n'utilisez pas PGP Desktop dans un environnement géré par un PGP Universal Server, l'authentification SMTP n'est pas nécessaire. Elle *est* requise lorsque vous utilisez un PGP Universal Server en tant que serveur SMTP ou lorsque vous possédez plusieurs comptes de messagerie sur le même serveur SMTP.
- Recherchez dans les entrées du journal de PGP d'éventuels indices sur l'origine du problème.
- Si la protection SSL/TLS est activée dans votre client de messagerie, vous devez la désactiver ici pour que PGP Desktop puisse envoyer vos messages par serveur proxy. (La connexion entre votre client et votre serveur de messagerie n'en est *pas* pour autant non protégée. Par défaut, PGP Desktop tente automatiquement d'appliquer la protection SSL/TLS pour sécuriser toute connexion non protégée. Le serveur de messagerie doit prendre en charge le protocole SSL/TLS pour que la connexion puisse être protégée.)
- Si l'option **STARTTLS requis** ou **SSL requis** est sélectionnée dans les paramètres SSL/TLS de la boîte de dialogue Paramètres du serveur, votre serveur de messagerie *doit* prendre en charge le protocole SSL/TLS, faute de quoi PGP Desktop ne pourra ni envoyer, ni recevoir de messages.
- Si votre compte de messagerie utilise des numéros de port non standard, vérifiez qu'ils sont bien inclus dans les paramètres de votre service de messagerie.

- Si PGP Desktop crée plusieurs services de messagerie pour le même compte de messagerie électronique, utilisez un caractère de remplacement dans le nom de votre serveur de messagerie. Pour plus d'informations, reportez-vous à la section *Services multiples* (à la page 109).
- Supprimez le service de messagerie PGP qui pose problème et envoyez/recevez des messages électroniques. PGP Desktop regénèrera le service de messagerie.

Si aucune des solutions ci-dessus ne résout le problème, suivez la procédure ci-dessous :

1. Supprimez le service de messagerie PGP qui ne fonctionne pas correctement.
2. Arrêtez tous les services PGP Desktop et quittez PGP Desktop, s'il est ouvert. Pour arrêter les services :
   - Sous Windows, cliquez avec le bouton droit de la souris sur l'icône de PGP Desktop dans la zone de notification et sélectionnez **Quitter les services PGP** dans la liste des commandes.
   - Sous Mac OS X, maintenez enfoncée la touche Option et sélectionnez **Quitter** dans l'icône PGP Desktop de la barre de menus.
3. Vérifiez que votre connexion Internet fonctionne et que vous pouvez envoyer et recevoir des messages électroniques lorsque les services de messagerie PGP sont arrêtés.
4. Ouvrez votre client de messagerie et notez les paramètres de votre compte de messagerie électronique (y compris le nom d'utilisateur, l'adresse de courrier électronique, le serveur de messagerie entrant et sortant, le protocole du serveur de messagerie entrant et le numéro des ports non standard du serveur de messagerie).
5. Fermez votre client de messagerie et redémarrez PGP Desktop, ce qui a pour effet de redémarrer les services PGP :
   - Sous Windows, redémarrez votre ordinateur ou ouvrez PGP Desktop depuis le menu Démarrer.
   - Sous Mac OS X, redémarrez votre ordinateur ou ouvrez PGP Desktop.
6. Créez manuellement un service de messagerie PGP en utilisant les paramètres du compte que vous avez notés.
7. Ouvrez votre client de messagerie et envoyez et recevez des messages.
8. Si les problèmes persistent, recherchez de l'aide ici :
   - *Site Web de PGP Corporation* (http://www.pgp.com)
   - *Site Web de support de PGP* (https://support.pgp.com)
   - *Forums de support de PGP* (http://forum.pgp.com)

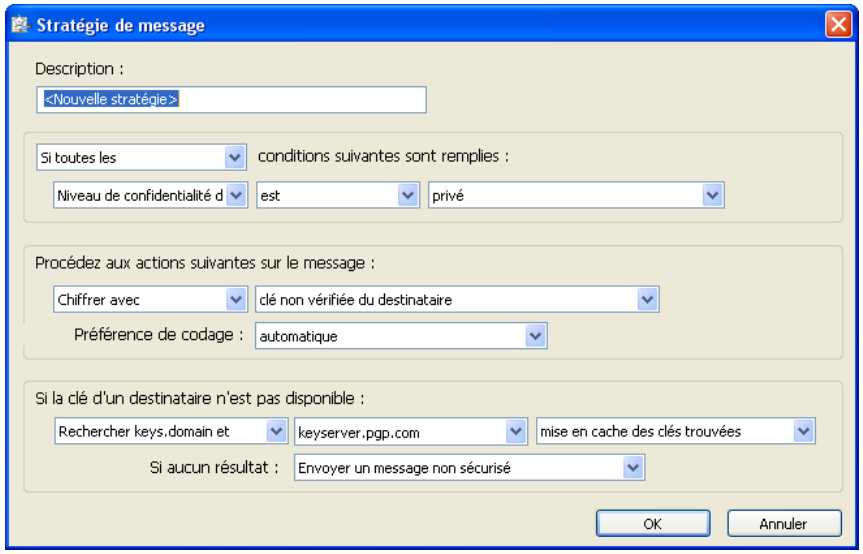
Création d'une stratégie de sécurité

Les stratégies de sécurité permettent de contrôler la manière dont PGP Desktop gère les messages électroniques sortants.

Remarque : Lorsque vous créez une stratégie de sécurité, vous créez une stratégie de sécurité de messagerie, pas une stratégie de liste de publipostage. Vous ne pouvez pas créer de stratégie de liste de publipostage, mais vous pouvez modifier celles par défaut.

Pour créer une stratégie de sécurité

1. Dans la boîte de contrôle Messagerie PGP, cliquez sur le nom du service pour lequel vous voulez créer une stratégie de sécurité. Les paramètres du service, y compris la liste des stratégies de sécurité existantes, apparaissent dans la zone de travail de la messagerie PGP.
2. Effectuez l'une des opérations ci-dessous :
   - Dans la boîte de contrôle Messagerie PGP, cliquez sur **Nouvelle stratégie**.
   - Sélectionnez **Messagerie > Nouvelle stratégie de messagerie**. La boîte de dialogue Stratégie de message apparaît.



   Si votre domaine de messagerie est protégé par un PGP Universal Server, les champs proposés dans la boîte de dialogue Stratégie de message pour une stratégie à partir d'un PGP Universal Server peuvent être différents de ceux présentés ci-dessus.
3. Dans le champ **Description**, tapez un nom descriptif pour la stratégie que vous êtes en train de créer.

4 Dans le champ **Si** de la première section (indiquant les conditions de la stratégie), sélectionnez :

- **Si au moins une** : la stratégie s'applique lorsque au moins une condition est remplie.
- **Si toutes** : la stratégie s'applique uniquement lorsque toutes les conditions sont remplies.
- **Si aucune** : la stratégie s'applique uniquement si aucune condition n'est remplie.

5 Dans le premier champ de condition, sélectionnez :

- **Destinataire** : la stratégie s'applique uniquement aux messages envoyés au destinataire spécifié.
- **Domaine du destinataire** : la stratégie s'applique uniquement aux messages électroniques du domaine de destinataire spécifié.
- **Expéditeur : la stratégie s'applique uniquement aux messages possédant l'adresse d'expéditeur spécifiée.**
- **Message : la stratégie s'applique uniquement aux messages possédant l'état signé ou chiffré spécifié.**
- **Objet du message** : la stratégie s'applique uniquement aux messages possédant l'objet spécifié.
- **En-tête de message** : la stratégie s'applique uniquement aux messages pour lesquels l'en-tête spécifié correspond au critère indiqué. Les conditions décrites dans la section suivante (est, n'est pas, contient, etc.) s'appliquent au texte tapé dans la zone de texte qui s'affiche lorsque vous sélectionnez **En-tête de message**.

Remarque : lorsque vous recherchez des en-têtes de message dans les systèmes de messagerie MAPI, vous pouvez uniquement utiliser les en-têtes Objet, Niveau de confidentialité, Priorité et Importance.

- **Corps du message** : la stratégie s'applique uniquement aux messages possédant le corps spécifié.
- **Taille du message : la stratégie s'applique uniquement aux messages possédant la taille spécifiée (en octets).**
- **Priorité du message** : la stratégie s'applique uniquement aux messages possédant la priorité spécifiée.
- **Niveau de confidentialité du message** : la stratégie s'applique uniquement aux messages possédant le niveau de confidentialité spécifié.

6 Dans le deuxième champ de condition, sélectionnez :

- **est** : la condition est remplie lorsque le texte du premier champ de condition *correspond* à celui tapé dans la zone de texte.
- **n'est pas** : la condition est remplie lorsque le texte du premier champ de condition *ne correspond pas* à celui tapé dans la zone de texte.

- **contient** : la condition est remplie lorsque le texte du premier champ de condition *contient* celui tapé dans la zone de texte.
- **ne contient pas** : la condition est remplie lorsque le texte du premier champ de condition *ne contient pas* celui tapé dans la zone de texte.
- **commence par** : la condition est remplie lorsque le texte du premier champ de condition *commence par* celui tapé dans la zone de texte.
- **finit par** : la condition est remplie lorsque le texte du premier champ de condition *finit par* celui tapé dans la zone de texte.
- **correspond au modèle** : la condition est remplie lorsque le texte du premier champ de condition *correspond au modèle* tapé dans la zone de texte.
- **supérieur à** : la condition est remplie lorsque la taille du message est *supérieure à* celle du texte tapé dans la zone de texte.
- **inférieur à** : la condition est remplie lorsque la taille du message est *inférieure à* celle du texte tapé dans la zone de texte.

7 Dans le troisième champ de condition, sélectionnez :

- **zone de texte** : saisissez le texte du critère correspondant. Par exemple, si vous avez sélectionné **Taille du message** est **supérieur à**, tapez un nombre représentant la taille du message.
- **normale** : le critère correspondant au niveau de confidentialité du message est *normal*.
- **aucun** ou **normal** : le critère correspondant au niveau de confidentialité du message est *aucun* (sous Mac OS X) ou *normal* (sous Windows).
- **personnel** : le critère correspondant au niveau de confidentialité du message est *personnel*.
- **privé** : le critère correspondant au niveau de confidentialité du message est *privé*.
- **confidentiel** : le critère correspondant au niveau de confidentialité du message est *confidentiel*.
- **signé** : le critère correspondant au message est signé.
- **chiffré** : le critère correspondant au message est chiffré.
- **chiffré avec ID de clé** : critère correspondant à la valeur « chiffré avec ID de clé » (vous devez ensuite taper un ID de clé dans la zone de texte qui s'affiche).
- **faible** : le critère correspondant à la priorité du message est *faible*.
- **normale** : le critère correspondant à la priorité du message est *normale*.
- **haute** : le critère correspondant à la priorité du message est *haute*.

Créez plus de lignes de conditions en cliquant sur l'icône plus.

8 Dans le premier champ d'action de la section **Procédez aux actions suivantes sur le message**, sélectionnez :

- **Envoyer en texte en clair** : cette option indique que le message doit être envoyé en clair, c'est-à-dire ni signé, ni chiffré.
- **Signer** : cette option indique que le message doit être signé.
- **Chiffrer avec** : cette option indique que le message doit être chiffré.

9 Dans le deuxième champ d'action, sélectionnez :

- **clé vérifiée du destinataire** : le message peut uniquement être chiffré avec une clé vérifiée du destinataire souhaité.
- **clé non vérifiée du destinataire** : le message peut être chiffré avec une clé non vérifiée du destinataire souhaité. Le chiffrement peut également se faire avec une clé vérifiée, le cas échéant.
- **clé de bout en bout vérifiée du destinataire** : le message peut uniquement être chiffré avec une clé de bout en bout vérifiée du destinataire souhaité. Une clé de bout en bout est une clé que seul le destinataire individuel possède. Dans un environnement géré par un PGP Universal Server, il s'agit d'une clé Mode clé client qui est différente d'une clé Mode clé de serveur, où le PGP Universal Server est en possession de la clé.

  Le fait que la clé soit de bout en bout ou non est indiqué dans le champ **Groupe** de la boîte de dialogue Propriétés de la clé sous Windows ou de la boîte de dialogue Infos sur la clé sous Mac OS X. **Non** signifie que la clé *est* une clé de bout en bout (elle ne fait pas partie d'un groupe) et **Oui** indique qu'elle *n'est pas* une clé de bout en bout.
- **clé de bout en bout non vérifiée du destinataire** : le message peut être chiffré avec une clé de bout en bout non vérifiée du destinataire souhaité. Le chiffrement peut également se faire avec une clé vérifiée, le cas échéant.
- **une liste de clés** : cette option indique que le message peut uniquement être chiffré avec les clés de la liste.

Créez plus de lignes d'actions en cliquant sur l'icône plus.

10 Dans le champ de préférence de codage du message, sélectionnez :

- **automatique** : PGP Desktop choisit le format de codage du message. Il s'agit généralement de l'option à utiliser de préférence, sauf si vous savez exactement pourquoi vous devez utiliser l'un des autres formats de codage de message de manière explicite.
- **PGP partitionné** : cette option définit PGP partitionné en tant que format de codage de message par défaut. Ce format est celui qui présente la meilleure compatibilité ascendante avec les anciens produits PGP et OpenPGP.

- **PGP/MIME** : cette option définit PGP/MIME en tant que format de codage de message par défaut. Le format PGP/MIME permet de chiffrer et de signer l'ensemble du message, pièces jointes comprises, en une seule passe. Il est par conséquent généralement plus rapide et plus efficace pour la reproduction fidèle d'un message.
- **S/MIME** : cette option définit S/MIME en tant que format de codage de message par défaut. Choisissez S/MIME si, pour une raison ou pour une autre, vous devez appliquer ce format de façon forcée à des messages même si l'utilisateur possède une clé PGP.

11 Dans la section **Si la clé d'un destinataire n'est pas disponible** (ou dans la section **Si une clé de destinataire est introuvable** sous Mac OS X), dans le premier champ **Clé introuvable**, sélectionnez :

- **Rechercher keys.domain et : cette option indique une recherche qui inclut les deux keys.domain, ainsi qu'un autre serveur que vous spécifiez.**
- **Rechercher** : cette option permet la recherche d'une clé appropriée si aucune n'est trouvée dans le trousseau de clés local.
- **Message avec signature numérique lisible : cette option indique que le message doit être envoyé en texte en clair, mais signé.**
- **Envoyer un message non sécurisé : cette option indique que le message doit être envoyé en texte en clair.**
- **Bloquer message** : cette option indique que le message ne doit pas être envoyé si aucune clé appropriée n'est trouvée.

12 Dans le deuxième champ Clé introuvable, sélectionnez :

- **Tous les serveurs de clés** : cette option permet de rechercher une clé appropriée dans tous les serveurs de clés, y compris le PGP Global Directory.
- **PGP Global Directory ou keyserver.pgp.com** : cette option indique que la recherche a lieu uniquement dans le PGP Global Directory.
- **[serveurs de clés configurés]** : cette option indique que la recherche a lieu uniquement dans le serveur de clés que vous choisissez dans la liste des serveurs de clés actuellement configurés. Les serveurs de clés autres que le PGP Global Directory peuvent fournir des clés non vérifiées qu'il n'est pas possible d'utiliser si la stratégie requiert des clés vérifiées. À moins que vous ne sachiez exactement pourquoi vous devez effectuer la recherche sur un autre serveur de clés et que vous ne soyez prêt à chercher ces clés manuellement pour les vérifier lorsque cela s'avère nécessaire, limitez la recherche au PGP Global Directory. Elle est disponible uniquement sur les systèmes Windows.
- **Modifier la liste des serveurs de clés** : cette option permet d'ajouter des serveurs de clés à la liste des serveurs de clés actuellement configurés. Elle est disponible uniquement sur les systèmes Windows.

13 Dans le dernier champ Clé introuvable, indiquez :

- **cache temporaire des clés trouvées** : cette option indique qu'une clé trouvée doit être temporairement enregistrée dans la mémoire. Les clés figurant dans ce cache sont automatiquement utilisées lors de la vérification des messages signés. Elles le sont également pour le chiffrement si elles ont été vérifiées.
- **demander d'enregistrer les clés trouvées** : cette option indique que PGP Desktop doit vous demander si vous voulez enregistrer dans votre trousseau de clés local une clé trouvée spécifique.
- **enregistrer les clés trouvées** : cette option indique que les clés trouvées doivent être automatiquement enregistrées dans votre trousseau de clés local.

14 Dans le champ Si aucun résultat, sélectionnez :

- **Message avec signature numérique lisible : les messages pour lesquels aucune clé de chiffrement n'a été trouvée peuvent être signés et envoyés en texte en clair.**
- **Envoyer un message non sécurisé : avec cette option, les messages ne sont pas chiffrés.**
- **Bloquer message : cette option empêche l'envoi d'un message pour lequel aucune clé de chiffrement n'a été trouvée.**

15 Cliquez sur **OK** lorsque les paramètres de stratégie sont configurés. La nouvelle stratégie s'affiche dans la liste des stratégies de sécurité.

Expressions normales dans les stratégies

PGP Desktop prend en charge l'utilisation des expressions normales dans les zones de texte des stratégies de sécurité. L'emploi d'expressions normales vous permet de faire référence à différentes chaînes de texte à l'aide d'une seule chaîne de texte.

Remarque : hormis les exemples ci-dessous, PGP Desktop prend en charge des expressions normales plus larges respectant les formats standard. Les critères « correspond au modèle » signifient « correspond à l'expression normale ».

Selon certaines conditions de règle applicables aux stratégies de messagerie, une partie d'un message doit nécessairement correspondre à un modèle. Les modèles inclus dans la condition se présentent sous la forme d'une expression normale. Une expression normale est une chaîne de caractères qui définit le format que doit respecter un terme. Tout terme dont le format correspond à celui de l'expression normale est considéré comme valable.

Voici quelques éléments courants dans les expressions normales :

?	indique que zéro ou un seul caractère de l'expression précédente doit être repris.

`+`	indique qu'au moins un caractère de l'expression précédente doit être repris.
`.`	remplace un caractère unique.
`*`	indique que zéro, un seul ou plusieurs caractères de l'expression précédente doivent être repris.
`[ ]`	remplace le caractère unique précisé entre les crochets.
`[a-z]`	fait référence à une lettre minuscule allant de a à z.
`[1-9]`	fait référence à un chiffre compris entre 1 et 9.
`{n}`	représente une suite de n correspondances pour l'expression.

Ci-après sont fournis des exemples d'expressions normales destinées à rechercher les éléments courants pouvant apparaître dans un message électronique sensible.

Données	Exemple	Expression normale
Numéro de téléphone	(555)555-4567	\(?[2-9][0-9]{2}[\]-.)[2-9][0-9]{2}[-.][0-9]{4}
Adresse de courrier électronique	jean@exemple.fr	[a-zA-Z0-9._%-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,6}
Numéro de carte bancaire	1234 1234 1234 1234	[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
Numéro de sécurité sociale	123-45-6789	[0-9]{3}-[0-9]{2}-[0-9]{4}
Ville, abréviation d'État	Palo Alto, CA	.*, [A-Z][A-Z]
Abréviation d'État à 2 caractères	CA	[A-Z][A-Z]
Code postal	12345	[0-9]{5}(-[0-9]{4})?
Montants en dollars, avec symbole $ devant	$3.95	\$[0-9]+.[0-9][0-9]
Date au format numérique	2003-08-06	[0-9]{4}-[0-9]{2}-[0-9]{2}
Date au format alphanumérique	Jan 3, 2003	(Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)\.?(3[0-1]|[1-2][0-9]|0?[0-9]), [0-9]{4}
URL HTTP	http://www.example.com	https?://(([012][0-9]{0,2}\.){3}[012][0-9]{0,2}|([a-zA-Z0-9]+\.)+[a-zA-Z0-9

Données	Exemple	Expression normale
		]{2,6})(/.*)?
Adresse IP	123.123.123.123	([012][0-9]{0,2}\.){3}[012][0-9]{0,2}
Ligne vide		^$

Informations sur les stratégies de sécurité et exemples

Lorsque vous créez un service, plusieurs stratégies de sécurité par défaut sont créées automatiquement :

- Demander le chiffrement : confidentiel [PGP]
- Boutons Signer + Chiffrer*
- Bouton Signer*
- Bouton Chiffrer*
- Demandes administrateur de liste de publipostage
- Envois de listes de publipostage
- Chiffrement opportuniste

* *Ces stratégies sont disponibles uniquement dans PGP Desktop pour Windows.*

L'ordre des règles de stratégie par défaut est important. Il doit être entièrement conforme à la description fournie plus haut.

Cette section décrit le fonctionnement des stratégies de sécurité par défaut. Elle présente également deux situations dans lesquelles vous pouvez souhaiter créer une stratégie de sécurité et en explique la configuration dans chaque cas.

Remarque : si vous modifiez les stratégies par défaut et que vous souhaitiez rétablir les paramètres par défaut, cliquez sur **Revenir à la valeur par défaut** (sous Windows) ou **Rétablir** (sous Mac OS X) dans la boîte de dialogue Stratégie de message.

Bouton Chiffrer (stratégie par défaut)

Le bouton Chiffrer est l'une des stratégies de sécurité par défaut que PGP Desktop crée automatiquement pour un service. Les paramètres de cette stratégie sont les suivants :

- Si : Si tous
- Conditions : l'en-tête de message « X-PGP-Encrypt-Button » contient « selected ».
- Actions : chiffrer avec la clé vérifiée du destinataire

- Préférence de codage : automatique
- Si la clé d'un destinataire n'est pas disponible : rechercher dans keys.domain et keyserver.pgp.com et mettre temporairement en cache les clés trouvées
- Si aucun résultat : bloquer message

Cette règle doit figurer en quatrième position dans la liste des stratégies par défaut.

Remarque : si vous avez effectué une mise à niveau à partir de la version 9.x de PGP Desktop pour Windows, cette stratégie n'est pas automatiquement incluse, et vous devez la créer manuellement avec les paramètres décrits ci-dessus. Pour savoir comment créer une stratégie, reportez-vous à la section *Création d'une stratégie de sécurité* (à la page 112). Si vous n'envisagez pas d'utiliser le bouton Chiffrer avec Microsoft Outlook, il est inutile de créer cette stratégie.

Demandes administrateur de liste de publipostage (stratégie par défaut)

Demandes administrateur de liste de publipostage est une autre des stratégies de sécurité par défaut que PGP Desktop crée automatiquement pour un service.

Les paramètres de cette stratégie sont les suivants :

- Si : au moins un
- Conditions : Destinataire / correspond au modèle/ .*-subscribe@.*, .*-unsubscribe@.*, .*-report@.*, .*-request@.*, .*-bounce@.*,
- Actions : envoyer en texte en clair

Cette règle doit figurer en cinquième position dans la liste des stratégies par défaut.

Envois de listes de publipostage (stratégie par défaut)

Les envois de listes de publipostage constituent une autre stratégie de sécurité par défaut que PGP Desktop crée automatiquement pour un service.

Les paramètres de cette stratégie sont les suivants :

- Si : au moins un
- Conditions : Destinataire / correspond au modèle/ .*-users@.*, .*-bugs@.*, .*-docs@.*, .*-help@.*, .*-news@.*, .*-digest@.*, .*-list@.*, .*-devel@.*, .*-announce@.*,
- Actions : signer
- Préférence de codage : PGP partitionné

Cette règle doit figurer en sixième position dans la liste des stratégies par défaut.

Chiffrement opportuniste (stratégie par défaut)

Le chiffrement opportuniste est l'une des stratégies de sécurité par défaut que PGP Desktop crée automatiquement pour un service. Les paramètres de cette stratégie sont les suivants :

- Si : au moins un
- Conditions : Domaine du destinataire / est / *
- Actions : signer et chiffrer avec la clé vérifiée du destinataire
- Préférence de codage du message : automatique
- Clé introuvable : rechercher dans keys.domain et keyserver.pgp.com et mettre temporairement en cache les clés trouvées
- Si aucun résultat : envoyer un message non sécurisé

Cette règle doit figurer en septième (dernière) position dans la liste des stratégies par défaut.

Avec le chiffrement opportuniste, les messages pour lesquels une clé vérifiée a été trouvée sont envoyés signés et chiffrés. Ceux pour lesquels aucune clé vérifiée n'a été trouvée sont envoyés non chiffrés (en clair). Ainsi, tous vos messages sont envoyés, même si certains peuvent l'être en clair.

Cette stratégie a été conçue pour être placée en dernière position dans la liste des stratégies de sécurité, car elle est applicable à tous les messages. Si cette stratégie est placée avant une stratégie plus appropriée dans la liste, PGP Desktop n'atteindra jamais cette dernière, la rendant alors inutile.

Demander le chiffrement : confidentiel [PGP] (stratégie par défaut)

Demander le chiffrement : confidentiel [PGP] est une autre des stratégies de sécurité par défaut que PGP Desktop crée automatiquement pour un service. Les paramètres de cette stratégie sont les suivants :

- Si : au moins un
- Conditions : Objet du message / contient / [PGP]
  Niveau de confidentialité du message / est / confidentiel
- Actions : signer et chiffrer avec la clé vérifiée du destinataire
- Préférence de codage du message : automatique
- Clé introuvable : rechercher dans keys.domain et sur tous les serveurs de clés et mettre temporairement en cache les clés trouvées

Si aucun résultat : bloquer message Cette règle doit figurer en première position dans la liste des stratégies. Demander le chiffrement : confidentiel [PGP] a pour effet de soumettre l'envoi des messages dont l'objet contient [PGP] ou qui sont marqués comme confidentiels dans votre client de messagerie à un chiffrement obligatoire avec une clé vérifiée. Si aucune clé vérifiée n'a pu être trouvée, le message n'est *pas* envoyé.

Boutons Signer + Chiffrer (stratégie par défaut)

Les boutons Chiffrer et Signer constituent une autre stratégie de sécurité par défaut que PGP Desktop crée automatiquement pour un service. Les paramètres de cette stratégie sont les suivants :

- Si : Si tous
- Conditions : l'en-tête de message « X-PGP-Sign-Button » contient « selected » ; l'en-tête de message « X-PGP-Encrypt-Button » contient « selected ».
- Actions : signer ; chiffrer avec la clé vérifiée du destinataire
- Préférence de codage : automatique
- Si la clé d'un destinataire n'est pas disponible : rechercher dans keys.domain et keyserver.pgp.com et mettre temporairement en cache les clés trouvées
- Si aucun résultat : bloquer message

Cette règle doit figurer en deuxième position dans la liste des stratégies par défaut.

Remarque : si vous avez effectué une mise à niveau à partir de la version 9.x de PGP Desktop pour Windows, cette stratégie n'est pas automatiquement incluse, et vous devez la créer manuellement avec les paramètres décrits ci-dessus. Pour savoir comment créer une stratégie, reportez-vous à la section *Création d'une stratégie de sécurité* (à la page 112). Si vous n'envisagez pas d'utiliser le bouton Chiffrer avec Microsoft Outlook, il est inutile de créer cette stratégie.

Bouton Signer (stratégie par défaut)

Le bouton Signer représente une autre des stratégies de sécurité par défaut que PGP Desktop crée automatiquement pour un service. Les paramètres de cette stratégie sont les suivants :

- Si : Si tous
- Conditions : l'en-tête de message « X-PGP-Sign-Button » contient « selected ».
- Actions : Signer
- Préférence de codage : automatique

Cette règle doit figurer en troisième position dans la liste des stratégies par défaut.

Remarque : si vous avez effectué une mise à niveau à partir de la version 9.x de PGP Desktop pour Windows, cette stratégie n'est pas automatiquement incluse, et vous devez la créer manuellement avec les paramètres décrits ci-dessus. Pour savoir comment créer une stratégie, reportez-vous à la section *Création d'une stratégie de sécurité* (à la page 112). Si vous n'envisagez pas d'utiliser le bouton Chiffrer avec Microsoft Outlook, il est inutile de créer cette stratégie.

Exemple de stratégie d'obligation de chiffrement pour l'envoi de messages vers un <Domaine> particulier

Si vous utilisez le chiffrement opportuniste, avec ses paramètres par défaut, et que vous placez cette stratégie à la fin de la liste des stratégies, les messages pour lesquels aucune clé vérifiée n'aura pu être trouvée seront envoyés en clair. Certes, grâce à cette stratégie, tous vos messages seront envoyés, mais certains d'entre eux seront envoyés en clair.

Si, pour certains domaines, l'envoi en clair est inenvisageable, vous pouvez créer une stratégie de sécurité qui *requiert* le chiffrement et/ou la signature des messages pour que ceux-ci puissent être envoyés. Lorsque vous créez cette stratégie, assurez-vous de la placer avant le chiffrement opportuniste dans la liste des stratégies.

- Si : au moins un
- Conditions : Domaine du destinataire / est / exemple.com
- Actions : Chiffrer avec / clé vérifiée du destinataire
- Préférence de codage du message : automatique
- Clé introuvable : Rechercher keys.domain et / Tous les serveurs de clés / mise en cache temporaire des clés trouvées
- Si aucun résultat : Bloquer message

Cette stratégie de sécurité est semblable à la stratégie Demander le chiffrement : confidentiel [PGP]. En effet, toutes deux requièrent le chiffrement du message pour qu'il puisse être envoyé. Toutefois, le critère à satisfaire ici n'est pas que le message soit marqué comme confidentiel, mais que le domaine de messagerie du destinataire soit exemple.com. L'utilisation de cette stratégie vous garantit que tous les messages envoyés vers exemple.com sont chiffrés à l'aide d'une clé vérifiée.

Exemple de stratégie de signature et d'envoi d'un message en clair vers un domaine particulier

Si vous envoyez régulièrement des messages électroniques vers un domaine pour lequel vous souhaitez que tous les messages soient signés mais non chiffrés, vous devez configurer une stratégie pour ce domaine.

- Si : au moins un

- Conditions : Domaine du destinataire / est / exemple.com
- Actions : Signer
- Préférence de codage du message : automatique

Utilisation de la liste des stratégies de sécurité

Vous pouvez intervenir de différentes manières sur la liste des stratégies de sécurité. En effet, vous pouvez modifier une stratégie, en ajouter une (cf. *Création d'une stratégie de sécurité* (à la page 112)), en supprimer une ou encore modifier l'ordre des stratégies dans la liste.

Modification d'une stratégie de sécurité

Pour modifier une stratégie de sécurité

1. Ouvrez PGP Desktop et cliquez sur le panneau de contrôle Messagerie PGP. Le panneau de contrôle est mis en surbrillance.
2. Dans celui-ci, cliquez sur le nom du service qui contient la stratégie de sécurité que vous souhaitez modifier. Les propriétés du service choisi s'affichent dans la zone de travail de la messagerie PGP.
3. Cliquez sur **Modifier les stratégies**.
4. Sélectionnez la stratégie de sécurité que vous souhaitez modifier, puis effectuez l'une des opérations suivantes :
   - Pour modifier la stratégie, cliquez sur **Modifier la stratégie**. La boîte de dialogue Stratégie de message s'ouvre et affiche les paramètres actuels de la stratégie sélectionnée. Apportez les changements souhaités à la stratégie. Pour plus d'informations sur les champs de la boîte de dialogue Stratégie de message, reportez-vous à la section *Création d'une stratégie de sécurité* (à la page 112). Une fois que les modifications ont été effectuées, cliquez sur **OK** pour fermer la boîte de dialogue Stratégie de message. La stratégie de sécurité spécifiée est modifiée.
   - Pour supprimer la stratégie, cliquez sur **Supprimer la stratégie**.
   - Pour créer une copie de la stratégie (à utiliser comme base d'une nouvelle stratégie), cliquez sur **Dupliquer la stratégie**.
   - Pour déplacer la stratégie vers le haut ou vers le bas de la liste (et modifier ainsi l'ordre d'application des stratégies), cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.

Vous pouvez consulter, modifier et désactiver les stratégies par défaut, mais vous ne pouvez pas les supprimer.

5 Cliquez sur **Terminé**.

Modification d'une stratégie de liste de publipostage

Pour modifier une stratégie de liste de publipostage par défaut

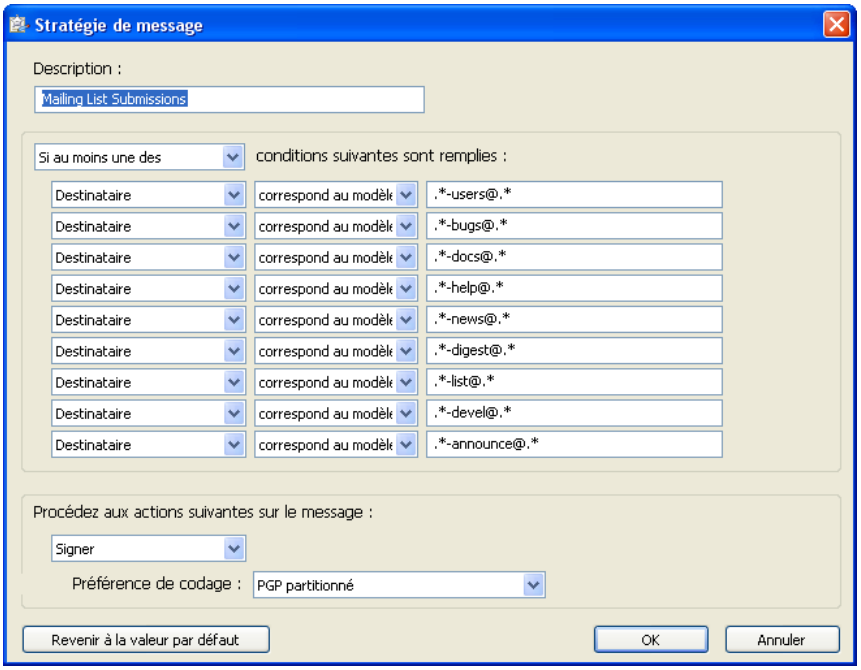
1 Ouvrez PGP Desktop et cliquez sur la boîte de contrôle Messagerie PGP. La boîte de contrôle Messagerie PGP est sélectionnée.

2 Dans la boîte de contrôle Messagerie PGP, cliquez sur le nom du service qui contient la stratégie de sécurité que vous souhaitez modifier. Les propriétés du service choisi s'affichent dans la zone de travail de la messagerie PGP.

3 Cliquez sur le bouton **Modifier les stratégies**.

4 Dans la liste des stratégies de sécurité, cliquez sur la stratégie de liste de publipostage que vous voulez modifier. La stratégie sélectionnée est alors mise en surbrillance.

5 Cliquez sur **Modifier la stratégie**. La boîte de dialogue Stratégie de message s'ouvre et affiche les paramètres actuels de la stratégie sélectionnée.



Vous pouvez consulter, modifier et désactiver les stratégies par défaut, mais vous ne pouvez pas les supprimer.

6 Apportez les changements souhaités à la stratégie. Dans le premier champ, sélectionnez :

- **Si au moins une** : la stratégie s'applique lorsque au moins une condition est remplie.
- **Si toutes** : la stratégie s'applique uniquement lorsque toutes les conditions sont remplies.
- **Si aucune** : la stratégie s'applique uniquement si aucune condition n'est remplie.

7 Dans le premier champ de condition, sélectionnez :

- **Destinataire** : la stratégie s'applique uniquement aux messages envoyés au destinataire spécifié.
- **Domaine du destinataire** : la stratégie s'applique uniquement aux messages électroniques du domaine de destinataire spécifié.
- **Expéditeur : la stratégie s'applique uniquement aux messages possédant l'adresse d'expéditeur spécifiée.**
- **Message : la stratégie s'applique uniquement aux messages possédant l'état signé ou chiffré spécifié.**
- **Objet du message** : la stratégie s'applique uniquement aux messages possédant l'objet spécifié.
- **En-tête de message** : la stratégie s'applique uniquement aux messages pour lesquels l'en-tête spécifié correspond au critère indiqué. Les conditions décrites dans la section suivante (est, n'est pas, contient, etc.) s'appliquent au texte tapé dans la zone de texte qui s'affiche lorsque vous sélectionnez **En-tête de message**.

Remarque : la recherche d'en-têtes de message dans les systèmes de messagerie Lotus Notes et MAPI n'est pas implémentée, car les messages de ces systèmes ne comportent pas d'en-têtes.

- **Corps du message** : la stratégie s'applique uniquement aux messages possédant le corps spécifié.
- **Taille du message : la stratégie s'applique uniquement aux messages possédant la taille spécifiée (en octets).**
- **Priorité du message** : la stratégie s'applique uniquement aux messages possédant la priorité spécifiée.
- **Niveau de confidentialité du message** : la stratégie s'applique uniquement aux messages possédant le niveau de confidentialité spécifié.

8 Dans le deuxième champ de condition, sélectionnez :

- **est** : la condition est remplie lorsque le texte du premier champ de condition *correspond* à celui tapé dans la zone de texte.
- **n'est pas** : la condition est remplie lorsque le texte du premier champ de condition *ne correspond pas* à celui tapé dans la zone de texte.

- **contient** : la condition est remplie lorsque le texte du premier champ de condition *contient* celui tapé dans la zone de texte.
- **ne contient pas** : la condition est remplie lorsque le texte du premier champ de condition *ne contient pas* celui tapé dans la zone de texte.
- **commence par** : la condition est remplie lorsque le texte du premier champ de condition *commence par* celui tapé dans la zone de texte.
- **finit par** : la condition est remplie lorsque le texte du premier champ de condition *finit par* celui tapé dans la zone de texte.
- **correspond au modèle** : la condition est remplie lorsque le texte du premier champ de condition *correspond au modèle* tapé dans la zone de texte.

9 Dans la zone de texte du troisième champ de condition, saisissez le texte du critère correspondant.

10 Dans le premier champ d'action de la section Procédez aux actions suivantes sur le message, sélectionnez :

- **Envoyer en texte en clair** : cette option indique que le message doit être envoyé en clair, c'est-à-dire ni signé, ni chiffré.
- **Signer** : cette option indique que le message doit être signé.
- **Chiffrer avec** : cette option indique que le message doit être chiffré.

11 Dans le deuxième champ d'action, sélectionnez :

- **clé vérifiée du destinataire** : le message peut uniquement être chiffré avec une clé vérifiée du destinataire souhaité.
- **clé non vérifiée du destinataire** : le message peut être chiffré avec une clé non vérifiée du destinataire souhaité.

  clé de bout en bout vérifiée du destinataire : le message peut uniquement être chiffré avec une clé de bout en bout vérifiée du destinataire souhaité. Une clé de bout en bout est une clé que seul le destinataire individuel possède. Dans un environnement géré par un PGP Universal Server, il s'agit d'une clé Mode clé client qui est différente d'une clé Mode clé de serveur, où le PGP Universal Server est en possession de la clé.

  Le fait que la clé soit de bout en bout ou non est indiqué dans le champ **Groupe** de la boîte de dialogue Propriétés de la clé sous Windows ou de la boîte de dialogue Infos sur la clé sous Mac OS X. **Non** signifie que la clé *est* une clé de bout en bout (elle ne fait pas partie d'un groupe) et **Oui** indique qu'elle *n'est pas* une clé de bout en bout.

- **clé de bout en bout non vérifiée du destinataire** : le message peut être chiffré avec une clé de bout en bout non vérifiée du destinataire souhaité.
- **une liste de clés** : cette option indique que le message peut uniquement être chiffré avec les clés de la liste.

12 Dans le champ de préférence de codage du message, sélectionnez :

- **automatique** : PGP Desktop choisit le format de codage du message. Il s'agit généralement de l'option à utiliser de préférence, sauf si vous savez exactement pourquoi vous devez utiliser l'un des autres formats de codage de message de manière explicite.
- **PGP partitionné** : cette option définit PGP partitionné en tant que format de codage de message par défaut. Ce format est celui qui présente la meilleure compatibilité ascendante avec les anciens produits PGP et OpenPGP.
- **PGP/MIME** : cette option définit PGP/MIME en tant que format de codage de message par défaut. Le format PGP/MIME permet de chiffrer et de signer l'ensemble du message, pièces jointes comprises, en une seule passe. Il est par conséquent généralement plus rapide et plus efficace pour la reproduction fidèle d'un message.
- **S/MIME** : cette option définit S/MIME en tant que format de codage de message par défaut. Choisissez S/MIME si, pour une raison ou pour une autre, vous devez appliquer ce format de façon forcée à des messages même si l'utilisateur possède une clé PGP.

13 Dans la section **Si la clé d'un destinataire n'est pas disponible**, dans le premier champ **Clé introuvable**, sélectionnez :

- **Rechercher keys.domain et** : cette option indique une recherche qui inclut les deux keys.domain, ainsi qu'un autre serveur que vous spécifiez.
- **Rechercher** : cette option permet la recherche d'une clé appropriée si aucune n'est trouvée dans le trousseau de clés local.
- **Message avec signature numérique lisible** : cette option indique que le message doit être envoyé en texte en clair, mais signé.
- **Envoyer un message non sécurisé** : cette option indique que le message doit être envoyé en texte en clair.
- **Bloquer message** : cette option indique que le message ne doit pas être envoyé si aucune clé appropriée n'est trouvée.

14 Dans le deuxième champ Clé introuvable, sélectionnez :

- **Tous les serveurs de clés** : cette option permet de rechercher une clé appropriée dans tous les serveurs de clés, y compris le PGP Global Directory.
- **PGP Global Directory ou keyserver.pgp.com** : cette option indique que la recherche a lieu uniquement dans le PGP Global Directory.

- **[serveurs de clés configurés]** : cette option indique que la recherche a lieu uniquement dans le serveur de clés que vous choisissez dans la liste des serveurs de clés actuellement configurés. Les serveurs de clés autres que le PGP Global Directory peuvent fournir des clés non vérifiées qu'il n'est pas possible d'utiliser si la stratégie requiert des clés vérifiées. À moins que vous ne sachiez exactement pourquoi vous devez effectuer la recherche sur un autre serveur de clés et que vous ne soyez prêt à chercher ces clés manuellement pour les vérifier lorsque cela s'avère nécessaire, limitez la recherche au PGP Global Directory. Cette option est disponible uniquement sur les systèmes Windows.
- **Modifier la liste des serveurs de clés** : cette option permet d'ajouter des serveurs de clés à la liste des serveurs de clés actuellement configurés. Elle est disponible uniquement sur les systèmes Windows.

15 Dans le dernier champ Clé introuvable, indiquez :

- **cache temporaire des clés trouvées** : cette option indique qu'une clé trouvée doit être temporairement enregistrée dans la mémoire. Les clés figurant dans ce cache sont automatiquement utilisées lors de la vérification des messages signés. Elles le sont également pour le chiffrement si elles ont été vérifiées.
- **demander d'enregistrer les clés trouvées** : cette option indique que PGP Desktop doit vous demander si vous voulez enregistrer dans votre trousseau de clés local une clé trouvée spécifique.
- **enregistrer les clés trouvées** : cette option indique que les clés trouvées doivent être automatiquement enregistrées dans votre trousseau de clés local.

16 Dans le champ Si aucun résultat, sélectionnez :

- **Message avec signature numérique lisible** : les messages pour lesquels aucune clé de chiffrement n'a été trouvée peuvent être signés et envoyés en texte en clair.
- **Envoyer un message non sécurisé** : avec cette option, les messages ne sont pas chiffrés.
- **Bloquer message** : cette option empêche l'envoi d'un message pour lequel aucune clé de chiffrement n'a été trouvée.

17 Une fois que les modifications ont été effectuées, cliquez sur **OK** pour fermer la boîte de dialogue Stratégie de message. La stratégie de sécurité spécifiée est modifiée.

Suppression d'une stratégie de sécurité

▸ **Pour supprimer une stratégie de sécurité existante**

1. Dans la boîte de contrôle Messagerie PGP, cliquez sur le nom du service qui contient la stratégie de sécurité que vous souhaitez supprimer. Les propriétés du service choisi s'affichent dans la zone de travail de la messagerie PGP.
2. Cliquez sur **Modifier les stratégies**.
3. Dans la liste des stratégies de sécurité, cliquez sur celle que vous voulez supprimer. La stratégie est alors sélectionnée.
4. Cliquez sur **Supprimer la stratégie**. Une boîte de dialogue de confirmation de PGP Desktop apparaît.
5. Cliquez sur **Supprimer la stratégie** pour supprimer la stratégie ou sur **OK** pour la désactiver. La stratégie de sécurité spécifiée est supprimée ou désactivée.
6. Cliquez sur **Terminer**.

Remarque : Vous pouvez désactiver les stratégies par défaut, mais vous ne pouvez pas les supprimer.

Modification de l'ordre des stratégies dans la liste

▸ **Pour modifier l'ordre des stratégies dans la liste des stratégies de sécurité**

1. Dans la boîte de contrôle Messagerie PGP, cliquez sur le nom du service qui contient la stratégie de sécurité que vous souhaitez déplacer. Les propriétés du service choisi s'affichent dans la zone de travail de la messagerie PGP.
2. Cliquez sur **Modifier les stratégies**.
3. Dans la liste des stratégies de sécurité, cliquez sur la stratégie que vous souhaitez déplacer dans la liste. La stratégie est alors sélectionnée.
4. Cliquez sur **Déplacer vers le haut** ou sur **Déplacer vers le bas** jusqu'à ce que la stratégie se trouve à la position qui vous convient dans la liste. Assurez-vous que la stratégie **Chiffrement opportuniste** se trouve en dernière position dans la liste. Toute stratégie placée après ne sera pas appliquée.
5. Cliquez sur **Terminer**.

PGP Desktop et SSL

PGP Corporation a conçu PGP Desktop dans le but de protéger vos données automatiquement dès que possible. Ceci inclut la protection de vos données en transit entre votre client et votre serveur de messagerie.

Conseil : SSL est l'acronyme de Secure Sockets Layer, un protocole cryptographique destiné à la sécurisation des communications entre deux périphériques, dans le cas présent entre votre client de messagerie ou PGP Desktop et votre serveur de messagerie.

PGP Desktop protège vos données à destination et en provenance de votre serveur de messagerie de différentes manières, en fonction des situations. Les informations suivantes ne s'appliquent que si vous avez sélectionné **Automatique** (la valeur par défaut) pour le paramètre SSL/TLS dans la boîte de dialogue Paramètres du serveur :

- **Lorsque la connexion n'est pas protégée par SSL.** Si la connexion entre votre client et votre serveur de messagerie n'est pas protégée par SSL, PGP Desktop tentera automatiquement de mettre à niveau cette connexion vers SSL, c'est-à-dire qu'il négociera avec votre serveur de messagerie afin de protéger la connexion par SSL, à condition que votre serveur de messagerie prenne en charge ce protocole.

  Si ce n'est pas le cas, les messages envoyés et reçus par PGP Desktop pendant la session le seront via une connexion non sécurisée. Le chiffrement ou non des messages par PGP Desktop n'a aucune incidence sur la tentative de mise à niveau de la connexion par PGP Desktop. Les messages chiffrés par PGP Desktop peuvent être envoyés ou reçus via une connexion protégée par SSL ou non.

  Remarque : PGP Desktop tente toujours de mettre à niveau une connexion au serveur de messagerie non protégée vers une connexion protégée par SLL**, car non seulement ce type de connexion protège tous les messages non chiffrés par PGP à destination ou en provenance du serveur de messagerie, mais il protège également la phrase secrète d'authentification du serveur de messagerie lorsqu'elle est transmise à celui-ci.**

- **Lorsque la connexion est protégée par SSL.** Si la protection par SSL de la connexion à votre serveur de messagerie est activée dans votre client de messagerie, vous devez la désactiver pour que PGP Desktop puisse chiffrer et déchiffrer les messages. En effet, PGP Desktop ne peut pas traiter des messages déjà chiffrés par SSL.

La désactivation de la protection SSL dans votre client de messagerie ne signifie pas que le transfert des messages non chiffrés par PGP depuis ou vers votre serveur de messagerie n'est pas sécurisé. Comme pour n'importe quelle connexion non protégée par SSL, PGP Desktop tentera automatiquement de protéger la connexion par SSL, si le serveur de messagerie prend en charge ce type de connexion (si vous avez réglé le paramètre SSL/TLS sur **Automatique** dans la boîte de dialogue Paramètres du serveur). Si ce n'est pas le cas, les messages envoyés par PGP Desktop pendant la session le seront via une connexion non protégée.

Les seuls cas où vos messages seront transmis en clair à votre serveur de messagerie ne sont que lorsque les messages ne sont pas chiffrés par PGP et que la connexion au serveur de messagerie ne prend pas en charge les connexions SSL ou lorsque vous avez réglé le paramètre SSL/TLS sur **Aucune tentative**.

- **Lorsque vos messages ne doivent pas être envoyés en clair.** Certaines stratégies de sécurité restreignent l'envoi des messages aux messages protégés uniquement. En d'autres termes, les messages non protégés ne sont jamais envoyés. Si nécessaire, vous pouvez configurer PGP Desktop de sorte à prendre en charge ce type de stratégie de sécurité.

  Sélectionnez le service de messagerie PGP qui vous intéresse, ouvrez la boîte de dialogue Paramètres du serveur en cliquant sur le nom du serveur indiqué dans le champ Serveur de la section Propriétés du compte pour ce service, puis choisissez une option *autre* qu'**Automatique** dans la liste SSL/TLS.

  Une fois cette nouvelle option sélectionnée, PGP Desktop recevra et transmettra des messages à votre serveur de messagerie uniquement si la connexion entre eux est protégée par SSL. S'il est impossible d'établir une connexion protégée par SLL, PGP Desktop ne communiquera pas avec le serveur.

  Remarque : Vous ne devez sélectionner cette option que si vous êtes sûr que votre serveur de messagerie prend en charge les connexions SSL. Cela permet de vous assurer que les messages ne seront pas transférés entre PGP Desktop et le serveur de messagerie via une connexion non sécurisée si, par exemple, un problème survient lors de la négociation de la protection SSL pour la connexion. Si vous sélectionnez cette option et que votre serveur de messagerie ne prend pas en charge SSL, PGP Desktop n'enverra ni ne recevra aucun message.

- **Lorsque vous souhaitez que le protocole SSL soit activé dans votre client de messagerie.** Pour utiliser PGP Desktop en ayant activé le protocole SSL dans votre client de messagerie, désélectionnez l'option **M'avertir si le client de messagerie fait une tentative de connexion SSL/TLS** pour votre serveur de messagerie entrant, sortant ou les deux. Lorsque vous désactivez cette option pour une connexion à un serveur de messagerie, PGP Desktop ignore le trafic entrant et sortant sur cette connexion lorsque celle-ci est protégée par SSL.

PGP Desktop surveille les connexions depuis et vers ce serveur, et ignore le trafic envoyé et reçu via les connexions protégées par SSL. Si PGP Desktop détecte une connexion non protégée par SSL, il traite alors le trafic comme n'importe quelle autre connexion non protégée et tente de mettre à niveau la connexion vers SSL (si vous êtes en mode Automatique) et applique les stratégies appropriées aux messages.

Modes clé

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, l'application disposera d'un mode clé.

Remarque : les informations contenues dans la présente section concernent *uniquement* les utilisateurs de PGP Desktop qui se trouvent dans un domaine de messagerie protégé par un PGP Universal Server.

Les modes clé disponibles sont les suivants :

- **Mode clé de serveur (SKM) :** les clés sont générées et gérées par le PGP Universal Server. Elles sont partagées uniquement avec l'ordinateur sur lequel vous exécutez PGP Desktop, en fonction des besoins. Votre clé privée est stockée uniquement sur le PGP Universal Server, qui se charge également de toute la gestion des clés privées. L'administrateur PGP Universal dispose d'un accès sans restriction à votre clé privée et peut, de ce fait, accéder à tous les messages que vous chiffrez. Ce mode clé n'est *pas* compatible avec les cartes à puce (ces dernières peut être utilisées seulement sur les systèmes Windows).

  À compter de la version 10.0 de PGP Desktop, les clés SKM qui auparavant ne pouvaient être utilisées que pour la messagerie peuvent dorénavant l'être pour toutes les autres opérations de chiffrement dans PGP Desktop. Celles-ci incluent le chiffrement de disques et de fichiers, ainsi que le déchiffrement des messages électroniques MAPI hors ligne.

  Si vous utilisez une clé SKM, vous n'aurez jamais besoin de saisir une phrase secrète pour vous authentifier. Les phrases secrètes associées aux clés SKM sont générées de façon aléatoire par PGP Desktop et sont stockées sous forme chiffrée. Lorsque PGP Desktop a besoin d'une phrase secrète, il récupère celle chiffrée dans le système sans vous solliciter.

- **Mode clé client (CKM) :** les clés sont générées et gérées par l'ordinateur sur lequel vous exécutez PGP Desktop. Les clés privées ne sont pas partagées avec le PGP Universal Server. Toutes les opérations cryptographiques (chiffrement, déchiffrement, signature, vérification) sont également gérées par ce même ordinateur. Sur les systèmes Windows, ce mode clé est compatible avec les cartes à puce.

- **Mode clé protégée (GKM) :** ce mode est semblable au mode CKM, si ce n'est qu'une copie *chiffrée* de la clé privée est stockée sur le PGP Universal Server, ce qui vous permet d'y accéder en cas de changement d'ordinateur. Étant donné que la clé est chiffrée, l'administrateur PGP Universal ne peut pas y accéder ; vous êtes le seul à pouvoir le faire. Ce mode clé est compatible avec les cartes à puce (sur les systèmes Windows uniquement), à condition que la clé ne soit pas générée directement sur la carte à puce, mais plutôt copiée dessus.
- **Mode clé client serveur (SCKM) :** ce mode est également très proche du mode CKM, si ce n'est qu'une copie de la clé de *chiffrement* privée est stockée sur le PGP Universal Server. Les clés de *signature* privées sont en permanence stockées sur l'ordinateur sur lequel vous exécutez PGP Desktop. Ce mode clé garantit le respect des réglementations et politiques d'entreprise stipulant que l'utilisateur doit toujours garder le contrôle de sa clé de signature privée, tout en assurant un stockage de secours pour la clé de chiffrement privée. Il est compatible avec les cartes à puce (sur les systèmes Windows uniquement), à condition que la clé ne soit pas générée directement sur la carte. Le mode SCKM requiert une clé avec une sous-clé de signature distincte, laquelle peut être créée pour une nouvelle clé ou ajoutée à une ancienne clé PGP à l'aide de PGP Desktop 9.5 ou une version ultérieure.

En fonction de la manière dont votre administrateur PGP a configuré votre copie de PGP Desktop, il se peut que vous ne puissiez pas choisir votre mode clé. Il se peut également que vous ne puissiez pas en changer.

Contactez votre administrateur PGP pour toute question supplémentaire sur votre mode clé.

Détermination du mode clé

N'oubliez pas que seuls les utilisateurs de PGP Desktop dans un environnement protégé par un PGP Universal Server disposent d'un mode clé, ce qui n'est pas le cas des utilisateurs autonomes de PGP Desktop.

Pour déterminer votre mode clé

- Ouvrez PGP Desktop et sélectionnez le service de messagerie PGP dont vous voulez déterminer le mode clé. Les propriétés du compte et les stratégies de sécurité relatives au service sélectionné apparaissent.

  Le mode clé du service est indiqué entre parenthèses après le nom du PGP Universal Server dans le champ **Universal Server** (par exemple, **clés.exemple.com (GKM)**). Ceci signifie que le mode clé du service sélectionné est ici Mode clé protégée et que le PGP Universal Server associé est clés.exemple.com.

Changement de mode clé

En fonction de la manière dont votre administrateur PGP a configuré votre copie de PGP Desktop, il se peut que vous ne puissiez pas changer de mode clé.

Pour changer de mode clé

1. Ouvrez PGP Desktop et sélectionnez le service de messagerie PGP dont vous voulez modifier le mode clé. Les propriétés du compte et les stratégies de sécurité relatives au service sélectionné apparaissent.
2. Cliquez sur **Mode clé**. La fenêtre Mode clé de PGP Universal apparaît, décrivant le mode actuel de gestion des clés.
3. Cliquez sur **Réinitialiser la clé**, puis sur **Oui** dans le message de confirmation qui apparaît. L'assistant d'installation de clé PGP s'ouvre.
4. Lisez les informations, puis cliquez sur **Suivant**. La fenêtre Sélection de la gestion des clés s'affiche.
5. Sélectionnez le mode clé souhaité. En fonction de la manière dont votre administrateur PGP Universal a configuré votre copie de PGP Desktop, il se peut que certains modes clé ne soient pas disponibles.
6. Cliquez sur **Suivant**. La fenêtre Sélection de la source de clé s'affiche.
7. Choisissez l'une des options suivantes :
   - **Nouvelle clé** : le système vous invite à créer une clé PGP qui sera utilisée pour protéger vos messages électroniques.
   - **Clé PGP Desktop** : le système vous invite à indiquer une clé PGP existante à utiliser pour protéger vos messages électroniques.
   - **Importer la clé** : le système vous invite à importer une clé PGP qui sera utilisée pour protéger vos messages électroniques.
8. Choisissez l'option qui vous intéresse, puis cliquez sur **Suivant**.
9. Si vous avez sélectionné **Nouvelle clé**, procédez comme suit :
   - Saisissez une phrase secrète pour la clé, puis cliquez sur **Suivant**.
   - Une fois que la clé a été générée, cliquez sur **Suivant**.
   - Cliquez sur **Terminer**.
10. Si vous avez sélectionné **Clé PGP Desktop**, procédez comme suit :
    - Sélectionnez la clé à utiliser dans le trousseau de clés local, puis cliquez sur **Suivant**.
    - Cliquez sur **Terminer**.
11. Si vous avez sélectionné **Importer la clé**, procédez comme suit :
    - Naviguez jusqu'au dossier qui contient la clé PGP à importer (il doit contenir une clé privée), puis cliquez sur **Suivant**.

- Cliquez sur **Terminer**.

Conseil : vous pouvez également changer votre mode clé à partir de la boîte de dialogue Options de PGP. Choisissez **Outils > Options de PGP** et sélectionnez l'onglet Avancé. Cliquez sur **Réinitialiser la clé** et suivez les étapes ci-dessus lorsque l'Assistant d'installation de clé PGP s'affiche. Cette option est disponible uniquement si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server.

Affichage du journal de PGP

Ce journal répertorie les mesures prises par PGP Desktop pour sécuriser vos messages.

Pour afficher le journal de PGP Desktop

1. Pour afficher les journaux, vous devez activer la journalisation. Pour cela, dans PGP Desktop, sélectionnez **Outils > Journalisation PGP**.
2. Dans le panneau de contrôle Messagerie PGP, cliquez sur **Journal de PGP**. Le journal de PGP s'affiche dans la fenêtre de l'application.
3. Pour modifier les options d'affichage ou filtrer certaines informations de journalisation, procédez comme suit :
   - Cliquez sur la flèche à droite du champ **Afficher le journal de** pour sélectionner les jours pour lesquels vous souhaitez consulter les journaux.
   - Cliquez sur la flèche à droite du champ **Afficher la rubrique** pour sélectionner les types des journaux que vous souhaitez consulter. Les rubriques disponibles sont : **Tous**, **PGP**, **Courrier électronique**, **MI**, **Disque complet**, **NetShare**, **Zip/SDA** et **Virtual Disk**.
   - Cliquez sur la flèche à droite du champ **Afficher le niveau** pour sélectionner le niveau de gravité minimal des entrées du journal à afficher. Les niveaux disponibles sont : **Erreur**, **Avertir, Info** et **Informations détaillées**. Remarque : le niveau **Informations détaillées** peut engendrer des fichiers journaux volumineux.
4. Une fois la consultation du journal terminée :
   - Pour enregistrer une copie du journal de PGP, cliquez sur **Enregistrer**.
   - Pour effacer les entrées du journal, cliquez sur **Décomposer**.

8 Sécurité de la messagerie instantanée

Cette section décrit comment sécuriser vos sessions de messagerie instantanée à l'aide de PGP Desktop. Pour en savoir plus sur les options de PGP utilisées lors des sessions de messagerie instantanée, consultez la section *Options de messagerie* (à la page 320).

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

À propos de la compatibilité de la messagerie instantanée avec PGP Desktop

PGP Desktop chiffre automatiquement les sessions de messagerie instantanée AOL et iChat standard, les connexions directes, ainsi que les transferts de fichiers dans les conditions suivantes :

- PGP Desktop 9.0 (ou une version ultérieure) doit être installé et exécuté sur le système des deux utilisateurs de la session en cours. Pour savoir si vous disposez de PGP Desktop 9.0 ou version ultérieure, cliquez sur l'icône de la zone de notification PGP et sélectionnez **À propos de PGP** dans le menu contextuel (dans la fenêtre de PGP Desktop, sélectionnez **Aide > À propos de PGP**).
- Le paramètre **Chiffrer les messages instantanés** doit être activé sur le système des deux utilisateurs. Pour ce faire :

- Sous Windows, sélectionnez **Outils > Options**, cliquez sur l'onglet Messagerie, puis cochez la case **Chiffrer les messages instantanés AOL (AIM)**.
- Sous Mac OS X, sélectionnez **PGP > Préférences**, cliquez sur l'icône Messagerie, puis cochez la case **Chiffrer les messages instantanés AOL (AIM)**.

Conseil : Sous Windows, cliquez sur l'icône de la zone de notification PGP pour vérifier rapidement si le chiffrement de la messagerie instantanée est activé. Une coche doit apparaître en regard de l'option **Utiliser le proxy PGP AIM** dans le menu contextuel.

- Les deux utilisateurs doivent utiliser des clients de messagerie instantanée compatibles. Pour plus d'informations sur les clients de messagerie instantanée compatibles, consultez la section suivante.
- L'adresse AIM de l'appelant doit figurer sur la liste des amis du destinataire de la session (dans le cas contraire, elle ne sera pas chiffrée).

La fonctionnalité de messagerie instantanée sécurisée est compatible avec tout client prenant en charge le protocole OSCAR d'AOL pour la messagerie instantanée, tel qu'AOL Instant Messenger, Trillian Pro, iChat et Gaim.

Pour chiffrer le transfert de fichiers et les sessions de connexion directe à l'aide de PGP Desktop, vous devez disposer de la dernière version de ces clients. En outre, PGP Corporation vous recommande de configurer la connexion des fonctionnalités de messagerie directe et du transfert de fichiers de sorte à utiliser le proxy AOL, plutôt que d'autoriser votre ami à se connecter directement à votre ordinateur.

Remarque :

PGP Desktop ne chiffre pas les connexions audio et vidéo.

Pour améliorer la sécurité de la fonctionnalité de messagerie instantanée, PGP Desktop utilise PFS (Perfect Forward Secrecy). Toutes les clés assurant la sécurité de vos sessions de messagerie instantanée sont générées au début de la connexion, puis détruites après la déconnexion. Un jeu de clés est créé pour chaque session afin de renforcer la sécurité.

Compatibilité avec les clients de messagerie instantanée

PGP Desktop est compatible avec les clients de messagerie instantanée suivants lors du chiffrement de messages instantanés AIM, de transferts de fichier et de connexions directes :

- AOL AIM 6.5.5

- Si vous possédez AIM 6.5 et souhaitez que les messages instantanés soient chiffrés, vous devez remplacer le port par défaut utilisé par AIM (493) par le port 5190.
- Les connexions audio et vidéo ne sont pas chiffrées par PGP Desktop.
- Si vous apportez des modifications aux protocoles AIM sous-jacents après la commercialisation de PGP Desktop 10.0, l'interopérabilité continue avec le service AIM risque d'en être affectée.

- Trillian 3.1 (Basic et Pro)

D'autres clients de messagerie instantanée peuvent être compatibles pour un fonctionnement de base, mais leur possibilité d'utilisation n'a pas été vérifiée.

À propos des clés utilisées pour le chiffrement

Une clé RSA de 1024 bits est générée à chacune de vos connexions au logiciel de messagerie instantanée, puis détruite lorsque vous vous déconnectez. Cette clé sert à échanger des données initiales générées aléatoirement avec les personnes avec lesquelles vous communiquez. La combinaison et le hachage de ces données permettent à chaque participant de créer un jeu de clés symétriques exclusivement pour cette communication (une pour chaque direction). Ces clés symétriques servent à chiffrer tous les messages avec AES256.

Certaines de ces données permettent également de générer un code d'authentification de message haché par clé, ou HMAC, pour chaque message afin d'en vérifier l'intégrité.

Remarque : Vous ne pouvez pas configurer les clés utilisées pour sécuriser la communication par messagerie instantanée.

Chiffrement des sessions de messagerie instantanée

Lorsque vous avez rempli les conditions décrites dans la section *À propos de la compatibilité de la messagerie instantanée avec PGP Desktop* (à la page 137), lancez votre session de messagerie instantanée normalement. Vos sessions de messagerie instantanée avec un autre utilisateur de PGP Desktop ayant recours à un client compatible sont protégées automatiquement et en toute transparence.

Plusieurs procédures permettent de vérifier que votre session est protégée :

- Lorsque vous lancez une session de messagerie instantanée, le Notificateur PGP s'affiche, vous informant qu'une session sécurisée a démarré.
- Au début de la session, le premier message envoyé par l'autre utilisateur est accompagné du texte suivant : « Conversation chiffrée par PGP Desktop. »

- Une icône de cadenas affichée en regard des noms dans la liste des amis indique que les utilisateurs emploient probablement PGP Desktop pour sécuriser leurs sessions de messagerie instantanée.

  Le cadenas peut également signaler l'utilisation de la sécurité intégrée d'AIM.

- Si vous ouvrez le journal de PGP après avoir lancé votre session, une entrée indique qu'elle est chiffrée. Par exemple :

  ```
  17:01:06 Info    Initiation d'une session AIM chiffrée par
  PGP Desktop avec breynolds à l'aide de votre clé dont l'ID
  est 0xEFDDCE3C.
  ```

9 Affichage des messages électroniques à l'aide de la Visionneuse PGP

Cette section comporte des informations sur l'utilisation de la Visionneuse PGP pour déchiffrer, vérifier et afficher les messages chiffrés.

Remarque : la Visionneuse PGP ne peut être exécutée que sur les systèmes sur lesquels PGP Desktop est installé. La Visionneuse PGP ne s'utilise pas de manière autonome.

Contenu du chapitre

Présentation 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.

Les types de messages chiffrés suivants peuvent se trouver hors du flux de messagerie :

- **Messages chiffrés enregistrés de façon sécurisée :** de nombreuses entreprises stockent les messages sous forme chiffrée pour des raisons de sécurité. Le fait de les stocker les fait sortir du flux de messagerie, mais la Visionneuse PGP peut les déchiffrer, les vérifier et les afficher tout en conservant le message chiffré d'origine.
- **Texte chiffré dans un message Web :** les messages chiffrés envoyés à un compte de messagerie Web ne peuvent pas être déchiffrés par PGP Desktop. Toutefois, la Visionneuse PGP peut déchiffrer ces messages. Il vous suffit d'ouvrir dans celle-ci la pièce jointe au fichier message.pgp.
- **Texte chiffré non déchiffré par PGP Desktop :** si un message a été téléchargé automatiquement par votre client de messagerie alors que PGP Desktop n'était pas en cours d'exécution ou que votre phrase secrète n'était pas mise en cache, cela peut avoir entraîné la sortie du texte du message chiffré du flux de messagerie.

La Visionneuse PGP déchiffre, vérifie et affiche divers types de contenus de messages :

- Contenu moderne chiffré par PGP (PGP/MIME et PGP partitionné)
- Contenu hérité chiffré par PGP (PGP/MIME et PGP partitionné)
- Contenu chiffré conforme RFC-2822

La Visionneuse PGP utilise les trousseaux de clés PGP Desktop pour les opérations nécessitant des clés.

Elle tient compte des préférences PGP Desktop applicables, telles que les options de mise en cache des phrases secrètes.

Dans un environnement géré par un PGP Universal Server, la Visionneuse PGP recherche les clés de vérification sur la base de la stratégie adéquate.

Elle affiche les informations de signature des messages qu'elle déchiffre dans la fenêtre du message, et non dans le message lui-même. Cela garantit l'accès à l'ensemble des informations de signature et évite toute imitation des annotations de signatures en ligne.

Clients de messagerie compatibles

Utilisez la Visionneuse PGP pour copier le texte d'un message déchiffré/vérifié vers les clients de messagerie suivants :

- Windows Mail (Windows)
- Microsoft Outlook (Windows)
- Thunderbird (Windows et Mac OS X)
- Outlook Express (Windows)
- Lotus Notes (Windows)
- Mail.app (Mac OS X)

De par la conception de l'architecture Lotus Notes, il est impossible de faire glisser un message chiffré depuis le client de messagerie Lotus Notes vers la Visionneuse PGP pour qu'il soit déchiffré.

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

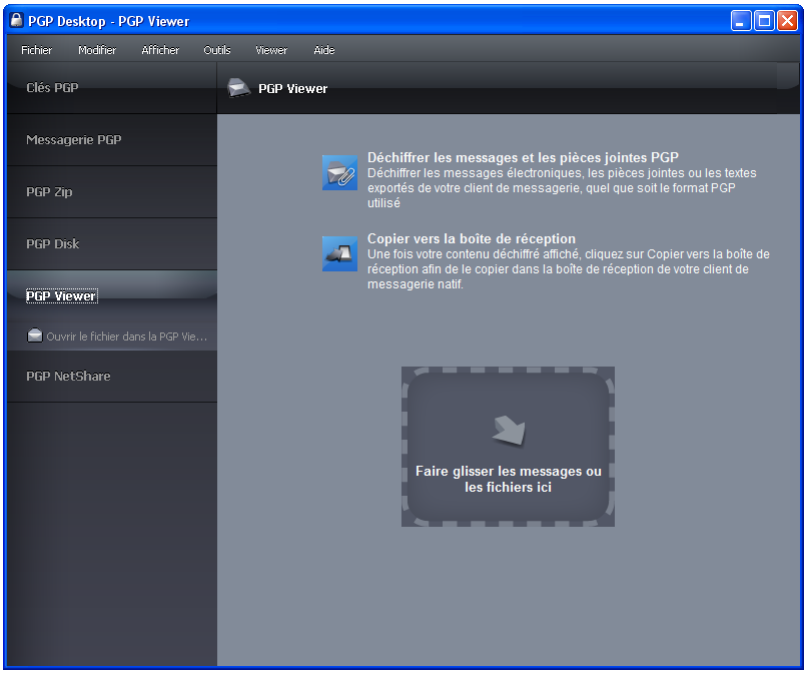
Utilisez la Visionneuse PGP pour ouvrir (déchiffrer, vérifier et afficher) les fichiers de messages chiffrés des types suivants :

- ***.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 la Visionneuse PGP. Pour cela, cliquez sur l'icône PGP dans la zone de notification et sélectionnez Visionneuse PGP ou, si vous vous trouvez déjà dans PGP Desktop, cliquez sur le panneau de contrôle Visionneuse PGP.



2 Cliquez sur **Ouvrir le fichier dans la Visionneuse PGP**, ou ouvrez le menu **Visionneuse** et sélectionnez **Ouvrir le fichier dans la Visionneuse PGP**.

La boîte de dialogue **Ouvrir le fichier du message** s'affiche.

3 Dans celle-ci, accédez au fichier à ouvrir, sélectionnez-le et cliquez sur **Ouvrir**. La Visionneuse PGP déchiffre, vérifie et affiche le message dans une fenêtre séparée.

Conseil : vous pouvez faire glisser le fichier à ouvrir 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. Un volet présentant tous les messages ouverts apparaît sur la gauche de l'écran Visionneuse PGP.

5 Pour ouvrir ce volet ou le fermer s'il est ouvert, cliquez sur le bouton Volet dans la barre d'outils.

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 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 contient le nom du client de messagerie vers lequel le message va être copié. Pour savoir comment modifier ce paramètre, reportez-vous à la section *Définition d'options dans la Visionneuse PGP* (à la page 145).

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.

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.

3 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**. La boîte de dialogue Exporter le fichier du message apparaît.
2. Indiquez dans celle-ci l'emplacement, le nom et le format souhaités pour le fichier, puis cliquez sur **Enregistrer**. 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.

Définition d'options dans la Visionneuse PGP

La Visionneuse PGP inclut des options (préférences) qui permettent de contrôler certaines fonctionnalités.

Pour accéder aux préférences de la Visionneuse PGP

1. Ouvrez la Visionneuse à partir de la zone de notification PGP ou utilisez-la pour déchiffrer, vérifier et afficher un message.

   L'écran Visionneuse PGP apparaît.

2. Cliquez sur l'icône Outils (à l'extrême droite de la barre d'outils de la Visionneuse) et sélectionnez **Préférences**. La boîte de dialogue des préférences s'affiche.

3. Cliquez sur l'onglet Général et indiquez les options suivantes :

   - **Demander à l'utilisateur de confirmer la commande Copier vers la boîte de réception** : permet d'indiquer si une demande de confirmation doit être affichée ou non lorsque vous copiez le texte de la Visionneuse PGP dans la boîte de réception de votre client de messagerie. Par défaut, cette option est activée.
   - **Charger automatiquement les images distantes** : permet d'indiquer si les ressources externes, telles que les images, les feuilles de style CSS ou le contenu iframe, entre autres, doivent être chargés automatiquement par la Visionneuse PGP. Cette option est désactivée par défaut, étant donné qu'elle peut représenter un risque pour la sécurité.
   - **Utiliser le client de messagerie** : permet d'indiquer le client de messagerie dans lequel la Visionneuse PGP doit copier le contenu. Le client par défaut est **Valeur par défaut de Windows (messagerie)** ; la Visionneuse PGP détermine votre client de messagerie Windows par défaut et l'utilise par défaut. Vous pouvez aussi sélectionner **Outlook**, **Outlook Express** et **Thunderbird**.

4. Cliquez sur l'onglet Texte et indiquez les options suivantes :

   - **Police** : indique la police que doit utiliser la Visionneuse PGP pour afficher le texte.
   - **Couleur du texte** : indique la couleur que doit afficher la Visionneuse PGP pour le texte.
   - **Couleur d'arrière-plan** : indique la couleur d'arrière-plan du texte que doit afficher la Visionneuse PGP.

Fonctionnalités de sécurité dans la Visionneuse PGP

La Visionneuse PGP applique des mesures de protection proactives :

- Les plug-ins, JavaScript et Java Applets sont désactivés dans le navigateur Web intégré à la Visionneuse PGP et qui affiche le contenu des messages. Cela évite ainsi à la Visionneuse PGP de charger un virus.

- Les ressources externes, comme les images, feuilles de style CSS, contenus iframe (cadre en ligne contenant un autre document), etc., sont chargées automatiquement en fonction de la préférence **Charger automatiquement les images distantes**. Pour des raisons de sécurité, cette préférence est désactivée par défaut. Dans ce cas, la Visionneuse PGP ne génère aucun trafic réseau vers des sites externes.

10 Protection des disques à l'aide de PGP Whole Disk Encryption

PGP Whole Disk Encryption (PGP WDE) verrouille l'ensemble du contenu d'un ordinateur portable ou de bureau, d'un disque dur externe ou d'un périphérique Flash USB, notamment les secteurs de démarrage, ainsi que les fichiers système et d'échange. Il permet également de chiffrer uniquement la partition de démarrage ou les partitions Windows. Le chiffrement fonctionne comme un processus en arrière-plan, invisible, qui protège automatiquement les données importantes sans que vous ayez à procéder à d'autres opérations.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, l'administrateur PGP peut avoir défini un chiffrement de tous les disques de démarrage, par stratégie. Le cas échéant, PGP Desktop vérifie régulièrement que les disques sont chiffrés et applique la stratégie en chiffrant automatiquement les disques de démarrage qui ne le sont pas.

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, l'administrateur PGP peut avoir personnalisé l'écran PGP Whole Disk Encryption BootGuard pour inclure du texte supplémentaire ou une image personnalisée, telle que le logo de votre entreprise. Les graphiques inclus dans ce guide illustrent l'installation par défaut. Votre écran d'ouverture de session peut être différent si l'administrateur l'a personnalisé.

Contenu du chapitre

À propos de PGP Whole Disk Encryption

Lorsque vous chiffrez un disque à l'aide de la fonctionnalité PGP Whole Disk Encryption, chaque secteur est chiffré à l'aide d'une clé symétrique. Cette fonctionnalité permet de chiffrer tous les fichiers : fichiers du système d'exploitation, d'application, de données et d'échange, d'espace libre et fichiers temporaires.

Aux démarrages suivants, PGP Whole Disk Encryption vous invite à saisir la phrase secrète appropriée. Les données chiffrées sont ensuite déchiffrées lorsque vous y accédez. Toutes les données sont chiffrées avant d'être écrites sur le disque. Si vous êtes authentifié sur le disque chiffré par PGP WDE (vous devez saisir la phrase secrète dans l'écran PGP BootGuard), les fichiers sont disponibles. Lorsque vous arrêtez votre système, le disque est protégé et ne peut être utilisé par d'autres personnes.

Avant de chiffrer votre disque avec PGP WDE, il est important que vous compreniez le processus de création et d'utilisation d'un disque chiffré par PGP WDE.

1 Assurez-vous que votre licence PGP Desktop prend en charge son utilisation, comme décrit dans la section *Gestion des licences PGP Whole Disk Encryption* (à la page 152).

2 Suivez la procédure décrite dans la section *Préparation du disque au chiffrement* (à la page 152).

3 Choisissez la façon dont vous souhaitez vous authentifier pour chiffrer le disque, comme indiqué à la section *Définition de la méthode d'authentification du disque* (à la page 160).

4 Choisissez les options de chiffrement à utiliser dans *Définition des options de chiffrement* (à la page 163).

5 Lancez le processus de chiffrement : *Chiffrement d'un disque ou d'une partition* (à la page 170).

6 Reportez-vous à la section *Utilisation d'un disque chiffré par PGP WDE* (à la page 176) pour apprendre à utiliser un disque chiffré.

7 Pour savoir comment assurer la maintenance de votre disque chiffré, consultez la section *Continuité de la sécurité du disque* (à la page 185).

8 Pour savoir comment déchiffrer le disque, si nécessaire, reportez-vous à la section *Déchiffrement d'un disque chiffré par PGP WDE* (à la page 202).

9 Prenez connaissance des fonctionnalités permettant d'éviter les problèmes de sécurité décrites dans Précautions spéciales de sécurité prises par PGP Desktop.

Si vous êtes un administrateur de PGP Universal ou si vous utilisez PGP WDE dans un environnement géré par un PGP Universal Server, reportez-vous à la section *Utilisation de PGP WDE dans un environnement géré par un PGP Universal Server* (à la page 197) pour plus informations.

Avertissement : lorsque vous déverrouillez un disque, toute personne en mesure d'utiliser physiquement votre système peut accéder aux fichiers. Les fichiers sont déverrouillés jusqu'à ce que vous les verrouilliez de nouveau en arrêtant l'ordinateur. Utilisez un volume PGP Virtual Disk pour les fichiers qui doivent être sécurisés même lorsque votre ordinateur est en cours d'utilisation. Pour plus d'informations, reportez-vous à la section *Utilisation des PGP Virtual Disks* (à la page 211).

Quelles sont les différences entre PGP WDE et PGP Virtual Disk ?

Les PGP Virtual Disks jouent le rôle de volumes complémentaires sur votre système pouvant être verrouillés même lorsque vous utilisez l'ordinateur. Ces volumes sont comme une chambre forte dans laquelle vous stockez les fichiers à protéger. Il ne s'agit pas d'un disque physique ; en effet, la fonctionnalité PGP Virtual Disk crée et gère un disque virtuel.

PGP WDE protège l'ensemble de votre disque dur physique.

Ces deux produits fonctionnent indépendamment et peuvent être utilisés conjointement. Pour plus d'informations, reportez-vous à la section *Utilisation des PGP Virtual Disks* (à la page 211).

Gestion des licences PGP Whole Disk Encryption

Pour utiliser la fonctionnalité PGP Whole Disk Encryption, vous devez disposer d'une licence PGP Desktop appropriée.

Pour vérifier que votre licence prend en charge PGP Whole Disk Encryption

1. Ouvrez PGP Desktop.
2. Sélectionnez **Aide > Licence**. La boîte de dialogue contenant la licence PGP Desktop apparaît.
3. Dans la section **Informations produit**, recherchez l'icône **PGP Whole Disk Encryption**. Positionnez le curseur sur le nom du produit pour afficher des informations sur celui-ci et savoir si vous disposez d'une licence vous permettant de l'utiliser.

Si votre licence ne prend pas en charge PGP WDE, pour en savoir plus sur la gestion des licences PGP Desktop, suivez l'une des méthodes ci-après :

- Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, contactez votre administrateur PGP pour plus de détails sur la prise en charge de la fonctionnalité PGP WDE par votre licence. Pour plus d'informations, reportez-vous à la section *Utilisation de PGP Desktop avec le PGP Universal Server* (cf. "Utilisation de PGP Desktop avec un PGP Universal Server" à la page 341).
- Si vous utilisez PGP Desktop dans un autre environnement, accédez au *site Web de PGP Corporation* (http://www.pgp.com) pour en savoir plus sur l'ajout de la fonctionnalité PGP WDE à votre licence.

Expiration de la licence

Avec une licence d'abonnement, vous pouvez utiliser la fonctionnalité de déchiffrement de PGP WDE jusqu'à 90 jours après l'expiration de la licence, uniquement pour les disques de démarrage. 90 jours après l'expiration de la licence, la fonctionnalité PGP WDE déchiffre vos données (après vous en avoir informé) afin que vous puissiez récupérer vos fichiers.

Préparation du disque au chiffrement

Avant de chiffrer votre disque, vous devez effectuer certaines tâches afin de garantir le bon chiffrement du disque.

- **Déterminer si le disque concerné est pris en charge.** Reportez-vous à *Types de disques pris en charge* (à la page 154).
- **S'assurer que la configuration du clavier est prise en charge.** Reportez-vous à *Claviers pris en charge* (à la page 155).
- **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 *Vérification du bon fonctionnement du disque avant le chiffrement* (à la page 157).
- **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 sauvegarder régulièrement votre disque.
- **Créer un disque de récupération.** Bien qu'il soit très peu probable qu'un enregistrement d'amorçage principal soit endommagé sur un disque ou une partition de démarrage bénéficiant d'une protection via PGP Whole Disk Encryption, cela reste une éventualité. Avant de chiffrer un disque ou une partition de démarrage à l'aide de PGP Whole Disk Encryption, créez un disque de récupération. Reportez-vous à *Création de disques de récupération* (cf. "Création et utilisation de disques de récupération" à la page 200).
- **Évaluer le temps nécessaire pour chiffrer le disque** et se préparer en fonction. Reportez-vous à *Calcul de la durée du chiffrement* (à la page 158).
- **S'assurer de disposer d'un accès à l'alimentation secteur** pendant tout le processus de chiffrement. Reportez-vous à la section *Alimentation continue pendant le chiffrement* (à la page 159).
- **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. Consultez la section *Effectuer un test pilote afin de vérifier la compatibilité du logiciel* (cf. "Réalisation d'un test pilote afin de vérifier la compatibilité du logiciel" à la page 159), 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.

- **S'assurer de disposer du jeton et des pilotes requis**. Si vous utilisez un jeton USB pour vous authentifier sur un disque fixe sécurisé à l'aide de PGP Whole Disk Encryption, vérifiez que vous possédez le jeton correspondant et que le pilote requis est installé. Reportez-vous à la section *Préparation d'un jeton à utiliser pour l'authentification* (cf. "Préparation d'une carte à puce ou d'un jeton à utiliser pour l'authentification" à la page 164).

Remarque : N'utilisez pas PGP Whole Disk Encryption pour chiffrer le matériel de serveurs. PGP WDE n'est pas pris en charge sous Windows 2000 Server ou Windows 2003 Server.

Types de disques pris en charge

La fonctionnalité PGP WDE protège le contenu des types de disques suivants :

- Disques d'ordinateurs portables ou de bureau, y compris les disques à mémoire statique (partitions ou disque entier)

  Remarque : N'utilisez pas PGP Whole Disk Encryption pour chiffrer le matériel de serveurs. PGP WDE n'est pas pris en charge sous Windows 2000 Server ou Windows 2003 Server.

- Disques externes, sauf périphériques de musique et appareils photos numériques
- Disques Flash USB

Vous pouvez chiffrer les disques et les partitions formatés à l'aide des systèmes de fichiers FAT16, FAT32 et NTFS. Si vous utilisez PGP Whole Disk Encryption avec un disque ou une partition FAT, vous pouvez effectuer une conversion en NTFS ultérieurement.

Pour utiliser la fonctionnalité PGP Whole Disk Encryption sur un système à double amorçage, PGP WDE doit être installé et prendre en charge le système d'exploitation de démarrage (tel que Windows XP, Windows 2000 ou Windows Vista). Le double amorçage avec un autre système d'exploitation (tel que Linux) est possible, mais seule la partition Windows peut être chiffrée. Le deuxième système d'exploitation doit se trouver sur une autre partition non chiffrée.

La taille du disque chiffré par PGP WDE n'est soumise à aucune restriction. Tout disque ou toute partition compatible avec le système d'exploitation (ou votre BIOS matériel pour le disque ou la partition de démarrage) doit pouvoir fonctionner avec PGP Desktop.

Pour repartitionner un disque chiffré avec PGP WDE, vous devez d'abord déchiffrer le disque. Une fois le disque déchiffré, vous pouvez le partitionner, puis chiffrer les nouvelles partitions.

Tous les modes de gestion de l'alimentation de Windows (mise en veille prolongée, veille, arrêt) sont pris en charge.

Types de disques non pris en charge

Les types de disques suivants ne sont *pas* pris en charge :

- Tout type de matériel de serveurs, y compris les disques RAID
- Disques dynamiques
- Disquettes et CD-RW/DVD-RW

Avertissement : Windows XP permet de convertir les disques normaux en disques dynamiques, afin de prendre en charge des fonctionnalités supplémentaires. N'effectuez jamais cette conversion sur le disque de démarrage d'un système déjà protégé à l'aide de PGP Whole Disk Encryption, car le disque deviendrait alors inutilisable.

Algorithme de chiffrement utilisé par PGP WDE

L'algorithme de chiffrement utilisé par PGP WDE est AES-256. L'algorithme de hachage est SHA-1. Vous ne pouvez pas modifier ces options.

Claviers pris en charge

Assurez-vous que vous utilisez un clavier présentant l'une des langues prises en charge.

L'écran d'ouverture de session PGP Whole Disk Encryption prend en charge les configurations de clavier suivantes :

- Belge (belge ; virgule)
- Belge (belge ; point)
- Bosniaque (Bosnie)
- Bosniaque (Bosnie ; cyrillique)
- Bulgare (Bulgarie)
- Bulgare (Bulgarie ; latin)
- Bulgare (Bulgarie ; clavier type machine à écrire)
- Canadien multilingue standard (Canada)
- Chinois simplifié (Chine, Singapour)
- Chinois traditionnel (Hong Kong, Taïwan)
- Croate (Croatie)
- Tchèque (Tchécoslovaquie ; clavier QWERTY)
- Danois (Danemark)
- Néerlandais (Pays-Bas)

- Anglais (États-Unis)
- Anglais (Royaume-Uni)
- Anglais (États-Unis/International)
- Estonien (Estonie)
- Finnois (Finlande)
- Français (Belgique)
- Français (Canada)
- Français (France)
- Français (Suisse)
- Allemand (Allemagne/Autriche)
- Allemand (IBM)
- Allemand (Suisse)
- Hébreu (Israël)
- Hongrois (Hongrie)
- Hongrois (Hongrie ; clavier 101 touches)
- Islandais (Islande)
- Irlandais (Irlande)
- Italien (Italie)
- Italien (Italie ; clavier 142 touches)
- Japonais (Japon)
- Coréen (Corée)
- Norvégien (Norvège)
- Polonais (Pologne ; programmeurs)
- Polonais (Pologne ; clavier 214)
- Portugais (Brésil ; claviers ABNT)
- Portugais (Brésil ; claviers ABNT2)
- Portugais (Portugal)
- Roumain (Roumanie)
- Russe (Russie ; cyrillique)
- Serbe (Serbie et Monténégro ; cyrillique)
- Serbe (Serbie et Monténégro ; latin)
- Slovaque (Slovaquie)
- Slovène (Slovénie)
- Espagnol (Espagne)

- Espagnol (Amérique latine)
- Espagnol (variante)
- Suédois (Suède)
- Turc (Turquie ; F)
- Turc (Turquie ; Q)
- Ukrainien (Ukraine)

Les mappages entre les caractères peuvent varier selon les configurations de clavier, ce qui peut provoquer des problèmes lorsque vous saisissez votre phrase secrète afin de vous authentifier. Sélectionnez la configuration dont le mappage se rapproche le plus du clavier que vous utilisez, puis veillez à employer cette même configuration chaque fois que vous vous authentifiez.

Pour plus d'informations sur les caractères pris en charge pour les phrases secrètes, reportez-vous à la section *Caractères autorisés dans les phrases secrètes PGP WDE* (à la page 170).

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 ou une partition avec des secteurs défectueux, PGP WDE 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 un 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). L'utilitaire de vérification du disque de Microsoft Windows (`chkdsk.exe`) ne permet pas de détecter ces erreurs sur le disque dur cible. Faites plutôt appel à un logiciel tel que SpinRite ou Norton Disk Doctor™. 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.

Si vous installez PGP WDE sur un système Windows Server, consultez l'*article 1737 de la base de connaissances de PGP* (http://support.pgp.com/?faq=1737) pour plus d'informations sur les meilleures pratiques.

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 ou de la partition. 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 ou de la partition
- 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 ou d'une partition 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 ou cette partition en moins d'une heure.

Vous pouvez, sans problème, utiliser votre système lors du chiffrement. Son fonctionnement sera toutefois 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.

Si vous n'avez pas besoin de votre ordinateur pendant le chiffrement, activez l'option **Utilisation maximale du CPU** afin d'accélérer le processus, comme décrit dans *Définition des options de chiffrement* (à la page 163). Cela permet de donner la priorité à l'exécution du chiffrement sur toutes les autres opérations de l'ordinateur.

Alimentation continue pendant le chiffrement

Dans la mesure où le chiffrement est un processus très consommateur en CPU, il ne peut être lancé sur un ordinateur portable alimenté par batterie. L'ordinateur *doit* impérativement être branché au secteur. Si un ordinateur portable passe sur l'alimentation par batterie au cours du processus de chiffrement initial (ou un déchiffrement ou nouveau chiffrement), PGP WDE interrompt l'opération. Celle-ci reprend lorsque l'ordinateur est rebranché à l'alimentation secteur.

Quel que soit le type d'ordinateur utilisé, il est impératif que son alimentation ne soit pas coupée, ou qu'il soit arrêté subitement, au cours du processus de chiffrement, à moins que vous ayez activé l'option **Sécurité en cas de panne de courant**. Ne retirez pas le câble d'alimentation avant la fin du chiffrement. Pour pallier cette éventualité, ou si vous ne disposez pas d'onduleur, activez l'option **Sécurité en cas de panne de courant** décrite dans *Définition des options de chiffrement* (à la page 163).

Attention : Il en est de même pour les disques amovibles, tels que les périphériques USB. À moins d'avoir activé l'option **Sécurité en cas de panne de courant**, vous risquez d'endommager le périphérique en le retirant au cours du processus.

Réalisation d'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. Consultez les problèmes d'interopérabilité connus répertoriés ci-après, ainsi que les Notes de publication de PGP Desktop contenant les mises à jour apportées à cette liste.

Incompatibilités logicielles :

- Faronics Deep Freeze (toutes éditions confondues).
- Utimaco Safeguard Easy 3.x.
- Produit de suivi et de sécurisation de portable CompuTrace d'Absolute Software. PGP Whole Disk Encryption est compatible uniquement avec la configuration BIOS de CompuTrace. Il ne peut pas être utilisé si CompuTrace fonctionne en mode MBR.
- Produits de chiffrement de disque dur de GuardianEdge Technologies : Encryption Anywhere Hard Disk et Encryption Plus Hard Disk, anciennement connus sous le nom de PC Guardian.

Les programmes suivants peuvent être installés sur le même système que PGP Desktop, mais bloqueront la fonctionnalité PGP Whole Disk Encryption :

- Safeboot Solo
- SecureStar SCPP

Définition de la méthode d'authentification du disque

Lorsque vous chiffrez un disque ou une partition à l'aide de PGP Whole Disk Encryption, vous choisissez une méthode d'authentification vous permettant de déchiffrer le disque.

Vous disposez des options suivantes :

- *Authentification par phrase secrète et authentification unique* (à la page 160)
- *Authentification par clé publique* (à la page 161)
- *Authentification par jeton* (à la page 161)
- *Authentification à deux facteurs à l'aide d'un périphérique Flash USB* (cf. "Authentification à deux facteurs à l'aide d'un périphérique USB Flash" à la page 161)
- *Authentification par module de plateforme sécurisée (TPM, Trusted Platform Module)* (cf. "Authentification à partir du module de plateforme sécurisée (TPM, Trusted Platform Module)" à la page 162)

Remarque : Sur un système sur lequel travaillent plusieurs utilisateurs, veillez à créer des méthodes d'authentification distinctes pour chaque utilisateur.

Remarque : Les utilisateurs de Windows PE ou BartPE doivent s'authentifier par phrase secrète. Les utilisateurs de jeton ou TPM ne sont pas pris en charge sur ces systèmes.

Authentification par phrase secrète et authentification unique

L'authentification par phrase secrète consiste à spécifier une phrase secrète à saisir lorsque vous redémarrez un ordinateur avec un disque (ou une partition) de démarrage chiffré ou tentez d'accéder à un autre disque (ou une partition) chiffré. Cette méthode ne nécessite aucun fichier ou matériel supplémentaire et convient aux périphériques fixes et amovibles.

Deux possibilités s'offrent à vous :

- Vous pouvez choisir une phrase secrète applicable uniquement avec PGP WDE.

- Vous pouvez synchroniser votre phrase secrète PGP WDE avec les informations d'ouverture de session Windows. Ainsi vous ne saisissez la phrase secrète qu'une fois pour déverrouiller le disque ou la partition et ouvrir une session Windows. Lorsqu'elle est synchronisée à la connexion Windows, cette option s'intitule *Authentification unique*.

Pour définir l'authentification unique, reportez-vous aux instructions de la section *Utilisation de l'authentification unique de PGP WDE* (à la page 182).

Authentification par clé publique

L'authentification par clé publique consiste à spécifier une clé publique lors du chiffrement d'un disque ou d'une partition à l'aide de PGP Whole Disk Encryption. Seul le détenteur de la clé privée correspondante peut accéder au contenu du disque ou de la partition. Pour ce faire, il doit fournir la phrase secrète de sa clé privée.

L'authentification par clé publique est uniquement disponible pour les disques amovibles utilisés avec votre système. Pour les disques fixes, notamment les disques ou partitions de démarrage et les disques dans les boîtiers USB, vous avez la possibilité de recourir à une authentification par phrase secrète ou par jeton, mais pas par clé publique.

Authentification par jeton

Lors du chiffrement d'un disque fixe (disque et partition de démarrage compris) à l'aide de la fonctionnalité PGP WDE, si vous souhaitez utiliser une clé PGP sur un jeton, vous devez disposer d'une paire de clés PGP sur un jeton ou une carte à puce compatible avec PGP WDE. Pour une liste des périphériques compatibles, reportez-vous à la section *Utilisation de cartes à puce pour l'authentification dans l'écran PGP BootGuard* (cf. "Utilisation de cartes à puce ou de jetons pour l'authentification sur l'écran PGP BootGuard" à la page 165).

La paire de clés sur un jeton renforce le niveau de sécurité, puisque vous pouvez conserver le jeton où que vous alliez.

Vous devez installer les pilotes du périphérique avant de procéder au chiffrement. Pour plus d'informations, reportez-vous à *Préparation d'un jeton à utiliser pour l'authentification* (cf. "Préparation d'une carte à puce ou d'un jeton à utiliser pour l'authentification" à la page 164).

Authentification à deux facteurs à l'aide d'un périphérique USB Flash

Vous pouvez utiliser l'authentification à deux facteurs pour améliorer la sécurité des données de votre système. Ce type d'authentification utilise « quelque chose que vous connaissez » (votre phrase secrète) et « quelque chose que vous avez » (votre périphérique USB Flash) pour vérifier que vous êtes bien qui vous dites être et que vous avez le droit d'accéder au disque.

Pour l'authentification à deux facteurs, vous créez un utilisateur de phrase secrète , puis vous sélectionnez une autre sorte de matériel pour identifier l'utilisateur. Vous avez le choix entre utiliser un lecteur flash USB et, si ce matériel est disponible sur votre système, un module de plateforme sécurisée (TPM, Trusted Platform Module).

Remarque : si vous utilisez un périphérique USB Flash pour l'authentification à deux facteurs, vous devez redémarrer votre ordinateur avec le périphérique USB inséré pour que la méthode d'authentification prenne effet. Tant que vous n'avez pas redémarré avec le périphérique USB, vous ne pouvez vous authentifier à l'écran PGP BootGuard qu'à l'aide de votre phrase secrète.

Pour plus d'informations sur la création d'une authentification à deux facteurs à l'aide d'un périphérique USB Flash, reportez-vous à la section *Chiffrement du disque* (à la page 171).

Authentification à partir du module de plateforme sécurisée (TPM, Trusted Platform Module)

Si le module de plateforme sécurisée (TPM) est disponible sur votre système, vous avez la possibilité de l'utiliser. L'ajout d'un utilisateur à TPM signifie que cet utilisateur peut uniquement s'authentifier auprès du disque sur ce système spécifique (il est « verrouillé » au système). TPM peut uniquement être utilisé avec des utilisateurs de phrases secrètes et fonctionne avec l'authentification unique.

PGP Whole Disk Encryption est compatible avec TPM version 1.1 ou 1.2.

Parmi les ordinateurs prenant en charge TPM et compatibles avec PGP WDE figurent les suivants :

- Hewlett-Packard Compaq nx6325 (TPM Infineon avec BIOS HP)
- Dell D630 (TPM Broadcom)
- Lenovo ThinkPad T60 (TPM Atmel)
- Fujitsu LifeBook T2010 (TPM Infineon avec BIOS Phoenix)
- Panasonic Toughbook T5, W5 ou Y5 (TPM Infineon avec BIOS Matsushita)

Votre fournisseur de TPM peut implémenter des fonctionnalités de sécurité qui affectent l'utilisation du TPM. Consultez la documentation de votre système pour plus d'informations.

Remarque : si vous restaurez les paramètres d'usine de votre TPM ou si vous remplacez la carte système comportant le TPM, vous ne pourrez plus accéder à votre disque chiffré quand vous utiliserez l'utilisateur TPM car vos informations d'identification stockées sur le TPM ne seront plus accessibles. Veillez donc à disposer d'une autre méthode pour accéder à votre disque chiffré (reportez-vous à la section « Considérations spéciales pour l'utilisation de TPM » ci-dessous).

Pour plus d'informations sur la création d'une authentification à deux facteurs à l'aide de TPM, reportez-vous à la section *Chiffrement du disque* (à la page 171).

Pourquoi TPM ?

Les ordinateurs équipés de TPM disposent d'un générateur de nombres aléatoires sécurisé intégré qui peut être interrogé et utilisé en tant que source de bits aléatoires. Il peut générer, charger et travailler avec des clés RSA 2048 bits. Il possède en outre des fonctionnalités anti-attaque par force brute. Si une phrase secrète incorrecte est saisie un trop grand nombre de fois, le TPM se verrouille ou ralentit considérablement ses réponses, ce qui rend l'attaque par force brute de la phrase secrète trop lente pour être utile. Ceci permet aux clés TPM protégées par des phrases secrètes de disposer d'un niveau de sécurité nettement supérieur à celui proposé par le logiciel.

Considérations spéciales pour l'utilisation de TPM

- Avant de chiffrer votre disque, veillez à établir la propriété du TPM sur le système, à configurer le TPM, puis à redémarrer votre système avant de lancer le processus de chiffrement. Lorsque vous établissez la propriété, vous configurez une phrase secrète pour TPM (différente de celle de PGP Desktop ou Windows) qui est utilisée pour modifier le TPM. Ceci vous permet de configurer des produits et de les utiliser avec TPM.
- Veillez à disposer d'une autre méthode d'authentification pour votre disque chiffré. Si vous utilisez PGP WDE dans un environnement géré par un PGP Universal Server, vous pouvez utiliser votre jeton de récupération de disque complet (Whole Disk Recovery Token). Pour plus d'informations, reportez-vous à la section *Création d'un jeton de récupération* (à la page 198). Si vous utilisez PGP WDE dans un environnement autonome, créez un utilisateur de phrase secrète en tant que sauvegarde ou créez un utilisateur de phrase secrète avec un périphérique USB Flash pour l'authentification à deux facteurs (pour plus d'informations, reportez-vous à la section *Chiffrement du disque* (à la page 171)).

Définition des options de chiffrement

Après avoir effectué les tâches de préparation du disque au chiffrement, étudiez la procédure relative au lancement du chiffrement initial :

1. Déterminez si vous souhaitez chiffrer l'ensemble du disque ou des partitions spécifiques. Reportez-vous à *Chiffrement de partitions* (à la page 164).
2. Choisissez les options à activer lors du chiffrement, telles que la sécurité en cas de panne de courant ou une vitesse de chiffrement plus rapide. Reportez-vous à *Utilisation des options de PGP Whole Disk Encryption* (à la page 168).

3 Sélectionnez une option d'authentification. Reportez-vous à la section *Définition de la méthode d'authentification du disque* (à la page 160).

Remarque : Pour une authentification par jeton, gardez le jeton à portée. Reportez-vous à *Préparation d'un jeton à utiliser pour l'authentification* (cf. "Préparation d'une carte à puce ou d'un jeton à utiliser pour l'authentification" à la page 164).

4 Suivez la procédure décrite à la section *Chiffrement d'un disque ou d'une partition* (à la page 170).

Remarque : Dans un environnement géré par un PGP Universal Server, PGP WDE crée un jeton de récupération afin de pouvoir restaurer les disques en cas d'oubli de la phrase secrète. Reportez-vous à la section *Création d'un jeton de récupération* (à la page 198).

Chiffrement de partitions

Si votre disque est divisé en partitions, vous pouvez décider de chiffrer des partitions plutôt que l'ensemble du disque. Cette flexibilité vous permet de chiffrer :

- une seule partition du disque ;
- toutes les partitions du disque sauf une ;
- le nombre de partitions souhaité.

Seuls les fichiers des partitions sélectionnées sont chiffrés.

Le double amorçage avec un autre système d'exploitation (tel que Linux) est possible, mais seule la partition Windows peut être chiffrée. Le deuxième système d'exploitation doit se trouver sur une autre partition non chiffrée.

Remarque : Une fois le chiffrement d'un disque ou de l'une de ces partitions effectué, vous ne pouvez plus modifier le partitionnement du disque (par exemple, ajouter ou supprimer une partition ou modifier la taille d'une partition). Veillez à partitionner le disque comme désiré *avant* de le protéger à l'aide de PGP Whole Disk Encryption.

Préparation d'une carte à puce ou d'un jeton à utiliser pour l'authentification

Si vous optez pour une authentification par carte à puce ou par jeton, veillez à utiliser un périphérique compatible (consultez la liste des périphériques compatibles à la section *Utilisation de cartes à puce pour l'authentification dans l'écran PGP BootGuard* (cf. "Utilisation de cartes à puce ou de jetons pour l'authentification sur l'écran PGP BootGuard" à la page 165)).

- Utilisez le modèle de jeton approprié.
- Pensez à ajouter d'autres utilisateurs (un utilisateur de phrase secrète, par exemple) pour le disque chiffré en cas de perte du jeton.

- *Avant* d'utiliser le jeton, installez les pilotes du jeton sur le système sur lequel vous l'utiliserez.

Conditions requises pour l'authentification par carte à puce ou par jeton

Lisez attentivement ces conditions et veillez à les appliquer avant de procéder au chiffrement.

Avertissement : Pour une sécurité optimale, vous pouvez choisir une authentification par une paire de clés sur un jeton pour un chiffrement avec PGP Whole Disk Encryption, mais en cas de perte du jeton, vous ne pourrez plus vous authentifier à l'écran de connexion PGP BootGuard et toutes les données du disque ou de la partition seront perdues. Aussi, il est recommandé d'ajouter d'autres utilisateurs (phrase secrète, jeton ou les deux) sur les disques et partitions chiffrés à l'aide de PGP Whole Disk Encryption. En cas de perte ou de vol du jeton, ces utilisateurs supplémentaires peuvent s'authentifier et déverrouiller le disque ou la partition pour que vous puissiez y accéder.

- Seules les paires de clés stockées sur le jeton sont valides. Vous devez créer une paire de clés sur le jeton Aladdin eToken ou envoyer une paire de clés existante vers le jeton en choisissant **Ajouter à** dans le menu contextuel.
- Lorsque vous créez ou envoyez une paire de clés sur un jeton, la phrase secrète pour la clé privée de cette paire est remplacée par le code confidentiel du jeton. Pour un jeton Aladdin eToken, le code confidentiel par défaut est 1234567890. Celui-ci étant beaucoup trop simple, modifiez immédiatement ce code à l'aide des outils de configuration d'Aladdin afin de garantir le niveau de sécurité de la paire de clés.

Utilisation de cartes à puce ou de jetons pour l'authentification sur l'écran PGP BootGuard

Cette section décrit la configuration requise (cartes à puce/jetons et lecteurs pris en charge) et fournit des instructions sur l'utilisation des cartes à puce pour l'authentification sur l'écran PGP BootGuard.

Lecteurs de cartes à puce pris en charge pour l'authentification PGP WDE

Les lecteurs de cartes à puces ci-dessous sont pris en charge lors de la communication avec une carte à puce au moment du prédémarrage. Ces lecteurs peuvent être utilisés avec toute carte à puce amovible compatible (il n'est pas nécessaire d'utiliser la même marque de carte et de lecteur).

Lecteurs de cartes à puce génériques

La plupart des lecteurs de cartes à puce CCID sont pris en charge. Les lecteurs suivants ont été testés par PGP Corporation :

- OMNIKEY CardMan 3121 USB pour systèmes de bureautique (076b:3021)
- OMNIKEY CardMan 6121 USB pour systèmes mobiles (076b:6622)
- ActivIdentity USB 2.0 (09c3:0008)
- SCM Microsystem, modèle SCR3311

Lecteurs de cartes à puce CyberJack

- Pinpad Reiner SCT CyberJack (0c4b:0100).

Lecteurs de cartes à puce ASE

- Lecteur USB Athena ASEDrive IIIe (0dc3:0802)

Lecteurs de cartes à puce intégrés

- Lecteur intégré Dell D430
- Lecteur intégré Dell D630
- Lecteur intégré Dell D830

Cartes à puce ou jetons pris en charge pour l'authentification PGP WDE

PGP Whole Disk Encryption est compatible avec les cartes à puce suivantes pour l'authentification au prédémarrage :

- Cartes ActiveIdentity ActivClientCAC, modèle 2005
- Aladdin eToken PRO 64K, 2 048 bits avec prise en charge RSA
- Clé USB Aladdin eToken PRO 32K, 2 048 bits avec prise en charge RSA
- Aladdin eToken PRO sans fonctionnalité 2 048 bits (cartes à puce plus anciennes)
- Aladdin eToken PRO Java 72K
- Aladdin eToken NG-OTP 32K

  Remarque : les autres Aladdin eTokens, tels que les jetons avec mémoire flash, fonctionnent du moment qu'ils sont compatibles APDU avec les jetons pris en charge. Les versions OEM d'Aladdin eTokens, telles que celles émises par VeriSign, fonctionnent dans la mesure où elles sont compatibles APDU avec les jetons pris en charge.

- Jeton USB Athena ASEKey Crypto pour Microsoft ILM
- Carte à puce Athena ASECard Crypto pour Microsoft ILM

Remarque : les jetons Athena sont pris en charge uniquement pour le stockage des informations d'identification.

- Axalto Cyberflex Access 32K V2
- Clé CryptoIdentity de Charismathics avec carte à puce « plug 'n' crypt » uniquement
- Jeton EMC RSA SecurID SID800 (v1 et 2)

Remarque : ce jeton est pris en charge uniquement pour le stockage de clés. SecurID n'est pas pris en charge.

- Carte à puce EMC RSA 5200
- Jeton USB Marx Cryp
- Rainbow iKey 3000
- Carte à puce S-Trust StarCOS

Remarque : les cartes S-Trust SECCOS ne sont pas prises en charge.

- Jeton USB SafeNet iKey 2032
- Carte à puce T-Systems Telesec NetKey 3.0
- Carte à puce IEI T-Systems TCOS 3.0

Cartes individuelles de vérification d'identité (PIV)

- Cartes individuelles de vérification d'identité Oberthur ID-One Cosmo V5.2D utilisant le logiciel client ActivClient version 6.1
- Cartes individuelles de vérification d'identité Giesecke and Devrient Sm@rtCafe Expert 3.2 utilisant le logiciel client ActivClient version 6.1

Pilotes requis pour le jeton Aladdin eToken

Avant d'utiliser Aladdin eToken, installez les derniers pilotes du logiciel sur le système sur lequel vous utiliserez le jeton. Il se peut que Microsoft Windows reconnaisse le jeton de manière générique même si vous n'installez pas les pilotes, mais PGP Desktop *requiert* leur installation. La dernière version des pilotes est disponible sur le *site Web du support technique Aladdin* (http://www.aladdin.com/support/default.asp).

Téléchargez la dernière version du pilote **eToken PKI Client (RTE)** (la version 4.5 était la plus récente au moment de la rédaction de ce document), puis installez-la sur votre ordinateur. Une fois le pilote installé, ouvrez PGP Desktop et cliquez sur la boîte de contrôle Clé PGP. Si le pilote est installé correctement, **Clés de carte à puce** s'affiche dans la liste de la boîte de contrôle Clés PGP.

Si **Aucune clé adéquate disponible** apparaît dans le champ **Sélectionner une clé** lorsque vous définissez la méthode d'authentification sur **Utilisateur de clés de jeton** pour le disque ou la partition que vous chiffrez à l'aide de PGP Whole Disk Encryption, plusieurs causes sont possibles :

- Votre jeton Aladdin eToken n'est pas inséré.
- Vous ne disposez pas de la bonne version du pilote ou ce dernier n'est pas installé correctement.
- La paire de clés sur le jeton est inutilisable ou le eToken ne contient aucune clé (il est vide).

Utilisation des options de PGP Whole Disk Encryption

La fonctionnalité PGP Whole Disk Encryption propose deux options à sélectionner avant de protéger le disque ou la partition :

- **Utilisation maximale du CPU :** méthode la plus rapide, et tout aussi sûre, d'effectuer le chiffrement initial du disque à l'aide de PGP Whole Disk Encryption. Elle permet de donner la priorité à l'exécution du chiffrement sur toutes les autres opérations de l'ordinateur. Activez cette option lorsque vous n'avez pas besoin de votre ordinateur.
- **Sécurité en cas de panne de courant :** vous pouvez interrompre le processus de chiffrement initial à tout moment en arrêtant ou en redémarrant votre ordinateur correctement, mais vous devez rester extrêmement vigilent afin d'éviter tout arrêt intempestif (panne de courant, retrait du câble d'alimentation, etc.). Pour pallier cette éventualité, ou si vous ne disposez pas d'onduleur, activez l'option **Sécurité en cas de panne de courant**. **Le chiffrement est alors journalisé, ce qui permet au processus de reprendre précisément où il a été interrompu, en toute sécurité, en cas de coupure de l'alimentation. Cette option peut toutefois allonger la durée du chiffrement initial.**

  Elle est également utile pour le chiffrement des périphériques USB. Si le chiffrement est interrompu par le retrait du périphérique, ce dernier peut être endommagé et nécessiter un reformatage. Le mode Sécurité en cas de panne de courant vous permet de retirer le périphérique USB au cours du chiffrement et de reprendre le processus en l'insérant de nouveau.

Ce tableau peut vous aider à déterminer les options adaptées :

Option sélectionnée	Avantages	Éléments à prendre en compte
Aucune option (normal)	Chiffrement du disque ou de la partition avec un bon compromis entre vitesse et sécurité. Vous pouvez utiliser l'ordinateur pendant le processus de	Le chiffrement est effectué à une vitesse normale. Vous devez veiller à ce que l'ordinateur ne s'arrête pas inopinément pour éviter toute perte de données.

Option sélectionnée	Avantages	Éléments à prendre en compte
	chiffrement. Adapté à la majorité des utilisateurs.	
Utilisation maximale du CPU	Chiffrement du disque ou de la partition plus rapidement qu'en mode normal. Bien que plus rapide, le processus reste aussi sûr.	Cette option monopolise la puissance de l'ordinateur, réduisant ainsi la réactivité du système au cours du processus de chiffrement du disque ou de la partition.
Sécurité en cas de panne de courant	Chiffrement du disque ou de la partition à l'aide d'une méthode permettant de reprendre le processus facilement et en toute sécurité en cas de coupure de l'alimentation. Idéal pour les environnements présentant un risque de coupure de courant.	Durée du processus supérieure à celle du mode normal.
Activation des deux options	Protection du disque ou de la partition avec la sécurité accrue du mode Sécurité en cas de panne de courant. Fonctionnement plus rapide qu'avec le mode Sécurité en cas de panne de courant seul.	Ralentissement du système beaucoup plus important qu'en mode normal.

Chiffrement d'un disque ou d'une partition

Après avoir préparé le disque et défini les options de chiffrement, vous pouvez chiffrer le disque ou la partition. Tenez compte des informations suivantes avant de commencer.

- Si vous utilisez un jeton USB pour vous authentifier sur un disque fixe sécurisé à l'aide de PGP Whole Disk Encryption, vérifiez que vous possédez le jeton correspondant et que le pilote requis est installé. Pour plus d'informations, reportez-vous à la section *Authentification par jeton* (à la page 161).

  Remarque : L'authentification par jeton n'est pas disponible en mode d'authentification unique.

- Au cours du processus de chiffrement, vous pouvez utiliser le système, mais son fonctionnement est ralenti. Il fonctionne de nouveau normalement une fois le chiffrement terminé.

  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.

- Vous pouvez minimiser ou fermer PGP Desktop lors du chiffrement. Cela n'affecte pas le processus, mais permet d'accélérer le chiffrement.

- Pour interrompre le processus de chiffrement pour une courte période, cliquez sur **Arrêter**, puis sur **Pause** dans la boîte de dialogue. Cliquez sur **Reprendre** pour redémarrer. Il se peut que vous soyez invité à vous authentifier**.**

- Pour arrêter le système avant la fin du chiffrement, procédez à un arrêt normal. Il n'est pas nécessaire d'interrompre le processus. Lorsque vous redémarrez, le chiffrement reprend automatiquement où il s'était arrêté.

- Vous pouvez uniquement chiffrer ou déchiffrer un disque ou une partition à la fois. Lorsque vous commencez une opération sur un disque ou une partition, vous ne pouvez pas lancer le chiffrement d'un autre disque avant la fin du premier, et ce, même si vous interrompez la première opération.

Caractères autorisés dans les phrases secrètes PGP WDE

Lorsque vous créez des phrases secrètes avec PGP Whole Disk Encryption, vous pouvez saisir des caractères alphanumériques, des signes de ponctuation, des métacaractères standard et des caractères ASCII étendus. Les caractères de tabulation et de contrôle ne sont pas autorisés. Lorsque vous choisissez une phrase secrète, tenez compte des informations suivantes.

Les caractères pris en charge sont les suivants :
abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789

`~!@#$%^&*()_+={}\|:;[]'"<>,.?/-

- La plupart des caractères ASCII étendus (tels que ç é è ê ë î ï ô û ù ü ÿ) ou les symboles (tels que ¢ ® œ) sont pris en charge.

Les caractères non pris en charge lors de la saisie d'une phrase secrète sont répertoriés dans le tableau ci-dessous, pour le clavier associé :

Clavier	Caractères non pris en charge
Italien (Italie)	`~
Hébreu (Israël)	abcdefghijklmnopqrstuvwxyz`
Russe (Russie)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ`@#$^&{}|[]'<>~
Bosniaque (Bosnie ; cyrillique)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
Bulgare (Bulgarie)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUWXYZ'[]<>{}@#$^&*
Polonais (Pologne ; clavier 214)	[]|
Serbe (Serbie ; cyrillique)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ[]{}|@^
Ukrainien (Ukraine)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ'[]`<>{}|~@#$^&

Chiffrement du disque

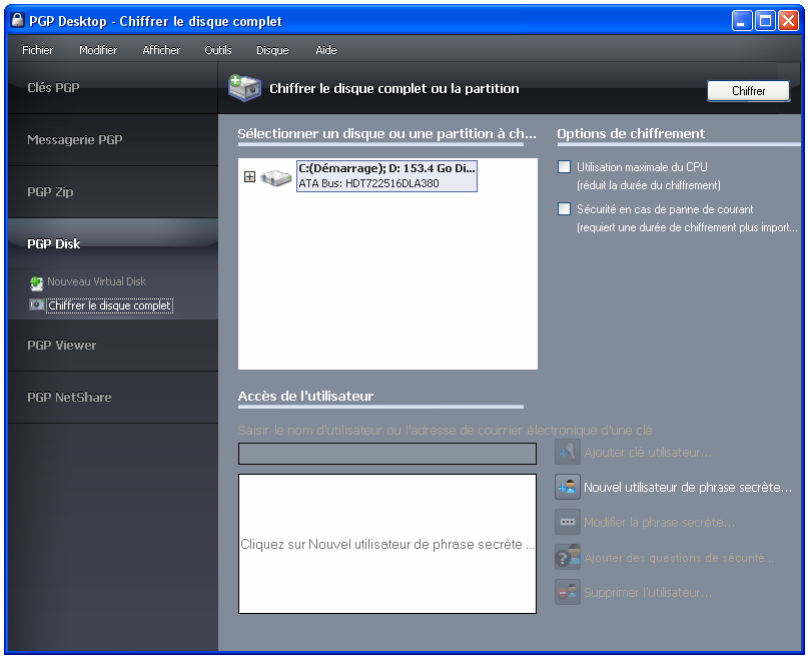
Avant de chiffrer votre disque, assurez-vous de sauvegarder son contenu afin de ne perdre aucune donnée en cas de perte ou de vol de l'ordinateur ou d'incapacité à déchiffrer le disque.

Vous pouvez uniquement chiffrer ou déchiffrer un disque ou une partition à la fois. Lorsque vous commencez une opération sur un disque ou une partition, vous ne pouvez pas lancer le chiffrement d'un autre support avant la fin du premier, et ce, même si vous interrompez la première opération.

Pour protéger un disque ou une partition à l'aide de PGP Whole Disk Encryption

1 Ouvrez PGP Desktop et cliquez sur le panneau de contrôle PGP Disk. Le panneau de contrôle est alors mis en surbrillance.

2 Cliquez sur **Chiffrer le disque complet**. La zone de travail Chiffrer le disque complet (partition) apparaît, présentant la liste des disques de votre système pouvant être protégés par PGP Whole Disk Encryption : disques, partitions de disque, supports amovibles, etc.



3 Dans la section supérieure **Sélectionner un disque ou une partition à chiffrer** de cette zone de travail, cliquez sur le disque ou la partition que vous souhaitez protéger avec PGP Whole Disk Encryption.

4 Sélectionnez les **options de chiffrement désirées, le cas échéant. Pour plus d'informations sur ces options, reportez-vous à la section** *Utilisation des options de PGP Whole Disk Encryption* (à la page 168).

5 Dans la section **Accès de l'utilisateur**, précisez la méthode d'accès aux disques et partitions souhaitée :

- **Utilisateur de clé publique basée sur une autorisation de jeton** : cette option permet de protéger un disque fixe (non amovible) du système.

- Saisissez le nom d'utilisateur ou l'adresse de courrier électronique associé à la clé, puis appuyez sur **Entrée** pour rechercher la clé. Vous pouvez également sélectionner **Ajouter clé utilisateur**. La liste des paires de clés présentes dans votre trousseau de clés s'affiche. Dans la boîte de dialogue Source de clé, sélectionnez la clé publique ou les clés à utiliser. Cliquez sur **Ajouter** pour déplacer les clés vers le champ **Clés à ajouter**, puis cliquez sur **OK**. Cliquez sur **Chiffrer**.

- **Utilisateur de phrase secrète** : pour protéger votre disque ou partition avec une phrase secrète, sélectionnez **Nouvel utilisateur de phrase secrète**. La boîte de dialogue Assistant de PGP Disk : Chiffrement complet du disque - Nouvel utilisateur apparaît.

  - **Pour déverrouiller le disque chiffré à l'aide des informations d'ouverture de session Windows**, sélectionnez **Utiliser le mot de passe Windows**, puis cliquez sur **Suivant.** Dans la boîte de dialogue Assistant de PGP Disk : Authentification à 2 facteurs, sélectionnez **Poursuivre avec l'authentification de la phrase secrète uniquement** et cliquez sur **Suivant**. Dans la boîte de dialogue Assistant de PGP Disk : Informations d'ouverture de session Windows, saisissez votre nom d'utilisateur Windows, le domaine et le mot de passe, puis cliquez sur **Suivant**. Cliquez sur **Terminer**.

  Si vous sélectionnez l'option **Utiliser le mot de passe Windows**, après le chiffrement initial, saisissez votre mot de passe Windows lorsque l'écran PGP BootGuard s'affiche au démarrage. La fonctionnalité d'authentification unique de PGP ouvre automatiquement une session Windows. Vous ne saisissez la phrase secrète qu'une seule fois. Pour plus d'informations sur cette fonctionnalité, reportez-vous à la section *Utilisation de l'authentification unique de PGP WDE* (à la page 182).

  - **Pour déverrouiller le disque chiffré ou la partition chiffrée à l'aide d'une phrase secrète**, sélectionnez **Créer une phrase secrète,** puis cliquez sur **Suivant**. Dans la boîte de dialogue Assistant de PGP Disk : Authentification à 2 facteurs, sélectionnez **Poursuivre avec l'authentification de la phrase secrète uniquement** et cliquez sur **Suivant**. Dans la boîte de dialogue Assistant de PGP Disk : Créer un nom d'utilisateur et une phrase secrète, saisissez le nom du nouvel utilisateur et la phrase secrète à associer à cet utilisateur. Tapez à nouveau la phrase secrète dans le champ **Confirmer** et cliquez sur **Suivant**. Cliquez sur **Terminer**.

  - **Pour déverrouiller le disque chiffré ou la partition chiffrée à l'aide d'une authentification à deux facteurs avec une phrase secrète et un lecteur USB Flash**, sélectionnez **Créer une phrase secrète,** puis cliquez sur **Suivant**.

Dans la boîte de dialogue Assistant de PGP Disk : Authentification à 2 facteurs, sélectionnez **Périphérique USB Flash générique**, choisissez le périphérique dans la liste et cliquez sur **Suivant**. Dans la boîte de dialogue Assistant de PGP Disk : Créer un nom d'utilisateur et une phrase secrète, saisissez le nom du nouvel utilisateur et la phrase secrète à associer à cet utilisateur. Tapez à nouveau la phrase secrète dans le champ **Confirmer** et cliquez sur **Suivant**. Cliquez sur **Terminer**.

- **Pour déverrouiller le disque chiffré ou la partition chiffrée à l'aide d'une authentification à deux facteurs avec une phrase secrète et un module de plateforme sécurisée**, sélectionnez **Créer une phrase secrète,** puis cliquez sur **Suivant**. Dans la boîte de dialogue Assistant de PGP Disk : Authentification à 2 facteurs, sélectionnez **Module de plateforme sécurisée**, puis cliquez sur **Suivant**. Dans la boîte de dialogue Assistant de PGP Disk : Créer un nom d'utilisateur et une phrase secrète, saisissez le nom du nouvel utilisateur et la phrase secrète à associer à cet utilisateur. Tapez à nouveau la phrase secrète dans le champ **Confirmer** et cliquez sur **Suivant**. Cliquez sur **Terminer**.

Normalement, afin de renforcer le niveau de sécurité, les caractères que vous saisissez pour la phrase secrète ne sont pas visibles à l'écran. Cependant, si vous êtes certain que personne ne surveille vos activités (soit physiquement, par-dessus votre épaule, soit en analysant les ondes radio émises par votre écran), vous pouvez afficher les caractères saisis pour la phrase secrète en cochant la case **Afficher les frappes**. Reportez-vous à la section *Indicateur de qualité de la phrase secrète* (à la page 336).

Attention : il est vivement recommandé d'utiliser une configuration de clavier prise en charge lorsque vous créez une phrase secrète pour les disques et partitions protégés par PGP Whole Disk Encryption (pour plus d'informations, reportez-vous à la section *Claviers pris en charge* (à la page 155)). L'écran d'ouverture de session de PGP Whole Disk Encryption suppose que vous utilisez une configuration de clavier compatible lorsque vous saisissez la phrase secrète pour l'authentification. L'utilisation d'une configuration différente peut causer des problèmes d'authentification. Pour plus d'informations, reportez-vous à la section *Authentification dans l'écran PGP BootGuard* (cf. "Authentification à partir de l'écran PGP BootGuard" à la page 176).

6 Vérifiez que vous disposez de la méthode d'accès utilisateur souhaitée, puis cliquez sur **Chiffrer**.

7 Lisez les informations de la boîte de dialogue, puis cliquez sur **OK**.

8 Pour connaître l'avancement du chiffrement sur le disque, observez la barre **Progression du chiffrement**.

9 Pour interrompre temporairement le processus, cliquez sur **Arrêter**, puis sur **Pause** dans la boîte de dialogue qui s'affiche. Pour reprendre le chiffrement, cliquez sur **Reprendre**. Vous pouvez être invité à saisir la phrase secrète.

Remarque : si le processus s'arrête pour signaler une erreur de lecture/écriture sur le disque, cela signifie que PGP Desktop a identifié des secteurs défectueux sur votre disque ou partition au cours du chiffrement. Vous pouvez continuer le chiffrement ou l'annuler afin de corriger les erreurs. Reportez-vous à la section *Identification d'erreurs sur le disque lors du chiffrement* (à la page 175). Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, les secteurs défectueux identifiés lors du chiffrement sont consignés sur ce serveur et le processus se poursuit.

À l'issue du chiffrement, l'utilisateur qui a chiffré le disque est indiqué dans la section Accès de l'utilisateur, et des options d'accès utilisateur supplémentaires permettant d'ajouter un nouvel utilisateur, de modifier la phrase secrète ou de supprimer un utilisateur deviennent disponibles.

10 Lorsque le chiffrement du disque est terminé, PGP Corporation vous recommande de créer un disque de récupération. Pour plus d'informations, reportez-vous à la section *Création de disques de récupération* (cf. "Création et utilisation de disques de récupération" à la page 200).

Identification d'erreurs sur le disque lors du chiffrement

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

De nombreux disques durs présentent des secteurs défectueux. Si PGP WDE identifie des secteurs défectueux lors du chiffrement, le processus est suspendu. Un message d'avertissement vous informe que PGP WDE a détecté des erreurs sur le disque. (Remarque : ces erreurs ne sont pas liées au chiffrement et indiquent que votre disque dur doit faire l'objet d'une maintenance.)

Vous pouvez effectuer l'une des opérations suivantes :

- Forcer la poursuite du chiffrement en cliquant sur **Oui**. Les erreurs sur le disque sont fréquentes et souvent inoffensives. Si vous cliquez sur **Oui**, le processus de chiffrement se poursuit et PGP WDE ignore les erreurs ultérieures.
- Arrêter le chiffrement en cliquant sur **Non**, déchiffrer entièrement le disque, puis réparer les erreurs à l'aide d'un outil tel que SpinRite ou Norton Disk Doctor avant toute autre tentative de chiffrement. Si vous savez que votre disque est très fragmenté ou qu'il comporte de nombreux secteurs défectueux, exécutez les procédures de maintenance nécessaires avant de le chiffrer.

Utilisation d'un disque chiffré par PGP WDE

Votre ordinateur démarre différemment lorsque vous utilisez PGP Whole Disk Encryption pour protéger le disque de démarrage, ou un disque fixe secondaire, sur votre système. Au démarrage, l'écran de connexion PGP BootGuard s'affiche et vous invite à saisir votre phrase secrète.

PGP WDE procède ensuite au déchiffrement du disque. Si la fonctionnalité d'authentification unique est activée (synchronisation de votre phrase secrète PGP WDE et des informations d'ouverture de session Windows), vous ouvrez également une session Windows.

Lorsque vous utilisez un disque chiffré par PGP WDE, il est déchiffré et ouvert automatiquement, si nécessaire. Avec la plupart des ordinateurs modernes, une fois le disque entièrement chiffré, vous ne constatez aucune interruption de vos activités.

Lorsque vous déverrouillez un disque ou une partition, les fichiers sont accessibles à tout utilisateur en mesure d'utiliser physiquement votre ordinateur. Les fichiers sont déverrouillés jusqu'à ce que vous les verrouilliez de nouveau en arrêtant l'ordinateur.

Avertissement : Vos fichiers étant accessibles tant que vous ne les verrouillez pas de nouveau, il est préférable de stocker sur un volume PGP Virtual Disk les fichiers à sécuriser même lorsque l'ordinateur est utilisé. Reportez-vous à *Utilisation des PGP Virtual Disks* (à la page 211).

Lorsque vous arrêtez un système avec un disque (ou une partition) de démarrage chiffré, ou si vous retirez un disque amovible chiffré du système, tous les fichiers du disque (ou de la partition) restent chiffrés et entièrement protégés. Les données ne sont jamais écrites sur le disque ou la partition sous une forme non chiffrée. Pour accéder aux fichiers, une authentification est requise (phrase secrète, jeton ou clé privée).

Authentification à partir de l'écran PGP BootGuard

L'écran de connexion PGP BootGuard vous invite à saisir la phrase secrète du disque (ou de la partition) protégé pour l'une des deux raisons suivantes :

- Lorsque PGP Whole Disk Encryption protège votre disque ou partition de démarrage, vous devez vous authentifier afin de démarrer le système. Cette procédure est obligatoire, car les fichiers du système d'exploitation qui contrôlent le démarrage sont chiffrés et doivent être déchiffrés avant de pouvoir être utilisés pour lancer le système. La fonctionnalité d'authentification unique de PGP ouvre automatiquement une session Windows, si vous choisissez l'option correspondante lors du chiffrement initial du disque ou de la partition.

- Si PGP Whole Disk Encryption protège un disque fixe ou une partition secondaire, vous pouvez vous authentifier au démarrage. Ainsi, vous n'avez plus à le faire lorsque vous souhaitez utiliser des fichiers sur un disque ou une partition secondaire. Les fichiers du disque ou de la partition secondaire n'étant pas nécessaire pour le démarrage, l'authentification au démarrage n'est pas obligatoire. Si vous disposez de droits d'administration, et à condition que votre stratégie PGP Universal Server l'autorise, vous pouvez utiliser la fonctionnalité Contournement pour ignorer l'étape d'authentification au démarrage. Il vous sera demandé de vous authentifier ultérieurement lorsque vous tenterez d'utiliser les fichiers du disque ou de la partition secondaire.

Remarque : L'écran PGP BootGuard accepte les informations d'authentification de tous les utilisateurs configurés lors du chiffrement du disque ou de la partition. Par exemple, si deux utilisateurs sont configurés pour un disque ou une partition de démarrage et deux autres utilisateurs pour un disque fixe ou une partition secondaire sur le même système, *chacun* des quatre utilisateurs peut s'authentifier sur l'écran de connexion PGP BootGuard au démarrage à l'aide de leur phrase secrète.

Sur l'écran de connexion PGP BootGuard, vous pouvez :

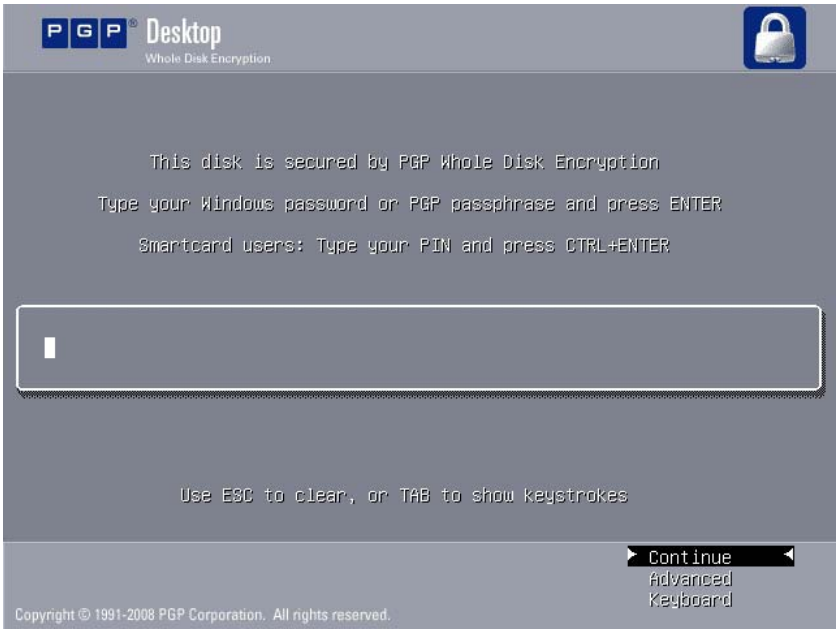
- vous authentifier sur un disque ou une partition de démarrage du système ;
- afficher les informations relatives aux disques ou aux partitions sur votre système et accéder à la fonctionnalité Contournement (cette fonctionnalité peut être utilisée par les utilisateurs disposant de droits d'administration uniquement si la stratégie PGP Universal l'autorise) ;
- choisir la configuration du clavier.

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, l'administrateur PGP peut avoir personnalisé l'écran PGP Whole Disk Encryption BootGuard pour inclure du texte supplémentaire ou une image personnalisée, telle que le logo de votre entreprise. Les graphiques inclus dans ce guide illustrent l'installation par défaut. Votre écran d'ouverture de session peut être différent si l'administrateur l'a personnalisé.

Pour une authentification à partir de l'écran d'ouverture de session PGP BootGuard

1. Démarrez ou redémarrez le système sur lequel PGP Whole Disk Encryption protège un disque ou une partition. Lors du démarrage, l'écran d'ouverture de session PGP BootGuard s'affiche.

Remarque : Si vous utilisez un périphérique USB pour une authentification à deux facteurs, veillez à insérer le périphérique correctement *avant* de démarrer ou redémarrer le système.



2 Saisissez une phrase secrète valide ou le mot de passe Windows et appuyez sur **Entrée**.

Attention : L'écran de connexion PGP BootGuard suppose que vous utilisez une configuration de clavier compatible lorsque vous saisissez la phrase secrète. L'utilisation d'une configuration différente lors de la création d'une phrase secrète pour les disques ou partitions protégés par PGP Whole Disk Encryption peut causer des problèmes d'authentification en raison de la différence de mappage entre les configurations. Reportez-vous à *Sélection des configurations de clavier* (à la page 180).

Pour afficher les caractères lors de la saisie, appuyez sur la touche **Tabulation** avant de commencer à taper.

Si vous vous trompez lors de la saisie ou pensez avoir fait une erreur, appuyez sur la touche **Échap** pour effacer tous les caractères et recommencer.

Si l'auto-récupération en local a été configurée et que vous avez oublié votre phrase secrète, sélectionnez **J'ai oublié ma phrase secrète**. Pour plus d'informations, reportez-vous à la section *Utilisation de l'auto-récupération en local* (cf. "Vous avez oublié votre phrase secrète" à la page 190).

Remarque : Pour l'authentification par jeton dans PGP BootGuard, appuyez sur Ctrl+Entrée. L'authentification des jetons dans PGP BootGuard peut prendre un certain temps.

3 Si vous saisissez une phrase secrète valide, l'écran d'ouverture de session PGP BootGuard disparaît et le système démarre normalement.

Si vous avez choisi une authentification à l'aide des informations d'ouverture de session Windows lors du chiffrement du disque initial, la fonctionnalité PGP Whole Disk Encryption ouvre automatiquement une session Windows. Vous ne saisissez la phrase secrète qu'une seule fois.

Si la phrase secrète saisie est incorrecte, un message d'erreur apparaît. Ressaisissez la phrase secrète.

Sons perceptibles lors de l'authentification

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server et que votre administrateur PGP a activé cette option, votre système émet des sons perceptibles au cours de l'authentification PGP BootGuard. Il existe trois paires de sons différentes qui indiquent quand saisir une phrase secrète, ainsi que la réussite ou l'échec de l'authentification.

Chaque indicateur commence par un son moyen, tandis que le deuxième son est plus fort, identique ou moins fort.

- Lorsque le système est prêt pour la saisie de la phrase secrète ou du code confidentiel, le son moyen-moyen (prêt) est joué. Lorsque vous l'entendez, tapez votre phrase secrète et appuyez sur Entrée.
- Une fois la phrase secrète entrée, les sons joués dépendent de sa réussite ou de son échec :
  - Si l'authentification de la phrase secrète réussit, le son moyen-fort est joué. Le système poursuit alors son démarrage.
  - Si l'authentification de la phrase secrète échoue, le son moyen-faible est joué. L'écran d'authentification PGP BootGuard s'affiche et le champ contenant la phrase secrète est effacé afin que vous puissiez la saisir à nouveau.

Ces sons ne peuvent pas être personnalisés par l'administrateur PGP. Celui-ci peut uniquement activer ou désactiver ces sons au cours de l'authentification PGP BootGuard.

Verrouillage de l'écran PGP BootGuard

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, l'administrateur PGP peut avoir défini un verrouillage de PGP BootGuard. Vous êtes « verrouillé » si vous dépassez le nombre maximal autorisé de tentatives de saisie de phrase secrète sur l'écran PGP BootGuard. Ceci est valable uniquement pour les utilisateurs de phrases secrètes (les utilisateurs de jeton ou TPM ne sont pas concernés).

Pour annuler le verrouillage, contactez votre administrateur PGP.

Sélection des configurations de clavier

L'écran d'ouverture de session PGP Whole Disk Encryption prend en charge les configurations de clavier suivantes :

- Belge (belge ; virgule)
- Belge (belge ; point)
- Bosniaque (Bosnie)
- Bosniaque (Bosnie ; cyrillique)
- Bulgare (Bulgarie)
- Bulgare (Bulgarie ; latin)
- Bulgare (Bulgarie ; clavier type machine à écrire)
- Canadien multilingue standard (Canada)
- Chinois simplifié (Chine, Singapour)
- Chinois traditionnel (Hong Kong, Taïwan)
- Croate (Croatie)
- Tchèque (Tchécoslovaquie ; clavier QWERTY)
- Danois (Danemark)
- Néerlandais (Pays-Bas)
- Anglais (États-Unis)
- Anglais (Royaume-Uni)
- Anglais (États-Unis/International)
- Estonien (Estonie)
- Finnois (Finlande)
- Français (Belgique)
- Français (Canada)
- Français (France)
- Français (Suisse)
- Allemand (Allemagne/Autriche)
- Allemand (IBM)
- Allemand (Suisse)
- Hébreu (Israël)
- Hongrois (Hongrie)
- Hongrois (Hongrie ; clavier 101 touches)
- Islandais (Islande)

- Irlandais (Irlande)
- Italien (Italie)
- Italien (Italie ; clavier 142 touches)
- Japonais (Japon)
- Coréen (Corée)
- Norvégien (Norvège)
- Polonais (Pologne ; programmeurs)
- Polonais (Pologne ; clavier 214)
- Portugais (Brésil ; claviers ABNT)
- Portugais (Brésil ; claviers ABNT2)
- Portugais (Portugal)
- Roumain (Roumanie)
- Russe (Russie ; cyrillique)
- Serbe (Serbie et Monténégro ; cyrillique)
- Serbe (Serbie et Monténégro ; latin)
- Slovaque (Slovaquie)
- Slovène (Slovénie)
- Espagnol (Espagne)
- Espagnol (Amérique latine)
- Espagnol (variante)
- Suédois (Suède)
- Turc (Turquie ; F)
- Turc (Turquie ; Q)
- Ukrainien (Ukraine)

Les mappages entre les caractères peuvent varier selon les configurations de clavier, ce qui peut provoquer des problèmes lorsque vous saisissez votre phrase secrète afin de vous authentifier. Sélectionnez la configuration dont le mappage se rapproche le plus du clavier que vous utilisez, puis veillez à employer cette même configuration chaque fois que vous vous authentifiez.

Pour sélectionner une configuration de clavier

1. Démarrez ou redémarrez le système comportant la partition ou le disque protégé par PGP Whole Disk Encryption. Lors du démarrage, l'écran d'ouverture de session PGP BootGuard s'affiche.
2. Appuyez sur la flèche vers le bas de votre clavier jusqu'à ce que le mot **Clavier** apparaisse en surbrillance.

3 Appuyez sur **Entrée**. L'écran Configurations du clavier apparaît.

4 Appuyez sur la touche **Tabulation** pour activer la liste des configurations de clavier, puis utilisez les flèches haut et bas de votre clavier pour sélectionner la configuration de votre choix.

5 Appuyez à nouveau sur la touche **Tabulation**. L'option **Retour** est mise en surbrillance.

6 Appuyez sur **Entrée**. L'écran d'ouverture de session PGP BootGuard s'affiche à nouveau.

Utilisation de l'authentification unique de PGP WDE

L'authentification unique permet de s'authentifier sur le disque chiffré par PGP WDE et d'ouvrir une session Windows à l'aide de la phrase secrète Windows.

Fonctionnement de l'authentification unique

L'authentification unique utilise l'une des méthodes offertes par Microsoft Windows pour personnaliser la connexion Windows. PGP WDE s'appuie sur les informations d'authentification définies afin de créer de manière dynamiques des entrées de registre spécifiques lors de la tentative de connexion.

Remarque : Votre mot de passe Windows n'est *jamais* stocké dans le registre, ni sous aucune forme sur le disque, chiffrée ou non.

Conditions préalables à l'utilisation de l'authentification unique

- Vous devez avoir installé PGP Whole Disk Encryption.

Utilisateurs locaux et authentification unique

Si un ordinateur n'est pas membre d'un domaine, PGP Whole Disk Encryption désactive automatiquement certaines fonctionnalités d'accès lors de l'ajout d'un utilisateur avec authentification unique à un disque, dont Utiliser l'écran d'accueil et Utiliser la bascule rapide utilisateur (qui dépend de l'écran d'accueil), de manière à rendre le panneau Sécurité de Windows disponible lors de l'utilisation de la combinaison de touches Ctrl+Alt+Suppr.

Ces fonctionnalités sont déjà automatiquement désactivées si les ordinateurs sont membres d'un domaine.

Chiffrement du disque afin d'utiliser l'authentification unique

▸ **Pour chiffrer le disque afin d'utiliser l'authentification unique**

1. Cliquez sur la boîte de contrôle PGP Disk, puis sélectionnez **Chiffrer le disque complet**.
2. Sélectionnez le disque ou la partition à chiffrer, puis choisissez les options PGP Whole Disk Encryption souhaitées, le cas échant. Pour plus d'informations sur ces options, reportez-vous à la section *Définition des options de chiffrement* (à la page 163).
3. Dans la section **Accès de l'utilisateur**, sélectionnez **Nouvel utilisateur de phrase secrète**.
4. Sélectionnez **Utiliser le mot de passe Windows**, puis cliquez sur **Suivant**.
5. Saisissez votre mot de passe d'ouverture de session Windows, puis cliquez sur **Terminer**.

   PGP Whole Disk Encryption vérifie que votre nom est correct sur le domaine, et que le mot de passe Windows correspond. PGP Whole Disk Encryption vérifie également votre mot de passe afin de s'assurer qu'il contient uniquement des caractères autorisés. Si ce n'est pas le cas, vous ne serez pas autorisé à continuer. Reportez-vous à la section *Caractères pris en charge pour les phrases secrètes PGP WDE* (cf. "Caractères autorisés dans les phrases secrètes PGP WDE" à la page 170) pours plus d'informations sur les caractères autorisés.
6. Cliquez sur **Chiffrer**, puis sur **OK**.

Utilisateurs multiples et authentification unique

Vous pouvez configurer jusqu'à 28 utilisateurs pour l'authentification unique. Cependant, PGP Corporation recommande de limiter leur nombre au moins de personnes possibles devant partager le système. Bien qu'il soit techniquement possible de le faire, un grand nombre d'utilisateurs partageant un ordinateur chiffré unique n'est pas une solution offrant un niveau de sécurité suffisant, et PGP Corporation déconseille cette pratique.

Remarque : la fonctionnalité d'authentification unique s'utilise exclusivement avec des phrases secrètes ; vous ne pouvez donc pas l'utiliser avec des clés utilisateur, et elle n'est pas compatible avec des cartes à puce ou jetons.

Ouverture de session avec authentification unique

Après avoir configuré l'authentification unique, l'écran PGP BootGuard s'affiche lorsque vous démarrez le système. Si vous indiquez le nom d'utilisateur et le mot de passe corrects, PGP WDE ouvre la session Windows et offre un accès aux partitions de disque chiffrées avec PGP WDE.

Modification de votre phrase secrète avec l'authentification unique

Pour synchroniser les modifications apportées à votre mot de passe Windows avec PGP WDE, vous devez modifier votre mot de passe pour l'authentification unique à l'aide de la fonctionnalité **Modifier le mot de passe...** de la boîte de dialogue Sécurité de Windows, accessible à l'aide de la combinaison de touches CTRL+ALT+SUPPR.

Pour modifier votre phrase secrète

1. Appuyez sur Ctrl+Alt+Suppr.
2. Saisissez votre ancien mot de passe.
3. Entrez et confirmez le nouveau.
4. Cliquez sur **OK**.

   L'authentification unique se synchronise de manière automatique et transparente avec ce nouveau mot de passe. Vous pouvez utiliser ce nouveau mot de passe immédiatement, lors de votre prochaine tentative d'ouverture de session.

Attention : si vous modifiez votre mot de passe d'une autre manière (via le contrôleur de domaine, le Panneau de configuration Windows, par l'intermédiaire de l'administrateur système ou à partir d'un autre système) votre prochaine tentative d'ouverture de session sur l'écran PGP BootGuard échouera. Vous devrez alors indiquer votre ancien mot de passe Windows. L'ouverture de session réussie sur l'écran PGP BootGuard à l'aide de votre ancien mot de passe Windows ouvrira ensuite l'écran de saisie du nom d'utilisateur/mot de passe d'ouverture de session Windows. Puis, vous devrez ouvrir une session à l'aide de votre nouveau mot de passe Windows, stade auquel PGP WDE se synchronisera avec le nouveau mot de passe.

Affichage de la boîte de dialogue Connexion Windows

Lorsque vous utilisez PGP WDE avec SSO, une fois que vous avez entré votre phrase secrète dans l'écran PGP BootGuard, vous êtes automatiquement connecté à votre ordinateur. Dès que Windows est démarré, votre bureau Windows s'affiche.

Il peut cependant arriver que vous ayez à vous connecter à votre système à l'aide de la boîte de dialogue Connexion Windows, au lieu d'être automatiquement connecté. Par exemple, vous pouvez avoir besoin d'accéder à certaines boîtes de dialogue réseau, telles que le réseau privé virtuel (VPN) de votre entreprise, qui peuvent être contournées par SSO.

Pour ignorer l'ouverture de session PGP WDE SSO et afficher la boîte de dialogue Connexion Windows

1. Connectez-vous comme d'habitude à votre ordinateur à l'écran PGP BootGuard en saisissant votre phrase secrète et en appuyant sur la touche Entrée.
2. Lorsque l'écran de démarrage Microsoft Windows s'affiche, appuyez sur la touche Maj et maintenez-la enfoncée jusqu'à ce que la boîte de dialogue Connexion Windows s'affiche. Remarque : vous pouvez appuyer sur la touche Maj lorsque l'écran de démarrage se trouve à environ la moitié du processus de démarrage de Windows.
3. Lorsque la boîte de dialogue Connexion Windows s'affiche, tapez vos informations de connexion au système.

Continuité de la sécurité du disque

Les sections suivantes décrivent comment travailler avec votre disque chiffré avec PGP WDE.

Obtention d'informations sur les disques ou les partitions

Pour afficher les informations sur les partitions ou disques en lecture seule dans l'écran avancé d'ouverture de session PGP BootGuard

1. Démarrez ou redémarrez le système comportant une partition ou un disque protégé à l'aide de PGP Whole Disk Encryption. Lors du démarrage, l'écran d'ouverture de session PGP BootGuard s'affiche.
2. Appuyez sur la flèche vers le bas de votre clavier. Dans le coin inférieur droit, **Avancé** est affiché en surbrillance.
3. Appuyez sur **Entrée**. L'écran avancé d'ouverture de session PGP BootGuard s'affiche.

   Il fournit les informations suivantes :

   - L'ensemble des disques ou des partitions sur le système, y compris l'état du chiffrement de ceux protégés à l'aide de PGP Whole Disk Encryption.
   - Le nom de l'ordinateur.

- L'ID de l'ordinateur.
- La partition ou le disque actuellement sélectionné, et si la fonctionnalité Contournement est ou non disponible pour cet élément. (La fonctionnalité Contournement peut être utilisée uniquement par les utilisateurs possédant des droits administrateur sur le système et si la stratégie de votre PGP Universal Server l'autorise.)

4 Pour revenir à l'écran d'ouverture de session PGP BootGuard, mettez **Retour** en surbrillance dans le coin inférieur droit de l'écran, puis appuyez sur **Entrée**.

Modification de la partition système

N'apportez pas de modifications à la partition système d'un disque de démarrage chiffré par PGP WDE. Il ne pourrait alors plus démarrer correctement. Si vous devez absolument apporter des modifications au partitionnement d'un disque chiffré, déchiffrez le disque avant de le modifier.

Utilisation de la fonctionnalité Contournement

Remarque : cette fonction est disponible uniquement pour les utilisateurs disposant de droits d'administration sur le système et si la stratégie de PGP Universal Server l'autorise.

La fonctionnalité Contournement vous permet d'ignorer l'étape d'authentification au démarrage. Si votre partition ou disque de démarrage n'est pas protégé à l'aide de PGP Whole Disk Encryption, mais qu'une autre partition ou un autre disque fixe sur votre système l'est, l'écran d'ouverture de session PGP BootGuard s'affiche au démarrage. La fonctionnalité Contournement vous permet d'ignorer l'étape d'authentification afin que la partition ou le disque puisse démarrer.

Attention : vous pouvez utiliser la fonctionnalité Contournement uniquement si votre partition ou disque n'est *pas* protégé à l'aide de PGP Whole Disk Encryption. Si votre partition ou disque de démarrage est protégé et que vous ne vous authentifiez pas, le système d'exploitation ne se chargera pas et l'ordinateur ne démarrera pas.

Pour utiliser la fonctionnalité Contournement

1 Démarrez ou redémarrez le système comportant la partition ou le disque protégé à l'aide de PGP Whole Disk Encryption. Lors du démarrage, l'écran d'ouverture de session PGP BootGuard s'affiche.

2 Appuyez sur la flèche vers le bas de votre clavier. Dans le coin inférieur droit, Avancé est affiché en surbrillance.

3 Appuyez sur **Entrée**. L'écran avancé d'ouverture de session PGP BootGuard s'affiche.

4 Ré-appuyez sur la flèche vers le bas de votre clavier. Dans le coin inférieur droit, **Contournement** est affiché en surbrillance.

5 Appuyez sur **Entrée**. L'écran avancé d'ouverture de session PGP BootGuard disparaît, puis le système démarre normalement.

Ajout d'autres utilisateurs à une partition ou un disque chiffré

L'utilisateur qui crée une partition ou un disque chiffré peut le mettre à la disposition d'autres utilisateurs. Ces utilisateurs supplémentaires peuvent accéder à la partition ou au disque en utilisant leur propre phrase secrète, clé privée ou jeton (y compris cartes individuelles de vérification d'identité). Il est possible d'associer jusqu'à 120 utilisateurs à chaque disque chiffré.

Pour déterminer le type de l'utilisateur associé au disque chiffré, placez le curseur sur son nom dans la liste Accès de l'utilisateur. Une « info-bulle » apparaît, indiquant le type d'utilisateur. Une icône de clé de jeton permet d'identifier un utilisateur de jeton et le domaine/nom d'utilisateur Windows est affiché pour un utilisateur SSO.

Attention : le fait que plusieurs utilisateurs puissent accéder à une partition ou un disque protégé par PGP Whole Disk Encryption sert de voie de secours si une personne oublie sa phrase secrète ou perd son jeton d'authentification. Les utilisateurs ainsi configurés peuvent s'authentifier dans l'écran d'ouverture de session PGP Whole Disk Encryption afin de déverrouiller les partitions ou disques protégés sur ce système.

Pour ajouter des utilisateurs supplémentaires à une partition ou un disque protégé par PGP Whole Disk Encryption

1 Cliquez sur le panneau de contrôle PGP Disk dans le volet gauche de l'écran principal de PGP Desktop.

2 Dans la liste des disques située en haut de la zone de travail de PGP Disk, sélectionnez la partition ou le disque chiffré auquel vous voulez ajouter un autre utilisateur.

3 Cliquez sur **Nouvel utilisateur de phrase secrète**. La boîte de dialogue de sélection du type d'utilisateur s'affiche.

4 Suivez les instructions indiquées à l'étape Accès de l'utilisateur dans la section *Chiffrement du disque* (à la page 171).

Remarque : le chiffrement par clé publique est la méthode de protection qui offre le niveau de sécurité maximal lors de l'ajout d'autres utilisateurs aux partitions ou disques chiffrés à l'aide de PGP Whole Disk Encryption, pour les raisons ci-après : (1) Il n'est pas nécessaire de révéler les phrases secrètes aux nouveaux utilisateurs, le risque qu'elles soient interceptées ou entendues étant ainsi minimal. (2) Il n'est pas nécessaire que les utilisateurs supplémentaires mémorisent une autre phrase secrète. (3) Il est plus facile de gérer des listes d'utilisateurs si chacun utilise sa propre clé privée pour accéder au disque. Si vous protégez une partition ou un disque de démarrage à l'aide de PGP Whole Disk Encryption, la clé publique doit être sur un jeton.

Suppression d'utilisateurs de la partition ou du disque chiffré.

Il se peut qu'un jour vous souhaitiez interdire l'accès à une partition ou à un disque chiffré à un utilisateur.

Pour supprimer un utilisateur d'une partition ou d'un disque chiffré

1. Dans l'écran Chiffrer le disque complet (Partition), sélectionnez la partition ou le disque approprié protégé par PGP Whole Disk Encryption.
2. Dans la liste **Accès de l'utilisateur**, sélectionnez le nom de l'utilisateur à supprimer.
3. Cliquez sur **Supprimer l'utilisateur**. La boîte de dialogue Phrase secrète s'affiche, vous invitant à vous authentifier.
4. Saisissez une phrase secrète valide, puis cliquez sur OK. L'autre utilisateur est supprimé.

Modification des phrases secrètes des utilisateurs

Si vous utilisez l'authentification unique, modifiez votre mot de passe comme le décrit la section *Modification de votre phrase secrète en cas d'utilisation de la fonctionnalité d'authentification unique* (à la page 189).

Pour modifier les phrases secrètes des utilisateurs sur une partition ou un disque chiffré

1. Dans l'écran Chiffrer le disque complet (partition), sélectionnez la partition ou le disque approprié protégé par PGP Whole Disk Encryption.
2. Dans la liste **Accès de l'utilisateur**, sélectionnez le nom de l'utilisateur dont vous souhaitez modifier la phrase secrète.
3. Cliquez sur **Modifier la phrase secrète**. Vous êtes invité à saisir la phrase secrète actuelle.

4 Saisissez la phrase secrète appropriée, puis cliquez sur **OK**. La boîte de dialogue Modifier phrase secrète utilisateur s'affiche.

5 Tapez une nouvelle phrase secrète.

6 Dans le champ Confirmer la phrase secrète, indiquez à nouveau la phrase secrète, puis cliquez sur **OK**. La phrase secrète est modifiée.

L'indicateur de qualité de la phrase secrète donne une information de base sur le niveau de confidentialité de la phrase secrète créée. Pour plus d'informations, reportez-vous à la section *Indicateur de qualité de la phrase secrète* (à la page 336).

Normalement, afin de renforcer le niveau de sécurité, les caractères que vous saisissez pour une phrase secrète ne sont pas visibles à l'écran. Pour les afficher lors de la saisie, cochez la case **Afficher les frappes.**

Modification de votre phrase secrète en cas d'utilisation de la fonctionnalité d'authentification unique

Si vous optez pour la fonctionnalité d'authentification unique PGP Whole Disk Encryption, nous vous recommandons de modifier votre phrase secrète à l'aide de la fonctionnalité **Modifier le mot de passe** de la boîte de dialogue Sécurité de Windows.

Remarque : la boîte de dialogue Sécurité de Windows est accessible à l'aide de la combinaison de touches **CTRL+ALT+SUPPR**.

Pour modifier votre phrase secrète tout en utilisant la fonctionnalité d'authentification unique

1 Appuyez sur Ctrl+Alt+Suppr. La boîte de dialogue Sécurité de Windows s'affiche.

2 Saisissez votre ancienne phrase secrète.

3 Entrez et confirmez la nouvelle.

4 Cliquez sur **OK**. Votre mot de passe Windows et la phrase secrète PGP Whole Disk Encryption sont modifiés ensemble. Utilisez la nouvelle phrase secrète lors de votre prochaine tentative d'ouverture de session.

Attention : si vous modifiez votre phrase secrète d'une manière autre que celle décrite ici, votre prochaine tentative d'ouverture de session sur l'écran PGP BootGuard échouera. Vous devrez alors indiquer votre ancienne phrase secrète. L'ouverture de session réussie sur l'écran PGP BootGuard à l'aide de votre ancienne phrase secrète ouvrira ensuite l'écran de saisie du nom d'utilisateur/mot de passe d'ouverture de session Windows. Puis, vous devrez ouvrir une session à l'aide de l'écran d'ouverture de session Windows, stade auquel la fonctionnalité PGP Whole Disk Encryption se synchronisera avec la nouvelle phrase secrète.

Utilisateurs locaux et fonctionnalité d'authentification unique PGP Whole Disk Encryption

Si un ordinateur n'est pas membre d'un domaine, PGP Whole Disk Encryption s'assure automatiquement de l'obligation pour les utilisateurs d'ouvrir une session en utilisant la combinaison de touches Ctrl+Alt+Suppr. Pour ce faire, PGP Whole Disk Encryption désactive certaines fonctionnalités d'accès utilisateur Windows, dont les options **Utiliser l'écran d'accueil** et Ctrl+Alt+Suppr après l'ajout d'un utilisateur avec authentification unique.

Ces fonctionnalités sont automatiquement désactivées lorsqu'un ordinateur est membre d'un domaine.

Nouveau chiffrement d'une partition ou d'un disque

Envisagez le nouveau chiffrement d'une partition ou d'un disque protégé si vous suspectez qu'une phrase secrète ou qu'un jeton d'authentification a été compromis, ou si des utilisateurs qui avaient précédemment accès ont été supprimés.

Pour chiffrer à nouveau une partition ou un disque, la fonctionnalité PGP Whole Disk Encryption utilise le même algorithme de chiffrement (AES256), mais une clé de chiffrement sous-jacente différente. Le résultat est identique à un déchiffrement suivi d'un nouveau chiffrement, mais est beaucoup plus rapide.

Remarque : le nouveau chiffrement s'applique à toutes les partitions déjà chiffrées. La sélection d'une partition à chiffrer implique que toutes les partitions sur le même disque qui sont déjà chiffrées le soient à nouveau une par une.

Pour chiffrer à nouveau une partition ou un disque

1. Sélectionnez la partition ou le disque chiffré approprié.
2. Sélectionnez **Disque > Chiffrer à nouveau**. Vous êtes invité à vous authentifier.
3. Saisissez la phrase secrète appropriée, puis cliquez sur **OK**. Le processus de nouveau chiffrement commence.

Vous avez oublié votre phrase secrète

Si vous avez oublié votre phrase secrète, et à condition que la configuration de votre système le prévoie, vous pouvez contourner PGP BootGuard en répondant correctement à trois des cinq questions de sécurité que vous avez créées. Ce mécanisme s'apparente à la récupération de clé effectuée si vous perdez votre clé ou oubliez la phrase secrète qui lui est associée.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé l'option d'auto-récupération en local. Il peut en outre avoir précisé que ce mécanisme doit être configuré au moment de l'inscription. Dans ce cas, vous devez saisir les questions de sécurité lors de l'installation de PGP Desktop.

Pour créer vos questions de sécurité

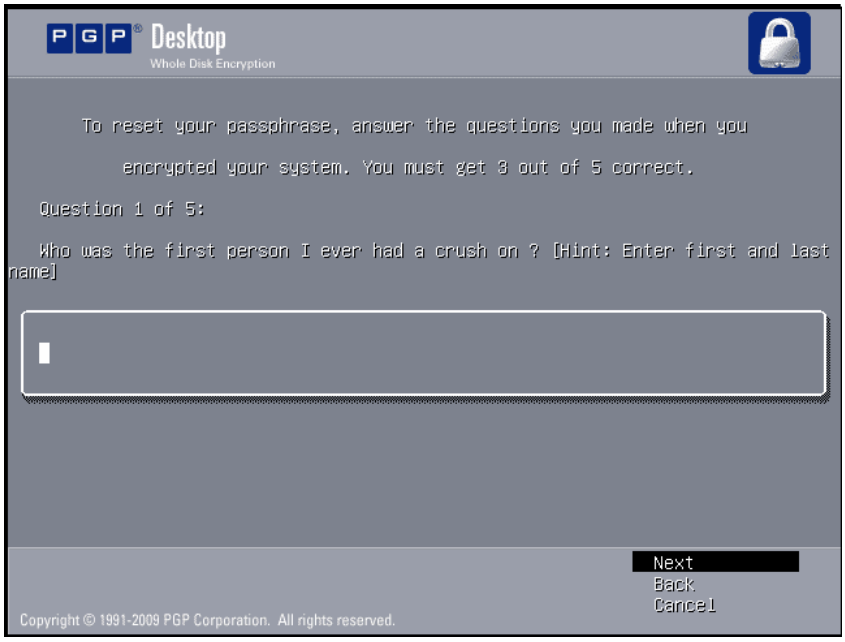
1. Chiffrez votre lecteur interne à l'aide de PGP Desktop. Vous pouvez avoir recours soit à un utilisateur de phrase secrète, soit à un utilisateur SSO Windows.
2. Cliquez avec le bouton droit sur le nom de l'utilisateur dans PGP Desktop et sélectionnez **Ajouter des questions de sécurité**.

   Remarque : vous ne pouvez pas créer de questions de sécurité pour l'administrateur WDE ou la clé de déchiffrement supplémentaire (ADK).
3. Créez les cinq questions de sécurité et les réponses correspondantes. La mention **ARL**, accompagnée d'une info-bulle, s'affiche alors à droite du nom de l'utilisateur et indique que l'auto-récupération en local a été configurée pour ce dernier.

Pour récupérer votre phrase secrète dans PGP BootGuard

1. Sur l'écran PGP BootGuard, sélectionnez **J'ai oublié ma phrase secrète** à l'aide des touches fléchées, puis appuyez sur Entrée.

2 Répondez à la première question de sécurité affichée. Tapez votre réponse et appuyez sur Entrée.



3 Continuez à répondre aux questions. Vous devez répondre correctement à trois des cinq questions.

4 Lorsque vous avez répondu correctement à au moins trois questions, le système d'exploitation Windows est lancé. Lorsque la boîte de dialogue Ouverture de session Windows apparaît, saisissez votre nom de connexion et votre mot de passe Windows.

Une fois que Windows est opérationnel, la boîte de dialogue PGP Disk - Modifier phrase secrète utilisateur apparaît.

5 Saisissez une nouvelle phrase secrète pour l'utilisateur, confirmez-la, puis cliquez sur **OK**. La phrase secrète est créée pour l'utilisateur.

L'indicateur de qualité de la phrase secrète donne une information de base sur le niveau de confidentialité de la phrase secrète créée. Pour plus d'informations, reportez-vous à la section *Indicateur de qualité de la phrase secrète* (à la page 336).

Normalement, afin de renforcer le niveau de sécurité, les caractères que vous saisissez pour une phrase secrète ne sont pas visibles à l'écran. Pour les afficher lors de la saisie, cochez la case **Afficher les frappes**.

Les mêmes questions de sécurité sont affichées si vous oubliez de nouveau votre phrase secrète. Pour les modifier, cliquez avec le bouton droit sur le nom de l'utilisateur et sélectionnez **Créer des questions de sécurité**.

Sauvegarde et restauration

Alors que la plupart des programmes de sauvegarde modernes parviennent à sauvegarder les données sur un disque chiffré par PGP WDE sans problème, d'autres peuvent rencontrer des difficultés. Ces derniers programmes échouent lorsqu'ils rencontrent le fichier PGPWDE01, utilisé par PGP WDE. La solution consiste à configurer ces programmes de façon à ce qu'ils excluent PGPWDE01 de la sauvegarde (la plupart des programmes de sauvegarde permettent d'exclure des fichiers individuels). Dès que vos sauvegardes fonctionnent à nouveau avec ces programmes, pensez à les tester afin de vous assurer que tout va bien.

Utilisation d'un logiciel de sauvegarde automatique sur un disque chiffré par PGP WDE

Vous pouvez sauvegarder automatiquement la partition ou le disque une fois que celle-ci ou celui-ci est protégé à l'aide de PGP WDE. Veillez à sauvegarder d'abord votre système avant de le chiffrer à l'aide de PGP WDE.

Remarque importante : les fichiers que le logiciel sauvegarde sont auparavant déchiffrés. Pour sauvegarder des données chiffrées, utilisez des dossiers protégés PGP Virtual Disk ou PGP NetShare.

Désinstallation de PGP Desktop des partitions ou disques chiffrés

Si des partitions ou disques sur votre système sont protégés par PGP Whole Disk Encryption, ils deviendront inaccessibles lorsque PGP Desktop sera désinstallé. Pour cette raison, une fonctionnalité de sécurité vous empêche de désinstaller PGP Desktop si votre système comporte des partitions ou disques de ce type. Dans ce cas, un message d'erreur s'affiche expliquant que le processus de désinstallation est arrêté afin de protéger la partition ou le disque chiffré.

Pour désinstaller PGP Desktop, déchiffrez d'abord les partitions ou disques sur votre système qui sont protégés à l'aide de PGP Whole Disk Encryption.

Utilisation de disques amovibles

Cette section explique comment utiliser des disques amovibles. Si vous utilisez PGP Whole Disk Encryption dans un environnement géré par un PGP Universal Server, votre stratégie de sécurité peut exiger que les disques amovibles soient chiffrés. Elle peut également exiger que ces disques soient montés en tant que disques en lecture seule, mais une option vous est proposée pour que vous chiffriez le disque.

Attention : utilisez toujours l'option **Retirer le périphérique en toute sécurité** de Microsoft Windows pour arrêter les périphériques USB liés avant de les retirer.

Chiffrement des disques amovibles

Si vous utilisez PGP Whole Disk Encryption dans un environnement géré par un PGP Universal Server, votre stratégie de sécurité peut exiger que les disques amovibles soient chiffrés. Lorsque vous insérez le disque amovible, la boîte de dialogue PGP Desktop - Périphérique de stockage connecté s'affiche.

Effectuez l'une des opérations suivantes :

- S'il s'agit d'un lecteur externe, tel qu'un disque USB Flash ou un disque dur externe, cliquez sur **Chiffrer**. Le périphérique est automatiquement chiffré avec votre clé. Remarque : si votre disque de démarrage est chiffré avec les clés d'autres utilisateurs, ceux-ci sont ajoutés en tant qu'utilisateurs pour votre disque amovible. Si votre clé ou les clés d'autres utilisateurs sont introuvables, vous êtes invité à créer un utilisateur de phrase secrète.

  Remarque : si votre administrateur PGP Universal Server a précisé que tous les disques amovibles devaient être chiffrés automatiquement et que votre disque de démarrage ne le soit pas, la première paire de clés du trousseau de l'utilisateur servira à chiffrer le périphérique.

  Selon la taille du disque, l'exécution du processus de chiffrement peut prendre un certain temps. Vous pouvez continuer à utiliser le disque amovible pendant le chiffrement.

  Avertissement : assurez-vous que le processus de chiffrement est terminé avant de retirer le disque.

- Si vous ne voulez pas chiffrer le périphérique, cliquez sur **Verrouiller**. Le périphérique est verrouillé et reste en lecture seule. Si vous tentez de modifier ou de supprimer des fichiers du périphérique, un message d'erreur Windows apparaît.

  Si le disque amovible est un périphérique musical ou un appareil photo numérique, cliquez sur **Verrouiller**. Ces types de périphériques ne fonctionnent pas si le contenu est chiffré. Si vous chiffrez accidentellement un périphérique musical ou un appareil photo numérique, vous devez le déchiffrer. Selon la stratégie de sécurité de votre entreprise, il peut s'avérer nécessaire de contacter votre service informatique ou administrateur PGP afin d'obtenir de l'aide concernant le déchiffrement de ce périphérique.

Si votre stratégie de sécurité exige que tous les disques amovibles soient chiffrés et que le PGP Universal Server ne soit pas disponible (par exemple, si vous êtes en avion et non connecté au réseau de votre entreprise), le périphérique amovible ne peut pas être chiffré. Par conséquent, il sera « verrouillé » et en lecture seule. La prochaine fois que vous vous connecterez au PGP Universal Server, vous pourrez chiffrer le contenu du disque (si cela n'a pas encore été fait).

Remarque : si votre administrateur PGP a précisé que tous les disques amovibles devaient être chiffrés, l'option **Quitter les services PGP** n'est plus disponible dans le menu de la zone de notification PGP.

Utilisation de disques verrouillés (lecture seule) en lecture seule

Si vous utilisez PGP Whole Disk Encryption dans un environnement géré par un PGP Universal Server, votre stratégie de sécurité peut exiger que les disques amovibles soient montés sous la forme de périphériques en lecture seule. Lorsque vous insérez le disque amovible, la boîte de dialogue PGP Desktop - Périphérique de stockage connecté s'affiche.

Le disque amovible est verrouillé et vous ne pouvez pas y ajouter des données tant que vous ne le chiffrez pas. Si vous décidez de le chiffrer, vous pouvez continuer à l'utiliser de façon normale.

Effectuez l'une des opérations ci-dessous :

- Si le disque amovible est un lecteur externe, tel qu'un disque flash USB ou un disque dur externe, et que vous voulez pouvoir écrire dessus, cliquez sur **Chiffrer**. Le périphérique est automatiquement chiffré avec votre clé. Remarque : si votre disque de démarrage est chiffré avec les clés d'autres utilisateurs, elles seront ajoutées en tant qu'utilisateurs à votre disque amovible. Si votre clé ou les clés d'autres utilisateurs sont introuvables, vous êtes invité à créer un utilisateur de phrase secrète.

  Selon la taille du disque, l'exécution du processus de chiffrement peut prendre un certain temps. Vous pouvez continuer à utiliser le disque amovible pendant le chiffrement.

  Avertissement : assurez-vous que le processus de chiffrement est terminé avant de retirer le disque.

- Si vous ne voulez pas chiffrer le périphérique, cliquez sur **Verrouiller**. Le périphérique est verrouillé et reste en lecture seule. Si vous tentez de modifier ou de supprimer des fichiers du périphérique, un message d'erreur Windows apparaît.

Si le disque amovible est un périphérique musical ou un appareil photo numérique, cliquez sur **Verrouiller**. Ces types de périphériques ne fonctionnent pas si le contenu est chiffré. Si vous chiffrez accidentellement un périphérique musical ou un appareil photo numérique, vous devez le déchiffrer. Selon la stratégie de sécurité de votre entreprise, il peut s'avérer nécessaire de contacter votre service informatique ou administrateur PGP afin d'obtenir de l'aide concernant le déchiffrement de ce périphérique.

Déplacement des disques amovibles sur d'autres systèmes

Si vous utilisez PGP Whole Disk Encryption pour protéger un disque amovible (un disque Flash USB, par exemple), vous pouvez déplacer celui-ci sur un autre système Windows ou Mac OS X et accéder aux fichiers chiffrés du disque sur l'autre système. Pour accéder aux disques amovibles créés à l'aide de PGP WDE sur Linux, utilisez PGP Desktop version 10.0 ou ultérieure.

Vous devrez être en mesure de vous authentifier pour accéder au contenu du disque.

Remarque : envisagez de définir une licence pour PGP Desktop lors du déplacement d'un disque amovible chiffré. Pour protéger un disque à l'aide de la fonctionnalité PGP Whole Disk Encryption, vous devez disposer de la licence PGP Desktop appropriée. Cependant, si vous avez protégé un disque amovible à l'aide de PGP Whole Disk Encryption, vous pourrez l'utiliser sur un autre ordinateur doté de PGP Desktop version 9.5.2 ou ultérieure, et ce même si l'autre système ne dispose pas de licence PGP Desktop prenant en charge Whole Disk Encryption.

Reformatage d'un disque amovible chiffré

Si vous avez chiffré un disque amovible, puis utilisé l'utilitaire Windows Disk Management pour le reformater, la prochaine fois que vous l'insérerez, vous serez invité à saisir votre phrase secrète.

Pour annuler cette exigence, procédez comme suit :

1. Démarrez une invite de commande (**Démarrer > Exécuter**, puis tapez `cmd`) et accédez à `C:\Program Files\PGP Corporation\PGP Desktop`.
2. Saisissez la commande suivante :

   ```
   pgpwde --fixmbr --disk 1
   ```

   Si votre système comporte plusieurs disques chiffrés, il se peut que vous ayez d'abord à exécuter la commande `pgpwde --enum`. Cette commande répertorie vos disques chiffrés. Si la commande indique que votre disque USB n'est pas le disque « 1 », utilisez son numéro à la place (par exemple, si votre disque USB est le disque « 2 », saisissez la commande de suppression du chiffrement `pgpwde --fixmbr --disk 2`).

Vous ne serez plus invité à saisir la phrase secrète lorsque vous insérerez le disque.

Utilisation de PGP WDE dans un environnement géré par un PGP Universal Server

Dans un environnement géré par un PGP Universal Server, les utilisateurs de PGP Desktop peuvent gérer la fonctionnalité PGP Whole Disk Encryption. Les administrateurs peuvent déployer les programmes d'installation de PGP Desktop dans toute l'entreprise.

Administration de PGP Whole Disk Encryption

L'administrateur PGP peut contrôler :

- **si la fonctionnalité PGP Whole Disk Encryption est accessible aux utilisateurs**. Si vous êtes dans un environnement géré par un PGP Universal Server et que la fonctionnalité PGP Whole Disk Encryption n'est *pas* disponible, contactez votre administrateur PGP pour vérifier si la fonctionnalité a été désactivée par la stratégie.

  Cette fonctionnalité requiert également une licence appropriée de PGP Corporation. Si la fonctionnalité est désactivée, et ce même si elle est activée par la stratégie, contactez votre administrateur PGP afin de vérifier que vous disposez d'une licence appropriée.

- **si vous pouvez ou non récupérer les partitions ou disques qui sont protégés à l'aide de PGP Whole Disk Encryption**. Si vous oubliez la phrase secrète d'une partition ou d'un disque chiffré à l'aide de PGP Whole Disk Encryption, ou si vous perdez le jeton d'authentification, la partition ou le disque ne sera pas accessible. Cependant, si vous utilisez la fonctionnalité PGP Whole Disk Encryption dans un environnement géré par un PGP Universal Server, contactez votre administrateur PGP pour vérifier si la récupération de la partition ou du disque est possible.

- **si votre disque de démarrage doit ou non être chiffré à l'aide de PGP Whole Disk Encryption lorsque vous installez PGP Desktop**.

  Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, contactez votre administrateur PGP pour plus d'informations.

- **si votre ordinateur utilise ou non la fonctionnalité d'authentification automatique (SSO) PGP Whole Disk Encryption**.

  Pour plus d'informations, reportez-vous à la section *Utilisation de l'authentification unique PGP WDE* (cf. "Utilisation de l'authentification unique de PGP WDE" à la page 182).

- **les modes que vous pouvez utiliser avec la fonctionnalité PGP Whole Disk Encryption**.
- **s'il peut ou non utiliser une clé administrateur (avec carte à puce) pour accéder à votre partition ou disque chiffré.**

Pour plus d'informations sur les modes de chiffrement, reportez-vous à la section *Définition de la méthode d'authentification du disque* (à la page 160).

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, il peut s'avérer nécessaire après son installation de chiffrer votre partition ou disque de démarrage à l'aide de la fonctionnalité PGP WDE. Inversement, votre administrateur PGP peut désactiver la fonctionnalité PGP WDE.

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, vous pouvez être invité à chiffrer un disque amovible lors de son insertion. Pour plus d'informations, reportez-vous à la section *Chiffrement des disques amovibles* (à la page 194).

En cas de modification de votre stratégie, en particulier de la désactivation de la fonctionnalité de chiffrement d'un disque, sachez que vous avez toujours la possibilité d'utiliser des lecteurs qui sont déjà des disques complets chiffrés. Toutefois, vous ne pourrez pas chiffrer d'autres lecteurs, chiffrer à nouveau des lecteurs chiffrés existants ou ajouter de nouveaux utilisateurs.

Pour plus d'informations, reportez-vous à la section *Utilisation de PGP Desktop avec un PGP Universal Server* (à la page 341).

Création d'un jeton de récupération

Si vous travaillez dans un environnement géré par un PGP Universal Server et que vous soyez autorisé à créer des jetons de récupération pour le disque entier, PGP Desktop génère un jeton de récupération chaque fois que vous chiffrez un disque, une partition (sur des systèmes Windows) ou un disque amovible à l'aide de PGP Whole Disk Encryption. Le jeton de récupération permet d'accéder au disque ou à la partition (sur des systèmes Windows) en cas de perte de la phrase secrète ou du jeton d'authentification (systèmes Windows).

Si, en revanche, vous ne disposez pas de ces droits, ou si vous ne travaillez pas dans un environnement géré par un PGP Universal Server avec une installation prédéfinie de PGP Desktop, vous ne pouvez pas utiliser les jetons de récupération du disque entier.

Ce jeton de récupération est automatiquement envoyé à la sécurité de gestion du PGP Universal Server du disque ou de la partition (sur des systèmes Windows) que PGP Whole Disk Encryption protège.

Si, dans un environnement géré par un PGP Universal Server, vous perdez la phrase secrète ou le jeton d'authentification utilisé pour protéger un disque ou une partition (sur des systèmes Windows) à l'aide de PGP Whole Disk Encryption, contactez votre administrateur PGP afin d'utiliser le jeton de récupération.

Le jeton de récupération est à usage unique et permet d'accéder à un disque ou une partition (sur des systèmes Windows) dont le chiffrement a été effectué à l'aide de PGP Whole Disk Encryption. Lorsqu'un jeton de récupération est utilisé, un nouveau jeton est généré automatiquement et envoyé au PGP Universal Server. L'utilisateur de PGP Desktop a la possibilité de créer un utilisateur ou de conserver le ou les utilisateurs existants sur le disque ou la partition.

Le jeton de récupération permet uniquement d'accéder à un disque chiffré ou une partition protégée (sur des systèmes Windows), et non de chiffrer ou déchiffrer des données.

Attention : Vous devrez effectuer un nouveau chiffrement des disques ou des partitions (sur des systèmes Windows) protégés par PGP Whole Disk Encryption si la sécurité des données est compromise, en raison de la divulgation d'une phrase secrète ou la perte du jeton d'authentification (systèmes Windows). Le nouveau processus de chiffrement a recours au même algorithme, mais à une clé de chiffrement sous-jacente différente. Le résultat est identique à un déchiffrement suivi d'un nouveau chiffrement, mais l'opération est beaucoup plus rapide.

Utilisation d'un jeton de récupération

Une fois que vous avez reçu le jeton de récupération de votre administrateur PGP Universal, suivez la procédure ci-après pour déverrouiller le disque.

Lorsque vous saisissez un jeton de récupération, il n'est pas nécessaire de respecter la casse (tout en majuscules) ni les tirets du jeton reçu de votre administrateur PGP Universal. Si vous le souhaitez, vous pouvez le saisir tout en minuscules sans les tirets.

Pour utiliser un jeton de récupération sur un disque de démarrage

- Sur l'écran PGP BootGuard, saisissez le jeton de récupération dans le champ de la phrase secrète.

Pour utiliser un jeton de récupération sur un disque amovible

- Insérez le disque et saisissez le jeton de récupération lorsque vous êtes invité à saisir la phrase secrète.

Récupération de données à partir d'un lecteur chiffré

Bien que ce cas de figure soit rare, il se peut que vous ayez un jour à récupérer des données à partir d'un lecteur chiffré endommagé ou altéré. Vous pouvez aussi découvrir que vous ne disposez pas des informations d'ouverture de session requises pour accéder à un lecteur, par exemple le lecteur chiffré d'un ancien employé. Dans ces cas, plusieurs possibilités s'offrent à vous :

1. Utilisez un disque de récupération. Si un disque de récupération a été créé avant le chiffrement du disque ou de la partition, vous pouvez l'utiliser pour déchiffrer le disque. Pour plus d'informations, reportez-vous à la section *Création et utilisation de disques de récupération* (à la page 200).
2. Utilisez un autre système pour déchiffrer le lecteur. Pour plus d'informations, reportez-vous à la section *Déchiffrement d'un disque chiffré par PGP WDE* (à la page 202).
3. Utilisez le jeton de récupération de disque complet (Whole Disk Recovery Token, WDRT). Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, le jeton de récupération est automatiquement créé lors du chiffrement du disque. Pour plus d'informations, reportez-vous à la section *Utilisation d'un jeton de récupération* (à la page 199).

Création et utilisation de disques de récupération

Bien qu'il soit très peu probable qu'un enregistrement d'amorçage principal soit endommagé sur un disque ou une partition de démarrage bénéficiant d'une protection via PGP Whole Disk Encryption, cela reste une éventualité. Cette situation peut empêcher le démarrage de votre système.

Anticipez cette éventualité : créez un CD ou une disquette de récupération, ou les deux, **avant** de chiffrer un disque ou une partition de démarrage à l'aide de PGP Whole Disk Encryption.

Attention : les disques de récupération fonctionnent uniquement avec la version de PGP Desktop utilisée pour les créer. Par exemple, si vous tentez d'utiliser un disque de récupération 9.0.x pour déchiffrer un disque protégé à l'aide du logiciel PGP WDE 9.5, le disque PGP WDE 9.5 sera inutilisable.

Cette section décrit les procédures de création d'un CD et d'une disquette de récupération, ainsi que l'utilisation de ces supports.

Pour créer un CD de récupération

1. Vérifiez que PGP Desktop pour Windows et Roxio Easy Media Creator ou Roxio Easy CD Creator (ou tout autre logiciel permettant de créer un CD à partir d'une image ISO) sont installés sur votre système.

2. Ouvrez Roxio Easy Media Creator ou Roxio Easy CD Creator et créez un projet de disque de données.
3. Sélectionnez **Fichier > Graver un fichier image disque**. L'écran Graver un fichier image disque s'affiche.
4. Sélectionnez **Fichiers de type > Fichiers image disque (ISO)**.
5. Accédez au répertoire PGP. Le répertoire par défaut est `C:\Program Files\PGP Corporation\PGP Desktop\`.
6. Sélectionnez `bootg.iso` et cliquez sur **Ouvrir**. L'écran Configuration de la gravure s'affiche.
7. Insérez un CD enregistrable vierge dans le lecteur de CD.
8. Dans l'écran Configuration de la gravure, cliquez sur **Commencer la gravure**. L'écran Progression de la gravure d'un fichier image disque s'affiche pendant la gravure du fichier ISO sur le CD.
9. Lorsque la gravure est terminée, cliquez sur **OK**. Le CD de récupération PGP Whole Disk Encryption est prêt.
10. Retirez-le du lecteur et étiquetez-le.

Pour créer une disquette de récupération

1. Assurez-vous que PGP Desktop pour Windows et une application permettant de créer une disquette de récupération (telle que MagicISO) sont installés.
2. Insérez une disquette vierge dans le lecteur.
3. Ouvrez MagicISO.
4. Sélectionnez **Outils > Écrire une image disquette**. La boîte de dialogue Ouvrir s'affiche.
5. Accédez au répertoire PGP. Le répertoire par défaut est `C:\Program Files\PGP Corporation\PGP Desktop\`.
6. Sélectionnez `Bootg.img` et cliquez sur **Ouvrir**. Le fichier est écrit sur la disquette.
7. Retirez la disquette de récupération du lecteur et étiquetez-la.
8. Quittez MagicISO.

Pour utiliser un disque ou une disquette de récupération

Attention : après avoir lancé le déchiffrement d'un disque ou d'une partition à l'aide d'un CD ou d'une disquette de récupération, n'interrompez pas le processus. En fonction de la taille du disque déchiffré, celui-ci peut durer un certain temps. Pour accélérer le déchiffrement du disque, utilisez un autre système disposant de la même version de PGP Desktop. Pour plus d'informations, reportez-vous à la section *Déchiffrement d'un disque chiffré par PGP WDE* (à la page 202).

1. Si l'écran d'ouverture de session PGP Whole Disk Recovery n'apparaît pas lorsque vous redémarrez votre système ou lorsque vous êtes invité à insérer un disque de récupération PGP Whole Disk Encryption, insérez le CD ou la disquette dans le lecteur correspondant.
2. Redémarrez le système. L'écran d'ouverture de session PGP Whole Disk Encryption s'affiche à partir du disque de récupération.
3. Saisissez la phrase secrète du disque ou de la partition de démarrage définie lors du chiffrement avec PGP Whole Disk Encryption. Vous pouvez alors :
   - appuyer sur **Entrée** pour tenter de démarrer le système ;
   - taper `D` pour déchiffrer le disque.

Déchiffrement d'un disque chiffré par PGP WDE

Si vous devez procéder à des opérations de récupération sur un disque protégé à l'aide PGP Whole Disk Encryption, PGP Corporation vous recommande de commencer par déchiffrer le disque. Pour déchiffrer un disque, suivez l'une des procédures suivantes :

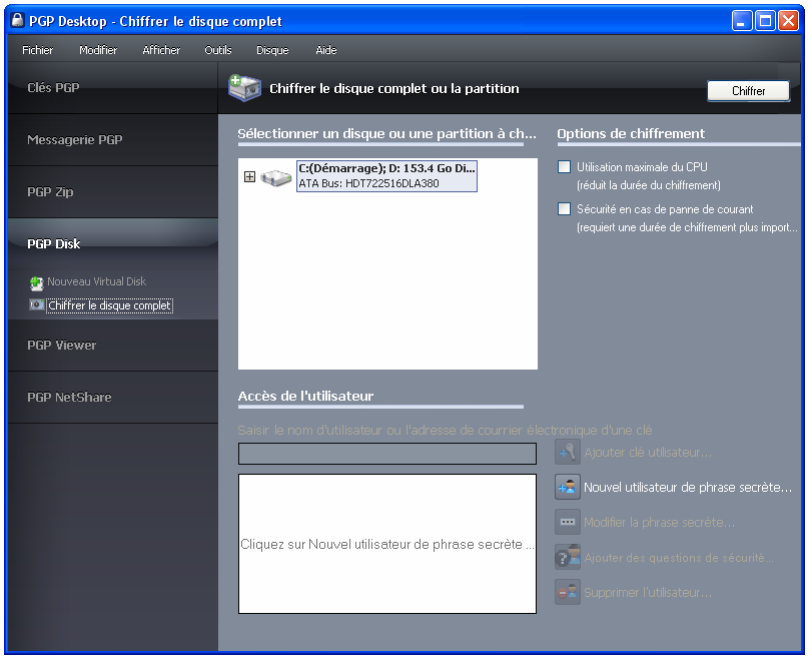
- Dans PGP Desktop, cliquez sur **Disque > Déchiffrer** (la procédure suivante détaille l'utilisation de cette option pour le déchiffrement d'un disque).
- Utilisez le disque de récupération PGP WDE préparé (reportez-vous à la section *Création de disques de récupération* (cf. "Création et utilisation de disques de récupération" à la page 200) pour plus d'informations sur la création d'un disque de récupération).
- Connectez le disque dur au second système à l'aide d'un câble USB et déchiffrez-le avec PGP Desktop installé sur ce système.

Une fois le disque déchiffré, vous pouvez effectuer la récupération.

Utilisation de PGP Desktop pour déchiffrer un disque

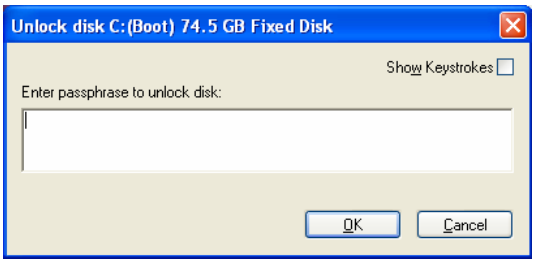
1. Ouvrez PGP Desktop et cliquez sur la boîte de contrôle PGP Disk. La boîte de contrôle PGP Disk est alors mise en surbrillance.

2 Cliquez sur **Chiffrer le disque complet ou la partition**. La zone de travail Chiffrer le disque complet (partition) affiche une liste des disques de votre système pouvant être protégés par PGP Whole Disk Encryption : disques, partitions de disque, supports amovibles, etc.

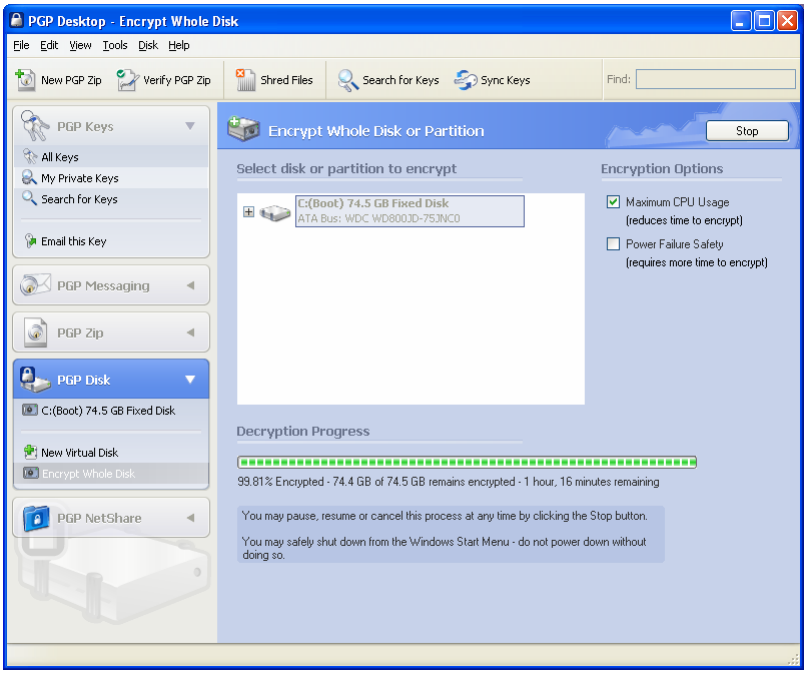


3 Dans la section supérieure **Sélectionner un disque ou une partition à chiffrer** de la zone de travail **Chiffrer le disque complet (partition)**, cliquez sur le disque ou la partition à déchiffrer.

4 Sélectionnez **Disque** > **Déchiffrer** ou cliquez sur **Déchiffrer**. La boîte de dialogue Déverrouiller le disque s'affiche.



5 Saisissez la phrase secrète pour déverrouiller le disque. La Progression du déchiffrement s'affiche dans la fenêtre PGP Desktop.



La durée nécessaire pour le déchiffrement est indiquée dans la fenêtre PGP Desktop. Pour interrompre ou annuler le processus de déchiffrement, cliquez sur **Arrêter**. Si nécessaire, arrêtez l'ordinateur via le menu **Démarrer** > **Arrêter**. *N'arrêtez pas le système en appuyant sur le bouton marche/arrêt.*

Utilisation d'un autre système pour déchiffrer un disque chiffré par PGP WDE

1 Retirez le disque dur à déchiffrer de l'ordinateur et placez-le dans un boîtier de disque.

2 À l'aide d'un câble USB, reliez le boîtier à un ordinateur sur lequel PGP Desktop est installé.

3 À l'invite, saisissez la phrase secrète pour déchiffrer le disque placé dans le boîtier.

Précautions spéciales de sécurité prises par PGP Desktop

PGP Desktop offre des fonctionnalités permettant d'éviter des problèmes de sécurité liés à la fonctionnalité PGP Whole Disk Encryption. Ces précautions s'appliquent également aux volumes PGP Virtual Disk.

Effacement de la phrase secrète

Lorsque vous indiquez une phrase secrète, PGP Desktop l'utilise seulement un très court instant, puis l'efface de la mémoire. L'application ne fait en principe pas de copies de cette phrase. En conséquence, votre phrase secrète demeure généralement en mémoire pour une fraction de seconde. Cette fonctionnalité primordiale permet d'éviter à quiconque de rechercher votre phrase secrète dans la mémoire de votre ordinateur lorsque vous ne travaillez pas dessus. Si une telle situation se présentait, l'intrus aurait alors un accès complet aux données protégées par cette phrase secrète, bien que vous n'en soyez pas conscient.

Protection de la mémoire virtuelle

Votre phrase secrète ou d'autres clés risquent d'être enregistrées sur le disque lorsque le système de mémoire virtuelle y remplace de la mémoire. PGP Desktop veille à ce que cela ne se produise jamais. Cette fonctionnalité permet d'empêcher les intrus potentiels d'analyser le fichier de mémoire virtuelle en quête de phrases secrètes.

Mise en veille prolongée ou veille

Sous Windows, le mode Mise en veille prolongée écrit une image de l'intégralité du stockage de mémoire de votre ordinateur dans un fichier de votre disque dur, mais *pas* votre phrase secrète. PGP Corporation vous recommande de toujours utiliser la mise en veille prolongée plutôt que la simple veille, car la mise en veille prolongée éteint votre ordinateur et exige ensuite que vous vous authentifiiez à nouveau sur l'écran PGP BootGuard pour ouvrir une nouvelle session.

Protection de la migration d'ions statiques dans la mémoire

Lorsque vous protégez un disque ou une partition (sous Windows) avec PGP Whole Disk Encryption, votre phrase secrète est transformée en clé. Cette clé sert à chiffrer et déchiffrer les données stockées sur le disque ou la partition chiffré(e). Tandis que la phrase secrète est immédiatement effacée de la mémoire, la clé (dont votre phrase secrète ne peut pas être dérivée) demeure en mémoire.

Cette clé est protégée de la mémoire virtuelle ; cependant, si une zone spécifique de la mémoire stocke exactement les mêmes données pendant de très longues périodes sans être éteinte ou réinitialisée, cette mémoire tend à conserver une charge statique, qui pourrait être lue par des personnes malveillantes. Si votre disque ou partition chiffré(e) (sous Windows) reste déchiffré(e) sur de longues périodes, avec le temps, des traces discernables de votre clé pourraient demeurer en mémoire. Des périphériques permettent de récupérer la clé. Vous ne les trouverez pas dans votre magasin d'électronique habituel, mais les principaux gouvernements sont susceptibles d'en posséder.

PGP Desktop protège contre cette faiblesse en conservant deux copies de la clé en RAM (une copie normale et une en bits inversés) et en les intervertissant très fréquemment.

Autres éléments de sécurité à prendre en compte

En général, votre capacité à protéger vos données dépend des précautions que vous prenez, et aucun programme de chiffrement ne peut vous prémunir de négligences dans vos pratiques de sécurité. Par exemple, si vous quittez votre bureau en laissant des fichiers sensibles ouverts sur votre ordinateur, n'importe qui peut accéder à ces informations, et ce même si le disque ou la partition (sous Windows) est protégé(e) avec PGP Whole Disk Encryption.

Voici quelques conseils vous permettant d'assurer une sécurité optimale :

- Utilisez un économiseur d'écran bloqué par un mot de passe lorsque vous êtes loin de votre ordinateur, afin de décourager les tiers d'accéder à votre poste ou de consulter votre écran.
- Assurez-vous que vos disques ou partitions chiffrés (sous Windows) ne sont pas accessibles aux autres ordinateurs du réseau. Vous devrez peut-être faire appel aux gestionnaires du réseau de votre entreprise. Une fois que vous avez déverrouillé votre disque ou votre partition, PGP Whole Disk Encryption ne peut plus protéger les fichiers. Ceux-ci sont alors visibles par toutes les personnes ayant accès au réseau. Pour stocker des fichiers qui doivent être verrouillés même lorsque vous utilisez votre ordinateur, vous pouvez avoir recours à la fonctionnalité PGP Virtual Disk.
- Ne notez jamais votre phrase secrète. Choisissez-en une dont vous pouvez vous rappeler. Si vous éprouvez des difficultés à vous souvenir de votre phrase secrète, utilisez un élément qui vous permettra de la retrouver facilement, comme un poster, une chanson, un poème ou une blague, mais *ne la notez pas*.
- Si vous utilisez PGP Desktop à domicile et partagez votre ordinateur avec d'autres personnes, ces dernières seront probablement en mesure de voir les fichiers ouverts sur un disque ou une partition (sous Windows) protégé(e) avec PGP WDE. Dès lors que vous arrêtez un système doté d'un disque ou d'une partition chiffré(e) avec WDE ou retirez un disque amovible chiffré du système, tous les fichiers du disque ou de la partition restent chiffrés et entièrement protégés.

Utilisation de l'environnement de préinstallation Windows

La création d'un CD/UFD (lecteur USB Flash) d'environnement de préinstallation (PE) Windows personnalisé permet de disposer d'un outil de démarrage pouvant être utilisé à des fins de récupération. Vous pouvez ainsi employer les commandes DOS pour copier, modifier, sauvegarder et supprimer des fichiers.

Vous pouvez également utiliser Windows PE pour mettre à niveau un ordinateur chiffré par PGP WDE vers Windows Vista.

Pour obtenir les pilotes et outils PGP WDE, reportez-vous à l'*article 807 de la base de connaissances du PGP Support* (https://support.pgp.com/?faq=807). Cet article contient également une note technique que vous pouvez télécharger et qui contient toutes les instructions de cette section.

Utilisation de PGP Whole Disk Encryption avec les systèmes IBM Lenovo ThinkPad

Utilisez l'environnement de préinstallation Windows (PE) pour préinstaller le pilote PGP WDE dans la solution Rescue and Recovery d'IBM Lenovo ThinkPad et détecter automatiquement la fonctionnalité Rescue and Recovery de Lenovo.

Cette option est disponible uniquement pour les systèmes les systèmes IBM Lenovo exécutant Rescue and Recovery version 3.0 et ultérieures. Elle préinstalle le pilote PGP WDE dans la solution Lenovo Rescue and Recovery et détecte automatiquement la prise en charge de la fonctionnalité Rescue and Recovery de Lenovo. Elle récupère le pilote PGP WDE dans le répertoire \windows\system32\drivers. Les deux fichiers installés dans la solution Rescue and Recovery d'IBM Lenovo sont le pilote PGP WDE (`pgpwded.sys`) et le fichier `PGPstart.exe` (pour plus d'informations sur ce fichier, reportez-vous à la procédure ci-dessous).

Les fichiers requis pour installer PGP Whole Disk Encryption dans la solution Rescue and Recovery d'IBM Lenovo sont :

- les fichiers de l'outil pgppe : `pgppe.exe` et `pgpstart.exe` ;
- les fichiers d'installation de PGP Desktop : `pgpwded.sys`, `pgpbootb.bin`, `pgpbootg.bin`, `pgpsdk.dll`, `pgpsdknl.dll`, `pgpwd.dll` et `pgpwde.exe` ;
- les fichiers de Windows Vista uniquement : les pilotes wimfltr doivent être installés (dans le cadre du Kit d'installation automatisée Windows).

Attention : utilisez cette option uniquement après installation de PGP Desktop sur le système.

Pour activer la solution Rescue and Recovery de Lenovo

1. Installez PGP Desktop.
2. Procurez-vous et installez les outils de l'environnement de préinstallation Windows à partir de l'*article 807 de la base de connaissances du support de PGP* (https://support.pgp.com/?faq=807).
3. Copiez les fichiers `PGPstart.exe` et `PGPpe.exe` à partir du fichier zip dans le répertoire d'installation de PGP Desktop (généralement, `c:\Program Files\PGP Corporation\PGP Desktop`).
4. Démarrez une invite de commande et passez au répertoire PGP Desktop.
5. Exécutez la commande pgppe de la façon suivante :

   ```
   pgppe /recovery
   ```

Pour supprimer la prise en charge de la solution Rescue and Recovery de Lenovo

Exécutez la commande pgppe de la façon suivante : `pgppe /recovery /remove`

Utilisation de PGP Whole Disk Encryption avec la console de récupération Microsoft Windows XP

Si vous utilisez la console de récupération Windows XP dans un objectif d'administration, vous devez installer les pilotes PGP WDE sur la console de récupération Microsoft Windows lorsque le disque est chiffré. Autrement, la console ne peut pas être utilisée.

Remarque : les utilisateurs de Windows PE ou BartPE doivent s'authentifier par phrase secrète. Les utilisateurs de jeton ou TPM ne sont pas pris en charge sur ces systèmes.

Attention : installez ces pilotes une fois PGP Desktop installé et le disque chiffré avec PGP WDE.

Pour installer les pilotes PGP WDE sur la console de récupération Windows XP

1. Installez PGP Desktop.
2. Procurez-vous et installez les outils de l'environnement de préinstallation Windows à partir de l'*article 807 de la base de connaissances du support de PGP* (https://support.pgp.com/?faq=807).

3. Copiez les fichiers `PGPstart.exe` et `PGPpe.exe` à partir du fichier zip dans le répertoire d'installation de PGP Desktop (généralement, `c:\Program Files\PGP Corporation\PGP Desktop`).
4. Démarrez une invite de commande et passez au répertoire d'installation de PGP Desktop.
5. Exécutez la commande pgppe de la façon suivante :

   ```
   pgppe /cmdcons
   ```

Pour supprimer les pilotes de la console de récupération Windows XP

Exécutez la commande pgppe de la façon suivante : `pgppe /cmdcons /remove`

11 Utilisation des PGP Virtual Disks

Les PGP Virtual Disks vous permettent d'organiser votre travail, de conserver séparément des fichiers aux noms similaires, ou de conserver séparément plusieurs versions des mêmes documents ou programmes.

Cette section décrit la fonctionnalité PGP Virtual Disk de PGP Desktop.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

Remarque : les PGP Virtual Disks étaient appelés *PGP Disks* dans les versions précédentes de PGP Desktop. L'expression *PGP Disk* inclut désormais à la fois les fonctionnalités PGP Virtual Disk et PGP Whole Disk Encryption.

À propos des PGP Virtual Disks

Un PGP Virtual Disk est une zone d'espace, sur n'importe quel disque connecté à votre ordinateur, qui est gardée en réserve et chiffrée. Les PGP Virtual Disks s'apparentent en grande partie à une chambre forte, et sont très utiles pour protéger les dossiers sensibles lorsque le reste de votre ordinateur est déverrouillé afin de pouvoir travailler.

Un PGP Virtual Disk ressemble et se comporte comme un disque dur supplémentaire, même s'il s'agit en fait d'un fichier unique résidant sur l'un des disques de votre ordinateur. Il offre de l'espace de stockage pour vos fichiers (vous pouvez même y installer des applications ou y enregistrer des fichiers), mais il est également possible de le verrouiller à tout moment sans affecter d'autres parties de votre ordinateur. Pour utiliser les applications ou les fichiers stockés sur un PGP Virtual Disk, déverrouillez le disque et rendez les fichiers accessibles à nouveau.

Les PGP Virtual Disks sont déverrouillés et verrouillés en les montant et en les démontant de votre ordinateur. PGP Desktop gère cette opération pour vous.

Même si vous spécifiez une taille pour votre PGP Virtual Disk, vous pouvez également créer un disque à dimensionnement dynamique dont la taille augmentera en fonction des besoins. La taille que vous spécifiez lors de la création du disque correspond à la taille maximale qu'aura le disque.

Lorsqu'un PGP Virtual Disk est monté, vous pouvez :

- déplacer/copier des fichiers dans ou hors de celui-ci ;
- enregistrer les fichiers sur celui-ci ;
- installer des applications dans celui-ci.

Les fichiers et applications d'un PGP Virtual Disk sont stockés chiffrés. Si votre ordinateur s'arrête alors qu'un PGP Virtual Disk est démonté, le contenu reste chiffré de manière sécurisée.

Lorsqu'un PGP Virtual Disk est démonté, il n'apparaît pas dans l'Explorateur Windows ou le Finder sous Mac OS X, et est inaccessible à quiconque ne dispose pas de l'authentification appropriée.

Rappelez-vous que toutes vos données restent sécurisées dans le fichier chiffré et sont uniquement déchiffrées lorsque vous accédez à l'un des fichiers. Le stockage des données d'un volume de cette manière simplifie la manipulation et l'échange des PGP Virtual Disks avec d'autres personnes, mais augmente également le risque de perte des données si le fichier vient d'une manière ou d'une autre à être supprimé. Il est donc judicieux de conserver une copie de sauvegarde de ces fichiers chiffrés afin de pouvoir récupérer les données en cas de problème.

Pour plus d'informations sur les options de PGP qui affectent les volumes PGP Virtual Disk, reportez-vous à la section *Options de l'onglet Disque* (à la page 327).

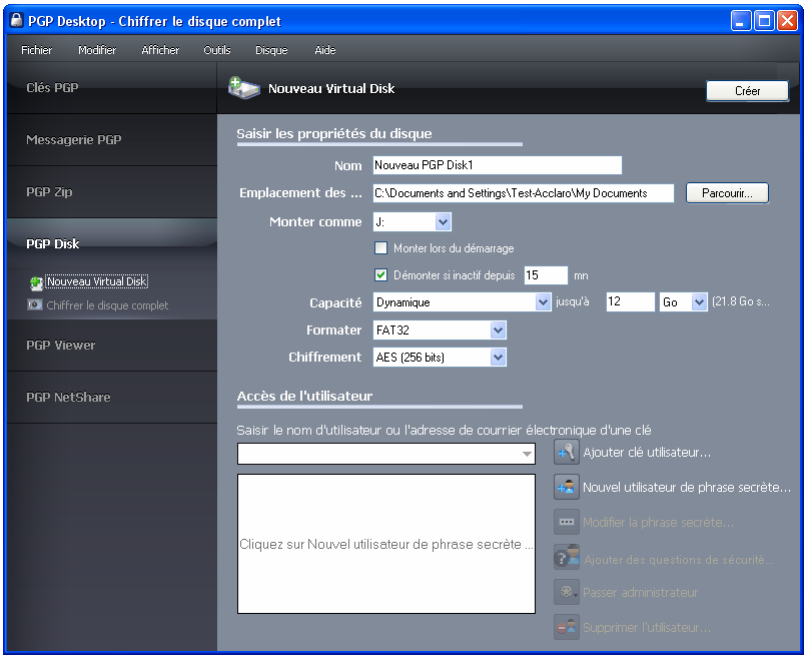
Attention : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, il peut s'avérer nécessaire de créer un PGP Virtual Disk après installation de PGP Desktop. Dans ce cas, la taille, le système de fichiers et l'algorithme ont pu être spécifiés. Pour plus d'informations, reportez-vous à la section *Utilisation de PGP Desktop avec un PGP Universal Server* (à la page 341).

Création d'un volume PGP Virtual Disk

Pour créer un volume PGP Virtual Disk

1 Ouvrez PGP Desktop.

2 Cliquez sur le panneau de contrôle PGP Disk dans le volet gauche de l'écran principal de PGP Desktop, puis sur **Nouveau Virtual Disk. Vous pouvez également sélectionner Fichier > Nouveau > PGP Virtual Disk**. L'écran Nouveau Virtual Disk s'affiche dans le volet droit de l'écran.



3 Dans le champ **Nom**, saisissez le nom que vous souhaitez attribuer au nouveau PGP Virtual Disk.

4 Dans le champ **Emplacement des fichiers de disque**, acceptez l'emplacement par défaut pour le volume PGP Virtual Disk que vous créez ou cliquez sur **Parcourir** pour spécifier un autre emplacement.

5 Dans le menu **Monter comme**, sélectionnez la lettre de lecteur souhaitée pour le nouveau PGP Virtual Disk.

Vous pouvez :

- accepter la lettre de lecteur que PGP Desktop vous suggère.
- Dans le menu **Monter comme**, sélectionnez un lecteur disponible dans la liste.
- sélectionner **Dossier** dans le menu **Monter comme** si vous voulez monter le nouveau PGP Virtual Disk dans un dossier au lieu d'une lettre de lecteur. Un champ s'affiche ensuite en regard du menu **et vous permet de spécifier l'emplacement du dossier.**

6 Sélectionnez **Monter lors du démarrage** pour monter automatiquement votre nouveau volume PGP Virtual Disk au démarrage. Lorsque vous démarrerez votre ordinateur, vous serez invité à saisir la phrase secrète de votre PGP Virtual Disk.

7 Sélectionnez **Démonter si inactif depuis n min** [où *n* correspond au nombre de minutes] pour démonter le PGP Virtual Disk si vous n'avez pas utilisé votre ordinateur pendant l'intervalle de temps spécifique que vous spécifiez (en minutes). Cela s'avère utile si vous laissez souvent votre ordinateur sans surveillance : il s'agit d'un dispositif de protection supplémentaire qui verrouille votre PGP Virtual Disk si vous oubliez de le faire.

8 Dans le menu **Capacité**, sélectionnez le type de PGP Virtual Disk souhaité. Les options disponibles sont les suivantes :

- **Dynamique (redimensionnable)** : ce type de disque augmente en capacité au fur et à mesure que vous y ajoutez des fichiers, mais reste de petite taille tant que l'espace supplémentaire n'est pas nécessaire. PGP Desktop gère ce processus ; vous devez uniquement définir la taille maximale du disque. Vous pouvez également compresser ce disque ultérieurement. Ce type de volume PGP Virtual Disk est disponible uniquement pour les disques avec systèmes de fichiers FAT ou FAT32.
- **Extensible** : ce type de disque augmente en capacité au fur et à mesure que vous y ajoutez des fichiers, mais reste de petite taille tant que l'espace supplémentaire n'est pas nécessaire. PGP Desktop gère ce processus ; vous devez uniquement définir la taille maximale du disque. Vous pouvez également compresser ce disque ultérieurement. Ce type de volume PGP Virtual Disk est disponible uniquement pour les disques avec systèmes de fichiers NTFS.
- **Taille fixe** : ce type de disque conserve la même taille, quel que soit le nombre de fichiers que vous y ajoutez. Ces volumes PGP Virtual Disk sont disponibles pour tous les disques, indépendamment du système de fichiers utilisé.

9 Dans le menu **Capacité**, définissez la taille (en cas de disques dynamiques, la taille maximale) de votre nouveau PGP Virtual Disk. Utilisez des nombres entiers, sans décimales. Dans le menu, sélectionnez **Ko** (kilo-octets), **Mo** (méga-octets) ou **Go** (giga-octets).

La taille maximale autorisée pour un PGP Virtual Disk dépend de la taille et du format de votre disque dur.

10 Spécifiez un format de système de fichiers pour le volume :

- **FAT** : le volume doit être de 100 Ko ou plus.
- **FAT32** : le volume doit être de 260 Mo ou plus.
- **NTFS** : le volume doit être de 5 Mo ou plus (12 Mo pour Windows Vista).

11 Précisez l'algorithme de chiffrement à utiliser pour protéger vos données :

- **AES (256 bits)** : AES (Advanced Encryption Standard) est un chiffrement par blocs qui peut être utilisé à 128, 192 ou 256 bits. La version 256 bits plus sécurisée permet de créer des volumes PGP Virtual Disk par défaut.
- **EME2-AES (256 bits)**. EME2 (Encrypt-Mix-Encrypt v2) est un algorithme plus performant qui chiffre deux fois plus de données par opération. Il fonctionne par blocs volumineux et est actuellement en cours de révision par le groupe de travail sur les normes de l'IEEE.
- **CAST5 (128 bits)** : CAST est un chiffrement par blocs de 128 bits. Il s'agit d'un algorithme de chiffrement de sécurité de niveau militaire qui bénéficie d'une solide réputation en raison de sa capacité à résister aux tentatives d'accès non autorisées.
- **Twofish (256 bits)** : Twofish est un algorithme symétrique de chiffrement par blocs de 256 bits. C'est l'un des cinq algorithmes à avoir été envisagés par le NIST (U.S. National Institute of Standards and Technology) pour le standard de chiffrement avancé AES (Rijndael a finalement été choisi).

12 Au moins un utilisateur doit pouvoir accéder à votre nouveau PGP Virtual Disk. Dans la section **Accès de l'utilisateur**, spécifiez l'utilisateur auquel vous souhaitez donner accès, ainsi que la méthode d'accès utilisée :

- **Clé utilisateur** : pour ajouter des utilisateurs qui s'authentifieront à l'aide du chiffrement par clé publique :
  - Cliquez sur **Ajouter clé utilisateur**. La boîte de dialogue Ajouter utilisateurs clés s'affiche et indique les paires de clés figurant actuellement dans votre trousseau.
  - Dans la zone **Ajouter utilisateurs clés**, sélectionnez les utilisateurs de clés souhaités en double-cliquant sur la liste. Vous pouvez également faire glisser la liste de la gauche vers la droite, ou sélectionner une liste et cliquer sur **Ajouter**. Cliquez sur **OK** lorsque vous avez terminé.
- **Phrase secrète** : cliquez sur **Nouvel utilisateur de phrase secrète**. La boîte de dialogue Créer un utilisateur s'affiche.
  - Pour chaque nouvel utilisateur de phrase secrète, saisissez un nom, la phrase secrète correspondante, puis confirmez la phrase secrète. Cliquez sur **OK** pour créer l'utilisateur de phrase secrète. Pour autoriser davantage d'utilisateurs, répétez la procédure.

- Pour modifier la phrase secrète d'un utilisateur, sélectionnez-le, puis cliquez sur **Modifier la phrase secrète**.

Pour plus d'informations sur la création de phrases secrètes efficaces et performantes, reportez-vous à la section *Création de phrases secrètes fortes* (à la page 337).

13 Cliquez sur **Créer** pour commencer à créer le PGP Virtual Disk. Une barre de progression indique quelle quantité du PGP Virtual Disk a été initialisée et formatée. Une fois que la procédure est terminée, votre nouveau PGP Virtual Disk s'affiche dans la zone de contrôle PGP Disk.

14 Le statut administrateur est accordé au premier utilisateur que vous créez, un seul administrateur ne pouvant exister à la fois. Toutefois, vous pouvez accorder ce statut à n'importe lequel des autres utilisateurs, qu'il s'agisse d'utilisateurs de clé publique ou de phrase secrète. Cliquez sur son nom dans la liste Accès de l'utilisateur, puis sur **Passer administrateur**.

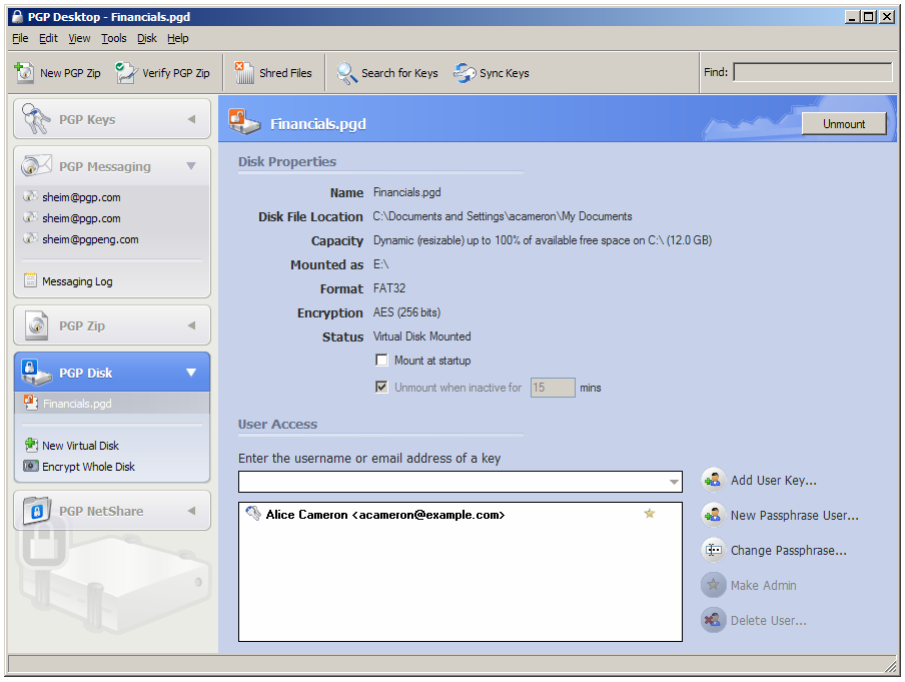
15 Pour supprimer un utilisateur autre que l'administrateur, sélectionnez son nom et cliquez sur **Supprimer l'utilisateur**. Pour supprimer l'administrateur, accordez tout d'abord son statut à un autre utilisateur, puis supprimez l'ancien administrateur.

Affichage des propriétés d'un PGP Virtual Disk

Dès qu'un PGP Virtual Disk est créé, les informations relatives à ce disque et les paramètres que vous pouvez modifier sont accessibles à partir de l'écran Propriétés du disque.

Pour afficher les propriétés d'un volume PGP Disk

- Dans la boîte de contrôle PGP Disk située sur la gauche de l'écran principal de PGP Desktop, cliquez sur le nom du disque. Le panneau Propriétés du disque s'affiche dans la partie droite de l'écran principal.



Recherche de PGP Virtual Disks

Si vous créez des PGP Virtual Disks en utilisant des installations précédentes de PGP Desktop, ces volumes sont facilement identifiables à l'aide de l'assistant de recherche de PGP Disk.

Pour rechercher des PGP Virtual Disks sur votre système

1. Dans PGP Desktop, cliquez sur la boîte de contrôle **PGP Disk**. L'écran principal de PGP Disk s'affiche.
2. Sélectionnez **Fichier > Recherche de PGP Disks**. La boîte de dialogue PGP Disk Search Assistant s'affiche.
3. Suivez les instructions affichées dans l'assistant.

Conseil : pour rechercher le volume monté d'un PGP Virtual Disk spécifique, dans PGP Desktop, cliquez avec le bouton droit sur le nom du volume et sélectionnez **Afficher l'emplacement du disque dans l'explorateur**. L'Explorateur Windows s'ouvre dans une nouvelle fenêtre affichant le contenu de ce volume.

Utilisation d'un PGP Virtual Disk monté

Créez, copiez, déplacez et supprimez des fichiers et dossiers sur un PGP Virtual Disk tout comme vous le feriez habituellement avec n'importe quel autre disque sur votre système.

Toute autre personne ayant accès au volume (soit sur le même ordinateur, soit sur le réseau) peut également accéder aux données qui y sont stockées. Les données ne sont protégées qu'à partir du moment où vous démontez le volume.

Attention : même si chaque fichier PGP Virtual Disk est chiffré et est inaccessible à quiconque ne dispose pas de l'autorisation appropriée, il peut toujours être supprimé de votre système. Toute personne accédant à votre système peut supprimer le fichier chiffré contenant le PGP Virtual Disk. Pour cette raison, la conservation d'une copie de sauvegarde de ce fichier est une excellente mesure de sécurité, de même que de garder votre ordinateur verrouillé lorsque vous n'êtes pas à proximité de celui-ci.

Montage d'un PGP Virtual Disk

Lorsque vous créez un PGP Virtual Disk, il est automatiquement monté afin que vous puissiez commencer à y stocker vos fichiers.

Pour sécuriser le contenu d'un volume, vous devez le démonter. Une fois celui-ci démonté, son contenu reste sécurisé dans un fichier chiffré où il reste inaccessible tant que le volume n'est pas monté à nouveau.

Il existe plusieurs méthodes pour monter un PGP Virtual Disk :

- Dans PGP Desktop, sélectionnez le PGP Virtual Disk à monter et sélectionnez **Disque > Monter**.
- Dans PGP Desktop, sélectionnez le PGP Virtual Disk à monter, puis cliquez sur **Monter** dans le coin supérieur droit sur les systèmes Windows, ou sur l'icône **Monter** de la barre d'outils sur les systèmes Mac OS X.
- Modifiez les propriétés du PGP Virtual Disk afin qu'il se monte au démarrage de votre ordinateur.

Sur les systèmes Windows uniquement :

- Pendant la création du PGP Virtual Disk, cochez la case **Monter lors du démarrage**. Le volume se montera automatiquement lorsque vous démarrerez Windows. Si vous ne cochez pas cette case pendant la création du PGP Virtual Disk, vous pourrez la définir en tant qu'option ultérieurement.
- Dans l'Explorateur Windows, cliquez avec le bouton droit sur le fichier PGP Virtual Disk, puis sélectionnez **PGP > Monter le disque** dans le menu contextuel.

Les volumes PGP Virtual Disk montés apparaissent sous forme de lecteurs vides dans l'Explorateur Windows et le Finder sous Mac OS X.

Démontage d'un PGP Virtual Disk

Le démontage d'un PGP Virtual Disk vous permet de le verrouiller. Lorsqu'un PGP Virtual Disk est démonté, son contenu est verrouillé dans le fichier chiffré associé au volume. Son contenu reste inaccessible tant que le volume n'est pas monté à nouveau.

Attention : vous pouvez perdre des données si vous démontez un PGP Virtual Disk alors que certains fichiers qu'il contient sont ouverts. Spécifiez des options de démontage des disques en sélectionnant **Outils > PGP** et en cliquant sur l'onglet **Disque**. L'une des options est **Autoriser le démontage des PGP Disks même si certains fichiers sont encore ouverts**. Si cette option est sélectionnée, l'option **Ne pas demander confirmation avant le démontage** devient également disponible. **N'utilisez ces options que si vous y êtes familiarisé.** Bien que ces options puissent s'avérer utile pour les utilisateurs avancés qui protègent leurs données à l'aide de sauvegardes régulières, leur utilisation est déconseillée pour la plupart des utilisateurs.

Il existe plusieurs méthodes pour démonter un volume PGP Virtual Disk :

- Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le volume à démonter. Cliquez sur **Démonter** dans le coin supérieur droit, ou sélectionnez **Disque > Démonter**.
- Dans l'Explorateur Windows, cliquez avec le bouton droit sur le fichier PGP Virtual Disk, puis sélectionnez **PGP > Démonter le PGP Virtual Disk** dans le menu contextuel.
- Utilisez le raccourci clavier pour démonter tous les PGP Virtual Disks. Le raccourci clavier par défaut est **Ctrl+Maj+U**. Le raccourci clavier doit d'abord être activé.

Une fois le PGP Virtual Disk démonté, son contenu reste verrouillé et inaccessible tant que le volume n'est pas monté à nouveau.

Compactage d'un PGP Virtual Disk

Pour libérer de l'espace supplémentaire sur votre PGP Virtual Disk, compactez le disque. Si le PGP Virtual Disk est monté, vous devez le démonter avant de le compacter.

Remarque : seuls les PGP Virtual Disks dynamiques (à taille variable) avec un système de fichiers FAT ou FAT32 peuvent être compactés. Cette opération est impossible pour les disques dotés du système de fichiers NTFS ou à taille fixe.

Pour compacter un PGP Virtual Disk

- Effectuez l'une des opérations suivantes :
  - Dans l'Explorateur Windows, accédez à l'emplacement du fichier .pgd. Cliquez avec le bouton droit sur ce fichier et sélectionnez **PGP Desktop > Compacter l'espace inutilisé**.
  - Dans PGP Desktop, cliquez sur le panneau de contrôle PGP Disk situé dans le volet gauche de l'écran principal, sélectionnez le PGP Virtual Disk à compacter, puis choisissez **Disque > Compacter**. Vous pouvez également cliquer avec le bouton droit sur le PGP Virtual Disk dans le panneau de contrôle PGP Disk et sélectionner **Compacter** dans le menu contextuel.

Nouveau chiffrement des PGP Virtual Disks

Vous pouvez chiffrer à nouveau toutes les données stockées sur un PGP Virtual Disk. Vous pouvez être amené à le faire pour l'une ou les deux raisons suivantes :

- Vous souhaitez modifier l'algorithme de chiffrement actuellement utilisé pour protéger le volume.
- Vous suspectez une violation de la sécurité.

Un nouveau chiffrement vous permet de chiffrer à nouveau votre PGP Virtual Disk, mais d'utiliser une autre clé de chiffrement sous-jacente.

Attention : des utilisateurs expérimentés pourraient rechercher dans la mémoire d'un ordinateur la clé de chiffrement sous-jacente d'un PGP Virtual Disk, et l'utiliser pour accéder au volume même après avoir été supprimés de la liste des utilisateurs. Le nouveau chiffrement du disque change cette clé sous-jacente et empêche ce type d'intrusion.

Pour chiffrer à nouveau un PGP Virtual Disk

1. Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk à chiffrer à nouveau.
2. S'il est monté, démontez-le.
3. Sélectionnez le PGP Virtual Disk à chiffrer à nouveau.
4. Sélectionnez **Disque > Chiffrer à nouveau**.
5. Saisissez la phrase secrète pour le volume. L'assistant de nouveau chiffrement de PGP s'ouvre.
6. Lisez les informations d'introduction, puis cliquez sur **Suivant**. Une boîte de dialogue s'affiche et présente :
   - l'algorithme de chiffrement actuel protégeant votre PGP Virtual Disk ;
   - les algorithmes de chiffrement disponibles autres que celui initialement sélectionné.

   Par exemple, si votre PGP Virtual Disk est actuellement chiffré avec AES, les options **CAST5** et **Twofish** apparaissent dans la liste **Nouvel algorithme**.
7. Effectuez l'une des opérations suivantes :
   - Pour chiffrer à nouveau le volume en utilisant l'algorithme actuel, cochez la case **Chiffrer à nouveau avec le même algorithme**, puis cliquez sur **Suivant**. Le volume PGP Virtual Disk est à nouveau chiffré à l'aide du même algorithme qu'auparavant.
   - Pour chiffrer à nouveau le volume en utilisant un autre algorithme, sélectionnez celui-ci dans le menu **Nouvel algorithme**, puis cliquez sur **Suivant**. Le volume PGP Virtual Disk est à nouveau chiffré à l'aide du nouvel algorithme sélectionné.
8. Lorsque l'état actuel indique Terminé, cliquez sur **Suivant**.
9. Cliquez sur **Terminer** pour finaliser le processus de nouveau chiffrement.

Gestion des autres utilisateurs

Cette section décrit comme ajouter, supprimer ou désactiver d'autres comptes d'utilisateur pour vos PGP Virtual Disks. Elle contient également des informations sur la modification des droits des utilisateurs, notamment l'attribution de droits d'administrateur à un utilisateur.

Ajout de comptes autre utilisateur à un PGP Virtual Disk

L'administrateur d'un PGP Virtual Disk peut le rendre accessible à d'autres utilisateurs. Ceux-ci peuvent accéder au volume à l'aide de leur propre phrase secrète ou clé privée.

Assurez-vous que le PGP Virtual Disk n'est *pas* monté, sinon vous ne pourrez pas ajouter de comptes autre d'utilisateur.

Pour ajouter des comptes autre utilisateur à un PGP Virtual Disk

1. Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk auquel vous souhaitez ajouter un compte autre utilisateur.
2. Effectuez l'une des opérations suivantes :
   - Pour ajouter un nouvel utilisateur de clé publique, cliquez sur **Ajouter clé utilisateur**. La boîte de dialogue Ajouter utilisateurs clés s'affiche.
   - Pour ajouter un nouvel utilisateur de phrase secrète, cliquez sur **Nouvel utilisateur de phrase secrète**. La boîte de dialogue Nouvel utilisateur de PGP Disk s'affiche.
3. Effectuez l'une des opérations suivantes :
   - Si vous avez sélectionné **Ajouter clé utilisateur**, dans la boîte de dialogue Ajouter utilisateurs clés, sélectionnez une clé publique dans la liste, puis cliquez sur **OK**.
   - Si vous avez sélectionné **Nouvel utilisateur de phrase secrète**, dans la boîte de dialogue Nouvel utilisateur de PGP Disk, saisissez le nom d'utilisateur, la phrase secrète pour le PGP Virtual Disk auquel vous ajoutez l'utilisateur, puis ressaisissez la phrase secrète et cliquez sur **OK**.

   Le compte autre utilisateur est ajouté.

Suppression de comptes autre utilisateur d'un PGP Virtual Disk

Il se peut qu'un jour vous souhaitiez interdire l'accès à un PGP Virtual Disk à un autre utilisateur.

Assurez-vous que le PGP Virtual Disk n'est *pas* monté. Vous ne pouvez pas supprimer un compte autre utilisateur si le volume est monté.

Pour supprimer un compte autre utilisateur d'un PGP Virtual Disk

1. Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk du compte d'utilisateur à supprimer.

2 Dans la liste Accès de l'utilisateur, sélectionnez le nom de l'autre utilisateur dont le compte est à supprimer. Vous ne pouvez pas supprimer l'administrateur.

3 Cliquez sur **Supprimer l'utilisateur**. La boîte de dialogue Phrase secrète s'affiche vous demandant d'indiquer la phrase secrète de l'administrateur ou celle pour le compte d'utilisateur à supprimer.

4 Saisissez la phrase secrète, puis cliquez sur **OK**. Le compte autre utilisateur est supprimé.

Désactivation et activation de comptes autre utilisateur

Pour interdire l'accès à un PGP Virtual Disk à un autre utilisateur sans supprimer totalement son compte, vous pouvez à la place désactiver temporairement son accès.

Assurez-vous que le PGP Virtual Disk n'est *pas* monté. Vous ne pouvez pas désactiver ou activer un compte autre utilisateur si le volume est monté.

Pour désactiver ou activer un compte autre utilisateur d'un PGP Virtual Disk

1 Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk du compte d'utilisateur à modifier.

2 Dans la liste Accès de l'utilisateur, effectuez l'une des opérations suivantes :

- Pour désactiver un utilisateur, cliquez avec le bouton droit sur le nom du compte autre utilisateur à désactiver et sélectionnez **Désactiver**. La boîte de dialogue Phrase secrète s'affiche et vous demande d'indiquer la phrase secrète de l'administrateur ou celle pour le compte d'utilisateur en cours de désactivation. Saisissez la phrase secrète, puis cliquez sur **OK**. Le compte autre utilisateur est désactivé.
- Pour activer un utilisateur qui a été précédemment désactivé, cliquez avec le bouton droit sur le nom du compte autre utilisateur à activer et sélectionnez **Activer**. La boîte de dialogue Phrase secrète s'affiche et vous demande d'indiquer la phrase secrète de l'administrateur ou celle pour le compte d'utilisateur en cours d'activation. Saisissez la phrase secrète, puis cliquez sur **OK**. Le compte autre utilisateur est activé.

Passage à l'état lecture/écriture et lecture seule

Les utilisateurs d'un PGP Virtual Disk peuvent disposer de privilèges illimités de lecture et d'écriture ou de privilèges de lecture uniquement. Vous pouvez modifier ces privilèges pour un utilisateur à tout moment.

Assurez-vous que le PGP Virtual Disk sélectionné n'est pas monté. Vous ne pouvez pas modifier les droits si le volume est monté.

Pour modifier les droits d'un utilisateur sur un PGP Virtual Disk

1. Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk du compte d'utilisateur à modifier.
2. Dans la liste Accès de l'utilisateur, sélectionnez le nom de l'utilisateur dont l'état est à modifier.
3. Effectuez l'une des opérations suivantes :
   - Pour passer l'utilisateur en accès lecture seule, cliquez avec le bouton droit sur son nom et sélectionnez **Lecture seule**.
   - Pour passer l'utilisateur en accès lecture/écriture, cliquez avec le bouton droit sur son nom et sélectionnez **Lecture/écriture**.

   La boîte de dialogue Veuillez saisir la phrase secrète s'affiche.
4. Saisissez la phrase secrète de l'administrateur pour le PGP Virtual Disk, puis cliquez sur **OK**. Les droits de l'utilisateur sélectionné sont modifiés.

Attribution du statut administrateur à un autre utilisateur

Vous pouvez modifier le statut d'un compte utilisateur de autre à administrateur

Assurez-vous que le PGP Virtual Disk sélectionné n'est *pas* monté. Vous ne pouvez pas attribuer le statut administrateur à un utilisateur si le volume est monté.

Pour attribuer le statut administrateur

1. Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk du compte d'utilisateur à modifier.
2. Dans la liste Accès de l'utilisateur, sélectionnez l'utilisateur que vous souhaitez faire passer administrateur du PGP Virtual Disk. Sélectionnez un utilisateur de phrase secrète ou vous-même (si vous n'est pas l'administrateur actuel). Remarque : vous ne pouvez pas faire passer un utilisateur de clé publique administrateur du PGP Virtual Disk.
3. Dans la barre d'options à gauche, cliquez sur **Passer administrateur**. Le compte d'utilisateur sélectionné est passé à administrateur.

Remarque : vous pouvez attribuer le statut administrateur à un seul compte d'utilisateur à la fois. En accordant le statut administrateur à un compte, vous le supprimez également d'un autre.

Modification des phrases secrètes des utilisateurs

Assurez-vous que le PGP Virtual Disk sélectionné n'est *pas* monté. Vous ne pouvez pas modifier la phase secrète si le volume est monté.

Pour modifier la phrase secrète d'un utilisateur pour un PGP Virtual Disk

1. Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk dont vous êtes utilisateur.
2. Sélectionnez le nom d'un utilisateur de phrase secrète dans la liste Accès de l'utilisateur, puis cliquez sur **Modifier la phrase secrète**. La boîte de dialogue Veuillez saisir la phrase secrète s'affiche.

   Conseil : vous pouvez également cliquer avec le bouton droit sur le nom de l'utilisateur et sélectionner **Modifier phrase secrète utilisateur** dans le menu contextuel.
3. Saisissez la phrase secrète actuelle pour l'utilisateur et cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète de confirmation PGP s'affiche.
4. Saisissez une nouvelle phrase secrète, puis ressaisissez-la pour confirmation et cliquez sur **OK**. La phrase secrète est modifiée.

Suppression des PGP Virtual Disks

Il se peut qu'un jour vous décidiez n'avoir plus besoin d'un PGP Virtual Disk en particulier et que vous choisissiez de supprimer entièrement ce disque.

Attention : lorsque vous supprimez un PGP Virtual Disk, toutes les données qu'il contient le sont également. *Il n'existe aucun moyen de récupérer les données une fois que vous supprimez un PGP Virtual Disk*. Assurez-vous d'avoir copié les données à conserver dans un autre emplacement *avant de supprimer un PGP Virtual Disk*.

Assurez-vous que le PGP Virtual Disk sélectionné n'est *pas* monté. Vous ne pouvez pas supprimer le PGP Virtual Disk si le volume est monté.

Pour supprimer un PGP Virtual Disk

1. Cliquez sur la boîte de contrôle PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk à supprimer.

2 Sélectionnez **Disque > Supprimer**. Une boîte de dialogue de confirmation apparaît.

3 Effectuez l'une des opérations suivantes :

- Cliquez sur **OK** pour supprimer le PGP Virtual Disk de la liste PGP Desktop. Le PGP Virtual Disk reste sur votre système.
- Cliquez sur **Supprimer le PGP Disk** pour supprimer le PGP Virtual Disk de la liste PGP Desktop, ainsi que de votre disque dur.

Gestion des PGP Virtual Disks

Cette section décrit comment assurer la gestion appropriée du PGP Virtual Disk que vous utilisez avec votre ordinateur.

Montage des volumes PGP Virtual Disk sur un serveur distant

Vous pouvez placer des volumes PGP Virtual Disk sur n'importe quel type de serveur (Windows ou UNIX). Les volumes peuvent être montés par quiconque dispose d'un ordinateur Windows et de PGP Desktop.

Remarque : la première personne à monter le volume PGP Virtual Disk localement dispose d'un accès en lecture-écriture au volume. Personne d'autre n'est alors en mesure d'accéder au volume. Pour que d'autres utilisateurs puissent accéder aux fichiers du volume, vous devez monter le volume en mode lecture seule (s'applique aux formats de système de fichiers FAT et FAT32 uniquement). Tous les utilisateurs du volume disposent alors d'un accès en lecture seule.

Si le volume PGP Virtual Disk est stocké sur un serveur Windows, vous pouvez également le monter à distance sur le serveur et autoriser des personnes à partager le volume monté. Toutefois, cela n'assure pas la sécurité des fichiers du volume.

Sauvegarde des volumes PGP Virtual Disk

La sauvegarde du contenu de votre volume PGP Virtual Disk est le meilleur moyen de protéger vos informations contre les défaillances matérielles ou toute autre perte.

Il est déconseillé de sauvegarder le contenu d'un PGP Virtual Disk monté (et par conséquent, déchiffré) tout comme vous le feriez avec n'importe quel autre volume. Le contenu n'est pas chiffré, et il est accessible à toute personne qui peut restaurer la sauvegarde. Faites plutôt une copie de sauvegarde du volume chiffré.

Pour sauvegarder un PGP Virtual Disk

1. Démontez le volume.
2. Copiez le fichier chiffré démonté sur une disquette, bande ou cartouche amovible tout comme vous le feriez avec n'importe quel autre fichier. Même si une personne autorisée a accès à la sauvegarde, elle ne sera pas en mesure de déchiffrer son contenu.

Lorsque vous faites des sauvegardes des fichiers chiffrés, gardez ceci à l'esprit :

- La sauvegarde des fichiers chiffrés sur un lecteur réseau offre aux autres pléthore d'opportunités pour deviner une phrase secrète à faible niveau de sécurité. Il est beaucoup moins risqué de faire votre sauvegarde uniquement sur des périphériques sur lesquels vous avez un contrôle physique.
- Une phrase secrète compliquée et assez longue permet de renforcer la sécurité de vos données.
- Si vous êtes sur un réseau, assurez-vous qu'aucun système de sauvegarde réseau ne sauvegarde les fichiers dans votre PGP Virtual Disk *monté*. (Il se peut que vous deviez en discuter avec votre administrateur système.) Une fois qu'un PGP Virtual Disk est monté, les fichiers qu'il contient sont déchiffrés et peuvent être copiés sur un système de sauvegarde réseau de cette manière.

Échange des PGP Virtual Disks

Vous pouvez échanger un PGP Virtual Disk avec d'autres utilisateurs disposant de PGP Desktop sur leur ordinateur. Pour ce faire, envoyez-leur une copie du fichier de données PGP Virtual Disk qui contient les données du volume. Voici quelques-unes des méthodes d'échange d'un PGP Virtual Disk :

- En tant que pièces jointes au courrier
- Sur un CD ou disque amovible
- Sur un réseau

Une fois que l'autre utilisateur dispose du fichier PGP Virtual Disk, il peut le monter sur un système exécutant PGP Desktop et utiliser la phrase secrète appropriée pour y accéder. Si le volume a été chiffré avec sa clé publique, il utilisera sa clé privé pour y accéder.

Remarque : la clé publique est la méthode de protection qui offre le niveau de sécurité maximal lors de l'ajout d'autres utilisateurs à un PGP Virtual Disk car : (1) vous n'avez pas à échanger de phrase secrète avec l'autre utilisateur qui, selon votre méthode, pourrait être interceptée ou entendue ; (2) l'autre utilisateur n'a pas besoin de mémoriser une autre phrase secrète qu'il pourrait oublier ; (3) il est plus facile de gérer une liste d'autres utilisateurs si chacun utilise sa propre clé privée pour déverrouiller le volume.

Algorithmes de chiffrement des PGP Virtual Disks

Le chiffrement utilise une formule mathématique pour brouiller vos données afin que personne d'autre ne puisse les utiliser. Lorsque vous appliquez la clé mathématique correcte, vous effectuez le débrouillage des données. La formule de chiffrement des volumes PGP Virtual Disk utilise des données aléatoires pour une partie du processus de chiffrement.

L'application PGP Desktop offre des options d'algorithmes performantes permettant de protéger vos volumes PGP Virtual Disk : AES-256, CAST et Twofish.

- AES (Advanced Encryption Standard) est le standard de chiffrement approuvé par le NIST. Le chiffrement sous-jacent est Rijndael, un chiffrement par blocs conçu par Joan Daemen et Vincent Rijmen. L'AES remplace le standard précédent, DES (Data Encryption Standard). Les volumes PGP Virtual Disk peuvent être protégés à l'aide de la variante plus performante d'AES, AES-256 (c'est-à-dire, AES avec une taille de clé de 256 bits).
- CAST est considéré comme un excellent chiffrement par blocs car il est rapide et très difficile à casser. Son nom est dérivé des initiales de ses concepteurs, Carlisle Adams et Stafford Tavares de Northern Telecom (Nortel). Nortel a déposé une demande de brevet pour CAST, mais la société s'est engagée à mettre CAST à la disposition de tous libre de droit. CAST semble être exceptionnellement bien conçu par des personnes bénéficiant d'une solide réputation dans le domaine.

  La conception est basée sur une approche très formelle, avec un nombre d'assertions formellement démontrables qui offrent de bonnes raisons de croire que pour casser sa clé 128 bits, il faudrait probablement un épuisement de celle-ci. CAST n'a pas de clés faibles. Il existe des arguments solides sur le fait que CAST est immunisé à la fois contre la cryptanalyse linéaire et la cryptanalyse différentielle, les deux formes les plus puissantes dans la documentation publiée, celles-ci étant toutes deux parvenues à craquer DES (Data Encryption Standard).
- Twofish est relativement récent, mais est un algorithme symétrique de chiffrement par blocs de 256 bits qui bénéficie d'une bonne réputation. C'est l'un des cinq algorithmes à avoir été envisagés par le NIST (U.S. National Institute of Standards and Technology) pour le nouveau standard de chiffrement avancé AES (Advanced Encryption Standard).

Précautions spéciales de sécurité prises par PGP Virtual Disk

À la différence d'autres programmes, PGP Desktop prend des précautions spéciales afin d'éviter des problèmes de sécurité avec les volumes PGP Virtual Disk.

Ces précautions s'appliquent également aux lecteurs chiffrés par WDE.

Effacement de la phrase secrète

Lorsque vous indiquez une phrase secrète, PGP Desktop l'utilise seulement un très court instant, puis l'efface de la mémoire. L'application ne fait en principe pas de copies de cette phrase. En conséquence, votre phrase secrète demeure généralement en mémoire pour une fraction de seconde. Cette fonctionnalité primordiale permet d'éviter à quiconque de rechercher votre phrase secrète dans la mémoire de votre ordinateur lorsque vous ne travaillez pas dessus. Si une telle situation se présentait, l'intrus aurait alors un accès complet aux données protégées par cette phrase secrète, bien que vous n'en soyez pas conscient.

Protection de la mémoire virtuelle

Votre phrase secrète ou d'autres clés risquent d'être enregistrées sur le disque lorsque le système de mémoire virtuelle y remplace de la mémoire. PGP Desktop veille à ce que cela ne se produise jamais. Cette fonctionnalité permet d'empêcher les intrus potentiels d'analyser le fichier de mémoire virtuelle en quête de phrases secrètes.

Mise en veille prolongée

Sous Windows, le mode Mise en veille prolongée écrit une image de l'intégralité du stockage de mémoire de votre ordinateur, dont les informations sur les PGP Virtual Disks, dans un fichier de votre disque dur. Si votre PGP Virtual Disk est ouvert lorsque vous appelez la mise en veille prolongée, des données sensibles seront écrites sur votre disque dur, dont la clé de session, mais *pas* votre phrase secrète.

Étant donné que la mise en veille prolongée est peu sûre par nature, PGP Corporation vous recommande d'utiliser PGP Whole Disk Encryption si vous utilisez cette fonction. Vous pouvez également activer les options PGP Virtual Disk **Démonter lorsque l'ordinateur se met en veille** et **Échec du mode veille si le démontage du disque ou des disques est impossible**, situées dans l'onglet Disque des options de PGP.

Protection de la migration d'ions statiques dans la mémoire

Lorsque vous montez un volume PGP Virtual Disk, votre phrase secrète est transformée en clé. Cette clé permet de déchiffrer et de chiffrer les données sur votre volume PGP Virtual Disk. Tandis que la phrase secrète est immédiatement effacée de la mémoire, la clé (dont votre phrase secrète ne peut pas être dérivée) reste en mémoire tant que le disque est monté.

Cette clé est protégée de la mémoire virtuelle ; cependant, si une zone spécifique de la mémoire stocke exactement les mêmes données pendant de très longues périodes sans être éteinte ou réinitialisée, cette mémoire tend à conserver une charge statique, qui pourrait être lue par des personnes malveillantes. Si votre volume PGP Virtual Disk reste monté pendant de longues périodes, avec le temps, des traces discernables de votre clé pourraient demeurer en mémoire. Des périphériques permettent de récupérer la clé. Cependant, vous ne les trouverez pas dans votre magasin d'électronique habituel, mais les principaux gouvernements sont susceptibles d'en posséder.

PGP Desktop se protège de cette faiblesse en conservant deux copies de la clé en RAM (une copie normale et une en bits inversés) et en les intervertissant très fréquemment.

Autres éléments de sécurité à prendre en compte

En général, votre capacité à protéger vos données dépend des précautions que vous prenez, et aucun programme de chiffrement ne peut vous protéger des négligences dans vos pratiques de sécurité. Par exemple, si vous quittez votre bureau en laissant des fichiers sensibles ouverts sur votre ordinateur, n'importe qui peut accéder à ces informations ou même obtenir la clé utilisée pour accéder aux données.

Voici quelques conseils vous permettant d'assurer une sécurité optimale :

- Démontez les volumes PGP Virtual Disk lorsque vous quittez votre ordinateur. De cette manière, leur contenu demeurera en sécurité dans le fichier chiffré associé au volume jusqu'à ce que vous y accédiez à nouveau.
- Utilisez un économiseur d'écran muni d'un mot de passe de sorte qu'il soit plus difficile pour quelqu'un d'accéder à votre ordinateur ou de voir votre écran quand vous vous éloignez de votre bureau.
- Veillez à ce que vos volumes PGP Virtual Disk ne puissent pas être vus par d'autres ordinateurs sur le réseau. Pour ce faire, il se peut que vous deviez faire appel aux personnes qui gèrent votre réseau. Les fichiers d'un volume PGP Virtual Disk monté sont accessibles par quiconque peut le voir sur le réseau.

- N'écrivez jamais vos phrases secrètes. Choisissez-en une dont vous pouvez vous rappeler. Si vous éprouvez des difficultés à vous souvenir de votre phrase secrète, utilisez un élément qui vous permettra de la retrouver facilement, comme un poster, une chanson, un poème, une blague, mais *n'écrivez pas vos phrases secrètes*.
- Si vous utilisez PGP Desktop à domicile et partagez votre ordinateur avec d'autres personnes, elles seront probablement en mesure de voir les fichiers de vos volumes PGP Virtual Disk. Tant que vous démonterez les volumes PGP Virtual Disk après les avoir utilisés, personne d'autre ne pourra lire leur contenu.
- Si un autre utilisateur peut accéder physiquement à votre ordinateur, il peut effacer vos fichiers PGP Virtual Disk, ainsi que d'autres fichiers ou volumes. Si l'accès physique pose problème, essayez de sauvegarder ou de conserver vos fichiers PGP Virtual Disk sur un périphérique externe sur lequel vous avez un contrôle physique exclusif.
- Sachez que les copies de votre volume PGP Virtual Disk utilisent la même clé de chiffrement sous-jacente que l'original. Si vous échangez une copie de votre volume avec quelqu'un d'autre et changez tous les deux vos mots de passe principaux, vous utiliserez toujours tous les deux la même clé pour chiffrer les données. Bien qu'une récupération de la clé ne soit pas à la portée du premier venu, elle n'est pas impossible.

  Vous pouvez modifier la clé sous-jacente en chiffrant de nouveau le volume.

12 Création de données mobiles et accès à celles-ci à l'aide de PGP Portable

PGP Portable vous permet de distribuer des fichiers chiffrés à des utilisateurs ne disposant pas du logiciel PGP Desktop. Grâce à ce logiciel, vous pouvez transférer en toute sécurité vos fichiers sur d'autres systèmes sur lesquels PGP n'est pas (ou ne peut pas être) installé.

PGP Portable apporte :

- une capacité de transfert de documents sécurisés ;
- une distribution facilitée de ce type de documents.

Deux types d'utilisateurs ont recours à PGP Portable : l'utilisateur qui crée le disque PGP Portable contenant les données sécurisées et l'utilisateur qui a besoin d'accéder à ces dernières, mais ne possède pas le logiciel PGP. Ces deux utilisateurs peuvent néanmoins n'en faire qu'un, par exemple lorsqu'une personne crée un disque PGP Portable portable qui pourra être utilisé sur un ordinateur sur le site d'un client.

Sur les systèmes Windows, vous pouvez créer des PGP Portable Disks et également accéder aux données chiffrées.

Contenu du chapitre

Création de disques PGP Portable

Vous pouvez créer des disques PGP Portable selon les deux méthodes suivantes : à l'aide d'un menu contextuel de l'Explorateur Windows ou à l'aide d'un utilitaire de ligne de commande. Cette section décrit l'utilisation normale d'un menu contextuel. Pour plus d'informations sur la ligne de commande, reportez-vous à la section Utilisation de l'utilitaire de ligne de commande PGP Portable.

Pour créer un disque PGP Portable, assurez-vous que vous disposez des éléments suivants :

- PGP Portable est installé sur un système Windows sur lequel s'exécute déjà PGP Desktop ;
- l'installation de PGP Desktop liée à un PGP Universal Server est dotée de la licence requise.

Vous pouvez créer un disque PGP Portable sur l'une des deux cibles suivantes :

- un dossier sur un lecteur local, une partie de fichier partagé à distance ou un CD/DVD ;
- un périphérique amovible monté localement, tel qu'un lecteur USB Flash, d'une capacité n'excédant pas 128 Go.

Lorsque vous créez un disque PGP Portable, la stratégie de PGP Universal Server impose également une limite de longueur à la phrase secrète. Si vous utilisez un phrase secrète qui ne respecte pas la stratégie de PGP Universal Server, un message d'erreur s'affiche.

Création d'un disque PGP Portable à partir d'un dossier

Lorsque vous voulez graver un CD ou un DVD contenant le disque PGP Portable, utilisez cette option.

Remarque : assurez-vous que vous avez copié les données que vous souhaitez protéger et partager dans le dossier.

Pour créer un disque PGP Portable à partir d'un dossier :

1. Localisez le dossier source, cliquez dessus avec le bouton droit, puis sélectionnez **Créer un dossier de disque PGP Portable** dans le menu contextuel.
2. Dans la boîte de dialogue Créer un disque PGP Portable, saisissez et confirmez la phrase secrète. Cette phrase secrète sera requise pour accéder aux données contenues dans le disque PGP Portable.
3. Cliquez sur **Créer**.
   - Si le dossier que vous utilisez pour créer le disque PGP Portable est un périphérique en lecture seule (tel qu'un CD ou un DVD), une boîte de dialogue Enregistrer sous s'affiche. Recherchez l'emplacement du lecteur local sur lequel vous voulez créer le dossier de destination du disque PGP Portable et cliquez sur **Enregistrer**.

   Le dossier de destination est alors créé. Le nom du dossier est le nom du dossier source suivi de « -PGP Portable ».
4. Gravez l'intégralité du contenu du dossier de destination sur le CD/DVD. Le dossier de destination du disque PGP Portable contient les éléments suivants :
   - le fichier exécutable Windows de PGP Portable (`pgpportable.exe`) ;

- les fichiers exécutables Mac OS X de PGP Portable (`PGP Portable App`) ;
- un fichier d'autoexécution Windows (`autorun.inf`) ;
- un fichier de disque PGP Portable (`pgpportable.pgd`).

Le fichier de disque PGP Portable (`pgpportable.pgd`) contient tous les fichiers trouvés dans le dossier cible d'origine. Le fichier de disque PGP Portable est chiffré avec la phrase secrète spécifiée.

Veillez à ne supprimer aucun de ces fichiers du disque PGP Portable.

Conseil : assurez-vous de graver uniquement le contenu du dossier sur le disque et non le dossier lui-même. Si vous gravez le dossier sur un disque, PGP Portable ne démarrera pas automatiquement sur les systèmes sur lesquels la fonction d'exécution automatique est activée.

Création d'un disque PGP Portable à partir d'un périphérique USB amovible

Lorsque vous créez le disque PGP Portable directement sur un périphérique USB amovible, tel qu'un lecteur Flash, utilisez cette option.

Remarque : La capacité du périphérique USB amovible doit être inférieure à 128 Go (137438953472 octets). Si vous tentez de créer un disque PGP Portable sur un périphérique USB amovible d'une capacité supérieure à 128 Go, vous recevrez un message d'erreur.

Pour créer un disque PGP Portable à partir d'un périphérique USB amovible :

1. Localisez le périphérique USB amovible monté, cliquez dessus avec le bouton droit, puis sélectionnez **Créer un disque PGP Portable** dans le menu contextuel.
2. L'application de création de disque PGP Portable s'affiche avec un avertissement indiquant que le contenu du lecteur sera effacé.
3. Dans la boîte de dialogue Créer un disque PGP Portable, saisissez et confirmez la phrase secrète. Cette phrase secrète sera requise pour accéder aux données contenues dans le disque PGP Portable.
4. Cliquez sur **Formater**. Le disque PGP Portable est alors créé. Le fichier de disque PGP Portable est chiffré avec la phrase secrète spécifiée.
5. Vous êtes invité à saisir la phrase secrète, puis le disque PGP Portable est monté. Un message s'affiche dans la zone de notification pour vous indiquer le numéro de lecteur du PGP Portable Disk monté.
6. Si vous le souhaitez, copiez les données que vous voulez protéger sur le disque PGP Portable monté. Le disque PGP Portable ne contient aucun fichier lors de sa création.

7 Démontez le disque PGP Portable (dans la zone de notification, cliquez sur l'icône de PGP Portable et sélectionnez **Démonter et quitter). Le lecteur monté pour le PGP Portable Disk est démonté.**

8 Éjectez correctement le périphérique USB et retirez-le de l'ordinateur. Vous avez à présent accès au contenu du disque PGP Portable sur un autre système qui prend en charge PGP Portable.

Avertissement : avant de retirer un périphérique USB du système, veillez à le démonter correctement. Sinon, vous risquez d'endommager le contenu des fichiers présents sur ce support.

Ce périphérique amovible contient les fichiers suivants :

- le fichier exécutable Windows de PGP Portable (`pgpportable.exe`) ;
- les fichiers exécutables Mac OS X de PGP Portable (`PGP Portable App`) ;
- un fichier d'autoexécution Windows (`autorun.inf`) ;
- le fichier de disque PGP Portable (`pgpportable.pgd`).

Veillez à ne supprimer aucun de ces fichiers du disque PGP Portable.

Création de disques PGP Desktop en lecture/écriture ou en lecture seule

L'accès en lecture/écriture à un disque PGP Desktop est possible uniquement si celui-ci réside sur un support accessible en lecture/écriture (tel qu'un lecteur Flash ou tout autre disque amovible). L'accès en lecture/écriture est activé pour un disque PGP Desktop uniquement si celui-ci réside sur le périphérique amovible sur lequel il a été créé.

- Les disques PGP Desktop créés sur des supports accessibles en lecture seule sont eux-mêmes accessibles en lecture seule (par exemple, les CD-ROM).
- L'accès aux disques PGP Desktop sur le périphérique sur lequel ils ont été créés s'effectue en lecture/écriture (par exemple, un lecteur USB qui est monté en accès lecture/écriture).

Accès aux données sur un disque PGP Portable

Pour accéder au contenu d'un disque PGP Portable, utilisez l'une des trois méthodes suivantes :

- Sous Windows, montez le CD, le DVD ou le lecteur USB amovible et exécutez l'application PGP Portable Disk (qui démarre automatiquement si la fonction d'exécution automatique est activée).

- Sous Mac OS X, montez le CD, le DVD ou le lecteur USB amovible et exécutez l'application PGP Portable Disk.

Lorsque vous accédez aux données d'un disque PGP Portable, n'oubliez pas que vous montez en réalité les deux éléments suivants : le périphérique amovible sur lequel réside le disque PGP Portable et le disque PGP Portable lui-même (monté en tant qu'élément distinct). Lorsque vous avez terminé, veillez à démonter le disque PGP Portable avant d'éjecter le périphérique amovible.

La procédure d'accès aux données d'un disque PGP Portable est similaire pour les systèmes Windows et Mac OS X.

Avertissement : avant de retirer physiquement un périphérique amovible du système, veillez à le démonter correctement. Sinon, vous risquez d'endommager le contenu des fichiers présents sur ce support.

Pour accéder aux données d'un PGP Portable Disk sur un système Windows

1. Insérez le périphérique amovible sur lequel réside le PGP Portable Disk. Il peut s'agir d'un CD/DVD, ou d'un lecteur Flash ou amovible.
2. Effectuez l'une des opérations suivantes :
   - Sur les systèmes Windows sur lesquels la fonction d'exécution automatique est activée, sélectionnez **Monter le PGP Portable Disk**.
   - Sur les systèmes Windows sur lesquels cette fonction est désactivée, ouvrez le périphérique amovible monté et recherchez l'application PGP Portable (`pgpportable.exe`). Double-cliquez sur cette application.
   - Sur les systèmes exécutés sous Windows 7, ouvrez le disque en double-cliquant sur l'icône de disque USB dans l'Explorateur Windows.

   La boîte de dialogue PGP Portable apparaît.

3. Saisissez la phrase secrète d'accès au PGP Portable Disk. Le PGP Portable Disk est monté.

   Un message s'affiche dans la zone de notification pour vous indiquer le numéro de lecteur du PGP Portable Disk monté. Si celui-ci est monté en tant que périphérique en lecture/écriture, vous pouvez y ajouter des données. S'il est monté en tant que périphérique en lecture seule, ce n'est pas le cas.

Remarque : le nom de volume du PGP Portable Disk est unique dans PGP Portable et peut être différent du nom du volume lors de sa création.

4 Lorsque vous avez fini d'utiliser le PGP Portable Disk, démontez-le (dans la zone de notification, cliquez sur l'icône PGP Portable, puis choisissez **Démonter et quitter**). Le lecteur monté pour le PGP Portable Disk est démonté.

5 Éjectez correctement le périphérique USB ou le disque de votre ordinateur.

Modification de la phrase secrète d'accès à un PGP Portable Disk

Il est parfois nécessaire de modifier la phrase secrète associée à un PGP Portable Disk. Remarque : vous ne pouvez pas modifier la phrase secrète sur les disques PGP Portable en lecture seule (notamment les disques PGP Portable gravés sur un CD/DVD).

▸ **Pour modifier la phrase secrète sur un disque PGP Portable sous Windows :**

1 Insérez le périphérique amovible sur lequel réside le PGP Portable Disk. Il peut s'agir d'un CD/DVD, ou d'un lecteur Flash ou amovible.

2 Effectuez l'une des opérations suivantes :

- Sur les systèmes Windows sur lesquels la fonction d'exécution automatique est activée, sélectionnez **Monter le PGP Portable Disk**.
- Sur les systèmes Windows sur lesquels cette fonction est désactivée, ouvrez le périphérique amovible monté et recherchez l'application PGP Portable (`pgpportable.exe`). Double-cliquez sur cette application.
- Sur les systèmes exécutés sous Windows 7, ouvrez le disque en double-cliquant sur l'icône de disque USB dans l'Explorateur Windows.

3 À l'invite, saisissez la phrase secrète d'accès au PGP Portable Disk. Le PGP Portable Disk est monté. Un message s'affiche dans la zone de notification pour vous indiquer le numéro de lecteur du PGP Portable Disk monté.

4 Ouvrez PGP Portable en cliquant avec le bouton droit sur l'icône de la zone de notification et choisissez **Ouvrir PGP Portable**.

5 Dans la boîte de dialogue PGP Portable, cliquez sur **Modifier la phrase secrète**.

6 Saisissez la phrase secrète actuelle, puis tapez et confirmez la nouvelle phrase secrète, et cliquez sur **Modifier**. La phrase secrète est modifiée.

L'indicateur de qualité de la phrase secrète donne une information de base sur le niveau de confidentialité de la phrase secrète créée. Pour plus d'informations, reportez-vous à la section *Indicateur de qualité de la phrase secrète* (à la page 336).

Démontage d'un disque PGP Portable

Avant de retirer physiquement un périphérique amovible du système, veillez à le démonter correctement. Sinon, vous risquez d'endommager le contenu des fichiers présents sur ce support.

Pour démonter un disque PGP Portable :

1. Ouvrez PGP Portable. Pour ce faire, procédez de l'une des manières suivantes :
   - Pour ouvrir PGP Portable sur un système Windows, cliquez avec le bouton droit sur l'icône de zone de notification et choisissez **Démonter et quitter.**
   - Pour ouvrir PGP Portable sur un système Mac OS, cliquez sur l'icône dans la station d'accueil et cliquez sur **Démonter et quitter.**

   Le disque PGP Portable est démonté.
2. Éjectez et retirez le périphérique de votre système en toute sécurité.

13 Utilisation de PGP NetShare

PGP NetShare permet un chiffrement bout en bout et transparent pour le stockage des fichiers partagés.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

À propos de PGP NetShare

PGP NetShare permet à des utilisateurs spécifiques de partager des fichiers protégés dans un espace partagé, tel que sur un serveur de fichiers d'entreprise, dans un dossier partagé, ou sur un support amovible de type lecteur USB.

Remarque : si les conditions ne vous permettent pas de disposer d'un espace partagé facilement accessible, l'utilisation d'un lecteur amovible USB est l'une des méthodes permettant de partager vos fichiers PGP NetShare.

Les fichiers sont protégés par chiffrement, mais continuent d'apparaître comme des fichiers d'applications normaux : Notepad, Microsoft Word, HTML, Microsoft Excel, etc. Les applications peuvent directement lire depuis et écrire sur les fichiers ; le fait que les fichiers soient protégés est transparent pour les applications. Toute autre personne ayant accès à l'espace partagé peut voir les fichiers, mais ne peut pas les lire ou les utiliser.

PGP NetShare étant un logiciel client exclusivement, son utilisation n'implique aucune installation supplémentaire sur le serveur de fichiers et il fonctionne avec votre infrastructure de stockage existante. Le chiffrement et le déchiffrement des dossiers et fichiers protégés s'exécutent uniquement sur le client. Les sauvegardes du serveur archiveront les fichiers chiffrés (texte chiffré) qui seront illisibles à toute personne non autorisée à les consulter.

Ceux qui ont accès aux fichiers protégés sont appelés *utilisateurs,* et les dossiers contenant les fichiers protégés sont appelés *dossiers protégés*.

Des rôles sont attribués aux utilisateurs et spécifient le type des actions qu'ils peuvent faire. Pour plus d'informations sur les rôles, reportez-vous à la section *Rôles PGP NetShare* (à la page 244).

Le dossier protégé est un dossier désigné pour contenir les fichiers protégés. Les fichiers d'un dossier converti en dossier protégé sont automatiquement chiffrés, alors que ceux déplacés dans un fichier protégé après sa création sont chiffrés lors de leur ajout. Vous pouvez également protéger des fichiers individuels en sélectionnant **Protéger les fichiers individuels** sous l'onglet NetShare du menu **Outils > Options de PGP.**

Attention : PGP NetShare n'offre *pas* de contrôle d'accès aux fichiers d'un dossier protégé. Le contrôle d'accès s'effectuant au niveau des fichiers, toute personne ayant accès aux fichiers d'un dossier protégé peut ajouter de nouveaux fichiers déchiffrés et/ou supprimer des fichiers chiffrés existants. Il est donc important que vous établissiez votre dossier protégé dans un espace partagé sécurisé, mais cela implique également que votre administrateur réseau puisse sauvegarder les fichiers dans le dossier protégé sans pouvoir les lire.

PGP NetShare est compatible avec les fonctionnalités PGP Virtual Disk et PGP Whole Disk Encryption de PGP Desktop. Par conséquent, vous pouvez créer un dossier protégé dans un PGP Virtual Disk ou si votre lecteur est chiffré par PGP WDE. La protection PGP NetShare est conçue pour les fichiers d'un environnement collaboratif partagé, généralement sur un réseau. PGP Virtual Disk et PGP Whole Disk Encryption protègent les lecteurs individuels ou les parties des lecteurs d'un système local. Il s'agit de trois produits de sécurité performants conçus pour être utilisés dans des situations légèrement différentes. En effet, vous pouvez les utiliser tous les trois sur le même système afin d'assurer une sécurité optimale de vos données.

L'exemple suivant vous permet de comprendre comment vous pouvez utiliser PGP NetShare :

> Supposons que vous êtes vice-président du département Finance d'une société de petite taille ayant deux gammes de produits principales. La présidente de la société vous fait venir dans son bureau et vous demande d'étudier si l'ajout d'une autre gamme de produits principale serait un succès.
>
> Elle souhaite que vous, ainsi que les représentants des départements Marketing, Vente, Ingénierie, Fabrication et Support examiniez la question sous tous ses aspects et fassiez une recommandation. L'ensemble du projet doit être confidentiel.
>
> Bien heureusement, tous les collaborateurs de votre société utilisent PGP Desktop dans un environnement géré par un PGP Universal Server, ainsi, la solution de création, de partage, de mise à jour et de stockage en toute sécurité des fichiers dont vous avez besoin est déjà en place : PGP NetShare.
>
> Les membres de votre projet étant physiquement dispersés, vous devez créer le dossier protégé du projet dans un emplacement accessible à chacun d'entre eux. À titre d'exemple, créer le dossier protégé sur le réseau d'entreprise permettrait à tous les membres du projet d'y accéder.
>
> Une fois celui-ci créé, ils pourront y ajouter de nouveaux fichiers, ouvrir et travailler sur des fichiers existants, ou supprimer des fichiers sans avoir à se soucier du fait qu'ils sont protégés par chiffrement, le chiffrement et le déchiffrement étant totalement transparents.

Un autre avantage de PGP NetShare est que les fichiers apparaissent normalement à tout utilisateur autorisé, permettant ainsi à votre administrateur réseau de les sauvegarder dans le dossier protégé de la même manière qu'il enregistre tous les autres fichiers sur le réseau d'entreprise. Les sauvegardes sont également protégées par chiffrement.

Remarque : le moteur de suivi de PGP NetShare ignore les objets protégés par EFS. Ceci permet d'éviter tout complication due au fait que EFS est étroitement lié à NTFS. Tous les fichiers ou dossiers chiffrés par EFS déplacés ou copiés dans un dossier protégé par PGP NetShare conservent leur chiffrement EFS, mais ne sont pas protégés par PGP NetShare. Pour que PGP NetShare protège ces objets, supprimez le chiffrement EFS avant de les déplacer/copier dans un dossier.

PGP NetShare assure la sécurité complète des fichiers d'un dossier protégé. Les données sont systématiquement chiffrées, même lorsqu'un dossier protégé est en cours d'accès ou de transfert depuis ou vers les membres du projet.

Attention : si vous sélectionnez l'option **Enregistrer sous** pour un fichier protégé et que vous l'enregistrez *hors* du dossier protégé, la nouvelle version ne sera *pas* protégée.

Rôles PGP NetShare

- **Administrateur** : il s'agit du « propriétaire » du dossier protégé. L'administrateur peut ajouter et supprimer des utilisateurs, ainsi que changer les rôles des utilisateurs et administrateurs de groupes. Il dispose de droits complets en lecture/écriture pour le dossier protégé. Il ne peut y avoir qu'un seul administrateur par dossier protégé ; ce dernier est créé automatiquement. Il n'est pas obligatoire de spécifier un administrateur manuellement. Chaque dossier ne compte qu'un seul administrateur.

  Vous devenez un administrateur en créant un dossier protégé, en vous ajoutant en tant que membre à ce dossier et en vous appliquant le rôle d'administrateur. Vous pouvez être membre de plusieurs ensembles d'administrateurs à la fois.

  Le rôle d'administrateur ne peut pas être supprimé par un administrateur de groupe, mais un administrateur peut affecter son rôle à un autre membre.

  Les administrateurs doivent disposer d'un accès complet en écriture au dossier protégé.

- **Administrateur du groupe** : il s'agit de l'« administrateur » du dossier protégé. L'administrateur de groupe peut ajouter et supprimer des utilisateurs, promouvoir des utilisateurs au rôle d'administrateur de groupe ou rétrograder des administrateurs de groupes au rôle d'utilisateur. Les administrateurs de groupe peuvent être aussi nombreux que nécessaire. Ils disposent de droits complets en lecture/écriture pour le dossier protégé. Il peut y avoir plusieurs administrateurs de groupes pour chaque dossier protégé PGP NetShare.

  Les administrateurs de groupes doivent disposer d'un accès complet en écriture au dossier protégé.

- **Utilisateurs** : il s'agit de l'ensemble des utilisateurs qui ont l'autorisation d'accéder aux fichiers protégés au sein de l'espace partagé. Les fichiers du dossier protégé sont chiffrés avec les clés des utilisateurs. Vous devenez un utilisateur lorsqu'un dossier protégé est créé, que vous êtes ajouté à PGP NetShare, et que l'administrateur ou l'administrateur du groupe vous affecte le rôle d'utilisateur. Tous les utilisateurs ont les mêmes droits en lecture/écriture sur le dossier protégé. Ils ne peuvent pas changer le rôle des autres utilisateurs. Vous pouvez être membre de plusieurs ensembles d'utilisateurs à la fois. Les utilisateurs ne sont pas habilités à déchiffrer des fichiers ou des dossiers. Cela permet d'éviter que les utilisateurs déchiffrent des fichiers, puis les chiffrent à nouveau lorsqu'un nouveau rôle leur a été affecté.

Remarque : si l'un de vos dossiers est protégé avec une version précédente de PGP Desktop, vous devez sélectionner manuellement de nouveaux rôles pour les utilisateurs existants. Pour plus d'informations, reportez-vous à la section *Modification du rôle d'un utilisateur* (à la page 260).

Gestion des licences de PGP NetShare

Pour utiliser PGP NetShare, vous devez exécuter PGP Desktop 9.5 ou une version ultérieure ou avoir une licence qui prend en charge PGP NetShare.

Pour vérifier si votre copie de PGP Desktop prend en charge PGP NetShare

1. Ouvrez PGP Desktop.
2. Sélectionnez **Aide > Licence**. La boîte de dialogue contenant la licence PGP Desktop apparaît.
3. Dans la section **Informations produit**, recherchez l'icône **PGP NetShare**. Positionnez le curseur sur le nom du produit pour afficher des informations sur celui-ci et savoir si vous disposez d'une licence vous permettant de l'utiliser. Si PGP NetShare n'est pas pris en charge, contactez votre administrateur PGP pour obtenir une licence appropriée.

Si vous avez créé un ou plusieurs dossiers protégés avec une licence PGP NetShare qui a maintenant expiré, vous ne pourrez pas créer d'autres dossiers protégés, utiliser les fichiers se trouvant actuellement dans les dossiers protégés, ajouter des fichiers à ces dossiers ni être ajouté en tant qu'utilisateur autorisé d'un nouveau dossier protégé.

Pour accéder à nouveau aux versions déchiffrées des fichiers d'un dossier protégé, vous devez soit obtenir une nouvelle licence PGP NetShare, soit déchiffrer les fichiers/dossiers de vos dossiers protégés à l'aide de la commande **Supprimer <file name> de PGP NetShare** (pour plus d'informations, reportez-vous à la section *Accès aux fonctionnalités de PGP NetShare à l'aide du menu contextuel* (à la page 269)).

Clés des utilisateurs autorisés

PGP NetShare utilise les clés PGP des utilisateurs que vous désignez pour contrôler l'accès aux fichiers déchiffrés dans le dossier protégé, et utilise les clés privés des utilisateurs autorisés pour signer les nouveaux fichiers qui sont ajoutés au dossier protégé.

Remarque : PGP NetShare ne prend pas en charge l'utilisation de phrases secrètes pour protéger des fichiers. Pour ce faire, des clés PGP doivent être utilisées.

Lorsqu'un ensemble d'utilisateurs est créé, son créateur spécifie les clés publiques des utilisateurs qui pourront utiliser les fichiers du dossier protégé. Pour utiliser ces fichiers, les utilisateurs doivent disposer de la clé correspondante sur leur système afin d'obtenir un accès déchiffré à ces fichiers.

Désignation d'un administrateur PGP NetShare (propriétaire)

Bien qu'un administrateur PGP NetShare ne soit pas obligatoire pour un dossier partagé, vous pouvez en désigner un parmi les utilisateurs autorisés ou les administrateurs du groupe. Il lui incombera de surveiller les fichiers et les dossiers du dossier protégé, d'ajouter et de supprimer des utilisateurs et administrateurs du groupe, et de s'assurer que l'activité dans le dossier protégé se déroule comme prévu.

Tous les utilisateurs autorisés pouvant ajouter ou supprimer des fichiers, des dossiers et (dans certains cas) des utilisateurs, il est possible qu'avec le temps, des fichiers ou des utilisateurs soient ajoutés ou supprimés de manière inappropriée du dossier protégé.

L'administrateur d'un dossier protégé doit surveiller les utilisateurs et le dossier protégé afin de rechercher ces problèmes éventuels et les résoudre.

Fichiers, dossiers et applications « sur liste noire » et « sur liste blanche »

Certains fichiers, dossiers et applications peuvent figurer « sur liste noire » ou « sur liste blanche ». Ces éléments sont soit toujours protégés, soit jamais protégés.

Fichiers sur liste noire ou autres fichiers impossibles à protéger

PGP NetShare ne vous permet pas de protéger certains fichiers ou dossiers. Avant d'être protégé par PGP NetShare, un fichier ou dossier est vérifié par rapport à cette liste connue sous le nom de « liste noire ». Si un fichier ou dossier est identifié comme étant sur liste noire, PGP NetShare poursuit la création du dossier protégé, mais le fichier et/ou dossier est ignoré et un message indiquant que l'élément est sur liste noire s'affiche dans l'écran Progression de l'assistant de PGP NetShare.

Les fichiers sur liste noire sont les suivants :

- Tous les fichiers d'extension `*.skr`, `*.pkr` et `*.pgd`, afin de vous empêcher de chiffrer vos clés ou les PGP Virtual Disks.
- Le dossier d'installation de PGP Desktop et tous les fichiers qu'il contient (par défaut, ce dossier se trouve à l'emplacement suivant : `C:\Program Files\PGP Corporation\PGP Desktop`).
- Le dossier Préférences de PGP et tous les fichiers qu'il contient (par défaut, ce dossier se trouve dans votre dossier utilisateur à l'emplacement suivant : `C:\Documents and Settings\[votre nom d'utilisateur]\Application Data\PGP Corporation\PGP`).
- Le dossier de trousseau de clés par défaut de PGP (par défaut, le trousseau de clés se trouve dans le dossier Mes documents).

Les autres fichiers que PGP NetShare empêche d'ajouter aux dossiers protégés sont les fichiers ou dossiers dont l'attribut System est défini, tous les fichiers et dossiers du répertoire d'installation de Windows (par défaut, `C:\Windows` et `C:\Windows\System32`), ainsi que le fichier `Thumbs.db` créé lors de l'affichage des graphiques miniatures dans l'Explorateur Windows. Lors de l'ajout de ce type de fichier ou dossier à PGP NetShare, le fichier et/ou dossier est ignoré et un message indiquant que l'élément est un fichier ou dossier système s'affiche dans l'écran Progression de l'assistant de PGP NetShare.

Dossiers « sur liste noire » et « sur liste blanche » spécifiés par le PGP Universal Server

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, l'administrateur PGP peut avoir placé certains dossiers « sur liste noire » ou « sur liste blanche ».

Dossiers sur liste noire

Les dossiers sur liste noire ne sont *jamais* ajoutés à PGP NetShare, ni chiffrés. Vos dossiers `C:\Program Files` et `C:\Windows\Temp` sont des exemples de dossiers sur liste noire. Si l'administrateur PGP indique qu'un dossier doit figurer sur liste noire et que ce dossier n'existe pas, il n'est pas créé sur votre système.

Remarque : les dossiers ou les fichiers protégés par PGP NetShare ne sont pas déchiffrés automatiquement s'ils figurent sur liste noire (par la stratégie PGP Universal Server). Pour supprimer la protection de PGP NetShare, vous devez déchiffrer manuellement le dossier ou le fichier. Tous les nouveaux objets ajoutés à un dossier sur liste noire protégé ne reçoivent pas de chiffrement PGP NetShare.

Dossiers sur liste blanche

Les dossiers sur liste blanche sont *systématiquement* ajoutés à PGP NetShare et leur contenu est chiffré. Si l'administrateur PGP indique qu'un dossier doit figurer sur liste blanche et que ce dossier n'existe pas, il est créé sur votre système. Ainsi, si l'administrateur PGP indique que `C:\Documents and Settings\[nom utilisateur]\Mes documents\sécurisé` est un dossier sur liste blanche, et que le sous-dossier `\sécurisé` n'existe pas, il est créé. Vous ne pouvez pas supprimer les dossiers sur liste blanche de PGP NetShare.

Remarque : si vous supprimez un dossier que l'administrateur de PGP Universal a spécifié comme figurant sur la liste blanche, ce dossier est automatiquement recréé lors de l'accès suivant à PGP NetShare ou du redémarrage de PGP Desktop.

Listes de contournement de chiffrement/déchiffrement en fonction de l'application

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir classé certaines applications de façon à ce que les fichiers créés par ces applications ne soient jamais déchiffrés ou soient toujours chiffrés.

Liste de chiffrement en fonction de l'application

Les applications de cette liste sont les applications dans lesquelles les fichiers créés sont systématiquement chiffrés. Les fichiers créés par les applications figurant dans la liste de chiffrement en fonction de l'application sont automatiquement chiffrés avec votre clé et restent chiffrés où qu'ils se trouvent, notamment les fichiers temporaires et les caches système. Microsoft Office, Microsoft Excel et Adobe Acrobat sont des exemples de types d'applications susceptibles de figurer dans cette liste.

D'autres types de chiffrement (par exemple, les dossiers sur liste blanche) ont la priorité sur les fichiers créés par les applications de la liste de chiffrement en fonction de l'application.

Votre administrateur PGP peut spécifier que Microsoft Excel figure dans les listes de chiffrement en fonction de l'application afin que toutes les feuilles de calcul créées par votre service financier soient protégées.

Liste de contournement de déchiffrement

Les applications de cette liste sont les applications dans lesquelles les fichiers créés ne sont pas automatiquement déchiffrés. Ces applications reçoivent le contenu des fichiers du disque, notamment le texte chiffré de fichier et d'en-tête PGP NetShare. Les applications de la liste de contournement de déchiffrement contournent en fait le filtre PGP NetShare lors de la lecture du fichier. Les fichiers restent donc chiffrés en lecture, ce qui permet à ces applications de passer les données chiffrées à d'autres applications. Les programmes de sauvegarde et FTP sont des exemples de types d'applications pouvant figurer dans cette liste.

D'autres types de chiffrement (par exemple, les dossiers sur liste noire) ont la priorité sur les fichiers créés par les applications de la liste de contournement de déchiffrement.

L'administrateur PGP peut placer votre programme de sauvegarde d'entreprise dans la liste de contournement de déchiffrement. Tous les fichiers de sauvegarde créés par cette application sont protégés et le chiffrement est préservé lorsque le fichier de sauvegarde est transféré en un autre emplacement.

Utilisation des dossiers protégés

Le dossier protégé est un dossier désigné pour contenir les fichiers protégés. Les fichiers d'un dossier converti en dossier protégé sont automatiquement chiffrés, alors que ceux déplacés vers un dossier protégé après sa création sont chiffrés lors de leur ajout. Vous pouvez également protéger des fichiers individuels en sélectionnant **Protéger les fichiers individuels** sous l'onglet NetShare du menu **Outils > Options de PGP**.

À partir de PGP NetShare version 9.10, les dossiers stockés sur les serveurs Web qui prennent en charge le protocole WebDAV, tels que Microsoft SharePoint, peuvent être protégés par PGP NetShare. Remarque : certains types de fichier, comme les fichiers `.mht`, sont requis pour que SharePoint fonctionne correctement et, lorsqu'ils sont utilisés à cette fin, ne peuvent pas être chiffrés par PGP NetShare. Pour des détails techniques sur la protection de fichiers SharePoint, consultez l'*article 1120 de la base de connaissances du support de PGP Corporation* (http://support.pgp.com/?faq=1120).

Lorsque vous utilisez PGP NetShare avec Sharepoint, veillez à définir l'option de demande d'extraction **sur Non** pour le site Sharepoint. Tous les utilisateurs autorisés peuvent alors accéder à l'ensemble des fichiers gérés par le dossier PGP NetShare.

Conseil : assurez-vous d'appliquer une stratégie de sauvegarde appropriée et de sauvegarder régulièrement tous les dossiers protégés PGP NetShare.

Sélection de l'emplacement d'un dossier protégé

PGP Corporation vous recommande de créer votre dossier protégé PGP NetShare dans un espace accessible à tous les utilisateurs autorisés, mais qui est protégé des autres.

Bien que vous puissiez créer le dossier protégé dans un espace accessible au public, n'oubliez pas que PGP NetShare n'offre *pas* de contrôle d'accès aux fichiers d'un dossier protégé.

Ce que vous faites avec les fichiers d'un dossier protégé et les personnes qui peuvent y accéder a une incidence sur la protection qu'assure PGP NetShare. Tenez compte des conditions suivantes lors de la sélection de l'emplacement d'un dossier protégé PGP NetShare.

- *Utilisation normale* (à la page 250)
- *Accès aux fichiers* (à la page 251)
- *Accès direct au texte chiffré* (cf. "Accès direct aux données chiffrées (texte chiffré)" à la page 251)
- *Fichiers protégés altérés, supprimés ou écrasés* (à la page 251)
- *Fichiers sur liste noire ou autres fichiers impossibles à protéger* (à la page 247)

Utilisation normale

Dans des conditions d'utilisation normale par un utilisateur autorisé, PGP NetShare protège totalement les fichiers d'un dossier protégé. Par « utilisation normale » on entend ouverture d'un fichier protégé, application de modifications, puis enregistrement de celui-ci ; création d'un nouveau fichier dans un dossier protégé ; ou déplacement ou copie d'un fichier dans un dossier protégé.

Lorsqu'un fichier est déplacé ou copié hors d'un dossier protégé PGP NetShare, PGP NetShare tente d'en assurer la protection. Cela vous permet de copier des fichiers d'un dossier protégé vers un lecteur USB par exemple, et de conserver leur protection. Si vous déplacez ou copiez un fichier hors d'un dossier protégé, vous devez systématiquement vérifier que le fichier de destination est toujours protégé en recherchant l'indicateur de verrouillage visuel ou en examinant les propriétés du fichier.

Accès aux fichiers

Chaque application que vous utilisez aura un accès total aux données déchiffrées de vos fichiers protégés par PGP NetShare. Cela inclut d'autres applications PGP Corporation, telles que PGP Zip. Par conséquent, si vous créez une archive PGP Zip et incluez un fichier protégé par PGP NetShare, l'archive PGP Zip contiendra une version déchiffrée du fichier.

Sachez également que si vous sélectionnez l'option **Enregistrer sous** pour un fichier protégé et que vous l'enregistrez *hors* du dossier protégé, la nouvelle version ne sera *pas* protégée.

Accès direct aux données chiffrées (texte chiffré)

Il est possible dans certains cas de contourner PGP NetShare, et d'accéder ainsi directement aux données chiffrées (ou texte chiffré) d'un fichier.

Cela permet aux fichiers protégés sur un serveur d'être, par exemple, sauvegardés, déplacés, copiés ou mis sur FTP par un utilisateur (tel que l'administrateur réseau) bénéficiant d'un accès physique aux fichiers protégés, mais ne disposant pas de PGP Desktop. Dans ces cas, le texte chiffré des fichiers protégés sera sauvegardé, déplacé, copié ou mis sur FTP.

Fichiers protégés altérés, supprimés ou écrasés

PGP NetShare n'offre *pas* de contrôle d'accès aux fichiers. Même si des utilisateurs sans autorisation appropriée ne peuvent pas ouvrir les fichiers des dossiers protégés, il est toujours possible qu'ils y accèdent. Cela signifie que même la protection des fichiers à l'aide PGP NetShare ne garantit en rien qu'ils ne pourront pas être altérés, supprimés ou écrasés par les utilisateurs qui y accèdent. PGP NetShare protège le contenu d'un fichier, mais pas le fichier lui-même.

Nous vous recommandons vivement de conserver des contrôles d'accès aux fichiers performants, outre le contrôle d'accès cryptographique et la protection assurée par PGP NetShare.

Création d'un dossier protégé PGP NetShare

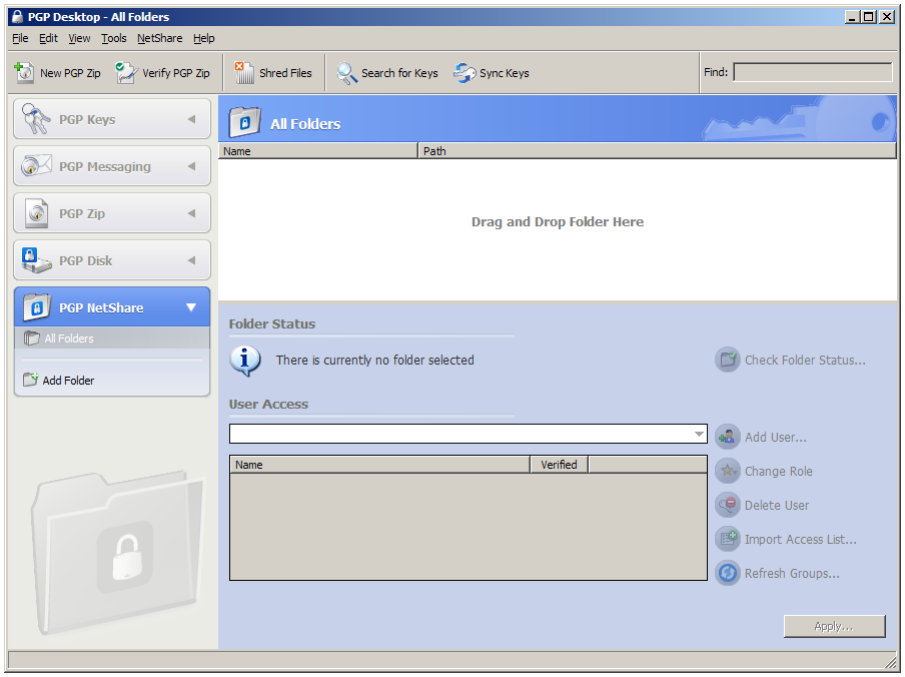
Le dossier protégé est le dossier qui contient les fichiers protégés par PGP NetShare.

Conseil : lorsque vous créez un dossier protégé PGP NetShare, les dates de dernière modification des fichiers qu'il contient déjà passent à la date de l'opération PGP NetShare. Pour conserver les dates de modification, créez *d'abord* un dossier PGP NetShare, *puis* ajoutez-y les fichiers.

Remarque : vous devez disposer des autorisations en écriture pour pouvoir créer un dossier protégé PGP NetShare.

Pour créer un dossier protégé PGP NetShare

1 Ouvrez PGP Desktop et cliquez sur le panneau de contrôle PGP NetShare. La zone de travail de PGP NetShare s'affiche.



2 Effectuez l'une des opérations suivantes :

- Faites glisser le dossier qui sera le dossier protégé vers le champ intitulé « Faites un glisser-déplacer des dossiers ici », ce qui a pour effet d'ouvrir l'assistant de PGP NetShare et de passer outre l'étape d'indication du dossier protégé.
- Cliquez sur **Ajouter un dossier** dans le panneau de contrôle PGP NetShare ou sélectionnez **NetShare > Ajouter un dossier**. L'écran Sélectionner le dossier de l'assistant de PGP NetShare s'affiche.
  - Cliquez sur **Parcourir**. La boîte de dialogue Rechercher un dossier s'affiche.
  - Naviguez vers le dossier contenant les fichiers à inclure dans le dossier protégé que vous créez. Pour créer un dossier vide dans lequel vous placerez les fichiers à inclure dans le dossier protégé, cliquez sur **Nouveau dossier**.
  - Cliquez sur **OK** pour fermer la boîte de dialogue **Rechercher un dossier**. L'écran **Sélectionner le dossier** s'affiche à nouveau.
- (Facultatif) Dans le champ **Description**, saisissez une description pour le dossier protégé que vous créez.

3 Cliquez sur **Suivant**. L'écran Ajouter des utilisateurs s'affiche.

4 Pour ajouter des utilisateurs pour le dossier protégé que vous créez, cliquez sur l'icône avec la flèche vers le bas. La liste des clés faisant partie de votre trousseau apparaît.

5 Sélectionnez un utilisateur, puis cliquez sur **Ajouter**.

Remarque : pour pouvoir accéder au contenu du dossier protégé, n'oubliez pas d'ajouter votre propre clé, sans quoi vous ne pourrez pas utiliser les fichiers qu'il contient.

Pour ajouter également des utilisateurs autorisés, cliquez sur **Ajouter**. La boîte de dialogue Sélection d'utilisateurs s'affiche.

6 Effectuez l'une des opérations suivantes :

- Faites glisser des clés de la colonne **Source de clé** dans la colonne **Clés à ajouter**.
- Cliquez sur une clé dans la colonne **Source de clé**, puis sur **Ajouter**.
- Double-cliquez sur une clé dans la colonne **Source de clé**.
- Pour ajouter des clés provenant du serveur PGP Global Directory, cliquez sur l'icône PGP Global Directory, saisissez un terme à rechercher dans le champ **Rechercher**, puis cliquez sur la loupe pour lancer la recherche. Les résultats de la recherche apparaissent dans la colonne **Source de clé** ; faites-les glisser de cette colonne dans la colonne **Clés à ajouter**.

Remarque : PGP NetShare n'informe pas automatiquement les nouveaux membres qu'ils ont été ajoutés à un dossier protégé en tant qu'utilisateurs autorisés. En général, il incombe au créateur d'un dossier protégé d'informer les membres que le dossier protégé a été créé et qu'ils sont utilisateurs autorisés.

7 Cliquez sur **OK** lorsque vous avez terminé. L'écran **Ajouter des utilisateurs** s'affiche à nouveau.

8 Pour attribuer un rôle à chaque utilisateur, cliquez avec le bouton droit sur son nom et sélectionnez le rôle souhaité :

- **Administrateur** : créez un seul administrateur par dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture, permet d'ajouter et de supprimer des utilisateurs, d'attribuer des rôles à d'autres utilisateurs et de promouvoir un autre utilisateur au rôle d'administrateur.
- **Administrateur du groupe** : créez autant d'administrateurs du groupe que nécessaire pour chaque dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture, permet d'ajouter et de supprimer des utilisateurs, ainsi que d'attribuer des rôles à d'autres utilisateurs.

- **Utilisateur** : créez autant d'utilisateurs que nécessaire pour chaque dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture pour le dossier.

Vous pouvez modifier le rôle d'un utilisateur à tout moment après la création du dossier protégé. Cliquez sur le dossier protégé dans PGP Desktop, puis cliquez avec le bouton droit sur le nom de l'utilisateur afin de modifier le rôle.

9 Cliquez sur **Suivant**. L'écran Sélectionner le signataire s'affiche.

10 Sélectionnez une clé dans les clés privées du trousseau local. Cette clé permettra de signer les fichiers qui sont protégés par chiffrement dans le dossier protégé.

11 Saisissez la phrase secrète **pour la clé.**

12 Cliquez sur **Suivant**. L'écran Progression s'affiche.

Les fichiers du dossier protégé spécifié sont chiffrés et les utilisateurs désignés sont ajoutés en tant qu'utilisateurs autorisés.

Remarque : si vous annulez le processus de chiffrement, les fichiers qui ont déjà été chiffrés le restent. Pour savoir comment leur redonner leur forme non chiffrée initiale, reportez-vous à la section *Suppression d'un dossier* (cf. "Déchiffrement de dossiers protégés PGP NetShare" à la page 264).

13 Une fois que le processus est achevé, cliquez sur **Terminer**.

Utilisation des fichiers dans un dossier protégé PGP NetShare

Une fois que vous êtes utilisateur protégé PGP NetShare, vous pouvez utiliser les fichiers du dossier protégé de trois manières :

- Double-cliquez sur le dossier protégé pour l'ouvrir, puis sur le fichier spécifique à utiliser.
- Ouvrez le fichier à utiliser à partir de l'application qui l'a créé.
- Ouvrez le dossier protégé en cliquant sur son chemin d'accès (s'affiche sous forme de lien hypertexte), puis double-cliquez sur le fichier spécifique à utiliser.

Si la phrase secrète d'une clé privée utilisée pour être membre du fichier protégé PGP NetShare est en cache sur votre système, vous n'avez rien d'autre à faire pour ouvrir les fichiers, car ils s'ouvriront automatiquement.

Cependant, si votre phrase secrète n'est pas en cache, le dossier protégé est verrouillé. Vous devrez vous authentifier avant de pouvoir ouvrir les fichiers dans le dossier protégé. Pour plus d'informations, reportez-vous à la section *Déverrouillage d'un dossier protégé* (à la page 255).

Remarque : lorsque vous ouvrez un document de texte protégé par PGP NetShare à l'aide du Bloc-notes sous Windows Vista, vous recevez deux notifications indiquant que le fichier en question est en cours de déverrouillage. Ce comportement résulte de la méthode par laquelle le Bloc-notes accède au fichier.

Déverrouillage d'un dossier protégé

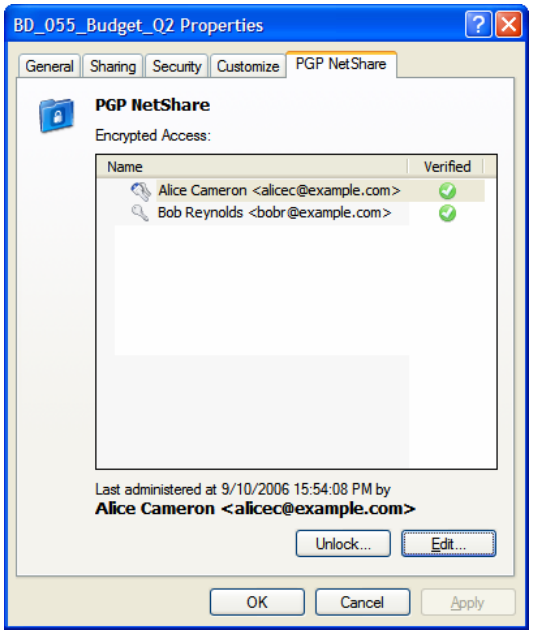
Utilisez le bouton **Déverrouiller** pour accéder à un dossier auquel vous semblez ne pas pouvoir accéder, mais que vous pensez être capable de déverrouiller, ou si un dossier requiert un déverrouillage manuel. Vous devez déverrouiller manuellement un dossier protégé lorsqu'il est verrouillé pour l'une des raisons suivantes :

- Le temporisateur de la boîte de dialogue d'invite Phrase secrète arrive à expiration.
- Vous cliquez sur **Annuler** dans la boîte de dialogue Phrase secrète sans saisir de phrase secrète valide.

Toute tentative ultérieure d'accès au dossier protégé se traduit par l'affichage d'une boîte de dialogue Accès refusé, et vous devez déverrouiller chaque dossier protégé avant de pouvoir utiliser les fichiers qu'il contient.

Pour déverrouiller un dossier protégé

1. Cliquez avec le bouton droit sur le dossier protégé et sélectionnez **PGP Desktop > Propriétés PGP NetShare**.
2. L'onglet Propriétés PGP NetShare s'affiche.



3 Cliquez sur **Déverrouiller**. La boîte de dialogue de déverrouillage **s'affiche.**

4 Saisissez la phrase secrète appropriée, puis cliquez sur **OK**. La boîte de dialogue de déverrouillage disparaît. Votre phrase secrète est mise en cache et vous avez accès à tous les fichiers du dossier protégé.

Remarque : si votre administrateur PGP Universal Server l'a activée, vous pouvez sélectionner l'option **Nouvelle recherche de verrouillages NetShare** dans le menu de la zone de notification PGP. Cette option vous permet de déverrouiller un dossier protégé PGP NetShare lorsque votre clé se trouve sur une carte à puce ou un jeton qui n'a pas été inséré au moment de la tentative d'accès au dossier.

Détermination des fichiers d'un dossier protégé

Lorsque vous devenez utilisateur autorisé, vous disposez d'un accès complet à tous les fichiers du dossier protégé. Si vous créez le dossier protégé, vous saurez probablement quels fichiers il contient. Toutefois, si vous avez été ajouté au dossier protégé par un autre membre, il se peut que vous ne sachiez pas immédiatement les fichiers qu'il contient.

▸ **Pour déterminer les fichiers d'un dossier protégé :**

1 Ouvrez PGP Desktop et cliquez sur la boîte de contrôle PGP NetShare.

2 Cliquez sur le chemin d'accès vers le dossier protégé (s'affiche sous forme de lien hypertexte). Le contenu du dossier protégé apparaît dans une nouvelle fenêtre qui présente les fichiers et dossiers du dossier protégé.

Si l'accès est refusé, cela signifie que le dossier protégé est verrouillé. Vous devrez accéder à l'onglet PGP NetShare de l'écran Propriétés du dossier verrouillé et le déverrouiller, ou redémarrer votre système pour y accéder. Pour plus d'informations sur le déverrouillage d'un dossier protégé, reportez-vous à la section *Utilisation des fichiers dans un dossier protégé PGP NetShare* (à la page 254).

Ajout de sous-dossiers à un dossier protégé

PGP NetShare prend en charge l'ajout de fichiers et de dossiers à un dossier protégé une fois celui-ci créé.

L'ensemble des fichiers d'un dossier que vous ajoutez à un dossier protégé seront automatiquement protégés ; une fois ajoutés au dossier protégé, le dossier et les fichiers qu'il contient seront uniquement accessibles aux utilisateurs autorisés.

Assurez-vous de ne pas ajouter de dossier qui soit déjà un dossier protégé pour un autre ensemble d'utilisateurs autorisés. Le nouveau sous-répertoire aurait un ensemble d'utilisateurs autorisés différent du dossier parent.

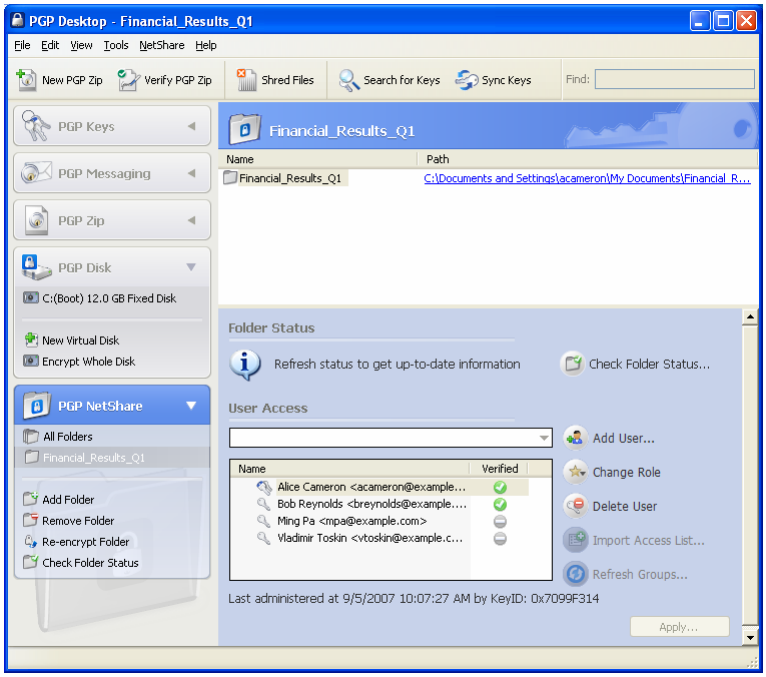
Remarque : le moteur de suivi de PGP NetShare ignore les objets protégés par EFS. Ceci permet d'éviter tout complication due au fait que EFS est étroitement lié à NTFS. Tous les fichiers ou dossiers chiffrés par EFS déplacés ou copiés dans un dossier protégé par PGP NetShare conservent leur chiffrement EFS, mais ne sont pas protégés par PGP NetShare. Pour que PGP NetShare protège ces objets, supprimez le chiffrement EFS avant de les déplacer/copier dans un dossier.

Vérification de l'état du dossier

La commande **Vérifier l'état du dossier**, disponible à partir de la zone de travail du dossier NetShare, du panneau de contrôle PGP NetShare ou du menu NetShare, fournit des informations à jour sur l'état du dossier PGP NetShare spécifié.

Pour vérifier l'état d'un dossier dans un dossier protégé

1 Dans la zone de travail de PGP NetShare, sous la section État du dossier, cliquez sur **Vérifier l'état du dossier**. Vous devez avoir sélectionné un dossier PGP NetShare.



2 Lisez le texte à gauche du bouton **Vérifier l'état du dossier** pour connaître l'état du dossier sélectionné (par exemple : « Tous les dossiers et fichiers sont chiffrés »).

Conseil : la date, l'heure et l'ID de clé de la dernière personne à avoir administré le dossier protégé s'affichent au-dessous de la liste des utilisateurs.

Copie des dossiers protégés vers d'autres emplacements

Vous obtiendrez une sécurité optimale si vous travaillez systématiquement dans un dossier protégé ; si vous devez copier un dossier, PGP Corporation vous recommande de créer au préalable un dossier protégé de destination. Chaque fois que vous déplacerez des fichiers d'un dossier protégé vers un autre, votre environnement restera protégé.

PGP NetShare conserve le chiffrement des fichiers même lorsque le dossier protégé est déplacé vers un autre emplacement. Cependant, selon la méthode utilisée pour copier les fichiers et l'emplacement sélectionné, il se peut que le processus entraîne la perte de la protection du *dossier*. Les fichiers du dossier conservent leur état protégé, mais le dossier peut perdre ses informations PGP NetShare, et donc son icône PGP également.

Si vous avez copié un dossier vers un emplacement non protégé, nous vous recommandons de vérifier l'état du dossier tel que décrit dans la section *Vérification de l'état du dossier* (à la page 257) afin de vous assurer que le dossier et les fichiers sont chiffrés.

Si le dossier n'est pas chiffré, procédez comme suit :

1. Si vos autorisations PGP NetShare le permettent, créez un nouveau dossier protégé au niveau de la destination tel que décrit dans la section *Création d'un dossier protégé PGP NetShare* (à la page 251).
2. Copiez le contenu du dossier ayant perdu sa protection dans le nouveau dossier protégé.
3. Importez la liste d'accès de l'ancien dossier dans le nouveau tel que décrit dans la section *Importation des listes d'accès PGP NetShare* (à la page 262).

Gestion des utilisateurs de PGP NetShare

Toute personne disposant de PGP Desktop 9.5 ou version ultérieure qui possède une paire de clés appropriée dans PGP Desktop peut être utilisateur d'un dossier protégé PGP NetShare.

Les paires de clés peuvent être :

- créées dans PGP Desktop ;
- créées par une application OpenPGP et importées dans PGP Desktop ;
- un certificat X.509 qui a été importé dans PGP Desktop.

Il existe deux manières de devenir utilisateur :

- Vous pouvez créer un dossier protégé à l'aide de PGP Desktop et vous ajouter vous-même en tant qu'utilisateur.
- Un membre existant peut vous ajouter en tant qu'utilisateur.

Une fois que vous devenez utilisateur, vous disposez des mêmes droits que tous les autres.

Ajout d'un utilisateur de PGP NetShare

La plupart des utilisateurs de PGP NetShare sont ajoutés lors de la création du dossier protégé, mais vous pouvez ajouter des membres à tout moment après sa création à condition d'être administrateur ou administrateur du groupe de ce dossier protégé.

Attention : soyez prudent lorsque vous ajoutez une personne en tant qu'utilisateur à PGP NetShare. Une fois cette personne ajoutée, elle dispose de tous les droits et privilèges comme tout autre utilisateur. Ce nouveau membre peut ajouter de nouveaux fichiers au, ou supprimer des fichiers existants du, dossier protégé.

Pour ajouter un nouvel utilisateur de PGP NetShare

1. Sélectionnez le dossier PGP NetShare auquel vous souhaitez ajouter un nouveau membre.
2. Dans la section Accès de l'utilisateur, cliquez sur **Ajouter un utilisateur**. La boîte de dialogue Sélection d'utilisateurs s'affiche.
3. Effectuez l'une des opérations suivantes :
   - Faites glisser des clés de la colonne **Source de clé** dans la colonne **Clés à ajouter**.
   - Cliquez sur une clé dans la colonne **Source de clé**, puis sur **Ajouter**.
   - Pour ajouter des clés à partir de PGP Global Directory, cliquez sur l'icône PGP Global Directory, saisissez un terme à rechercher dans le champ **Rechercher**, puis cliquez sur la loupe ou appuyez sur **Entrée** pour lancer la recherche. Les résultats de la recherche apparaissent dans la colonne **Source de clé** ; faites-les glisser de cette colonne dans la colonne **Clés à ajouter**.

   Remarque : PGP NetShare n'informe pas les nouveaux membres qu'ils ont été ajoutés en tant qu'utilisateurs autorisés. En général, il incombe à la personne qui ajoute un nouvel utilisateur de l'en informer.
4. Cliquez sur **OK**. L'utilisateur est ajouté à la liste.
5. Cliquez sur **Appliquer**. L'écran Sélectionner le signataire s'affiche.

6 Sélectionnez une clé dans les clés privées du trousseau local ou acceptez celle par défaut. Cette clé permettra de signer les fichiers lors de leur nouveau chiffrement. Le nouveau chiffrement des fichiers d'un dossier protégé s'exécute automatiquement à titre de mesure de sécurité lorsque des utilisateurs sont ajoutés.

7 Saisissez la phrase secrète pour la clé sélectionnée, si elle n'est pas en cache, puis cliquez sur **Suivant**. L'écran Progression s'affiche et les fichiers du dossier protégé spécifié sont chiffrés à nouveau.

8 Cliquez sur **Terminer**.

Modification du rôle d'un utilisateur

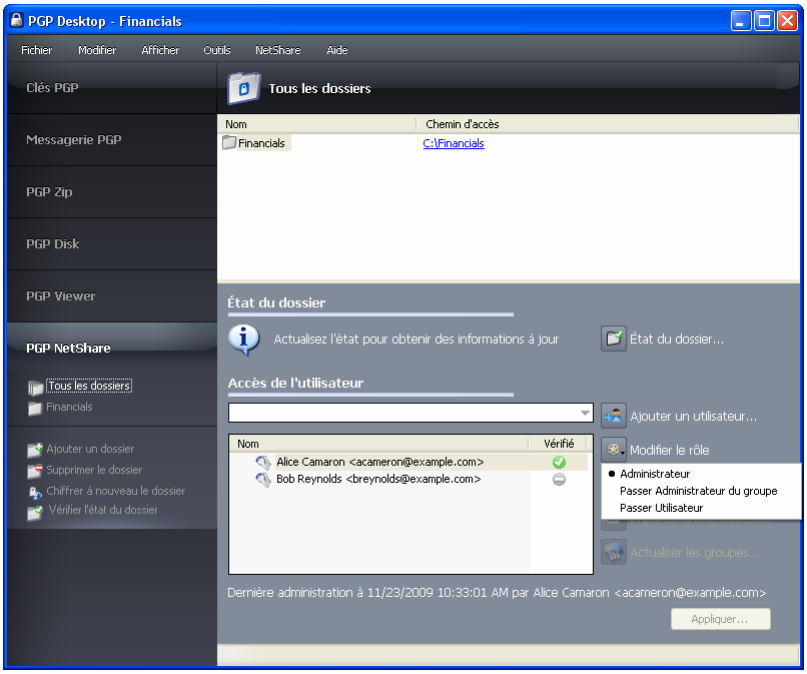
Vous pouvez modifier le rôle d'un utilisateur à tout moment après la création du dossier protégé. Pour plus d'informations sur les rôles, reportez-vous à la section *Rôles PGP NetShare* (à la page 244).

Pour changer un utilisateur en un administrateur ou un administrateur de groupe, assurez-vous que cet utilisateur possède l'ensemble des droits liés au dossier protégé.

Pour modifier le rôle d'un utilisateur

1 Dans PGP Desktop, sélectionnez le dossier PGP NetShare auquel vous souhaitez ajouter un nouveau membre.

2 Dans la section Accès de l'utilisateur, sélectionnez le nom de l'utilisateur et cliquez sur **Modifier le rôle**.



Conseil : vous pouvez également cliquer avec le bouton droit sur le nom de l'utilisateur et sélectionner le rôle.

3 Dans la liste qui s'affiche, choisissez le rôle à appliquer à l'utilisateur :

- **Administrateur** : créez un seul administrateur par dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture, permet d'ajouter et de supprimer des utilisateurs, d'attribuer des rôles à d'autres utilisateurs et de promouvoir un autre utilisateur au rôle d'administrateur.
- **Administrateur du groupe** : créez autant d'administrateurs du groupe que nécessaire pour chaque dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture, permet d'ajouter et de supprimer des utilisateurs, ainsi que d'attribuer des rôles à d'autres utilisateurs.
- **Utilisateur** : créez autant d'utilisateurs que nécessaire pour chaque dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture pour le dossier.

4 Cliquez sur **Appliquer** pour enregistrer vos modifications.

Suppression d'un utilisateur d'un dossier protégé

Pour retirer un membre d'un dossier protégé PGP NetShare, vous devez le supprimer.

▸ **Pour supprimer un utilisateur d'un dossier protégé PGP NetShare**

1 Dans l'écran PGP NetShare, sélectionnez le dossier protégé duquel vous souhaitez supprimer l'utilisateur.

2 Dans la liste Accès de l'utilisateur située à proximité du bas de l'écran, cliquez sur le nom de l'utilisateur à supprimer, puis sur **Supprimer l'utilisateur**. L'utilisateur est supprimé de la liste.

3 Cliquez sur **Appliquer**. L'écran Sélectionner le signataire s'affiche.

4 Sélectionnez une clé dans les clés privées du trousseau local ou acceptez celle par défaut. Cette clé permettra de signer les fichiers lors de leur nouveau chiffrement. PGP NetShare chiffre à nouveau automatiquement les fichiers d'un dossier protégé à titre de mesure de sécurité lorsqu'un membre est supprimé du dossier.

5 Si vous y êtes invité, saisissez la phrase secrète pour la clé sélectionnée, puis cliquez sur **Suivant**. L'écran Progression s'affiche et les fichiers du dossier protégé spécifié sont chiffrés à nouveau.

6 Cliquez sur **Terminer**. L'utilisateur supprimé n'est plus membre du dossier protégé et ne pourra plus accéder aux fichiers qu'il contient.

Importation des listes d'accès PGP NetShare

L'importation des listes d'accès vous permet d'importer les membres et leurs clés d'un ensemble d'utilisateurs autorisés dont vous faite partie vers un autre ensemble d'utilisateurs autorisés dont vous êtes membre également.

Cette option est disponible uniquement lorsque vous disposez de plusieurs dossiers protégés.

Pour importer une liste d'accès

1. Dans l'écran PGP NetShare, sélectionnez le dossier protégé dans lequel vous souhaitez importer les membres d'un autre dossier protégé.
2. Dans la liste **Accès de l'utilisateur** située à proximité du bas de l'écran, cliquez sur **Importer la liste d'accès**. La boîte de dialogue Importation PGP de la liste d'accès des utilisateurs s'affiche.
3. Cliquez sur le nom du dossier protégé existant dont vous souhaitez importer les membres, puis cliquez sur **Importer**.
4. Cliquez sur **Appliquer**. La boîte de dialogue Sélectionner le signataire s'affiche.
5. Sélectionnez une clé dans les clés privées du trousseau local ou acceptez celle par défaut. Cette clé permettra de signer les fichiers lors de leur nouveau chiffrement. Le nouveau chiffrement des fichiers d'un dossier protégé s'exécute automatiquement à titre de mesure de sécurité lorsque les membres de ce dossier sont modifiés.
6. Si vous y êtes invité, saisissez la phrase secrète pour la clé sélectionnée, puis cliquez sur **Suivant**. L'écran Progression s'affiche et les fichiers du dossier protégé spécifié sont chiffrés à nouveau.
7. Cliquez sur **Terminer**. Les nouveaux membres sont ajoutés au dossier protégé.

Utilisation des groupes Active Directory

PGP NetShare s'intègre avec Active Directory afin de vous permettre d'affecter des utilisateurs aux dossiers protégés d'un groupe Active Directory. PGP NetShare utilise le protocole LDAP (Lightweight Directory Access Protocol) pour récupérer des informations sur les groupes à partir du service d'annuaire Active Directory de votre entreprise.

Configuration de PGP NetShare afin d'utiliser des groupes

Pour récupérer des informations sur les groupes, vous devez établir une liaison à votre PGP Universal Server et activer l'option **Utilisation pour l'expansion du groupe**. Les procédures suivantes décrivent ces étapes si vous avez installé PGP Desktop dans un environnement autonome. Si PGP Desktop est installé et intégré avec un environnement géré par un PGP Universal Server, il n'est pas nécessaire de suivre cette procédure, car l'intégration LDAP est automatique.

Remarque : le nombre d'utilisateurs que vous pouvez ajouter à la fois à un dossier PGP NetShare est limité à 50. Même s'il est possible de personnaliser cette limite codée en dur, cela entraîne des implications et ne doit pas être tenté sans l'assistance de PGP Corporation. Pour plus d'informations, consultez l'*article 830 de la base de connaissances du support de PGP* (https://support.pgp.com/?faq=830).

Pour configurer PGP NetShare afin d'utiliser des groupes

1. Ajoutez le PGP Universal Server à votre liste des serveurs de clés par défaut. Pour ce faire, créez un service de messagerie et spécifiez le nom de votre PGP Universal Server. Pour plus d'informations, reportez-vous à la section *Création d'un service et modification des propriétés des comptes* (cf. "Création d'un service de messagerie" à la page 103).
2. Établissez une liaison au PGP Universal Server. Pour ce faire, suivez les instructions d'établissement manuel d'une liaison à un PGP Universal Server indiquées dans la section *Messagerie avec Lotus Notes et MAPI* (cf. "Utilisation de PGP Desktop avec IBM Lotus Notes" à la page 345).
3. Dans l'assistant de génération de clé PGP, sélectionnez le mode clé GKM, CKM ou SCKM. Ne sélectionnez pas SKM.
4. Vérifiez que la clé est disponible sur le PGP Universal Server. Pour ce faire, dans PGP Desktop, sélectionnez la boîte de contrôle Clés PGP. Cliquez sur **Rechercher des clés**, sélectionnez le nom du PGP Universal Server, saisissez votre nom, puis cliquez sur **Rechercher**.
5. Activez l'expansion du groupe. Pour ce faire, dans PGP Desktop, sélectionnez la boîte de contrôle Messagerie PGP.
6. Sélectionnez **Messagerie** > **Utilisation pour l'expansion du groupe**. Une coche apparaît en regard de l'option pour indiquer qu'elle est activée.

Actualisation des groupes

Si vous utilisez PGP NetShare dans un environnement géré par un PGP Universal Server, et que votre administrateur PGP a établi des groupes Active Directory, PGP NetShare peut vérifier que les groupes sont à jour.

Pour actualiser des groupes Active Directory

1. Dans l'écran PGP NetShare, sélectionnez le dossier protégé dont vous souhaitez actualiser les groupes Active Directory.
2. Dans la section **Accès de l'utilisateur**, cliquez sur **Actualiser les groupes**. PGP NetShare vérifie les membres des groupes Active Directory et les actualise si nécessaire.

Déchiffrement de dossiers protégés PGP NetShare

La commande Supprimer le dossier permet de rétablir l'état non chiffré initial des fichiers à présent inclus dans un dossier protégé.

Tous les dossiers et fichiers du dossier protégé seront déchiffrés ; la superposition de l'icône PGP sur les fichiers sera supprimée.

Pour supprimer la protection d'un dossier protégé PGP NetShare

1. Dans l'écran PGP NetShare, sélectionnez le dossier protégé dont vous souhaitez supprimer la protection.
2. Dans le panneau de contrôle PGP NetShare, cliquez sur **Supprimer le dossier**, à gauche de la fenêtre de PGP Desktop. La boîte de dialogue Confirmer le déchiffrement s'affiche.
3. Assurez-vous de supprimer la protection du dossier souhaité, puis cliquez sur **Suivant**. La boîte de dialogue de déverrouillage du dossier s'affiche si votre phrase secrète n'a pas été mise en cache.
4. Saisissez la phrase secrète associée à l'une des clés avec lesquelles les fichiers ont été chiffrés, puis cliquez sur **OK**. Vous devez saisir une phrase secrète appropriée dans le temps imparti, sinon le processus de chiffrement sera annulé. L'écran Progression s'affiche et les fichiers sont déchiffrés.
5. Cliquez sur **Terminer**. Les fichiers dans le dossier protégé ne sont plus protégés par chiffrement, le dossier est supprimé de la liste des dossiers protégés PGP NetShare et son icône de verrouillage disparaît.

Conseil : pour déchiffrer le contenu d'un dossier, vous pouvez également cliquer avec le bouton droit sur le dossier dans l'Explorateur Windows et choisir l'option **Supprimer le dossier de PGP NetShare** dans le menu contextuel.

Nouveau chiffrement d'un dossier

Ce processus consiste à chiffrer à nouveau les fichiers du dossier protégé spécifié. Le nouveau chiffrement modifie la clé sous-jacente, interdisant ainsi l'accès à toute personne susceptible de pouvoir déterminer la clé actuelle. Vous devez être administrateur du groupe ou administrateur du dossier pour le chiffrer à nouveau.

La commande Chiffrer à nouveau le dossier vous permet de procéder à un nouveau chiffrement chaque fois que vous le souhaitez (par exemple si vous pensez qu'une personne non autorisée est parvenue à accéder aux fichiers du dossier protégé).

Exemples pouvant justifier un nouveau chiffrement :

- Vous êtes préoccupé par le fait qu'une partie du contenu du dossier protégé n'est pas chiffrée (par exemple si un utilisateur non autorisé place un fichier dans un dossier protégé).
- Les informations sur la clé d'un utilisateur autorisé ont été compromises.
- Un nouvel utilisateur autorisé est ajouté et doit accéder au dossier protégé (cela ne se fait pas automatiquement).

Pour chiffrer à nouveau un dossier protégé

1. Dans l'écran PGP NetShare, sélectionnez le dossier protégé que vous souhaitez chiffrer à nouveau.
2. Dans le panneau de contrôle PGP NetShare, cliquez sur **Chiffrer à nouveau le dossier**, à gauche de la fenêtre de PGP Desktop. L'écran Ajouter des utilisateurs s'affiche.

   Vous pouvez ajouter de nouveaux membres ou supprimer des membres existants d'un dossier protégé en cours de nouveau chiffrement.
3. Cliquez sur **Suivant** pour continuer. L'écran Sélectionner le signataire s'affiche.
4. Sélectionnez une clé dans les clés privées du trousseau local ou acceptez celle par défaut. Cette clé permettra de signer les fichiers lors de leur nouveau chiffrement.
5. Si vous y êtes invité, saisissez la phrase secrète, puis cliquez sur **Suivant**. L'écran Progression s'affiche et les fichiers du dossier protégé spécifié sont chiffrés à nouveau.
6. Cliquez sur **Terminer**. Le processus de nouveau chiffrement est terminé.

Effacement d'une phrase secrète

Par défaut, PGP NetShare met en cache les phrases secrètes en fonction des paramètres indiqués sous l'onglet Général de la boîte de dialogue Options de PGP Desktop. Cela permet de simplifier l'utilisation de PGP NetShare, car vous n'avez pas besoin de saisir votre phrase secrète pour utiliser les fichiers chiffrés du dossier protégé.

Cependant, si vous êtes sur le point de quitter votre système, il se peut que vous ne souhaitiez pas le faire avec votre phrase secrète en cache, car cela permettrait à une personne non autorisée d'effectuer des actions sans avoir besoin de la fournir.

Pour effacer une phrase secrète

1. Sous Windows, cliquez sur l'icône PGP dans la zone de notification.
2. Sélectionnez **Effacer les caches** dans le menu affiché. Au moins une phrase secrète doit être en cache pour que cette commande soit active. Les phrases secrètes en cache sont effacées.

Protection des fichiers hors d'un dossier protégé

PGP NetShare dispose d'une option avancée vous permettant de protéger des fichiers individuels qui ne se trouvent *pas* dans un dossier protégé PGP NetShare. Cette option est désactivée par défaut.

Remarque : il se peut que votre administrateur PGP ne vous autorise pas à sélectionner cette option si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server.

Pour protéger des fichiers individuels hors d'un dossier protégé PGP NetShare, vous devez d'abord sélectionner l'option **Protéger les fichiers individuels sous l'onglet NetShare de la commande Options de PGP ; pour plus d'informations, reportez-vous à la section** *Options de PGP NetShare* (à la page 326). Vous ne pouvez pas protéger les fichiers qui se trouvent hors d'un dossier protégé PGP NetShare tant que cette option n'est pas activée.

Une fois sélectionnée, l'option **Protéger les fichiers individuels** vous permet de protéger des fichiers individuels qui se trouvent hors d'un dossier protégé à l'aide du menu contextuel de PGP Desktop dans l'Explorateur Windows. *Les fichiers protégés de manière individuelle n'apparaissent pas dans la zone de travail de PGP NetShare de l'interface utilisateur de PGP Desktop.*

Attention : PGP NetShare déploie tous les efforts possibles pour protéger les fichiers protégés de manière individuelle, mais certaines applications (Microsoft Word, par exemple) enregistrent les fichiers modifiés de telle sorte qu'il apparaisse à PGP NetShare que le fichier protégé a été supprimé. Dans ces conditions, PGP NetShare ne peut pas continuer à protéger ces fichiers. Cela ne s'applique qu'aux fichiers protégés de manière individuelle qui ne se trouvent pas dans un dossier protégé, et non pas à ceux d'un dossier protégé PGP NetShare. Pour éviter que des fichiers protégés ne le soient plus, PGP Corporation vous recommande vivement de les conserver dans un dossier protégé PGP NetShare.

Pour activer l'option Protéger les fichiers individuels

1. Sélectionnez **Outils > Options de PGP**.
2. Cliquez sur l'onglet **NetShare**.
3. Sous l'onglet NetShare, assurez-vous que l'option **Protéger les fichiers individuels** est sélectionnée. Par défaut, cette option n'est *pas* sélectionnée.

Pour protéger des fichiers individuels à l'aide de PGP NetShare

1. Dans l'Explorateur Windows, cliquez avec le bouton droit sur le fichier à protéger à l'aide de PGP NetShare.
2. Dans le menu contextuel, sélectionnez **PGP Desktop > Ajouter [nom du fichier] à PGP NetShare.**
3. Lorsque l'assistant de PGP NetShare s'affiche, ajoutez des utilisateurs autorisés et sélectionnez une clé privée pour la signature.
4. Lorsque le processus de chiffrement est terminé, cliquez sur **Terminer**. Le fichier protégé affiche une icône PGP NetShare dans l'Explorateur Windows.

Vous pouvez également utiliser le menu contextuel pour afficher les propriétés PGP NetShare d'un fichier protégé, chiffrer à nouveau des fichiers protégés de manière individuelle qui se trouvent hors d'un dossier protégé et supprimer leur protection.

Pour afficher les propriétés PGP NetShare d'un fichier protégé à l'aide du menu contextuel

1. Dans l'Explorateur Windows, cliquez avec le bouton droit sur le fichier protégé dont vous souhaitez afficher les propriétés PGP NetShare.
2. Dans le menu contextuel, sélectionnez **PGP Desktop > Propriétés PGP NetShare.** La fenêtre Propriétés s'affiche pour le fichier sélectionné.
3. Une fois les propriétés consultées, cliquez sur **OK**.

Pour chiffrer à nouveau des fichiers protégés à l'aide du menu contextuel

1. Dans l'Explorateur Windows, cliquez avec le bouton droit sur le fichier protégé à chiffrer à nouveau.
2. Dans le menu contextuel, sélectionnez **PGP Desktop > Chiffrer à nouveau.**
3. Lorsque l'assistant de PGP NetShare s'affiche, ajoutez et/ou supprimez des utilisateurs autorisés et sélectionnez une clé privée pour la signature.
4. Une fois le processus de nouveau chiffrement exécuté, cliquez sur **Terminer**.

Pour supprimer la protection de fichiers protégés de manière individuelle à l'aide du menu contextuel

1. Dans l'Explorateur Windows, cliquez avec le bouton droit sur le fichier protégé dont vous souhaitez supprimer la protection.
2. Dans le menu contextuel, sélectionnez **PGP Desktop > Supprimer [nom du fichier] de PGP NetShare**.
3. Lorsque l'assistant de PGP NetShare s'affiche, confirmez que vous souhaitez supprimer la protection du fichier en cliquant sur **Suivant**.
4. Une fois le fichier déchiffré, cliquez sur **Terminer**.

Sauvegarde de fichiers protégés par PGP NetShare

Vous pouvez sauvegarder des fichiers et dossiers protégés par PGP NetShare. La façon dont les fichiers sont gérés au cours du processus de sauvegarde change selon si vous utilisez PGP NetShare dans un environnement géré par un PGP Universal Server ou non.

Sauvegarde de fichiers avec un client non géré

Lorsqu'un client non géré (autonome) sauvegarde des fichiers et dossiers protégés, ces fichiers sont déchiffrés de façon transparente lors de la sauvegarde et stockés en clair sur le support de sauvegarde. Leur restauration au chiffrement d'origine permet de les chiffrer à nouveau de façon transparente.

Sauvegarde de fichiers avec un client géré par un PGP Universal Server

Lorsqu'un client géré est utilisé pour sauvegarder des fichiers et dossiers protégés, la gestion du chiffrement change selon si l'application de sauvegarde est définie en tant que contournement par l'administrateur de PGP Universal Server.

- Si l'application de sauvegarde fait partie de la liste de contournement de déchiffrement, les fichiers protégés restent chiffrés sur le support de sauvegarde après la sauvegarde. Leur restauration à leur emplacement d'origine conserve le chiffrement.
- Si l'application de sauvegarde ne fait pas partie de la liste de contournement du chiffrement, le processus de sauvegarde est similaire à celui d'un client non géré. Dans ce cas, les fichiers protégés sont déchiffrés de façon transparente lors de la sauvegarde et stockés en texte en clair sur le support de sauvegarde. Leur restauration au chiffrement d'origine permet de les chiffrer à nouveau de façon transparente.

Remarque : PGP Corporation vous recommande de ne pas mélanger les différents scénarios de sauvegarde et restauration de données. Par exemple, si vous utilisez un client non géré pour sauvegarder les fichiers, vous devez utiliser un client non géré pour les restaurer.

Accès aux fonctionnalités de PGP NetShare à l'aide du menu contextuel

Certaines fonctionnalités de PGP NetShare sont disponibles à partir du menu contextuel accessible à l'aide du bouton droit dans l'Explorateur Windows.

Vous pouvez protéger des dossiers (ainsi que des fichiers si vous avez activé l'option **Protéger les fichiers individuels**) à partir de l'Explorateur Windows en cliquant avec le bouton droit sur l'élément. Sélectionnez **PGP Desktop > Ajouter [nom] à PGP NetShare** dans le menu contextuel affiché pour lancer le processus visant à désigner cet élément comme protégé par PGP NetShare.

Pour plus d'informations sur la protection des fichiers individuels hors d'un dossier protégé à l'aide de PGP NetShare, reportez-vous à la section *Protection des fichiers hors d'un dossier protégé* (à la page 266).

Lorsqu'un dossier ou fichier est protégé par PGP NetShare, vous pouvez exécuter trois commandes dans l'Explorateur Windows à l'aide du menu contextuel :

- **Propriétés PGP NetShare**. Cette commande ouvre l'onglet PGP NetShare de l'écran Propriétés pour le fichier ou le dossier. Sous cet onglet, vous pouvez afficher ou ajouter des personnes qui peuvent utiliser les fichiers protégés, et déverrouiller un fichier ou un dossier s'il est verrouillé.

- **Chiffrer à nouveau**. Cette commande chiffre à nouveau le dossier ou fichier spécifié avec une nouvelle clé sous-jacente.
- **Supprimer <nom du fichier> de PGP NetShare**. Cette commande supprime la protection PGP NetShare du dossier ou fichier spécifié.

Pour connaître les procédures applicables, reportez-vous à la section *Protection des fichiers hors d'un dossier protégé* (à la page 266).

PGP NetShare dans un environnement géré par un PGP Universal Server

Si vous utilisez PGP NetShare dans un environnement géré par un PGP Universal Server, il se peut que votre administrateur PGP ait configuré des paramètres qui affectent son fonctionnement sur votre système.

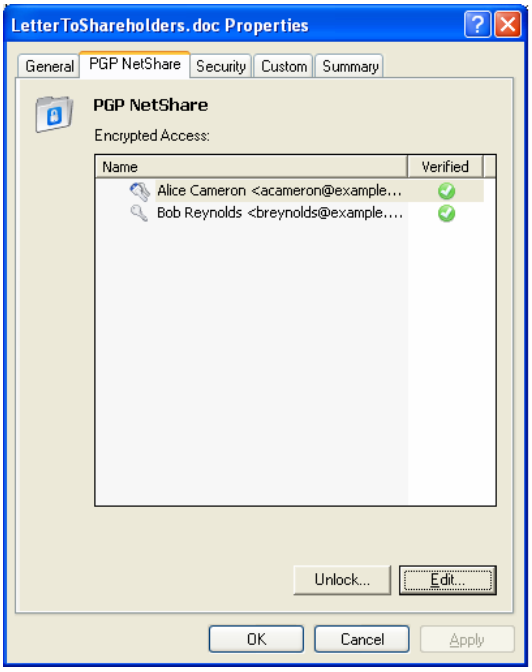
Ces paramètres sont les suivants :

- **Autoriser l'utilisateur à créer et à gérer des dossiers PGP NetShare**. Lorsqu'il est activé, ce paramètre vous permet de créer des dossiers protégés PGP NetShare. Lorsqu'il est désactivé, vous pouvez utiliser un dossier protégé créé par une autre personne, mais vous ne pouvez pas en créer un vous-même. Ce paramètre est activé par défaut.
- **Autoriser l'utilisateur à activer le mode Utilisateur avancé**. Lorsqu'il est activé, ce paramètre vous permet d'activer le mode Utilisateur avancé dans vos options de PGP, ce qui signifie que vous pouvez protéger des fichiers individuels déplacés hors d'un dossier protégé. Ce paramètre est désactivé par défaut.
- **Forcer le chiffrement des fichiers dans les dossiers suivants**. Ces dossiers sont appelés dossiers « sur liste blanche ». Ils sont *systématiquement* ajoutés à PGP NetShare et leur contenu est chiffré. Pour plus d'informations, reportez-vous à la section *Dossiers « sur liste noire » et « sur liste blanche » spécifiés par le PGP Universal Server* (à la page 247).
- **Empêcher le chiffrement des fichiers dans les dossiers suivants**. Ces dossiers sont appelés dossiers « sur liste noire ». Ils ne sont *jamais* ajoutés à PGP NetShare et sont chiffrés. Pour plus d'informations, reportez-vous à la section *Dossiers « sur liste noire » et « sur liste blanche » spécifiés par le PGP Universal Server* (à la page 247).

Contactez votre administrateur PGP pour toute question concernant ces paramètres.

Accès aux propriétés d'un dossier ou fichier protégé

Les fichiers protégés par PGP NetShare comportent un onglet PGP NetShare sur leur écran Propriétés qui affiche des informations sur le fichier.



Pour accéder à l'onglet PGP NetShare dans la boîte de dialogue Propriétés d'un fichier

1. Dans l'Explorateur Windows, effectuez l'une des opérations suivantes :
   - Cliquez avec le bouton droit sur le fichier et sélectionnez **Propriétés** dans la liste.
   - Sélectionnez **Fichier > Propriétés** dans la liste.

   L'écran Propriétés s'affiche pour le fichier spécifié.
2. Cliquez sur l'onglet **PGP NetShare**. Son contenu s'affiche.
3. L'onglet PGP NetShare d'un fichier affiche les noms des utilisateurs qui peuvent utiliser le fichier chiffré. Dans celui-ci, effectuez l'une des opérations suivantes :
   - **Déverrouiller**. Cliquez sur cette option pour déverrouiller un dossier protégé qui a été verrouillé.
   - **Modifier**. Cliquez sur cette option pour afficher l'écran Ajouter des utilisateurs qui vous permet d'ajouter ou de supprimer des utilisateurs qui peuvent accéder au fichier ou dossier sélectionné. Le fichier ou dossier sera à nouveau chiffré si un utilisateur est ajouté ou supprimé.

- Pour afficher le rôle d'un utilisateur, cliquez avec le bouton droit sur son nom. Cet onglet ne vous permet pas de modifier le rôle de l'utilisateur. Pour ce faire, reportez-vous à la section *Modification du rôle d'un utilisateur* (à la page 260).

4 Pour fermer la boîte de dialogue Propriétés, cliquez sur **OK**.

Utilisation des menus PGP NetShare dans PGP Desktop

Trois menus PGP Desktop comportent des commandes qui affectent PGP NetShare : Fichier, Modifier et NetShare.

Menu Fichier

Lorsque la boîte de contrôle PGP NetShare est sélectionnée, la commande **Fichier > Nouveau dossier PGP NetShare** vous permet de créer un dossier protégé.

Ce processus est identique à celui décrit dans la section *Création d'un dossier protégé PGP NetShare* (à la page 251).

Menu Modifier

Lorsque la boîte de contrôle PGP NetShare est sélectionnée, la commande **Renommer** disponible dans le menu Modifier de PGP Desktop vous permet de renommer un dossier protégé.

Pour renommer un dossier protégé PGP NetShare via le menu Modifier

1 Ouvrez PGP Desktop et cliquez sur la boîte de contrôle **PGP NetShare**.

2 Si plusieurs dossiers protégés s'affichent, cliquez sur le nom de celui à renommer.

3 Sélectionnez **Modifier > Renommer**.

4 Saisissez un nouveau nom pour le dossier protégé.

5 Appuyez sur **Entrée** ou cliquez en dehors du nom du dossier protégé. Le dossier protégé est renommé.

L'option **Afficher le fichier dans l'Explorateur...** disponible dans le menu Modifier donne le même résultat que cliquer sur le chemin d'accès d'un dossier protégé. Si vous cliquez sur cette option, le dossier sélectionné s'ouvre dans l'Explorateur Windows.

Menu NetShare

Lorsque la boîte de contrôle PGP NetShare est sélectionnée, le menu NetShare vous permet de sélectionner les commandes suivantes :

- **Ajouter un dossier** : sélectionnez cette commande pour créer un dossier protégé. Ce processus est identique à celui décrit dans la section *Création d'un dossier protégé PGP NetShare* (à la page 251). Vous devez sélectionner la boîte de contrôle PGP NetShare pour que cette commande soit active.
- **Supprimer le dossier** : sélectionnez cette commande pour lancer le processus de restauration d'un dossier protégé à son état normal déchiffré. Tous les dossiers et fichiers du dossier protégé seront déchiffrés ; la superposition de l'icône PGP sur les fichiers sera supprimée. Vous devez sélectionner un dossier protégé pour que cette commande soit active.
- **Chiffrer à nouveau le dossier** : sélectionnez cette commande pour chiffrer à nouveau les fichiers d'un dossier protégé. Le nouveau chiffrement modifie la clé sous-jacente, interdisant ainsi l'accès à toute personne susceptible de pouvoir déterminer la clé actuelle. Ce processus s'exécute automatiquement lorsqu'un utilisateur est ajouté à ou supprimé d'un dossier protégé. La commande **Chiffrer à nouveau le dossier** vous permet de procéder à un nouveau chiffrement chaque fois que vous le souhaitez (par exemple si vous pensez qu'une personne non autorisée est parvenue à accéder aux fichiers du dossier protégé). Vous devez sélectionner un dossier protégé pour que cette commande soit active.
- **Vérifier l'état du dossier** : sélectionnez cette commande pour obtenir des informations à jour sur l'état du dossier protégé sélectionné. Vous devez sélectionner un dossier protégé pour que cette commande soit active.
- **Effacer le dossier récent** : sélectionnez cette commande pour le supprimer de la liste des dossiers protégés. Toutefois, contrairement à la commande **Supprimer le dossier**, celle-ci ne déchiffre pas les fichiers du dossier protégé. Vous devez sélectionner un dossier protégé pour que cette commande soit active.

14 Utilisation de PGP Zip

PGP Zip vous permet de créer, d'ouvrir et de modifier des packages chiffrés et compressés appelés « archives PGP Zip ». Cette section explique comment utiliser la fonctionnalité PGP Zip de PGP Desktop.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

Présentation

Un package d'archive PGP Zip est un fichier unique qui est chiffré et compressé afin de faciliter sa sauvegarde ou son transport. Ces fichiers d'archive peuvent contenir n'importe quelle combinaison de fichiers et/ou dossiers, et s'avèrent particulièrement pratiques pour assurer une sauvegarde ou un transport sécurisé.

L'assistant de PGP Zip vous permet de créer de nouveaux packages d'archive PGP Zip. Il vous guide dans le processus de sélection des fichiers et/ou dossiers pour votre archive et de la méthode de chiffrement ou de compression :

- Chiffrement et compression de vos fichiers et/ou dossiers à l'aide des clés PGP d'un ou de plusieurs destinataires (les destinataires doivent avoir installé PGP Desktop sur leur ordinateur).

- Chiffrement et compression de vos fichiers et/ou dossiers à l'aide d'une phrase secrète (les destinataires doivent avoir installé PGP Desktop sur leur ordinateur).
- Chiffrement et compression de vos fichiers et/ou dossiers dans une archive à auto-déchiffrement (SDA PGP Zip) protégée par une phrase secrète (il n'est pas nécessaire que les destinataires disposent de PGP Desktop, mais leur ordinateur doit exécuter Microsoft Windows).
- Pas de chiffrement ou de compression, mais création d'un fichier que vous pouvez envoyer à vos destinataires afin de vérifier que vous êtes bien l'expéditeur.

Lorsque vous utilisez l'assistant de PGP Zip pour créer un fichier d'archive PGP Zip, vous avez la possibilité d'envoyer automatiquement les fichiers originaux vers PGP Shredder afin qu'ils puissent être supprimés en toute sécurité et définitivement de votre ordinateur.

Lorsque vous recevez un fichier d'archive PGP Zip, vous pouvez :

- extraire l'ensemble des fichiers et/ou dossiers qu'elle contient ;
- extraire des fichiers et/ou dossiers spécifiques ;
- extraire des fichiers et/ou dossiers spécifiques tout en en ajoutant d'autres ;
- ajouter de nouveaux fichiers et/ou dossiers à l'archive ;
- modifier l'archive en :
  - changeant le type de chiffrement ;
  - changeant la clé de signature ;
  - changeant les destinataires.

Les archives PGP Zip sont chiffrées avec le chiffrement par défaut pour PGP Desktop (si configuré par un administrateur de PGP Universal Server) ou avec AES256. Elles peuvent êtres déplacées entre les plates-formes Windows et Mac OS X. PGP Desktop doit être installé sur le système de destination.

Création d'archives PGP Zip

Pour créer une archive PGP Zip :

1. Cliquez sur la boîte de contrôle PGP Zip, puis sur **Nouveau PGP Zip**. L'assistant PGP Zip apparaît.
2. Effectuez l'une des opérations suivantes :
   - Faites glisser vos fichiers dans la zone indiquée dans l'assistant.
   - Pour ajouter un annuaire entier à l'archive PGP Zip en cours de création, cliquez sur **Ajouter annuaire**  .

- Pour ajouter un fichier à l'archive PGP Zip en cours de création, cliquez sur **Ajouter fichiers**  .
- Pour supprimer un fichier ou un annuaire de l'archive PGP Zip en cours de création, cliquez sur **Supprimer les fichiers sélectionnés**  .
- Pour sélectionner des options supplémentaires pour l'archive PGP Zip en cours de création, cliquez sur **Options avancées de PGP Zip**  . Les paramètres par défaut conviennent à la plupart des utilisateurs.

Remarque : pour ajouter une différents fichiers et dossiers, utilisez une combinaison des boutons  et  . Lors de l'ajout d'un répertoire à la liste des fichiers, l'assistant de PGP Zip affiche tous les fichiers séparément, ce qui permet de tous les voir facilement. Si vous devez ajouter beaucoup de fichiers à votre archive PGP Zip, vous gagnerez peut-être du temps en ajoutant un répertoire entier à la liste des fichiers d'archive PGP Zip, puis en enlevant les fichiers en trop. *Si vous choisissez cette approche, assurez-vous avant procéder que vous avez bien enlevé tous les fichiers à exclure de l'archive PGP Zip.*

3 Pour supprimer en toute sécurité les fichiers originaux une fois l'archive PGP Zip créée, sélectionnez **Envoyer les fichiers originaux vers PGP Shredder lorsque l'opération est terminée**.

Attention : si vous choisissez d'envoyer les fichiers originaux vers PGP Shredder après la création de l'archive PGP Zip, vous ne pourrez pas récupérer vos fichiers ultérieurement, même à l'aide d'un logiciel de récupération de fichiers. Vos fichiers sont définitivement supprimés et irrécupérables. Soyez prudent si vous sélectionnez cette option.

4 Pour spécifier des options spéciales, cliquez sur **Options avancées de PGP Zip**  :

- Pour créer des fichiers chiffrés distincts au lieu de tous les rassembler en un seul fichier d'archive PGP Zip chiffré, sélectionnez **Ne pas zipper (fichiers de sortie individuels)**.
- Pour créer des archives zip de fichiers texte uniquement, sélectionnez **Convertir les sauts de ligne pour les fichiers texte**.
- Pour créer une archive zip qui requiert l'utilisation de la visionneuse sécurisée de PGP, le cas échéant et conformément aux stratégies de sécurité de votre entreprise, sélectionnez **Visionneuse sécurisée PGP requise lors du déchiffrement**. Si vous avez sélectionné ce mode, le fichier déchiffré sera affiché dans une fenêtre de la visionneuse sécurisée de PGP. Cette option permet de se protéger des anciennes attaques par interception de rayonnement.

- Pour envoyer cette archive zip en tant que fichier binaire avec une application de messagerie plus ancienne, sélectionnez **Sortie texte**. La taille du fichier chiffré augmente d'environ 30 % lorsque le fichier est enregistré au format texte ASCII. Cette option n'est pas disponible quand vous utilisez PGP Desktop dans un environnement géré par le PGP Universal Server.
- Pour enregistrer ces paramètres d'Option de PGP Zip afin de les réutiliser ultérieurement, sélectionnez **Mémoriser ces paramètres pour la prochaine fois**.
- Cliquez sur **OK** quand vous avez fini de sélectionner les options spéciales. Cliquez sur **Annuler** si vous choisissez de ne modifier aucune de ces options.

La boîte de dialogue Nouveau PGP Zip est à nouveau affichée.

5 Quand vous avez fini la sélection des fichiers à inclure dans l'archive PGP Zip, cliquez sur **Suivant**.

6 Sélectionnez le type de chiffrement souhaité, puis cliquez sur **Suivant**.

Conseil : pointez votre curseur sur chaque option pour afficher des détails supplémentaires dans le champ d'information situé au-dessous de la liste d'options.

- **Clés des destinataires** : Crée une archive PGP Zip par le chiffrement de fichiers avec les clés publiques du ou des destinataires, et garantit ainsi que seuls ces destinataires pourront utiliser PGP Desktop pour ouvrir l'archive. Il s'agit de l'option la plus sécurisée. Reportez-vous à la section *Chiffrement avec les clés des destinataires* (à la page 279).
- **Phrase secrète** : Crée une archive PGP Zip par le chiffrement de fichiers avec une phrase secrète que vous spécifiez lors de l'enregistrement de l'archive. Seules les personnes qui connaissent la phrase secrète et qui utilisent PGP Desktop peuvent ouvrir l'archive. Reportez-vous à la section *Chiffrement avec une phrase secrète* (cf. "Chiffrement avec phrase secrète" à la page 281).
- **Archive à auto-déchiffrement de PGP.** Crée une archive à auto-déchiffrement de PGP avec une phrase secrète que vous spécifiez lors de l'enregistrement de l'archive. L'utilisation de PGP Desktop n'est pas nécessaire pour le déchiffrement d'une archive à auto-déchiffrement de PGP, mais les destinataires *doivent* utiliser un ordinateur sous le système d'exploitation Microsoft Windows. Reportez-vous à la section *Création d'une archive à auto-déchiffrement de PGP (SDA)* (à la page 283).
- **Signer uniquement**. Ajoute votre signature PGP à un fichier zip non chiffré. Le ou les destinataires peuvent alors ouvrir l'archive zip avec PGP Desktop, et la signature incluse est la preuve qu'elle provient bien de vous et n'a pas été modifiée pendant le transit. Pour plus d'informations, reportez-vous à la section *Signer uniquement* (cf. "Création d'une archive uniquement signée" à la page 285).

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, le chiffrement conventionnel par phrase secrète peut être désactivé.

Chiffrement avec les clés des destinataires

Utilisez les **Clés des destinataires** :

- pour offrir le plus haut niveau de sécurité à vos fichiers ;
- quand PGP Desktop est installé sur l'ordinateur de chacun des destinataires (Windows ou Mac OS X) ;
- quand vous avez une clé publique pour chaque destinataire (dans votre trousseau de clés ou sur un serveur de clés PGP) ;
- quand vous ne voulez pas révéler une phrase secrète aux destinataires des fichiers.

Le chiffrement de votre archive PGP Zip avec les clés publiques de tous les destinataires est l'option la plus sécurisée. Ce devrait être votre premier choix si vous avez besoin de la plus grande sécurité et que les conditions requises sont remplies.

Une fois vos dossiers sécurisés, il vous suffit d'envoyer l'archive PGP Zip à ses destinataires par le moyen de votre choix. Les destinataires utilisent ensuite PGP Desktop pour ouvrir le fichier d'archive PGP Zip. Toute personne dont vous avez utilisé la clé lors du chiffrement du fichier peut ouvrir le fichier d'archive PGP Zip, et toutes voient les mêmes éléments. Si vous avez besoin de restreindre les éléments que certains destinataires peuvent voir, vous devez créer des fichiers d'archive PGP Zip distincts pour chacun d'eux.

Pour chiffrer avec les clés des destinataires

1. Si ne vous l'avez pas encore fait, suivez la procédure de création de fichier d'archive PGP Zip comme décrit dans la section *Création d'archives PGP Zip* (à la page 276).
2. Dans la boîte de dialogue Chiffrer, sélectionnez **Clés des destinataires**.
3. Cliquez sur **Suivant**. La boîte de dialogue Ajouter des clés utilisateur s'affiche.
4. Sélectionnez les destinataires de votre archive PGP Zip. Effectuez l'une des opérations suivantes :
   - Pour sélectionner une clé dans la liste des clés de votre trousseau, cliquez sur la flèche.
   - Pour envoyer le dossier à un destinataire dont la clé n'est pas sur votre trousseau, cliquez sur **Ajouter**. La boîte de dialogue Sélection des destinataires s'affiche.

   Quand vous avez fini de sélectionner les noms supplémentaires, cliquez sur **OK** pour retourner au panneau **Ajouter des clés utilisateur**.

Pour enlever une clé quelle qu'elle soit, sélectionnez le nom du destinataire puis cliquez sur **Supprimer**.

5 Cliquez sur **Suivant.** L'écran **Signer et enregistrer** s'affiche.

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

La clé de signature spécifiée sert à signer numériquement l'archive PGP Zip. Le ou les destinataires peuvent vérifier qui a envoyé l'archive en vérifiant la signature numérique avec la clé publique correspondante.

- Si vous n'avez pas besoin de signer le fichier ou que vous préférez ne pas le signer, choisissez **Aucun** dans la liste Clé de signature.
- Si vous choisissez de signer votre archive PGP Zip, choisissez votre clé dans la liste Clé de signature, puis saisissez la phrase secrète de la clé sélectionnée pour signer (et non pas la phrase secrète de sécurisation du fichier zip). Pour voir les frappes à mesure que vous saisissez la phrase secrète, sélectionnez **Afficher les frappes**.

Si vous avez déjà saisi votre phrase secrète au cours de la session actuelle avec PGP Desktop, il est possible qu'elle soit en cache selon les paramètres d'**Options** que vous avez choisis. Dans ce cas, un message indiquant que la phrase secrète est en cache s'affiche. Même si votre phrase secrète est en cache, vous pouvez choisir de ne pas signer le fichier d'archive PGP Zip.

7 Confirmez que l'archive PGP Zip est enregistrée à l'emplacement et sous le nom de fichier que vous voulez. Si nécessaire, vous pouvez :

- modifier l'emplacement d'enregistrement du fichier en cliquant sur **Parcourir** puis en en choisissant un nouveau dans la boîte de dialogue Fichier de Windows ;
- modifier manuellement l'emplacement de l'enregistrement du fichier en saisissant le nouvel emplacement où vous aimeriez enregistrer l'archive PGP Zip ;
- modifier le nom de fichier de l'archive PGP Zip en le saisissant manuellement à la fin de la chaîne de texte de l'emplacement du fichier.

Par défaut, le nom de fichier d'une archive PGP Zip qui ne contient qu'un seul fichier, répertoire ou lecteur est le nom dudit élément, auquel vient s'ajouter l'extension `.pgp`. Si l'archive PGP Zip contient plus d'un élément, son nom de fichier est celui de l'un des éléments auquel vient s'ajouter l'extension `.pgp`. Si vous le souhaitez, modifiez le nom de fichier de l'archive PGP Zip.

8 Si vous avez choisi l'option **Signer uniquement**, cliquez pour sélectionner **Enregistrer la ou les signatures détachées**.

9 Cliquez sur **Suivant**. L'archive PGP Zip est créée.

10 Cliquez sur **Terminer**. Votre archive PGP Zip est prête à être envoyée aux destinataires dont les clés ont servi au chiffrement. Si votre clé est l'une de celles qui ont servi au chiffrement, le fichier peut être stocké où vous le souhaitez.

Chiffrement avec phrase secrète

Utilisez la **Phrase secrète** :

- quand vous voulez créer une archive PGP Zip sans utiliser les clés des destinataires, ce qui peut s'avérer moins sécurisé que le chiffrement avec les clés des destinataires mais reste extrêmement sécurisé ;
- quand PGP Desktop est installé sur l'ordinateur de chacun des destinataires (Windows ou Mac OS X) ;
- quand vous ne voulez pas révéler une phrase secrète aux destinataires des fichiers ;
- quand vous n'avez pas une clé publique pour chaque destinataire (dans votre trousseau de clés ou sur un serveur de clés PGP).

Conseil : le chiffrement avec une phrase secrète est aussi appelé *chiffrement conventionnel*.

Le chiffrement d'une archive PGP Zip avec une phrase secrète peut être extrêmement sécurisé, surtout si vous utilisez une phrase secrète forte. Le chiffrement avec les clés du destinataire n'apporte pas une sécurité accrue. Quand vous chiffrez avec les clés des destinataires, ceux d'entre eux qui possèdent l'archive PGP Zip ont besoin de leurs clés privées et de leurs phrases secrètes pour déchiffrer le fichier (et chaque clé de destinataire a sa propre phrase secrète).

Quand le fichier est chiffré avec une phrase secrète, tous les destinataires l'ouvrent avec la même phrase secrète et aucune clé privée n'est nécessaire. Quiconque possède le fichier, utilise PGP Desktop et connaît la phrase secrète peut déchiffrer le fichier.

Attention : prenez toutes les précautions nécessaires pour vous assurer que la phrase secrète de votre archive PGP Zip n'est révélée à personne d'autre que les destinataires souhaités. Si la phrase secrète est révélée à des personnes non autorisées, créez une nouvelle archive PGP Zip avec une phrase secrète différente. Remarque : il n'y a aucun moyen de sécuriser à nouveau le fichier d'archive original et son contenu.

Une fois vos fichiers sécurisés, envoyez l'archive PGP Zip à ses destinataires par le moyen de votre choix. Les destinataires utilisent ensuite PGP Desktop pour ouvrir le fichier d'archive PGP Zip. *Quiconque en possession du fichier et de la phrase secrète peut ouvrir le fichier d'archive PGP Zip généré,* et tous voient les mêmes éléments. S'il faut que différents destinataires voient des éléments différents, vous devez créer des fichiers d'archive PGP Zip distincts pour chacun.

Attention : si vous utilisez PGP Desktop dans un environnement géré par le PGP Universal Server, le chiffrement par phrase secrète est peut-être désactivé.

Pour chiffrer à l'aide d'une phrase secrète

1. Si ne vous l'avez pas encore fait, suivez la procédure de création de fichier d'archive PGP Zip comme décrit dans la section *Création d'archives PGP Zip* (à la page 276). Suivez les instructions jusqu'à l'étape 6. Ensuite, revenez à la section présente.
2. Dans la fenêtre Chiffrer, sélectionnez **Phrase secrète**.
3. Cliquez sur **Suivant**. La boîte de dialogue Créer une phrase secrète s'affiche.
4. Pour voir les frappes à mesure que vous saisissez la phrase secrète, sélectionnez **Afficher les frappes**.
5. Dans le champ **Phrase secrète**, entrez la phrase secrète que vous voulez utiliser.

   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* (à la page 336).
6. Saisissez à nouveau votre phrase secrète dans le champ **Confirmer**.
7. Cliquez sur **Suivant**. La boîte de dialogue Signer et enregistrer s'affiche.
8. Si vous le souhaitez, spécifiez sur votre trousseau de clés une clé privée à utiliser comme clé de signature pour l'archive PGP Zip en cours de création.

   La clé de signature spécifiée sert à signer numériquement l'archive PGP Zip. Le ou les destinataires peuvent vérifier qui a envoyé l'archive en vérifiant la signature numérique avec la clé publique correspondante.

   - Si vous n'avez pas besoin de signer le fichier ou que vous préférez ne pas le signer, choisissez **Aucun** dans la liste Clé de signature.
   - Si vous choisissez de signer votre archive PGP Zip, choisissez votre clé dans la liste Clé de signature, puis saisissez la phrase secrète de la clé sélectionnée pour signer (et non pas la phrase secrète de sécurisation du fichier zip). Pour voir les frappes à mesure que vous saisissez la phrase secrète, sélectionnez **Afficher les frappes**.

Si vous avez déjà saisi votre phrase secrète au cours de la session actuelle avec PGP Desktop, il est possible qu'elle soit en cache selon les paramètres d'**Options** que vous avez choisis. Dans ce cas, un message indiquant que la phrase secrète est en cache s'affiche. Même si votre phrase secrète est en cache, vous pouvez choisir de ne pas signer le fichier d'archive PGP Zip.

9 Confirmez que l'archive PGP Zip est enregistrée à l'emplacement et sous le nom de fichier que vous voulez. Si nécessaire, vous pouvez :

- modifier l'emplacement d'enregistrement du fichier en cliquant sur **Parcourir** puis en en choisissant un nouveau dans la boîte de dialogue Fichier de Windows ;
- modifier manuellement l'emplacement de l'enregistrement du fichier en saisissant le nouvel emplacement où vous aimeriez enregistrer l'archive PGP Zip ;
- modifier le nom de fichier de l'archive PGP Zip en le saisissant manuellement à la fin de la chaîne de texte de l'emplacement du fichier.

Par défaut, le nom de fichier d'une archive PGP Zip qui ne contient qu'un seul fichier, répertoire ou lecteur est le nom dudit élément, auquel vient s'ajouter l'extension `.pgp`. Si l'archive PGP Zip contient plus d'un élément, son nom de fichier est celui de l'un des éléments auquel vient s'ajouter l'extension `.pgp`. Si vous le souhaitez, modifiez le nom de fichier de l'archive PGP Zip.

10 Cliquez sur **Suivant**. L'archive PGP Zip est créée.

11 Cliquez sur **Terminer**. Votre archive PGP Zip est prête à être envoyée aux destinataires. N'oubliez pas de communiquer la phrase secrète aux destinataires pour qu'ils puissent ouvrir l'archive.

Création d'une archive à auto-déchiffrement de PGP (SDA)

Utilisez l'**archive à auto-déchiffrement de PGP** :

- quand vous voulez créer une archive à auto-déchiffrement de PGP Zip sans utiliser les clés des destinataires, ce qui peut s'avérer moins sécurisé que le chiffrement avec les clés des destinataires mais reste extrêmement sécurisé ;
- quand PGP Desktop n'est pas installé sur les ordinateurs de vos destinataires et que tous utilisent des systèmes Windows ;
- quand vous ne voulez pas révéler une phrase secrète aux destinataires des fichiers ;
- quand vous n'avez pas une clé publique pour chaque destinataire (dans votre trousseau de clés ou sur un serveur de clés PGP).

Une archive à auto-déchiffrement de PGP (SDA) est une archive PGP Zip qui peut être ouverte sur tout ordinateur Windows, même si PGP Desktop n'est pas installé. Les fichiers SDA PGP Zip sont des fichiers exécutables Windows standard (.exe) qui s'ouvrent avec un simple double-clic.

Les fichiers SDA PGP Zip sont légèrement plus gros que les archives PGP Zip habituelles car le « mécanisme » d'auto-déchiffrement exige un certain espace supplémentaire (généralement environ 100 Ko).

Remarque : si vous utilisez PGP Desktop dans un environnement géré par le PGP Universal Server, la création de fichiers SDA PGP Zip est peut-être désactivée.

Une fois créé votre fichier SDA PGP Zip, envoyez-le à ses destinataires par le moyen de votre choix. *Quiconque en possession du fichier et de la phrase secrète peut ouvrir le fichier d'archive PGP Zip généré,* et tous voient les mêmes éléments. S'il faut que différents destinataires voient des éléments différents, vous devez créer des fichiers d'archive PGP Zip distincts pour chacun.

Attention : prenez toutes les précautions nécessaires pour vous assurer que la phrase secrète de votre archive SDA PGP Zip n'est révélée à personne d'autre que les destinataires souhaités. Si la phrase secrète est révélée à des personnes non autorisées, créez une nouvelle archive SDA PGP Zip avec une phrase secrète différente. Remarque : il n'y a aucun moyen de sécuriser à nouveau le fichier d'archive original et son contenu.

Pour créer une archive SDA PGP Zip

1. Si ne vous l'avez pas encore fait, suivez la procédure de création de fichier d'archive PGP Zip comme décrit dans la section *Création d'archives PGP Zip* (à la page 276). Suivez les instructions jusqu'à l'étape 6. Ensuite, revenez à la section présente.
2. Dans la boîte de dialogue Chiffrer, sélectionnez **Archive à auto-déchiffrement de PGP**.
3. Cliquez sur **Suivant**. La boîte de dialogue Créer une phrase secrète s'affiche.
4. Pour voir les frappes à mesure que vous saisissez la phrase secrète, sélectionnez **Afficher les frappes**.
5. Dans le champ **Phrase secrète**, entrez la phrase secrète que vous voulez utiliser.

   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* (à la page 336).
6. Saisissez à nouveau votre phrase secrète dans le champ **Confirmer**.

7 Cliquez sur **Suivant**.

8 Confirmez que l'archive PGP Zip est enregistrée à l'emplacement et sous le nom de fichier que vous voulez. Si nécessaire, vous pouvez :

- modifier l'emplacement d'enregistrement du fichier en cliquant sur **Parcourir** puis en en choisissant un nouveau dans la boîte de dialogue Fichier de Windows ;
- modifier manuellement l'emplacement de l'enregistrement du fichier en saisissant le nouvel emplacement où vous aimeriez enregistrer l'archive PGP Zip ;
- modifier le nom de fichier de l'archive PGP Zip en le saisissant manuellement à la fin de la chaîne de texte de l'emplacement du fichier.

Par défaut, le nom de fichier d'une archive PGP Zip qui ne contient qu'un seul fichier, répertoire ou lecteur est le nom dudit élément, auquel vient s'ajouter l'extension `.pgp`. Si l'archive PGP Zip contient plus d'un élément, son nom de fichier est celui de l'un des éléments auquel vient s'ajouter l'extension `.pgp`. Si vous le souhaitez, modifiez le nom de fichier de l'archive PGP Zip.

9 Cliquez sur **Suivant**. L'archive SDA PGP Zip est créée.

10 Cliquez sur **Terminer**. Votre archive SDA PGP Zip est prête à être envoyée aux destinataires.

Création d'une archive uniquement signée

Utilisez **Signer uniquement** :

- quand vous n'avez pas besoin de chiffrer vos fichiers (il ne sera donc pas nécessaire de révéler une phrase secrète aux destinataires) ;
- quand vous voulez générer un fichier de signature que les destinataires peuvent utiliser pour confirmer que vous êtes l'expéditeur de l'archive PGP Zip. Chaque fichier est traité séparément et un fichier sig distinct est créé pour chaque fichier ;
- quand PGP Desktop est installé sur l'ordinateur de chacun des destinataires (Windows ou Mac OS X) ;
- quand vous voulez garantir que vous êtes la personne qui a envoyé le fichier, et que vous voulez certifier au destinataire que le fichier n'a subi aucune modification pendant le transit.

Pour les fois où vous n'avez pas besoin de chiffrer le ou les fichiers pour les destinataires, vous pouvez choisir l'option Signer uniquement. Au lieu de chiffrer vos fichiers et de les compresser en une archive PGP Zip, cette option ne fait que les compresser.

Pour chiffrer avec l'option Signer uniquement

1. Si ne vous l'avez pas encore fait, suivez la procédure de création de fichier d'archive PGP Zip comme décrit dans la section *Création d'archives PGP Zip* (à la page 276). Suivez les instructions jusqu'à l'étape 6. Ensuite, revenez à la section présente.

   Remarque : quand vous sélectionnez les fichiers pour compression et signature, l'option **Envoyer les fichiers originaux vers PGP Shredder lorsque l'opération est terminée** est ignorée même si vous la sélectionnez.

2. Dans la boîte de dialogue Chiffrer, sélectionnez **Signer uniquement**.
3. Cliquez sur **Suivant**. Le panneau **Signer et enregistrer** s'affiche.
4. Spécifiez sur votre trousseau de clés une clé privée à utiliser comme Clé de signature pour l'archive PGP Zip en cours de création.

   La clé de signature spécifiée sert à signer numériquement l'archive PGP Zip. Le ou les destinataires peuvent vérifier qui a envoyé l'archive en vérifiant la signature numérique avec la clé publique correspondante.

   - Si vous n'avez pas besoin de signer le fichier ou que vous préférez ne pas le signer, choisissez **Aucun** dans la liste Clé de signature.
   - Si vous choisissez de signer votre archive PGP Zip, choisissez votre clé dans la liste Clé de signature, puis saisissez la phrase secrète de la clé sélectionnée pour signer (et non pas la phrase secrète de sécurisation du fichier zip). Pour voir les frappes à mesure que vous saisissez la phrase secrète, sélectionnez **Afficher les frappes**.

   Si vous avez déjà saisi votre phrase secrète au cours de la session actuelle avec PGP Desktop, il est possible qu'elle soit en cache selon les paramètres d'**Options** que vous avez choisis. Dans ce cas, un message indiquant que la phrase secrète est en cache s'affiche. Même si votre phrase secrète est en cache, vous pouvez choisir de ne pas signer le fichier d'archive PGP Zip.
5. Confirmez que l'archive PGP Zip est enregistrée à l'emplacement que vous souhaitez. Si nécessaire, vous pouvez :

   - modifier l'emplacement d'enregistrement du fichier en cliquant sur **Parcourir** puis en en choisissant un nouveau dans la boîte de dialogue Fichier de Windows ;
   - modifier manuellement l'emplacement de l'enregistrement du fichier en saisissant le nouvel emplacement où vous aimeriez enregistrer l'archive PGP Zip ;

   Le nom de fichier par défaut d'une archive PGP Zip uniquement signée est le nom de l'élément auquel vient s'ajouter l'extension `.sig`.
6. Si vous préférez avoir un fichier de signature distinct avec votre archive PGP Zip, cliquez pour sélectionner **Enregistrer la ou les signatures détachées**.

7 Cliquez sur **Suivant**. L'archive PGP Zip uniquement signée est créée.

8 Cliquez sur **Terminer**.

Ouverture d'une archive PGP Zip

Pour que vous puissiez ouvrir une archive PGP Zip, PGP Desktop doit être installé sur le système.

Pour ouvrir une archive PGP Zip

1 Double-cliquez sur le fichier d'archive PGP Zip, comportant l'extension `.pgp`.

- Si l'archive PGP Zip a été sécurisée avec une clé, la boîte de dialogue Saisissez la phrase secrète d'une clé répertoriée PGP s'ouvre.
- Si l'archive PGP Zip a été sécurisée avec une phrase secrète, la boîte de dialogue Saisissez la phrase secrète PGP s'ouvre.

PGP Desktop affiche le contenu de l'archive PGP Zip. (Si l'application PGP Desktop n'est pas ouverte, elle s'ouvre et l'élément PGP Zip est actif.)

2 Pour extraire des éléments, procédez comme suit :

- Pour extraire un seul élément, cliquez dessus avec le bouton droit et sélectionnez **Extraire** dans le menu contextuel.
- Pour extraire plusieurs éléments, sélectionnez-les, cliquez sur l'un d'entre eux avec le bouton droit, puis choisissez **Extraire** dans le menu contextuel.

La boîte de dialogue Rechercher un dossier s'affiche.

3 Recherchez le dossier dans lequel vous souhaitez extraire les fichiers, puis cliquez sur OK. Pour créer un dossier, cliquez sur **Nouveau dossier**. Les fichiers sont extraits dans l'emplacement que vous avez spécifié.

Si vous extrayez les fichiers déchiffrés à partir de l'archive PGP Zip dans leur emplacement d'origine, les fichiers d'origine sont écrasés. Pour empêcher ceci, pour chaque fichier, vous êtes invité à confirmer que vous voulez écraser le fichier existant.

Ouvrir une archive SDA PGP Zip

Il n'est pas nécessaire que PGP Desktop soit installé pour ouvrir une archive SDA PGP Zip.

Pour ouvrir une archive SDA PGP Zip

1. Double-cliquez sur le fichier SDA PGP Zip (qui devrait avoir un `.exe` comme extension de fichier). La boîte de dialogue Archive à auto-déchiffrement de PGP - Veuillez saisir la phrase secrète s'affiche.
2. Confirmez que la sortie doit être extraite à l'emplacement désiré. Dans le cas contraire, cliquez sur **Parcourir** pour rectifier l'emplacement, ou saisissez-le dans le champ.

   Remarque : si vous enregistrez les fichiers déchiffrés de l'archive SDA PGP Zip dans leur emplacement d'origine, les fichiers originaux sont écrasés. Pour l'empêcher, vous serez invité à sélectionner un emplacement différent pour chaque fichier. Vous pouvez aussi saisir un nom de fichier différent. Si vous cliquez sur **Enregistrer** sans le faire, une boîte de dialogue d'avertissement s'affiche. Si vous passez outre, le fichier de l'archive SDA PGP Zip écrasera l'original.
3. Saisissez la phrase secrète pour l'archive SDA PGP Zip, puis cliquez sur **OK**. L'archive SDA PGP Zip est déchiffrée.

Modification d'une archive PGP Zip

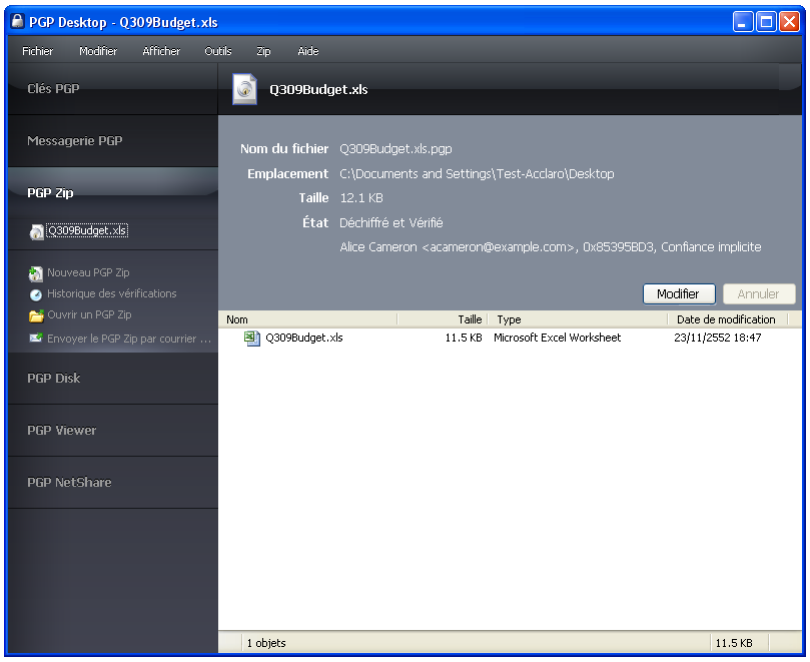
Les archives PGP Zip ne sont pas statiques. Vous pouvez à tout moment :

- en extraire des fichiers ;
- y ajouter des fichiers ;
- éditer les paramètres de l'archive elle-même.

Pour modifier une archive PGP Zip

1. Dans PGP Desktop, cliquez sur la boîte de contrôle PGP Zip. La boîte de contrôle PGP Zip est mise en surbrillance.
2. Cliquez sur le nom de l'archive PGP Zip que vous voulez modifier dans la liste des archives PGP Zip dans la zone supérieure de la boîte de contrôle PGP Zip. Les paramètres définis pour l'archive et les fichiers et/ou les dossiers que celle-ci contient s'affichent.

Si l'archive PGP Zip que vous voulez ouvrir n'est pas dans la liste, cliquez sur **Ouvrir un PGP zip**, accédez au fichier `.pgp`, sélectionnez-le puis cliquez sur **Ouvrir**.



3 Pour modifier les paramètres de l'archive PGP Zip, cliquez sur **Modifier** et effectuez les modifications souhaitées :

- **Pour ajouter un fichier à une archive PGP Zip**, cliquez sur **Ajouter fichiers** dans la boîte de contrôle PGP Zip, sélectionnez le ou les fichiers à ajouter puis cliquez sur **Ouvrir**. Les fichiers sont ajoutés à l'archive.
- **Pour ajouter un dossier à l'archive et mettre des fichiers dans ce dossier**, cliquez sur **Nouveau dossier** dans la boîte de contrôle PGP Zip, et saisissez si vous le souhaitez un nom descriptif pour le nouveau dossier. Sélectionnez le nouveau dossier, cliquez sur **Ajouter fichiers** dans la boîte de contrôle PGP Zip, sélectionnez le ou les fichiers à ajouter au dossier, puis cliquez sur **Ouvrir**. Les fichiers sont ajoutés à l'archive dans le dossier.
- **Pour extraire un fichier d'une archive**, cliquez avec le bouton droit sur le fichier à extraire, sélectionnez **Extraire** dans le menu contextuel, spécifiez un emplacement pour le fichier, puis cliquez sur **OK**. Une copie du fichier est créée à l'emplacement indiqué ; l'original reste dans l'archive PGP Zip.
- **Pour supprimer un fichier ou un dossier d'une archive**, sélectionnez les éléments à supprimer, puis appuyez sur la touche **Supprimer** de votre clavier. Vous pouvez aussi sélectionner **Modifier > Supprimer**. Les éléments spécifiés sont supprimés.

- **Pour enregistrer les modifications apportées à une archive PGP Zip**, cliquez sur **Enregistrer** dans le coin supérieur droit de la boîte de contrôle PGP Zip ou sur **Enregistrer le PGP Zip**. Spécifiez un emplacement et un nom. Si le nom que vous sélectionnez existe déjà à cet emplacement, vous serez invité à confirmer que vous souhaitez écraser le fichier existant. Saisissez la phrase secrète qui protège l'archive, puis cliquez sur **OK**.
- **Pour modifier la clé de signature**, sélectionnez le fichier PGP Zip à modifier dans la boîte de contrôle PGP Zip, cliquez sur **Modifier** puis sélectionnez une nouvelle **Clé de signature**. Cliquez sur **Enregistrer** lorsque vous avez terminé.
- **Pour modifier le type de chiffrement** (à clé ou conventionnel), sélectionnez le fichier PGP Zip à modifier dans la boîte de contrôle PGP Zip, cliquez sur **Modifier** puis sélectionnez le type de chiffrement (**Clé** or **Conventionnel**). Cliquez sur **Enregistrer** lorsque vous avez terminé.
- **Pour ajouter des destinataires à l'archive PGP Zip**, sélectionnez le fichier PGP Zip à modifier dans la boîte de contrôle PGP Zip, cliquez sur **Modifier** puis sur **Ajouter destinataires**. Dans la boîte de dialogue Ajouter destinataires, sélectionnez les destinataires à ajouter et cliquez sur **OK**. Cliquez sur **Enregistrer** lorsque vous avez terminé.
- **Pour supprimer des destinataires de l'archive PGP Zip**, sélectionnez le fichier PGP Zip à modifier dans la boîte de contrôle PGP Zip, cliquez sur **Modifier**, sélectionnez le destinataire à supprimer puis cliquez sur **Supprimer les destinataires**. Cliquez sur **Enregistrer** lorsque vous avez terminé.

4 Quand vous avez fini, cliquez sur **Enregistrer. Vous pouvez soit écraser l'archive PGP Zip modifiée, soit l'enregistrer sous un nom différent.**

Vérification des archives PGP Zip signées

Si vous avez reçu une archive PGP Zip signée, vous devriez vérifier la signature pour en connaître l'expéditeur, et confirmer que l'archive n'a pas été falsifiée avant sa réception.

Pour vérifier une archive PGP Zip

1 Cliquez sur la boîte de contrôle PGP Zip, puis sur **Ouvrir un PGP Zip**. La boîte de dialogue Ouvrir s'affiche.

2 Accédez au fichier signé `.pgp` que vous voulez vérifier, cliquez dessus pour le sélectionner puis cliquez sur **Ouvrir**.

Si le message est chiffré en plus d'être signé, vous êtes invité à saisir la phrase secrète de votre clé privée, ou de la clé privée quelle qu'elle soit qui correspond à la clé publique ayant servi au chiffrement du message.

Si la clé privée n'est pas sur votre trousseau de clés, PGP Desktop vous indiquera qu'il est impossible de déchiffrer le message. Malheureusement, ceci signifie aussi qu'il vous est impossible de vérifier l'archive. Cliquez sur **Annuler pour mettre fin à la vérification.**

3 Saisissez la phrase secrète de la clé privée, puis cliquez sur **OK**.

Remarque : si la phrase secrète de la clé privée est en cache, vous n'êtes pas invité à la saisir.

Le contenu de l'archive est enregistré au même emplacement que l'archive PGP Zip, et l'écran Historique des vérifications affiche les informations de l'archive que vous vérifiez.

4 Pour effacer la liste des archives vérifiées, cliquez sur **Effacer l'historique des vérifications**. Toutes les listes de l'écran Historique des vérifications sont supprimées.

15 Décomposition de fichiers avec PGP Shredder

Si vous voulez détruire complètement des fichiers sensibles sans laisser aucune trace de leurs données, utilisez l'utilitaire PGP Shredder.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

Utilisation de PGP Shredder pour supprimer définitivement des dossiers et des fichiers

Si vous voulez détruire complètement des dossiers ou des fichiers sensibles, utilisez la fonctionnalité PGP Shredder. Quand vous supprimez des dossiers ou fichiers avec PGP Shredder, toutes les traces de l'élément sont enlevées.

Le principe de la fonctionnalité de PGP Shredder consiste à écraser vos données avec des données textuelles aléatoires. L'écrasement est répété plusieurs fois ou *passes*. Vous pouvez régler le nombre de passes auquel procède la fonctionnalité de PGP Shredder lors de la suppression d'un dossier dans le panneau Disque de l'écran Préférences. Pour plus d'informations sur la paramétrage des options et préférences, reportez-vous à la section *Options de disque/Préférences* (cf. "Options de l'onglet Disque" à la page 327).

La session de décomposition peut être assez longue selon des facteurs tels que le nombre de passes spécifié, la vitesse du processeur, et le nombre d'autres applications en cours d'exécution.

Remarque : il suffit de paramétrer trois passes pour que PGP Shredder excède les exigences de la norme du Ministère de la défense américain DoD 5220.22-M en matière de nettoyage de supports. Même si davantage de passes sont autorisées, le matériel de disque moderne ne nécessite pas plus de deux passes. La sécurité continue d'augmenter jusqu'à environ 28 passes. La fonctionnalité PGP Shredder peut effectuer jusqu'à 49 passes, mais n'oubliez pas que plus le nombre de passes est élevé, plus longue sera la suppression sécurisée.

Il y a plusieurs façons d'utiliser PGP Shredder :

- Utilisez l'icône PGP Shredder sur votre bureau (placée là lors de l'installation de PGP Desktop).
- Sélectionnez **Outils > Décomposer les fichiers** puis naviguez jusqu'au dossier/fichier que vous voulez décomposer.
- Utilisez les menus contextuels de Windows Explorer (cliquez avec le bouton droit sur le fichier, puis sélectionnez **PGP Desktop > Décomposer [nom-du-fichier] par PGP**).

PGP Shredder ne supprime pas les éléments suivants :

- les fichiers système Windows ou les fichiers en lecture seule.

  Remarque : le fichier de Thumbs.db, créé lors de l'affichage des graphiques des miniatures dans Windows Explorer, est un cas particulier et peut être décomposé bien que le fichier ait l'attribut système.

- Fichiers WebDav ou Sharepoint.

  Les fichiers qui peuvent être supprimés sont les fichiers locaux et les fichiers partagés CIFS.

- Les répertoires contenant des fichiers qui ne peuvent pas être supprimés.

Vous pouvez aussi utiliser PGP Desktop et son assistant de décomposition de l'espace libre par PGP pour effacer du disque de l'espace libre qui pourrait contenir des données de fichiers et programmes supprimés antérieurement.

L'utilisation de l'assistant de décomposition de l'espace libre par PGP sur des systèmes de fichiers de journalisation comme NTFS est particulièrement importante puisque ces systèmes de fichiers réalisent une seconde copie de tout ce qui est écrit sur le disque dans un journal de système de fichiers. Cette fonctionnalité aide à récupérer le disque après un incident mais représente une charge de travail supplémentaire lors de la suppression de données sensibles. La décomposition d'un fichier ne supprime pas les éventuelles entrées de journal qui peuvent avoir été créées. NTFS en particulier peut stocker de petits fichiers (moins de 1 Ko) dans les structures de données internes qui ne peuvent pas être convenablement supprimées sans l'option **Décomposer les structures de données internes NTFS** de l'assistant de décomposition de l'espace libre par PGP.

Conseil : pensez aux autres occurrences des données susceptibles d'être conservées ailleurs sur votre disque, par exemple dans des fichiers temporaires. Veillez donc à utiliser PGP Whole Disk Encryption pour protéger toutes les données de votre système.

Décomposition des fichiers avec l'icône PGP Shredder sur votre bureau

▸ **Pour décomposer des fichiers avec l'icône PGP Shredder située sur votre bureau**

1. Glissez et déplacez les fichiers/dossiers à décomposer sur l'icône PGP Shredder. Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers et/ou les dossiers indiqués.
2. Cliquez sur **Oui.** Les fichiers sont supprimés de votre système de manière sécurisée.

Décomposition de fichiers à partir de PGP Desktop

▸ **Pour décomposer des fichiers dans PGP Desktop**

1. Dans la fenêtre principale de l'application PGP Desktop, sélectionnez **Outils > Décomposer les fichiers**. La boîte de dialogue Ouvrir s'affiche.
2. Sélectionnez les fichiers de votre système à décomposer, puis cliquez sur **Ouvrir.** 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 **Oui** . Les fichiers sont supprimés de votre système de façon sécurisée.

Décomposition de fichiers dans l'Explorateur Windows

▸ **Pour décomposer des fichiers en cliquant dessus avec le bouton droit dans l'Explorateur Windows**

1. Dans l'Explorateur Windows, cliquez avec le bouton droit sur les fichiers/dossiers à 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.

2 Cliquez sur **Oui** . Les fichiers sont supprimés de votre système de façon sécurisée.

Utilisation de l'assistant de décomposition de l'espace libre par PGP

Pour décomposer de l'espace libre sur vos disques

1 Avec PGP Desktop ouvert, sélectionnez **Outils** > **Décomposer de l'espace libre par PGP**. L'écran Introduction de l'assistant de décomposition de l'espace libre par PGP s'affiche.

2 Lisez les informations, puis cliquez sur **Suivant.** La boîte de dialogue Collecte des informations en cours s'affiche.

3 Dans le champ **Décomposer le lecteur**, sélectionnez le disque ou le volume que vous voulez décomposer et le nombre de **passes** que PGP doit effectuer pour décomposer l'espace libre. Bien qu'avec PGP Shred Free Space Assistant, trois passes suffisent pour supprimer les données de manière sécurisée, vous pouvez spécifier jusqu'à 49 passes. Le nombre de passes recommandé est :

- 3 passes pour un usage personnel ;
- 10 passes pour un usage commercial ;
- 18 passes pour un usage militaire ;
- 26 passes pour une sécurité maximale.

4 Choisissez s'il faut décomposer les structures de données internes NTFS. Cette option n'est pas disponible sur tous les systèmes.

Attention : Si la partition sélectionnée *n'est pas* votre partition de démarrage, vous pouvez exécuter une opération de décomposition intensive et écraser les structures de données internes NTFS qui pourraient contenir des données résiduelles. La partition sera entièrement remplie pendant ce processus, et donc *vous ne devriez pas utiliser le disque pour quoi que ce soit d'autre tant que l'opération de décomposition de l'espace libre est en cours*. Certaines de ces structures ne sont généralement pas considérées comme espace libre sur votre lecteur, mais les techniques que cette option emploie entraîneront leur décomposition. Cette option n'augmente pas le risque d'incident de votre disque suite à l'opération de décomposition.

5 Cliquez sur **Suivant.** La boîte de dialogue Effectuer une décomposition s'affiche avec des informations statistiques sur le lecteur ou le volume sélectionné.

6 Effectuez l'une des opérations suivantes :

- Pour commencer à décomposer l'espace libre immédiatement, cliquez sur **Démarrer la décomposition.** L'assistant de décomposition de l'espace libre par PGP analyse puis décompose les restes fragmentaires du disque ou du volume spécifié.

  Quand la session de décomposition est terminée, un message s'affiche près du bas de l'écran Effectuer une décomposition indiquant que le lecteur sélectionné a été décomposé.

- Pour planifier une heure pour l'opération de décomposition de l'espace libre, cliquez sur **Planification**. Un message s'affiche et vous informe que le planificateur de tâches de Windows est utilisé lors de la planification des opérations de décomposition de l'espace libre par PGP, et que l'exécution de la tâche exige un mot de passe d'ouverture de session Windows.

  Pour planifier la tâche, cliquez sur **OK**, saisissez votre mot de passe d'ouverture de session Windows dans la boîte de dialogue Saisissez la phrase secrète de confirmation PGP, puis saisissez les informations de planification.

  Pour annuler la tâche et retourner à la boîte de dialogue Effectuer une décomposition, cliquez sur **Annuler**.

7 Cliquez sur **Suivant.** La boîte de dialogue Fin s'affiche.

8 Cliquez sur **Terminer**.

Planification de la décomposition de l'espace libre

Utilisez le planificateur de tâches de Windows pour planifier une décomposition périodique de l'espace libre sur votre système.

Pour planifier la décomposition de l'espace libre

1 Suivez les étapes décrites dans la section *Utilisation de l'assistant de décomposition de l'espace libre par PGP* (à la page 296) jusqu'à l'affichage de la boîte de dialogue Effectuer une décomposition.

2 Cliquez sur **Planification**.

3 Un message s'affiche et vous informe que le planificateur de tâches de Windows est utilisé lors de la planification des opérations de décomposition de l'espace libre par PGP, et que l'exécution de la tâche exige un mot de passe d'ouverture de session Windows. Pour continuer, cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète de confirmation PGP s'affiche.

4 Saisissez votre mot de passe de session Windows dans le premier champ, puis à nouveau dans le second champ pour le confirmer, puis cliquez sur **OK.** La boîte de dialogue Planificateur de tâches de Windows s'affiche.

5 Dans la zone **Tâche planifiée**, spécifiez la fréquence d'exécution de la tâche :

- **Tous les jours.** La tâche est exécutée une fois à l'heure que vous spécifiez et les jours que vous indiquez. Cliquez sur **OK** pour fermer la boîte de dialogue, puis saisissez l'heure d'exécution quotidienne de la tâche dans la zone de texte Heure de début.
- **Toutes les semaines.** La tâche est exécutée sur une base hebdomadaire à la date et à l'heure que vous spécifiez. Saisissez le nombre de semaines souhaité entre chaque décomposition de disque dans la zone de texte, puis choisissez un jour dans la liste Planification hebdomadaire.
- **Tous les mois.** La tâche est exécutée sur une base mensuelle à la date et à l'heure que vous spécifiez. Saisissez l'heure dans la zone de texte, puis saisissez le jour du mois où la tâche est exécutée. Cliquez sur **Choix des mois** pour spécifier les mois d'exécution de la tâche.
- **Une seule fois.** La tâche est exécutée exactement une fois à la date et à l'heure que vous spécifiez. Saisissez l'heure dans la zone de texte, puis sélectionnez un mois et une date dans la zone de texte Exécuter le.
- **Au démarrage du système.** La tâche est exécutée uniquement au démarrage du système.
- **En cas de connexion.**La tâche est exécutée quand vous ouvrez une session sur votre ordinateur.
- **Si inactif.** La tâche est exécutée quand votre système est inactif pendant une période de temps à spécifier dans la zone de texte des minutes.

6 Dans le champ de **Heure de début**, saisissez l'heure de démarrage de la tâche.

7 Dans le champ Planification quotidienne, spécifiez la fréquence d'exécution de la tâche.

8 Cliquez sur **Avancées** pour ouvrir une boîte de dialogue où vous pouvez sélectionner des options de planification supplémentaires, comme la date de début, la date de fin, et la durée de la tâche.

9 Cliquez sur **OK.** Une boîte de dialogue de confirmation apparaît.

Votre nouveau dossier PGP ou tâche de nettoyage d'espace libre est maintenant planifiée. Pour modifier ou supprimer vos tâches PGP, utilisez le planificateur de tâches de Windows.

16 Stockage des clés sur des cartes à puce et jetons

Utilisez PGP Desktop pour créer une paire de clés PGP sur une carte à puce ou un jeton, ou pour copier une paire de clés PGP sur une carte à puce ou un jeton. Les deux options vous apportent une couche de sécurité supplémentaire puisque vous pouvez garder votre paire de clés PGP sur vous, sur votre carte à puce ou votre jeton, au lieu de la laisser sur votre système : une paire de clés PGP sur une carte à puce ou un jeton est moins vulnérable que la même paire de clés stockée sur votre ordinateur car vous pouvez garder la carte à puce ou le jeton sur vous. Cette section décrit l'utilisation des cartes à puce avec PGP Desktop.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

À propos des cartes à puce et des jetons

Pour utiliser PGP Desktop avec une carte à puce ou un jeton d'un fabricant particulier, vous devez avoir un lecteur de carte à puce compatible (si vous utilisez une carte à puce) et les pilotes logiciels appropriés doivent être installés sur votre système (pour les cartes à puce et les jetons). Les pilotes *doivent* inclure la bibliothèque PKCS-11 (norme d'interface de jeton de chiffrement).

PGP Corporation recommande fortement d'utiliser les pilotes logiciels du fabricant de la carte à puce ou du jeton.

PGP Desktop reconnaît et fonctionne avec une grande variété de cartes à puce, y compris celles d'Athena, d'AET SafeSign, d'Axalto (anciennement Schlumberger), de SafeNet (anciennement Rainbow), d'Aladdin, et de GemPlus. PGP Desktop fonctionne aussi avec les cartes d'accès Common Access Card du Ministère de la défense américain avec le profil ActivCard Gold 2.0.

En plus de ceux-ci, PGP Desktop reconnaît et fonctionne avec les cartes à puce des fournisseurs qui incluent une bibliothèque PKCS-11 conforme aux normes dans leurs pilotes logiciels. Si la bibliothèque PKCS-11 d'un fournisseur est installée sur votre système et fonctionne avec d'autres applications PKCS-11, telles que Mozilla Firefox ou Thunderbird, il est probable que PGP Desktop la reconnaisse et utilise les cartes à puce de ce fournisseur.

Quand vous créez et stockez une paire de clés PGP sur une carte à puce, vous accédez à la clé privée en utilisant le code confidentiel de la carte à puce plutôt qu'une phrase secrète. Si vous avez une carte à puce qui contrôle sa propre authentification (par exemple, avec son propre clavier numérique ou via un périphérique biométrique), PGP Desktop fonctionne avec ces cartes à puce ; quand PGP Desktop affiche une boîte de dialogue de phrase secrète, ne saisissez pas de phrase secrète, cliquez simplement sur OK. Le périphérique devrait alors afficher sa propre méthode d'authentification.

Remarque : la partie privée de votre paire de clés générée sur une carte à puce ne quitte jamais le périphérique, elle ne peut pas être exportée. Les opérations de déchiffrement et de signature se produisent directement sur le périphérique. Si vous générez une paire de clés sur votre ordinateur plutôt que sur la carte à puce, puis que vous la copiez sur votre carte à puce en laissant la paire de clés sur votre ordinateur, vous pouvez toujours exporter la partie privée de votre paire de clés à partir de votre ordinateur.

Cartes Common Access Card (CAC) du Ministère de la défense américain

Les cartes Common Access Card du Ministère de la défense américain ont un fonctionnement légèrement différent des autres cartes à puce. Elles sont en lecture seule et comprennent deux certificats distincts : l'un pour signer et l'autre pour chiffrer. PGP Desktop filtre les deux certificats selon l'utilisation souhaitée. Par exemple, quand vous êtes invité à sélectionner une clé pour signer un fichier, seul le certificat de signature d'un CAC apparaît dans la liste.

Cartes JavaCard

Les cartes à puce d'Axalto sont des cartes JavaCard. Un petit module Java, ou applet Java, est exécuté sur la carte. La carte peut être configurée pour exécuter des applets différents qui modifient le comportement ou la configuration de la carte à puce, un processus appelé personnalisation. Pour utiliser des cartes JavaCard avec PGP Desktop, seuls quelques-uns des profils de personnalisation disponibles sont possibles.

De plus, tous les profils de personnalisation actuellement disponibles exigent quelques modifications mineures de leurs configurations pour fonctionner avec PGP Desktop. En particulier :

- le profil doit activer la prise en charge de PKCS-11. Dans la plupart des cas, le nom « Netscape » ou « Entrust » apparaît dans les intitulés des profils qui prennent en charge PKCS-11.
- Une clé PGP Desktop utilise au moins deux clés privées PKCS-11. Pour fonctionner avec PGP Desktop, un profil doit avoir une valeur de 2 ou plus dans le nombre maximum de clés privées autorisé.

Pour plus d'informations, reportez-vous à la documentation de votre carte JavaCard.

Cartes à puce compatibles

PGP Desktop reconnaît et prend en charge les cartes suivantes :

- Les cartes Common Access Card (CAC) du Ministère de la défense américain avec le profil **ActivCard** Gold 2.0. Pour plus d'informations sur ce profil, consultez le *site Web d'ActivCard* (www.activcard.com).
- Les cartes à puce **AET SafeSign**, y compris la carte ASEKey 1.0. Pour plus d'informations sur ces cartes à puce, consultez le *site Web de Cryptoshop* (www.cryptoshop.com).
- Les cartes à puce **Aladdin**, y compris les jetons eToken PRO USB 16K, 32K et 64K, Aladdin eToken NG-OTP 32K et eToken PRO Java. Pour plus d'informations sur les produits eToken d'Aladdin, consultez le *site Web d'assistance d'Aladdin* (http://www.aladdin.com/support/default.asp).

- Les cartes à puce **Athena Smart Card Solutions**, y compris le jeton ASEKey USB. Pour plus d'informations sur ces cartes à puce, consultez le *site Web d'Athena Smart Card* (www.athena-scs.com).
- Les cartes à puce **Axalto** (anciennement Schlumberger), y compris la carte Cryptoflex 32K. Pour plus d'informations sur ces cartes à puce, consultez le *site Web d'Axalto* (www.axalto.com).
- Les cartes à puce **Axalto Cyberflex Access 32K V2**. Pour plus d'informations sur ces cartes à puce, consultez le *site Web d'Axalto* (www.axalto.com).
- Les **jetons EMC RSA SecurID SID800** (v1 et 2). Pour plus d'informations sur les jetons d'EMC, consultez le *site Web* (http://www.rsa.com/) EMC/RSA.
- Les cartes à puce **Gemalto .NET v2**. Pour plus d'informations sur ces cartes à puce, consultez le *site Web de Gemalto* (http://www.gemalto.com).
- Les cartes à puce **GemPlus**, y compris les cartes SafesITe et GemXpresso Pro qui utilisent les bibliothèques GemSafe Libraries 4.2.0-015 (Gold). Pour plus d'informations sur ces cartes à puce, consultez le *site Web de GemPlus* (www.gemplus.com).
- Les cartes individuelles de vérification d'identité **Giesecke and Devrient** Sm@rtCafe Expert 3.2 qui utilisent le logiciel client ActivClient version 6.1. Pour plus d'informations sur ces cartes à puce, consultez le *site Web de Giesecke and Devrient* (http://www.gi-de.com/).
- Les cartes individuelles de vérification d'identité **Oberthur** ID-One Cosmo V5.2D qui utilisent le logiciel client ActivClient version 6.1. Pour plus d'informations sur ces cartes à puce, consultez le *site Web d'Oberthur* (http://www.oberthurcs.com/index.aspx).
- Les cartes à puce **SafeNet**, y compris la carte iKey 2032. (PGP Desktop ne prend plus en charge les cartes SafeNet iKey 1000 et 4000.) Pour plus d'informations sur les cartes à puce et les jetons USB de SafeNet, consultez le *site Web de SafeNet* (www.safenet-inc.com/products/tokens/index.asp).
- Cartes **T-Systems** Telesec NetKey 3.0 et TCOS 3.0 IEI. Pour plus d'informations sur ces cartes à puce, consultez le *site Web de T-Systems* (www.t-systems.com).

Par ailleurs, PGP Desktop reconnaît et prend en charge les cartes à puce d'autres fabricants si ces derniers incluent une bibliothèque PKCS-11 conforme aux normes dans leurs pilotes logiciels. Dans le cas où une carte à puce non standard ne fonctionne pas avec PGP Desktop, **Clés de carte à puce** n'apparaît pas dans le panneau de contrôle Clés PGP lorsque la carte à puce est installée sur le système.

Reconnaissance des cartes à puce

Avant d'examiner les propriétés d'une carte à puce que vous voulez utiliser avec PGP Desktop, ou de créer une paire de clés PGP sur une carte à puce, assurez-vous que PGP Desktop reconnaît que la carte à puce que vous voulez utiliser est disponible sur le système.

Les exigences générales sont les suivantes :

- Les pilotes logiciels de la carte à puce, avec prise en charge de PKCS-11, doivent être installés sur le système.
- La carte à puce doit être installée sur le système. Pour un jeton USB, cela signifie généralement qu'il est inséré dans un port USB. Pour une carte à puce, cela signifie généralement qu'elle est insérée dans le lecteur de carte à puce approprié.

Une fois les pilotes et la carte à puce installés, vérifiez que PGP Desktop reconnaît le système. Il y a deux façons de le faire :

- Le plus simple pour déterminer si PGP Desktop « voit » une carte à puce est d'ouvrir PGP Desktop puis de cliquer sur la boîte de contrôle Clés PGP. Si l'entrée « clés de carte à puce » est dans la liste au-dessous de « Toutes les clés » dans la boîte de contrôle Clés PGP, alors PGP Desktop voit la carte à puce sur le système.
- Une façon légèrement plus compliquée est d'ouvrir PGP Desktop, de cliquer sur boîte de contrôle Clés PGP puis, dans le menu **Fichier**, de sélectionner **Nouvelle clé PGP**. Quand l'écran Assistant de génération de clé PGP est affiché, regardez en bas. Si la case **Générer une clé sur le jeton : <informations de la carte à puce>** est cochée, alors PGP Desktop voit la carte à puce sur le système. Cette méthode a un léger avantage sur la méthode précédente : PGP Desktop vous montre les informations sur la carte à puce donnée qu'il voit sur le système.

Examen des propriétés de la carte à puce

Une clé PGP stockée sur une carte à puce est indiquée dans l'écran PGP Desktop par une icône particulière montrant une clé sur une carte. Dans ses propriétés, vous pouvez trouver des informations sur la carte à puce elle-même, comme le fabricant, le numéro de série et les types de clé pris en charge.

Pour afficher les propriétés d'une carte à puce

1. Insérez la carte à puce dans le lecteur de carte à puce ou introduisez le jeton dans un port USB. La clé s'affiche dans la section Clés de carte à puce de la boîte de contrôle Clés PGP.
2. Ouvrez PGP Desktop.

3 Mettez en surbrillance la clé dont vous voulez afficher les propriétés.

Sélectionnez **Clés > Propriétés de la carte à puce**. La boîte de dialogue Propriétés de la carte à puce PGP s'affiche et fournit des informations sur la carte à puce où réside la clé :

- le nom du fabricant ;
- le modèle de la carte à puce ;
- le numéro de série associé à la carte à puce ;
- les capacités de la carte à puce, y compris le type de clé PGP que la carte peut stocker et le nombre de caractères que peut contenir le code confidentiel ;
- le nombre total de clés privées que vous avez actuellement sur la carte à puce, y compris les sous-clés.

4 Cliquez sur **OK.**

Génération d'une paire de clés PGP sur une carte à puce

Pour générer une paire de clés PGP sur une carte à puce

1 Insérez la carte à puce dans le lecteur de carte à puce ou introduisez le jeton dans un port USB. La clé s'affiche dans la section Clés de carte à puce de la boîte de contrôle Clés PGP.

2 Ouvrez PGP Desktop.

3 Cliquez sur la boîte de contrôle Clés PGP. Si la carte à puce est détectée, l'entrée « Clés de carte à puce » est affichée dans la boîte de contrôle Clés PGP.

4 Sélectionner **Fichier > Nouvelle clé PGP**. La boîte de dialogue Assistant de génération de clé PGP s'affiche.

PGP Desktop reconnaît les pilotes logiciels d'un seul fabricant de carte à puce à la fois. Si vous avez des pilotes logiciels de plus d'un fabricant de carte à puce sur votre système, vous devrez spécifier de quel fabricant proviennent les cartes à puce que vous voulez utiliser avec PGP Desktop. Pour plus d'informations, reportez-vous à la section *Utilisation de plusieurs cartes à puce* (à la page 309).

5 Sélectionnez la case nommée **Générer une clé sur le jeton : [nom de la carte à puce ou du jeton sur le système]** puis cliquez sur **Suivant**. La boîte de dialogue Nom et affectation de messagerie s'affiche.

6 Saisissez votre nom dans le champ **Nom complet** et votre adresse de courrier électronique dans le champ **Adresse de courrier électronique principale**. Si vous voulez entrer plus d'une adresse de courrier électronique pour cette clé, cliquez sur **Plus** et saisissez la ou les adresses supplémentaires dans les champs **Autres adresses**.

Conseil : il n'est pas absolument nécessaire de saisir vos vrais nom ou adresse de courrier électronique. Les autres personnes vous identifieront plus facilement en tant propriétaire de votre clé publique si vous utilisez votre vrai nom.

7 Pour spécifier les paramètres de clé avancés, cliquez sur **Avancé**. La boîte de dialogue Paramètres de clé avancés s'affiche. Spécifiez les paramètres suivants :

- **Type de clé** : RSA (les clés Diffie-Hellman/DSS ne sont pas prises en charge)
- **Taille de clé** : De 1028 à 2048
- **Expiration** : Jamais ou une date que vous spécifiez
- **Chiffrements autorisés** : AES, CAST, TripleDes, IDEA et Twofish
- **Chiffrement par défaut** : Veuillez choisir un des algorithmes autorisés
- **Hachages autorisés** : SHA-2-256, SHA-2-384, SHA-2-512, RIPEMD-160, SHA-1, MD-5
- **Hachage par défaut** : Veuillez choisir un des hachages autorisés

Certains paramètres ne sont peut-être pas disponibles si la carte à puce que vous utilisez ne les prend pas en charge.

Cliquez sur **OK** pour enregistrer vos paramètres et fermez la boîte de dialogue Paramètres de clé avancés.

8 Cliquez sur **Suivant**.

9 Dans la boîte de dialogue Affectation de la phrase secrète, saisissez le code confidentiel de la carte à puce. Le code confidentiel sert de phrase secrète pour la clé. Normalement, afin de renforcer le niveau de sécurité, les caractères que vous saisissez pour la phrase secrète ne sont pas visibles à l'écran. Cependant, si vous êtes certain que personne ne vous voit, vous pouvez afficher les caractères saisis pour la phrase secrète en cochant la case **Afficher les frappes.**

10 Cliquez sur **Suivant** pour lancer le processus de génération de clé. PGP Desktop génère votre nouvelle paire de clés directement sur la carte à puce. Ce processus peut durer plusieurs minutes.

11 Quand le processus de génération de clé indique qu'il a terminé, cliquez sur **Suivant**. Vous êtes invité à ajouter à PGP Global Directory la partie de clé publique de la clé que vous venez de créer.

12 Lisez le texte à l'écran et effectuez l'une des opérations suivantes :

- Pour poster votre clé publique dans PGP Global Directory, cliquez sur **Suivant**.
- Pour empêcher que votre clé publique soit postée dans PGP Global Directory, cliquez sur **Ignorer**.

13 Cliquez sur **Terminé**. Votre nouvelle paire de clés est générée et directement stockée sur votre carte à puce.

Parce que la partie privée de votre paire de clés réside uniquement sur votre carte à puce, quand vous enlevez la carte à puce du système, l'icône de clé devient une clé simple pour refléter le fait que la partie publique reste dans trousseau de clés mais que la partie privée a été enlevée en même temps que la carte à puce.

Copie de votre clé publique d'une carte à puce sur un trousseau de clés

Le stockage de vos clés sur une carte à puce vous permet d'aller physiquement à un ordinateur doté d'un lecteur de carte à puce compatible ou d'un port USB libre ainsi que de PGP Desktop et des pilotes appropriés, et de copier automatiquement la partie *publique* de votre paire de clés dans le trousseau de clés PGP Desktop de ce système.

Pour copier votre clé publique de votre carte à puce dans le trousseau de clés d'un autre utilisateur :

1 Insérez la carte à puce dans le lecteur de carte à puce ou introduisez le jeton dans un port USB. La clé s'affiche dans la section Clés de carte à puce de la boîte de contrôle Clés PGP.

2 Ouvrez PGP Desktop.

3 Attendez que votre clé s'affiche dans PGP Desktop. Quand vous voyez votre clé affichée, c'est le signe que votre clé publique a été copiée sur le système.

4 Retirez votre carte à puce du système. Votre clé publique reste enregistrée dans le système.

Copie d'une paire de clé du trousseau de clés sur une carte à puce

PGP Desktop vous permet de copier une paire de clé de votre système sur une carte à puce. Vous pouvez ainsi facilement sauvegarder votre paire de clé et/ou distribuer votre clé publique. Seules les clés RSA peuvent être copiées sur une carte à puce.

Remarque : vous ne pouvez pas copier les clés Diffie-Hellman/DSS sur une carte à puce.

La copie d'une paire de clé et sa création directement sur la carte à puce (non disponible pour toutes les cartes à puce) sont des procédures différentes. Lorsque vous créez une paire de clés directement sur une carte à puce, la carte *doit* se trouver sur le système pour que vous puissiez utiliser votre clé privée.

Lorsque vous copiez une paire de clés existante sur une carte à puce, la clé privée est conservée sur la carte *et sur le système* (sauf si vous décidez de la supprimer du système).

Deux raisons principales justifient la copie d'une paire de clés existante sur une carte à puce :

- Vous conservez une sauvegarde de la paire de clés sur le système et copiez la clé publique de votre carte à puce sur les trousseaux d'autres personnes. Vous disposez ainsi de deux copies d'une même clé privée : une sur le système où elle a été créée et une autre sur la carte à puce.
- Vous conservez une copie unique de la clé privée, comme si vous l'aviez créée directement sur la carte à puce. Vous devez alors supprimer la clé privée du système (PGP Desktop vous en donne la possibilité). Sélectionnez l'option permettant de supprimer la clé privée de votre système, si vous avez déjà utilisé les cartes à puce après la création de la paire de clés, mais souhaitez disposer de la paire de clés sur votre carte à puce sans créer une nouvelle paire.

Lorsque vous copiez votre paire de clés PGP sur une carte à puce, la phrase secrète associée est automatiquement remplacée par le code confidentiel de la carte à puce. Toutefois, la phrase secrète de la paire de clés stockée sur le système, et qui a été copiée sur la carte à puce, *ne change pas*. Vous possédez deux copies de la même paire de clés, chacune disposant de sa propre phrase secrète.

Si vous décidez de supprimer la clé privée du système et de conserver uniquement celle sur votre carte à puce, la phrase secrète associée correspond au code confidentiel de la carte à puce.

Copie d'une paire de clé PGP existante sur la carte à puce

1. Insérez la carte à puce dans le lecteur de carte ou introduisez le jeton dans un port USB. La clé s'affiche dans la section Clés de carte à puce de la boîte de contrôle Clés PGP.
2. Ouvrez PGP Desktop.
3. Cliquez avec le bouton droit sur la paire de clés à copier et sélectionnez **Ajouter à > Clés de carte à puce**. Une boîte de dialogue d'avertissement vous informe que lorsque la paire de clés est copiée sur la carte à puce, la phrase secrète PGP associée est automatiquement remplacée par le code confidentiel de la carte.
4. Cliquez sur **OK** pour continuer. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
5. Tapez la phrase secrète de votre clé, puis cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
6. Tapez le code confidentiel de la carte à puce, puis cliquez sur **OK**. La paire de clés est copiée sur la carte à puce. Un message de PGP Desktop vous invite à supprimer la partie privée de la paire de clés de votre trousseau, si vous le souhaitez, afin de la conserver uniquement sur la carte à puce.
7. Effectuez l'une des opérations suivantes :
   - Pour supprimer la partie privée de la paire de clés de votre trousseau, cliquez sur **Oui**. La partie privée de votre paire de clés est supprimée du trousseau de clés sur le système et existe seulement sur la carte à puce.
   - Pour conserver la partie privée de la paire de clés sur le trousseau, cliquez sur **Non**. La partie privée n'est pas supprimée et vous disposez alors de deux copies de la même paire de clés (une sur le système et une autre sur la carte à puce).

Effacement des clés de votre carte à puce

Vous pouvez supprimer toutes les données stockées sur une carte à puce avec la fonctionnalité **Nettoyer le contenu** dans la boîte de dialogue Propriétés de carte à puce.

Pour nettoyer une carte à puce

1. Insérez la carte à puce dans le lecteur de carte à puce ou introduisez le jeton dans un port USB. La clé s'affiche dans la section Clés de carte à puce de la boîte de contrôle Clés PGP.
2. Ouvrez PGP Desktop.

3 Dans la boîte de dialogue Clés PGP, sélectionnez **Clés de carte à puce**. Les clés PGP de la carte à puce s'affichent.

4 Sélectionnez les cartes à puce ou les jetons que vous voulez nettoyer.

5 Sélectionnez **Clés > Nettoyer la carte à puce**. PGP Desktop vous invite à confirmer que voulez vous supprimer toutes les clés actuellement sur la carte à puce ou le jeton.

6 Cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.

7 Saisissez le code confidentiel de la carte à puce. Normalement, afin de renforcer le niveau de sécurité, les caractères que vous saisissez pour la phrase secrète ne sont pas visibles à l'écran. Cependant, si vous êtes certain que personne ne vous voit, vous pouvez afficher les caractères saisis pour la phrase secrète en cochant la case **Afficher les frappes**.

8 Cliquez sur **OK**. PGP Desktop supprime toutes les clés stockées sur la carte à puce.

Utilisation de plusieurs cartes à puce

PGP Desktop est compatible avec les cartes à puce d'un large éventail de fabricants. En même temps, PGP Desktop ne fonctionne qu'avec des cartes à puce d'un seul fabricant à la fois.

Au démarrage, PGP Desktop cherche automatiquement dans votre système les pilotes logiciels qui prennent en charge les cartes à puce d'un fabricant particulier. Quand il trouve ces pilotes logiciels, il les charge : l'hypothèse est que vous avez des cartes à puce de ce fournisseur et que vous voulez les utiliser.

Si seuls les pilotes logiciels d'un fournisseur sont installés sur votre système, cette méthode fonctionne parfaitement ; PGP Desktop trouve automatiquement les pilotes logiciels et vous permet d'utiliser les cartes à puce de ce fournisseur. Vous n'avez rien à faire ; ça fonctionne, tout simplement.

Cependant, en certaines occasions vous pouvez avoir besoin d'utiliser les cartes à puce de plus d'un fournisseur. Dans ce cas, quand vous avez besoin des pilotes logiciels de plus d'un fournisseur sur un système, vous devez indiquer à PGP Desktop le fournisseur des cartes à puce que vous voulez utiliser. Autrement, PGP Desktop n'a pas la capacité de déterminer les pilotes logiciels à utiliser et peut sélectionner ceux dont vous n'avez pas besoin.

Pour spécifier les pilotes logiciels des cartes à puce

1 Ouvrez PGP Desktop.

2 Sélectionnez **Outils > Options de PGP**. La boîte de dialogue Options PGP s'affiche.

3 Cliquez sur l'onglet Clés.

4 Dans la section **Synchronisation**, dans la liste **Synchroniser le trousseau de clés avec les jetons et les cartes à puce, sélectionnez le fournisseur pour les pilotes logiciels que vous voulez utiliser :**

- Quand vous n'avez les pilotes logiciels que d'un seul fournisseur sur votre système, utilisez le paramètre par défaut **Automatiquement**.
- Pour empêcher PGP Desktop d'utiliser des cartes à puce quel que soit le fournisseur, sélectionnez **Aucun**.
- Pour spécifier un fournisseur qui n'est *pas* dans la liste, sélectionnez **Autre.** Dans la boîte de dialogue Sélectionner le pilote de la carte à puce, allez au fichier DLL des pilotes logiciels du fournisseur de votre carte à puce, sélectionnez-le puis cliquez sur **Ouvrir.** Vous pouvez dorénavant utiliser des cartes à puce prises en charge par le fichier de pilotes logiciels que vous avez sélectionné.

PGP Desktop suppose désormais que les cartes à puce utilisées seront celles du fournisseur sélectionné. Si vous ajoutez une carte à puce d'un autre fournisseur à votre système, PGP Desktop ne la reconnaîtra pas. Vous devrez suivre cette procédure pour modifier le fournisseur de carte à puce.

Jetons spéciaux

Lorsque PGP Desktop chiffre l'ensemble du disque de *démarrage* du système, l'authentification au démarrage s'effectue au moyen d'un jeton Aladdin eToken Pro USB (pour plus d'informations sur la protection d'un disque de démarrage avec PGP Whole Disk Encryption, reportez-vous à la section *Protection des disques à l'aide de PGP Whole Disk Encryption* (à la page 149)). Dans ce cas, seule cette méthode d'authentification est possible. Pour en savoir plus sur la configuration du jeton, consultez la section *Configuration du jeton Aladdin eToken* (à la page 310).

Configuration du jeton Aladdin eToken

Vous devez disposer d'un jeton Aladdin eToken Pro USB avec une paire de clés PGP pour utiliser la fonctionnalité PGP Whole Disk Encryption de PGP Desktop pour Windows.

Pour créer un jeton Aladdin eToken Pro USB pour PGP Whole Disk Encryption

1 Vous devez obtenir un jeton Aladdin eToken Pro USB. Seul ce jeton peut être utilisé avec PGP Whole Disk Encryption. Trois modèles sont disponibles : 16K, 32K ou 64K. Les modèles 16K et 32K prennent en charge les clés 1 024 bits et le modèle 64K les clés jusqu'à 2 048 bits.

2 Veillez à installer le pilote Aladdin approprié sur votre système. Pour plus d'informations sur les pilotes Aladdin, consultez la section *Pilotes requis pour le jeton Aladdin eToken* (à la page 167).

   Lorsque le pilote est installé, PGP Desktop affiche **Clés de carte à puce** dans le panneau de contrôle Clés PGP.

3 Ouvrez PGP Desktop pour Windows.

4 Créez une paire de clés sur le jeton Aladdin eToken (reportez-vous aux instructions de la section *Génération d'une paire de clés PGP sur une carte à puce* (à la page 304)) ou copiez une paire de clés existante sur le jeton par le biais du menu contextuel **Ajouter à** (reportez-vous aux instructions de la section *Copie d'une paire de clés du trousseau de clés sur une carte à puce* (cf. "Copie d'une paire de clé du trousseau de clés sur une carte à puce" à la page 307)).

   Vous pouvez uniquement transférer une paire de clés sur un jeton pour une clé RSA 1 024 bits ou 2 048 bits. Le jeton Aladdin eToken Pro ne prend pas en charge les clés d'autres tailles ou DH/DSS.

   Lorsque vous créez ou transférez une paire de clés sur le jeton, la phrase secrète associée est remplacée par le code confidentiel du jeton. Le code confidentiel par défaut du jeton Aladdin eToken Pro est 1234567890. Il est communément admis, alors n'oubliez pas de le modifier à l'aide du logiciel Aladdin.

5 Vous pouvez maintenant utiliser la paire de clés PGP sur le jeton Aladdin eToken avec PGP Whole Disk Encryption.

A Définition des options de PGP Desktop

PGP Desktop est configuré pour s'adapter aux exigences de la plupart des utilisateurs, mais vous avez la possibilité de régler les paramètres en fonction de vos besoins. Cette section décrit les options réglables dans PGP Desktop.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.

Contenu du chapitre

Accès à la boîte de dialogue Options de PGP

Accès aux options de PGP

1 Effectuez l'une des opérations suivantes :

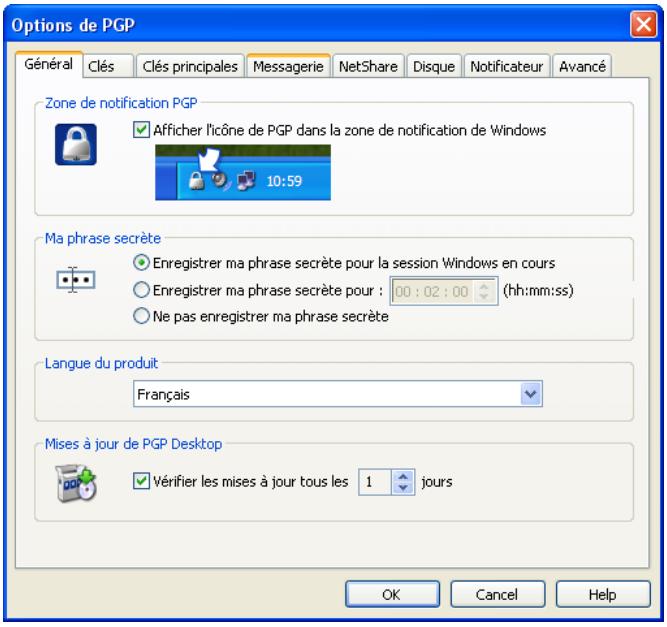
- Cliquez sur l'icône **Zone de notification PGP** dans la zone de notification de Windows, puis sélectionnez **Options**.
- Ouvrez PGP Desktop, puis sélectionnez **Outils > Options de PGP**.

2 Sélectionnez un onglet et effectuez les modifications souhaitées. Passez ensuite à un autre onglet.

3 Pour enregistrer les modifications et fermer la boîte de dialogue, cliquez sur **OK**. Pour annuler les modifications, cliquez sur **Annuler**.

Options de l'onglet Général

L'onglet Général contient divers paramètres de PGP Desktop.



Les options de l'onglet Général de la boîte de dialogue des préférences sont les suivantes :

- **Afficher l'icône de PGP dans la zone de notification de Windows** : lorsque cette case est cochée, l'icône PGP s'affiche dans la zone de notification de Windows et PGP Desktop est actif sur le système. L'icône de la zone de notification PGP permet d'accéder rapidement aux fonctionnalités de PGP Desktop. Désactivez la case pour supprimer l'icône PGP de la zone de notification de Windows. Pour afficher de nouveau l'icône PGP, lancez PGP Desktop, puis sélectionnez **Options de PGP** dans le menu **Outils.** Affichez l'onglet Général et cochez la case.

  Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, activez cette option.

  La suppression de l'icône PGP de la zone de notification de Windows n'interrompt pas l'exécution des services de PGP Desktop.

Pour arrêter les services de PGP, cliquez sur l'icône de la zone de notification PGP. Sélectionnez **Arrêter Services PGP** dans la liste des commandes affichées. Confirmez l'arrêt des services dans la boîte de dialogue d'avertissement qui s'affiche.

Remarque : PGP Corporation conseille de ne pas arrêter les services de PGP Desktop, sauf en cas de nécessité.

- **Ma phrase secrète** : options d'enregistrement de votre phrase secrète.
  - **Enregistrer ma phrase secrète pour la session Windows en cours** : votre phrase secrète est enregistrée jusqu'à la fermeture de votre session. Elle est *mise en cache*. Lorsque vous activez cette option, vous êtes invité à saisir votre phrase secrète une seule fois pour chaque clé privée, mais vous n'avez pas à la fournir de nouveau pour la même clé tant que la session reste ouverte.

Attention : lorsque cette option est activée, il est essentiel que vous fermiez votre session si vous vous absentez. Votre phrase secrète peut rester en cache pendant plusieurs semaines si vous ne fermez jamais votre session, avec le risque qu'une personne lise vos messages chiffrés ou chiffre des messages avec votre clé durant votre absence. Si vous restez généralement connecté pendant de longues périodes, choisissez une autre option de mise en cache de la phrase secrète.

  - **Enregistrer ma phrase secrète pendant X (hh:mm:ss)** : votre phrase secrète est automatiquement enregistrée pendant la période définie. Lorsque vous activez cette option, vous êtes invité à saisir votre phrase secrète une seule fois, lors de la première signature ou du premier déchiffrement. Vous n'avez pas à la taper de nouveau avant la fin de la durée définie. Le réglage par défaut est de 00:02:00 (2 minutes).
  - **Ne pas enregistrer ma phrase secrète** : votre phrase secrète n'est pas enregistrée. Lorsque vous activez cette option, vous devez saisir votre phrase secrète pour chaque opération la nécessitant.

    Même si vous choisissez de ne pas enregistrer votre phrase secrète, vous n'êtes invité à la saisir qu'une fois pour accéder à tous les fichiers d'un dossier ajouté à PGP NetShare.

- **Langue du produit** : cette option permet de sélectionner la langue d'affichage de l'interface utilisateur de PGP Desktop. Options disponibles : Anglais (par défaut), Allemand, Français, Japonais et Espagnol.

Remarque : si vous changez la langue, vous devez fermer la session et en ouvrir une nouvelle.

- **Vérifier les mises à jour tous les X jours** : lorsque cette case est cochée, PGP Desktop recherche les mises à jour logicielles automatiquement, selon l'intervalle spécifié. La valeur par défaut est un jour. Si une version plus récente de PGP Desktop est disponible, un écran de notification s'affiche et vous permet de la télécharger. Lorsque cette case est désactivée, PGP Desktop ne recherche pas automatiquement les mises à jour logicielles.

Cette option nécessite une connexion Internet active.

Une fois la mise à jour téléchargée, suivez les invites pour l'installer.

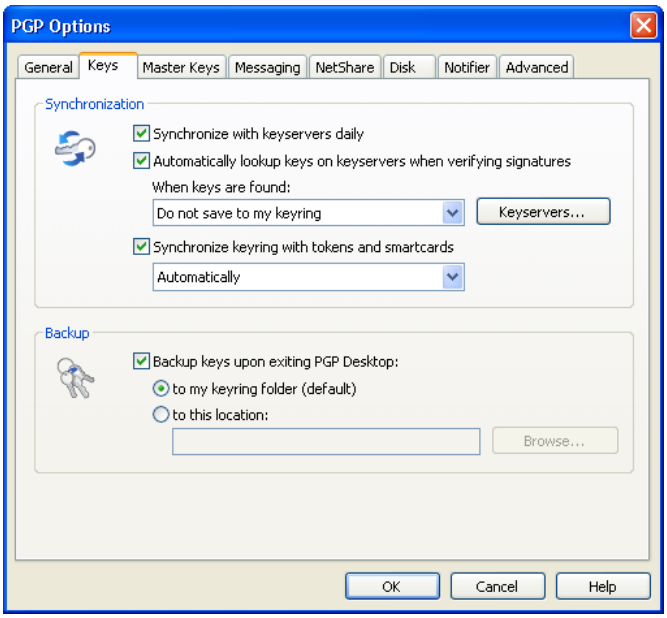
Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, cette option peut être requise. PGP Desktop recherche alors des mises à jour sur le PGP Universal Server associé.

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

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, cette option peut être requise. PGP Desktop recherche alors des mises à jour sur le PGP Universal Server associé.

Options de l'onglet Clés

L'onglet Clés contient des paramètres applicables aux clés PGP Desktop.



Les options disponibles sont les suivantes :

- **Synchronisation** : ces paramètres permettent de définir la synchronisation souhaitée entre les clés de votre trousseau et les serveurs publics.
  - **Synchroniser avec les serveurs de clés tous les jours** : lorsque cette case est cochée, PGP Desktop synchronise quotidiennement les clés publiques de votre trousseau avec la liste des serveurs de clés. Cette liste inclut le serveur PGP Global Directory.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, activez cette option.

Les nouvelles versions des clés sont téléchargées automatiquement, le cas échéant. Lorsqu'une clé est supprimée du serveur de clés, qui le notifie à PGP Desktop, l'application désactive cette clé dans le trousseau de clés local.

Si vous modifiez une paire de clés de votre trousseau à l'aide de PGP Desktop sur votre ordinateur, ce changement n'est pas automatiquement mis à jour sur le serveur de clés. Vous devez télécharger manuellement la clé modifiée sur le serveur de clés souhaité. Un message vous invite à le faire lorsque vous quittez PGP Desktop. Pour envoyer la clé vers le serveur, vous pouvez également cliquer dessus avec le bouton droit, sélectionner **Envoyer vers** dans le menu contextuel, puis choisir le serveur de clés dans la liste.

- **Rechercher automatiquement les clés lors de la vérification des signatures** : lorsque vous activez cette option, PGP Desktop recherche une clé vérifiée sur les serveurs de clés configurés si les clés publiques ne sont pas disponibles dans votre trousseau de clés local.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, cette option est inutile. Votre PGP Universal Server détermine si PGP Desktop doit rechercher les clés et mettre en cache les clés trouvées. Les clés présentes dans un environnement géré par un PGP Universal Server ne sont jamais enregistrées dans votre trousseau de clés.

Si une clé publique est identifiée, trois options sont disponibles :

- **Ne pas enregistrer dans mon trousseau de clés** : les clés trouvées sur les serveurs de clés configurés ne sont utilisées qu'une seule fois ; elles servent à vérifier la signature avec laquelle vous travaillez. Elles ne sont donc pas enregistrées dans votre trousseau de clés.
- **Me demander confirmation avant d'enregistrer dans mon trousseau de clés** : lorsque cette option est activée, vous devez confirmer l'enregistrement des clés trouvées dans votre trousseau de clés.
- **Enregistrer les clés dans mon trousseau de clés** : les clés trouvées sont automatiquement enregistrées dans votre trousseau de clés.

- **Synchroniser le trousseau de clés avec les jetons et les cartes à puce** : cette option vous permet de définir la synchronisation de PGP Desktop avec les cartes à puce et les jetons :

- **Automatiquement** : PGP Desktop charge et utilise automatiquement le pilote PKCS-11 du premier fournisseur de cartes à puce/jetons trouvé sur le système. Si vous avez installé le pilote PKCS-11 d'un seul fournisseur sur votre système, choisissez ce paramètre ; PGP Desktop reconnaîtra et utilisera automatiquement les cartes à puce/jetons de ce fournisseur.
- **Fournisseur disponible** : PGP Desktop charge et emploie le pilote PKCS-11 du fournisseur de cartes à puce/jetons sélectionné dans la liste. Si les pilotes PKCS-11 de plusieurs fournisseurs de cartes à puce/jetons sont installés sur le système, indiquez à PGP Desktop les cartes/jetons à utiliser.
- **Autre** : la boîte de dialogue **Sélectionner le pilote de la carte à puce** s'affiche et vous permet de choisir un pilote PKCS-11. Lorsque vous choisissez cette option, PGP Desktop reconnaît et utilise les cartes à puce/jetons du fournisseur dont vous avez sélectionné le pilote PKCS-11. Vous pouvez ainsi avoir recours aux cartes à puce/jetons d'un fournisseur qui n'apparaît pas dans la liste.

  Si la bibliothèque PKCS-11 d'un fournisseur de cartes à puce est installée sur votre système et fonctionne avec d'autres applications PKCS-11, telles que Mozilla Firefox ou Thunderbird, il est probable que PGP Desktop la reconnaisse et utilise les cartes à puce de ce fournisseur.

  Si une carte à puce non standard ne fonctionne pas avec PGP Desktop (cas assez rare), « Clés de carte à puce » n'apparaît *pas* dans le panneau de contrôle Clés PGP lorsque la carte est installée sur le système.

- **Aucun** : PGP Desktop ne reconnaît ni n'utilise aucune carte à puce ni aucun jeton sur votre système.

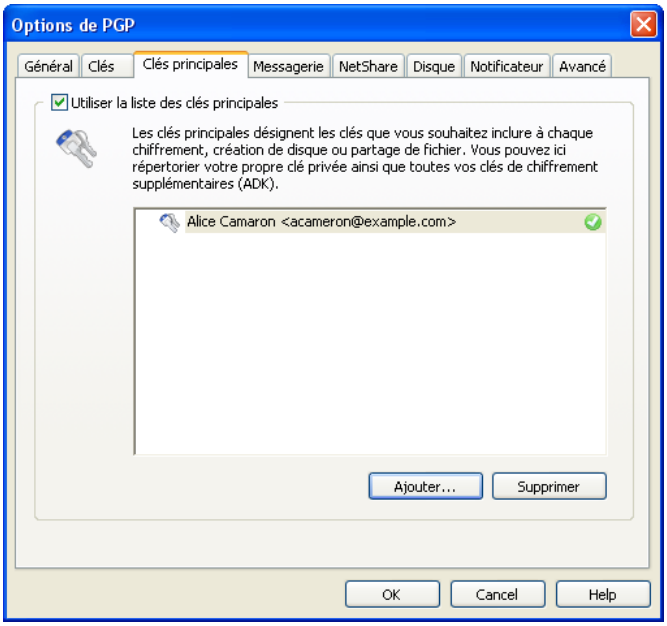
- **Serveurs de clés** : cliquez sur ce bouton pour afficher la boîte de dialogue Liste des serveurs de clés PGP. Cette boîte de dialogue permet d'ajouter, de modifier et de supprimer la liste des serveurs de clés à utiliser lors de la recherche automatique de clés.

- **Sauvegarder** : ces paramètres permettent de définir à quel emplacement et à quel moment les clés doivent être sauvegardées.
  - **Sauvegarder les clés à la fermeture de PGP Desktop :** lorsque cette case est cochée, PGP Desktop sauvegarde automatiquement les clés à l'emplacement indiqué :
    - **vers mon dossier de trousseau de clés (par défaut) :** lorsque cette option est activée, vos clés sont sauvegardées dans le dossier de trousseau de clés par défaut sur votre système. L'emplacement par défaut est le dossier Mes documents.

- **vers cet emplacement :** lorsque cette option est activée, vos clés sont sauvegardées à l'emplacement que vous définissez sur votre ordinateur. Tapez le chemin complet ou cliquez sur **Parcourir** pour accéder à l'emplacement souhaité.

Options de l'onglet Clés principales

La liste des clés principales est un ensemble de clés que vous souhaitez voir ajoutées par défaut chaque fois que vous choisissez des clés pour la messagerie, le chiffrement de disque, PGP NetShare et PGP Zip. Elle vous permet de ne pas avoir à faire glisser dans le champ **Destinataires** les clés que vous utilisez régulièrement.



Pour utiliser la liste des clés principales, cochez la case **Utiliser la liste des clés principales**. Vous ne pouvez pas ajouter de clés à cette liste, ni en supprimer, si vous n'avez pas coché cette case.

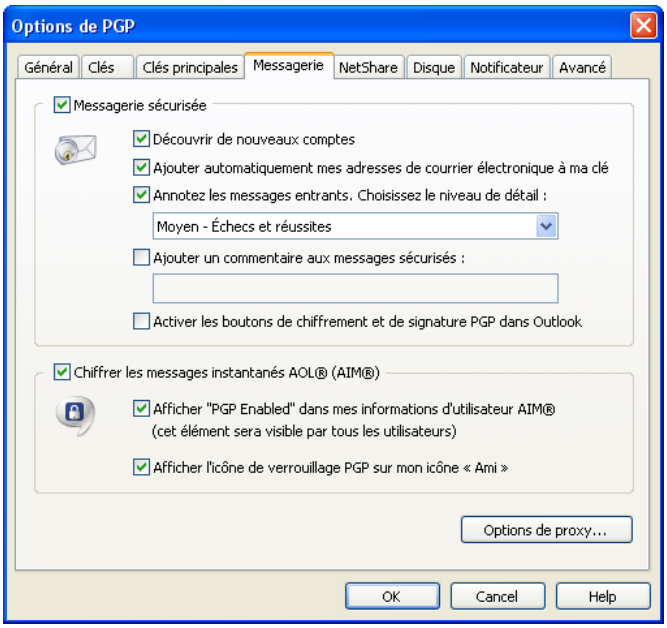
Pour plus d'informations sur l'ajout de clés principales, reportez-vous à la section *Ajout de clés à la liste des clés principales* (à la page 57). Pour plus d'informations sur la suppression de clés principales, reportez-vous à la section *Suppression de clés de la liste des clés principales* (à la page 58).

Remarque : si vous avez généré votre clé à l'aide de l'assistant d'installation, celle-ci est automatiquement ajoutée à la liste des clés principales. Si, en revanche, vous avez importé votre clé dans PGP Desktop, elle n'est pas automatiquement ajoutée à la liste.

Options de messagerie

L'onglet Messagerie contient des paramètres applicables aux messageries électronique et instantanée.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.



Les options de l'onglet Messagerie sont les suivantes :

- **Messagerie sécurisée :** cochez la case **Messagerie sécurisée** pour que PGP Desktop sécurise automatiquement tous vos comptes de messagerie. Lorsque cette option est activée, PGP Desktop intercepte les messages électroniques entrants et sortants et applique les stratégies de sécurité appropriées.

  Désactivez l'option **Messagerie sécurisée** si vous ne souhaitez pas que PGP Desktop sécurise vos comptes de messagerie.

  Lorsque la case **Messagerie sécurisée** est cochée, les options suivantes sont disponibles :

- **Découvrir de nouveaux comptes :** cochez cette case afin que PGP Desktop surveille l'activité de votre messagerie et recherche automatiquement vos nouveaux comptes. Lorsque PGP Desktop détecte un nouveau compte, vous pouvez choisir de sécuriser les messages envoyés via ce compte.

Remarque : dans un environnement géré par PGP Universal, si vous utilisez une liaison de caractère de remplacement (*), cette fonctionnalité sera désactivée, car tous les services de messagerie correspondront à la liaison de *. Par conséquent, tous les nouveaux comptes appliqueront cette stratégie et seront créés même si cette option n'est pas sélectionnée.

- **Ajouter automatiquement mes adresses de courrier électronique à ma clé :** si vous cochez cette case, PGP Desktop ajoute automatiquement à votre clé les adresses de courrier électronique utilisées pour envoyer des messages. Cette option est sélectionnée par défaut. Si PGP Desktop est exécuté dans un environnement géré par un PGP Universal Server, cette option peut être désactivée.

  Désactivez cette option pour que PGP Desktop n'ajoute pas automatiquement les adresses de courrier électronique à votre clé. Cela permet de préserver la confidentialité de vos informations, par exemple, si vous ne souhaitez pas qu'une personne trouve votre adresse électronique.

- **Annotez les messages entrants :** cochez cette case si vous souhaitez que les messages électroniques soient annotés avec des explications détaillant les actions prises par PGP Desktop lors du traitement de vos messages entrants. Trois niveaux d'annotation sont disponibles :

  - **Maximal - Annotation informations détaillées :** des annotations sont ajoutées à vos messages entrants pour détailler chaque action prise par PGP Desktop lors du traitement de ces messages.
  - **Moyen - Échecs et réussites** : option par défaut. Des annotations sont ajoutées pour signaler un échec, tel qu'une clé ou un signataire inconnu. Le paramètre Moyen ajoute des annotations lorsque le message entrant a été déchiffré et/ou signé.
  - **Minimal - Échecs uniquement :** des annotations sont ajoutées uniquement pour signaler un échec.

- **Ajouter un commentaire aux messages sécurisés :** lorsque cette case est cochée, le texte que vous tapez ici est toujours inclus dans les messages chiffrés ou signés. Les commentaires saisis dans ce champ apparaissent sous l'en-tête `--DÉBUT BLOC DE MESSAGE PGP--` et le numéro de version de PGP Desktop de chaque message sécurisé. Ils ne sont pas visibles dans le message déchiffré.

- **Activer les boutons de chiffrement et de signature PGP dans Outlook** : cochez cette case si vous souhaitez utiliser les boutons de chiffrement et de signature de PGP Desktop dans Microsoft Outlook. Cette option est sélectionnée par défaut. Pour plus d'informations sur le boutons de chiffrement et de signature, reportez-vous à la section *Utilisation des boutons Signer et Chiffrer dans Microsoft Outlook* (à la page 98).

Remarque :si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, il se peut que ce champ contiennent déjà du texte.

- **Chiffrer les messages instantanés AOL® (AIM®) :** activez cette option si vous souhaitez que PGP Desktop chiffre les sessions de messagerie instantanée utilisant un logiciel compatible.

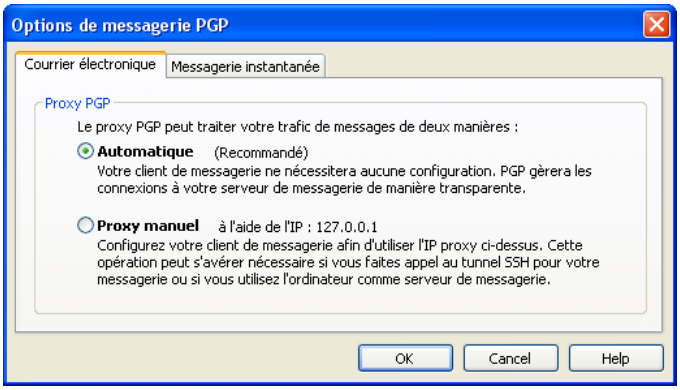
  AOL® Instant Messenger™ et d'autres applications sont compatibles.

  - **Afficher "Compatible PGP" dans mes informations d'utilisateur (AIM®)** : lorsque cette option est cochée, la mention **Compatible PGP** s'affiche en regard du nom de l'écran dans la liste des amis d'AIM et la commande Obtenir des infos. Si elle est désactivée, la mention n'apparaît pas. L'affichage de ce texte varie selon le client de messagerie instantanée.
  - **Afficher l'icône de verrouillage PGP sur mon icône « Ami »** : lorsque cette case est cochée, l'icône de verrouillage PGP s'affiche en regard de l'icône Ami afin d'informer les autres personnes que la session de messagerie instantanée est sécurisée. Lorsqu'elle est désactivée, votre icône apparaît normalement.

Options de proxy

Cliquez sur le bouton **Options de proxy** pour accéder aux options de messagerie avancées.

Onglet Courrier électronique



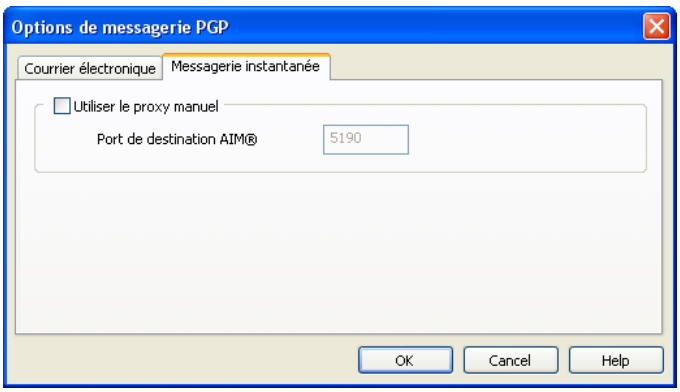
Utilisez les options de cet onglet si vous devez configurer un proxy manuellement sur votre ordinateur afin de pouvoir envoyer et recevoir des messages électroniques.

PGP Desktop « se trouve » entre votre application de messagerie et le serveur de messagerie associé. Grâce à cette configuration, PGP Desktop filtre le trafic des messages électroniques automatiquement ou *envoie des messages par serveur proxy*. PGP Desktop protège vos messages, en fonction de la stratégie applicable, sans interrompre votre travail.

Il n'est généralement pas nécessaire de modifier les paramètres du proxy PGP. Certains utilisateurs doivent toutefois spécifier les paramètres de proxy manuellement. Choisissez l'option recommandée par votre administrateur réseau :

- **Automatique :** option par défaut recommandée. Votre messagerie électronique est protégée automatiquement et de manière transparente. PGP Corporation vous conseille de sélectionner cette option, sauf indication contraire de l'administrateur.
- **Proxy manuel :** vous devez sélectionner cette option lorsque votre ordinateur est relié à votre serveur de messagerie par tunnel SSH ou si vous utilisez l'ordinateur hébergeant PGP Desktop comme serveur de messagerie. Pour plus d'informations, reportez-vous à la section *Configuration du mode manuel* (à la page 324).

Onglet Messagerie instantanée



Si votre ordinateur est protégé par un pare-feu de réseau, vous devrez peut-être modifier le port réseau utilisé pour les sessions AIM. La modification de ce paramètre n'est pas nécessaire pour la plupart des utilisateurs.

- **Utiliser le proxy manuel :** cochez cette case pour modifier le port utilisé pour les sessions de messagerie instantanée AIM. Définissez cette option sur une valeur différente de celle par défaut (5190). Votre administrateur réseau peut vous indiquer si vous devez ou non modifier ce paramètre, et le cas échéant, le numéro de port à utiliser.

Configuration du mode manuel

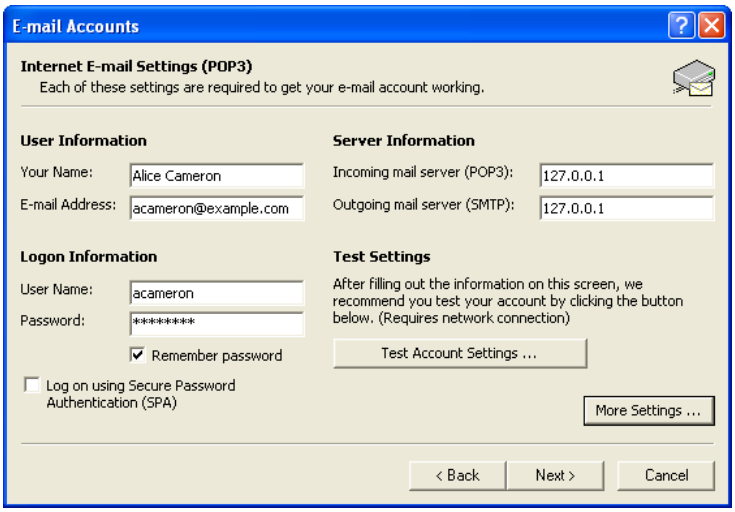
Si vous définissez le proxy de messagerie en mode **Manuel**, vous devez également configurer les paramètres de messagerie PGP, ainsi que certaines options de votre client de messagerie (demandez à votre administrateur système les valeurs à utiliser) :

1. Dans le panneau de contrôle Messagerie PGP, sélectionnez le service à employer en mode Manuel. Le panneau Nouveau service s'affiche.
2. Cliquez sur **Paramètres du serveur**. La boîte de dialogue correspondante s'affiche.
3. Sélectionnez le type de serveur qui sera utilisé par le nouveau service :
   - **Messagerie sur Internet**, pour les utilisateurs de PGP Desktop autonomes disposant d'une connexion de messagerie POP ou IMAP.
   - **PGP Universal**, pour les utilisateurs de PGP Desktop dont l'ordinateur se trouve dans un environnement géré par un PGP Universal Server. Pour plus d'informations sur les paramètres à utiliser, contactez votre administrateur PGP Universal Server.
   - **MAPI/Exchange**, pour les utilisateurs de PGP Desktop qui emploient Microsoft Outlook comme client de messagerie sur un serveur Microsoft Exchange/MAPI. Pour plus d'informations sur les paramètres à utiliser, contactez votre administrateur de messagerie.
   - **Lotus Notes**, pour les utilisateurs de PGP Desktop qui emploient Lotus Notes comme client de messagerie avec un serveur Lotus Domino. Pour plus d'informations sur les paramètres à utiliser, contactez votre administrateur de messagerie.
4. Dans la section **Serveur de messagerie entrant**, saisissez une valeur dans le champ **Rediriger le port local X vers ce serveur**.

   PGP Desktop surveille ce port pour les messages électroniques partant de votre serveur de messagerie vers votre client de messagerie.
5. Dans la section **Serveur de messagerie sortant (SMTP)**, saisissez une valeur dans le champ **Rediriger le port local X vers ce serveur**.

   PGP Desktop surveille ce port pour les messages électroniques partant de votre client de messagerie vers votre serveur de messagerie.
6. Cliquez sur **OK**. La boîte de dialogue Paramètres du serveur se ferme.

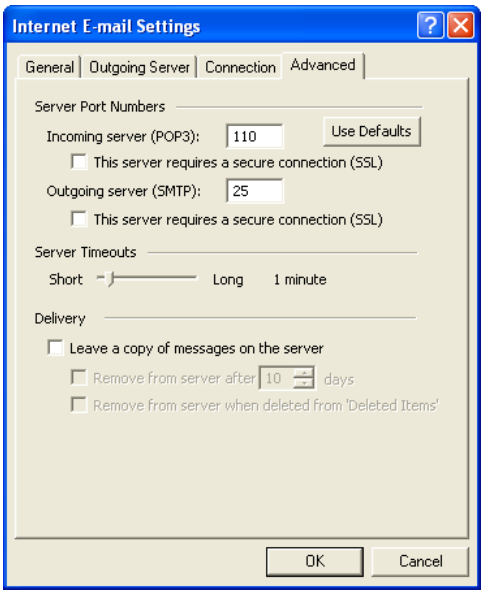
7 Ouvrez votre client de messagerie et accédez aux paramètres de votre compte de messagerie (si vous avez plusieurs comptes, vous devez tous les configurer séparément).



8 Pour les paramètres **Serveur de courrier entrant (POP3 ou IMAP)** et **Serveur de courrier sortant (SMTP)** de Microsoft Outlook, saisissez **127.0.0.1**.

9 Cliquez sur **Paramètres supplémentaires**.

10 Dans la boîte de dialogue Paramètres de messagerie Internet, cliquez sur **Options avancées**. L'onglet **Options avancées** devient actif dans la boîte de dialogue.



11 Dans le champ **Serveur entrant** (POP3 ou IMAP), saisissez la valeur définie précédemment pour le serveur de messagerie *entrant* dans le champ Rediriger le port local X vers ce serveur, à l'étape 7 de cette procédure.

12 Dans le champ **Serveur sortant (SMTP)**, saisissez la valeur définie précédemment pour le serveur de messagerie *sortant* dans le champ Rediriger le port local X vers ce serveur, à l'étape 8 de cette procédure.

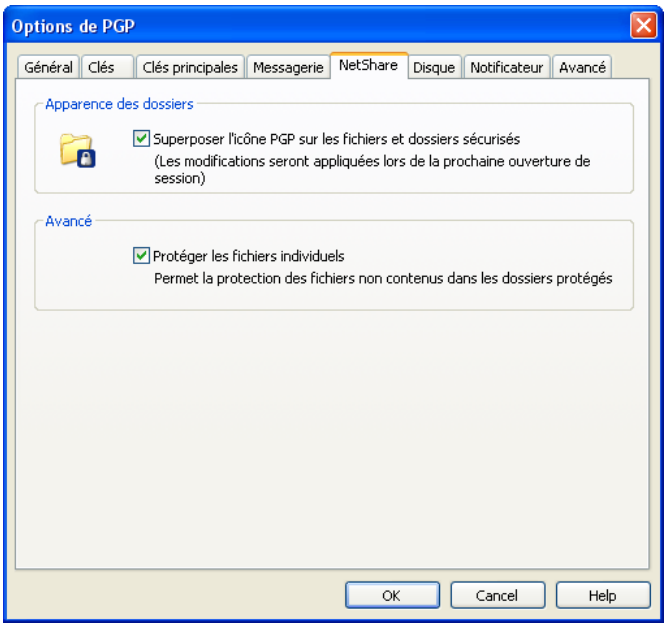
13 Cliquez sur **OK**, puis terminez la configuration des paramètres du compte. Le mode manuel est configuré pour le service sélectionné.

14 Une fois que la configuration du mode Manuel est terminée pour tous les services, redémarrez votre ordinateur.

Options de PGP NetShare

L'onglet des options de PGP NetShare permet de modifier les paramètres de protection des fichiers réseau partagés.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.



- **Apparence des dossiers :** cochez la case **Superposer l'icône PGP sur les fichiers et dossiers sécurisés** si vous souhaitez afficher une petite icône de verrouillage PGP sur les fichiers protégés à l'aide de PGP NetShare.

- **Avancé :** cochez la case **Protéger les fichiers individuels** pour protéger les fichiers individuels stockés hors du dossier protégé à l'aide PGP NetShare.

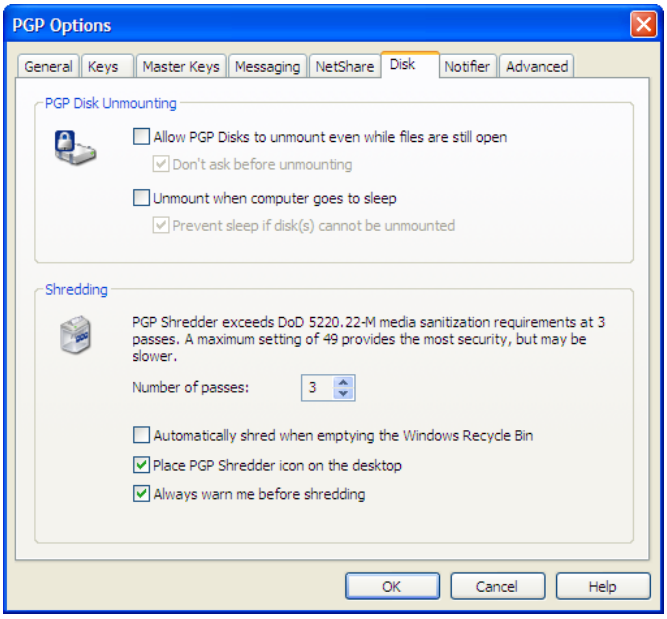
  Remarque : il se peut que votre administrateur PGP ne vous autorise pas à sélectionner cette option si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server.

Pour plus d'informations sur la protection des fichiers individuels hors d'un dossier protégé à l'aide de PGP NetShare, reportez-vous à la section *Protection des fichiers hors d'un dossier protégé* (à la page 266).

Options de l'onglet Disque

L'onglet Disque contient des paramètres applicables aux volumes protégés à l'aide de la fonctionnalité PGP Virtual Disk. Il présente également les options de PGP Shredder.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu et les autres options de cette fonctionnalité ne sont pas disponibles. Les graphiques inclus dans ce guide illustrent l'installation par défaut du produit avec toutes les fonctionnalités activées. Si l'administrateur de PGP Universal Server a désactivé cette fonctionnalité, cette section ne vous concerne pas.



Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, ces options peuvent être déjà configurées.

Démontage du PGP Disk

Les options de PGP Virtual Disk sont les suivantes :

- **Autoriser le démontage des PGP Disks même si certains fichiers sont encore ouverts :** généralement, vous ne pouvez pas démonter automatiquement un volume PGP Virtual Disk lorsque l'un des fichiers du volume est ouvert. Cette option vous permet de le démonter même si des fichiers sont ouverts (démontage forcé).
  - L'option **Ne pas demander confirmation avant le démontage** permet à PGP Desktop d'effectuer un démontage forcé du volume PGP Virtual Disk *sans* vous informer qu'un des fichiers est ouvert, le cas échéant.

Avertissement : vous risquez de perdre des données en cas de démontage forcé d'un volume PGP Virtual Disk lorsque des fichiers sont ouverts.

- **Démonter lorsque l'ordinateur se met en veille :** si cette case est cochée, PGP Desktop démonte automatiquement les volumes PGP Virtual Disk lorsque votre ordinateur se met en veille ou en veille prolongée.
  - Sélectionnez **Échec du mode veille si le démontage du disque ou des disques est impossible** pour éviter que votre ordinateur se mette en veille lorsqu'un PGP Virtual Disk ne peut pas être démonté. Cette option est indisponible sur les systèmes Microsoft Windows Vista (Windows Vista n'autorise plus les applications à empêcher la mise en veille).

Avertissement : le mode de veille prolongée de Windows est peu sûr par nature, car Windows inscrit les données sensibles sur le disque si votre PGP Virtual Disk est ouvert lorsque la mise en veille prolongée est appelée. PGP Corporation vous recommande donc d'utiliser la fonctionnalité PGP Whole Disk Encryption si vous utilisez la mise en veille prolongée. Autrement, veillez à activer les options **Démonter lorsque l'ordinateur se met en veille** et **Échec du mode veille si le démontage du disque ou des disques est impossible**.

Décomposition

La fonctionnalité PGP Shredder constitue un moyen sûr de supprimer des fichiers sensibles. Vous pouvez ajuster le niveau de sécurité de cette fonctionnalité, ainsi que d'autres paramètres.

Les options de la fonctionnalité PGP Shredder sont les suivantes :

- **Nombre de passes :** la fonctionnalité PGP Shredder supprime vos fichiers en toute sécurité en les supprimant d'abord normalement, puis en utilisant de nombreux caractères « 0 » pour remplacer l'espace disque qui était occupé par les fichiers supprimés.

Grâce à cette méthode, vos fichiers peuvent être supprimés de façon sûre avec seulement quelques « passes » de remplacement. Ainsi, **3** constitue le paramètre par défaut. Il offre un niveau extrêmement élevé de sécurité, mais vous pouvez le modifier afin de refléter le niveau de sécurité de votre choix (jusqu'à un maximum de 49 passes).

Sachez que le coût de cette plus grande sécurité est l'augmentation du temps nécessaire pour décomposer vos fichiers, qui dépend de plusieurs facteurs, en particulier la rapidité du processeur de votre ordinateur.

Le nombre de passes recommandé est :

- 3 passes pour un usage personnel ;
- 10 passes pour un usage commercial ;
- 18 passes pour un usage militaire ;
- 26 passes pour une sécurité maximale.

- **Décomposer lorsque la corbeille Windows est vidée** : cochez cette case afin que la fonctionnalité PGP Shredder décompose le contenu de la corbeille Windows chaque fois que celle-ci est vidée. Soyez prudent lorsque vous utilisez cette option, car la fonctionnalité PGP Shredder décompose alors tous les fichiers de la corbeille, qu'ils soient sensibles ou non, ce qui peut demander beaucoup de temps quand de très grands fichiers sont concernés.

  Cette option décompose également automatiquement les fichiers que vous supprimez sans passer par la corbeille (lorsque vous appuyez sur la touche Maj lors de la suppression), ainsi que les fichiers temporaires du système et des applications automatiquement supprimés par le système d'exploitation.

  Cette décomposition automatique utilise les paramètres de la fonctionnalité PGP Shredder que vous avez choisis, de la même manière que lorsque vous décomposez les fichiers manuellement.

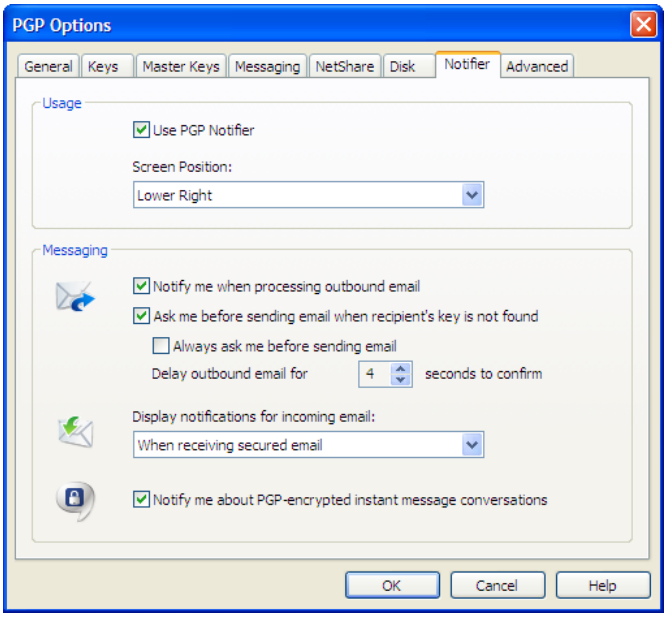
- **Placer l'icône de PGP Shredder sur le bureau** : cochez cette case si vous voulez placer l'icône de la fonctionnalité PGP Shredder sur le bureau de votre ordinateur, pour une utilisation plus facile. Utilisez cette icône de la même façon que l'icône de la corbeille Windows : faites-y glisser les fichiers. Cette option est sélectionnée par défaut.

- **Toujours m'avertir avant une décomposition** : cochez cette case si vous voulez qu'une boîte de dialogue de confirmation s'affiche avant chaque décomposition. Cela vous permet de vous assurer que seuls les fichiers appropriés sont décomposés. Cette option est sélectionnée par défaut.

Conseil : pensez aux autres occurrences des données susceptibles d'être conservées ailleurs sur votre disque, par exemple dans des fichiers temporaires. Veillez donc à utiliser PGP Whole Disk Encryption pour protéger toutes les données de votre système.

Options du Notificateur

L'onglet **Notificateur** contient les paramètres applicables au Notificateur PGP Desktop, qui affiche des messages d'état dans un angle de l'écran, lorsque vous envoyez ou recevez des messages électroniques, ainsi que lors de l'utilisation des fonctionnalités PGP Whole Disk Encryption et PGP NetShare.



Pour plus d'informations sur le Notificateur PGP Desktop, reportez-vous à la section *Alertes du Notificateur PGP Desktop* (à la page 35).

Options d'utilisation

- Pour activer les notifications, sélectionnez **Utiliser le Notificateur PGP**, puis spécifiez la position à l'écran.
- **Position à l'écran :** les notifications de PGP Desktop peuvent apparaître dans l'un des quatre angles de l'écran **(En bas à droite**, **En bas à gauche**, **En haut à droite** ou **En haut à gauche**). Choisissez celui dans lequel vous souhaitez les voir apparaître. La position par défaut est **En bas à droite**.

Options de messagerie

Les paramètres du Notificateur PGP Desktop sont les suivants :

- **M'avertir du traitement des messages sortants :** cochez cette case si vous souhaitez que PGP Desktop vous informe, par le biais de notifications, de l'état du chiffrement ou de la signature lors de l'envoi de courrier électronique. Désactivez-la pour arrêter l'affichage de ces notifications.

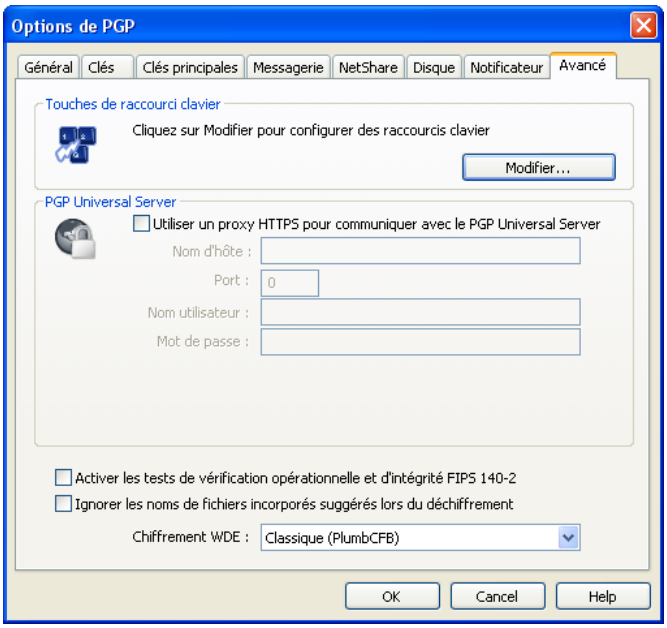
- **Me demander confirmation avant l'envoi d'un courrier électronique lorsque la clé du destinataire est introuvable :** PGP Desktop recherche une clé publique pour chaque destinataire des messages envoyés. Par défaut, s'il ne trouve pas de clé publique, il envoie le message en clair (sans chiffrement). Si vous cochez cette case, vous êtes informé de cette situation et avez la possibilité de bloquer l'envoi du message.

  (Pour plus d'informations sur les paramètres de stratégie par défaut de PGP Desktop, reportez-vous à la section *Services et stratégies* (à la page 100).)

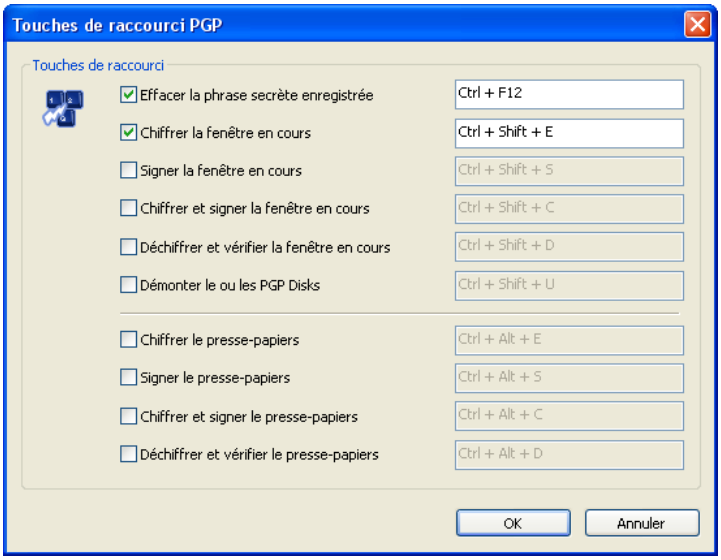
  - **Toujours me demander confirmation avant l'envoi d'un courrier électronique :** cochez cette case si vous souhaitez confirmer l'envoi de chaque message électronique. Vous pouvez consulter l'état du chiffrement dans le Notificateur et choisir d'envoyer ou de bloquer le message.
  - **Différer les messages sortants pendant n seconde(s) pour confirmer** (où *n* est un nombre entre 1 et 30 ; la valeur par défaut est de 4 secondes) : pour modifier le temps d'attente avant l'envoi des messages sortants et l'affichage des notifications PGP Desktop, cliquez sur les flèches haut et bas. Cette période vous permet de consulter le message du Notificateur PGP Desktop.
- **Afficher des notifications pour les messages entrants :** vous pouvez choisir le niveau de notification de l'état d'un message entrant. Les options disponibles sont les suivantes :
  - **À la réception de messages sécurisés** : une notification s'affiche à la réception d'un message sécurisé. Elle indique l'expéditeur et l'objet du message, l'état de chiffrement et de vérification, ainsi que l'adresse de courrier électronique de l'expéditeur.
  - **Uniquement en cas d'échec de vérification du message** : un message de notification s'affiche uniquement lorsque PGP Desktop ne parvient pas à vérifier la signature du message entrant.
  - **Jamais** : si vous ne souhaitez pas voir de message de notification lors de la réception de courriers électroniques, sélectionnez cette option. Cela n'a aucune incidence sur les messages de notification relatifs aux messages sortants.
- **M'avertir des conversations par messagerie instantanée chiffrées par PGP** : lorsque vous cochez cette case, une notification PGP Desktop apparaît brièvement au début et à la fin d'une conversation sécurisée de messagerie instantanée.

Options avancées

L'onglet des options avancées de PGP contiennent des paramètres très spécifiques. La modification de ces paramètres n'est pas nécessaire pour la plupart des utilisateurs.



- **Touches de raccourci clavier** : PGP Desktop propose de nombreuses méthodes de création de raccourcis clavier afin de vous aider à accélérer et faciliter votre travail. Un ensemble de raccourcis clavier sont préconfigurés dans PGP Desktop, mais vous pouvez les modifier en fonction de vos besoins. Cliquez sur **Modifier** pour afficher la boîte de dialogue Touches de raccourci PGP.



- **PGP Universal Server. Utiliser un proxy HTTPS pour communiquer avec PGP Universal :** ne modifiez pas ces paramètres sauf si votre administrateur réseau vous le demande.

  Si l'installation de PGP Universal Server requiert une connexion client/serveur sécurisée via un proxy, définissez-la à l'aide de ces options. Pour définir une configuration appropriée, votre administrateur peut vous fournir le nom du serveur, le port de communication, votre ID d'utilisateur et votre mot de passe.

- Pour modifier votre clé (ou mode clé), cliquez sur **Réinitialiser la clé**. Pour plus d'informations sur les modes clés, reportez-vous à la section *Modes clés* (cf. "Modes clé" à la page 133). Cette option est uniquement disponible dans un environnement géré par un PGP Universal Server.

- **Activer les tests de vérification opérationnelle et d'intégrité FIPS 140-2 :** cochez cette case pour effectuer des vérifications FIPS 140-2. Cette opération diminue les performances du système. Redémarrez votre ordinateur pour appliquer ce paramètre.

- **Ignorer les noms de fichiers incorporés suggérés lors du chiffrement** : sélectionnez cette option pour ignorer les suggestions de PGP Desktop lors du chiffrement des fichiers.

si vous utilisez PGP Desktop version 8.1 à l'étranger (au Japon, par exemple), le codage du nom de fichier suggéré sera incorrect. Vous devez vérifier l'interaction entre PGP Desktop 8.1 et 9.x lors du déchiffrement avec PGP Desktop 9.x des fichiers chiffrés dans PGP Desktop 8.1.

B Utilisation des mots de passe et phrases secrètes

Les mots de passe et les phrases secrètes protègent vos données. Les phrases secrètes sont généralement plus longues et utilisent des caractères plus variés que les mots de passe.

Par exemple, un mot de passe simple peut être composé de deux mots de quatre lettres concaténés : « plusinfo » sans les guillemets. Pour un mot de passe plus fort, vous pouvez utiliser des majuscules (PlusInfo) ou encore ajouter des chiffres (Plus9Info4).

Les phrases secrètes, en revanche, sont plus longues et utilisent d'autres caractères. Voici un exemple de phrase secrète simple : « Mf&Ms>eq0. » sans les guillemets, mais avec le point. Cette phrase secrète peut sembler difficile à mémoriser, mais elle repose en réalité sur une expression beaucoup plus facile à retenir.

Il peut s'agir d'un énoncé simple comportant une ponctuation et des majuscules, issu d'un livre connu par exemple : "Car ce n'est pas du golf, ai-je répondu" avec les guillemets. Bien que cela ne semble pas une phrase secrète forte, elle l'est en fait deux fois plus que les autres exemples.

Cette section explique les différences entre les mots de passe et les phrases secrètes, décrit l'indicateur de qualité de la phrase secrète dans PGP Desktop et donne des conseils sur la création de phrases secrètes fortes.

Contenu du chapitre

Mot de passe ou phrase secrète ?

Comment savoir si vous devez utiliser un mot de passe ou une phrase secrète ? En fait, tout dépend de ce que vous voulez protéger. Plus les informations à protéger sont importantes, plus la protection doit être élevée.

La plupart des documents Word ne sont pas du tout protégés ; leur contenu n'est, en effet, pas suffisamment important pour justifier un tel effort de protection. Pour les comptes bancaires en ligne, certains établissements obligent à saisir un code PIN de 4 lettres en fonction de la somme d'argent présente sur le compte. Bel effort, mais reconnaissez tout de même que cette sécurité est bien faible ! Vous pouvez utiliser un compte de messagerie Hotmail gratuit pour vos correspondances de faible importance. Un simple mot de passe convient parfaitement comme dispositif de sécurité. Votre compte de messagerie professionnelle vous permet quant à lui d'envoyer et de recevoir des informations propriétaires relatives à des produits, à des clients et à des opérations financières.

Dans PGP Desktop, par exemple, vous pouvez créer des phrases secrètes pour votre paire de clés PGP et pour vos volumes PGP Virtual Disk. Si vous associez une phrase secrète faible à votre paire de clés PGP et qu'un pirate réussit à prendre le contrôle physique de votre fichier de clé privée, il lui suffit de déchiffrer cette phrase pour pouvoir lire vos messages et envoyer des messages en votre nom.

Indicateur de qualité de la phrase secrète

Lorsque vous créez des phrases secrètes dans PGP Desktop, l'indicateur de qualité de la phrase secrète donne des informations de base sur le niveau de sécurité de la phrase secrète. Il fournit néanmoins une indication bien plus précise que le simple nombre de caractères.

En général, le niveau de remplissage de la barre indique le niveau de sécurité de la phrase secrète. Mais à quoi correspond le niveau de remplissage de l'indicateur de qualité de la phrase secrète ?

L'indicateur de qualité de la phrase secrète compare l'entropie (caractère aléatoire) de la phrase secrète saisie par rapport à une chaîne aléatoire de 128 bits réelle (entropie identique à une clé AES128), soit 128 bits d'entropie.

(L'entropie mesure la difficulté à déterminer un mot de passe ou une clé.)

Ainsi, lorsque la phrase secrète remplit la moitié de l'indicateur de qualité, cela signifie que la phrase secrète a 64 bits d'entropie. Un indicateur de qualité entièrement rempli correspond à une phrase secrète d'environ 128 bits d'entropie.

Que représente un niveau de sécurité de 128 bits d'entropie ? À la fin des années 1990, des ordinateurs spécialement mis au point pour craquer un chiffrement DES, étaient capables de déchiffrer une clé DES en quelques heures en essayant toutes les valeurs possibles.

En supposant qu'il est possible de créer un ordinateur capable de déchiffrer une clé DES en une seconde (soit d'essayer 255 clés par seconde), il faudrait alors près de 149 mille milliards d'années pour craquer une clé AES de 128 bits. À titre de comparaison, l'univers aurait moins de 20 milliards d'années.

Comment l'entropie d'un caractère est-elle mesurée ? L'entropie d'un caractère choisi est fonction du pool de caractères disponibles au moment du choix d'un caractère particulier.

Par exemple, si vous devez choisir un code confidentiel numérique, vous êtes limité aux chiffres de zéro à neuf, ce qui fait un total de 10 caractères. Ce pool étant plutôt restreint, l'entropie pour un caractère choisi est assez faible.

Lorsque vous choisissez une phrase secrète à l'aide de la version de PGP Desktop en anglais, l'entropie est plus importante. En effet, vous disposez de trois pools : les lettres en minuscule et en majuscule (52 caractères), les chiffres de zéro à neuf (10 caractères) et les signes de ponctuation d'un clavier standard (32 caractères).

Lorsque vous tapez un caractère, PGP Desktop détermine la valeur de l'entropie de ce caractère en fonction du pool dans lequel il se trouve et applique cette valeur à l'indicateur de qualité de la phrase secrète.

Ce concept est valable pour les jeux de caractères des autres langues : plus le pool est important, plus l'entropie du caractère est élevée. Si vous utilisez un jeu de caractères asiatique ou arabe, par exemple, qui peut contenir des centaines de caractères, le niveau d'entropie d'un caractère est plus important et remplit l'indicateur de qualité d'autant plus rapidement.

Création de phrases secrètes fortes

La création d'une bonne phrase secrète repose sur un compromis entre facilité d'utilisation et niveau de sécurité. Les phrases secrètes longues, comportant à la fois des lettres en minuscule et en majuscule, des chiffres et des signes de ponctuation, sont plus fortes mais également plus difficiles à mémoriser.

Des études ont démontré que les phrases secrètes plus difficiles à retenir sont aussi plus fréquemment écrites, ce qui va l'encontre du but d'avoir une phrase secrète forte. Il est recommandé d'utiliser une phrase secrète forte plus courte que vous pouvez mémoriser, plutôt qu'une phrase secrète forte plus longue que vous noterez ou risquez d'oublier.

Généralement, pour créer une phrase secrète forte, il suffit de prendre une phrase et de la réduire à des caractères uniques. Par exemple, la phrase :

```
Mon frère et moi sommes plus forts ensemble que seuls.
```

devient la phrase secrète :

```
Mf&Ms>eq0.
```

Cette phrase secrète contient 10 caractères avec des lettres en minuscule et en majuscule, des chiffres et des signes de ponctuation. Elle est donc assez courte. Si vous pensez que 10 caractères ne sont pas suffisants, créez-en une autre à l'aide de la même méthode, puis combinez-les ou utilisez une phrase différente plus longue.

Vous pouvez également prendre des phrases simples contenant des signes de ponctuation et des lettres en majuscule. Par exemple :

```
Modifié par Jean Dupont (pas Jean Dupont, éditeur)
```

Bine qu'elle ne soit ni longue, ni compliquée, cette phrase secrète est forte. Si vous souhaitez tirer une phrase secrète d'un livre, veillez à ne pas le perdre.

Dans PGP Desktop, une phrase secrète peut comporter jusqu'à 255 caractères, espaces compris.

Vous pouvez également choisir de concaténer plusieurs mots courants et courts. Une méthode appelée Diceware™ utilise des dés pour sélectionner des mots au hasard dans une liste contenant 7776 mots courts anglais, abréviations et chaînes de caractères faciles à mémoriser. Lorsque vous en combinez suffisamment, vous pouvez créer une phrase secrète forte. Selon les réponses aux questions fréquentes de Diceware, une phrase secrète de 10 mots Diceware atteint 128 bits d'entropie.

Pour plus d'informations sur Diceware, reportez-vous à la *page d'accueil du site Diceware* (http://world.std.com/~reinhold/diceware.html).

Voici quelques recommandations quant à la création de phrases secrètes :

- Utilisez une phrase que vous pouvez mémoriser à long terme. Vous aurez ainsi moins de risque de l'oublier.
- Composez une phrase secrète d'au moins huit caractères. La longueur ne constitue pas un indicateur fiable, mais une phrase secrète est plus forte moins elle est courte.
- Utilisez des lettres en minuscule et en majuscule, des chiffres et des signes de ponctuation.

  Attention : n'utilisez que des caractères ASCII, si possible, notamment si vous disposez d'un clavier international, car certains caractères spéciaux ne sont pas pris en charge dans les phrases secrètes (§ par exemple).

- Modifiez régulièrement votre phrase secrète : changez-le en moyenne tous les trois mois. Si vous conservez longtemps la même phrase secrète, il devient plus facile pour une personne de la trouver.

Quelques conseils ce qu'il ne faut **pas** faire lorsque vous créez des phrases secrètes :

- N'écrivez pas votre phrase secrète.
- Ne divulguez pas votre phrase secrète.
- Veillez à ce que personne ne vous voit saisir votre phrase secrète.
- N'utilisez pas « mot de passe » ou « phrase secrète ».
- N'utilisez pas de séquences logiques, telles que abcdefgh ou 12345678 ou azertyui ou 88888888 ou AAAAAAAA.
- N'utilisez pas de mots courants. La plupart des pirates ont recours à un dictionnaire de piratage de mot de passe qui essaie des mots couramment employés. Ne combinez pas deux mots courants, n'utilisez pas le pluriel d'un mot courant, ni un mot courant avec la première lettre en majuscule.

- N'utilisez pas de chiffres vous concernant personnellement. Si une personne connaît ces nombres, un pirate peut les trouver : date d'anniversaire, numéro de téléphone ou de sécurité sociale, adresse, etc.
- N'utilisez pas de noms ou prénoms : ceux de personnes réelles ou de personnages de fiction, le nom de votre animal, votre dernière destination de vacances, votre nom d'utilisateur, le nom de votre société, votre équipe préférée, une partie du corps, un nom tiré d'un livre, notamment de la Bible.
- N'utilisez aucun des mots cités ci-dessus inversé ou précédé ou suivi d'un seul chiffre.

Que faire si vous avez oublié votre phrase secrète ?

Si vous avez oublié votre phrase secrète, vous ne pouvez plus déchiffrer les informations chiffrées à l'aide de celle-ci. Toutefois, vous pouvez reconstruire votre clé si votre administrateur PGP a implémenté une stratégie de restauration de clé pour votre entreprise. Pour plus d'informations, consultez la section *Reconstruction de clé PGP* (cf. "Reconstruction de clés avec PGP Universal Server" à la page 86, "Perte de votre clé ou phrase secrète" à la page 86) et contactez votre administrateur PGP.

C Utilisation de PGP Desktop avec un PGP Universal Server

PGP Universal Server est destiné aux entreprises souhaitant protéger les messages électroniques de façon automatique et transparente pour les utilisateurs finals à l'aide de stratégies configurables définies par l'administrateur PGP afin de renforcer les stratégies de sécurité de l'entreprise. PGP Universal permet également aux administrateurs PGP de gérer le déploiement de PGP Desktop dans l'entreprise. Pour plus d'informations sur PGP Universal Server, reportez-vous à la page dédiée à *PGP Universal Server sur le site Web PGP* (http://www.pgp.com/products/universal/index.html).

Dans un environnement géré par un PGP Universal Server, vous bénéficiez de la technologie de chiffrement PGP éprouvée, ainsi que des fonctionnalités de sécurité de PGP Desktop jusque dans votre ordinateur de bureau : PGP Whole Disk Encryption, volumes PGP Virtual Disk, archives PGP Zip, PGP Shred, etc.

Pour utiliser PGP Desktop dans un environnement géré par un PGP Universal Server, vous devez installer PGP Desktop à l'aide d'un programme d'installation fourni par votre administrateur PGP.

Si vous n'utilisez pas la version professionnelle de PGP Desktop au sein d'une entreprise, mais une version autonome pour votre ordinateur personnel, cette section ne vous concerne pas.

Attention : dans le cas d'une utilisation professionnelle de PGP Desktop pour lequel le programme d'installation dont vous disposez ne vous a pas été fourni par votre administrateur, consultez ce dernier **avant** d'installer ou d'utiliser cette version de PGP Desktop.

Cette section décrit les différences d'utilisation de PGP Desktop dans un domaine de messagerie géré par un PGP Universal Server.

Contenu du chapitre

Présentation

Votre administrateur PGP doit configurer le programme d'installation de PGP Desktop via l'une des méthodes suivantes :

- **Aucun paramètre de stratégie** : aucun paramètre n'est intégré à votre copie de PGP Desktop ; vous pouvez utiliser toutes les fonctionnalités permises par votre licence.
- **Détection automatique des paramètres de stratégie** : PGP Desktop contacte le PGP Universal Server qui a créé le programme d'installation et télécharge les paramètres correspondant. Selon les paramètres reçus, il se peut que vous deviez utiliser les fonctionnalités de PGP Desktop de manière spécifique.
- **Paramètres de stratégie prédéfinis** : Les paramètres sont intégrés à votre copie de PGP Desktop. Il se peut que vous deviez utiliser les fonctionnalités de PGP Desktop de manière spécifique.

Lorsqu'un PGP Universal Server transmet les paramètres à PGP Desktop, certaines fonctionnalités doivent être utilisées d'une certaine manière, notamment :

- Actions requises lors de l'installation de PGP Desktop : chiffrement de l'ensemble du disque de démarrage ou création d'un volume PGP Virtual Disk, par exemple.
- Possibilité ou obligation d'utiliser les fonctionnalités de PGP Desktop d'une certaine manière : chiffrement impératif de la messagerie instantanée AIM ou possibilité de décomposer automatiquement des fichiers lorsqu'ils sont supprimés, par exemple.
- Impossibilité d'utiliser certaines fonctionnalités de PGP Desktop : chiffrement conventionnel et création d'archives à auto-déchiffrement (SDA), par exemple.
- Stratégies de messagerie particulières imposées : chiffrement et signature de messages vers certains domaines de messagerie, par exemple.
- Désactivation de certaines fonctionnalités, telles que la Messagerie PGP ou PGP NetShare (sous Windows), ou écran PGP Whole Disk Encryption BootGuard personnalisé (sous Windows). Pour plus d'informations, reportez-vous à *Fonctionnalités personnalisées par votre administrateur PGP Universal Server* (cf. "Fonctionnalités personnalisées par l'administrateur de PGP Universal Server" à la page 5).

Ce Guide de l'utilisateur décrit les fonctionnalités de PGP Desktop administrées par l'administrateur PGP dans un environnement géré par un PGP Universal Server.

Contactez votre administrateur PGP pour en savoir plus sur les différences d'utilisation de PGP Desktop dans un environnement géré par un PGP Universal Server.

À l'attention des administrateurs PGP

Si vous êtes l'administrateur PGP en charge du fonctionnement de PGP Desktop pour certains ou tous les utilisateurs de votre société, PGP Corporation vous recommande de permettre aux utilisateurs de gérer leurs propres clés à l'aide du Mode clé client.

Lorsque vous préparez la création des programmes d'installation de PGP Desktop sur votre PGP Universal Server, vous pouvez contrôler si les utilisateurs de PGP Desktop sont capables de gérer leurs propres clés, en Mode clé client, ou si le PGP Universal Server gère leurs clés, en Mode clé de serveur.

Ces paramètres sont définis dans la section de gestion des clés dans l'écran Configuration de la clé : Par défaut, dans le cadre de la configuration de la stratégie de groupe d'utilisateurs par défaut pour les utilisateurs internes (**Groupe d'utilisateurs > Options de stratégie > Configuration de la clé : Par défaut** dans l'interface d'administration du PGP Universal Server).

Pour les utilisateurs de PGP Desktop, le Mode clé client constitue la meilleure méthode :

- pour de nombreuses fonctionnalités de PGP Desktop, l'utilisateur doit pouvoir contrôler sa clé privée. Si le PGP Universal Server gère cette clé privée, l'utilisateur ne peut pas accéder à ces fonctionnalités.
- Si vous spécifiez le Mode clé de serveur, certaines options prédéfinies pour les utilisateurs de PGP Desktop seront indisponibles, telles que la création automatique de PGP Virtual Disks.

Liaison manuelle à un PGP Universal Server

Si vous effectuez une liaison manuelle à un PGP Universal Server à l'aide de PGP Desktop (lorsqu'un service de messagerie est affiché, cliquez sur **Paramètres du serveur**) et que vous vous inscrivez, vous ne téléchargez que la stratégie relative aux messages électroniques, mais pas celle relative aux consommateurs. Il est possible que l'administrateur du PGP Universal Server ait défini d'autres options dans la stratégie relative aux consommateurs, par exemple les modes clé, le chiffrement forcé des disques, etc. Pour une gestion exhaustive et une application de la stratégie relative aux consommateurs, vous devez utiliser une installation estampillée du PGP Universal Server. Si nécessaire, contactez l'administrateur pour obtenir une installation estampillée.

En outre, lorsque vous établissez manuellement une liaison à un PGP Universal Server, le fichier `PGPtrustedcerts.asc` n'existe pas dans le dossier C:\Documents and Settings\AllUsers\Application Data\PGPCorporation\PGP. Si vous voulez effectuer une liaison manuelle à un PGP Universal Server, vous devrez créer ce fichier et faire en sorte que l'ID utilisateur de la clé d'entreprise figurant dans ce fichier corresponde au serveur spécifié par PGPSTAMP (le nom de domaine et l'adresse IP doivent correspondre).

D Utilisation de PGP Desktop avec IBM Lotus Notes

Cette section décrit l'utilisation de PGP Desktop avec Lotus Notes, notamment MAPI.

Contenu du chapitre

À propos de la compatibilité avec Lotus Notes et MAPI

Lorsqu'il est correctement défini, la messagerie PGP Desktop avec les clients de messagerie Lotus Notes et MAPI dans un environnement protégé par PGP Universal, fonctionne comme avec les clients POP ou IMAP, comme décrit dans la section *Sécurisation des messages électroniques* (à la page 93). Cette annexe complète les informations de ce chapitre.

Lotus Notes est une application groupware offrant des fonctionnalités de messagerie, d'agenda et de panification. Consultez les *Notes de publication de PGP Desktop pour Windows* pour plus d'informations sur les clients de messagerie Lotus Notes.

MAPI (Messaging Application Programming Interface) est une architecture de messagerie et une interface client utilisées dans les environnements Microsoft Exchange.

Grâce à la compatibilité de Lotus Notes et MAPI avec PGP Desktop, votre système de messagerie est protégé par la technologie PGP et vous conservez votre client existant, ainsi que les fonctionnalités offertes par Lotus Notes et MAPI.

L'installation de PGP Desktop est compatible avec Lotus Notes, quel que soit le nombre d'utilisateurs.

Utilisation de PGP Desktop avec Lotus Notes

Cette section présente l'interopérabilité de PGP Desktop et PGP Universal dans un environnement Lotus Notes.

Envoi de courriers électroniques au sein d'un environnement Lotus Notes

Dans un système exécutant Lotus Notes, PGP Desktop prend en charge l'envoi de messages avec les adresses SMTP et Notes.

Utilisation des adresses Notes

Les clients Lotus Notes utilisant PGP Desktop peuvent rechercher des clés à l'aide des adresses Notes. Lorsqu'un client de messagerie Lotus Notes envoie un courrier électronique, le client PGP Desktop ajoute automatiquement l'adresse Notes à la clé. Cette clé est ensuite synchronisée avec PGP Universal pour faciliter la recherche de clés par adresses Notes.

Toutes les clés PGP Universal Server sont associées à une adresse de courrier électronique SMTP (par exemple, josem@exemple.com). La clé des utilisateurs internes du client de messagerie Lotus Notes contient leur adresse Notes, ainsi que l'adresse SMTP. CN=josem/O=notes6@notes6, par exemple. En revanche la clé des utilisateurs externes ne contient jamais d'adresse Notes, car la communication s'effectue toujours via l'adresse SMTP. La clé des utilisateurs Lotus Notes internes comporte les deux adresses, car les requêtes de clé de PGP Universal Satellite pour Windows peuvent spécifier l'une ou l'autre adresse.

Utilisation d'adresses SMTP avec PGP Desktop

Les clients Lotus Notes utilisant PGP Desktop peuvent rechercher des clés au sein de l'entreprise à l'aide des ID SMTP. Certaines entreprises avec Lotus Notes font appel aux ID SMTP pour toute communication interne, tandis que d'autres donnent le choix à leurs employés. PGP Desktop s'intègre quelle que soit la configuration choisie. Dans ce cas, Lotus Notes construit le message dans MIME et le proxy de PGP Desktop exécute S/MIME.

Envoi de courriers électroniques hors d'un environnement Lotus Notes

Les clients Lotus Notes utilisant PGP Desktop acheminent les messages électroniques et recherchent les clés hors de l'entreprise à l'aide des ID SMTP. PGP Desktop s'intègre quelle que soit la configuration choisie. Dans ce cas, Lotus Notes construit le message dans MIME et le proxy de PGP Desktop exécute S/MIME ou PGP/MIME. Le destinataire reçoit et déchiffre le message.

Liaison à un PGP Universal Server

Lorsque vous utilisez les clients de messagerie Lotus Notes ou MAPI avec PGP Desktop *dans un environnement protégé par PGP Universal*, une étape de configuration supplémentaire peut être nécessaire, car ces clients doivent être connectés directement à leurs serveurs de messagerie respectifs Domino ou Exchange.

Cette section ne vous concerne pas si vous utilisez une version autonome de PGP Desktop, c'est-à-dire hors d'un environnement géré par un PGP Universal Server.

Vous devez établir une communication avec vos serveurs de messagerie, ainsi qu'avec votre PGP Universal Server. Pour ce faire, mettez une première stratégie en place pour le serveur de messagerie correspondant et une deuxième, conjointe pour le serveur de messagerie et le PGP Universal Server.

Cette « liaison » permet à votre client de messagerie d'accéder au serveur de messagerie pour envoyer et recevoir des courriers électroniques, ainsi qu'au PGP Universal Server pour obtenir des clés et des stratégies. Comme indiqué, une liaison est établie via des stratégies de messagerie PGP Desktop.

Deux méthodes permettent de créer les stratégies nécessaires pour la liaison : une liaison prédéfinie et une liaison manuelle.

Liaison prédéfinie

L'administrateur PGP configure le programme d'installation de PGP Desktop avec les informations nécessaires à la création de la liaison dans les stratégies de messagerie PGP Desktop. Les stratégies adaptées sont déjà configurées dans PGP Desktop.

Liaison manuelle

L'administrateur PGP ne configure pas le programme d'installation de PGP Desktop avec les informations nécessaires à la création de la liaison dans les stratégies de messagerie PGP Desktop ; vous les créez vous même.

Pour lier manuellement un serveur de messagerie et un PGP Universal Server, vous devez d'abord créer un service pour le PGP Universal Server et un autre service pour le serveur de messagerie avec une référence au PGP Universal Server.

Liaison manuelle entre un serveur de messagerie et un PGP Universal Server à l'aide de stratégies de messagerie PGP Desktop

1. Ouvrez PGP Desktop.
2. Cliquez sur la boîte de contrôle Messagerie PGP.

3 Sous le service autonome existant, cliquez sur **Universal Server <aucun>** et sélectionnez **Créer**.

4 Dans le menu Nouveau service de PGP Universal Server, saisissez le nom de votre Universal Server et cliquez sur **OK**.

5 Envoyez un message à vous-même via votre client de messagerie. Pour les utilisateurs MAPI, cela n'est pas nécessaire. Sinon, passez à l'étape 8.

6 Cliquez sur **OK** dans la boîte de dialogue **Opération interrompue à votre demande**.

7 Lisez le message de PGP Universal dans votre boîte de réception. La boîte de dialogue Assistant de génération de clé PGP s'affiche.

8 Cliquez sur **Suivant**.

9 Choisissez un **Mode clé** dans **Sélection de la gestion des clés**, puis cliquez sur **Suivant**.

10 Dans **Sélection de la source de clé**, choisissez **Clé PGP Desktop** si vous utilisez la version autonome de PGP Desktop. Sinon, sélectionnez **Nouvelle clé** ou **Importer la clé**.

11 Cliquez sur **Suivant**.

12 Sélectionnez la clé définie et cliquez sur **Suivant**.

13 Cliquez sur **Terminer**.

Adresses Notes

Les clés PGP Desktop sont généralement associées à au moins une adresse de courrier électronique SMTP : josem@exemple.com, par exemple.

Les clés PGP Desktop des utilisateurs du client de messagerie Lotus Notes dans un environnement géré par un PGP Universal Server peuvent contenir l'adresse Notes, ainsi que l'adresse SMTP : `CN=josem/O=notes6@notes6`, par exemple. (La clé des utilisateurs de la version autonome de PGP Desktop ne contient jamais l'ID Notes, car seule l'adresse SMTP est utilisée.)

Pour en savoir plus sur l'utilisation de PGP Desktop et d'un client de messagerie Lotus Notes dans un environnement géré par un PGP Universal Server, contactez votre administrateur PGP.

Paramètres du client Lotus Notes

Si vous utilisez PGP Desktop avec un client de messagerie Lotus Notes, dans le champ Home/Mail Server Setting de l'enregistrement de l'emplacement du client de messagerie, l'onglet Servers doit afficher le nom complet Notes (host/orgName), et non l'hôte WINS uniquement.

PGP Corporation vous recommande de renseigner le champ **Internet mail address** dans l'onglet Basics du document de l'emplacement actuel. OCNOTES s'appuie sur ce champ pour déterminer l'adresse de courrier électronique SMTP de l'utilisateur. Si ce champ est vide, PGP Desktop construit une adresse SMTP en fonction du document de domaine global du serveur Domino.

Si vous êtes en « mode Island » et que la recherche de clés échoue pour certains ou tous les destinataires, PGP Desktop essaie de chiffrer le message en recherchant les clés lorsque le réplicateur envoie le message vers votre serveur d'accueil.

Si la recherche de clés échoue pour certains destinataires et que l'option de chiffrement native Notes soit vérifiée, PGP Desktop autorise le client Lotus Notes à chiffrer le message aux destinataires dont le chiffrement PGP a échoué.

Fichier de configuration Notes.ini

PGP Desktop met à jour le fichier de configuration `notes.ini` et ajoute l'entrée suivante :

```
EXTMGR_ADDINS=nPGPNote.dll
```

Assurez-vous que cette entrée n'est pas modifiée, ni supprimée. PGP Desktop analyse le fichier `notes.ini` chaque fois qu'il démarre. Si cette entrée est absente, il l'ajoute à nouveau.

Utilisation du chiffrement natif Lotus Notes

La fonction de chiffrement natif de Lotus Notes permet aux utilisateurs de Lotus Notes d'envoyer des messages électroniques internes chiffrés à l'aide de la clé Notes de l'utilisateur. Lorsque la configuration de PGP Desktop prévoit le recours à cette fonction, il est possible d'envoyer des informations confidentielles sous forme chiffrée à des utilisateurs internes ; il suffit pour cela de cocher une case lors de la rédaction du message. Tous les utilisateurs de Lotus Notes disposent d'une clé Notes.

Si l'adresse de courrier électronique indiquée dans le champ À : est conforme au format Lotus Notes (CN = Alice Cameron/O = Example Corp) et que le chiffrement natif Notes soit activé, PGP Desktop autorise l'envoi de courrier électronique chiffré par le biais de Lotus Notes. Si l'adresse de courrier électronique indiquée dans le champ À : correspond à une adresse SMTP (acameron@example.com), PGP Desktop chiffre le courrier avec votre clé PGP.

Le chiffrement natif Lotus Notes est disponible tant pour les environnements gérés par un serveur PGP Universal Server que pour les environnements autonomes. Pour savoir comment l'activer dans un environnement autonome, consultez l'*article 1613 de la base de connaissances du support de PGP* (https://support.pgp.com/?faq=1613).

Lorsque les options de signature et/ou chiffrement des messages sont sélectionnées, PGP Desktop applique les stratégies de messagerie relatives aux boutons Signer et Chiffrer à l'ensemble des messages Lotus Notes sortants. Pour plus d'informations sur ces stratégies, reportez-vous à la section *Informations sur les stratégies de sécurité et exemples* (à la page 119). Si ce type de stratégies est introuvable dans votre environnement autonome, vous devrez en créer.

Pour utiliser le chiffrement natif Lotus Notes

1. Rédigez votre message dans Lotus Notes.
2. Dans la barre d'outils éventuellement disponible dans le modèle, cochez les cases **Signer** et/ou **Chiffrer**. En l'absence de barre d'outils, sélectionnez Options de remise et, dans la section relative aux options de sécurité, activez les options **Signer** et/ou **Chiffrer**.

   Remarque : vous devez cocher ces cases chaque fois que vous voulez envoyer un message électronique en ayant recours au chiffrement natif Lotus Notes.

3. Envoyez le message.
   - Si la stratégie de messagerie implique le chiffrement et si le destinataire du message utilise Lotus Notes, le message est envoyé après avoir été chiffré via le chiffrement natif Lotus Notes. Pour vous assurer que le message a été traité et chiffré par Lotus Notes, cliquez sur **Plus** lorsque le message du Notificateur apparaît. Lorsque le destinataire ouvre le message, aucune annotation PGP n'y est incluse.
   - Si la stratégie de messagerie implique le chiffrement et si le destinataire du message est représenté par une adresse SMTP, PGP Desktop recherche la clé PGP, et le message est envoyé après avoir été chiffré par PGP Desktop. Lorsque le destinataire ouvre le message, l'annotation PGP standard y est incluse.
   - Si la stratégie de messagerie implique le chiffrement, que le destinataire du message soit représenté par une adresse SMTP et que vous soyez connecté au serveur Domino de Lotus Notes, l'application tente de résoudre l'adresse SMTP en fonction de l'adresse Lotus Notes. Si l'opération peut être effectuée, le message est envoyé par le biais du chiffrement natif Lotus Notes. Pour vous assurer que le message a été traité et chiffré par Lotus Notes, cliquez sur **Plus** lorsque le message du Notificateur apparaît. Lorsque le destinataire ouvre le message, aucune annotation PGP n'y est incluse.
   - Si la stratégie de messagerie implique la signature, Lotus Notes signe le message avec la clé Notes de l'expéditeur. Aucun chiffrement n'est effectué, que ce soit par Lotus Notes ou PGP Desktop. Remarque : si l'option **Signer** n'est pas sélectionnée pour le message, PGP Desktop signe celui-ci à l'aide de la clé PGP de l'expéditeur.

Index

D

E

N

O

P

Q

R

S

T

U

V

W

X