

PGP® Desktop pour Mac OS X

Guide de l'utilisateur



Informations de version

Guide de l'utilisateur de PGP Desktop pour Macintosh OS X. PGP Desktop Version 10.0.0. Sortie en Décembre 2009.

Informations de copyright

Copyright © 1991-2009 - PGP Corporation. Tous droits réservés. Aucune partie du présent document ne doit être reproduite ni transmise, sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, à quelque fin que ce soit, sans le consentement écrit express de PGP Corporation.

Marques

PGP, Pretty Good Privacy et le logo PGP sont des marques déposées de PGP Corporation aux États-Unis et dans d'autres pays. IDEA est une marque de commerce d'Ascom Tech AG. Windows et ActiveX sont des marques déposées de Microsoft Corporation. AOL est une marque déposée, et AOL Instant Messenger une marque commerciale, d'America Online, Inc. Red Hat et Red Hat Linux sont des marques de commerce ou déposées de Red Hat, Inc. Linux est une marque déposée de Linus Torvalds. Solaris est une marque de commerce ou déposée de Sun Microsystems, Inc. AIX est une marque de commerce ou déposée d'International Business Machines Corporation. HP-UX est une marque commerciale ou déposée de Hewlett-Packard Company. SSH et Secure Shell sont des marques de commerce de SSH Communications Security, Inc. Rendezvous et Mac OS X sont des marques de commerce ou déposées d'Apple Computer, Inc. Toutes les autres marques, déposées ou non, mentionnées dans ce document appartiennent exclusivement à leur propriétaire respectif.

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.iig.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/LICENSE?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/license>.
- 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/license>.
- 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 informatisés, 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 objets 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

À propos de PGP Desktop 10.0 pour Mac OS X	1
Nouveautés de PGP Desktop pour Mac OS X version 10.0	2
Utilisation de ce manuel	3
Utilisateurs gérés/non gérés	4
Conventions employées dans ce manuel	4
À qui est destiné ce document	5
À propos des licences PGP Desktop	5
À propos des licences PGP Desktop	6
Consultation des détails de la licence	6
Si votre licence est arrivée à expiration	8
Assistance	9
Obtention d'informations sur le produit	9
Coordonnées	9
 Présentation de base de PGP Desktop	 11
Terminologie afférente à PGP Desktop	11
Composants du produit PGP	11
Terminologie utilisée dans PGP Desktop	13
Cryptographie conventionnelle et chiffrement par clé publique	14
Pour en savoir plus à propos de la cryptographie	15
Première utilisation de PGP Desktop	15
 Installation de PGP Desktop	 19
Configuration requise	19
Installation et configuration de PGP Desktop	19
Installation du logiciel	19
Utilisation de PGP Desktop avec Apple Boot Camp	20
Mise à niveau du logiciel	21
Définition d'une licence pour PGP Desktop	23
Exécution de l'assistant d'installation	23
Intégration à Entourage 2008	23
Désinstallation de PGP Desktop	24
Transfert d'une installation PGP Desktop vers un autre ordinateur	24
 Interface utilisateur de PGP Desktop	 27
Accès aux fonctions de PGP Desktop	27
Écran principal de PGP Desktop	28
Utilisation de l'icône PGP Desktop dans la barre de menus	29
Utilisation de l'icône PGP Dock	30
Utilisation du Finder sous Mac OS X	32

Alertes du Notificateur PGP Desktop	32
Notificateur PGP Desktop pour la messagerie	32
PGP Desktop et le Finder	37
Présentation	37
Chiffrer, signer, ou chiffrer et signer	38
Décomposer	40
Déchiffrer/vérifier	40
Monter ou démonter un volume PGP Virtual Disk	41
Importer une clé PGP	42
Ajouter des clés publiques PGP à votre trousseau	42
Extraire le contenu d'une archive PGP Zip	43
Affichage du journal de PGP	43

Utilisation des clés PGP 65

Affichage des clés	46
Création d'un trousseau de clés intelligent	47
Création d'une paire de clés	48
Paramètres de clé - Mode Expert	50
Protection de votre clé privée	51
Protection des clés et des trousseaux de clés	52
Sauvegarde de votre clé privée	53
Que faire si vous avez perdu votre clé ?	54
Distribution de votre clé publique	54
Mise de votre clé publique sur un serveur de clés	54
Inclusion de votre clé publique dans un message électronique	56
Exportation de votre clé publique dans un fichier	56
Obtention de clés publiques d'autres personnes	57
Obtention de clés publiques sur un serveur de clés	57
Obtention de clés publiques par message électronique	59
Utilisation des serveurs de clés	59
Utilisation de clés principales	60
Ajout de clés à la liste des clés principales	61
Suppression de clés de la liste des clés principales	61

Gestion des clés PGP 63

Examen et paramétrage des propriétés de la clé	63
Ajout et suppression de photographies	64
Gestion des noms d'utilisateur et des adresses de courrier électronique d'une clé	65
Modification de votre phrase secrète	66
Suppression de clés, d'ID d'utilisateur et de signatures	67
Désactivation et activation des clés publiques	68
Vérification d'une clé publique	69
Signature d'une clé publique	70
Révocation de votre signature à partir d'une clé publique	72
Attribution de confiance pour les validations de clés	72
Pour accorder de la confiance à une clé	73

Utilisation des sous-clés	73
Utilisation de sous-clés distinctes	75
Affichage des sous-clés	75
Création de sous-clés	76
Définition de l'utilisation des clés pour les sous-clés	77
Révocation de sous-clés	77
Suppression de sous-clés	78
Utilisation des clés de déchiffrement supplémentaire (ADK)	78
Ajout d'une clé de déchiffrement supplémentaire (ADK) à une paire de clés	79
Mise à jour d'une clé de déchiffrement supplémentaire	79
Suppression d'une clé de déchiffrement supplémentaire	80
Utilisation des révocateurs	80
Désignation d'un révocateur désigné	80
Révocation d'une clé	81
Scission et réassemblage de clé	82
Création d'une clé scindée	82
Réassemblage de clés scindées	83
Perte de votre clé ou phrase secrète	85
Reconstruction de clés avec PGP Universal Server	85
Création des données de reconstruction de clé	86
Reconstruction de votre clé en cas de perte de celle-ci ou de la phrase secrète	88
Protection de vos clés	89

Sécurisation des messages électroniques **91**

Processus PGP Desktop de sécurisation des messages électroniques	91
Messages entrants	92
Messages sortants	94
Utilisation de la stratégie hors connexion	94
Services et stratégies	95
Affichage des services et stratégies	96
Création d'un service de messagerie	97
Modification des propriétés du service de messagerie	100
Désactivation ou activation d'un service	100
Suppression d'un service	101
Services multiples	101
Dépannage des services de messagerie PGP	102
Création d'une stratégie de sécurité	104
Expressions normales dans les stratégies	110
Informations sur les stratégies de sécurité et exemples	111
Utilisation de la liste des stratégies de sécurité	115
Modification d'une stratégie de sécurité	115
Modification d'une stratégie de liste de publipostage	115
Suppression d'une stratégie de sécurité	120
Modification de l'ordre des stratégies dans la liste	121
PGP Desktop et SSL	121
Modes clé	123
Détermination du mode clé	125
Changement de mode clé	125

Affichage du journal de PGP	126
Utilisation de scripts PGP avec Entourage 2008	127

Sécurité de la messagerie instantanée **129**

À propos de la compatibilité de la messagerie instantanée avec PGP Desktop	129
Compatibilité avec les clients de messagerie instantanée	130
À propos des clés utilisées pour le chiffrement	131
Chiffrement des sessions de messagerie instantanée	131

Affichage des messages électroniques à l'aide de la Visionneuse PGP **133**

Présentation de la Visionneuse PGP	133
Clients de messagerie pris en charge	134
Ouverture d'un message électronique ou d'un fichier chiffré	135
Copie de messages électroniques dans votre boîte de réception	136
Exportation de messages électroniques	136
Préférences de la Visionneuse PGP	137
Fonctionnalités de sécurité dans la Visionneuse PGP	138

Protection des disques à l'aide de PGP Whole Disk Encryption **139**

À propos de PGP Whole Disk Encryption	140
Chiffrement de disques de démarrage	142
Quelles sont les différences entre PGP WDE et PGP Virtual Disk ?	142
Gestion des licences PGP Whole Disk Encryption	142
Expiration de la licence	143
Préparation du disque au chiffrement	143
Types de disques pris en charge	144
Claviers pris en charge	145
Vérification du bon fonctionnement du disque avant le chiffrement	146
Calcul de la durée du chiffrement	146
Effectuer un test pilote afin de vérifier la compatibilité du logiciel	147
Déterminer la méthode d'authentification du disque	147
Chiffrement d'un disque	148
Caractères pris en charge	148
Chiffrement du disque	149
Identification d'erreurs sur le disque lors du chiffrement	151
Utilisation d'un disque chiffré par PGP-WDE	151
Authentification à partir de l'écran PGP BootGuard	152
Continuité de la sécurité du disque	153
Affichage des informations sur la clé sur un disque chiffré	154
Modification de la partition système	154
Ajout d'utilisateurs supplémentaires à un disque chiffré	154
Suppression d'utilisateurs d'un disque chiffré	155
Modification des phrases secrètes des utilisateurs	156
Nouveau chiffrement d'un disque chiffré	156
Sauvegarde et restauration	157

Désinstallation de PGP Desktop des disques chiffrés	157
Utilisation de PGP WDE dans un environnement géré par un PGP Universal Server	158
Administration de PGP Whole Disk Encryption	158
Création d'un jeton de récupération	159
Utilisation d'un jeton de récupération	160
Récupération de données à partir d'un lecteur chiffré	160
Création et utilisation de disques de récupération	161
Déchiffrement d'un disque chiffré par PGP WDE	162
Déplacement des disques amovibles sur d'autres systèmes	162
Accès aux données stockées sur des disques amovibles chiffrés	163
Précautions spéciales de sécurité prises par PGP Desktop	163
Effacement de la phrase secrète	164
Protection de la mémoire virtuelle	164
Protection de la migration d'ions statiques dans la mémoire	164
Autres éléments de sécurité à prendre en compte	165
Détails techniques relatifs au chiffrement de disques de démarrage	166

Utilisation des PGP Virtual Disks

167

À propos des PGP Virtual Disks	168
Création d'un volume PGP Virtual Disk	169
Affichage des propriétés d'un PGP Virtual Disk	172
Utilisation d'un PGP Virtual Disk monté	172
Montage d'un PGP Virtual Disk	173
Démontage d'un PGP Virtual Disk	173
Définition de l'emplacement de montage	174
Compaction d'un PGP Virtual Disk	175
Nouveau chiffrement des volumes PGP Virtual Disk	175
Gestion des autres utilisateurs	176
Ajout de comptes autre utilisateur pour un volume PGP Virtual Disk	176
Suppression de comptes d'autres utilisateurs d'un PGP Virtual Disk	177
Désactivation et activation de comptes d'autres utilisateurs	178
Passage à l'état lecture/écriture et lecture seule	178
Attribution du statut administrateur à un autre utilisateur	179
Modification des phrases secrètes des utilisateurs	179
Suppression de volumes PGP Virtual Disk	180
Gestion des PGP Virtual Disks	181
Montage des volumes PGP Virtual Disk sur un serveur distant	181
Sauvegarde des volumes PGP Virtual Disk	181
Échange des PGP Virtual Disks	182
Algorithmes de chiffrement des PGP Virtual Disks	183
Précautions spéciales de sécurité prises par PGP Virtual Disk	184
Effacement de la phrase secrète	184
Protection de la mémoire virtuelle	184
Protection de la migration d'ions statiques dans la mémoire	184
Autres éléments de sécurité à prendre en compte	185

Accès aux données mobiles à l'aide de PGP Portable **187**

Accès aux données sur un disque PGP Portable	187
Modification de la phrase secrète d'accès à un PGP Portable Disk	189
Démontage d'un disque PGP Portable	189

Utilisation de PGP Zip **191**

Présentation	191
Création d'archives PGP Zip	192
Ouverture d'une archive PGP Zip	194
Vérification des archives PGP Zip signées	194

Décomposition de fichiers avec PGP Shredder **195**

Utilisation de PGP Shredder pour supprimer définitivement des dossiers et des fichiers	195
Décomposition de fichiers à l'aide de l'icône de PGP Shredder	197
Décomposition de fichiers à l'aide de l'icône Décomposer les fichiers dans la barre d'outils PGP Desktop	197
Décomposition de fichiers à l'aide de la fonction Décomposer du menu Fichier	197
Décomposition de fichier dans le Finder	198

Définition des préférences de PGP Desktop **199**

Accès aux préférences de PGP Desktop	199
Préférences générales	200
Préférences de clés	202
Préférences de clés principales	204
Préférences de messagerie	205
Options de proxy	207

Préférences liées aux disques	208
Préférences relatives aux notifications	210
Préférences avancées	212

Utilisation des mots de passe et phrases secrètes **213**

Mot de passe ou phrase secrète ?	213
Indicateur de qualité de la phrase secrète	214
Création de phrases secrètes fortes	215
Que faire si vous avez oublié votre phrase secrète ?	217
Enregistrement de votre phrase secrète dans la chaîne de clé	217

Utilisation de PGP Desktop avec un PGP Universal Server **219**

Présentation	220
À l'attention des administrateurs PGP	221
Liaison manuelle à un PGP Universal Server	221

Index **223**

1

À propos de PGP Desktop 10.0 pour Mac OS X

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 11). 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 14).

Contenu du chapitre

Nouveautés de PGP Desktop pour Mac OS X version 10.0	2
Utilisation de ce manuel.....	3
À qui est destiné ce document.....	5
À propos des licences PGP Desktop	5
Assistance.....	9

Nouveautés de PGP Desktop pour Mac OS X version 10.0

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

Généralités

- **Prise en charge de nouveaux systèmes d'exploitation.** Vous pouvez désormais installer PGP Desktop pour Mac OS X sur les systèmes exécutant Mac OS X 10.6.
- **Nouvelles versions localisées.** PGP Desktop a été localisé et peut maintenant être installé en français (France) et en espagnol (Amérique latine).
- **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.
- **Inscription après l'installation.** Une fois PGP Desktop pour Mac OS X installé, l'inscription à PGP Universal Server est lancée dès que l'utilisateur se connecte au système Mac OS X.

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.
- **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.
- **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 Whole Disk Encryption

- **Nouveaux claviers compatibles.** Quatre nouveaux claviers sont pris en charge pour la connexion à PGP BootGuard. Les voici : anglais (États-Unis - International), japonais (Japon), allemand (Allemagne), français (France), espagnol (Amérique latine), espagnol (Espagne, ISO).
- **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.
- **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 des caractères ASCII étendus.** Il est désormais possible d'utiliser les caractères ASCII étendus lors de la création d'utilisateurs PGP WDE.
- **Prise en charge supplémentaire de Boot Camp.** PGP Desktop pour Mac OS X peut maintenant être utilisé sur des systèmes sur lesquels Boot Camp est installé. Pour plus d'informations sur l'utilisation de Boot Camp avec PGP Desktop, reportez-vous aux instructions d'installation.

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 219).

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.

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 Mac OS X 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.

À propos des licences PGP Desktop

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 6) 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 6) pour consulter les détails de votre licence. Si vous devez enregistrer votre copie de PGP Desktop, suivez la procédure décrite dans la section *Autorisation de PGP Desktop pour Mac OS X* (cf. "Enregistrement de PGP Desktop pour Mac OS X" à la page 7).

Consultation des détails de la licence

► Pour afficher les détails de votre licence PGP Desktop

- 1 Ouvrez PGP Desktop.
- 2 Dans le menu **PGP**, sélectionnez **Licence**. La boîte de dialogue contenant les informations sur la licence apparaît. Cette boîte de dialogue apparaît :
 - **Nom** : nom attribué à la licence lors de son enregistrement.
 - **Entreprise** : entreprise à laquelle est octroyée la licence.
 - **Courrier électronique** : adresse de courrier électronique associée à votre licence.
 - **Type** : type de licence dont vous disposez (d'entreprise ou à usage personnel).
- 3 Cliquez sur **Détails**. Les détails relatifs à votre licence sont alors affichés.



- **Date d'expiration** : date à laquelle votre licence ne sera plus valide.

- **Nombre de postes** : Nombre de postes sur lesquels peut être installée la licence.
- **Fonctionnalités activées** : Composants actifs en fonction de la licence.
- **Fonctionnalités désactivées** : composants qui ne sont *pas* actifs avec la licence.

Remarque : si vous n'enregistrez pas votre copie de PGP Desktop, vous n'aurez accès qu'à un nombre limité de fonctionnalités (PGP Zip et Clés).

Enregistrement de PGP Desktop pour Mac OS X

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.

- 2 Ouvrez PGP Desktop.
- 3 Dans le menu **PGP**, sélectionnez **Licence**.
- 4 Cliquez sur **Modifier la licence**.
- 5 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.

- 6 Saisissez l'adresse de **courrier électronique** à associer à la licence du produit.

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 Effectuez l'une des opérations ci-dessous :

- Tapez votre numéro de licence à 28 caractères dans les champs **Numéro de licence** (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 **Essayer pendant 30 jours**. 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, cliquez sur **Acheter maintenant**. Votre navigateur s'ouvre, et vous pouvez accéder au magasin PGP Store en ligne.
- 8 Cliquez sur **Autoriser**.
- 9 Lorsque la licence a été autorisée, cliquez sur **OK** pour achever le processus.

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 de 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 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	11
Cryptographie conventionnelle et chiffrement par clé publique	14
Première utilisation de PGP Desktop.....	15

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* (à la page 6).

- **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 45).) 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.

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

Configuration requise	19
Installation et configuration de PGP Desktop	19
Désinstallation de PGP Desktop	24
Transfert d'une installation PGP Desktop vers un autre ordinateur.....	24

Configuration requise

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

- Apple Mac OS X 10.5.x ou 10.6.x (Intel)
- 512 Mo de RAM
- 64 Mo d'espace disque dur

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 la mise à jour, vous devez disposer de droits d'administration sur votre système.

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

► Pour installer PGP Desktop sur votre système Mac OS X

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

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

Utilisation de PGP Desktop avec Apple Boot Camp

Apple Boot Camp est compatible avec PGP Desktop version 10.0 ou ultérieure. Pour pouvoir utiliser PGP Desktop avec Boot Camp, vous devez installer le logiciel et chiffrer le disque dans un ordre précis.

Remarque : vérifiez que votre disque n'est pas chiffré (s'il l'est, déchiffrez-le avant d'installer Boot Camp), puis désinstallez PGP Desktop.

► Pour utiliser Apple Boot Camp

- 1** Installez Apple Boot Camp.
- 2** Installez PGP Desktop sur la partition Mac OS X et effectuez l'intégralité de l'inscription à l'aide de l'assistant d'installation.
- 3** Démarrez dans la partition Windows et installez PGP Desktop sous Windows, puis effectuez l'intégralité de l'inscription à l'aide de l'assistant d'installation.
- 4** Démarrez dans la partition Mac OS X et chiffrez le disque. À ce stade, si vous interrompez le processus de chiffrement pendant l'exécution de Mac OS X, vous pouvez le reprendre pendant l'exécution de Windows.

Si vous avez besoin de déchiffrer le disque, PGP Corporation vous recommande de procéder à partir de la partition Mac OS X.

Pour plus d'informations sur l'utilisation de PGP Desktop avec Apple Boot Camp, reportez-vous à l'*Article 1697 de la base de connaissances de PGP* (<https://support.pgp.com/?faq=1697>).

Mise à niveau du logiciel

Remarque : PGP Desktop pour Mac OS X et PGP Universal Satellite pour Mac OS X ne peuvent pas être installés conjointement sur un même système. Les programmes d'installation des deux produits sont capables de détecter la présence de l'autre application et, le cas échéant, de mettre fin à la procédure.

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

- PGP Desktop pour Mac OS X
- PGP Universal Satellite pour Mac OS X

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 de PGP Desktop avant d'effectuer la mise à niveau du système d'exploitation et d'installer cette version. 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 :

- **Dans PGP Desktop 8.x ou 9.x pour Mac OS X,** commencez l'installation de PGP Desktop 10.0 pour Mac OS X.

La version de PGP Desktop pour Mac OS X déjà présente est désinstallée automatiquement et PGP Desktop 10.0 pour Mac OS X est installé. Les trousseaux de clés et fichiers PGP Virtual Disk existants peuvent être utilisés dans la version plus récente.

- **Avec une version de PGP Desktop pour Mac OS X antérieure à la version 8.0,** vous devez désinstaller manuellement le logiciel existant pour pouvoir commencer l'installation de PGP Desktop 10.0 pour Mac OS X. Les trousseaux de clés et fichiers PGP Virtual Disk existants peuvent être utilisés dans la version mise à niveau.

Mise à niveau de PGP Universal Satellite

Effectuez l'une des opérations suivantes :

- **Dans PGP Universal Satellite version 1.2 (ou version antérieure) pour Mac OS X,** lancez l'installation de PGP Desktop 10.0 pour Mac OS X.

Les versions existantes de PGP Universal Satellite pour Mac OS X sont désinstallées automatiquement et PGP Desktop 10.0 pour Mac OS X 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 Mac OS X. Aucun des deux programmes ne fonctionnerait correctement. En cas d'installation conjointe, désinstallez les deux programmes, puis réinstallez seulement PGP Desktop.

- **Dans PGP Desktop pour Mac OS X (version 8.x) et PGP Universal Satellite :** suivez la procédure d'installation pour PGP Desktop 10.0 pour Mac OS X.

PGP Desktop pour Mac OS X et PGP Universal Satellite pour Mac OS X sont automatiquement désinstallés et PGP Desktop 10.0 pour Mac OS X est installé. Les trousseaux de clés et fichiers PGP Virtual Disk existants peuvent être utilisés dans la version plus récente, de même que les paramètres de PGP Universal Satellite pour Mac OS X.

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. "Préférences générales" à la page 200).

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 souhaitez 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), veuillez 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

Cet assistant vous présente une série d'écrans dans lesquels des questions vous sont posées, puis configure PGP Desktop en fonction de vos réponses.

Si vous avez des questions sur le contenu des écrans de l'assistant d'installation, cliquez sur **Aide**.

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.

Intégration à Entourage 2008

Le programme d'installation de PGP Desktop pour Mac OS X inclut des scripts permettant d'intégrer PGP Desktop à Entourage. Une fois que vous avez copié ces scripts dans les dossiers requis, le menu Scripts d'Entourage affiche une option nommée PGP. Utilisez les scripts d'Entourage pour chiffrer le contenu de vos messages sans avoir recours à un proxy de messagerie électronique.

► Pour intégrer les scripts PGP à Entourage

- 1 Si Entourage est en cours d'exécution, fermez l'application.
- 2 Ouvrez le dossier de téléchargement de PGP Desktop pour Mac OS X.

- 3 Dans celui-ci, ouvrez le dossier Extras.
- 4 Ouvrez ensuite le dossier Entourage.
- 5 Double-cliquez sur le fichier `EntourageScripts.zip` afin d'extraire les scripts suivants :
 - Decrypt & Verify\mod ;
 - Encrypt & Sign\moc ;
 - Encrypt\moe ;
 - Sign\mos.
- 6 Copiez les scripts et collez-les dans le dossier suivant :
 - User Profile\Documents\Microsoft User Data\Entourage Script Menu items\PGP
- 7 Lancez Entourage. Le menu Scripts inclut à présent une option dénommée PGP.

Pour plus d'informations concernant le chiffrement et le déchiffrement des messages, reportez-vous à la section *Utilisation de scripts PGP avec Entourage 2008* (à la page 127).

Désinstallation de PGP Desktop

► Pour désinstaller PGP Desktop

- 1 Dans le menu **PGP** de PGP Desktop, sélectionnez **Désinstaller**. Une boîte de dialogue de confirmation apparaît.
- 2 Cliquez sur **Oui** pour continuer la procédure de désinstallation.
- 3 Vous êtes invité à vous authentifier en tant qu'administrateur du système Mac OS X duquel vous désinstallez PGP Desktop. Entrez le mot de passe adéquat, puis cliquez sur **OK**. Le logiciel PGP Desktop est alors supprimé de votre système.

Vos trousseaux de clés et fichiers PGP Virtual Disk ne sont pas supprimés, en vue d'une réinstallation future de PGP Desktop.

Transfert d'une installation PGP Desktop vers 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 vers un autre ordinateur**

- 1** Désinstallez PGP Desktop. Pour ce faire, dans le menu **PGP** de PGP Desktop, sélectionnez **Désinstaller**.

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 un support amovible, par exemple un lecteur Flash, puis copiez le contenu du support sur le nouvel ordinateur. Par défaut, les fichiers de trousseau de clés sont placés dans le dossier 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.
- 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	27
Alertes du Notificateur PGP Desktop	32
PGP Desktop et le Finder.....	37
Affichage du journal de PGP	43

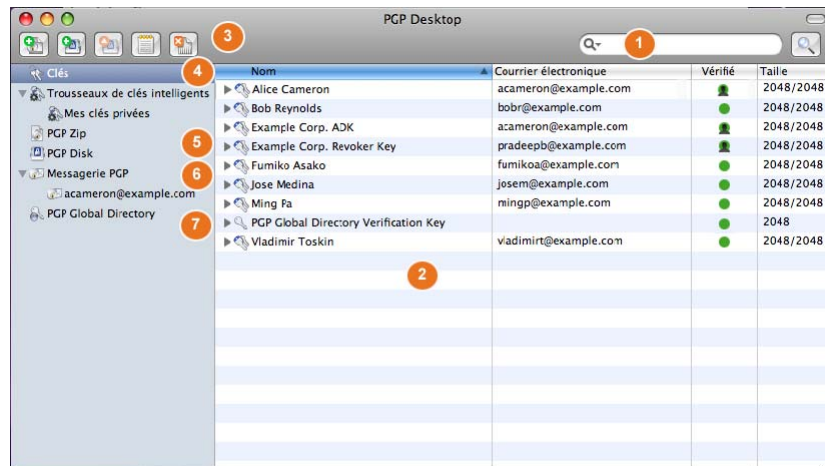
Accès aux fonctions de PGP Desktop

Quatre modes d'accès sont proposés :

- *Écran principal de PGP Desktop* (à la page 28)
- *Utilisation de l'icône PGP Desktop dans la barre de menus* (à la page 29)
- *Utilisation de l'icône PGP Dock* (à la page 30)
- *Utilisation du Finder sous Mac OS X* (à la page 32)

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 Le champ de recherche** : vous permet de rechercher des clés figurant dans le trousseau de clés local. Il suffit de saisir les caractères à rechercher pour que les noms et adresses de courrier électronique du trousseau de clés local qui comportent ces caractères s'affichent. Pour utiliser d'autres critères de recherche, cliquez sur **Recherche avancée**.
- 2 La zone de travail de PGP Desktop** : contient des informations sur l'élément sélectionné ainsi que sur les actions que vous pouvez lui appliquer.
- 3 La barre d'outils** : permet d'accéder aux fonctions fréquemment utilisées. Vous pouvez :
 - créer une archive PGP Zip ;
 - créer un volume PGP Virtual Disk ;
 - monter un volume PGP Virtual Disk existant ;
 - synchroniser des clés ;
 - décomposer des fichiers.
- 4 L'élément Clés** : vous permet de contrôler les clés PGP que PGP Desktop gère pour vous.
- 5 L'élément PGP Disk** : vous permet d'afficher et de gérer les volumes PGP Virtual Disk. Vous pouvez également l'utiliser pour créer d'autres volumes de ce type et pour chiffrer un disque non amorçable dans son intégralité à l'aide de la fonction PGP Whole Disk

Encryption.

6 L'élément Messagerie PGP : vous permet de gérer les services de messagerie PGP. Il sert en outre à créer des services et stratégies et à gérer ceux qui existent.

7 L'élément Serveurs de clés : vous permet d'afficher et de gérer les serveurs de clés.

(non visible) **L'élément PGP Zip** : vous permet d'afficher et de gérer les archives PGP Zip.

Utilisation de l'icône PGP Desktop dans la barre de menus

La plupart des fonctions de PGP Desktop sont accessibles via l'icône PGP Desktop dans la barre de menus.



Lorsque vous cliquez sur l'icône PGP Desktop dans la barre de menus, le menu PGP s'affiche. Remarque : selon que vous vous trouviez dans un environnement autonome ou géré, certaines options peuvent ne pas être disponibles.

- **À propos de PGP Desktop** : cette option permet d'afficher des informations sur la version de PGP Desktop que vous avez installée, y compris sur la licence, ainsi qu'une liste des personnes qui ont contribué à la création de PGP Desktop. Un bouton est également disponible pour lancer la désinstallation de PGP Desktop.
- **Aide** : cette option permet d'ouvrir l'aide en ligne intégrée à PGP Desktop.
- **Ouvrir PGP Desktop** : cette option permet d'ouvrir la fenêtre principale de PGP Desktop.
- **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.
- **Afficher le notificateur** : cette option affiche la fenêtre du Notificateur PGP Desktop dans laquelle vous pouvez consulter les notifications qui se sont affichées.
- **Afficher le journal** : cette option permet d'afficher le journal de PGP Desktop. Ce journal répertorie les mesures prises par PGP Desktop pour sécuriser vos données.
- **Effacer le journal** : cette option permet d'effacer le journal de PGP.

- **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.
- **Modifier la phrase secrète** : Fournit un raccourci pour vous aider à modifier la phrase secrète de votre clé. 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.
- **Masquer** : cette option permet de supprimer l'icône PGP de la barre de menus. Toutefois, l'exécution de l'application se poursuit en arrière-plan.

Lorsque vous maintenez la touche **Option** avant de cliquer sur l'icône PGP Desktop, l'option **Masquer** est remplacée par la commande **Quitter**. L'icône PGP Desktop disparaît ainsi de la barre de menus et *les processus de PGP Desktop exécutés en arrière-plan se ferment*. Les menus contextuels restent disponibles.

Attention : si vous arrêtez les processus de PGP Desktop exécutés en arrière-plan à l'aide de la touche Option et de l'icône de la barre de menus PGP, les fonctions de chiffrement, déchiffrement, signature et vérification des messages électroniques sont suspendues. Il vous sera également impossible de déchiffrer les messages reçus lorsque PGP Desktop n'était pas exécuté, même lorsque vous aurez redémarré l'application. Enfin, la gestion des clés ne peut être effectuée que lorsque les processus fonctionnent en arrière-plan. C'est pourquoi, il est recommandé de toujours conserver les processus en arrière-plan de PGP Desktop en cours d'exécution.

► **Pour redémarrer les processus en arrière-plan de PGP Desktop lorsque l'application n'est pas exécutée**

- 1 Localisez l'application PGP Desktop sur votre système. L'emplacement par défaut est le dossier Applications.
- 2 Double-cliquez sur l'icône PGP Desktop. L'application démarre et l'icône PGP Desktop s'affiche dans la barre de menus.

Utilisation de l'icône PGP Dock

La plupart des fonctions de PGP Desktop sont accessibles via l'icône PGP Dock.



Utilisation de l'icône PGP Desktop de la station d'accueil de Mac OS X de l'une des manières suivantes, puis choix d'une option dans le menu affiché.

- Cliquez sur l'icône PGP Desktop Dock et maintenez le bouton de la souris enfoncé.
- Appuyez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur l'icône Dock.
- Cliquez avec le bouton droit si celle-ci est munie de deux boutons.

L'icône PGP Desktop est affichée dans la station d'accueil lorsque l'application est ouverte ou si vous l'y avez placée manuellement.

Lorsque vous cliquez dessus *et maintenez* le bouton de la souris enfoncé alors que l'application est déjà ouverte (ou cliquez dessus tout en maintenant la touche Ctrl enfoncée, ou encore cliquez avec le bouton droit si votre souris est munie de deux boutons), un menu comportant les éléments suivants apparaît.

- Le nom de toutes les fenêtres ouvertes dans PGP Desktop : si PGP Desktop est en cours d'exécution, les fenêtres de l'application ouvertes apparaissent en haut de ce menu.
- **À propos de PGP Desktop** : cette option permet d'afficher la boîte de dialogue À propos de PGP Desktop. Cette dernière indique les mentions de source pour PGP Desktop et la version actuellement utilisée, et comprend un bouton permettant de désinstaller le logiciel.
- **Préférences** : cette option permet d'ouvrir la boîte de dialogue des préférences de PGP Desktop.
- **Presse-papiers** : cette option sert à chiffrer, signer, chiffrer et signer, ou déchiffrer et vérifier le contenu du Presse-papiers.
- **Rechercher les mises à jour** : cette option permet de vérifier si des versions plus récentes de PGP Desktop sont disponibles. Si une nouvelle version est détectée, vous pouvez la télécharger.
- **Effacer les caches** : cette option permet de supprimer les informations mises en cache, telles que les phrases secrètes et les clés publiques.

Les options restantes qui figurent à la fin du menu sont des options standard de la station d'accueil Mac OS X :

- **Supprimer du Dock/Garder dans le Dock** : cette option permet d'ajouter l'icône PGP Desktop dans la station d'accueil ou de la supprimer.
- **Ouvrir à l'ouverture de session** : cette option permet de paramétrer la préférence système de compte Mac OS X de sorte que PGP Desktop soit lancé lorsque vous vous connectez à l'ordinateur.
- **Afficher dans le Finder** : cette option indique l'emplacement de l'application PGP Desktop dans une fenêtre du Finder.
- **Masquer** : cette option permet de masquer les écrans de l'application PGP Desktop.
- **Quitter** : cette option permet de fermer PGP Desktop.

Si vous cliquez sur l'icône PGP Desktop dans la station d'accueil alors que l'application est fermée et maintenez le bouton de la souris enfoncé, les éléments standard de la station d'accueil Mac OS X apparaissent.

Utilisation du Finder sous Mac OS X

Dans Desktop ou une fenêtre du Finder, cliquez sur un fichier ou un dossier tout en maintenant la touche Ctrl enfoncée (ou cliquez dessus avec le bouton droit si votre souris est dotée de deux boutons) et, dans le menu contextuel qui apparaît, sélectionnez **PGP**.

Vous pouvez également accéder aux fonctionnalités de PGP Desktop à partir du Finder sous Mac OS X.

► Utilisation du Finder sous Mac OS X

- 1 Ouvrez une fenêtre du Finder.
- 2 Maintenez le bouton Ctrl et cliquez (ou cliquez avec le bouton droit si vous disposez d'une souris à deux boutons) sur le fichier ou le dossier désiré.
- 3 Sélectionnez l'option souhaitée dans le menu contextuel PGP. Sélectionnez **Chiffrer**, **Signer**, **Chiffrer et signer**, **Déchiffrer/vérifier**, **Décomposer** ou **Monter** (si vous disposez de PGP Virtual Disks).

Conseil : vous pouvez aussi cliquer avec le bouton droit sur un fichier ou un dossier à partir du Bureau.

Alertes du Notificateur PGP Desktop

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

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* (cf. "Préférences relatives aux notifications" à la page 210).

Messages entrants du notificateur PGP Desktop

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.

Messages sortants du notificateur PGP Desktop

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). Le message de notification affiche des informations dans lesquelles PGP Desktop recherche les clés publiques du destinataire. Lorsqu'il trouve les clés requises, la ligne État indique que le message envoyé est chiffré. Si les clés sont introuvables, PGP Desktop suit la stratégie adéquate et le message est alors bloqué ou envoyé en clair.

Après l'envoi du message chiffré, cliquez sur **Plus** pour consulter les détails relatifs au traitement du message par PGP Desktop. La consultation de ces informations supplémentaires est facultative. Pour les masquer à nouveau, cliquez sur **Moins**.

Vous pouvez retarder l'envoi du message en plaçant le curseur sur la fenêtre du notificateur. Sinon, après un délai 4 secondes (à définir dans les préférences du notificateur) le message est chiffré et envoyé, comme indiqué dans le champ État.

Lorsque vous placez le curseur sur le message, les boutons **Bloquer** et **Envoyer** apparaissent dans la fenêtre du notificateur. Cliquez sur **Bloquer** pour ne pas transmettre le message ou sur **Envoyer** pour l'envoyer.

Si lors de l'envoi d'un message à plusieurs destinataires, PGP Desktop ne trouve pas les clés de tous les destinataires, le notificateur vous informe de l'état du message. Vous avez alors deux possibilités :

- Envoyer le message chiffré aux destinataires dont la clé a été trouvée et non chiffré aux autres.
- Bloquer le message et ne l'envoyer à personne.

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.

Activation ou désactivation des messages de notification

► Pour activer ou désactiver des messages de notification

- 1** Ouvrez PGP Desktop et sélectionnez **PGP > Préférences**.
- 2** Cliquez sur l'icône 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 haut à gauche**.
- 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**. Décochez cette case 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 d'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 95).)
- 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. Il 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**.

5

PGP Desktop et le Finder

Cette section explique comment accéder à certaines fonctions de PGP Desktop en utilisant les menus contextuels du Finder.

Contenu du chapitre

Présentation	37
Chiffrer, signer, ou chiffrer et signer.....	38
Décomposer	40
Déchiffrer/vérifier	40
Monter ou démonter un volume PGP Virtual Disk	41
Importer une clé PGP.....	42
Ajouter des clés publiques PGP à votre trousseau.....	42
Extraire le contenu d'une archive PGP Zip.....	43

Présentation

Vous avez la possibilité d'accéder aux fonctions de PGP Desktop via les menus contextuels du Finder pour exécuter les mêmes commandes PGP Desktop que celles disponibles dans le menu Services de Mac OS X.

Selon l'option que vous choisissez, vous pouvez :

- Chiffrer, signer, ou chiffrer et signer
- Décomposer
- déchiffrer/vérifier ;
- monter, modifier ou démonter un volume PGP Virtual Disk ;
- importer une clé PGP ;
- ajouter des clés PGP à votre trousseau ;
- afficher le contenu d'une archive PGP Zip.

Méthodes d'accès aux menus contextuels du Finder :

- Ctrl+clic : si vous possédez une souris avec un seul bouton, appuyez sur la touche Ctrl de votre clavier et, tout en la maintenant enfoncée, cliquez sur l'option souhaitée.
- Clic droit : si vous possédez une souris à deux boutons, cliquez sur l'option avec le bouton droit.

Dans ce document, c'est la première méthode qui est utilisée. Si vous décidez d'employer le clic droit ou une autre méthode pour accéder aux menus contextuels du Finder, remplacez la méthode Ctrl+clic dans la configuration par la méthode choisie.

Remarque : les fichiers inclus dans le Finder comprennent des fichiers du bureau Mac OS X.

Chiffrer, signer, ou chiffrer et signer

PGP Desktop vous permet de chiffrer, signer, ou chiffrer et signer les fichiers et dossiers non chiffrés, voire des lecteurs complets, à partir du Finder.

Le chiffrement et/ou la signature de fichiers et dossiers constitue un bon moyen de protéger les quelques fichiers et/ou dossiers importants lorsque l'utilisation d'un volume PGP Virtual Disk ne s'impose pas.

Si vous envisagez de chiffrer et/ou signer un lecteur dans le Finder, ce type de volume peut néanmoins être une solution plus adéquate. Pour plus d'informations, reportez-vous à la section Utilisation des PGP Virtual Disks.

► Pour chiffrer et/ou signer des fichiers/dossiers dans le Finder

- 1 Dans le Finder, sélectionnez les fichiers/dossiers à chiffrer et/ou signer. Vous pouvez choisir toute combinaison de fichiers et dossiers à l'aide des touches Maj ou Commande.
- 2 Cliquez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur les fichiers et/ou dossiers sélectionnés ; vous pouvez aussi cliquer avec le bouton droit si vous disposez d'une souris à deux boutons. Dans le menu contextuel, choisissez **PGP**, puis **Chiffrer et signer**. (**Si vous choisissez uniquement Chiffrer**, il ne vous sera *pas* demandé de fournir une clé de signature ; de même, si vous choisissez uniquement **Signer**, vous n'aurez *pas* à sélectionner de clé publique à utiliser pour le chiffrement.) La boîte de dialogue Destinataires PGP apparaît.
- 3 Faites glisser les clés publiques des utilisateurs que vous souhaitez autoriser à déchiffrer les éléments que vous chiffrez dans la zone **Destinataires** située en bas de la boîte de dialogue.
- 4 Cliquez sur la flèche vers le bas située au-dessus du bouton **OK** pour préciser les options appropriées :

- **Chiffrement conventionnel** : cochez cette case si vous voulez recourir à une cryptographie par phrase secrète plutôt que par clé publique. Le fichier est alors chiffré à l'aide d'une clé de session, grâce à laquelle le chiffrement et le déchiffrement sont réalisés avec la phrase secrète spécifiée.

Si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, le chiffrement cryptographique peut être désactivé.

- **Sortie texte** : lors de l'envoi d'un fichier en pièce jointe via certaines applications de messagerie, vous pouvez être amené à enregistrer le fichier au format ASCII ; pour ce faire, cochez la case **Sortie texte**. Cette opération est parfois nécessaire lorsqu'un fichier binaire doit être envoyé avec des applications de messagerie anciennes. Lorsque cette option est activée, la taille du fichier chiffré augmente d'environ 30 %.
- **Décomposition originale** : cochez cette case pour remplacer le document original que vous chiffrez, de sorte que vos informations sensibles ne puissent être lues par personne ayant accès à votre système.
- **MacBinary** : MacBinary est la méthode standard de conversion d'un fichier Mac OS X en fichier unique en vue de son transfert vers un autre ordinateur Macintosh ou PC sans perte du segment de données ni de ressource. Les options disponibles sont Oui, Non et Intelligent.

Avec l'option **Oui**, le fichier est inclus dans son intégralité, y compris les informations propres à Mac OS X. Avec l'option **Non**, seul le segment de données est inclus. Enfin, avec l'option **Intelligent**, le type de fichier détermine si les informations propres à Mac OS X sont incluses.

- 5 Cliquez sur **OK**. Si vous avez sélectionné l'option de chiffrement conventionnel, vous êtes invité à fournir une phrase secrète pour protéger les éléments chiffrés.
- 6 Saisissez une phrase secrète, confirmez-la, puis cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
- 7 À l'aide de la liste Clé de signature, indiquez la clé privée à utiliser pour signer les éléments que vous chiffrez et signez, puis entrez la phrase secrète liée à la clé de signature. Si celle-ci est en cache, vous n'avez pas besoin de la saisir.

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 n'est témoin de votre saisie (physiquement ou via le réseau), vous pouvez afficher les caractères en cochant la case **Afficher les frappes**.

- 8 Pour enregistrer votre phrase secrète dans la chaîne de clé Mac OS X, activez cette option. La prochaine fois que vous utiliserez cette fonctionnalité, vous n'aurez pas besoin d'entrer la phrase secrète.
- 9 Cliquez sur **OK**. Une archive PGP Zip (<nom du fichier>.pgp) est créée à l'emplacement des éléments chiffrés et signés.

Décomposer

Lorsque vous souhaitez vous assurer que des fichiers et/ou dossiers spécifiques seront supprimés en toute sécurité de votre système, décomposez-les à partir du Finder.

Si vous vous contentez de placer un fichier ou un dossier dans la corbeille Mac OS X, celui-ci est seulement remplacé par de nouveaux fichiers. En fait, au bout de plusieurs jours, semaines, voire mois, un utilisateur ayant accès à votre système peut le récupérer.

La fonctionnalité Décomposer de PGP Desktop, au contraire, remplace vos fichiers à plusieurs reprises lors de leur décomposition. Pour plus d'informations concernant la portée d'effacement de cette fonctionnalité, reportez-vous à la section Décomposition de fichiers.

► Pour décomposer des fichiers et/ou dossiers dans le Finder

- 1 Dans le Finder, sélectionnez les fichiers et/ou dossiers à décomposer. Vous pouvez choisir toute combinaison de fichiers et dossiers à l'aide des touches Maj ou Commande.
- 2 Cliquez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur les fichiers et/ou dossiers sélectionnés ; vous pouvez aussi cliquer avec le bouton droit si vous disposez d'une souris à deux boutons.
- 3 Dans le menu contextuel, choisissez **PGP**, puis **Décomposer**. Un écran PGP s'affiche, et vous êtes invité à confirmer que vous voulez effectivement décomposer les fichiers répertoriés.
- 4 Cliquez sur **OK**. Les fichiers sont décomposés (supprimés en toute sécurité) de votre système ; ils n'apparaissent pas dans la corbeille.

Déchiffrer/vérifier

Si vous possédez un fichier PGP Zip (.pgp) sur votre système, vous pouvez le déchiffrer et le vérifier dans le Finder. Lors de l'opération de déchiffrement/vérification, c'est toujours un fichier chiffré (.pgp) qui est déchiffré. Cependant, si ce fichier chiffré n'a pas été signé, il ne sera pas vérifié (puisque aucune signature n'est disponible pour cette vérification).

Il est en outre possible de déchiffrer/vérifier un fichier de clés PGP (.asc), mais dans ce cas, le but n'est pas véritablement de déchiffrer ou vérifier le fichier, mais simplement de pouvoir importer les clés. Pour plus d'informations sur l'importation dans le Finder des clés PGP d'un fichier .asc, reportez-vous à la section *Importer une clé PGP* (à la page 42).

► **Pour déchiffrer/vérifier un fichier PGP Zip dans le Finder**

- 1 Dans le Finder, sélectionnez le fichier PGP Zip (.pgp) à déchiffrer/vérifier.
- 2 Cliquez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur les fichiers et/ou dossiers sélectionnés ; vous pouvez aussi cliquer avec le bouton droit si vous disposez d'une souris à deux boutons. Dans le menu contextuel, choisissez **PGP**, puis **Déchiffrer et vérifier**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
- 3 Saisissez la phrase secrète pour la clé privée. Si celle-ci est déjà en cache, elle ne vous sera pas demandée.

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 n'est témoin de votre saisie (physiquement ou via le réseau), vous pouvez afficher les caractères en cochant la case **Afficher les frappes**.

- 4 Pour enregistrer votre phrase secrète dans la chaîne de clé Mac OS X, activez cette option. La prochaine fois que vous utiliserez cette fonctionnalité, vous n'aurez pas besoin d'entrer la phrase secrète.
- 5 Cliquez sur **OK**. Le fichier est déchiffré à l'emplacement du fichier .pgp. S'il a été signé, PGP Desktop affiche les résultats de la vérification dans l'écran Infos de vérification.

Monter ou démonter un volume PGP Virtual Disk

Si vous possédez un fichier PGP Virtual Disk (.pgd) démonté, vous pouvez monter le volume PGP Virtual Disk correspondant à partir du Finder. Pour plus d'informations concernant les volumes PGP Virtual Disk, reportez-vous à la section Utilisation des PGP Virtual Disks.

► **Pour monter un volume PGP Virtual Disk à partir du Finder**

- 1 Dans le Finder, sélectionnez le fichier PGP Disk (.pgd) correspondant au volume à monter. Cliquez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur ce fichier .pgd ; vous pouvez aussi cliquer dessus avec le bouton droit si vous disposez d'une souris à deux boutons. Dans le menu **PGP**, sélectionnez **Monter**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
- 2 Entrez la phrase secrète qui permettra de protéger le volume PGP Disk que vous allez monter.

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 n'est témoin de votre saisie (physiquement ou via le réseau), vous pouvez afficher les caractères en cliquant sur **Frappe masquée**.

- 3 Cliquez sur **OK**. Le volume PGP Disk est alors monté.

► **Pour démonter un volume PGP Virtual Disk dans le Finder**

- 1 Sélectionnez le fichier PGP Disk (.pgd) correspondant au volume *monté* que vous voulez démonter.
- 2 Cliquez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur ce fichier .pgd ; vous pouvez aussi cliquer dessus avec le bouton droit si vous disposez d'une souris à deux boutons. Dans le menu contextuel, choisissez **PGP**, puis **Démonter**. **Le volume PGP Disk sélectionné est démonté.**

Conseil : si le menu comprend l'option **Monter**, cela signifie que le volume est déjà démonté.

Importer une clé PGP

Les clés PGP issues de PGP Desktop peuvent être exportées sous la forme de fichiers .asc. Ce type d'exportation vous permet de sauvegarder vos clés ou d'échanger vos clés publiques avec des tiers. Si, sur votre système, vous disposez d'un fichier .asc contenant une clé PGP que vous souhaitez inclure dans votre trousseau, vous pouvez l'importer dans le Finder.

► **Pour importer les clés d'un fichier .asc dans le Finder**

- 1 Dans le Finder, recherchez le fichier de clés PGP (.asc) contenant les clés à importer.
- 2 Double-cliquez dessus. PGP Desktop est alors lancé et la boîte de dialogue de sélection de clés apparaît.
- 3 Choisissez la ou les clés PGP que vous voulez importer, puis cliquez sur **OK**. Les clés sélectionnées sont ajoutées à votre trousseau.

Conseil : pour importer une clé, vous pouvez également sélectionner Fichier > Ouvrir et rechercher le fichier .asc souhaité.

Ajouter des clés publiques PGP à votre trousseau

PGP Desktop stocke vos clés PGP dans des trousseaux ; vous disposez toujours d'un fichier de trousseau de clés privées (.skr) qui contient les clés privées ainsi que d'un fichier de trousseau de clés publiques (.pkr) qui contient les clés publiques.

Si vous le souhaitez, vous pouvez ajouter les clés de l'un de vos fichiers de trousseau de clés publiques inactifs à votre trousseau actif sur le système à partir du Finder.

► **Pour ajouter les clés publiques PGP d'un fichier de trousseau à partir du Finder**

- 1 Dans le Finder, faites glisser le fichier de trousseau de clés publiques PGP (.pkx) ou de clés privées PGP (.skx) sur votre trousseau actif dans la fenêtre PGP DT. La boîte de dialogue de sélection de clés, qui contient les clés publiques du fichier de trousseau de clés publiques sélectionné, apparaît.
- 2 Choisissez les clés à ajouter au trousseau actif et cliquez sur **OK**. Pour sélectionner ces clés, vous pouvez utiliser l'option **Sélectionner tout** ou **Sélectionnez Aucun** et les touches Maj et Commande. La boîte de dialogue de sélection de clés est fermée et les clés sélectionnées sont ajoutées à votre trousseau actif.

Conseil : dans le Finder, double-cliquez sur le fichier de trousseau de clés publiques PGP (.pkx) ou de clés privées PGP (.skx). Le nouveau trousseau de clés est alors affiché dans PGP Desktop, en dessous des trousseaux existants, et signalé comme étant un trousseau de clés publiques PGP.

Extraire le contenu d'une archive PGP Zip

Si vous disposez sur votre système d'une archive PGP Zip, vous pouvez extraire son contenu dans le Finder.

► **Pour extraire le contenu d'une archive PGP Zip dans le Finder**

- 1 Dans le Finder, sélectionnez le fichier d'archive PGP Zip (.pgp) dont vous souhaitez extraire le contenu.
- 2 Cliquez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur ce fichier .pgp ; vous pouvez aussi cliquer dessus avec le bouton droit si vous disposez d'une souris à deux boutons. Dans le menu contextuel, choisissez PGP, puis **Déchiffrer et vérifier**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
- 3 Saisissez la phrase secrète qui protège l'archive PGP Zip dont vous allez extraire les fichiers, puis cliquez sur **OK**. Les fichiers sont extraits de l'archive à l'emplacement où celle-ci se trouve dans le Finder.
- 4 Si l'archive a été signée, la boîte de dialogue Infos de vérification apparaît.

Affichage du journal de PGP

Ce journal répertorie les mesures prises par PGP Desktop pour sécuriser vos données. Pour plus d'informations, reportez-vous à la section *Affichage du journal de PGP* (à la page 126).

6

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.

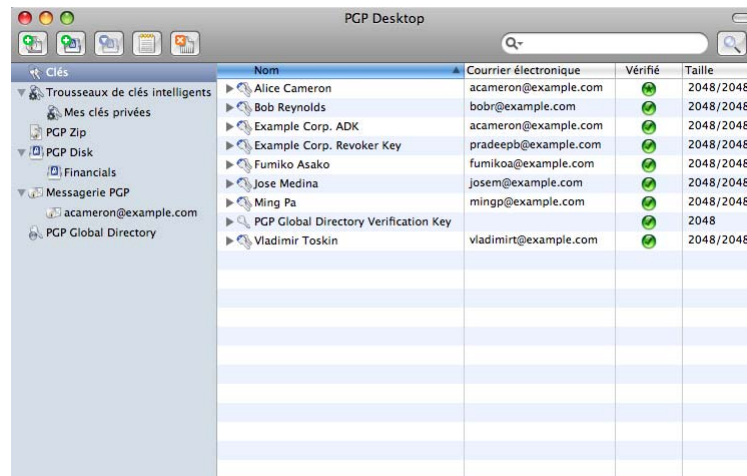
Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, votre administrateur PGP Universal Server peut avoir désactivé certaines fonctionnalités. Lorsqu'une fonctionnalité est désactivée, l'élément de contrôle situé à gauche de l'écran ne s'affiche pas, et le menu 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.....	46
Création d'une paire de clés	48
Protection de votre clé privée.....	51
Distribution de votre clé publique	54
Obtention de clés publiques d'autres personnes	57
Utilisation des serveurs de clés	59
Utilisation de clés principales.....	60

Affichage des clés

Pour afficher toutes les clés du trousseau local, ouvrez PGP Desktop et cliquez sur l'élément **Clés**.



Vous pouvez également avoir recours à la fonction *Trousseaux de clés intelligentes*. Un trousseau de clés intelligent est un groupe de clés qui correspond aux critères que vous avez définis. Par exemple, si vous envoyez souvent des messages aux utilisateurs de PGP Desktop provenant d'un domaine de messagerie particulier, vous pouvez créer un trousseau de clés intelligent qui n'inclura que les utilisateurs issus de ce domaine. Le trousseau de clés intelligent par défaut se nomme *Mes clés privées*.

Certaines des tâches les plus communes que vous voudrez peut-être effectuer sont disponibles dans la zone de travail Clés PGP. Les voici :

- Envoi d'un courrier électronique au propriétaire d'une clé publique. Pour exécuter cette tâche, dans n'importe quelle vue des clés PGP de vos trousseaux de clés, appuyez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur une clé publique (vous pouvez aussi cliquer dessus avec le bouton droit de votre souris), puis sélectionnez l'option **Envoyer un courrier électronique**.
- Si vous choisissez une clé publique trouvée dans les résultats d'une recherche, mais absente de vos trousseaux de clés locaux, vous devez l'ajouter à un trousseau. Pour cela, cliquez sur la clé tout en maintenant la touche Ctrl enfoncée (ou cliquez dessus avec le bouton droit) et sélectionnez **Ajouter au trousseau de clés par défaut**.
- Pour voir les propriétés d'une clé affichée dans la zone de travail, double-cliquez sur une partie quelconque de la clé afin d'afficher la boîte de dialogue Infos sur la clé correspondante.

Création d'un trousseau de clés intelligent

► Pour créer un trousseau de clés intelligent

- 1 Ouvrez PGP Desktop.
- 2 Cliquez sur l'élément **Clés**.
- 3 Sélectionnez **Fichier > Nouveau > Trousseau de clés intelligent**. La boîte de dialogue Nouveau trousseau de clés intelligent s'affiche.
- 4 Dans le champ **Nom du trousseau de clés intelligent**, tapez un nom descriptif pour le trousseau de clés intelligent que vous êtes en train de créer.
- 5 Dans le menu **Inclure les clés correspondant aux conditions suivantes**, sélectionnez l'une des options suivantes :
 - **Au moins un** : affiche les clés correspondant à l'un des critères spécifiés (« OU » logique).
 - **Tous** : affiche seulement les clés correspondant à tous les critères spécifiés (« ET » logique).
- 6 Dans la première colonne correspondante, sélectionnez l'une des options suivantes :
 - **La clé est** : affiche les clés correspondant aux critères.
 - **La clé n'est pas** : affiche les clés ne correspondant pas aux critères.
 - **Nom** : affiche les clés dont les critères indiqués figurent dans le nom.
 - **Courrier électronique** : affiche les clés dont les critères indiqués figurent dans l'adresse électronique.
 - **ID de clé** : affiche les clés dont les critères indiqués figurent dans l'ID de clé.
 - **Taille de clé** : affiche les clés ayant la taille indiquée.
 - **Date de création** : affiche les clés créées à la date indiquée.
 - **Date d'expiration** : affiche les clés arrivant à expiration à la date indiquée.
- 7 Les options de la seconde colonne correspondante changent en fonction des éléments sélectionnés dans la première colonne correspondante. Les options suivantes sont disponibles :
 - **Publique** : seules les clés publiques correspondent.
 - **Privée** : seules les clés privées correspondent.
 - **Révoquée** : seules les clés révoquées correspondent.
 - **Activé** : seules les clés activées correspondent.
 - **Expiré** : seules les clés expirées correspondent.

- **Signé par** : seules les clés signées par la personne indiquée correspondent.
 - **Contient** : une correspondance est trouvée lorsque la clé contient les critères indiqués.
 - **Ne contient pas** : une correspondance est trouvée lorsque la clé ne contient pas les critères indiqués.
 - **Est** : une correspondance est trouvée lorsque les critères indiqués (nom ou date) sont remplis.
 - **N'est pas** : une correspondance est trouvée lorsque les critères indiqués ne sont pas remplis.
 - **Est au moins** : une correspondance est trouvée lorsque la taille des critères indiqués est supérieure ou égale à la taille de clé spécifiée.
 - **Est au plus** : une correspondance est trouvée lorsque la taille des critères indiqués est inférieure ou égale à la taille de clé spécifiée.
 - **Ce jour ou avant** : une correspondance est trouvée lorsque la date indiquée est identique ou antérieure à la date affichée.
 - **Ce jour ou après** : une correspondance est trouvée lorsque la date indiquée est identique ou ultérieure à la date affichée.
- 8** Dans le champ associé à certains éléments correspondants, vous pouvez saisir du texte (adresse électronique ou domaine; par exemple ; les caractères génériques sont autorisés), des nombres ou des dates.
- 9** Pour ajouter des lignes de correspondance ou d'exclusion, cliquez sur le signe plus. Cliquez sur le signe moins pour supprimer des lignes.
- 10** Cliquez sur **Enregistrer**. Le trousseau de clés intelligent s'affiche dans la liste d'éléments.

Lorsque vous sélectionnez ce trousseau, seules les clés correspondant aux critères spécifiés s'affichent. Par exemple, le trousseau de clés ci-dessous correspond aux clés publiques des utilisateurs de PGP Desktop au cabinet d'avocats de votre entreprise.

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** Ouvrez PGP Desktop.
- 2** Dans le menu **Fichier**, sélectionnez **Nouveau > Clé PGP**. La boîte de dialogue Créez une clé pour sécuriser vos communications s'affiche. Les informations sur cette boîte de dialogue indiquent la définition et le mode d'utilisation d'une paire de clés.
- 3** Pour définir des propriétés avancées pour la nouvelle clé, cochez la case Mode Expert. Pour plus d'informations sur ces paramètres, reportez-vous à la section *Paramètres de clé - Mode Expert* (cf. "Paramètres de clé - Mode Expert" à la page 50). Ignorez cette étape si vous ne voulez pas utiliser le Mode Expert.
- 4** Cliquez sur **Continuer**. La boîte de dialogue Définissez les informations de contact de votre clé s'affiche.
- 5** Saisissez votre vrai nom dans le champ **Nom complet** et votre adresse de courrier électronique correcte dans le champ **Adresse de courrier électronique**.

Remarque : il n'est pas indispensable 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.

- 6** Cliquez sur **Continuer**. La boîte de dialogue Définissez la phrase secrète de votre clé s'affiche.
- 7** Saisissez une phrase secrète pour la clé que vous êtes en train de créer, puis tapez-la de nouveau pour la confirmer.

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 regarde, vous pouvez afficher les caractères saisis pour la phrase secrète en cliquant sur **Afficher les frappes**.

Attention : veuillez à indiquer une phrase secrète dont vous vous souviendrez sans avoir à l'écrire. 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.

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 214).

- 8 Pour enregistrer cette phrase secrète dans la chaîne de clé Mac OS X, cochez cette case.
- 9 Cliquez sur **Continuer**. La boîte de dialogue Récapitulatif de la création de clé PGP s'affiche.
- 10 Si nécessaire, procédez comme suit :
 - Pour afficher les détails sur la clé, sélectionnez **Afficher les détails**.
 - Pour modifier votre clé, cliquez sur **Retour**.
- 11 Cliquez sur **Créer une clé**. PGP Desktop génère votre nouvelle paire de clés. Ce processus peut durer plusieurs minutes.
- 12 À l'issue du processus de génération de clé, cliquez sur **Terminer**.

Paramètres de clé - Mode Expert

- 1 Lorsque vous sélectionnez **Mode Expert** dans la boîte de dialogue Nouvelle clé PGP, indiquez votre nom et votre adresse de courrier électronique ainsi que les informations suivantes :
 - **Type de clé** : choisissez entre **Diffie-Hellman/DSS** et **RSA**.

Remarque : à compter de PGP Desktop 9.0, l'ancien format de clés RSA héritées datant des années 1990 n'est plus pris en charge. Vous ne pouvez pas créer de **nouvelles** paires de clés PGP avec le format de clés RSA héritées. Les paires de clés **existantes** continuent cependant à être prises en charge dans PGP Desktop.

- **Serveur de clés** : indiquez un serveur de clés approuvé ou choisissez **<Aucun>**.
- **Compression autorisée** : désélectionnez tout type de compression que la paire de clés en cours de création ne doit pas prendre en charge.
- **Chiffrements autorisés** : désélectionnez tout chiffrement que la clé en cours de création ne doit pas prendre en charge.

- **Hachages autorisés** : désélectionnez tout hachage que la paire de clés en cours de création ne doit pas prendre en charge.
 - **Chiffrement par défaut** : sélectionnez le chiffrement à utiliser quand aucun n'est spécifié. Seul un chiffrement autorisé peut être sélectionné comme chiffrement par défaut.
 - **Hachage par défaut** : sélectionnez le hachage à utiliser quand aucun n'est spécifié. Seul un hachage autorisé peut être sélectionné comme hachage par défaut.
 - **Taille de clé** : saisissez de 1 024 bits à 4 096 bits. Plus la clé est grande, plus elle est sécurisée, mais plus il faudra de temps pour la générer.
 - **La clé expire** : sélectionnez **Jamais** ou spécifiez la date d'expiration de la clé en cours de création.
- 2 Cliquez sur **Continuer**. La boîte de dialogue Définissez la phrase secrète de votre clé s'affiche.
 - 3 Entrez la phrase secrète à utiliser avec cette clé, puis saisissez-la à nouveau dans le champ **Confirmez votre phrase secrète**. Il est important de préserver la confidentialité de cette phrase secrète.
 - 4 Cliquez sur **Continuer**.
 - 5 Vérifiez les informations fournies, puis cliquez sur **Créer une clé** pour lancer le processus de génération de clé. PGP Desktop génère votre nouvelle paire de clés.
Ce processus peut durer plusieurs minutes.
 - 6 Quand le processus de génération de clé est terminé, cliquez sur **Suivant**. Vous êtes invité à ajouter à PGP Global Directory la partie de clé publique de la clé créée.
 - 7 Lisez les informations affichées, puis cliquez sur **Suivant**.
 - 8 Cliquez sur **Ignorer** pour empêcher que la clé publique soit publiée dans PGP Global Directory. L'écran Fin de l'assistant du PGP Global Directory s'affiche.
 - 9 Cliquez sur **Terminer**. Votre nouvelle paire de clés PGP a été générée. Normalement, elle est visible dans la zone de travail des clés PGP. Si elle n'apparaît pas dans la liste, assurez-vous que l'option **Toutes les clés** ou **Mes clés privées** est sélectionnée dans l'option Clés PGP.

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 53).
- 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 66, à la page 67).

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 les 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 l'option Trousseaux de clés intelligents, cliquez sur **Mes clés privées**.
- 2 Cliquez sur l'icône qui représente votre paire de clés.
- 3 Dans le menu **Fichier**, sélectionnez **Exporter**.
- 4 Dans le champ **Enregistrer sous**, saisissez le nom du fichier et indiquez son emplacement dans le champ prévu à cet effet.
- 5 Cochez la case **Inclure la ou les clés privées**. Ceci est important : si vous ne le faites pas, seule votre clé *publique* sera exportée.
- 6 Cliquez sur **Enregistrer**.
- 7 Copiez le fichier dans un emplacement sécurisé. Ce peut être un CD que vous archivez soigneusement, un autre ordinateur personnel ou une clé 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 est SKM, vous ne pourrez 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 123).

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 85, "Perte de votre clé ou phrase secrète" à la page 85) 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 54).
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 56).
- *Export de votre clé publique ou copie dans un fichier texte* (cf. "Exportation de votre clé publique dans un fichier" à la page 56).

Sur les systèmes Windows, vous pouvez aussi :

- Copier directement d'une carte à puce vers le trousseau de clés de quelqu'un.

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'autres 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 Maintenez la touche Ctrl enfoncée et cliquez sur la paire de clés dont vous voulez envoyer la clé publique au serveur de clés.
- 3 Sélectionnez **Envoyer la clé au serveur**, puis choisissez dans la liste le serveur de clés auquel vous voulez envoyer la clé publique. Si le serveur de clés souhaité ne figure pas dans la liste, reportez-vous à la section *Utilisation des serveurs de clés* (à la page 59).

Dès que vous placez une copie de votre clé publique sur un serveur de clés, elle 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 en recherchant sur le serveur de clés votre nom ou 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 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 Ouvrez PGP Desktop.
- 2 Ouvrez votre client de messagerie, créez un message et adressez-le à la personne à laquelle vous souhaitez envoyer votre clé publique.
- 3 Dans PGP Desktop, faites glisser votre paire de clés dans le corps du message.
- 4 Envoyez le message.

Si cette méthode ne fonctionne pas, ouvrez PGP Desktop, sélectionnez votre paire de clés, puis **Édition > Copier**. Ouvrez un message électronique, puis collez 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.

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.
- 2 Cliquez sur l'option PGP Global Directory ou sur l'option d'un autre serveur de clés. L'écran Rechercher des clés s'affiche dans la zone de travail.
- 3 Indiquez vos critères de recherche, puis cliquez sur **Rechercher**.
 - Si le serveur de clés souhaité ne figure pas dans la liste, dans le menu **Clés**, sélectionnez **Ajouter un serveur de clés**, puis configurez ce dernier.
 - Vous pouvez rechercher des clés dans un serveur de clés en spécifiant des valeurs pour plusieurs caractéristiques de clé. Vous pouvez également rechercher des exclusions, et notamment 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, tout en maintenant la touche Ctrl enfoncée, cliquez dessus et sélectionnez **Ajouter au trousseau de clés par défaut**. 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.
- **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.

Le serveur PGP Global Directory est un serveur de clés d'accès gratuit et public, hébergé par PGP Corporation. Il offre un accès rapide et simple à l'univers 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 sorte 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.

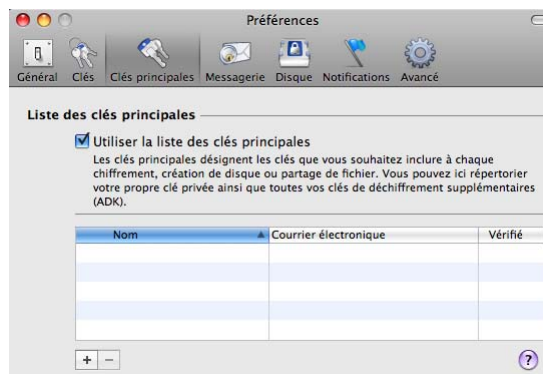
Pour PGP Desktop, PGP Global Directory est un serveur de clés approuvé ; PGP Desktop approuve automatiquement toute clé qu'il y trouve. Pendant la connexion initiale à PGP Global Directory, la clé de vérification de PGP Global Directory est téléchargée, signée et approuvée par la clé que vous publiez dans l'annuaire. Toutes les clés vérifiées par PGP Global Directory sont ainsi considérées comme valides par votre 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 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 *Préférences de clés* (à la page 202).

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 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.

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 Ouvrez PGP Desktop.
- 2 Sélectionnez **PGP > Préférences**.
- 3 Cliquez sur l'onglet l'icône **Clés principales**.
- 4 Cliquez sur l'icône de signe plus située sous la liste de clés. La boîte de dialogue Sélectionner des clés principales s'affiche.
- 5 Dans la liste **Nom** à gauche, cliquez pour sélectionner les clés à utiliser. Pour sélectionner plusieurs clés, cliquez sur leur nom tout en maintenant la touche Maj ou Cmd enfoncée.
- 6 Une fois que vous avez sélectionné les clés de votre choix, 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 Ouvrez PGP Desktop.
- 2 Sélectionnez **PGP > Préférences**.
- 3 Cliquez sur l'onglet l'icône **Clés principales**.
- 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 Cmd enfoncée.
- 5 Cliquez sur l'icône de signe moins située sous la liste de clés. La ou les clés sont supprimées.

7

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	63
Ajout et suppression de photographies	64
Gestion des noms d'utilisateur et des adresses de courrier électronique d'une clé.....	65
Modification de votre phrase secrète	66
Suppression de clés, d'ID d'utilisateur et de signatures	67
Désactivation et activation des clés publiques	68
Vérification d'une clé publique	69
Signature d'une clé publique	70
Attribution de confiance pour les validations de clés	72
Utilisation des sous-clés	73
Utilisation des clés de déchiffrement supplémentaire (ADK)	78
Utilisation des révocateurs.....	80
Scission et réassemblage de clé	82
Perte de votre clé ou phrase secrète.....	85
Protection de vos clés.....	89

Examen et paramétrage des propriétés de la clé

La boîte de dialogue Infos sur la clé affiche toutes les informations nécessaires sur une 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

Remarque : si votre ordinateur se trouve dans un environnement géré par un PGP Universal Server et que votre mode clé est SKM, vous ne pourrez 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 123).

► **Pour afficher les propriétés d'une clé**

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément 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.

Ajout et suppression de photographies

Vous pouvez ajouter une photographie à vos clés Diffie-Hellman/DSS et RSA.

Remarque : lorsque vous ajoutez ou modifiez des informations sur la clé, veillez à les mettre à jour sur le serveur de clés pour que la clé la plus récente soit toujours disponible.

Attention : bien que, pour vérification, vous puissiez consulter la photographie qui accompagne la clé de quelqu'un, l'empreinte digitale doit toujours prévaloir. Vérifiez-la toujours et comparez-la.

► **Pour ajouter votre photographie à la clé**

- 1 Ouvrez PGP Desktop, puis cliquez sur l'option **Mes clés privées**.

- 2 Double-cliquez sur la clé privée à laquelle vous ajoutez la photo. La boîte de dialogue Infos sur la clé de la clé choisie s'affiche.
- 3 Cliquez sur le signe plus situé sous la photo associée à la clé. La boîte de dialogue Ajouter une photo s'affiche.
- 4 Déplacez la photo dans la zone vide de cette boîte de dialogue par glisser-déposer ou par simple coller.

Remarque : la photographie peut être un fichier JPG ou BMP ou provenir du Presse-papiers. Pour une meilleure qualité d'image, rognez l'image à 120 x 144 pixels avant de l'ajouter. Si vous ne procédez pas ainsi, PGP Desktop la met à l'échelle à votre place.

- 5 Cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche si la phrase secrète de la clé en cours de modification n'est pas en mémoire cache.
- 6 Saisissez la phrase secrète de la clé que vous modifiez, puis cliquez sur **OK**. Votre ID photo est ajouté à votre clé privée.

► **Pour voir un agrandissement de la photo**

- Sous la photo existante, cliquez sur l'icône de loupe. Une fenêtre affichant une version agrandie de l'ID photo s'affiche. Pour supprimer l'agrandissement, cliquez à l'intérieur de la fenêtre.

► **Pour supprimer un ID photo**

- 1 Sous la photo existante, cliquez sur le signe moins. Une boîte de dialogue de confirmation apparaît.
- 2 Confirmez votre choix. 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/une nouvelle adresse à votre paire de clés**

- 1 Ouvrez PGP Desktop, puis double-cliquez sur la clé appropriée. La boîte de dialogue Infos sur la clé associée à la clé choisie s'affiche.
- 2 Cliquez sur **Ajouter une adresse de courrier électronique**. La boîte de dialogue **Ajouter un nom s'affiche**.
- 3 Saisissez les nouvelles informations dans les champs **Nom complet** et **Adresse de courrier électronique**, puis cliquez sur **OK**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche si la phrase secrète de la clé en cours de modification n'est pas en mémoire cache.
- 4 Saisissez la phrase secrète de clé privée de la clé que vous êtes en train de modifier, puis cliquez sur **OK**. Le nouveau nom est ajouté à la fin de la liste des noms d'utilisateurs associée à la clé.

Remarque : lorsque vous ajoutez ou modifiez des informations sur la paire de clés, veillez à les mettre également à jour sur le serveur de clés pour que la clé la plus récente soit toujours disponible.

► **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.

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 123).

► Pour changer votre phrase secrète de clé privée

- 1 Ouvrez PGP Desktop, puis double-cliquez sur la clé appropriée. La boîte de dialogue Infos sur la clé de la clé choisie s'affiche.
- 2 Cliquez sur **Modifier la phrase secrète**, puis sélectionnez à nouveau cette option dans la liste des commandes affichées. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
- 3 Saisissez la phrase secrète *actuelle* de la clé privée, puis cliquez sur **OK**. La boîte de dialogue Confirmer la phrase secrète PGP s'affiche.
- 4 Indiquez votre nouvelle phrase secrète dans le premier champ de texte.
- 5 Saisissez-la une deuxième fois dans le champ **Confirmation**.

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 214).
- 6 Cliquez sur **OK**. La boîte de dialogue d'informations qui s'affiche vous signale la modification de la phrase secrète.
- 7 Cliquez sur **OK**. La phrase secrète est modifiée.

Attention : si vous modifiez votre phrase secrète parce que vous pensez que sa confidentialité est compromise, il est recommandé de décomposer tous les trousseaux de clés de sauvegarde, puis de générer une copie de sauvegarde de la clé avec la nouvelle phrase secrète.

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 de votre trousseau de clés PGP

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément **Clés**. Toutes les clés de votre trousseau s'affichent.
- 2 Effectuez l'une des opérations ci-dessous :
 - Pour supprimer une clé, sélectionnez-la, choisissez **Modifier > Effacer** et, dans la boîte de dialogue de confirmation, cliquez sur **OK**. La clé est supprimée de votre trousseau.
 - Pour supprimer un ID utilisateur (d'une clé publique) ou une signature, cliquez sur le triangle situé à gauche de la clé associée à l'ID utilisateur ou à la signature à supprimer ; les ID utilisateur et signatures sont alors affichés. Localisez l'ID d'utilisateur ou la signature que vous voulez supprimer, cliquez dessus, sélectionnez **Modifier > Effacer**, puis cliquez sur **OK** dans la boîte de dialogue de confirmation. L'ID d'utilisateur ou la signature est supprimé.

Il est important de noter que vous ne pouvez pas supprimer un ID utilisateur d'une paire de clés.

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 voulez pas qu'elle encombre la liste de vos destinataires à chaque fois que vous envoyez un courrier électronique.

Vous ne pouvez pas désactiver vos paires de clés.

► Pour désactiver une clé publique

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément **Clés**. Toutes les clés de votre trousseau s'affichent.
- 2 Double-cliquez sur la clé publique à désactiver. La boîte de dialogue Infos sur la clé associée à 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 à des fins de chiffrement, de signature, de déchiffrement ou de vérification.

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 (ou appuyez sur Ctrl et cliquez) 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 digitale d'une clé publique

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément Clés. Toutes les clés de votre trousseau s'affichent.
- 2 Double-cliquez sur la clé publique dont vous voulez vérifier l'empreinte digitale. La boîte de dialogue Infos sur la clé s'affiche.

- 3 Localisez l'option **Empreinte digitale** dans la seconde section de la boîte de dialogue Infos sur la clé.

Si nécessaire, cliquez sur le triangle vers le bas pour afficher l'empreinte digitale, laquelle est présentée au format hexadécimal (10 ensembles de quatre caractères) ou sous la forme d'une liste de mots (quatre colonnes de cinq mots uniques).

- 4 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, la clé est vraisemblablement fausse.

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.

- 5 Si vous possédez une clé contrefaite, supprimez-la.
- 6 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, cette paire de clés doit 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 une clé

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément **Clés**. Toutes les clés de votre trousseau s'affichent.
- 2 Sélectionnez la clé à signer, puis dans le menu **Clés**, sélectionnez **Signer**. La boîte de dialogue Clé de signature s'affiche. Elle contient une zone de texte avec le nom d'utilisateur/l'adresse de courrier électronique, ainsi que l'empreinte hexadécimale.

Conseil : vous pouvez aussi cliquer sur la clé tout en maintenant la touche Ctrl enfoncée (ou cliquer avec le bouton droit si votre souris possède deux boutons). Dans le menu contextuel qui s'affiche, sélectionnez **Signer**.

- 3** Dans le menu **Signer avec la clé**, cliquez pour afficher et sélectionner la clé avec laquelle vous souhaitez signer.

- 4** Pour autoriser l'exportation de votre signature avec cette clé, sélectionnez **Autoriser l'exportation de la signature**.

Une signature exportable est une signature qui peut être envoyée à des serveurs et qui se déplace avec la clé à chaque exportation. La case à cocher indique que vous approuvez l'exportation de la clé.

- 5** Dans la zone **Sélectionner les éléments à signer**, vérifiez que vous signez bien la clé adéquate.

- 6** Si vous souhaitez configurer d'autres options, comme le type et l'expiration de la signature, cliquez sur **Options**.

- 7** Sélectionnez 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.

- 8** Dans le champ **Expire, sélectionnez Jamais** si vous ne voulez pas que la signature expire. Dans le cas contraire, sélectionnez une date d'expiration.

- 9** Dans le champ **Avancé**, indiquez le niveau de confiance maximal et une restriction de domaine :

- 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'introductions en dessous de la clé du méta-introducteur.
 - 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**.
- 10** Cliquez sur **Signer**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche (si votre phrase secrète n'est pas enregistrée dans la chaîne de clé).
 - 11** Si nécessaire, entrez la phrase secrète de la clé de signature. Vous n'avez pas besoin d'entrer votre phrase secrète si elle est en cache.
 - 12** 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, puis cliquez sur l'élément **Clés**. Toutes les clés de votre trousseau s'affichent.
- 2** Cliquez sur le triangle à gauche de la clé à partir de laquelle vous voulez révoquer votre signature. Les signatures apparaissent.
- 3** Cliquez sur votre clé de signature.
- 4** Sélectionnez **Modifier > Révoquer**. Une boîte de dialogue de confirmation apparaît.
- 5** 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.
- 6** Saisissez votre phrase secrète, puis cliquez sur **OK**. Votre signature est révoquée à partir de la clé.

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

► Pour accorder de la confiance à une clé

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément Clés. 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 Infos sur la clé s'affiche.
- 3 Dans la section **Informations générales**, cliquez sur le paramètre de champ **Confiance** actuel. Le menu des paramètres de confiance s'affiche.
- 4 Sélectionnez le paramètre souhaité.

Remarque : la sélection du paramètre de confiance **Aucun** ou **Marginal** ne signifie pas que le propriétaire d'une clé n'est pas digne de confiance ou qu'il est malhonnête. Cela signifie simplement que *vous ne disposez pas de suffisamment d'informations* pour vous assurer que le propriétaire ou la source de la clé est authentique.

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.

Clé	Description
	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 sur les sous-clés de vos paires de clés. Toutefois, seules les informations sur les sous-clés des clés publiques peuvent être consultées.

► **Pour déterminer les sous-clés incluses dans une clé**

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément 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.
- 3 Cliquez sur le triangle à gauche de **Sous-clés**. Les informations sur les sous-clés de la clé apparaissent.

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 15).

► **Pour créer de nouvelles sous-clés pour une paire de clés**

- 1 Dans la section **Sous-clés** de la boîte de dialogue Propriétés de la clé, cliquez sur le signe plus. 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 la clé**, saisissez une taille de clé comprise entre 1 024 et 4 096 bits.
- 4 Dans le champ **Date de début**, saisissez la date d'entrée en vigueur de la sous-clé que vous créez.
- 5 Dans le champ **Date d'expiration**, sélectionnez **Jamais** ou indiquez une date. Ces informations définissent la date d'expiration de la sous-clé.

Remarque : pour éviter toute confusion lors de la mise à jour de plusieurs sous-clés de votre paire de clés, veillez à ne pas faire chevaucher les dates de début et d'expiration de vos sous-clés.

- 6 Cliquez sur **Créer**. La boîte de dialogue Phrase secrète s'affiche.
- 7 Saisissez votre phrase secrète, puis cliquez sur **OK**. La sous-clé est alors créée.

Remarque : lorsque vous ajoutez ou modifiez des informations de la paire de clés, veillez à les mettre également à jour sur le serveur de clés pour que la clé la plus récente soit toujours disponible. Une fois la clé sélectionnée dans la liste Clés, dans le menu **Clés**, sélectionnez **Mettre à jour la sélection**.

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 voulez 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 est 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 123).

► Pour spécifier l'utilisation d'une clé

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément Clés. Toutes les clés de votre trousseau s'affichent.
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.
- 2 Dans celle-ci, cliquez sur l'en-tête **Sous-clés**. Les sous-clés de cette clé s'affichent.
- 3 Double-cliquez sur la sous-clé que vous voulez modifier.
- 4 Cliquez sur la flèche située en regard de **Modifier les propriétés d'utilisation de la clé**. Les propriétés d'utilisation de la clé s'affichent.
- 5 Dans la liste affichée, 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** pour enregistrer les propriétés de la sous-clé.
- 7 Cliquez de nouveau sur **Fermer** pour enregistrer les propriétés de la clé.

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.
- 2 Cliquez sur **Révoquer** (icône d'un cercle barré au-dessus de la liste des sous-clés). Une boîte de dialogue de confirmation apparaît.

- 3 Cliquez sur **OK** pour révoquer la sous-clé. La boîte de dialogue Phrase secrète s'affiche.
- 4 Saisissez votre phrase secrète, puis cliquez sur **OK**. La sous-clé est alors révoquée et l'icône est modifiée. Elle représente désormais une clé avec un cercle rouge barré.

Suppression de sous-clés

► Pour supprimer une sous-clé

- 1 Dans la section **Sous-clés** de la boîte de dialogue Propriétés de la clé, sélectionnez la sous-clé à supprimer.
- 2 Cliquez sur **Supprimer** (signe moins au-dessus de la liste des sous-clés). Une boîte de dialogue de confirmation apparaît.
- 3 Cliquez sur **OK** pour supprimer la sous-clé. 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) à une paire de clés

- 1** Ouvrez PGP Desktop, puis cliquez sur l'élément Clés. Toutes les clés de votre trousseau s'affichent.
- 2** Double-cliquez sur la paire de clés à laquelle vous ajoutez la clé de déchiffrement supplémentaire (ADK). La boîte de dialogue Infos sur la clé associée à la clé choisie s'affiche.
- 3** S'il y a lieu, cliquez sur l'icône en forme de triangle située à gauche de la section **Clés de déchiffrement supplémentaires** afin qu'elle ne pointe plus vers le bas. Les informations de clé de déchiffrement supplémentaire (ADK) associées à cette clé s'affichent, si elle ont été configurées.
- 4** Cliquez sur le signe plus à droite de la section **Clés de déchiffrement supplémentaires**.
- 5** Dans la liste qui s'affiche, sélectionnez la clé à utiliser en tant que clé de déchiffrement supplémentaire.
- 6** Cliquez sur **OK**. 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**. La clé est alors ajoutée.

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, puis cliquez sur l'option **Mes clés privées** sous l'élément Clés. Toutes les clés de votre trousseau s'affichent.
- 2 Double-cliquez sur la clé à laquelle vous ajoutez un révocateur. La boîte de dialogue Infos sur la clé associée à la clé choisie s'affiche.
- 3 Cliquez sur le signe plus à droite de la section **Révocateurs**. La boîte de dialogue Sélectionner une ou des clés s'affiche.

- 4 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.
- 5 Cliquez sur **Oui** pour continuer ou sur **Non** pour annuler. La boîte de dialogue Saisissez la phrase secrète de la clé PGP s'affiche.
- 6 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.
- 7 Cliquez sur **OK**. La ou les clés sélectionnées sont dorénavant autorisées à révoquer votre clé. Pour une gestion efficace des clés, distribuez une copie à jour de votre clé aux révocateurs ou téléchargez votre clé sur le serveur de clés.

Révocation d'une clé

S'il vous arrive de ne plus avoir confiance en votre paire de clés personnelle, vous pouvez révoquer votre clé et indiquer ainsi 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, puis cliquez sur l'option **Mes clés privées** sous l'élément Clés. Toutes les clés de votre trousseau s'affichent.
- 2 Maintenez le bouton Ctrl enfoncé et cliquez sur la clé à révoquer (ou cliquez avec le bouton droit si vous disposez d'une souris à deux boutons).
- 3 Dans le menu contextuel, sélectionnez **Révoquer**. La boîte de dialogue Confirmer la révocation vous invite à confirmer la révocation de la clé.
- 4 Cliquez sur **OK** pour confirmer que vous souhaitez révoquer la clé sélectionnée ou sur **Annuler** pour annuler l'opération.
- 5 Saisissez la phrase secrète de la paire de clés que vous révoquez, puis cliquez sur **OK**. Quand vous révoquez une clé, elle apparaît marquée d'une croix rouge (X) pour indiquer qu'elle n'est plus valide.
- 6 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

- 1 Ouvrez PGP Desktop, puis cliquez sur l'élément Clés PGP. Toutes les clés de votre trousseau 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 Scinder la clé s'affiche.
- 4 Ajoutez des actionnaires pour la clé scindée en glissant et déplaçant leurs clés dans la liste **Nom d'utilisateur/clé**.
- 5 Si vous voulez ajouter un actionnaire ne possédant pas de clé publique, *cette personne doit être physiquement présente pour saisir sa propre phrase secrète*. Cliquez sur **Ajouter**.
 - Demandez à l'actionnaire de taper deux fois sa phrase secrète et cliquez sur **OK**. La liste affiche alors un utilisateur sans nom.
 - Double-cliquez sur cet utilisateur, puis entrez un nom descriptif de personne ou de l'organisation qui détient les parts.
- 6 Pour indiquer l'emplacement des parts scindées, cliquez sur **Parcourir** dans le dossier de destination du fichier de partage, puis sélectionnez l'emplacement choisi.
- 7 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 d'un actionnaire, double-cliquez sur la valeur dans la colonne Parts et entrez le nombre de parts qu'il contrôle.

- 8 Cliquez sur **Scinder la clé**. La boîte de dialogue de confirmation de scission de la clé s'affiche.
- 9 Cliquez sur **OK** pour continuer à scinder la clé. L'écran Phrase secrète s'affiche.
- 10 Saisissez la phrase secrète de la clé, puis cliquez sur **OK**. La phrase secrète doit comporter au minimum six caractères. Une boîte de dialogue de confirmation s'affiche.

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 de l'extension `.shf`.

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

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 sur 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** Sur l'ordinateur de réassemblage, utilisez le Finder pour sélectionner le ou les fichiers à signer ou déchiffrer à l'aide de la clé scindée.

- 3** Maintenez la touche Ctrl enfoncée et cliquez sur le ou les fichiers, puis 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.

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

- 5** 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, un lecteur amovible ou un lecteur monté. Passez à l'étape suivante.
- Si vous collectez les parts de clé sur le réseau, cliquez sur **Démarrer le réseau**.

La boîte de dialogue Phrase secrète s'ouvre. 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, l'écran 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.

- 6 Cliquez sur **Confirmer** pour accepter le fichier de partage.
- 7 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.
- 8 Cliquez sur **OK**. Le fichier est signé ou déchiffré à l'aide de la clé 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 86).

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 réinitialisez votre clé.

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 l'élément Clés et sélectionnez votre clé.

- 2 Sélectionnez **Clés > Créer Mes questions PGP**. L'assistant des questions de sécurité de PGP apparaît.
- 3 Quand la boîte de dialogue de l'écran Reconstruction de clé s'affiche, saisissez cinq questions dont vous seul connaissez la réponse dans les champs Question (les questions par défaut ne sont que des exemples).



- 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.
- 9 Une fois que vous avez entré les cinq questions et réponses, la boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
- 10 Tapez la phrase secrète de votre clé, puis cliquez sur **OK**.
- 11 Vous êtes alors invité à enregistrer le fichier de reconstruction de clé. Saisissez le nom du fichier et l'emplacement où vous souhaitez l'enregistrer, puis cliquez sur **Enregistrer**.
- 12 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.

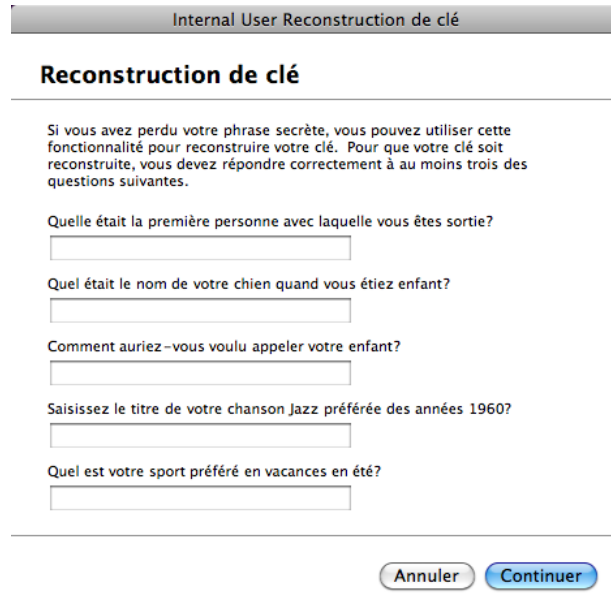
Reconstruction de votre clé en cas de perte de celle-ci ou de la phrase secrète

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 86).

► Pour reconstruire votre clé

- 1 Dans PGP Desktop, cliquez sur l'élément Clés et sélectionnez votre clé.
- 2 Sélectionnez **Clés > Reconstruire**.
 - Si votre ordinateur se trouve dans un environnement géré par un PGP Universal Server, la boîte de dialogue Répondre aux questions de sécurité de l'Assistant de phrase secrète PGP s'affiche.
 - Si votre environnement est autonome, la boîte de dialogue de sélection du fichier de reconstruction de clé s'affiche. Sélectionnez le fichier .krb que vous avez enregistré lors de la création de vos questions de sécurité et cliquez sur **Ouvrir**.

La boîte de dialogue Reconstruction de clé s'affiche.



- 3 Répondez correctement à trois des cinq questions de sécurité et cliquez sur **Continuer**. La boîte de dialogue Confirmer la phrase secrète PGP s'affiche.

- 4 Saisissez, puis confirmez votre nouvelle 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 214).

- 5 Cliquez sur **OK**. 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.

8

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	91
Utilisation de la stratégie hors connexion	94
Services et stratégies	95
Création d'une stratégie de sécurité	104
Utilisation de la liste des stratégies de sécurité	115
PGP Desktop et SSL	121
Modes clé	123
Affichage du journal de PGP	126
Utilisation de scripts PGP avec Entourage 2008	127

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 104).

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.

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).

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 96).

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 34).

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 104).

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.

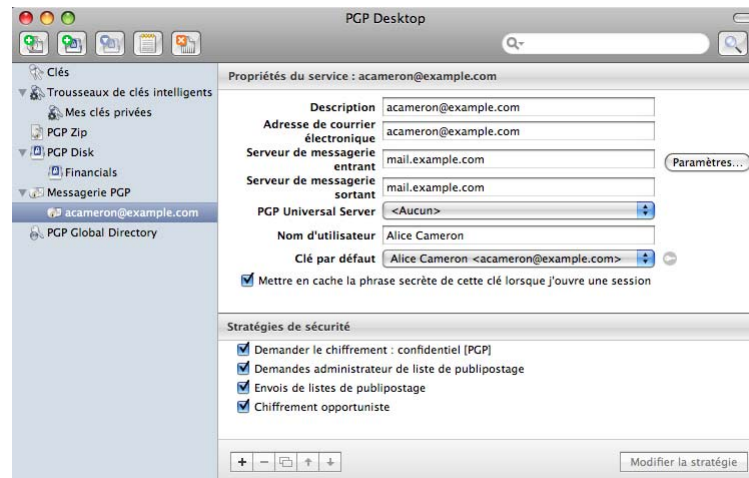
Remarque : Vous pouvez modifier les stratégies par défaut, mais vous ne pouvez pas les supprimer. Vous pouvez également les désactiver et en changer l'ordre dans la liste des stratégies.

Affichage des services et stratégies

► Pour afficher les services et stratégies

- 1 Ouvrez PGP Desktop et cliquez sur l'élément Messagerie PGP.
- 2 Cliquez sur le nom du service dont vous voulez afficher les propriétés de compte. Les paramètres du service sélectionné s'affichent dans la zone de travail de la messagerie PGP.

- 3 Pour afficher les détails d'une stratégie, sous **Stratégies de sécurité**, cliquez sur le nom de la stratégie à afficher et cliquez sur **Afficher la stratégie**. Les paramètres de la stratégie s'affichent. 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 un environnement géré par un PGP Universal Server, vous avez peut-être la possibilité de remplacer les stratégies du serveur par des stratégies locales. Si la stratégie le spécifie, vos stratégies locales peuvent être appliquées en cas d'indisponibilité de votre PGP Universal Server, quelle qu'en soit la raison.

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 l'élément Messagerie PGP. L'écran Messagerie PGP s'affiche.

- 2 Cliquez sur **Créer un service**. Vous pouvez également sélectionner l'option **Nouveau service** dans le menu **Messagerie**. L'écran Nouveau service apparaît. Dans la section **Propriétés du service** figurent les paramètres par défaut et, dans la section Stratégies de sécurité, les stratégies de sécurité par défaut.
- 3 Dans le champ **Description**, entrez un nom descriptif pour le service. (Cette opération est facultative, mais peut se révéler utile si vous devez gérer plusieurs services.)
- 4 Dans le champ **Adresse de courrier électronique**, saisissez l'adresse de courrier électronique associée au service (par exemple, mgrangier@exemple.com).
- 5 Tapez le nom de vos serveurs de messagerie électronique entrant et sortant ou cliquez sur **Paramètres du serveur** pour définir des options avancées.
- 6 Si vous décidez de définir des options avancées, la boîte de dialogue Paramètres du serveur s'affiche.

Indiquez les paramètres appropriés :

- **Type de serveur** : sélectionnez le type de serveur qui sera utilisé par le nouveau service :

PGP Universal Server, pour les utilisateurs de PGP Desktop dont l'ordinateur se trouve dans un environnement géré par un PGP Universal Server. Pour plus de détails sur les paramètres à définir, contactez votre administrateur PGP. Si vous utilisez PGP Desktop au sein d'un environnement géré par un PGP Universal Server, les paramètres corrects ont été automatiquement téléchargés dans la boîte de dialogue Paramètres du serveur.

Messagerie sur Internet, pour les utilisateurs de PGP Desktop autonomes disposant d'une connexion de messagerie POP ou IMAP.

- **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. Avec le paramètre **Automatique**, aussi bien les connexions POP qu'IMAP sont détectées automatiquement.
- **Port** : conservez la valeur par défaut **Automatique** ou indiquez le port du serveur de messagerie entrant auquel se connecter pour récupérer les messages (dans le cas où vous avez sélectionné le paramètre **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 :

- **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 l'application. (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 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 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.**

- **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 disponible pour le serveur de messagerie sortant uniquement 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 :

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 l'application. (Cette option est sélectionnée par défaut.)

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 221).

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 l'élément **Messagerie PGP**.
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.
- 2 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 97).

Désactivation ou activation d'un service

Si vous ne souhaitez plus utiliser un service, mais préférez tout de même le conserver, car vous pourriez en avoir à nouveau besoin, vous avez la possibilité de le désactiver. Cela s'avère particulièrement utile si vous voulez 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* (cf. "Suppression d'un service" à la page 101).

► Pour activer ou désactiver un service

- 1 Sous l'élément Messagerie PGP, sélectionnez le nom du service à désactiver. Les paramètres de ce service s'affichent. Confirmez que vous avez bien sélectionné le bon service.
- 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.

Conseil : vous pouvez aussi appuyer sur la touche Ctrl et, tout en la maintenant enfoncée, cliquer sur le nom du service (ou cliquer dessus avec le bouton droit si vous utilisez une souris à deux boutons), puis, dans le menu contextuel, sélectionner l'option permettant d'activer ou de désactiver le service.

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 Sous l'élément Messagerie PGP, sélectionnez le nom du service à activer. Les paramètres de ce service s'affichent. Confirmez que vous avez bien sélectionné le bon service.
- 2 Tout en maintenant la touche Ctrl enfoncée, cliquez sur le nom du service (ou cliquez dessus avec le bouton droit si vous utilisez une souris à deux boutons) et sélectionnez **Supprimer l'élément** dans le menu contextuel. Le service est supprimé.

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*.exemple.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 envoie 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 101).
- Supprimez le service de messagerie PGP qui pose problème et envoyez/recevez des messages électroniques. PGP Desktop régénérera 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

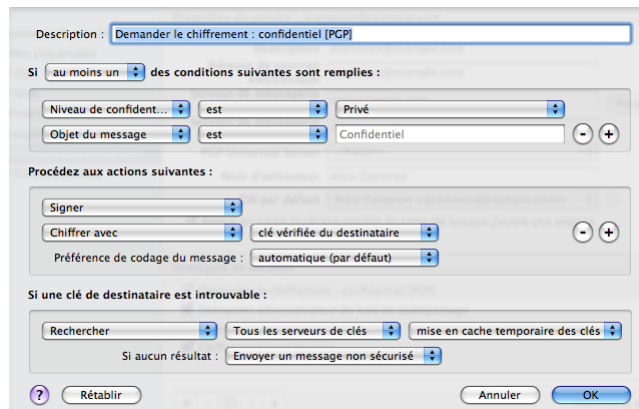
Les stratégies de sécurité permettent de contrôler la manière dont PGP Desktop gère les messages électroniques sortants.

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 l'élément 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, sont affichés.

- 2 Cliquez sur le signe plus situé au bas de l'écran. La boîte de dialogue Règle de messagerie sans titre 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.
- **finir par** : la condition est remplie lorsque le texte du premier champ de condition *finir 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}

Données	Exemple	Expression normale
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]{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 souhaitez 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.

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.

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.

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.

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 104)), 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 l'élément Messagerie PGP. L'écran Messagerie PGP s'affiche.
- 2 Cliquez sur le nom du service rattaché à la stratégie de sécurité à modifier. Les propriétés dudit service apparaissent.
- 3 Sélectionnez la stratégie de sécurité que vous souhaitez modifier, puis cliquez sur **Afficher la stratégie**. La boîte de dialogue Stratégie de message s'ouvre, présentant les paramètres de la stratégie sélectionnée.

Vous pouvez consulter, modifier et désactiver les stratégies par défaut, mais vous ne pouvez pas les supprimer.
- 4 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 104).
- 5 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.

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 l'élément Messagerie PGP. L'écran Messagerie PGP s'affiche.

- 2 Cliquez sur le nom du service rattaché à la stratégie de sécurité à modifier. Les propriétés dudit service apparaissent.
- 3 Sélectionnez la stratégie de liste de publipostage à modifier, puis cliquez sur **Afficher la stratégie**. La boîte de dialogue Stratégie de message s'ouvre, présentant les paramètres de la stratégie sélectionnée.

Description : **Mailing List Submissions**

Si **au moins un** des conditions suivantes sont remplies :

Domaine du destina...	correspond au ...	*-users@.*
Domaine du destina...	correspond au ...	*-bug@.*
Domaine du destina...	correspond au ...	*-docs@.*
Domaine du destina...	correspond au ...	*-help@.*
Domaine du destina...	correspond au ...	*-news@.*
Domaine du destina...	correspond au ...	*-digest@.*
Domaine du destina...	correspond au ...	*-list@.*
Domaine du destina...	correspond au ...	*-devel@.*
Domaine du destina...	correspond au ...	*-announce@.*

Procédez aux actions suivantes :

Signer

Préférence de codage du message : **PGP/MIME**

Si une clé de destinataire est introuvable :

Rechercher keys.domain et Tous les serveurs de clés mise en cache temporaire des clés

Si aucun résultat : **Bloquer message**

? Rétablir Annuler OK

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

- 4 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.
- 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 : 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.

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.
- **finir par** : la condition est remplie lorsque le texte du premier champ de condition *finir 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.

7 Dans la zone de texte du troisième champ de condition, saisissez le texte du critère correspondant.

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.

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.

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**, 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. 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.
- 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** 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

- 1** Cliquez sur le nom du service rattaché à la stratégie de sécurité à supprimer. Les propriétés dudit service apparaissent.
- 2** Désactivez la case à cocher correspondant à la stratégie que vous voulez supprimer.
- 3** Vérifiez que la stratégie est toujours sélectionnée et cliquez sur [-] au bas de la zone **Stratégies de sécurité**. Une boîte de dialogue de confirmation apparaît.
- 4** Cliquez sur **Supprimer** pour supprimer la stratégie. Celle-ci est alors supprimée de la liste.

Modification de l'ordre des stratégies dans la liste

► Pour modifier l'ordre des stratégies dans la liste des stratégies de sécurité

- 1 Dans Messagerie PGP, sélectionnez le nom du service qui contient la stratégie de sécurité que vous souhaitez déplacer. Les propriétés dudit service apparaissent.
- 2 Dans la liste **Stratégies de sécurité**, cliquez sur le nom de la stratégie que vous souhaitez déplacer dans la liste. La stratégie est alors mise en évidence.
- 3 Cliquez sur la flèche vers le haut ou vers le bas située dans la partie inférieure de la fenêtre Stratégies de sécurité jusqu'à ce que la stratégie se trouve à la position qui vous convient dans la liste.

Remarque : assurez-vous que la stratégie **Chiffrement opportuniste** se trouve en dernière position dans la liste. Toute stratégie placée après n'est pas appliquée.

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 SSL, 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'envoiera 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 peuvent 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**.

Affichage du journal de PGP

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

► Pour afficher le journal de PGP

- 1** Effectuez l'une des opérations suivantes :
- Cliquez sur l'icône PGP Desktop dans la barre de menus et sélectionnez **Afficher le journal** dans le menu. Le journal de PGP s'affiche.
 - Ouvrez PGP Desktop et sélectionnez **Windows > Journal de PGP**. Le journal de PGP s'affiche.
- 2** Procédez comme suit :
- Cliquez sur **Effacer** pour supprimer toutes les entrées du journal de PGP. Un message vous invite à confirmer l'effacement. Cliquez sur **Oui**.

- Cliquez sur **Rechercher** pour rechercher les entrées dans le journal de PGP. Saisissez les termes recherchés et cliquez sur **Suivant**.
- Cliquez sur la flèche du **niveau de journalisation** pour sélectionner le **niveau d'informations minimal des entrées du journal à afficher : Info** ou **Informations détaillées**. Remarque : la journalisation **Informations détaillées** peut générer des fichiers journaux volumineux.

Pour afficher les journaux **Informations détaillées**, la fenêtre d'affichage Journal de PGP doit rester ouverte. Lorsque vous la fermez, le niveau de journalisation revient à celui par défaut, c'est-à-dire **Info**. Remarque : la journalisation **Informations détaillées** peut générer des fichiers journaux volumineux.

- Cliquez sur **Enregistrer** pour enregistrer une copie des entrées dans le journal. Spécifiez le nom du fichier journal, un emplacement et un format (fichier en texte brut par défaut), puis cliquez sur **Enregistrer**.
- 3 Cliquez sur le cercle rouge dans l'angle supérieur gauche de l'écran pour fermer la fenêtre Journal de PGP.

Utilisation de scripts PGP avec Entourage 2008

► Pour utiliser les scripts PGP dans Entourage afin de chiffrer des courriers électroniques

- 1 Créez un message électronique.
- 2 Cliquez sur l'icône **Scripts** de la barre d'outils d'Entourage et sélectionnez **PGP**.
- 3 Sélectionnez l'option **Chiffrer** ou **Chiffrer et signer**, puis choisissez la clé de signature.
- 4 Le texte du message est chiffré et un bloc de texte chiffré s'affiche à sa place.
- 5 Vous pouvez alors envoyer votre courrier électronique en toute sécurité.

► Pour utiliser les scripts PGP dans Entourage afin de déchiffrer des courriers électroniques

- 1 Ouvrez le courrier électronique chiffré.
- 2 Cliquez sur l'option **Scripts** et sélectionnez **PGP**.
- 3 Choisissez **Déchiffrer et vérifier**, puis saisissez la phrase secrète lorsque vous y êtes invité. Le courrier électronique est déchiffré.

9

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* (cf. "Préférences de messagerie" à la page 205).

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.....	129
À propos des clés utilisées pour le chiffrement	131
Chiffrement des sessions de messagerie instantanée	131

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 :

- iChat 3.1.x, 4.0

Le chiffrement des transferts de fichiers et des connexions directes n'est possible qu'avec AIM 5.9.3702 sous Windows ou iChat 3.1 sous Mac OS X. PGP Desktop ne chiffre pas les connexions audio et vidéo.

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 129), 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. »
- Si vous ouvrez le journal de PGP après avoir lancé votre session, des entrées indiquent que celle-ci fait l'objet d'un traitement proxy, qu'elle est chiffrée, etc. Par exemple :

2006-09-15 11:39:49 Traitement proxy de la connexion AIM de AliceIM avec Apple iChat.

Initiation d'une session AIM chiffrée par PGP Desktop avec JMedinaX à l'aide de votre clé dont l'ID est 0x0910D29E.

Session AIM chiffrée établie avec JMedinaX.

10

Affichage des messages électroniques à l'aide de la Visionneuse PGP

Cette section propose des informations sur l'utilisation de PGP Desktop pour déchiffrer, vérifier et afficher les messages chiffrés à l'aide de la Visionneuse PGP.

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	133
Ouverture d'un message électronique ou d'un fichier chiffré	135
Copie de messages électroniques dans votre boîte de réception	136
Exportation de messages électroniques.....	136
Préférences de la Visionneuse PGP	137
Fonctionnalités de sécurité dans la Visionneuse PGP	138

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. Ouvrez la pièce jointe au fichier message.pgp à l'aide de la Visionneuse PGP ou copiez le texte chiffré et collez-le dans la Visionneuse 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 d'un 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 des trousseaux de clés PGP Desktop pour les opérations nécessitant des clés.

La Visionneuse PGP respecte les 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 associées à la stratégie en vigueur.

La Visionneuse PGP 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 pris en charge

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

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

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

Copie de messages électroniques dans votre boîte de réception

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

► **Pour copier un message dans la boîte de réception de votre client de messagerie**

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

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

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

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

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

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

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

Exportation de messages électroniques

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

► **Pour exporter un message depuis la Visionneuse PGP vers un fichier**

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

La Visionneuse PGP enregistre le fichier à l'emplacement choisi.

Préférences de la Visionneuse PGP

La Visionneuse PGP inclut des préférences qui permettent de contrôler certaines fonctionnalités.

► Pour accéder aux préférences de la Visionneuse PGP

- 1 Ouvrez la Visionneuse PGP ou utilisez-la pour déchiffrer, vérifier et afficher un message.
- 2 Ouvrez le menu **Visionneuse PGP** et sélectionnez **Préférences**.
La boîte de dialogue **Préférences** s'affiche.
- 3 Sélectionnez l'onglet **Général** et indiquez les préférences suivantes :
 - **Demander confirmation en cas d'utilisation de l'option 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 dans les messages HTML** : 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.
 - **Client de messagerie** : permet d'indiquer le client de messagerie dans lequel la Visionneuse PGP doit copier le contenu. Le client par défaut est le client de message par défaut du système (la Visionneuse PGP détermine le client de messagerie de votre système et l'utilise par défaut). Vous pouvez sélectionner **Mail.app** ou **Thunderbird**.
- 4 Sélectionnez l'onglet **Polices et couleurs** et indiquez les préférences suivantes :
 - **Police** : indique la police que doit utiliser la Visionneuse PGP pour afficher le texte. Cliquez sur **Sélectionner**, puis indiquez la **collection**, la **famille**, le **type de caractère** et la **taille souhaités**.
 - **Couleur du texte** : indique la couleur que doit afficher la Visionneuse PGP pour le texte. Cliquez sur le bloc de couleurs et choisissez-en une.
 - **Couleur d'arrière-plan** : indique la couleur d'arrière-plan du texte que doit afficher la Visionneuse PGP. Cliquez sur le bloc de couleurs et choisissez-en une.

Fonctionnalités de sécurité dans la Visionneuse PGP

La Visionneuse PGP protège activement la sécurité :

- 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, ce qui aurait été le cas sinon.
- 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.

11

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. 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 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 Universal Server peut avoir défini une stratégie exigeant le chiffrement de tous les disques système. Le cas échéant, PGP Desktop vérifie régulièrement que les disques sont chiffrés et applique la stratégie en chiffrant automatiquement les disques systèmes qui ne le sont pas.

Contenu du chapitre

À propos de PGP Whole Disk Encryption	140
Gestion des licences PGP Whole Disk Encryption	142
Préparation du disque au chiffrement.....	143
Déterminer la méthode d'authentification du disque	147
Chiffrement d'un disque	148
Utilisation d'un disque chiffré par PGP-WDE.....	151
Continuité de la sécurité du disque	153
Utilisation de PGP WDE dans un environnement géré par un PGP Universal Server.....	158
Récupération de données à partir d'un lecteur chiffré	160
Déchiffrement d'un disque chiffré par PGP WDE	162
Déplacement des disques amovibles sur d'autres systèmes	162
Accès aux données stockées sur des disques amovibles chiffrés.....	163
Précautions spéciales de sécurité prises par PGP Desktop	163
Détails techniques relatifs au chiffrement de disques de démarrage ...	166

À propos de PGP Whole Disk Encryption

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

Important : PGP Desktop version 9.9 et ultérieure font appel à une méthode de partitionnement différente de celle utilisée dans les versions de PGP Desktop antérieures à 9.9. Si vous avez utilisé la fonction PGP WDE des versions de PGP Desktop antérieures à 9.9, vous devez déchiffrer les disques *avant* d'installer la version 10.0, faute de quoi vous ne pourrez plus accéder aux données qu'ils contiennent.

Lorsque vous chiffrez un disque à l'aide de la fonctionnalité PGP WDE, 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 142).
- 2** Suivez la procédure décrite dans la section *Préparation du disque au chiffrement* (à la page 143).
- 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* (cf. "Déterminer la méthode d'authentification du disque" à la page 147).
- 4** Lancez le processus de chiffrement décrit dans la section *Chiffrement d'un disque* (à la page 148).
- 5** Reportez-vous à la section *Utilisation d'un disque chiffré par PGP WDE* (cf. "Utilisation d'un disque chiffré par PGP-WDE" à la page 151) pour apprendre à utiliser un disque chiffré.
- 6** Pour savoir comment assurer la maintenance de votre disque chiffré, consultez la section *Continuité de la sécurité du disque* (à la page 153).
- 7** Pour savoir comment déchiffrer le disque, si nécessaire, reportez-vous à la section *Déchiffrement d'un disque chiffré par PGP WDE* (à la page 162).
- 8** Prenez connaissance des fonctionnalités permettant d'éviter les problèmes de sécurité décrites dans *Précautions spéciales de sécurité prises par PGP Desktop* (à la page 163).

Si vous êtes un administrateur de PGP Universal Server 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 158) pour plus d'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 167).

Chiffrement de disques de démarrage

À partir de PGP Desktop pour Mac OS X version 10.0, vous avez la possibilité de chiffrer entièrement le disque de démarrage d'un ordinateur Macintosh Intel. Bien entendu, vous pouvez toujours chiffrer les disques amovibles et les disques flash USB, comme vous le faisiez avec les versions de PGP Desktop antérieures à la version 10.0.

Important : le produit Boot Camp d'Apple fonctionne uniquement lorsque le disque comporte deux partitions : une pour Mac OS X et une pour Boot Camp. Étant donné que PGP Desktop ajoute une autre partition, Boot Camp ne fonctionne pas sur les systèmes Mac OS X comportant PGP Desktop 10.0 ou version ultérieure. D'autres logiciels de virtualisation, tels que Parallels, fonctionnent normalement sur les systèmes Mac OS X avec PGP Desktop 10.0 ou version ultérieure. PGP Corporation recommande fortement de désinstaller Apple Boot Camp avant d'installer PGP Desktop. Pour plus d'informations sur l'utilisation de PGP Desktop avec Apple Boot Camp, reportez-vous à l'*Article 1697 de la base de connaissances de PGP* (<https://support.pgp.com/?faq=1697>).

La fonctionnalité PGP WDE prend en charge à la fois les systèmes Mac OS X Intel 32 et 64 bits.

Remarque : la fonctionnalité Safe Boot de Mac OS X ne fonctionne pas sur les disques de démarrage ayant été entièrement chiffrés ; Safe Boot désactive les extensions de noyau requises par PGP WDE. Si vous maintenez la touche Maj enfoncée après l'authentification sur l'écran PGP BootGuard, le système ne démarre *pas*. Il redémarre cependant après quelques minutes.

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 167).

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** Dans le menu **PGP**, sélectionnez **Licence**. La boîte de dialogue contenant les informations sur la licence apparaît.
- 3** Cliquez sur **Détails**. Les détails relatifs à votre licence sont alors affichés. Vérifiez que **PGP Whole Disk Encryption** figure bien dans la section Fonctionnalités activées.

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 219).
- 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 un chiffrement initial correct.

- **Déterminer si le disque concerné est pris en charge** : Reportez-vous à la section *Types de disques pris en charge* (à la page 144).
- **Vérifier que les caractères que vous avez utilisés pour votre phrase secrète sont tous pris en charge** : Reportez-vous à la section *Caractères pris en charge* (à la page 148).

- **Vérifier le bon fonctionnement du disque avant de commencer son chiffrement** : si PGP WDE rencontre des erreurs sur le disque lors du chiffrement, le processus sera interrompu afin que vous puissiez les corriger. Il est cependant plus efficace de les résoudre avant de commencer le chiffrement. Reportez-vous à la section *Vérification du bon fonctionnement du disque avant le chiffrement* (à la page 146).
- **Effectuer une sauvegarde du disque avant le chiffrement** : avant de chiffrer votre disque, assurez-vous de sauvegarder son contenu afin de ne perdre aucune donnée en cas de perte ou de vol de l'ordinateur, ou d'incapacité à déchiffrer le disque. Pensez également à effectuer des sauvegardes régulières.
- **Évaluer le temps nécessaire pour chiffrer le disque** et se préparer en conséquence. Reportez-vous à la section *Calcul de la durée du chiffrement* (à la page 146).
- **Effectuer un test pilote afin de vérifier la compatibilité du logiciel** : pour plus de sécurité, PGP Corporation conseille de tester PGP WDE sur quelques ordinateurs afin de vérifier qu'il n'existe aucun conflit avec d'autres logiciels installés avant un déploiement sur un grand nombre d'ordinateurs. Ce test peut s'avérer particulièrement utile dans les environnements utilisant une image COE (Corporate Operating Environment) standardisée. Certains logiciels de protection des disques sont incompatibles avec PGP WDE et peuvent causer de graves problèmes, tels que la perte de données. Reportez-vous à la section *Effectuer un test pilote afin de vérifier la compatibilité du logiciel* (à la page 147), qui répertorie les problèmes d'interopérabilité connus, ainsi que les *Notes de publication de PGP Desktop* contenant les mises à jour apportées à cette liste.
- **Vérifier que le mode veille a été désactivé**. PGP Desktop n'est pas compatible avec le mode mise en veille prolongée des systèmes Mac OS X.

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 ;

Remarque : n'utilisez pas PGP WDE pour chiffrer du matériel de serveur. PGP WDE n'est pas pris en charge par le matériel de serveur Mac OS X.

- disques externes, *sauf* périphériques musicaux et appareils photo numériques ;
- disques flash USB, parfois appelés clés USB.

La taille du disque chiffré par PGP WDE n'est soumise à aucune restriction. Tout disque 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 partitionner un lecteur chiffré avec PGP WDE, vous devez d'abord le déchiffrer. Une fois le lecteur déchiffré, vous pouvez le partitionner.

PGP WDE prend en charge tous les modes de gestion de l'alimentation Mac OS X.

Types de disques non pris en charge

Les types de disques suivants ne sont *pas* pris en charge :

- disques formatés à l'aide du schéma de partition APM ;
- tout type de matériel de serveur, y compris les disques RAID ;
- disquettes et CD-RW/DVD-RW.

Claviers pris en charge

L'écran d'ouverture de session PGP Whole Disk Encryption prend en charge les configurations de clavier suivantes :

- Anglais (États-Unis/International)
- Japonais (Japon)
- Allemand (Allemagne)
- Français (France)
- Espagnol (Amérique latine)
- Espagnol (Espagne ; ISO)

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. Veillez à spécifier la configuration de clavier prise en charge (dans Préférences système > Personnel > International), puis assurez-vous d'utiliser la même configuration chaque fois que vous vous authentifier.

Vérification du bon fonctionnement du disque avant le chiffrement

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

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

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

Recommandations

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

Si vous utilisez Apple Boot Camp, PGP Corporation vous recommande d'effectuer toutes les opérations de chiffrement et de déchiffrement à partir de la partition Mac OS X. Assurez-vous que vous avez installé PGP Desktop sur les partitions Mac OS X et Windows avant d'effectuer les opérations de chiffrement et de déchiffrement à partir de la partition Mac OS X.

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

Calcul de la durée du chiffrement

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

Facteurs ayant une incidence sur la vitesse du chiffrement :

- taille du disque ;
- nombre de processeurs et leur vitesse ;
- nombre de processus système exécutés sur l'ordinateur ;
- nombre d'applications exécutées sur le système ;

- quantité du temps processeur requise par ces applications.

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

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

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

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

Effectuer un test pilote afin de vérifier la compatibilité du logiciel

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

Déterminer la méthode d'authentification du disque

Lorsque vous chiffrez un disque à l'aide de PGP WDE, vous choisissez une méthode d'authentification vous permettant de déchiffrer le disque.

Vous disposez des possibilités suivantes :

- **Phrase secrète** : avec l'authentification par phrase secrète, vous spécifiez une phrase secrète lorsque vous chiffrez un disque. Lorsque vous essayez d'accéder au disque chiffré, vous devez entrer cette phrase secrète.
- **Clé publique** : avec l'authentification par clé publique, vous spécifiez une clé publique lors du chiffrement d'un disque. Seul le détenteur de la clé privée correspondante peut accéder au contenu du disque. Pour cela, 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. Les disques fixes, notamment les disques de démarrage et les disques dans des boîtiers USB, doivent être chiffrés à l'aide d'un utilisateur de phrase secrète.

Lors du chiffrement initial d'un *disque de démarrage*, vous pouvez choisir uniquement la méthode d'authentification par phrase secrète. Après le chiffrement initial, vous pouvez ajouter d'autres utilisateurs de phrase secrète au disque.

Pour le chiffrement initial d'un *disque autre qu'un disque de démarrage* (tel qu'un disque externe), vous avez le choix entre authentification par phrase secrète ou par clé publique.

Chiffrement d'un disque

Vous pouvez chiffrer un disque que vous avez au préalable préparé. Tenez compte des informations suivantes avant de commencer.

- Au cours du processus de chiffrement, vous pouvez utiliser le système, mais son fonctionnement est ralenti. Il fonctionne de nouveau normalement une fois que le chiffrement est 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 l'opération.
- 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 ne pouvez chiffrer ou déchiffrer qu'un seul disque à la fois. Lorsque vous commencez une opération sur un disque, 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 pris en charge

Lorsque vous créez des phrases secrètes avec PGP Whole Disk Encryption, vous pouvez saisir des caractères alphanumériques, des signes de ponctuation et des métacaractères standard. 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.

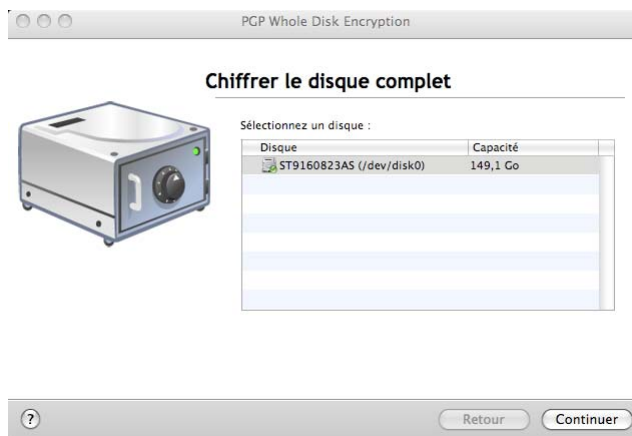
- Pour les versions japonaises de PGP Desktop, les autres *caractères non valides* sont :
` et ~

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.

► Pour protéger un disque à l'aide de la fonctionnalité PGP Whole Disk Encryption

- 1 Ouvrez PGP Desktop et cliquez sur l'élément PGP Disk. L'écran PGP Disk s'affiche.
- 2 Cliquez sur **Chiffrer le disque complet**. L'écran Chiffrer le disque complet apparaît et présente la liste des disques de votre système pouvant être protégés.



- 3 Dans la liste **Sélectionnez un disque**, cliquez sur le disque à protéger.
- 4 Dans la section **Sécuriser avec**, précisez la méthode d'accès au disque protégé : **Utilisateur de clé publique** or **Utilisateur de phrase secrète**.

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

- Si vous voulez protéger votre disque avec une clé publique, sélectionnez **Clé publique**, puis cliquez sur **Continuer**. L'écran Ajout d'un utilisateur de PGP Whole Disk s'affiche. Cette option n'est pas disponible si vous avez déjà chiffré votre disque.

Sélectionnez une clé dans la liste fournie et cliquez sur **Continuer**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.

Tapez la phrase secrète de la clé sélectionnée, puis cliquez sur **OK**. L'écran Récapitulatif de PGP Whole Disk Encryption apparaît, présentant un récapitulatif de la façon dont le disque va être chiffré, de la clé qui va être utilisée, etc.

- Si vous voulez protéger votre disque avec une phrase secrète, sélectionnez **Phrase secrète**, puis cliquez sur **Continuer**. L'écran Ajout d'un utilisateur de PGP Whole Disk s'affiche.

Complétez le champ **Nom** (ou acceptez le nom par défaut), puis saisissez la phrase secrète souhaitée dans le champ **Saisissez votre phrase secrète**, puis tapez-la à nouveau dans le champ **Confirmez votre phrase secrète**. **Pour que la phrase secrète s'affiche à mesure que vous saisissez les caractères, sélectionnez Afficher les frappes.**

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 214).

Cliquez sur **Continuer**. L'écran Récapitulatif de PGP Whole Disk Encryption apparaît, présentant un récapitulatif de la façon dont le disque va être chiffré, de la clé qui va être utilisée, etc.

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

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

- 7 Au cours du processus de chiffrement, vous pouvez effectuer les opérations suivantes :
 - Pour interrompre temporairement le processus de chiffrement, cliquez sur **Arrêter**. La boîte de dialogue Chiffrement non terminé s'affiche.
 - Cliquez sur **Pause** pour interrompre le processus de chiffrement, sur **Déchiffrer** pour déchiffrer la partie du disque déjà chiffrée ou sur **Annuler** pour fermer la boîte de dialogue et poursuivre le processus de chiffrement.

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

Lorsque le processus de chiffrement est terminé, les propriétés du disque chiffré s'affichent ; elles incluent des informations sur la description, le type de disque, la taille, l'état chiffré et l'accès utilisateur.

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 dans le PGP Universal Server 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 identifié 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 :

- Forcez 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.
- Arrêtez le chiffrement en cliquant sur **Non**, déchiffrez entièrement le disque, puis réparez les erreurs à l'aide d'un outil 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 d'ouverture de session PGP BootGuard s'affiche et vous invite à saisir votre phrase secrète. Une fois que vous avez entré votre phrase secrète, PGP WDE déchiffre le disque.

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, 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 la section *Utilisation des PGP Virtual Disks* (à la page 167).

Lorsque vous arrêtez un système avec un disque de démarrage chiffré, ou si vous retirez un disque amovible chiffré du système, tous les fichiers du disque restent chiffrés et entièrement protégés. Les données ne sont jamais écrites sur le disque sous une forme non chiffrée. Pour accéder aux fichiers, l'authentification appropriée (phrase secrète ou clé privée) est requise.

Authentification à partir de l'écran PGP BootGuard

L'écran d'ouverture de session PGP BootGuard vous invite à saisir la phrase secrète du disque protégé pour l'une des deux raisons suivantes :

- Lorsque PGP Whole Disk Encryption protège votre disque 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.
- Si PGP Whole Disk Encryption protège un disque fixe secondaire, vous pouvez vous authentifier au démarrage. Ainsi, vous n'avez pas à le faire lorsque vous souhaitez utiliser les fichiers de ce disque. Les fichiers du disque secondaire n'étant pas nécessaires pour le démarrage, l'authentification au démarrage n'est pas obligatoire. 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 secondaire.

Remarque : l'écran d'ouverture de session PGP BootGuard accepte les informations d'authentification de tous les utilisateurs configurés pour un disque chiffré. Par exemple, si deux utilisateurs sont configurés pour un disque de démarrage et deux autres utilisateurs pour un disque fixe secondaire sur le même système, *chacun* des quatre utilisateurs peut s'authentifier sur l'écran d'ouverture de session PGP BootGuard au démarrage à l'aide de sa phrase secrète.

Sur l'écran d'ouverture de session PGP BootGuard, vous pouvez authentifier un disque secondaire ou de démarrage chiffré sur le système.

► **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. Lors du démarrage, l'écran d'ouverture de session PGP BootGuard s'affiche.



- 2 Tapez une phrase secrète valide et appuyez sur la touche **Entrée**.

Remarque : certains caractères ne peuvent pas être saisis dans l'écran PGP BootGuard. Reportez-vous à la section *Caractères pris en charge* (à la page 148).

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.

- 3 Si vous saisissez une phrase secrète valide, l'écran d'ouverture de session PGP BootGuard disparaît et le système démarre normalement.

Si la phrase secrète saisie est incorrecte, un message d'erreur apparaît. Ressaisissez la phrase secrète.

Continuité de la sécurité du disque

Les sections suivantes décrivent comment travailler avec votre disque chiffré avec PGP WDE.

Affichage des informations sur la clé sur un disque chiffré

► **Pour afficher les informations sur la clé publique d'un utilisateur sur un disque chiffré**

- 1 Sélectionnez le disque chiffré auquel est associé l'utilisateur de la clé publique dont vous souhaitez consulter les informations.
- 2 Appuyez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur le nom de l'utilisateur dans la liste **Accès de l'utilisateur** ; vous pouvez également cliquer dessus avec le bouton droit si vous possédez une souris à deux boutons.
- 3 Dans le menu contextuel, sélectionnez **Afficher infos sur la clé**. L'écran **Infos sur la clé** correspondant à la clé indiquée apparaît.

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.

Ajout d'utilisateurs supplémentaires à un disque chiffré

Un utilisateur qui crée un disque chiffré peut le mettre à la disposition d'autres utilisateurs. Ces utilisateurs supplémentaires peuvent accéder au disque en utilisant leur propre phrase secrète ou clé privée. Vous pouvez avoir jusqu'à 120 utilisateurs par disque chiffré.

Attention : le fait que plusieurs utilisateurs puissent accéder à un disque protégé par PGP Whole Disk Encryption sert de voie de secours si une personne oublie sa phrase secrète. Les utilisateurs ainsi configurés peuvent s'authentifier dans l'écran d'ouverture de session PGP Whole Disk Encryption afin de déverrouiller les disques protégés sur ce système.

► **Pour ajouter des utilisateurs supplémentaires à un disque protégé par PGP Whole Disk Encryption**

- 1 Sélectionnez le disque chiffré auquel vous souhaitez ajouter un utilisateur supplémentaire.
- 2 Sous la liste **Accès de l'utilisateur**, cliquez sur le signe « plus » (+).
- 3 Dans la liste qui apparaît, sélectionnez **Ajouter un utilisateur de clé publique** ou **Ajouter un utilisateur de phrase secrète**.

- Si vous choisissez **Ajouter un utilisateur de clé publique**, vous êtes invité à sélectionner la clé publique du ou des utilisateurs à ajouter ; pour cela, faites glisser les utilisateurs concernés de la colonne **Source de clé** vers la colonne **Clés à ajouter**, puis cliquez sur **OK**.
- Si, en revanche, vous choisissez **Ajouter un utilisateur de phrase secrète**, vous devez indiquer un nom d'utilisateur et une phrase secrète pour l'utilisateur à ajouter. Saisissez le nom d'utilisateur dans le champ **Nom d'utilisateur**.

La phrase secrète doit être indiquée dans le champ **Saisir une phrase secrète pour cet utilisateur**. Ressaisissez la phrase secrète dans le champ **Confirmer la phrase secrète de l'utilisateur**. Pour que la phrase secrète s'affiche à mesure que vous saisissez les caractères, sélectionnez **Afficher les frappes**.

Cliquez sur **OK**.

Un message vous invite alors à indiquer la phrase secrète rattachée au disque chiffré.

- 4 Saisissez-la et cliquez sur **OK**. Le ou les utilisateurs de clé publique ou l'utilisateur de phrase secrète désignés sont ajoutés.

Remarque : le chiffrement par clé publique constitue la méthode de protection offrant le niveau de sécurité maximal lors de l'ajout d'utilisateurs supplémentaires aux disques chiffrés à l'aide de PGP Whole Disk Encryption, pour les raisons suivantes : (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.

Suppression d'utilisateurs d'un disque chiffré

Il se peut qu'un jour vous souhaitiez interdire l'accès à un disque chiffré à un utilisateur.

► Pour supprimer un utilisateur d'un disque chiffré

- 1 Sélectionnez le disque pour lequel vous souhaitez supprimer un utilisateur.
- 2 Dans la liste **Accès de l'utilisateur**, sélectionnez le nom de l'utilisateur à supprimer.
- 3 Sous cette liste, cliquez sur le signe « moins » (–). L'application vous demande alors de donner la phrase secrète rattachée au disque chiffré.
- 4 Saisissez-la et cliquez sur **OK**. L'autre utilisateur est supprimé.

Remarque : il est impossible de supprimer tous les utilisateurs d'un disque chiffré ; si la liste Accès de l'utilisateur ne comporte qu'un seul utilisateur, ce dernier ne peut pas être supprimé.

Modification des phrases secrètes des utilisateurs

► Pour modifier la phrase secrète d'un utilisateur sur un disque chiffré

- 1 Sélectionnez le disque chiffré auquel est associé l'utilisateur dont vous voulez modifier la phrase secrète.
- 2 Appuyez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur le nom de l'utilisateur dans la liste **Accès de l'utilisateur** ; vous pouvez également cliquer dessus avec le bouton droit si vous possédez une souris à deux boutons.
- 3 Dans le menu contextuel, sélectionnez **Modifier phrase secrète utilisateur**. L'application vous demande alors de donner la phrase secrète rattachée au disque chiffré.
- 4 Saisissez-la et cliquez sur **OK**. L'écran **Confirmer la phrase secrète PGP** s'affiche.
- 5 Saisissez une nouvelle phrase secrète dans la zone **Saisissez votre nouvelle phrase secrète**, entrez-la à nouveau dans le champ **Confirmation**, puis cliquez sur **OK**.
- 6 Dans la zone Phrase secrète modifiée, cliquez sur **OK**. La phrase secrète est modifiée.

Nouveau chiffrement d'un disque chiffré

Si vous pensez que la phrase secrète rattachée a pu être interceptée, il est vivement conseillé d'effectuer un nouveau chiffrement du disque protégé.

Pour chiffrer à nouveau un disque, la fonctionnalité PGP Whole Disk Encryption utilise le même algorithme de chiffrement (AES 256), mais 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.

► Pour chiffrer à nouveau un disque chiffré

- 1 Sélectionnez le disque chiffré concerné.
- 2 Dans le menu **Disque**, sélectionnez l'option **Chiffrer à nouveau le disque**. L'application vous demande alors de donner la phrase secrète rattachée au disque chiffré.
- 3 Saisissez-la et cliquez sur **OK**. Le processus de nouveau chiffrement commence.

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 tout disque protégé par PGP WDE. Les fichiers sauvegardés par le logiciel sont déchiffrés avant d'être sauvegardés.

Ainsi, les sauvegardes effectuées à l'aide de Time Machine, le logiciel de sauvegarde automatique intégré à Mac OS X 10.5 (Leopard), sont effectuées normalement et les fichiers ne sont pas chiffrés.

Remarque : le logiciel de récupération des données (tel que la version Mac OS X de Boomerang Data Recovery) essaie de récupérer les données à partir d'un disque dur actuellement inaccessible. Si le logiciel de récupération des données est utilisé sur un disque protégé par PGP WDE, il trouvera des données chiffrées qui ne seront pas utilisables.

Désinstallation de PGP Desktop des disques chiffrés

Si des disques de 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 disques de ce type. Dans ce cas, un message d'erreur s'affiche, expliquant que le processus de désinstallation est arrêté afin de protéger le disque chiffré.

Pour désinstaller PGP Desktop, déchiffrez d'abord les disques de votre système qui sont protégés à l'aide de PGP Whole Disk Encryption.

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 disques qui sont protégés à l'aide de PGP Whole Disk Encryption.** Si vous oubliez la phrase secrète qui permet d'accéder à un disque chiffré à l'aide de PGP Whole Disk Encryption, il vous est impossible d'accéder au disque. Cependant, si vous utilisez la fonctionnalité PGP Whole Disk Encryption dans un environnement géré par PGP Universal Server, contactez votre administrateur PGP pour vérifier si la récupération 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 PGP Universal Server, contactez votre administrateur PGP pour plus d'informations.

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 déjà chiffrés ou ajouter de nouveaux utilisateurs.

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. Il peut également vous arriver de 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*.
- 2** Utilisez un autre système pour déchiffrer le lecteur. Pour plus d'informations sur la création d'une stratégie ou sur la modification de stratégies existantes, reportez-vous à la section *Déchiffrement d'un disque chiffré par PGP WDE* (cf. "Déchiffrement d'un disque chiffré par PGP WDE" à la page 162).
- 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 160).

Pour en savoir plus sur la récupération de données, consultez l'*article 1018 de la base de connaissances du support de PGP* <https://support.pgp.com/?faq=1018>.

Pour plus d'informations sur la récupération de données à l'aide du mode disque cible, consultez l'*article 1583 de la base de connaissances du support de PGP* (<http://support.pgp.com/?faq=1583>).

Création et utilisation de disques de récupération

Bien qu'il soit très peu probable qu'un fichier boot.efi 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. Créez un CD de récupération avant de chiffrer un disque ou une partition de démarrage à l'aide de PGP Desktop.

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 9.5 pour déchiffrer un disque protégé à l'aide du logiciel PGP WDE 10.0, le disque PGP WDE 10.0 sera inutilisable.

Cette section décrit les procédures de création et d'utilisation d'un CD de récupération. Pour plus d'informations, consultez l'*article 1658 de la base de connaissances de PGP* (<http://support.pgp.com/?faq=1658>).

► Pour créer un CD de récupération

- 1 Téléchargez et enregistrez l'image ISO de récupération sur votre système.
- 2 Gravez l'image sur un CD-ROM à l'aide de l'utilitaire de disque Mac OS X. Pour en savoir plus sur cette opération, consultez l'*article HT2087 du support Apple* (<http://support.apple.com/kb/HT2087>).
- 3 Retirez le CD de récupération du lecteur et étiquetez-le.

► 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.

- 1 Démarrez le système Macintosh à l'aide du disque. Pour ce faire, maintenez la touche Option enfoncée lors du redémarrage du système et choisissez de démarrer à partir du disque de récupération. L'écran PGP BootGuard s'affiche.
- 2 Pour déchiffrer le disque, appuyez sur D, puis sur Entrée.

- 3 Saisissez votre phrase secrète à l'invite et appuyez sur Entrée.

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 ce 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).
- Connectez un disque amovible à un second système et effectuez le déchiffrement à partir du logiciel PGP Desktop de ce système. Si le disque amovible est formaté en tant que lecteur FAT, vous pouvez le déchiffrer à l'aide de PGP Desktop pour Windows ou Mac OS X. Si le disque est formaté en tant que lecteur HFS, vous devez utiliser PGP Desktop pour Mac OS X.

Une fois le disque déchiffré, vous pouvez effectuer la récupération.

► Pour utiliser PGP Desktop pour déchiffrer un disque

- 1 Ouvrez PGP Desktop, cliquez avec le bouton droit sur le disque à déchiffrer, puis choisissez **Déchiffrer**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
- 2 Saisissez la phrase secrète permettant de déverrouiller le disque et cliquez sur **OK**. 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**.

Déplacement des disques amovibles sur d'autres systèmes

Vous pouvez déplacer des disques Windows amovibles sur un autre système Mac OS X exécutant PGP Desktop 10.0 et accéder aux fichiers chiffrés sur ce dernier.

Pour pouvoir accéder au contenu du disque, vous devrez toutefois être en mesure de vous authentifier.

Remarque : 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 Windows amovible avec cette fonctionnalité, vous pourrez l'utiliser sur un autre ordinateur doté de PGP Desktop 10.0, et ce même si aucune licence PGP Desktop prenant en charge PGP WDE n'est installée sur celui-ci.

Accès aux données stockées sur des disques amovibles chiffrés

Si vous utilisez PGP Whole Disk Encryption pour Windows 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 uniquement PGP Desktop version 10.0.

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.

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.

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.
- Lorsque vous laissez votre ordinateur pendant un certain temps, PGP Corporation vous recommande d'arrêter votre système Macintosh, plutôt que de le mettre en veille. Vous êtes ainsi certain que personne ne peut accéder à votre système chiffré en le réactivant à partir du mode veille.

Détails techniques relatifs au chiffrement de disques de démarrage

Pour prendre en charge le chiffrement PGP Whole Disk Encryption de disques de démarrage sur Mac OS X, PGP Desktop crée une nouvelle partition (à l'aide de la table de partition GUID) et place un nouveau chargeur de démarrage sur cette nouvelle partition.

Important : les versions de PGP Desktop antérieures à la version 10.0 prennent en charge les partitions APM. Cette méthode de partitionnement ne prend *pas* en charge le chiffrement PGP Whole Disk Encryption de disques de démarrage. La version 9.9 et les versions ultérieures utilisent donc la méthode de partitionnement de table de partition GUID (GPT). En raison de ce changement, tous les disques entièrement chiffrés par PGP utilisant des versions de PGP Desktop antérieures à la version 9.9 doivent être déchiffrés *avant* installation de la version 9.9 ou d'une version ultérieure. Les disques entièrement chiffrés par des versions plus anciennes de PGP non déchiffrés avant installation de la version 9.9 ne seront plus accessibles une fois ces versions installées.

Le chargeur de démarrage installé par PGP Desktop a plusieurs fonctions : il authentifie les utilisateurs essayant de démarrer le disque, puis, après réussite de l'authentification, il appelle le chargeur de démarrage de Mac OS X et déchiffre les fichiers requis pour le démarrage normal du disque. Si l'authentification échoue, il n'appelle pas le chargeur de démarrage Mac OS X et ne déchiffre pas les fichiers nécessaires. Le disque ne démarre donc pas.

Attention : le produit Boot Camp d'Apple fonctionne uniquement lorsque le disque comporte deux partitions : une pour Mac OS X et une pour Boot Camp. Étant donné que PGP Desktop ajoute une autre partition, Boot Camp ne fonctionne pas sur les systèmes Mac OS X comportant PGP Desktop 10.0 ou version ultérieure. D'autres logiciels de virtualisation, tels que Parallels, fonctionnent normalement sur les systèmes Mac OS X avec PGP Desktop 10.0 ou version ultérieure. PGP Corporation recommande fortement de désinstaller Apple Boot Camp avant d'installer PGP Desktop.

12

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

À propos des PGP Virtual Disks	168
Création d'un volume PGP Virtual Disk.....	169
Affichage des propriétés d'un PGP Virtual Disk.....	172
Utilisation d'un PGP Virtual Disk monté.....	172
Gestion des autres utilisateurs	176
Modification des phrases secrètes des utilisateurs	179
Suppression de volumes PGP Virtual Disk	180
Gestion des PGP Virtual Disks	181
Algorithmes de chiffrement des PGP Virtual Disks	183
Précautions spéciales de sécurité prises par PGP Virtual Disk.....	184

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* (cf. "Préférences liées aux disques" à la page 208).

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 219).

Création d'un volume PGP Virtual Disk

► Pour créer un volume PGP Virtual Disk

- 1 Ouvrez PGP Desktop et sélectionnez l'élément **PGP Disk**. La fenêtre du même nom apparaît.

Remarque : si vous n'avez pas installé PGP Whole Disk (option disponible si vous choisissez **Personnaliser** lors de l'installation de PGP Desktop) avec une licence appropriée, seule la section Nouveau Virtual Disk est affichée dans cette fenêtre.

- 2 Cliquez sur **Nouveau PGP Virtual Disk**. L'écran Nouveau PGP Disk s'affiche.



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

- Pour le protéger avec une phrase secrète, sélectionnez **Utilisateur de phrase secrète**.
- 5 Pour afficher ou modifier les options avancées, cochez la case **Options avancées**. La case à cocher **Redimensionner automatiquement le volume PGP Virtual Disk selon les besoins** ainsi que les menus **Chiffrer** et **Formater** apparaissent.

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

- Pour que PGP Desktop gère de façon automatique la taille du nouveau volume **PGP Virtual Disk**, cochez la case **Redimensionner automatiquement le volume PGP Virtual Disk selon les besoins**. La taille du disque changera au fur et à mesure de l'ajout ou de la suppression de fichiers.

Attention : l'option **Redimensionner automatiquement le volume PGP Virtual Disk selon les besoins** est disponible uniquement lorsque vous créez un volume PGP Virtual Disk. Une fois que le volume PGP Virtual Disk est créé, vous ne pouvez plus modifier son statut (passer d'un disque à taille fixe à un disque à taille variable, ou inversement).

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

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

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

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

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

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

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

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

6 Cliquez sur **Continuer**.

7 L'étape suivante est différente selon que vous avez choisi une authentification avec clé publique ou phrase secrète.

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

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

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

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

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

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

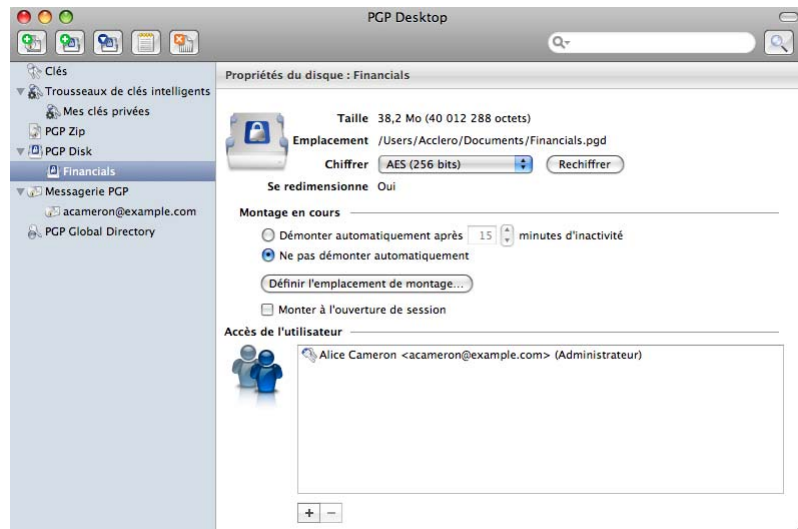
Dans le champ **Confirmez votre phrase secrète**, saisissez à nouveau la phrase secrète à utiliser. Cliquez sur **Continuer**. La boîte de dialogue Enregistrer sous s'affiche. Passez à l'étape suivante.

8 Saisissez un nom de fichier et un emplacement pour le volume PGP Virtual Disk, puis cliquez sur **Enregistrer**.

9 Vérifiez les informations figurant dans l'écran Récapitulatif de la création de PGP Disk. Cet écran affiche la taille du PGP Virtual Disk, le nom et l'emplacement du volume, le format, etc. Lorsque vous avez terminé, cliquez sur **Créer**.

10 L'écran Création de votre volume PGP Virtual Disk est affiché ; il indique l'état d'avancement de la création du volume. Lorsque le disque a été créé, l'écran Félicitations apparaît. Cliquez sur **Terminer**.

- 11 Votre nouveau volume PGP Virtual Disk est monté automatiquement, et les informations afférentes sont affichées dans une fenêtre du Finder. Le nom du disque est en outre fourni sous l'élément **PGP Disk**.



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

- Cliquez sur le nom du disque dans l'élément **PGP Disk**. L'écran Propriétés du disque apparaît.

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 risquez de perdre des données si vous démontez un PGP Virtual Disk alors que certains fichiers qu'il contient sont ouverts. Pour définir les options de démontage des disques, sélectionnez **PGP > Préférences** et cliquez sur l'icône **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 expérimentés 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 :

- Dans PGP Desktop, sélectionnez le PGP Virtual Disk à démonter dans PGP Disk, puis choisissez **Disque > Démontez** ou cliquez sur l'icône **Démontez le disque** de la barre d'outils.
- Faites glisser l'icône du volume PGP Virtual Disk monté vers la **Corbeille**.

Définition de l'emplacement de montage

Vous pouvez préciser l'endroit où le PGP Virtual Disk est monté (situé).

► Pour définir l'emplacement de montage

- 1 Sélectionnez la boîte de contrôle PGP Disk, puis choisissez le PGP Virtual Disk dont vous souhaitez définir l'emplacement de montage.
- 2 Cliquez sur **Définir l'emplacement de montage**. La boîte de dialogue Définissez le point de montage de votre PGP Disk s'affiche.
- 3 Sélectionnez l'une des options suivantes :
 - **Bureau (par défaut)** : sélectionnez cette option pour monter votre volume PGP Disk sur le bureau. Il s'agit de l'emplacement de montage par défaut du PGP Virtual Disk.
 - **À l'emplacement suivant** : sélectionnez cette option pour monter votre PGP Virtual Disk à un emplacement choisi par vos soins. Cliquez sur **Parcourir**, puis accédez à l'emplacement où vous voulez que votre PGP Virtual Disk soit monté. Cliquez sur **Ouvrir** pour confirmer votre choix.
- 4 Cliquez sur **OK**. L'emplacement de montage de votre PGP Virtual Disk est établi.

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.

► Pour compacter un PGP Virtual Disk

- Effectuez l'une des opérations ci-dessous :
 - Dans le Finder de Mac OS X, accédez à l'emplacement du fichier .pgd. Cliquez avec le bouton droit sur ce fichier et sélectionnez **PGP > Compacter**.

Si vous ne savez pas où se trouve le PGP Virtual Disk, dans PGP Desktop, cliquez avec le bouton droit sur le nom du disque et sélectionnez **Afficher dans le Finder**.

- Dans PGP Desktop, cliquez sur l'élément PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, sélectionnez le PGP Virtual Disk à compacter, puis choisissez **Disque > Compacter le disque**. Vous pouvez également cliquer sur le PGP Virtual Disk en maintenant la touche Ctrl enfoncée (ou cliquer dessus avec le bouton droit si vous possédez une souris à deux boutons) dans la boîte de contrôle PGP Disk et sélectionner **Compacter** dans le menu contextuel.

Nouveau chiffrement des volumes PGP Virtual Disk

Vous pouvez chiffrer à nouveau toutes les données stockées sur un volume PGP Virtual Disk. Vous pouvez être amené à le faire pour les 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 volume 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 volume 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 volume PGP Virtual Disk**

- 1 Dans le panneau gauche de l'écran principal de PGP Desktop, sélectionnez l'élément PGP Disk, puis choisissez le volume PGP Virtual Disk à chiffrer à nouveau.
- 2 S'il est monté, démontez-le.
- 3 Cliquez sur **Chiffrer à nouveau**. Une boîte de dialogue de confirmation apparaît.
- 4 Vérifiez les informations fournies, puis cliquez sur **Chiffrer à nouveau**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.
- 5 Saisissez la phrase secrète de l'administrateur du volume PGP Virtual Disk et cliquez sur **OK**. Le volume est chiffré à nouveau. Une barre de progression apparaît durant le processus.
- 6 Lorsque l'état Terminé est indiqué, cliquez sur **Suivant**.
- 7 Cliquez sur **Terminer** pour finaliser le processus de nouveau chiffrement.

Gestion des autres utilisateurs

Cette section décrit comment 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 pour un volume PGP Virtual Disk

L'administrateur d'un volume 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.

► **Pour ajouter des comptes autre utilisateur pour un volume PGP Virtual Disk**

- 1 Dans le panneau gauche de la fenêtre principale de PGP Desktop, cliquez sur l'élément PGP Disk, puis sélectionnez le nom du PGP Virtual Disk auquel vous souhaitez ajouter un compte autre utilisateur.
- 2 Dans l'écran Propriétés du disque, cliquez sur le signe « plus » situé sous la liste Accès de l'utilisateur et sélectionnez l'option **Ajouter un utilisateur de clé publique** ou **Ajouter un utilisateur de phrase secrète**, selon le type de compte autre utilisateur à ajouter.

- Si vous avez cliqué sur **Ajouter un utilisateur de clé publique**, sélectionnez la clé publique de l'utilisateur associé au compte à ajouter ; pour cela, faites-la glisser de la colonne **Source de clé** vers la colonne **Clés à ajouter**. Vous pouvez ajouter plusieurs utilisateurs si vous le souhaitez.
- De même, si vous avez cliqué sur **Ajouter un utilisateur de phrase secrète**, sélectionnez la clé publique de l'utilisateur associé au compte à ajouter en la faisant glisser de la colonne **Source de clé** vers la colonne **Clés à ajouter**. La boîte de dialogue Ajouter un utilisateur à votre PGP Disk apparaît.

Dans le champ **Nom**, saisissez un nom pour l'autre utilisateur que vous ajoutez.

Dans le champ **Saisir une phrase secrète pour cet utilisateur**, indiquez une phrase secrète pour ce dernier.

Entrez une nouvelle fois la phrase secrète dans le champ **Confirmer la phrase secrète de l'utilisateur**. L'indicateur de **qualité de la phrase secrète** indique le niveau de sécurité de la phrase secrète saisie. Cochez la case **Afficher les frappes** si vous souhaitez voir les caractères tapés.

- 3 Cliquez sur **OK**. L'écran Propriétés du disque réapparaît ; l'autre utilisateur de clé publique ou l'autre utilisateur de phrase secrète est affiché dans la liste B.

Suppression de comptes d'autres utilisateurs 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.

► Pour supprimer le compte d'un autre utilisateur d'un PGP Virtual Disk

- 1 Cliquez sur PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk dont le compte d'utilisateur doit être supprimé.
- 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 le signe moins situé sous la liste **Accès de l'utilisateur**. Une boîte de dialogue de confirmation apparaît.
- 4 Cliquez sur **Supprimer**. L'autre utilisateur est supprimé.

Désactivation et activation de comptes d'autres utilisateurs

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.

► Pour désactiver ou activer un compte d'autre utilisateur sur un PGP Virtual Disk

- 1 Cliquez sur PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk dont le compte d'utilisateur doit être modifié.
- 2 Dans la liste **Accès de l'utilisateur**, sélectionnez l'autre utilisateur à désactiver ou à activer. Vous ne pouvez pas désactiver l'administrateur.
- 3 Effectuez l'une des opérations suivantes :
 - Pour désactiver un utilisateur, sélectionnez **Disque > Désactiver un utilisateur**. Une boîte de dialogue de confirmation apparaît. Cliquez sur **Désactivé**. L'autre utilisateur est désactivé. L'utilisateur apparaît en grisé dans la liste **Accès de l'utilisateur**.
 - Pour activer un utilisateur que vous avez précédemment désactivé, sélectionnez **Disque > Activer un utilisateur**. L'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.

► Pour modifier les droits d'un utilisateur sur un PGP Virtual Disk

- 1 Cliquez sur PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk dont le compte d'utilisateur doit être modifié.
- 2 Dans la liste **Accès de l'utilisateur**, sélectionnez le nom de l'autre utilisateur dont l'état lecture/écriture est à modifier.
- 3 Effectuez l'une des opérations suivantes :
 - Pour accorder à l'utilisateur l'accès en lecture seule, appuyez sur Ctrl et cliquez (ou cliquez avec le bouton droit) sur son nom et sélectionnez **Définir l'accès en lecture seule**.
 - Pour accorder à l'utilisateur l'accès en lecture/écriture, appuyez sur Ctrl et cliquez (ou cliquez avec le bouton droit) sur son nom et sélectionnez **Accorder l'accès en écriture**.

Conseil : ces options sont également disponibles dans le menu Disque, lorsque l'utilisateur est sélectionné.

- 4 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

► Pour attribuer le statut administrateur

- 1 Cliquez sur PGP Disk dans le panneau gauche de l'écran principal de PGP Desktop, puis sélectionnez le PGP Virtual Disk dont le compte d'utilisateur doit être modifié.
- 2 Dans la liste Accès de l'utilisateur, sélectionnez l'utilisateur que vous souhaitez définir en tant qu'administrateur du PGP Virtual Disk. Sélectionnez un utilisateur de phrase secrète ou vous-même (si vous n'êtes pas l'administrateur actuel). Remarque : vous ne pouvez pas définir un utilisateur de clé publique comme administrateur du PGP Virtual Disk.
- 3 Tout en maintenant la touche Ctrl enfoncée, appuyez sur le bouton gauche (ou appuyez sur le bouton droit si vous utilisez une souris à deux boutons) et sélectionnez **Définir en tant qu'administrateur du disque** dans le menu contextuel. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.

Conseil : vous pouvez également sélectionner **Disque > Définir en tant qu'administrateur du disque**.

- 4 Saisissez la phrase secrète de l'administrateur du volume PGP Virtual Disk et cliquez sur **OK**. Le statut administrateur est attribué au compte d'utilisateur sélectionné.

Remarque : vous ne pouvez attribuer le statut administrateur qu'à un seul compte d'utilisateur à la fois. En accordant le statut administrateur à un compte, vous en privez un autre compte.

Modification des phrases secrètes des utilisateurs

► Pour modifier la phrase secrète d'un utilisateur pour un PGP Virtual Disk

- 1 Sélectionnez 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 choisissez **Modifier phrase secrète utilisateur** dans le menu **Disque**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche.

Conseil : vous pouvez également appuyer sur Ctrl et cliquer (ou 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 de l'administrateur du volume PGP Virtual Disk et cliquez sur **OK**.
- 4 Saisissez une nouvelle phrase secrète, puis ressaisissez-la pour confirmation et cliquez sur **OK**. La phrase secrète est modifiée.

Suppression de volumes PGP Virtual Disk

Il se peut qu'un jour vous décidiez n'avoir plus besoin d'un volume 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 avez supprimé le volume PGP Virtual Disk.* Veuillez à copier celles à conserver à un autre emplacement *avant de supprimer le volume*.

Assurez-vous que le volume sélectionné n'est *pas* monté. Vous ne pouvez pas supprimer un volume PGP Virtual Disk monté.

► Pour supprimer un volume PGP Virtual Disk

- 1 Sélectionnez le panneau de contrôle PGP Disk situé sur la gauche de l'écran principal de PGP Desktop, puis choisissez le volume PGP Virtual Disk à supprimer.
- 2 Dans le menu contextuel, sélectionnez **Afficher dans le Finder**. Le fichier correspondant au volume PGP Virtual Disk apparaît en surbrillance dans une fenêtre du Finder. Si vous avez choisi d'afficher les extensions de fichier dans Mac OS X, vous verrez que celui-ci porte l'extension .pgd.
- 3 Faites glisser le fichier vers la corbeille et, dans le menu Fichier du Finder, sélectionnez l'option **Vider la Corbeille**.
- 4 Dans PGP Desktop, cliquez sur le volume PGP Virtual Disk à supprimer en maintenant la touche Ctrl enfoncée (ou cliquez dessus avec le bouton droit si vous possédez une souris à deux boutons) et, dans le menu contextuel, sélectionnez **Supprimer l'élément**. Le volume est supprimé à la fois du système et de PGP Desktop.

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 volume PGP Virtual Disk sous forme chiffrée

- 1 Démontez le volume.
- 2 Dans le Finder, recherchez le fichier correspondant à ce volume PGP Virtual Disk. Si vous avez choisi d'afficher les extensions de fichier dans Mac OS X, localisez un fichier dont le nom se termine par `.pgd`.

Conseil : pour trouver facilement le fichier PGP Virtual Disk, appuyez sur la touche Ctrl et, tout en la maintenant enfoncée, cliquez sur le disque dans le panneau latéral de PGP Desktop (si vous avez une souris à deux boutons, vous pouvez aussi cliquer sur le disque à l'aide du bouton droit). Dans le menu contextuel qui apparaît, sélectionnez **Afficher dans le Finder**.

- 3 Copiez le fichier PGP Virtual Disk chiffré démonté sur un CD, un DVD, une bande, une cartouche amovible ou une disquette, comme vous le feriez avec n'importe quel autre fichier.

Même si une personne non autorisée a accès à la sauvegarde, elle ne sera pas en mesure de déchiffrer son contenu.

Lorsque vous faites des sauvegardes de fichiers PGP Virtual Disk 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 votre ordinateur fait partie d'un réseau, assurez-vous qu'aucun système de sauvegarde réseau ne sauvegarde les fichiers à partir de votre volume PGP Virtual Disk *monté*. (Il se peut que vous deviez en discuter avec votre administrateur système.) Une fois qu'un volume PGP Virtual Disk est monté, les fichiers qu'il contient sont déchiffrés et peuvent être copiés sur un système de sauvegarde réseau, mais sont vulnérables.

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 privée 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.

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.

13

Accès aux données mobiles 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 un système Mac OS X, vous pouvez *accéder* aux données chiffrées stockées sur un disque PGP Portable.

Contenu du chapitre

Accès aux données sur un disque PGP Portable 187

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 Desktop Disk sur un système Mac OS X**

- 1 Insérez le périphérique amovible sur lequel réside le PGP Desktop Disk. Il peut s'agir d'un CD/DVD, ou d'un lecteur Flash ou amovible.
- 2 Ouvrez le périphérique amovible monté et recherchez l'application PGP Desktop (PGP Portable). Double-cliquez sur cette application. La boîte de dialogue PGP Portable apparaît.



- 3 Saisissez la phrase secrète d'accès au PGP Desktop Disk.
- 4 Lorsque la phrase secrète correcte a été saisie, le PGP Desktop Disk est 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 est unique pour les PGP Desktop Disks et peut être différent du nom du volume lors de sa création.

- 5 Lorsque vous avez fini d'utiliser le PGP Desktop Disk, démontez-le (dans la station d'accueil, cliquez sur l'icône PGP Desktop, puis sur **Démonter**). Le lecteur monté pour le PGP Desktop Disk est démonté.
- 6 Éjectez correctement le périphérique USB ou le disque de votre ordinateur.

Avertissement : avant de retirer un périphérique amovible du système, veillez à le démonter correctement. Sinon, vous risquez d'endommager le contenu des fichiers présents sur ce support.

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 Desktop sur un système Mac OS X :

- 1 Insérez le périphérique amovible sur lequel réside le PGP Desktop Disk. Il peut s'agir d'un CD/DVD, ou d'un lecteur Flash ou amovible.
- 2 Ouvrez le périphérique amovible et recherchez l'application PGP Desktop (PGP Portable). Double-cliquez sur l'application et, à l'invite, saisissez la phrase secrète pour l'accès au PGP Desktop Disk. Lorsque la phrase secrète correcte a été saisie, le PGP Desktop Disk est monté.
- 3 Pour ouvrir PGP Desktop, cliquez sur la station d'accueil et, dans la boîte de dialogue de PGP Desktop, cliquez sur **Modifier la phrase secrète**.
- 4 Saisissez la phrase secrète actuelle, appuyez sur Entrée, confirmez la nouvelle phrase secrète, puis cliquez sur **Modifier**.

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.

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	191
Création d'archives PGP Zip	192
Ouverture d'une archive PGP Zip	194
Vérification des archives PGP Zip signées	194

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.

Lors de la création d'une archive PGP Zip, vous avez la possibilité de configurer l'application de sorte que les fichiers d'origine soient automatiquement supprimés du système (décomposés) une fois que l'archive a été créée. Lorsque vous recevez une archive PGP Zip, vous pouvez extraire soit l'ensemble des fichiers et/ou dossiers qu'elle inclut, soit uniquement ceux dont vous avez besoin.

Les archives PGP Zip que vous créez doivent être :

- **chiffrées avec une clé publique** : si vous envoyez l'archive PGP Zip à un ou plusieurs destinataires dont vous possédez les clés publiques, vous devez la chiffrer avec ces clés ; par conséquent, seuls ces derniers seront en mesure de l'ouvrir. Les destinataires doivent avoir installé PGP Desktop sur leur ordinateur.
- **chiffrées avec une phrase secrète** : si vous préférez chiffrer l'archive avec une phrase secrète ou l'envoyer à plusieurs destinataires, mais que vous ne disposez pas de la clé publique de toutes ces personnes, vous pouvez opter pour un chiffrement conventionnel et chiffrer l'archive à l'aide d'une phrase secrète. Le cas échéant, vous devrez communiquer cette phrase aux destinataires pour qu'ils puissent ouvrir l'archive. Ceux-ci doivent avoir installé PGP Desktop sur leur ordinateur.

Les archives PGP Zip sont chiffrées avec le chiffrement par défaut pour PGP Desktop (s'il a été configuré par un administrateur de PGP) ou avec AES 256. Elles peuvent être déplacées librement entre les plates-formes Mac OS X et Windows. PGP Desktop doit être installé sur le système de destination.

Création d'archives PGP Zip

► Pour créer une archive PGP Zip

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

Si vous ajoutez un fichier ou un dossier et vous apercevez par la suite que vous n'en avez plus besoin, sélectionnez-le dans la liste et cliquez sur le signe « moins » situé au-dessous. Le fichier ou dossier est alors supprimé de la liste.

- 4 Pour supprimer en toute sécurité de votre système les fichiers ou dossiers que vous placez dans l'archive PGP Zip, choisissez l'option **Décomposer les fichiers originaux**.
- 5 Lorsque vous avez précisé les fichiers ou dossiers à inclure dans l'archive, cliquez sur l'onglet **Sécurité**.

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

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

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

- 7** Sélectionnez le type de chiffrement à employer :

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

Si vous optez pour un chiffrement par clé publique, faites glisser les clés publiques des destinataires sur la liste, ou cliquez sur le signe « plus » et sélectionnez les clés publiques des destinataires souhaités.

- **Chiffrer avec la phrase secrète uniquement** : cette option permet de chiffrer l'archive PGP Zip à l'aide d'une phrase secrète que vous fournissez lors de l'enregistrement de l'archive. Seules les personnes qui connaissent la phrase secrète peuvent ouvrir l'archive. N'oubliez pas de communiquer cette phrase secrète aux personnes auxquelles vous voulez donner accès à l'archive.

Saisissez-la dans le champ **Phrase secrète**, puis retapez-la dans le champ **Confirmer**. Pour que la phrase secrète s'affiche à mesure que vous saisissez les caractères, sélectionnez **Afficher les frappes**.

- **Signer uniquement (aucun chiffrement)** : cette option permet de créer une archive PGP Zip non chiffrée. Néanmoins, étant donné que vous ne chiffrez pas l'archive, vous devez spécifier une clé de signature dans le champ **Signature**.

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

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

- 9** Cliquez sur **Enregistrer**.

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

- 11** Saisissez la phrase secrète, puis cliquez sur **OK**. L'archive PGP Zip est créée à l'emplacement indiqué.

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 l'archive et effectuez l'une des opérations suivantes :
 - Si l'archive a été chiffrée à l'aide de votre clé publique, vous devez saisir la phrase secrète associée à votre clé privée, qui sera utilisée pour déchiffrer l'archive (si la phrase secrète est déjà en cache, il est inutile de l'indiquer). Entrez la phrase secrète et cliquez sur **OK**.
 - Si l'archive a été chiffrée avec une phrase secrète, il vous faut fournir celle-ci. Entrez la phrase secrète et cliquez sur **OK**.

Si l'archive a en outre été signée, PGP Desktop vérifie la signature ; à l'issue du processus, un écran de vérification présentant les résultats apparaît.

- 2 Si l'archive PGP Zip comprend au moins deux fichiers/dossiers, un dossier les regroupant est créé.

En revanche, si elle ne compte qu'un seul fichier, seul ce dernier est créé à l'emplacement de l'archive.

Vérification des archives PGP Zip signées

Si vous avez reçu une archive PGP Zip *signée*, **vous devez la vérifier pour déterminer son expéditeur et vous assurer qu'elle n'a pas été falsifiée avant sa réception. Les fichiers non signés ne peuvent pas être vérifiés.**

► Pour vérifier une archive PGP Zip signée

- 1 Dans PGP Desktop, sélectionnez **Afficher > Infos de vérification**. L'écran Infos de vérification apparaît.
- 2 Faites glisser le fichier PGP Zip (.pgp) signé à vérifier sur la zone **Déplacez les fichiers signés ici**. PGP Desktop vérifie la signature et présente les informations de vérification.
- 3 Pour effacer la liste des archives vérifiées, cliquez sur **Effacer**. Toutes les listes figurant dans l'écran Infos de vérification sont alors 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..... 195

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. "Préférences liées aux disques" à la page 208).

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. Lors de l'installation de PGP Desktop, la fonction PGP Shredder a été installée dans le même répertoire que PGP Desktop. La création d'un alias vers l'icône PGP Shredder et le déplacement de cet alias vers la station ou le Bureau font de PGP Shredder un outil facile et pratique à utiliser.
- Utilisez l'icône PGP Shredder dans la barre d'outils PGP. Cliquez sur l'icône PGP Shredder dans la barre d'outils, puis accédez au dossier/fichier à décomposer.
- Sélectionnez **Fichier > Décomposer**, puis accédez au dossier/fichier à décomposer.
- Utilisez les menus contextuels du Finder (cliquez en maintenant la touche Ctrl enfoncée ou cliquez avec le bouton droit sur le fichier ou le dossier) et sélectionnez **PGP > Décomposer**.

Attention : certains systèmes de fichiers utilisent une fonction appelée Journalisation. Apple a introduit cette fonction pour les systèmes de fichiers Mac OS Extended (HFS+) dans Mac OS X 10.2.2. Avec la journalisation, une copie de tous les éléments enregistrés sur le disque est placée dans une zone privée du système de fichiers. Par conséquent, la décomposition du fichier d'origine s'accompagne de l'enregistrement des données de ce fichier sur une autre partie du disque. Pour éviter cela, *n'utilisez pas la fonction de journalisation*. Vous pouvez désactiver cette fonction à l'aide de l'utilitaire de disque Apple. Pour plus d'informations sur la journalisation du système de fichiers, reportez-vous à l'article 107249 du support technique d'Apple (<http://docs.info.apple.com/article.html?artnum=107249>).

Conseil : un grand nombre de programmes enregistrent automatiquement les fichiers en cours ; il existe donc peut-être des copies de sauvegarde du fichier supprimé. Une fois la copie principale d'un fichier supprimée, PGP Corporation vous recommande d'utiliser la fonction PGP Shredder pour supprimer en toute sécurité les copies de sauvegarde.

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

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

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

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

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

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

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

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

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

- 1 Sélectionnez **Fichier > Décomposer**.

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

Décomposition de fichier dans le Finder

► Pour décomposer un fichier ou un dossier dans le Finder

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

16

Définition des préférences 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 aux préférences de PGP Desktop	199
Préférences générales	200
Préférences de clés	202
Préférences de clés principales	204
Préférences de messagerie	205
Préférences liées aux disques	208
Préférences relatives aux notifications	210
Préférences avancées.....	212

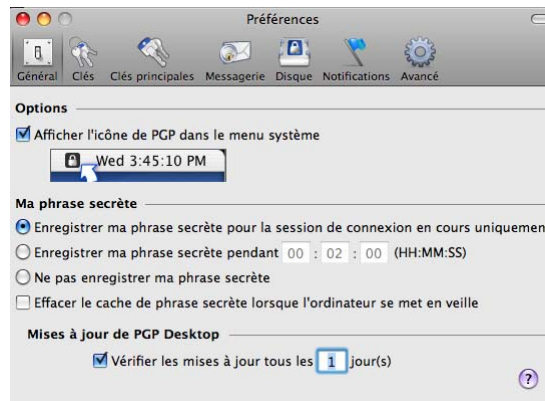
Accès aux préférences de PGP Desktop

► Pour accéder aux préférences de PGP Desktop

- 1 Ouvrez PGP Desktop.
- 2 Sélectionnez **PGP > Préférences**.
 - Pour accéder aux divers types de préférences, cliquez sur les icônes situées en haut de la boîte de dialogue Préférences.
- 3 Une fois les préférences définies, cliquez sur le bouton de fermeture (rond rouge dans l'angle supérieur gauche de l'écran).

Préférences générales

La boîte de dialogue des préférences générales couvre différents paramètres de PGP Desktop.



Les options de la page Général de la boîte de dialogue des préférences sont les suivantes :

- **Afficher l'icône de PGP dans le menu système** : lorsque cette case est cochée, l'icône PGP Desktop s'affiche dans la barre de menu MAC OS S quand PGP Desktop est actif sur le système. L'icône de la barre de menus PGP permet d'accéder rapidement aux fonctionnalités de PGP Desktop.
 - Pour supprimer l'icône de PGP Desktop dans la barre de menus, désélectionnez cette case à cocher.
 - Pour restaurer l'icône de PGP Desktop dans la barre de menus, accédez à l'écran des préférences générales et cochez l'option **Afficher l'icône de PGP dans le menu système**.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, activez cette option.

La suppression de l'icône PGP Desktop de la barre de menus n'a *pas* pour effet d'arrêter les services PGP Desktop ; ils restent actifs en arrière-plan.

- Pour arrêter les services PGP Desktop, cliquez sur **Option**. Dans la barre de menus, cliquez sur l'icône PGP Desktop, puis sélectionnez **Quitter**.

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 de connexion en cours uniquement** : 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 ressaisir pour la même clé jusqu'à la fermeture de la session.

Attention : lorsque cette option est activée, il est essentiel que vous fermiez votre session si vous vous absentez. (Pour fermer la session, sélectionnez l'option de fermeture de session de [votre nom] **dans le menu Apple.**) **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 lorsque vous n'êtes pas devant votre ordinateur. 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 pour** : 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 ressaisir avant la fin de la durée définie. Les trois champs numériques sont destinés aux **heures, minutes, secondes**, respectivement. La valeur par défaut est de deux 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.
- **Effacer le cache de phrase secrète lorsque l'ordinateur se met en veille** : activez les préférences pour que PGP Desktop supprime les phrases secrètes de la mémoire lorsque l'ordinateur passe en veille. (Tous les ordinateurs ne sont pas dotés du mode Veille.)
- **Vérifier les mises à jour tous les X jour(s)** : lorsque cette case est cochée, PGP Desktop recherche les mises à jour logicielles automatiquement, selon l'intervalle spécifié. L'intervalle par défaut est de un jour. Si une version plus récente de PGP Desktop est disponible, un écran de notification vous en informe et vous permet de la télécharger. Si cette option est désactivée, PGP Desktop ne recherche pas automatiquement les mises à jour logicielles.

Cette option nécessite une connexion Internet active et opérationnelle.

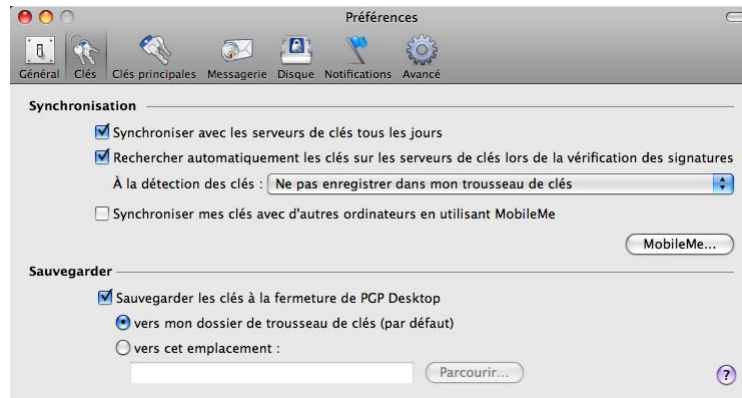
Une fois la mise à jour téléchargée, suivez les invites pour l'installer.

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 de droits d'administration sur votre système.

Préférences de clés

La boîte de dialogue Préférences de clés contient des paramètres applicables aux clés PGP Desktop.



Les options de la page Clés 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 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, ce dernier désactive cette clé sur le trousseau de clés local.

Si vous modifiez une clé publique 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 avec le bouton droit, sélectionner **Envoyer vers** dans le menu contextuel, puis choisir le serveur de clés dans la liste.

- **Rechercher automatiquement les clés sur les serveurs de clés lors de la vérification des signatures** : lorsque cette option est activée, vous pouvez indiquer à PGP Desktop de rechercher la clé publique demandée sur les serveurs de clés configurés quand vous recevez un message électronique signé avec une clé privée et que vous ne disposez *pas* de la clé publique correspondante 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 sur votre trousseau de clés.

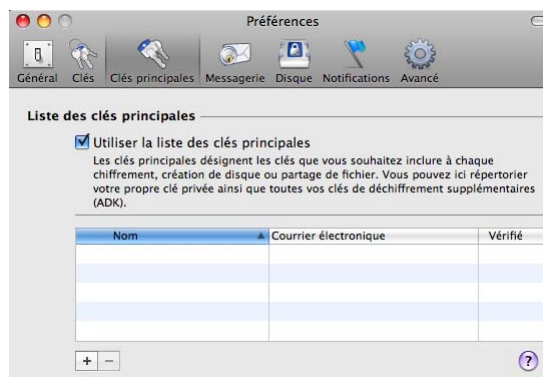
Si la clé publique est identifiée sur le serveur de clés, trois options sont disponibles :

- **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 mes clés avec d'autres ordinateurs en utilisant MobileMe** : (MobileMe est la nouvelle version Apple de Mac.) Cochez cette case pour synchroniser vos clés à l'aide de votre compte MobileMe. (Pour utiliser cette option, vous devez disposer d'un compte valide.) Lorsque cette option est sélectionnée, le moteur de synchronisation exécute et copie vos fichiers de clés dans un cache local que MobileMe utilise pour la mise à jour.
- Pour synchroniser immédiatement vos clés avec votre compte MobileMe, cliquez sur **MobileMe**. Le panneau des préférences système MobileMe s'affiche. Ouvrez une session, cliquez sur le panneau de synchronisation, sélectionnez l'option Clés PGP dans la liste, puis cliquez sur l'option de synchronisation.
- **Sauvegarder** : ces paramètres définissent l'emplacement de sauvegarde des clés et à quel moment l'effectuer.
- **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.
- **vers cet emplacement** : lorsque cette option est activée, vos clés sont sauvegardées à l'emplacement défini sur votre ordinateur. Cliquez sur **Parcourir** pour définir un emplacement.

Préférences 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 et PGP Zip. Elle vous permet de ne pas avoir à faire glisser dans le champ **Destinataires** les clés que vous utilisez régulièrement.

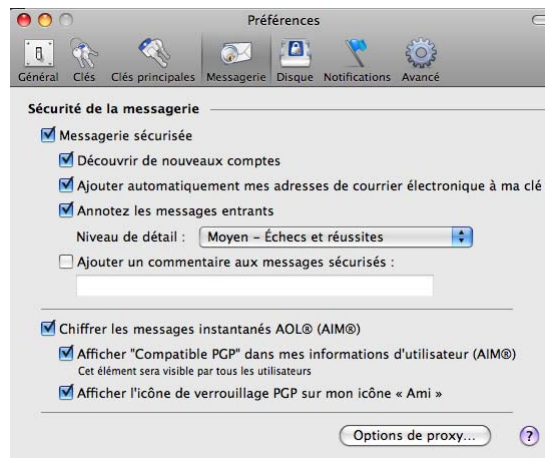


Pour utiliser la liste des clés principales, cochez la case **Utiliser la liste des clés principales**. Vous ne pouvez pas ajouter de clés à cette liste, ni en supprimer, si vous n'avez pas coché cette case.

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.

Préférences de messagerie

Le panneau des préférences de messagerie **contient des paramètres applicables à la sécurité de la messagerie. Il permet également d'accéder aux paramètres de la messagerie et de la messagerie instantanée.**



Les préférences de **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. Il sécurise ensuite les messages envoyés à ces comptes.

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.

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.

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 client compatible. L'autre participant à la session de messagerie instantanée doit également utiliser PGP Desktop.

AOL® Instant Messenger™ et iChat 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.
- Cliquez sur le bouton **Options de proxy** pour accéder aux paramètres de messagerie avancés.

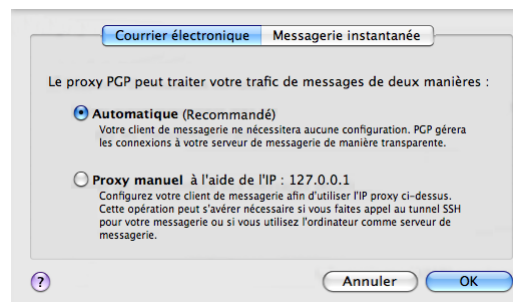
Options de proxy

Cliquez sur **Options de proxy** pour accéder aux préférences avancées des messageries électronique et instantanée.

Préférences de messagerie :

utilisez cette fonction si vous devez configurer un proxy manuellement sur votre ordinateur afin de pouvoir envoyer et recevoir des messages électroniques.

PGP Desktop « intervient » 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.

Préférences de 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.



- **Remplacer le port de destination** : 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 modifier ce paramètre, et le cas échéant, le numéro de port à utiliser.

Préférences liées aux disques

Le panneau **Disque** de l'écran Préférences contient des paramètres applicables aux volumes protégés à l'aide des fonctionnalités PGP Virtual Disk et PGP Shredder.



Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, ces préférences peuvent être déjà configurées.

Les préférences relatives aux **disques** sont les suivantes :

- **Autoriser le démontage des PGP Disks même si certains fichiers sont 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 ; c'est ce que l'on appelle le démontage forcé.

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** : lorsque cette case est cochée, PGP Desktop démonte automatiquement les volumes PGP Virtual Disk lorsque votre ordinateur se met en veille.
 - **Échec du mode veille si le démontage du disque ou des disques est impossible** : ce paramètre n'est actif que si vous avez coché la case **Démonter lorsque l'ordinateur se met en veille** au préalable. Il empêche l'ordinateur de se mettre en mode veille si un volume PGP Virtual Disk ne peut pas être démonté.
- **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. Le paramètre par défaut est **3**. 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).

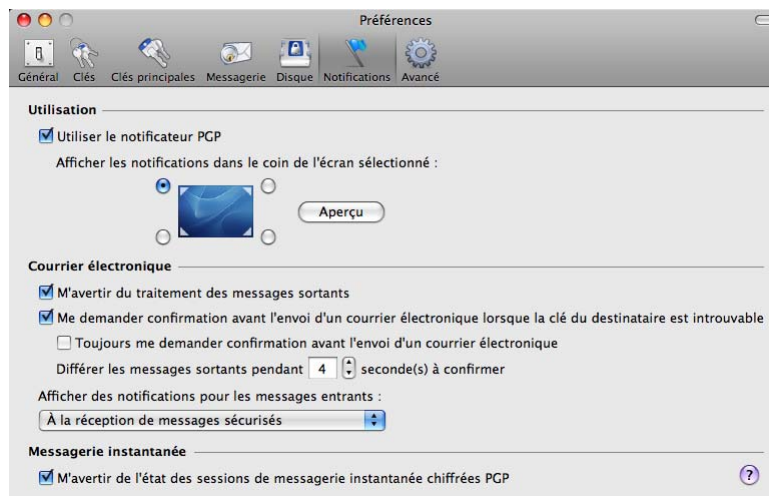
Sachez que le coût de cette plus grande sécurité est l'augmentation du temps nécessaire pour décomposer vos fichiers, qui dépend de plusieurs facteurs, en particulier la rapidité du processeur de votre ordinateur.

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.
- **Toujours m'avertir avant une décomposition** : cochez cette case si vous voulez qu'une boîte de dialogue de confirmation s'affiche avant chaque décomposition. Ainsi, vous pourrez vous assurer que seuls les fichiers appropriés sont décomposés. Cette option est sélectionnée par défaut.

Préférences relatives aux notifications

Le panneau **Notifications** dans la boîte de dialogue des préférences 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 de disques de PGP Desktop.



Les préférences relatives aux **Notifications** sont les suivantes :

- **Utiliser le notificateur PGP** : les notifications de PGP Desktop peuvent s'afficher dans l'un des quatre angles de l'écran. Indiquez l'angle dans lequel vous souhaitez les voir apparaître. Cliquez sur **Aperçu** pour voir l'aspect de la fenêtre d'alerte dans l'angle choisi.
- **M'avertir du traitement des messages sortants** : cochez cette case si vous souhaitez que des notifications de PGP Desktop vous informe de l'état du chiffrement et/ou de la signature lors de l'envoi de courrier électronique. Décochez cette case 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 en êtes informé et avez la possibilité de bloquer l'envoi du message.

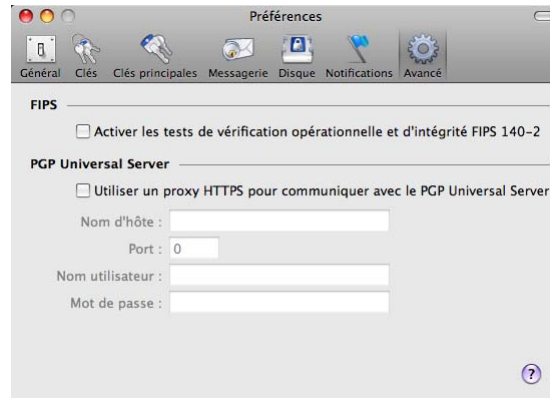
Pour plus d'informations sur les paramètres de stratégie par défaut de PGP Desktop, reportez-vous à *Services et stratégies* (à la page 95).

- **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 la zone de notification de PGP Desktop et choisir d'envoyer ou de bloquer le message.

- **Différer les messages sortants pendant n seconde(s) à confirmer** (où *n* est un chiffre entre 1 et 30 ; la valeur par défaut est de 4 secondes). Cochez cette case, si vous souhaitez être averti par une notification de PGP Desktop pour chaque message envoyé, mais ne voulez pas avoir à confirmer chaque envoi. L'envoi du message est retardé et une notification s'affiche selon la durée indiquée. Si vous n'effectuez aucune action, le message est envoyé une fois le temps spécifié écoulé. Pour consulter la notification de PGP Desktop, déplacez votre curseur sur celle-ci. La notification prend un aspect opaque et l'envoi du message est retardé pendant que vous vérifiez les informations qu'elle contient. Vous pouvez ensuite autoriser l'envoi du message ou le bloquer.
- **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** : la fenêtre du notificateur PGP Desktop s'affiche à la réception d'un message sécurisé. Elle indique l'expéditeur, l'objet du message, l'état de chiffrement et de vérification et l'adresse de courrier électronique de l'expéditeur.
 - **Uniquement en cas d'échec de vérification du message** : la fenêtre du notificateur s'affiche uniquement lorsque PGP Desktop est incapable de vérifier la signature du message entrant.
 - **Jamais** : si vous ne souhaitez pas que la fenêtre du notificateur PGP Desktop apparaisse lors de la réception de messages, sélectionnez cette option. Cela n'a aucune incidence sur la notification des messages sortants.
- **M'avertir de l'état des sessions de messagerie instantanée chiffrées PGP** : lorsque vous cochez cette case, la fenêtre du notificateur PGP Desktop apparaît brièvement au début et à la fin d'une conversation sécurisée de messagerie instantané.

Préférences avancées

Le panneau Préférences **avancées** contient des paramètres qui doivent être modifiés par la plupart des utilisateurs.



Les préférences **avancées** sont les suivantes :

- **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.
- **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.

A

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 ?	213
Indicateur de qualité de la phrase secrète	214
Création de phrases secrètes fortes.....	215
Que faire si vous avez oublié votre phrase secrète ?	217
Enregistrement de votre phrase secrète dans la chaîne de clé.....	217

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 à 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 85, "Perte de votre clé ou phrase secrète" à la page 85) et contactez votre administrateur PGP.

Enregistrement de votre phrase secrète dans la chaîne de clé

Si vous le souhaitez, vous pouvez placer vos phrases secrètes de clés en mémoire cache à l'aide de la chaîne de clé Mac OS X. Lorsque vous êtes invité à indiquer une phrase secrète, cochez la case **Enregistrer la phrase secrète dans la chaîne de clé**. Vous pouvez alors accéder à toutes les fonctionnalités de PGP Desktop sans avoir à taper votre phrase secrète à chaque fois.

Les sous-clés sont également enregistrées dans la chaîne de clé Mac OS X. Les actions liées à ces sous-clés sont donc automatiques lorsque la chaîne de clé est déverrouillée.

B

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	220
À l'attention des administrateurs PGP	221
Liaison manuelle à un PGP Universal Server	221

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 4).

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).

Index

•

.Mac, synchronisation de clés avec - 202

A

activation des clés publiques - 68

administrateur PGP - 158, 219, 220

AES, algorithme dans PGP Virtual Disk - 183

affichage des sous-clés - 73

archives PGP Zip

création - 192

description - 191

Effacer l'historique des vérifications - 194

extraire dans le Finder - 43

ouverture - 194

vérification de la signature - 194

attribution de confiance - 72

attribution de confiance pour les validations de
clés - 73

authentification dans PGP Whole Disk

Encryption

méthode utilisée, définition - 147

Automatique, mode - 207

B

barre de menus, icône - 29

biométriques, liste de mots - 63

BootGuard - See PGP BootGuard, écran

C

caractères génériques, dans les stratégies - 110

caractères pris en charge dans PGP WDE - 148

carte à puce - 13

CAST, algorithme dans PGP Virtual Disk - 183

certificats X.509, ajout à la paire de clés - 67

chaîne de clé, enregistrement de la phrase
secrète dans - 217

chiffrement

ajout d'utilisateurs - 154

algorithme utilisé - 183

calcul de la durée dans PGP WDE - 146

disques ou partitions - 149

erreurs de disques lors du chiffrement - 151

nouveau chiffrement du disque ou de la
partition - 156

suppression d'utilisateurs à partir de PGP
WDE - 155

test pilote - 147

utilisation d'un disque chiffré par PGP WDE -
158

chiffrement conventionnel - 38

chiffrer

dans le Finder - 38

chiffrer et signer

dans le Finder - 38

clavier pris en charge dans PGP WDE - 145

clé ou phrase secrète perdue - 85

clé, reconstruction - 23, 85, See reconstruction
de la clé

clés - 45, 63

- activation - 68
- adresses de courrier électronique, ajout - 66
- attribution de confiance pour les validations - 72, 73
- définition de la taille de - 76
- désactivation - 68
- distribution, publique - 54
- enregistrement de clé publique dans un fichier - 56
- exportation - 56
- Finder, ajout - 42
- message électronique, inclusion dans - 56
- modification de phrase secrète - 67
- noms, ajout - 66
- perdues - 85
- plusieurs noms d'utilisateur et adresses de courrier électronique - 65
- préférences - 202
- protection - 89
- réassemblage d'une clé scindée - 82, 83
- reconstruction - 85
- remplacement d'un ID photo - 64
- révocation - 80, 81
- scission - 82
- serveur de clés, chargement vers - 56
- signature - 70
- sous-clés - 73
- suppression de votre trousseau de clés - 67, 68
- synchronisation, préférences de clés - 202
- vérification publique - 69
- Clés de déchiffrement supplémentaires (ADK) - 78
- Clés PGP - See clés
 - affichage - 46
 - ajouter au trousseau de clés dans le Finder - 42
 - création d'une paire de clés - 48
 - importer dans le Finder - 42
 - paramètres de clé - Mode Expert - 50
- clés privées - 13, 51
- clés publiques - 13

- activation et désactivation - 68
- avantages de l'envoi de clés au serveur de clés - 54
- confiance - 73
- copie à partir de messages électroniques - 59
- distribution à d'autres - 54
- enregistrement dans un fichier - 56
- envoi vers le serveur de clés - 54
- exportation vers des fichiers - 56
- importation depuis les fichiers - 64
- inclusion dans un message électronique - 56
- obtention d'autres - 57
- obtention depuis un serveur de clés - 58
- recherche dans le serveur de clés - 57, 58
- signature - 70
- vérification - 69
- compactage, PGP Virtual Disk - 175
- confiance
 - attribution pour les validations de clés - 73
 - clés publiques - 73
- confiance, attribution pour les validations de clés - 72
- configuration requise - 19
- connexion, écran PGP BootGuard - 152
- création - 48, 215
 - nouveau volume PGP Virtual Disk - 169
 - phrases secrètes fortes - 215
 - service de messagerie - 97
 - stratégie de messagerie - 104
- cryptographie - 15

D

- déchiffrer et vérifier
 - dans le Finder - 40
- Décomposer par PGP - 11, 195
 - description - 195
- décomposition
 - dans le Finder - 40
 - description - 195
- décomposition de l'espace libre - 11
- default policies - 95, 111, 112, 113
- dépannage - 102
- déplacement de PGP Desktop vers un autre ordinateur - 24
- désactivation des clés publiques - 68
- désinstallation - 24, 157
- diagnostic, récupération des données - 160
- disques

- ajout d'utilisateurs aux disques chiffrés - 154
- amovible - 162
- chiffrement - 148, 149
- chiffrés, utilisation - 151
- erreurs lors du chiffrement - 151
- pris en charge dans PGP WDE - 144
- disques amovibles dans PGP WDE - 162
- disques de démarrage, chiffrement - 142, 166
- disques virtuels - See PGP Virtual Disk
- distribution des disques virtuels - 182
- Dock, icône - See PGP Dock, icône

E

- échange de disques virtuels - 182
- effacement de fichiers - See décomposition de l'espace libre
- Effacer l'historique des vérifications - 194
- empreinte numérique, vérification - 69
- encrypting IM sessions - 91, 129, See Messagerie PGP
- Entourage 2004, intégration à - 23
- erreur de lecture/écriture du disque - 148
- erreur de lecture/modification du disque - 148
- exportation
 - clé vers un fichier - 56
- extraction d'archives Zip PGP dans le Finder - 43

F

- fichiers
 - exportation de clés publiques - 56
 - importation de clés publiques - 64
- Finder, accès depuis - 32, 37

I

- ID photo - 64
 - ajout - 64
 - suppression - 64
 - suppression à partir d'une clé - 64
- importation
 - clé PGP dans le Finder - 42
 - clés publiques, depuis des fichiers - 64
- indicateur de qualité de la phrase secrète - 214
- installation - 24
- installation de PGP Desktop - 19
- instructions d'utilisation basiques - 15

J

- journal de la messagerie - 126
- Journal de la messagerie - 126
- Journal de PGP - 126

- journal, messagerie - 126

L

- lecture/écriture, erreur - 148
- licences - 142
- licences à abonnement - 5
- licences définitives - 5
- licences d'évaluation - 5
- licensing - 5, 6, 23, 142
- liste de mots biométriques - 63
- Liste des serveurs de clés PGP - See serveurs de clés

M

- mailing list policies - 111, 112, 113
- menu Services
 - fonctionnalité PGP - 37
- message électronique - 91
 - copie de clés publiques - 59
 - inclusion d'une clé publique - 56
 - modes clé - 123
 - notificateurs - 32
 - plusieurs comptes - 101
 - sécurisation - 91
 - services et stratégies - 95
- message entrant - 92
- message sortant - 94
- messagerie - 95
 - dépannage - 102
 - multiple - 101
 - notificateurs - 32
- messagerie instantanée - 129
 - options - 208
- messagerie instantanée sécurisée - 129
- Messagerie PGP - 11, 91
 - création d'un service - 97
 - création d'une stratégie - 104
 - description des services - 95
 - journal - 126
 - services et stratégies - 95
- mise à niveau - 22
- mise en veille prolongée - See mode veille, Mac OS X et PGP WDE
- Mode clé client (CKM) - 123
- Mode clé client serveur (SCKM) - 123
- Mode clé de serveur (SKM) - 123
- Mode clé protégée (GKM) - 123
- mode veille, Mac OS X et PGP WDE - 165
- modes clé - 123
- modification

phrase secrète d'une clé - 67
votre phrase secrète - 67
modification de la phrase secrète - 66
montage des volumes PGP Virtual Disk - 173
mots de passe - See phrases secrètes

N

NetShare - See PGP NetShare
nettoyage de l'espace libre - See
décomposition de l'espace libre
nom principal, de la clé - 66
noms d'utilisateur, des clés - 65
Notificateur
description - 32
pour la messagerie instantanée - 35
pour les messages sortants - 34
pour messages entrants - 33
nouveau chiffrement - 156
nouveau chiffrement d'un disque - 156, 175

O

options - See preferences
options de chiffrement
conventionnel - 38
décomposer l'original - 38
MacBinary - 38
sortie de texte - 38
options de messagerie - 207
oubli de la phrase secrète - 85

P

paire de clés - 13
partitions, chiffrement - 154
PGP BootGuard, écran - 148, 152
PGP Desktop

accès via le Finder - 32
Assistant d'installation - 23
configuration requise - 19
dans un environnement géré par PGP
Universal - 220
description - 11
désinstallation - 24
écran principal - 27, 28
icône de la barre de menus - 29
icône de la zone de notification PGP - 29
installation - 19
mise à niveau - 21
Notificateur - 32
prise en charge SSL/TLS - 121
stratégies décrites - 95
PGP Disk
préférences - 208
PGP Dock, icône - 30
PGP Global Directory - 11
PGP NetShare - 11
PGP Universal - 4, 85, 219
PGP Universal Server - 11, 85, 158, 219, 221
PGP Virtual Disk - 11, 167, 184
algorithmes de chiffrement - 183
autres utilisateurs - 176
création - 169
création d'un volume - 169
démontage - 172
échange - 182
gestion - 181
montage - 173
monter dans le Finder - 41
monter le volume dans le Finder - 41
nouveau chiffrement - 175
précautions de sécurité - 184
propriétés - 172
sauvegarde - 181
suppression - 180
PGP Virtual Disk volumes - 172
PGP Whole Disk Encryption - 11

- affichage des informations sur la clé - 154
- ajout d'utilisateurs - 154
- chiffrement d'un disque - 148
- déchiffrement d'un disque chiffré - 162
- désinstallation - 157
- disque, continuité de la sécurité - 153
- disques amovibles - 162
- disques chiffrés, utilisation - 151
- durée du chiffrement, calcul - 146
- erreur de lecture/modification du disque - 148
- jetons de récupération - 159
- licences - 142
- logiciel de sauvegarde automatique - 157
- modification d'une phrase secrète - 156
- nouveau chiffrement - 156
- nouveau chiffrement d'un disque chiffré - 156
- options d'authentification - 147
- PGP Universal Server, géré - 158
- précautions de sécurité - 163
- préparation au chiffrement - 143
- préparation du disque - 143
- suppression d'utilisateurs - 155
- types de disques pris en charge - 144
- types de disques, pris en charge - 144
- utilisateurs, gestion - 154, 155, 156
- PGP Zip - 11, 191
- phrase secrète
 - ajout de phrases secrètes alternatives pour PGP Virtual Disk - 154
 - enregistrement dans la chaîne de clé - 217
 - modification - 67
 - modification d'une clé - 67
 - oubli - 217
- phrases secrètes - 184, 213
 - caractères pris en charge dans PGP WDE - 148
 - changing - 66, 156, 189
 - fortes, création - 215
 - oubli - 85
- phrases secrètes alternatives - 154, 176
- précautions de sécurité - 163, 184
- preferences - 137, 199
 - Clés - 202
 - Général - 200
 - Messagerie - 205
 - messagerie instantanée - 208
 - PGP Disk - 208
- Préférences de messagerie - 205
- préférences générales - 200
- présentation de PGP Desktop - 1

- protection des clés - 89
- protocole des services de PGP Universal (USP) - 59

Q

- qualité des phrases secrètes - 215

R

- réassemblage de clés scindées - 82, 83
- recherche dans le serveur de clés - 57, 58
- reconstruction de clés - 85
- reconstruction de la clé - 54, 85
- récupération des données à partir d'un lecteur chiffré - 160
- récupération, jetons - 159
- réinitialisation du mode clé - 123
- removable disks - 162, 163
- révocateur désigné - 80
- révocateurs de clés - 80
- révocation
 - clés - 81
 - signature, à partir d'une clé - 72
 - sous-clés - 77

S

- scission des clés - 82
- serveur de clés
 - envoi d'une clé publique - 54
 - obtention d'une clé publique - 58
 - propagation de clés révoquées - 81
 - recherche - 58
- serveurs de clés - 13
 - envoi d'une clé publique - 54
 - obtention d'une clé publique - 57
 - recherche - 57
- serveurs de messagerie, voir services de messagerie - See messagerie
- services - 95
 - activation - 100
 - affichage - 96
 - création - 97
 - désactivation - 100
 - suppression - 100
- services de messagerie - 95, 101
- services de messagerie multiples - 101
- signature - 67, 68
 - clés - 67, 70
 - clés publiques - 70
 - dans le Finder - 38
- signature numérique, suppression - 68

- signatures numériques - 54, 57, 67, 75, 89
- signatures, suppression des clés - 67
- sortie de texte - 38
- sous-clé de signature distincte - 11
- sous-clés - 73
 - affichage - 73
 - création - 76
 - définition de la taille de - 76
 - distincte - 73
 - expiration - 73, 76
 - icônes - 73
 - propriétés - 73
 - recherche - 75
 - révocation - 77
 - suppression - 78
 - symboles - 73
 - taille - 73
 - utilisation - 73
 - validité - 73
- SSL/TLS, prise en charge - 121
- stratégie hors connexion - 34, 94, 96
- stratégie locale - See stratégie hors connexion
- stratégies - 95
 - affichage - 96
 - création - 104
 - création d'une stratégie de messagerie - 104
 - exemples - 104
 - exemples de stratégie de messagerie - 111
 - modification - 115
 - stratégies par défaut - See default policies
 - suppression - 120
- support technique - 9
- support technique, contacter - 9
- support, contacter - 9
- suppression
 - clés - 67
 - clés de votre trousseau - 68
 - ID d'utilisateur - 67, 68
 - signatures numériques - 68
 - sous-clés - 78
 - un ID photo depuis une clé - 64
- synchronisation de clés - 202

T

- taille de clé
 - compromis - 76
 - définition - 76
- terminologie - 4, 11, 14, 95, 123
- trousseaux de clés - 52, 67
- Twofish, algorithme dans PGP Virtual Disk - 183

U

- Universal Server - See PGP Universal
- USP - See protocole des services de PGP Universal (USP)
- utilisateurs - 176
 - PGP Whole Disk Encryption, ajout ou suppression - 154, 155
- utilisateurs gérés - 4
- utilisateurs non gérés - 4

V

- validation des clés - 72
 - attribution de confiance pour - 73
- validité - 63
- vérification
 - archives PGP Zip signées - 194
 - une clé publique - 69