

# Table des matières

<b>INTRODUCTION .....</b>	<b>1</b>
L'histoire du système cryptographique PGP et du long procès de son fondateur • 2	
La norme OpenPGP • 5	
Un système reposant sur OpenPGP est-il vraiment sûr ? • 5	
PGP Corporation aujourd'hui • 6	
Le logiciel libre GnuPG • 6	
PGP ou GnuPG ? • 7	
Simplicité d'emploi • 7	
La transparence, garantie de qualité • 8	
Algorithmes pris en charge • 9	
OpenPGP et la loi • 10	
<b>1. À QUOI SERVENT LA CRYPTOGRAPHIE ET OPENPGP ? .....</b>	<b>13</b>
Que garantit la norme OpenPGP ? • 14	
Comprendre les notions fondamentales • 15	
Chiffrer un texte pour le protéger des regards indiscrets • 15	
Chiffre • 16	
L'empreinte d'un message, version numérique de l'empreinte digitale • 16	
Cryptanalyse.. ou attaque • 17	
Les objectifs de la cryptographie OpenPGP • 18	
La confidentialité : protéger des messages sensibles • 18	
La garantie d'intégrité : le message n'est pas falsifié • 18	
La non-répudiation : le signataire ne peut nier être l'expéditeur du message • 19	
L'authenticité : on lit bien ce qui a été envoyé • 19	
Les rouages : les algorithmes de chiffrement • 20	
Algorithmes symétriques : l'efficacité pour protéger en dehors de tout échange • 21	
La magie des algorithmes asymétriques • 21	
Chiffrement à clé publique • 22	
Une signature pour du contenu numérique • 23	
Étapes techniques d'une signature numérique • 23	
Et si le message a été falsifié ? • 24	
Chiffrer et signer en même temps : la force d'OpenPGP • 24	
Phrases secrètes et clés privées • 26	
Qu'est-ce qu'une bonne phrase secrète • 26	
Élémentaire prudence • 27	
<b>2. LES CONCEPTS DE BASE DE LA NORME OPENPGP .....</b>	<b>29</b>
OpenPGP : quelle « sécurité » exactement ? • 30	
Le réseau de confiance • 32	
Questions de confiance • 33	
L'appartenance au réseau de confiance n'est pas un gage de bonne foi • 34	
Le nombre de signatures d'une clé n'est pas une mesure de confiance • 34	
Signer une clé, un engagement • 34	
Intégrer le réseau de confiance • 35	
Précautions pour installer OpenPGP • 36	
Précautions matérielles : sur quel ordinateur installer son logiciel et ses clés ? • 36	
Précautions en cas de partage sous Windows • 36	
Conseils pour créer sa première paire de clés • 37	
Choisir la longueur de la clé • 37	
Choisir le délai d'expiration des clés • 38	

- Nom, adresse électronique et commentaire • 39
  - Nom • 39
  - Adresse électronique • 39
  - Commentaire • 39
  - Identifiant utilisateur • 39
- Créer un certificat de révocation dès la création de la clé • 40
- Stocker en lieu sûr sa paire de clés • 40**
  - Stocker un certificat de révocation • 41
- Identification photographique et clés OpenPGP • 41**
  - Taille et format de la photo • 41
- Diffuser sa clé publique • 42**
  - Recourir à des serveurs publics de clés • 43
  - Publier sa clé publique sur son site web • 44
  - Diffusion ad hoc • 44
- 3. INSTALLER PGP SOUS WINDOWS ET MAC OS X ..... 47**
  - Téléchargement de PGP • 48
  - Installation de PGP • 48
  - Configurer les options de PGP • 51
    - Type de clé (Key Type) • 51
    - Taille de clé (Key Size) • 51
    - Expiration • 52
    - Méthodes de chiffrement (Ciphers) • 52
    - Empreintes • 52
  - Saisie de la phrase secrète et génération des clés • 53
  - Créer une copie de sauvegarde de sa paire de clés PGP • 55
  - Certificats de révocation et PGP • 57
    - Désactiver les mises à jour des serveurs de clés • 58
    - Générer un certificat de révocation (sans révoquer la clé) • 58
    - Réimportation de la clé privée • 60
  - Configurer les propriétés de la clé • 61
  - Révoquer sa clé avec le certificat de révocation • 62
  - Publier sa clé sur un serveur de clés public • 62
    - Publier sa clé sur le serveur de PGP Corporation • 62
    - Publier sa clé sur un autre serveur • 63
- 4. INSTALLER GnuPG POUR WINDOWS, UNIX/LINUX ET MAC OS X ..... 65**
  - Télécharger GnuPG • 66
  - Une bonne habitude à prendre : vérifier les sommes de contrôle • 67
    - Vérifier les sommes de contrôle sous Windows • 68
    - Vérifier les sommes de contrôle sous Mac OS X • 69
    - Vérifier les sommes de contrôle sous Linux/Unix • 69
  - Le répertoire de configuration de GnuPG • 70
    - Emplacement des trousseaux de clés GnuPG • 70
    - Spécificateur serveur de clés et autres options dans gpg.conf • 71
  - Logiciels d'interface graphique à installer pour GnuPG • 71
  - Installer GnuPG sous Windows • 73
    - Installer GnuPG seul • 73
    - Installer GnuPG à l'aide de Gpg4win • 75
  - L'interface graphique WinPT • 77
    - Créer une paire de clés dans WinPT • 77
    - Le gestionnaire de clés de WinPT • 79
    - Créer un certificat de révocation depuis WinPT • 80
    - Envoyer la clé sur un serveur de clés • 81
  - Le gestionnaire de clés d'Enigmail pour Mozilla Thunderbird • 81
    - Créer une paire de clés avec Enigmail • 82
    - Créer un certificat de révocation avec Enigmail • 83
    - Envoyer la clé sur un serveur de clés • 83
  - Installer GnuPG sous Mac OS X • 84
    - Télécharger et installer GPG • 84
    - Créer des clés avec Keychain Access • 85
    - Créer un certificat de révocation • 85
    - Envoyer la clé sur un serveur de clés • 86
  - Installer GnuPG sur Linux et autres systèmes Unix • 87
    - GnuPG et les nombres aléatoires • 88
      - EGD, le démon accumulateur d'entropie • 88
    - Compiler le code source de GnuPG • 90
      - Installer sa version compilée de GnuPG • 90
    - Régler les options de configuration • 91
    - Utiliser GnuPG en mode root setuid • 92
    - N'exécutez pas GnuPG en tant que root • 93
  - Créer une paire de clés GnuPG depuis l'invite de commande • 93
  - Créer un certificat de révocation • 99
  - Rendre publique votre clé • 100
    - Extraction de la clé • 100
    - Serveurs de clés • 102
    - Formulaires web • 103
- 5. LE RÉSEAU DE CONFIANCE ..... 105**
  - Rechercher les clés de ses correspondants sur les serveurs de clés • 106
    - Le réseau de serveurs subkeys.gpg.net • 106
    - Rechercher la clé d'un correspondant • 108

Signer une clé : pourquoi et comment ? • 109	Depuis l'invite de commande • 138
Signer les clés de personnes proches • 110	Avec Enigmail • 139
Que faire avant de signer la clé d'un inconnu ? • 110	Avec WinPT • 139
Que faire d'une clé que vous avez signée ? • 112	Exporter une clé • 139
Intégrer une nouvelle signature à sa clé • 112	Depuis l'invite de commande • 139
Séances de signature de clés • 113	Avec Enigmail • 140
Niveaux de fiabilité des clés • 114	Avec WinPT • 140
À l'écart du réseau de confiance • 115	Avec Keychain Access • 140
<b>6. GÉRER SON TROUSSEAU DE CLÉS AVEC PGP ..... 117</b>	Importer de nouvelles signatures • 140
Ajouter des serveurs de clés • 118	Envoyer des signatures sur des serveurs de clés • 141
Ajouter des clés au trousseau • 120	Depuis l'invite de commande • 141
Recherche sur les serveurs de clés • 120	Avec Enigmail • 141
Importation depuis un fichier • 121	Avec WinPT • 141
Comparaison d'empreintes • 121	Avec Keychain Access • 141
Renvoyer la clé signée • 123	<b>Mettre à jour des clés • 142</b>
Afficher les signatures • 124	<b>Effacer des clés publiques du trousseau • 142</b>
Mise à jour des signatures • 124	Depuis l'invite de commande • 143
Ajouter des photos à vos clés • 125	Avec Enigmail • 143
<b>7. GÉRER SON TROUSSEAU DE CLÉS AVEC GnuPG ..... 127</b>	Avec WinPT • 143
Ajouter des serveurs de clés • 128	Avec Keychain Access • 143
Options du serveur de clés • 128	<b>Ajouter de photos aux clés avec GnuPG • 143</b>
Avec Enigmail (Thunderbird) • 129	Ajouter une photo à une clé • 144
Avec WinPT (Windows) • 129	Afficher les photos avec GnuPG • 145
Avec Keychain Access (Mac OS X) • 130	Les photos dans WinPT • 145
Ajouter des clés au trousseau • 130	<b>GnuPG et le réseau de confiance • 147</b>
Afficher et importer des clés • 131	Affecter des niveaux de confiance • 148
Depuis l'invite de commande • 131	Depuis l'invite de commande • 148
Avec Enigmail • 133	Avec Enigmail • 148
Avec WinPT • 134	Avec WinPT • 149
Avec Keychain Access • 134	<b>8. LES PRINCIPES D'OPENPGP POUR LE</b>
Importer une clé • 134	<b>COURRIER ÉLECTRONIQUE ..... 151</b>
Depuis l'invite de commande • 134	<b>Chiffrement des messages • 153</b>
Avec Enigmail • 135	Chiffrement direct du texte des messages • 153
Avec WinPT • 135	Les inconvénients du chiffrement direct • 153
<b>Signature de clé • 135</b>	Les avantages du chiffrement direct • 154
Vérifier l'empreinte • 136	PGP/MIME • 155
Signer une clé • 136	<b>Intégration avec les logiciels de courrier électronique • 156</b>
Depuis l'invite de commande • 136	Proxys • 156
Avec Enigmail • 137	Plug-ins • 156
Avec WinPT • 138	<b>Stockage du courrier : chiffré ou non chiffré ? • 157</b>
Avec Keychain Access • 138	Stocker le courrier sous une forme non chiffrée • 157
Afficher les signatures d'une clé • 138	Chiffrer son courrier avec sa clé publique • 158

Messages provenant de l'extérieur de votre réseau de confiance • 158

Étendre son réseau de confiance • 159

Parcourir le réseau de confiance (pathfinder) • 159

Être anonyme mais identifiable • 160

Ce qui n'est jamais chiffré dans un courriel • 162

Stocker sous une forme non chiffrée • 162

## 9. ASSURER LA CONFIDENTIALITÉ DES MAILS

### AVEC PGP SOUS WINDOWS ..... 165

Interaction avec votre logiciel de courrier électronique • 166

Identifier les messages OpenPGP • 167

Stockage des messages • 168

Créer des règles pour le chiffrement du courrier • 168

Chiffrement en fonction du destinataire • 169

Chiffrement obligatoire • 170

Envoi sur les listes de diffusion • 170

Gestion des listes de diffusion • 171

Créer des règles personnalisées • 171

Conditions • 172

Actions • 173

Exceptions • 174

Exemple de règle personnalisée : exception à une règle par défaut • 175

Exemple de règle personnalisée : remplacer une règle par défaut • 175

Ordre des règles • 177

## 10. ... ET AVEC GNUPG SOUS WINDOWS, LINUX

### ET MAC OS X ..... 179

Thunderbird et GnuPG • 180

Installer Enigmail, le plug-in GnuPG de Thunderbird • 180

Configurer Enigmail • 181

Envoyer des messages chiffrés • 183

Règles en fonction des destinataires • 183

Ouvrir des messages chiffrés • 185

Apple Mail et GPGMail • 186

GnuPG et les logiciels de courrier électronique de

Microsoft • 186

Outlook et GnuPG • 187

Installer le plug-in GPGol • 187

Configurer le plug-in • 187

Options • 189

Phrase secrète, ou passphrase • 190

Avancé • 190

Envoyer des messages chiffrés • 190

Recevoir des messages chiffrés • 191

Outlook Express et GnuPG • 191

Configurer Outlook Express pour OpenPGP • 192

Envoyer des messages chiffrés • 193

Boîtes de dialogue et avertissement divers • 194

Recevoir et vérifier des messages signés et chiffrés • 194

Déchiffrer des messages PGP/MIME avec Outlook et Outlook Express • 194

## 11. VERS UNE MEILLEURE SECURITÉ AVEC OPENPGP ..... 197

D'où proviennent les risques ? • 198

Mauvaise utilisation • 198

Mauvaise signature • 199

Failles matérielles • 200

Failles logicielles • 200

Faiblesse humaine • 201

Fausse clés • 203

Interopérabilité d'OpenPGP • 204

OpenPGP et le travail d'équipe • 204

Nomadisme et systèmes partagés • 205

Autres fonctions • 207

Mémorisation de la phrase secrète • 207

Destruction de fichiers • 207

## A. INTRODUCTION À PGP COMMAND LINE ..... 209

Configurer PGP Command Line • 210

Vérification et licence • 211

Créer une paire de clés • 212

Choix du type de clé • 213

Choix de la phrase secrète • 213

Choix d'une date d'expiration • 213

Génération d'un certificat de révocation • 214

Exportation de la clé publique • 214

Serveur de clés • 214

Fichier au format texte • 215

Afficher des clés • 215

Gestion des clés • 217

Recherche de clés • 217

Importation de clés • 218

Signature d'une clé • 218

Mise à jour des clés sur un serveur • 218

Chiffrement et déchiffrement • 219

Signature et vérification de fichiers • 219

---

**B. RÉSUMÉ DES COMMANDES GNUPG ..... 221**

Configurer GnuPG • 222

Format et type de sortie • 222

Créer une paire de clés, révoquer et exporter • 222

Révocation d'une clé • 223

Exportation d'une clé • 223

Envoi d'une clé sur un serveur de clés • 223

Gestion des trousseaux de clés • 224

Affichage des clés • 224

Ajouter et ôter des clés • 224

Signatures de clés • 225

Chiffrement et déchiffrement • 225

Signer un fichier • 226

Formats de sortie • 226

**INDEX ..... 227**