



## Chiffrement des données locales des moyens nomades (ordinateurs portables et clés USB)

**7 avril 2009**

Moteurs et freins au déploiement de solutions de chiffrement : PGP en France  
2003 - 2009

Moteurs et freins au déploiement de  
solutions de chiffrement:  
PGP en France  
2003 - 2009



Alain Takahashi  
Hermitage Solutions  
[www.hermitagesolutions.com](http://www.hermitagesolutions.com)

# Définitions

- Le terme PGP (“pretty good privacy”) peut vouloir dire trois choses:
  - Une norme et un format d’échange: OpenPGP (RFC4880), qui prend le contre-pied des architectures reposant sur un “tiers de confiance”
  - Une société: PGP Corp., fondé en 1996 par Phil Zimmermann après l’abandon des poursuites par le Ministère de la Justice américain à propos de la publication du code source de PGP
  - Des produits logiciels interopérables supportant la norme OpenPGP
    - La gamme de produits de PGP Corp., mais aussi: GnuPG (logiciel libre), Veridis, SSH, Utimaco, Voltage, ...
    - A noter: les solutions des deux éditeurs français Arkoon et PrimX ne supportent pas la norme OpenPGP

# PGP Corporation

- Société américaine fondée en 1996, ayant son siège à Palo Alto, Californie
- > 250 employés
- Leader des solutions de cryptographie pour données mobiles et statiques
- L'offre PGP s'appuie sur la norme OpenPGP et X.509 (S/MIME)
- Plusieurs applications de chiffrement répondant à plusieurs besoins différents, l'offre la plus vaste actuellement
- Courriel, Whole Disk, répertoires chiffrés, chiffrement batch, IM, stockage et transfert de données, BlackBerry, Windows Mobile ...
- Le code source est librement disponible pour examen - plus de 66.000 téléchargements à ce jour

# Le marché des solutions de chiffrement

- Les moteurs de ce marché dans le monde:
  - Protection des données confidentielles ayant un impact financier direct (brevets, modèles, bases de données de clients, réponse à appel d'offres ...)
  - Protection des données nominatives (secteur hospitalier, sécurité sociale, caisses de retraite...)
  - Prévention de la perte de réputation
  - De loin la motivation la plus importante: éviter la responsabilité pénale du dirigeant.
    - Aux Etats-Unis: la loi oblige la déclaration publique de pertes de données nominatives
    - Au Royaume-Uni, plusieurs scandales récents ont incité le gouvernement à légiférer sur la perte de données confidentielles

# Le marché des solutions de chiffrement

- En France:

- En retard par rapport aux autres grandes puissances Européennes: le CA cumulé des éditeurs de solutions de chiffrement en France est estimé en 2008 à 10-15% de celui au Royaume-Uni ou en Allemagne, eux-mêmes en retard par rapport aux Etats-Unis rapporté aux tailles des économies,
- Il existe un biais culturel sur la nature et les priorités des données à chiffrer, par exemple en France on trouve une forte propension à vouloir chiffrer les feuilles de paie
- Cependant on se dirige vers le même type de législation, d'origine nationale ou européenne (Bâle II par ex.). Il n'y aura pas "d'exception française" très longtemps ...
- La crise économique semble accélérer ce processus de rattrapage

# Clients PGP Corp

- Utilisé par 84% des sociétés Fortune® 100 U.S.
- Utilisé par 65% des sociétés du CAC40
- Utilisé par 50% des sociétés du SBF 250
  
- 30,000 clients dans 175 pays
- +300 clients en France depuis 2003

Si l'on ajoute les ventes des éditeurs "compatibles PGP", la norme de chiffrement OpenPGP est de loin la plus répandue dans le monde pour le courriel, même si >90% des postes de travail Windows sont compatibles S/MIME ...

# Clients PGP en PME

- Secteurs précoces sur le déploiement de solutions de chiffrement, en France:
  - Preneurs d'ordres & sous-traitants de grands groupes déjà équipés
  - Banque d'affaires
  - Gestion de patrimoine
  - Cabinet d'audit et de conseil
  - Cabinets d'avocats (surtout: propriété intellectuelle)
  - Département des Ressources Humaines
  - Et toute PME ayant un vécu de vol ou pertes de données

# Clients PGP en PME

- Sur > 200 ventes en PME, très peu n'ont pas déployé du tout leur achat,
- ...mais le chiffrement est moins utilisé qu'imaginé à l'origine par la direction et les fournisseurs
- Beaucoup de PME ne réalisent pas leurs droits et obligations légales, par ex:
  - Droit absolu de contrôle des moyens électroniques, sous réserve de prévenir les employés selon le Code du Travail
  - Obligation de présenter des données déchiffrées en cas de demande du fisc, tribunaux, etc. -> “clef d'entreprise”

# Freins au déploiement en PME

- Le chef d'entreprise n'en voit pas l'utilité:
  - « Ca n'arrive qu'aux autres »
  - « Ca coûte mais ne rapporte rien »
- Le chef d'entreprise veut mais les utilisateurs freinent:
  - « C'est trop compliqué »
  - « Moi, je ne perds rien »
  - « Si je perd des données, ce n'est pas grave »

# Conseils pour un déploiement réussi

- Bien définir les données que l'on veut protéger, il y en a moins qu'on n'imagine parfois.
- Sensibiliser les utilisateurs finaux aux risques de la sécurité informatique au moyen d'ateliers, conférences, lectures, etc
- S'il s'agit de chiffrement de messagerie: bien comprendre les tenants et aboutissants d'un système qui se met en rupture de flux: que veut-on chiffrer, comment va-t-on échanger les clefs publiques, ...
- Pour le service des Achats: privilégier le mieux disant au moins disant ...