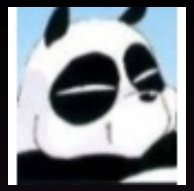
Clefs PGP

Genma

14 novembre 2013



A propos de moi

Où me trouver sur Internet ?

- Le Blog de Genma :
  http ://genma.free.fr
- Twitter :
  http ://twitter.com/genma

Mes centres d'intérêts ?

Plein de choses dont :

- La veille technologique
- Le chiffrement

Qu'est ce que GPG ?

Principe de la cryptographie

Le principe du chiffrement est de transformer à l'aide d'une clef un message clair en un message incompréhensible pour que celui qui ne dispose pas de la clef de déchiffrement. On distingue trois types d'algorithmes utilisés pour le chiffrement :

- algorithmes de chiffrement simples (code de CÉSAR) ;
- algorithmes de cryptographie symétrique fondés sur la présence d'une unique clef pour chiffrer et déchiffrer nécessitant autant de clef que de correspondants (AES) ;
- algorithmes de cryptographie asymétrique fondés sur la présence de 2 clefs, une publique (partageable) et une privée (RSA, DSA).

OpenPGP

OpenPGP est un format de cryptographie qui définit le format des messages, signatures ou certificats que peuvent s'envoyer des logiciels.
C'est un format pour l'échange sécurisé de données.

GNU Privacy Guard

C'est une implémentation du standard OpenPGP, procédé de chiffrement à clef publique.
C'est un logiciel très stable, distribué sous la licence GNU GPL et est souvent inclus d'origine sur les systèmes d'exploitation GNU/Linux.

Générer et gérer ses clefs

GNU Privacy Guard

GnuPG est un système cryptographique à clef publique caractérisé par :

- une clef publique, distribuée à toutes les personnes avec qui l'utilisateur souhaite communiquer ;
- une clef privée, gardée jalousement secrète.

Taille de la clef

Principe :

- standard entre 2048 et 4096 ;
- plus la clef est longue, plus elle est dure à casser ;
- plus la clef est longue, plus elle est lourde (mais chiffrement hybride) ;
- plus la clef est longue, plus elle est longue à générer

Date d'expiration

Validité d'une clef : temps au bout duquel les correspondants ne pourront plus utiliser cette clef pour chiffrer des données et vérifier les signatures.
Comment choisir ?

- 0 ou temps de vie illimité peu sécurisé : perte clef privée, vol, oubli du mot de passe,...
- possibilité de prolongement temps de vie avant expiration

Identité de la clef

Ce sont les informations qui apparaîtront au moment de la vérification des signatures. Attention à l'identité créée et au contexte.

Phrase de passe

À bien choisir !

- seule protection de la clef privée si quelqu'un possède le fichier contenant la clef privée, c'est le point faible de GnuPG ;
- ne devrait pas contenir de mot du dictionnaire ;
- devrait mélanger la casse caractères alphabétiques ;
- devrait utiliser des caractères non alphabétiques ;
- taille illimitée.

Générer un certificat de révocation

–gen-revoke génère un certificat de révocation signifiant qu'on ne peut plus utiliser la clef publique. 2 types différents :

- certificat de perte en cas d'oubli du mot de passe ou de perte de la clef ;
- certificat de compromission si la clef privée est compromise.

Utilité

Une bonne gestion des clefs est cruciale pour être certain que personne ne lise les messages chiffrés, en émette d'autres. Cela permet d'être sûr de son trousseau et de garantir l'intégrité du trousseau des autres.

Gérer la paire de clefs

Une clef publique est composée de :

- portion publique de la clef principale de signature ;
- portions publiques des clefs secondaires de signature et de chiffrement ;
- identifiants utilisés pour associer la clef à l'utilisateur (nom, commentaire optionnel, adresse mail, date de création, date d'expiration, degré de confiance,...).

Intégrité des clefs

La distribution des clefs publiques engendre un risque de falsification (substitution clefs, modifications identifiants utilisateurs).
Pour protéger une clef publique, on utilise la partie privée de la clé principale pour signer les composantes publiques et l'identifiant utilisateur : c'est une auto-signature.

Partager les clefs

Signer une clef

Une clef peut être validée en vérifiant son empreinte. En la signant, on certifie qu'elle est valide via la visulaisation de son 'empreinte
L'empreinte de la clef est vérifiée avec son propriétairare , on s'assure ainsi qu'on a une copie correcte de la clef. On s'assure également de l'identité de la personne que l'on a en face de soi.
Pour signer, on utilise alors la commande sign sur la clef que l'on veut éditer.

Confiance dans le propriétaire de la clef

Il existe 5 niveaux de confiance pour les propriétaires de clefs :

- 1 ou unknown, on ne sait rien de la façon dont la personne signe ses clefs (valeur par défaut) ;
- 2 ou none, on sait que la personne ne vérifie pas soigneusement avant de signer ;
- 3 ou marginal, on sait que le propriétaire a conscience de ce qu'il fait quand il signe ;
- 4 ou full, le propriétaire sait parfaitement ce qu'il fait et une signature de lui a la même valeur que la votre ;
- 5 ou réservé exclusivement à ses propres clefs.

Le niveau de confiance est une information personnelle et privée, enregistrée sur une base de donnée distincte.

Confiance dans le propriétaire de la clef

Idéalement, les clefs sont distribués personnellement. En pratique, les serveurs de clefs publiques sont utilisés pour collecter et distribuer les clefs publiques.
En cas d'envoi de clef :

- ajout de la clef à la base de donnée ;
- fusion de la clef avec la clef existante si elle existe.

En cas de requête de clef, le serveur renvoie la clef publique.

Distribuer ses clefs - principe des serveurs de clefs

Idéalement, les clefs sont distribués personnellement. En pratique, les serveurs de clefs publiques sont utilisés pour collecter et distribuer les clefs publiques.
En cas d'envoi de clef :

- ajout de la clef à la base de donnée ;
- fusion de la clef avec la clef existante si elle existe.

En cas de requête de clef, le serveur renvoie la clef publique.

Intérêt des serveurs de clefs

En cas de signature de sa clef, il faut récupérer sa clef signée et la redistribuer à tous ses contacts, pour qu'ils aient une version à jour.
. .
Quand quelqu'un signe une clef, il la renvoie au serveur de clef qui rajoute la signature à sa copie de la clef publique.
Les contacts peuvent récupérer de façon autonome la clef mise à jour : le propriétaire est affranchi de la distibution.
Le propriétaire récupère les signatures sur sa clef sur les serveurs.
Les grands serveurs se mettent à jour les uns avec les autres, il suffit d'en sélectionner un.
Il faut rafraîchir son trousseau régulièrement à cause des révocations et des expirations.

Importer une clef publique

Il faut procéder en 3 étapes :

- 1 trouver la clef publique souhaitée ;
- 2 choisir la clef de la personne que l'on cherche (et pense avoir trouver) ;
- 3 absorber la clef

On peut aussi avoir reçu la clef par e-mail, de la main à la main par clef USB ou autre.

Id de la clef

A une clef est associé un ID.

Utiliser ses clefs

Principe des messages chiffrés

Si Bob envoie un message à Alice, il le chiffre avec la clef publique d'Alice qui le déchiffrera avec sa clef privée. Et vice-versa.
Pour chiffrer un message à destination de plusieurs personnes, il faut la clef publique de chacun des destinataires.
Si l'on ne s'inclue pas dans les destinataires, on ne pourra pas lire son propre message.

Déchiffrer un message

Pour décrypter un message, il faut la clef privée pour laquelle le message a été chiffré.

Signer un document

Une signature sert à :

- certifier et dater un document ;
- permettre de vérifier que l'on est bien l'expéditeur ;
- permettre de vérifier que le document n'a pas été modifié depuis son envoi.

La signature se fait avec la clef privée de l'expéditeur.
Face à un document signé, on peut

- vérifier la signature ;
- extraire le document.

Protéger sa clef privée

Essentiel :

- si quelqu'un l'obtient, tout pourra être déchiffré et on peut signer en votre nom ;
- si on la perd, on peut plus rien déchiffrer.

Protéger sa clef privée

Il faut idéalement :

- conserver le certificat de révocation et une copie de sauvegarde de la clef publique sur un support protégé en écriture dans un lieu sûr ;
- conserver la clef privée sur un disque amovible protégé en écriture ;
- utiliser la clef privée sur une machine mono-utilisateur déconnectée du réseau ;
- avoir un bon mot de passe.

Conclusion : utiliser des sous-clefs

Définition des dates d'expiration

Selon la clef, les délais d'expiration varient :

- délai « long » pour la clef principale :
- délai court pour les sous-clefs :
- changer régulièrement est plus sécurisé (protection des documents à venir) ;
- en cas de perte de contrôle de la clef et de perte du certificat de révocation.

Utilisation des clefs secondaires

Les consignes sont :

- changer régulièrement afin de protéger les documents chiffrés ultérieurement ;
- publier la nouvelle clef avant l'expiration de la précédente ;
- faire valider sa clef principale par ses correspondants ;
- aucun intérêt à avoir plusieurs clefs secondaires de
- chiffrement actives à un temps donné ;
- aucun problème à avoir plusieurs clefs secondaires expirées dans une paire de clef donnée.

Gérer sa toile de confiance

Il faut garder en tête que l'appartenance au réseau de confiance n'est pas une garantie de bonne foi, c'est un indice de validité de l'identité de la personne.
Ce qui compte, ce n'est pas le nombre de signatures, mais la qualité des signatures.
Il existe deux façons de gérer sa confiance :

- modèle PGP ou la validité d'acquière par 1 confiance totale ou 3 confiances marginales ;
- modèle personnalisé en fonction de l'usage des indices de confiances.

Faire de la propagande !

- commencer avec les personnes avec qui vous avez appris ;
- introduiser subtilement une signature et répondre aux interrogations soulevées par la mystérieuse pièce-jointe ;
- aller à des key-signing parties !

Questions - Démonstration

ANNEXES

Ajouter des composantes à une clef

On peut vouloir ajouter différentes composantes :

- identifiants utilisateurs avec adduid en cas de multiples identités ;
- sous-clefs avec addkey car changer de clef principale nécessite de refaire les certifications, et il est recommandé de changer de sous-clefs régulièrement (3 ans) et d'utiliser des sous-clefs différentes sur des machines différentes.

Retirer des composantes à une clef

Les sous-clefs et les identifiants utilisateurs peuvent être effacés :

- sélection de l'item à effacer par les sélecteurs key et uid (key 2 sélectionne la seconde sous-clef) ;
- effacement de l'item sélectionné par delkey ou deluid.

L'effacement complique la distibution des clefs. Lors de l'import ou de l'envoi sur un serveur de la clef publique, la fusion restaure les éléments effacés.

Révoquer les composantes d'une clef

- pour une sous-clef, on utilise revkey après avoir sélectionné la sous-clef (auto-signature de révocation) ;
- pour une signature, on utilise revsig, l'interface révoquée ;
- pour un identifiant utilisateur, on révoque son auto-signature.

La révocation est toujours visible lors distribution et màj de la clef publique. Cela garantit que les autres aient une version intègre de la clef.