GNU Privacy Guard

du côté pratique

Pauline POMMERET

Séminaire Technique du Crans

18 juin 2014

Table of Contents

Communiquer de façon sûre

- recevoir un email de quelqu'un ne veut pas dire qu'il nous l'a effectivement envoyé ;
- un email est envoyé en clair sur le réseau et les informations envoyées peuvent être lues par n'importe qui.

Table of Contents

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 :

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

Table of Contents

C'est quoi 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.

Table of Contents

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.

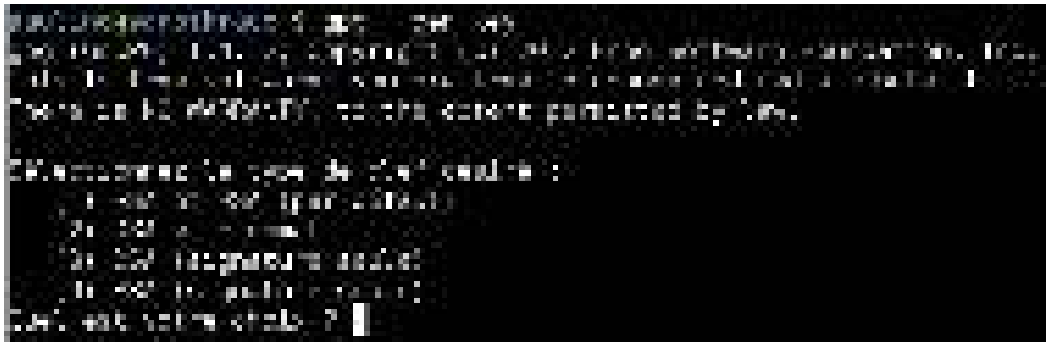
Table of Contents

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.

Table of Contents

`--gen-key` pour générer une paire de clefs



- RSA (RIVER SHAMIR ADLEMAN), le plus utilisé dans le commerce électronique ;
- DSA (*Digital Signature Algorithm*) ;
- utiliser RSA (ANSSI : taille minimale de 4096 bits pour usage au delà de 2020).

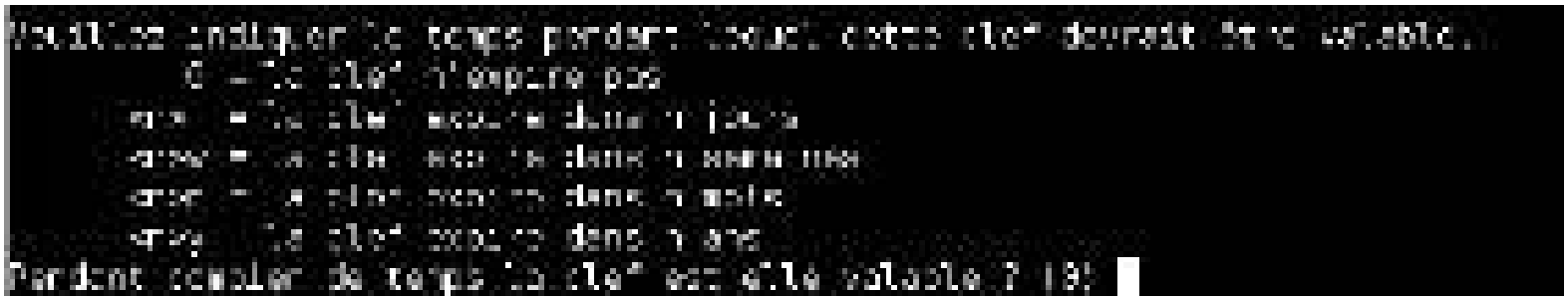
Taille de la clef

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 (artéfact : `cp Musique/ Musique2/`).

Date d'expiration

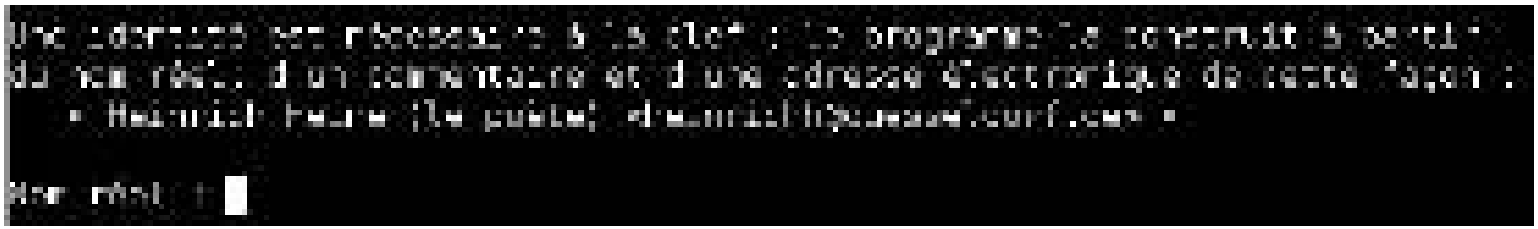
Validité d'une clef : temps au bout duquel les correspondants ne pourront plus utiliser cette clef pour chiffrer des données et vérifier les signatures.



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`

`--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.

Utilisation

```
$ gpg --output revocation_type.asc
      --gen-revoke id_clef
```

Table of Contents

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

Afficher les caractéristiques de la paire

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,...).

Utilisation

```
$ gpg --edit-keys pommeret@crans.org
```

Gérer la paire des clefs

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**.

```
gpg> check
uid  Pauline Pommeret <paulinepommeret@gmail.com>
sig!3        CF875FE1 2012-10-04  [autosignature]
uid  Pauline Pommeret [ma première clé !] <ppommeret@crans.org>
```

Gérer la paire des clefs

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.

Gérer la paire des clefs

Retirer des composantes à une clef

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

1. sélection de l'item à effacer par les sélecteurs `key` et `uid` (`key 2` sélectionne la seconde sous-clef) ;
2. 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.

Gérer la paire des clefs

Révoquer les composantes d'une clef

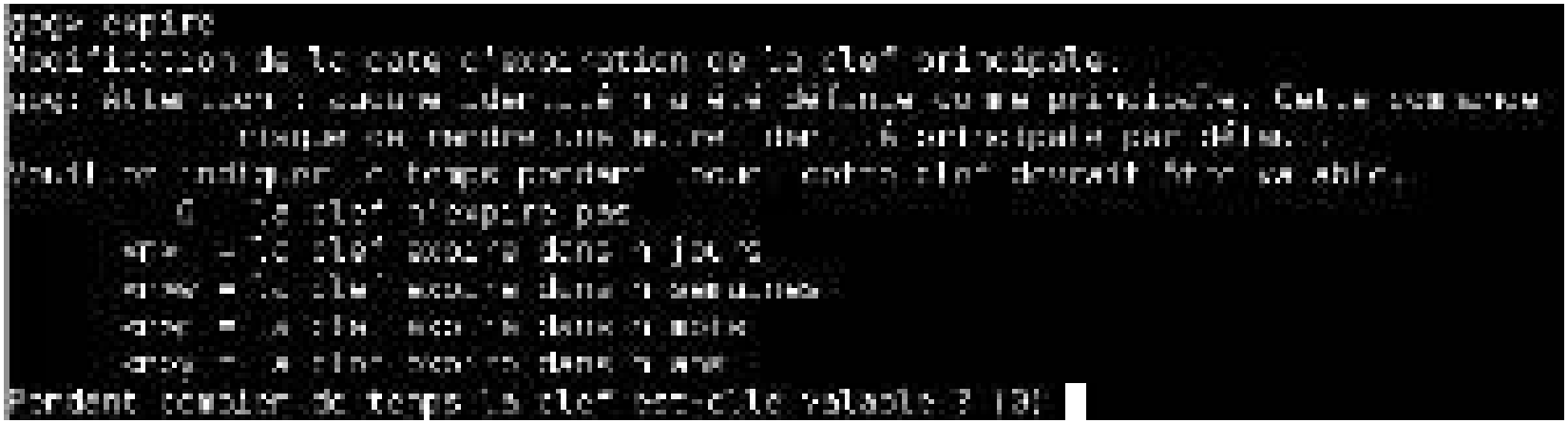
On peut révoquer différentes composantes :

- 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.

Gérer la paire des clefs

Mettre à jour la date d'expiration de la clef



`expire`

efface la dernière auto-signatur et la remplace. La dernière auto-signature fait référence pour ceux qui ont importé la clef.

Table of Contents

Signer une clef

Une clef peut être validée en vérifiant son empreinte. En la signant, on certifie qu'elle est valide. Pour visualiser l'empreinte de la clef on utilise `--fingerprint` ou `fpr` en édition.

L'empreinte de la clef est vérifiée avec son propriétaire, 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.

Table of Contents

Confiance dans le propriétaire de la clef

Niveaux de confiance

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*.

Confiance dans le propriétaire de la clef

`trust`

Le niveau de confiance est une information personnelle et privée, enregistrée sur une base de donnée distincte.
Pour définir le niveau de confiance dans un propriétaire, on utilise l'éditeur de clef avec la commande `trust`.

Utiliser la confiance pour valider une clef

Paramètres du réseau de confiance par défaut

Une clef est considérée comme valide si elle remplit 2 conditions :

1. elle est signée par suffisamment de clefs valides *i.e.*
   - on l'a signée personnellement ;
   - elle a été signée par une clef à laquelle on accorde toute sa confiance ;
   - elle a été signée par 3 clefs auxquelles on accorde une confiance marginale.
2. le chemin des clefs conduisant de cette clef à sa propre clef mesure moins de 5 étapes.

Utiliser la confiance pour valider une clef

Mettre à jour le réseau

Il s'agit des paramètres par défaut, ils sont modifiables avec un fichier de configuration approprié.
Il est possible d'interroger la base de données pour faire apparaître les personnes non signées mais valides dans le trousseau.

Utilisation

```
$  gpg --update-trustdb
```