OpenPGP - GNU Privacy Guard

OpenPGP

OpenPGP est un standard permettant de signer et chiffrer ses mails. De cette façon, l'identité de l'expéditeur peut être vérifiée et le courrier électronique reste confidentiel.

GPG

GNU Privacy Guard est une implémentation libre et complète du standard OpenPGP. Ce logiciel permet donc de mettre en application la signature et le chiffrement des e-mails décrits dans le standard.

Comment?

Chaque utilisateur possède deux clés personnelles

Une clé privée, qui permet de signer les messages, de déchiffrer les messages chiffrés avec la clé publique, de créer une clé de révocation et de signer d'autres clés publiques. Cette clé est privée et protégée par un mot de passe. Une fois perdue, il est impossible de la révoquer.

Une clé publique, qui permet aux autres de chiffrer des messages, de vérifier les signatures d'un e-mail, elle est distribuée généralement sur les serveurs de clés, peut être signée par les autres et est liée à la clé privée. Cette clé ne dispose pas de mot de passe et est lisible par tout un chacun.

Quelques dangers de ce système:

La clé privée peut être perdue, la rendant irrévocable.

La clé privée peut être volée.

N'importe qui peut créer des clés (même quelqu'un de mal intensionné).

Mais ces éléments sont contournables: la clé privée peut être dupliquée pour éviter de la perdre. On peut la protéger par un mot de passe afin d'éviter qu'un éventuel voleur ne l'utilise, et l'authenticité est vérifiable grace aux signatures qui accompagnent la clé.

Serveurs de cles

Les clés publiques sont envoyées sur un serveur de clé, où chacun peut la récupérer, la signer, consulter les signatures de la clé et ainsi se faire une idée sur son authenticité. Les serveurs de clés principaux sont repris dans la documentation annexe.

Keysigning Party

Munis d'une pièce d'identité valable et de l'empreinte de leur clé, les personnes le souhaitant se réunissent (sans ordinateur) afin d'échanger ces information. Après la key-signing party, ils signent les clés dont ils se sont assurés de l'authenticité.