# Comment vérifier une signature électronique ?

Avec la prolifération des virus et autres pirates informatiques, l'installation sur son ordinateur du moindre programme anodin est source d'inquiétude. La question est : Comment s'assurer que le programme à installer provient bien de l'éditeur souhaité et non d'un autre beaucoup moins souhaité ?
La solution proposée par nombre d'éditeurs dans le cas de programmes touchant au système de l'ordinateur est d'authentifier le programme à installer par un certificat unique.
Le certificat est fourni publiquement par l'éditeur et l'utilisateur a le moyen de vérifier que le programme produit bien le même certificat. Tout la complexité réside à produire un certificat unique de façon que deux programmes ne produisent pas le même. Une solution a été trouvée en utilisant les méthodes de cryptologie et notamment les signatures électroniques comme SHA, MD5 ou PGP.

**1) SHA**

SHA-1 ou SHA (Secure Hash Algorithm) est essentiellement une somme de contrôle pour un fichier de données. La somme SHA-1 est basée sur une norme cryptographique. On la connaît en tant que "Federal Information Processing Standard (FIPS 180-1) Secure Hash Standard (affixed)". Pour un fichier donné, SHA-1 produit une valeur de 160 bits connue sous le nom de "message digest" ou "signature". Cette valeur est réputée informatiquement infaisable à contrefaire. Il est fortement improbable que deux fichiers différents pourraient jamais produire la même valeur. Si un fichier est modifié pendant le transfert, sa valeur change également.
Vous pouvez ainsi vérifier (avec un degré élevé de probabilité) que le logiciel que vous avez téléchargé est le même logiciel vous avez eu l'intention de télécharger (voir la méthode ci-dessous). Quand la valeur SHA-1 pour le fichier que vous avez téléchargé correspond à la valeur pour le fichier comme affiché sur le site source, vous pouvez être sûr que le fichier est authentique.
Pour en savoir plus : http://fr.wikipedia.org/wiki/SHA-1

Pour vérifier un fichier avec une signature SHA-1, exécuter les étapes suivantes :

1. Ouvrir le Terminal.
2. Saisir la commande suivante : /usr/bin/openssl sha1 [chemin du fichier]
Exemple :
$ openssl sha1 SecUpd2006-004Ti.dmg
SHA1(SecUpd2006-004Ti.dmg)=
bb8011f3e8f293b906751e6cb9b6b667730e4717
3. Vérifier la signature sur la page Internet correspondante :
http://www.apple.com/downloads/macosx/apple/
securityupdate2006004macosx1047clientppc.html

## 2) MD5

MD5 (Message Digest 5) calcule une empreinte sous forme de somme de contrôle donnant pour un fichier sa signature numérique avec la propriété que les signatures de deux messages différents soient différentes.
Mais la possibilité de créer des signatures identiques à la demande est découverte par une équipe chinoise en 2004. MD5 n'est donc plus considéré comme sûr au sens cryptographique.
Cependant, MD5 est toujours employé pour vérifier que le logiciel que vous avez téléchargé est le même logiciel vous avez eu l'intention de télécharger (voir la méthode ci-dessous). Quand la valeur MD5 pour le fichier que vous avez téléchargé correspond à la valeur pour le fichier comme affiché sur le site source, vous pouvez être quasi sûr que le fichier est authentique.
Un deuxième emploi encore usité permet d'augmenter la sécurité de l'enregistrement des mots de passe en prenant l'empreinte MD5. Là aussi, la génération actuelle de "tables inverses" même gigantesques permet de trouver le mot de passe.
Pour en savoir plus : http://fr.wikipedia.org/wiki/MD5

Pour vérifier un fichier avec une signature MD5, exécuter les étapes suivantes:

1. Ouvrir le Terminal.
2. Saisir la commande suivante : /sbin/md5 [chemin du fichier]
Exemple :
$ md5 mysql-standard-4.1.4-gamma-apple-darwin7.5.0-powerpc.dmg
MD5 (mysql-standard-4.1.4-gamma-apple-darwin7.5.0-powerpc.dmg) = 28564ea5baf2355010c72dab3fbead12
3. Vérifier la signature sur la page Internet correspondante :
http://downloads.mysql.com/archives.php?p=mysql-4.1&v=4.1.4

### 3) PGP

Cette méthode est la plus sure. Elle fait appelle aux derniers algoritmes de cryptographie. Néanmoins elle est plus complexe à mettre en oeuvre car elle nécessite de récupérer la clé de chaque émetteur.
En 1991, PGP est créé au départ dans un but de préserver l'intimité des communications entre particuliers. PGP propose d'une part d'authentifier un message et d'autre part de chiffrer un message, le tout avec un système de jeux de clés entre l'émetteur et le destinataire. C'est l'authentification qui nous intéresse ici. PGP propose alors à l'émetteur de créé son jeu de clés, une clé privée pour lui permettre de signer un message et une clé publique (appairée à la première) qu'il va publier pour permettre au destinataire d'authentifier le message.
Pour en savoir plus : http://fr.wikipedia.org/wiki/Pretty_Good_Privacy

Pour vérifier un fichier avec une signature PGP, exécuter les étapes suivantes:
De base, Mac OS X ne possède pas PGP, nous prendrons la version GNU.

1. Récupérer et installer le logiciel GNU PGP (http://www.gnupg.org) pour Mac OS X sur http://macgpg.sourceforge.net/fr/index.html.
Le logiciel s'installe dans les répertoires suivants :
Aide : /Library/Documentation/GnuPG, /usr/local/share et /usr/local/info
Exécutable : /usr/local/bin, /usr/local/lib et /usr/local/libexec
2. Récupérer la clé publique de l'émetteur, par exemple celle de MySQL:
En recherchant "package mysql" sur http://www.keyserver.net
3. Renommer le fichier récupéré en "mysql_pubbey.asc".
4. Ouvrir le Terminal, saisir les commandes suivantes :
$ gpg --import mysql_pubkey.asc
2. Saisir la commande suivante : /usr/local/bin/gpg --verify [chemin du fichier signature] [chemin du fichier de données]
Exemple :
$ gpg --verify mysql-standard-4.1.4-gamma-apple-darwin7.5.0-powerpc.dmg.asc mysql-standard-4.1.4-gamma-apple-darwin7.5.0-powerpc.dmg
gpg: Signature made Mon Aug 30 19:05:38 2004 CEST using DSA key ID 5072E1F5
gpg: Good signature from "MySQL Package signing key (www.mysql.com) <build@mysql.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: A4A9 4068 76FC BD3C 4567 70C8 8C71 8D3B 5072 E1F5

Pascal Pignard, novembre, décembre 2006, janvier 2007.