# Utiliser PGP avec Java et Bouncy Castle

## Linux Gazette n°98 — Février 2004


### Graham Jenkins




## Table des matières



## 1. Pourquoi le feriez-vous ?

Les dernières versions (1.4.x) de Java contiennent à la fois les paquetages `java.security` et `javax.crypto`, ainsi que leurs sous-paquetages associés. Ceux-ci vous permettent de signer un objet et/ou de le crypter. Un outil standard est inclus pour accéder aux clés enregistrées dans un fichier de clés de format propriétaire. Si vous avez une version plus ancienne de Java, il est probable qu'elle comprenne `java.security` et qu'une version de JCE (Java Cryptography Extension) soit disponible pour celle-ci (visitez le site http://java.sun.com/security). Pourquoi souhaitez-vous utiliser PGP ? Il y a deux raisons : tout d'abord, vous pouvez être amené à signer ou crypter des informations susceptibles d'être éventuellement lues par un programme non Java. En second lieu, maintenir deux types séparés de fichiers de clés peut être fastidieux.

## 2. Le faire vite et sans affiner

Si vous avez une version de **gpg** sur votre ordinateur, utilisez la classe Java Runtime pour l'exécuter dans un thread séparé et lisez le résultat par l'intermédiaire d'un objet « InputStreamReader » Cette opération ne demande pas une grande quantité de mémoire et vous n'aurez pas besoin d'allouer des fichiers temporaires. Toutefois, le résultat est difficilement portable et ce n'est pas la manière dont il faut écrire des programmes Java.

# 3. *The legion of Bouncy Castle*

*The legion of Bouncy Castle* a un site web à l'adresse http://www.bouncycastle.org, qui se déclare lui-même comme un « endroit agréable où rester ». Ses membres sont vraiment passionnés par le cryptage. Ils ont cependant acquis la réputation d'avoir fourni un bon logiciel de cryptage Java open source. Une de leurs plus récentes créations est un paquetage qui offre un support d'Open PGP. Les versions concernant JDK 1.2, 1.3 et 1.4 sont disponibles en téléchargement sur leur site web.

# 4. Le faire avec Bouncy Castle

Dans un article intitulé « Impression sécurisée avec PGP », j'ai présenté quelques programmes Perl pour envoyer des tâches d'impression signées avec PGP. Il existe des versions plus récentes de ces programmes à l'adresse http://www.cpan.org/scripts.

Le problème ici était qu'il n'y avait pas de manière simple d'envoyer des tâches depuis quelque chose commme un dispositif de réseau Java. Le paquetage Bouncy Castle offre une solution. Un listing de `SEPclient.java` y est attaché. Il fonctionne comme son équivalent Perl trouvé sur le site de CPAN et il serait judicieux que vous lisiez la documentation qu'il contient.

Le programme commence par lire un fichier de configuration détaillant les adresses auxquelles les tâches doivent être envoyées, la taille pouvant être attribuée, l'adresse qualifiée de l'expéditeur et les hôtes SMTP susceptibles d'être employés. Il lit aussi la phrase confidentielle GPG de l'utilisateur. Il est normalement exécuté par cet utilisateur.

Il copie ensuite une entrée standard dans un fichier temporaire (pour faciliter le traitement par les routines de Bouncy Castle), extrait la clé privée de l'utilisateur et écrit une sortie signée sur un second fichier temporaire. Le message signé obtenu est alors divisé en deux parties, dont chacune est transmise tour à tour à un ensemble de routines Javamail à fins de répartition.

# 5. Améliorations à venir

Le programme SEPclient.java a été codé dans un but de simplicité plutôt que d'efficacité. La partie de l'extraction de la clé privée devra être étendue de façon à pouvoir recevoir de multiples clés privées sur un jeu de clés. La copie du fichier et les parties de la mise à jour de la signature devront être étendues pour traiter plus d'un caractère à la fois. Il y a eu précédemment quelques problèmes avec des versions précédentes du fichier `bcpg.jar`, et vous devrez vous assurer d'avoir au moins la version 1.22b04.

# 6. À essayer

J'ai constaté que `SEPclient.java` dans sa forme actuelle fonctionne bien avec ses équivalents Perl. Néanmoins, ce programme n'emploie qu'un sous-ensemble des capacités disponibles avec les paquetages Bouncy Castle OpenPGP. Je vous suggère donc de télécharger les paquetages OpenPGP, de jeter un coup d'½il à la documentation et de voir ce que vous pouvez en faire.

Télécharger le listing des programmes
(http://www.linuxgazette.com/node_files/2004-01/359/SEPclient.java).

Paru dans le n°99 de la Linux Gazette de février 2004.

Traduction française par Simon Depiets <`2df CHEZ tuxfamily POINT org`>.

Relecture de la traduction française par Joëlle Cornavin <`jcornavi CHEZ club TIRET internet POINT fr`>.