COMMENT RÉVOQUER UNE CLÉ GPG

par

Ainigmatias Cruptos

Résumé. — Nous donnons dans cette note le fonctionnement de la révocation des clés en OpenPGP.

1. Introduction

Quand on utilise gpg, il convient de distinguer trois lieux privilégiés : le **trousseau de clés**, qui se trouve dans le répertoire *.gnupg*, les **serveurs de clés**, **l'espace local** extérieur au trousseau (un répertoire de travail quelconque).

Quand on crée une paire de clés par la commande :

gpg --gen-key

celle-ci est rajoutée au **trousseau de clés**.

On peut constater que la clé est bien créée, retrouver son identifiant par la commande :

gpg --list-keys.

Afin de communiquer la **clé publique** à ses correspondants, il convient de l'exporter de son trousseau vers l'espace local de travail. Ceci se fait par la commande :

gpg --armor --export 8E08D1DD > macle.asc

Mots clefs. — cryptographie, protocole cryptographique, pgp, gpg, signature, chiffrement, crc-24, base64, radix-64.

qui exporte sous forme de fichier avec armure ASCII (à cause du --armor) la clé dont l'identifiant est 8E08D1DD. Le fichier obtenu est **macle.asc**. C'est ce dernier fichier qu'on doit communiquer à ses correspondants et qu'ils devront **importer** dans leur trousseau de clé par la commande :

gpg --import macle.asc.

Le meilleur moyen de communiquer largement sa clé publique est de la publier sur un serveur de clés, par exemple sur :

http ://wwwkeys.pgp.net

(on va avec son navigateur sur ce site, et on suit la procédure indiquée) et sur :

pgp.mit.edu.

2. Révocation de la clé

2.1. À la création de la clé. — Tout de suite après avoir créé une paire de clés, on a intérêt à tout de suite créer un certificat de révocation par la commande :

gpg --armor --gen-revoke 8E08D1DD > macle.rev

et mettre le fichier ASCII macle.rev, qui vient d'être créé dans l'espace local de travail, en lieu sûr.

Bien entendu ceci peut se faire plus tard, à tout moment. Mais la création d'un certificat de révocation demande la *passphrase*. Si on a oublié ce mot de passe on ne peut plus révoquer la clé.

2.2. S'il faut révoquer la clé. — Si on doit révoquer la clé :

– On importe le fichier macle.rev dans son trousseau de clés par la commande :

gpg --import macle.rev.

Ceci a pour effet de modifier la clé publique qu'on veut révoquer en la marquant « révoquée ».

– On exporte la clé publique (qui a été modifiée) de son trousseau de clés vers son espace local de travail comme cela a été déjà fait avec la commande :

gpg --armor --export 8E08D1DD > macle.asc.

– Le fichier ASCII macle.asc contient maintenant la version révoquée de la clé publique, qu'on va placer sur les serveurs de clés (comme

on l'a déjà fait lorsque la clé publique était valide). Ceci remplace la clé publique en question sur les serveurs par la nouvelle version révoquée. Elle apparaît maintenant avec la mention « révoquée ».

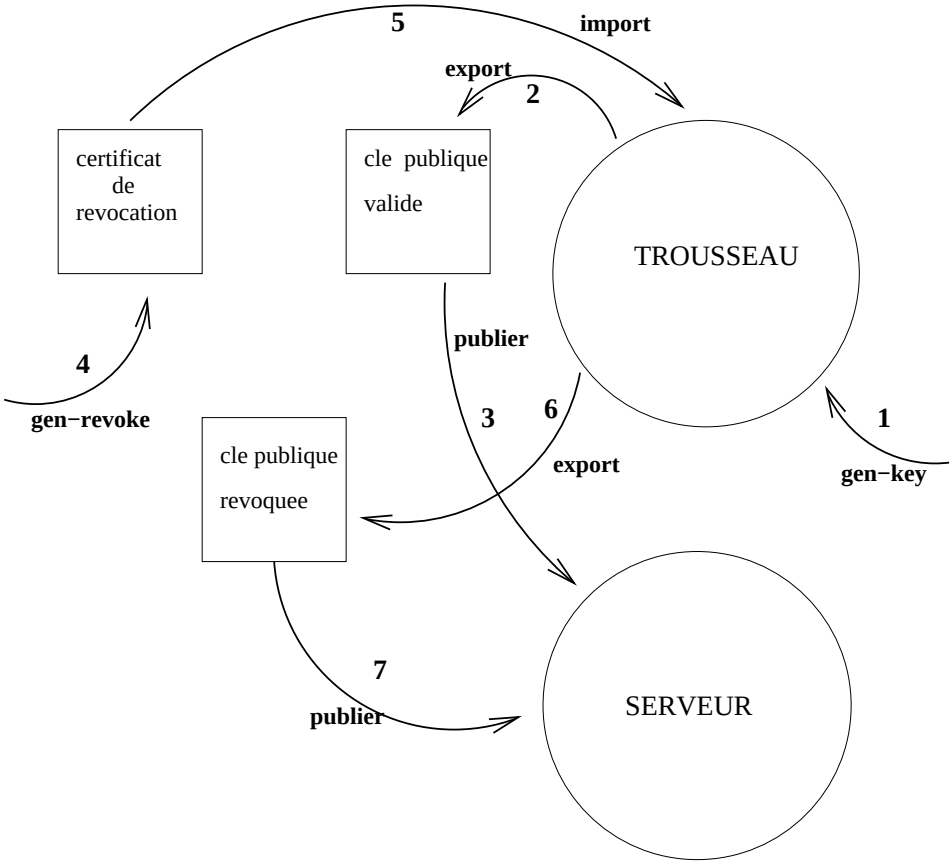

FIGURE 1. Révocation d'une clé

18 août 2007

A. CRUPTOS, Association ACrypTA. • *E-mail :* acrypta@acrypta.fr