http://www.coincoin.fr.eu.org/?De-la-migration-d-une-clef-GPG

De la migration d'une clef GPG

- 6- Webographie -

Date de mise en ligne : samedi 19 avril 2014

SHA1 est cassé, 1024 est trop court, ta clef a 10 ans, ...

Si pour une des raisons citées ci-dessus, tu penses qu'il est temps de changer de clef PGP, je te propose de te guider ici. Je m'inspire grandemenet de HOWTO prep for migration off of SHA-1 in OpenPGP

Bon, OpenPGP (version 1 ou 2) supporte la famille de fonction de hachage SHA-2 : SHA512, SHA384, SHA256, et SHA224 ; et des clefs de longueurs au moins égale à 4096 bits (pour 8192, c'est possible, il faut patcher.)

En route pour la transition

Voici en quelques mots l'idée générale du processus qui se déroule en 3 étapes : créer une clef plus longue et commencer à l'utiliser (signature de données ou de clefs) ; indiquer à vos correspondants que vous préferiez une clef plus longue et avec une autre fonction de hachage. migrez votre clef vers une clef plus longue

Les deux premières étapes sont faciles à réaliser, mais risquent de vous couper de votre réseau de confiance GPG existant. Pour la suite, il va falloir faire une migration de clef.

Changeons nos longueurs et fonction de hash

Le truc le plus simple à faire est de se créer une nouvelle clef. Ajoutons les lignes suivantes dans notre fichier de configuration de GnuPG : cat >> /.gnupg/gpg.conf <

Désormais, même sans changer votre clef, les messages seront signés avec un algorithme de la famille SHA-2. La dernière ligne vous assure que cette préférence d'algorithme sera également choisie pour la nouvelle clef que vous aller créer.

Publions nos préférences

On peut publier ses préférences avec la clef, ainsi ceux qui mettent à jour régulièrement les clefs depuis les serveurs (une bonne pratique) connaîtront vos préférences : user@computer : $ gpg â€"edit-key PUBKEYID gpg (GnuPG) 1.4.16 ; Copyright (C) 2013 Free Software Foundation, Inc. This is free software : you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law. La clef secrète est disponible. pub 4096R/PUBKEYID créé : 2013-08-25 expire : 2019-08-24 utilisation : SC confiance : ultime validité : ultime sub 4096R/SECKEYID créé : 2013-08-25 expire : 2019-08-24 utilisation : E [ultime] (1). Test User

Le truc important ici est de taper toute la commande setpref (en fait, de la copier/coller

Remplacer votre clef

Bon, si votre clef est encore en 1024 ou 2048, remplacez là par une clef en 4096.

Une migration raisonnable se prévoit sur 3 mois environ. (premier jour) Créez une nouvelle clef d'une longueur de 4096 bits. Assurez vous d'avoir suivi les commandes décrites ci-dessus, en particulier en ce qui concerne les préférences de clefs. Envoyez cette clef aux serveurs publics et générez un certificat révocation que vous garderez en lieu sûr (une clef usb ne servant qu'à ça restant chez vous !) (premier jour) Signez votre nouvelle clef avec l'ancienne et non le contraire ; publiez la signature ; écrivez une manifeste de migration ; signez en clair avec la nouvelle et l'ancienne signature et publiez le dans un endroit que vous contrôlez (premier jour encore) Comme pour votre première clef, imprimez votre empreinte sur un papier pour le donner à vos proches. (du premier jour à la fin de la période définie) Collectez les signatures sur votre nouvelles clefs, afin de recréer un réseau de confiance. Parmi les moyens : chiffrofête locale ; événements (FOSDEM, RMLL, ...) ; en demandant à vos bonnes connaissances de signer votre nouvelle clef sur la base du manifeste signé et de la signature de la nouvelle clef par l'ancienne. (du premier jour à la fin de la période définie) Passez en revue votre trousseau de clef ; assurez vous que les propriétaires n'ont pas révoqués leurs clefs et pour ceux en qui vous avez assez confiance, signez leurs clefs avec la nouvelle. (avant la fin de la période définie) Assurez vous que votre clef a bien été déployée partout ou vous pourriez en avoir besoin. (à l'expiration de la période définie) Révoquez votre clef. Si vous n'avez pas de certificat de révocation, faites le maintenant. Vous pouvez également indiquer une expiration à votre clef (ce qui ne vous empêchera pas de la révoquer)