Le chiffrement, maintenant (6)

Le chiffrement du courriel avec PGP (Pretty Good Privacy)

En 1991, Phil Zimmermann a développé un logiciel de chiffrement des courriels qui s'appelait PGP, destiné selon lui aux militants anti-nucléaires, pour qu'ils puissent organiser leurs manifestations.

Aujourd'hui, PGP est une entreprise qui vend un logiciel de chiffrement propriétaire du même nom. OpenPGP est le protocole ouvert qui définit comment fonctionne le chiffrement PGP, et GnuPGP (abrégé en GPG) est le logiciel libre, 100% compatible avec la version propriétaire. GPG est aujourd'hui beaucoup plus populaire que PGP parce que tout le monde peut le télécharger gratuitement, et les cyberphunks le trouvent plus fiable parce qu'il est *open source*. Les termes PGP et GPG sont fréquemment employés l'un pour l'autre.

Malheureusement, PGP est notoirement difficile à utiliser. Greenwald en a donné l'exemple quand il a expliqué qu'il ne pouvait pas dans un premier temps discuter avec Snowden parce que PGP était trop difficile à installer.

Paires de clés et trousseaux

Comme pour l'OTR, chaque utilisateur qui souhaite envoyer ou recevoir des messages chiffrés doit générer sa propre clé PGP, appelée paire de clés. Les paires de clés PGP sont en deux parties, la clé publique et la clé privée (secrète).

Si vous disposez de la clé publique de quelqu'un, vous pouvez faire deux choses : chiffrer des messages qui ne pourront être

déchiffrés qu'avec sa clé privée, et vérifier les signatures qui sont générées avec sa clé secrète. On peut donner sans problème sa clé publique à tout le monde. Le pire qu'on puisse faire avec est de chiffrer des messages que vous seul pourrez déchiffrer.

Avec votre clé privée vous pouvez faire deux choses : déchiffrer des messages qui ont été chiffrés avec votre clé publique et ajouter une signature numérique pour vos messages. Il est très important que votre clé privée reste secrète. Un attaquant disposant de votre clé privée peut déchiffrer des messages qui ne sont destinés qu'à vous et peut fabriquer de faux messages qui auront l'air de venir de vous. Les clés privées sont généralement chiffrées avec une phrase secrète, donc même si votre ordinateur est compromis et que votre clé privée est volée, l'attaquant devra obtenir votre phrase secrète avant de pouvoir l'utiliser. Contrairement à OTR, PGP n'utilise pas la sécurité itérative. Si votre clé PGP privée est compromise et que l'attaquant dispose de copies de courriels chiffrés que vous avez reçus, il pourra donc tous les déchiffrer.

Comme vous avez besoin des clés publiques des autres personnes pour chiffrer les messages à leur intention, le logiciel PGP vous laisse gérer un trousseau de clé avec votre clé publique et celles de tous les gens avec qui vous communiquez.

Utiliser PGP pour le chiffrement des courriels peut s'avérer problématique. Par exemple, si vous configurez PGP sur votre ordinateur mais que vous recevez un courriel chiffré sur votre téléphone, vous ne pourrez pas le déchiffrer pour le lire avant d'être de retour sur votre ordinateur.

Comme OTR, chaque clé PGP possède une empreinte unique. Vous pouvez trouver une copie de ma clé publique ici, et mon empreinte est 5C17 6163 61BD 9F92 422A C08B B4D2 5A1E 9999 9697. Si vous jetez un coup d'œil à ma clé publique, vous allez voir qu'elle est très longue et qu'il sera difficile de

la lire sur un téléphone. Une empreinte est une version plus courte et moins contraignante de représenter une clé de manière unique. Avec ma clé publique, vous pouvez chiffrer des messages que je serais seul à pouvoir déchiffrer, tant que ma clé privée n'a pas été compromise.

Phrases secrètes

La sécurité de la crypto repose souvent sur la sécurité d'un mot de passe. Comme les mots de passes sont très facilement devinés par les ordinateurs, les cryptographes préfèrent le terme phrase secrète pour encourager les utilisateurs à créer leurs propres mots de passe, très long et sécurisés.

Pour obtenir des conseils sur la façon de choisir de bonnes phrases secrètes, consultez la section phrase secrète du livre blanc de l'EFF (NdT : Electronic Frontier Foundation, http://www.eff.org) "Défense de la vie privée aux frontières des USA : un guide pour les voyageurs qui transportent des terminaux numériques". Voyez aussi la page d'accueil de Diceware Passphrase.

Mais protéger vos clés privées PGP ne suffit pas : vous devez aussi choisir de bonnes phrases secrètes pour le chiffrement de vos disques et trousseaux de mots-de-passe.

Logiciels

Pour installer GPG, les utilisateurs de Windows peuvent télécharger Gpg4win, et les utilisateurs de Mac OS X GPGTools. Si vous utilisez GNU/Linux, GPG est probablement déjà installé. GPG est un programme en ligne de commande, mais il y a des logiciels qui s'interfacent avec les clients de messagerie, pour une utilisation simplifiée.

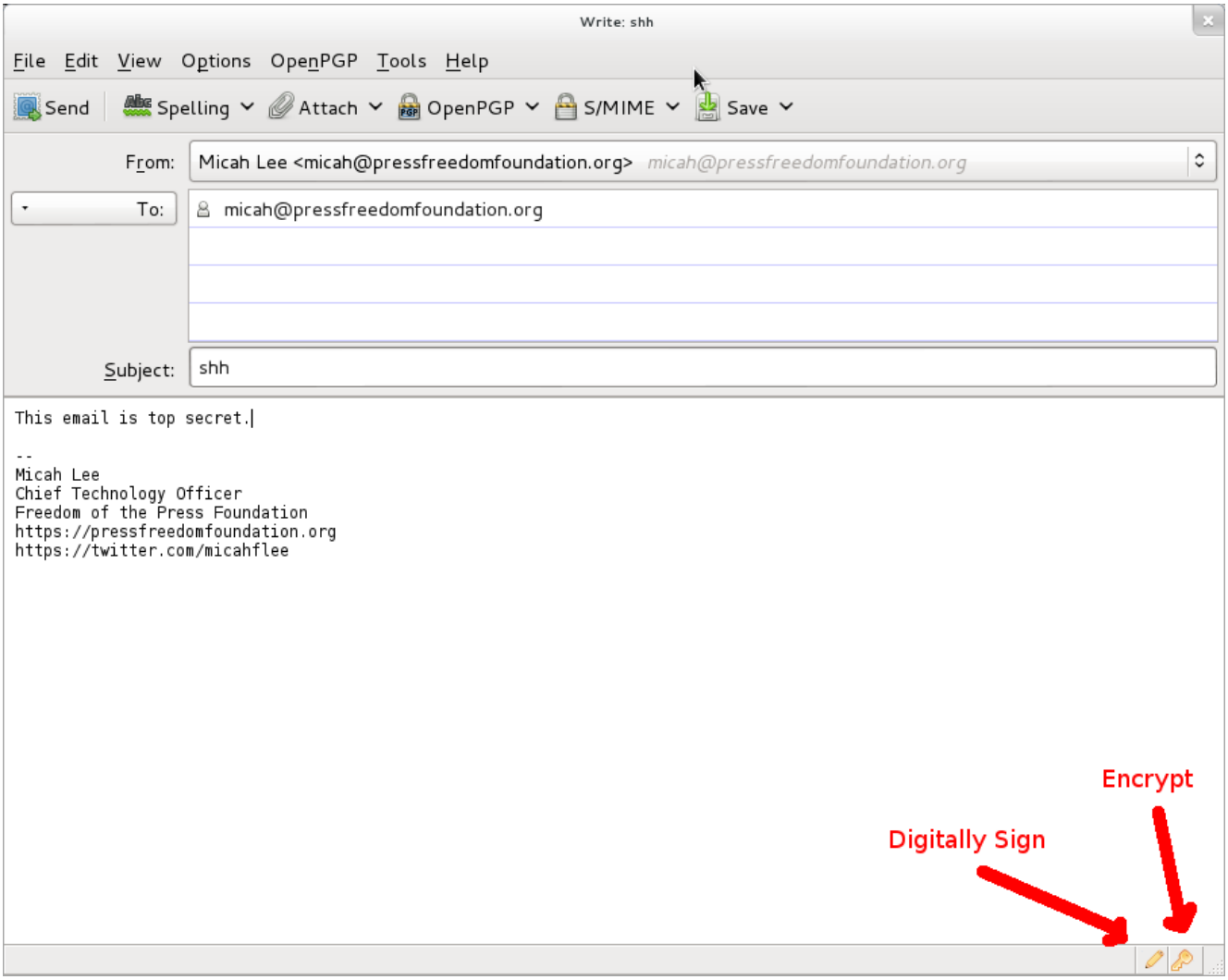
Vous devrez télécharger un client messagerie pour utiliser PGP correctement. Un client de messagerie est un programme sur votre ordinateur que vous ouvrez pour vérifier vos courriels,

contrairement à l’utilisation de votre navigateur web. La configuration PGP la plus populaire est le client de messagerie Thunderbird accompagné de l’add-on Enigmail. Thunderbird et Enigmail sont des logiciels libres disponibles sur Windows, Mac et GNU/Linux.

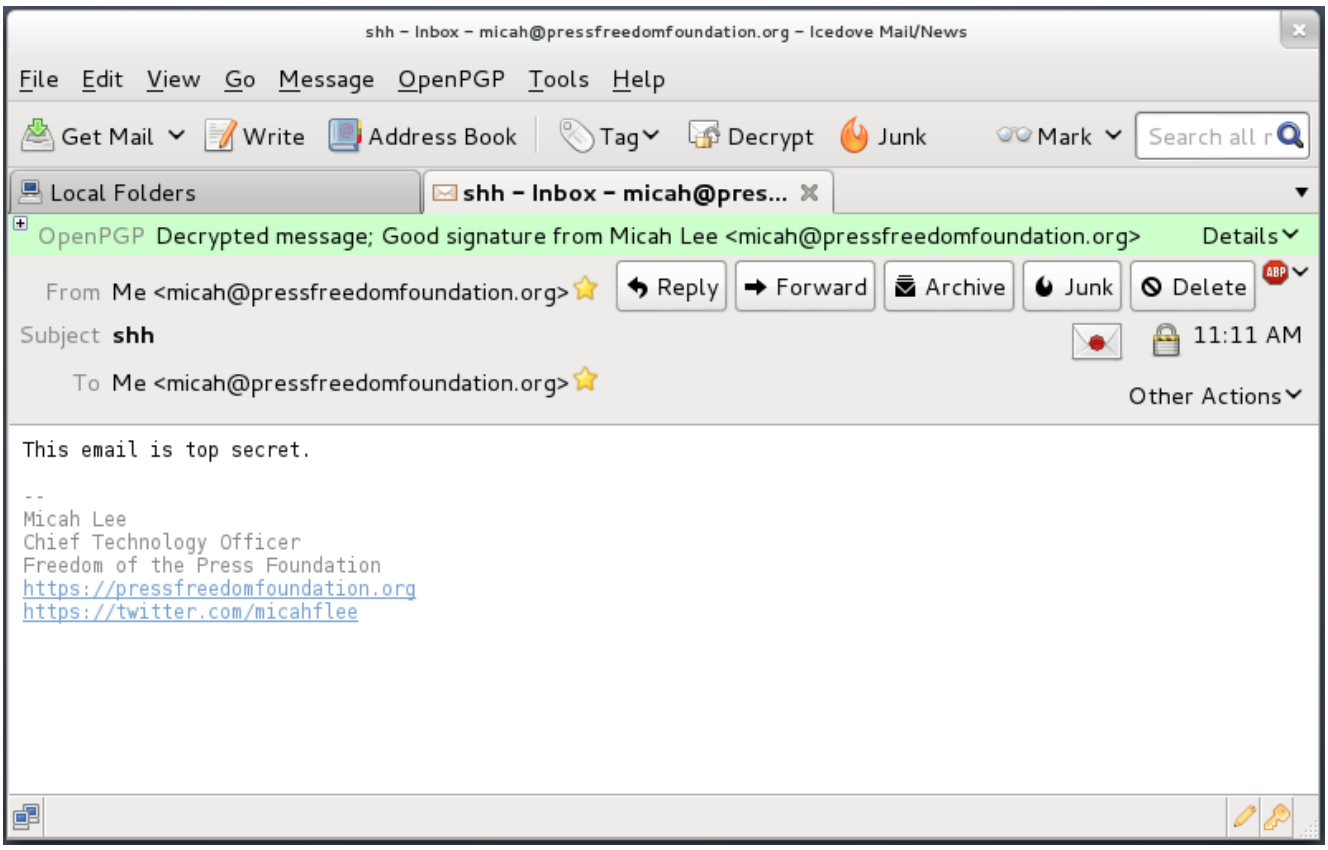
À l’heure actuelle, PGP est très difficile à utiliser de façon sécurisée à partir d’un navigateur web. Bien que quelques extensions de navigateurs existants puissent aider à le faire, je recommande de passer par un client de messagerie de bureau jusqu’à ce que le domaine de la crypto de navigateur mûrisse. Il est possible d’utiliser un chiffrement PGP avec Gmail, mais la façon la plus simple est de passer par un client de messagerie comme Thunderbird et de configurer votre compte Gmail à travers lui.

Chiffrement, déchiffrement, et signatures

Vous pouvez envoyer des courriels chiffrés et les signer numériquement en utilisant une interface utilisateur graphique via Thunderbird et Enigmail. Voici un exemple de courriel chiffré que je m’envoie à moi-même.



Quand je clique sur envoyer, mon logiciel prend le corps du message et le chiffre en utilisant ma clé publique, rendant son contenu incompréhensible pour les oreilles indiscrètes, y compris mon fournisseur de courriel.



Quand j'ai ouvert ce courriel, j'ai dû entrer ma phrase secrète de chiffrement pour le déchiffrer. Comme je l'avais chiffré en utilisant ma clé publique, le seul moyen que j'ai de le déchiffrer est d'utiliser ma clé privée. Comme ma clé privée est protégée par une phrase secrète, j'ai eu besoin de la taper pour déchiffrer temporairement ma clé privée qui est alors utilisée pour déchiffrer le message.

PGP n'est pas limité aux courriels

Bien que PGP soit principalement utilisé pour chiffrer les courriels, rien ne vous empêche de l'utiliser pour chiffrer autre chose et le publier en utilisant n'importe quel support. Vous pouvez poster des messages chiffrés sur les blogs, les réseaux sociaux et les forums.

Kevin Poulsen a publié un message PGP chiffré sur le site web de Wired à l'attention d'Edward Snowden. Aussi longtemps que Wired aura une copie de la vrai clé publique de Snowden, seul quelqu'un en possession de la clé privée de Snowden pourra déchiffrer ce message. Nous ne savons pas comment Wired a

obtenu une copie de cette clé publique.

Voici un message qui a été chiffré avec ma clé publique. Sans avoir accès à ma clé privée associée, la NSA ne sera pas en mesure de casser ce chiffrage (chère NSA, faites-moi savoir si vous avez réussi à le faire).

-----BEGIN PGP MESSAGE----- Version: GnuPG v1.4.12 (GNU/Linux)
hQIMA86M3VXog5+ZAQ//Wep9ZiiCMSmLk/Pt54d2wQk07fjxI4c1rw+jfkKQAi4n
6HzrX9YIbgTukuv/0Bjl+yp3qcm22n6B/mk+P/3Cbxo+bW3gsq5OLFNenQO3RMNM
i9RC+qJ82sgPXX6i9V/KszNxAyfegbMseoW9FcFwViD14giBQwA7NDw3ICm89PTj
y+YBMA50iRqdErmACz0fHfA/Ed5yu5cOVVa8DD12/upTzx7i0mmkAxwsKiktEaKQ
vg8i1gvzqeymWYnckGony08eCCIZFc78CeuhODy0+MXyrnBRP9p++fcQE7/GspKo
SbxVT3evwT2UkebezQT2+AL57NEnRsJzsgQM4R0sMgvZI7I6kfWKerhFMt3imSt1
QGphXmKZPRvKqib59U57GsZU1/2CMIlYBVMTZIpYKRh6NgE8ityaa4gehJDl16xa
pZ8z3DMNt3CRF8hqWmJNUfDwUvXBEk8d/8Lkh39/IFHbWqNJh6cgq3+CipXH5HjL
iVh7tzGPfB6yn+RETzcZjesZHtz4hFudOxTMV0YnTIv0FGtfxsfEQe7ZVmmfqGNG
glxE0EfbXt0psLXngFMneZYBJqXGFsK3r5bHjRm6wpC9EDAzXp+Tb+jQgs8t5eWV
xiQdBpNZnjnGiIOASOxJrIRuzbTjo389683NfLvPRY8eX1iEw58ebjLvDhvDZ2jS
pwGuWuJ/8QNZou1RfU5QL0M0SEe3ACm4wP5zfUGnW8o1vKY9rK5/9evIiA/DMAJ+
gF20Y6WzGg4llG9qCAnBkc3GgC7K1zkXU5N1VD50Y0qLoNsKy6eengXvmiL5EkFK
RnLtP45kD2rn6iZq3/Pnj1IfPonsdaNttb+2fhpFWa/r1sUyYadWeHs72vH83MgB I6h3Ae9ilF5tYLs2m6u8rKFM8zZhixSh =a8FR -----END PGP MESSAGE-----

Contrôle d’identité

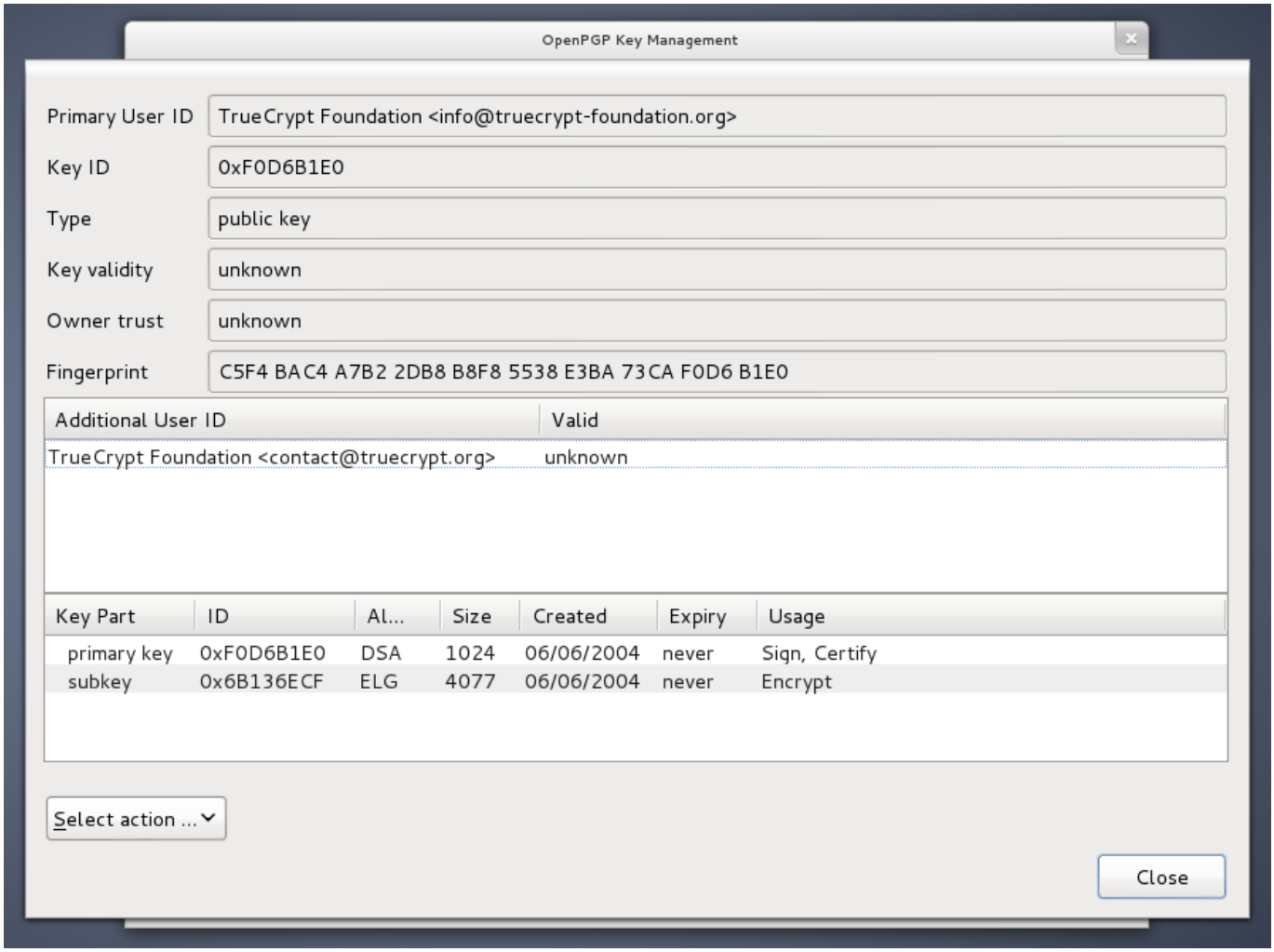
Comme avec l’OTR, il est important de vérifier les clés PGP

des personnes avec qui vous communiquez. Avec PGP, vous faites cela en utilisant votre clé privée pour signer numériquement la clé publique de quelqu'un d'autre.

Depuis Thunderbird, cliquez sur le menu OpenPGP et ouvrez le gestionnaire de clé. Cochez la case « afficher toutes les clés par défaut » pour voir toutes les clés de votre trousseau. De là, vous pouvez importer des clés à partir de fichiers, de votre presse-papier ou de serveurs de clés. Vous pouvez aussi générer une nouvelle paire de clé et voir le détail de toutes les clés de votre trousseau.

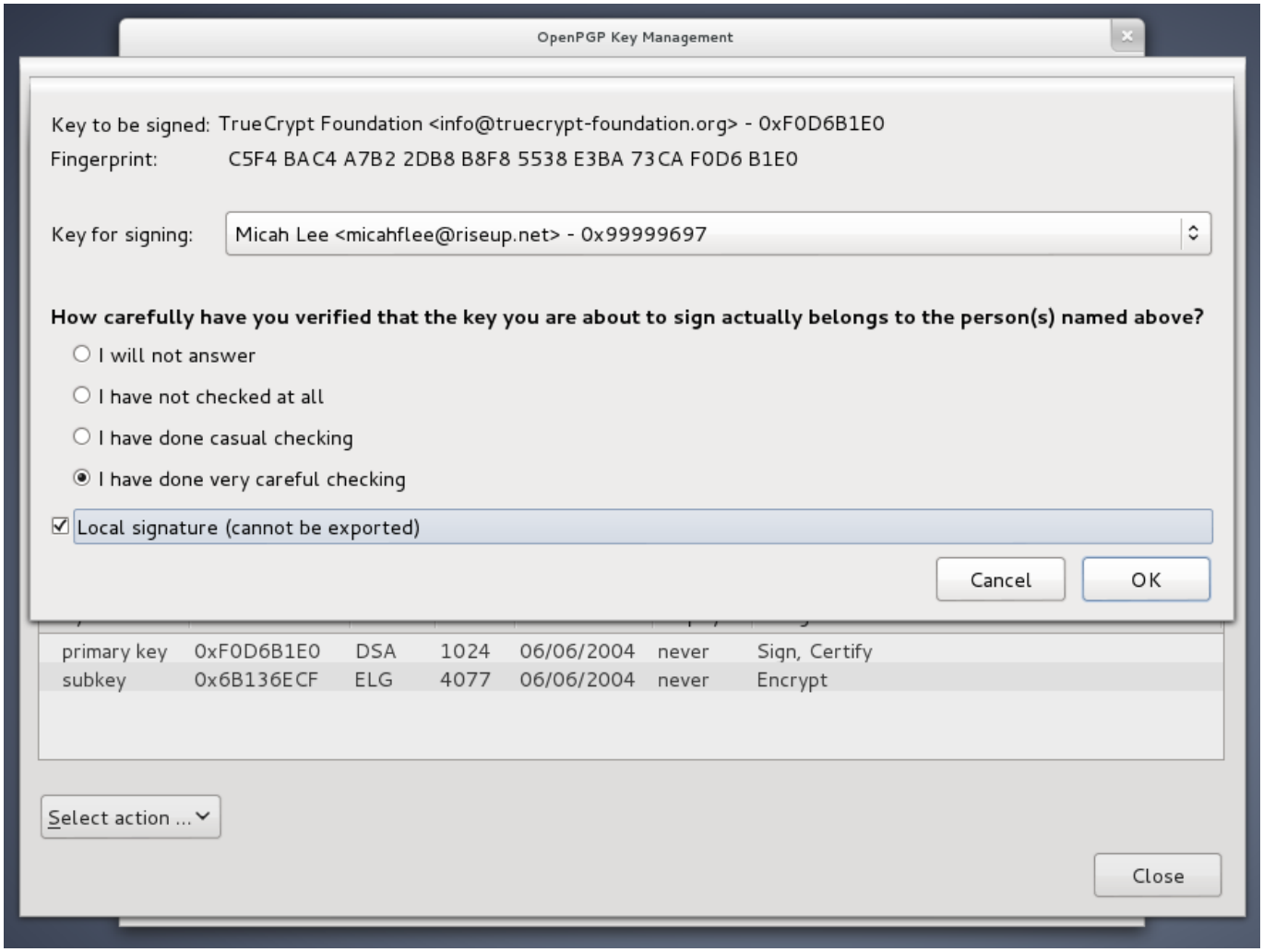
Comme avec les clés OTR, chaque clé PGP a une empreinte unique. Et comme pour OTR, vous avez besoin d'afficher l'intégralité de l'empreinte pour être sûr que la clé publique que vous êtes en train de regarder est bien celle de la personne à qui vous pensez qu'elle appartient.

Faites un clic droit sur une clé de cette liste et choisissez « détailler » pour voir son empreinte. Voici le détail de la clé PGP que le logiciel de chiffrement TrueCrypt utilise pour signer numériquement les r*eleases* de son logiciel.



Toujours comme OTR, vous avez besoin de vous rencontrer en personne, parler au téléphone ou utiliser une session OTR déjà vérifiée pour comparer chaque caractère de l'empreinte.

Après avoir vérifié que la clé publique dont vous disposez appartient bien à la personne que vous pensez, cliquez sur « choisir une action » et sélectionnez « Signer la clé ».



Sur la capture d'écran ci-dessus, j'ai coché la case « signatures locales (ne peuvent pas être exportées) ». De cette façon, vous pouvez signer les clé PGP, ce qui est nécessaire pour Enigmail et d'autres logiciels PGP pour afficher des messages de sécurité sensés, mais vous ne risquez pas de dévoiler accidentellement avec qui vous communiquez à un serveur de clés PGP.

Si vous recevez un courriel chiffré de quelqu'un que vous connaissez mais que le courriel n'est pas signé numériquement, vous ne pouvez pas être sûr qu'il a vraiment été écrit par la personne à laquelle vous pensez. Il est possible qu'il provienne de quelqu'un qui falsifie son adresse de courriel ou que son compte courriel soit compromis.

Si votre ami vous dit dans son courriel qu'il a généré une nouvelle clé, vous devez le rencontrer en personne ou lui parler au téléphone et inspecter l'empreinte pour être certain

que vous n’êtes pas victime d’une attaque.

Attaques

Si vous ne vérifiez pas les identités, vous n’avez pas la possibilité de savoir si vous n’êtes pas victime d’une attaque de l’homme du milieu (MITM).

Le journaliste du Washington Post Barton Gellman, à qui Edward Snowden a confié des informations à propos du programme PRISM de la NSA, a écrit ceci à propos de son expérience dans l’utilisation de PGP.

> *Le jeudi, avant que The Post ne publie la première histoire, je l’ai contacté sur un nouveau canal. Il ne m’attendait pas à cet endroit et m’a répondu alarmé. « Je te connais ? » a-t-il écrit.*
>
> *Je lui ai envoyé un message sur un autre canal pour vérifier mon « empreinte » numérique, une sécurité qu’il prennait depuis quelque temps. Fatigué, je lui en ai envoyé une mauvaise. « Ce n’est pas du tout la bonne empreinte », m’a-t-il dit, se préparant à se déconnecter. « Vous êtes en train de faire une attaque de MITM». Il parlait d’une attaque de type « homme du milieu », une technique classique de la NSA pour contourner le chiffrement. J’ai immédiatement corrigé mon erreur.*

Snowden avait raison de prendre des précautions et d’insister sur le fait qu’il vérifiait la nouvelle empreinte PGP de Gellman. PGP, s’il est bien utilisé, fournit les outils nécessaires pour éviter les attaques de l’homme du milieu. Mais ces outils ne fonctionnent que si les utilisateurs sont vigilants lors des vérifications d’identité.